HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Security Day 2011

Pentests:
Exposing real world attacks

Renaud Dubourguais <Renaud.Dubourguais@hsc.fr>
Jean-Baptiste Aviat <Jean-Baptiste.Aviat@hsc.f>

Hervé Schauer Consultants

- **Information security consulting company since 1989**
- **Fully independent intellectual expertise services**
  - Free of any distribution, integration, outsourcing, staff delegation or third-party investors biases
- **Services: consulting, research, audit, penetration tests, training**
- **Field of expertise**
  - OS Security : Windows, Unix ,Linux and embedded components
  - Application security
  - Network security
  - Organizational security
- **Consultants certifications :**
  - CISSP, ISO 20000-1 Lead Auditor, ISO 27001 Lead Auditor, ISO 27001 Lead Implementor, ISO 27005 Risk Manager, ITIL, ProCSSI, GIAC GCFA

What is a pentest?

- **Simulation of a real attack on:**
  - Infrastructure by exploiting badly designed firewall rules, exposed services, ...
  - Exposed Web applications by testing user inputs, application bugs, …
- **Mainly from two point of view:**
  - Blackbox, without information about the remote infrastructure, just a URL
  - Greybox, with a user account
- **Various purposes:**
  - Security assessment
  - Decision makers awareness
  - Technical staff awareness

Security assessment (1/3)

- **Assess the global security level of your infrastructure:**
  - Applications
  - Network
  - Websites...

- **Technical skills needed:**
  - Dedicated to real hackers
  - Or accessible to script kiddies ?

Security assessment (2/3)

- **Pentest** should not to be mistaken with v**ulnerability scanning** or vulnerability assessment.

  Vulnerability scanning (Qualys, Rapid7, Nessus...) is cheap and automated but :

  - Results are not **confirmed** by a **human** assessor
  - Does not necessarily **prove** that a vulnerability is there and actually **exploitable** (lots of 'might/could be vulnerable' in reports)
  - Can not look for for tricky vulnerabilities in **web applications** in an efficient and useful way
  - Can not **bounce** (from a compromised system to a vulnerable one) to prove that more systems are at risk
  - Has no notion of **business risk** (all vulnerabilities considered the same)
  - Are tools for regulatory and compliance, but not the ones used by hackers to penetrate systems
- This presentation is about **real pentests**, simulating **real-world attacks**

Security assessment (3/3)

- **Issues usually summarized in a table:**

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

Technical staff awareness

- **Provide technical details about the intrusion in order to:**
  - Reproduce attacks
  - Check vulnerability corrections

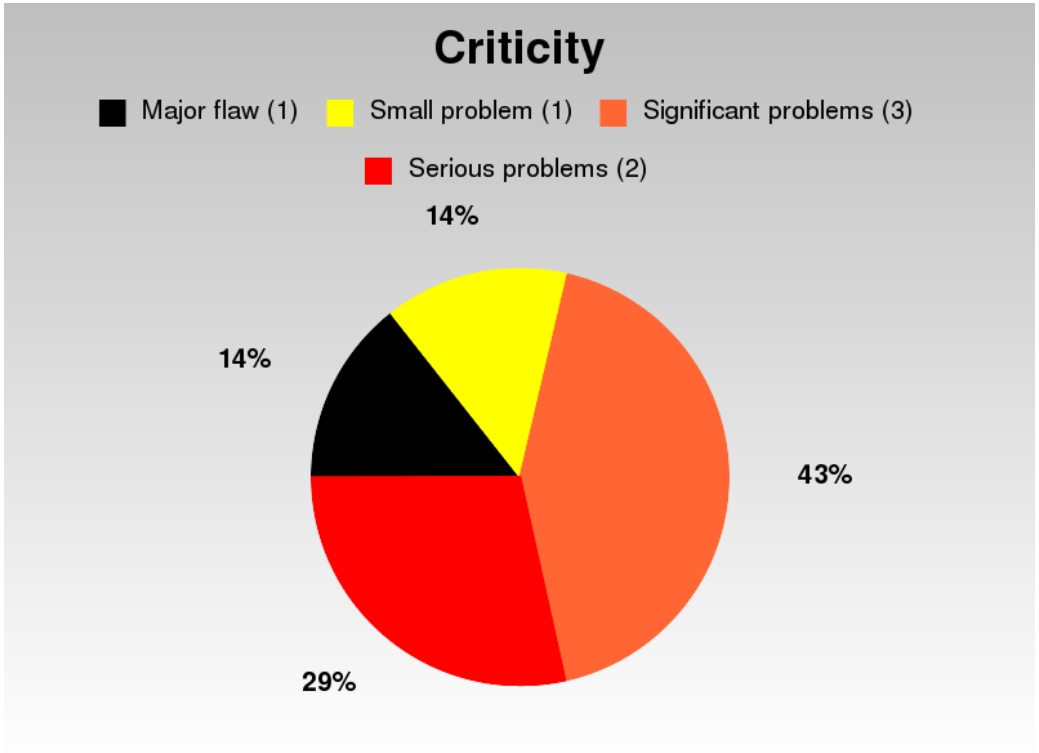
- **Give concrete recommendations for each vulnerability:**
  - Best pratices to fix it
  - And both:
    - State of the art practices
    - Pragmatic options to fix the issues

```
  memcpy(new->pktrtp.pcap.pkt, pktrtp->pcap.pkt, pktrtp
                      >pcap.hdr.caplen);
  new->pktrtp.len = pktrtp->len;


  if (rtp_stream->pkts.lh_first == NULL)
    {
      LIST_INSERT_HEAD(&rtp_stream->pkts, new,l);
    }
  else
    {
      if (before)
        {
          LIST_INSERT_BEFORE(before, new, l);
        }
      else
        {
          if (after)
            LIST_INSERT_AFTER(after, new, l);
          else FATAL("buffer not empty and before,after
NULL");
        }
    }
```

Decision makers awareness

- **Pentests are not relevant only to technical staff**
- **Decision makers want to know:**
  - Do we have vulnerabilities ?
  - Are they easy to exploit ?
  - Are they easy to fix ?
  - How good (or bad) are they related to other similar companies ?



Case study

Single information provided to the pentesters :

http://www.equivalency.co.uk

At first sight

EQUIVALENCY

TEMPLATE DESIGN BY FREE CSS TEMPLATES

Home » | Blog » | Photos » | About » | Links » | Contact »

WELCOME TO EQUIVALENCY

POSTED BY SOMEONE ON OCTOBER 8, 2010 • COMMENTS (64) • FULL ARTICLE

This is **Equivalency** , a free, fully standards-compliant CSS template designed by FreeCssTemplates for Free CSS Templates. Photos used in this template is from PDPhoto.org. This free template is released under a Creative Commons Attribution 3.0 license, so you're pretty much free to do whatever you want with it (even use it commercially provided you keep the links in the footer intact. Aside from that, have fun with it.

READ MORE | COMMENTS

GO

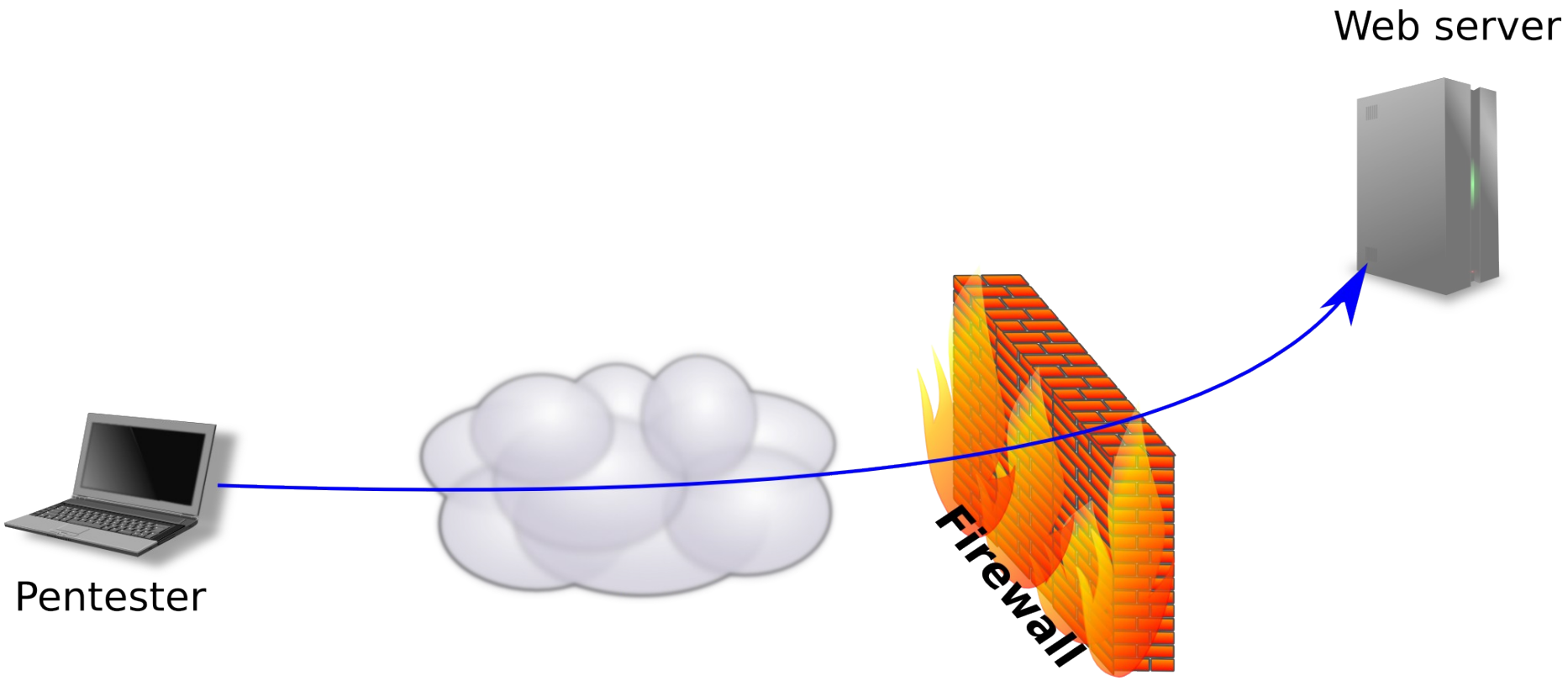
ALIQUAM TEMPUS

Mauris vitae nisl nec metus placerat perdiet est. Phasellus dapibus semper consectetuer hendrerit.

CATEGORIES

- Aliquam libero
- Consectetuer adipiscing elit
- Metus aliquam pellentesque
- Suspendisse iaculis mauris
- Urnanet non molestie semper
- Proin gravida orci porttitor

Guessing the infrastructure...



After browsing for a few minutes

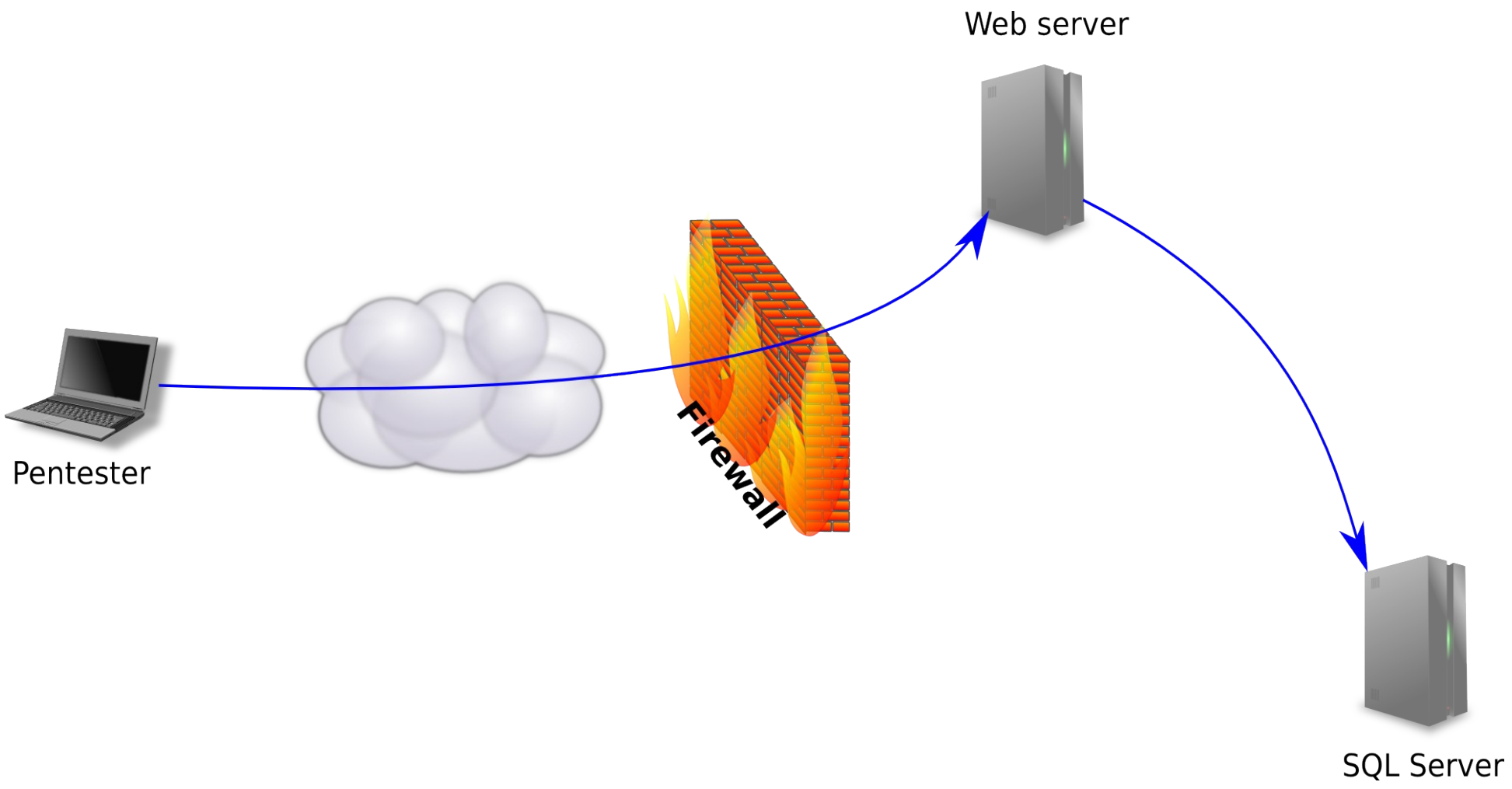
WELCOME TO EQUIVALENCY

POSTED BY SOMEONE ON OCTOBER 8, 2010 • COMMENTS (64) • FULL ARTICLE

SQL Error: Syntax error (missing operator) in query expression 'SELECT id, username FROM cmd_users WHERE [...]'.

READ MORE | COMMENTS

What does it look like now?



SQL Injection issue

- **Possibility to extract database information:**
  - Using a custom script
  - No sensitive information on such a website
  - Except for the user accounts authorized to edit content

Demonstration

In the vulnerabilities summary...

- Looks like an SQL injection flaw !

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

Weak passwords policy

- **Retrieved accounts passwords are encrypted**
  - To be precise : they are 'hashed' ('one-way encryption')
- **If some of them are simple:**
  - They can be retrieved !

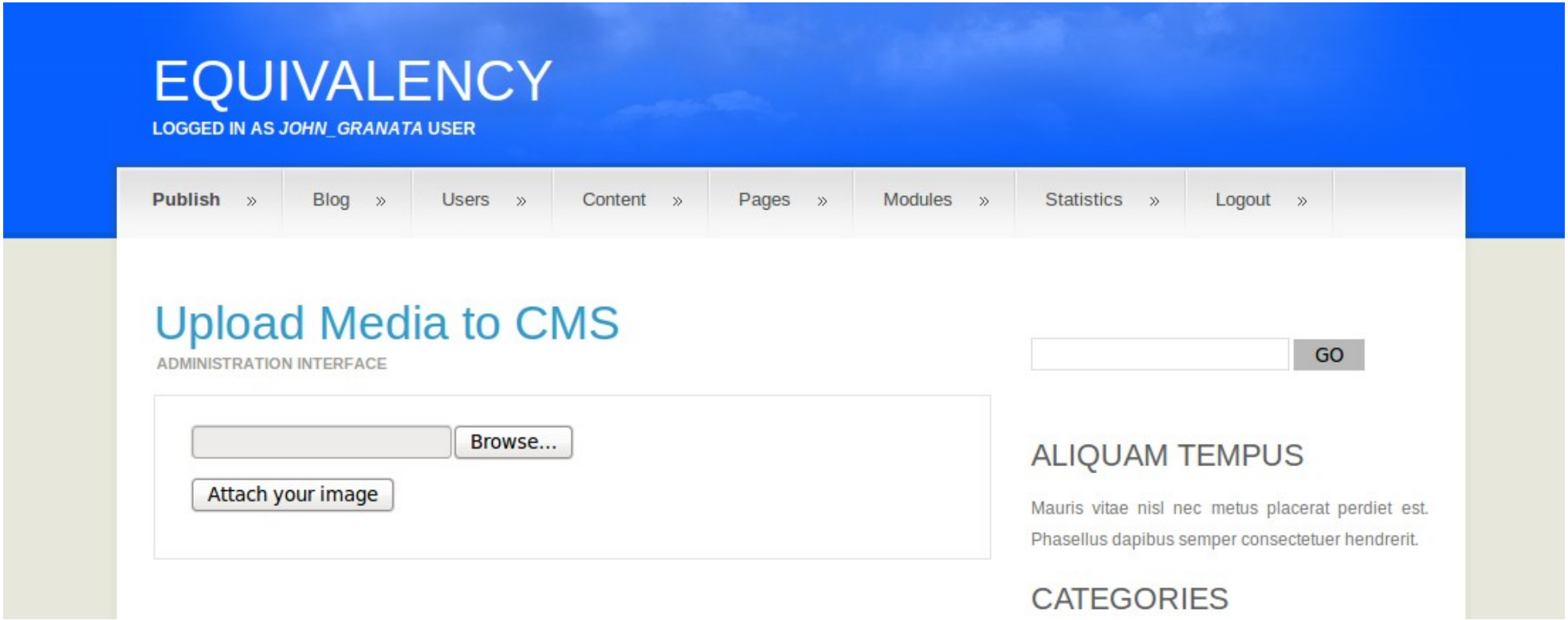
Demonstration

In the vulnerabilities summary...

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

No filtering on file extensions (1/2)

- **Editing users are allowed to upload images**



No filtering on file extensions (2/2)

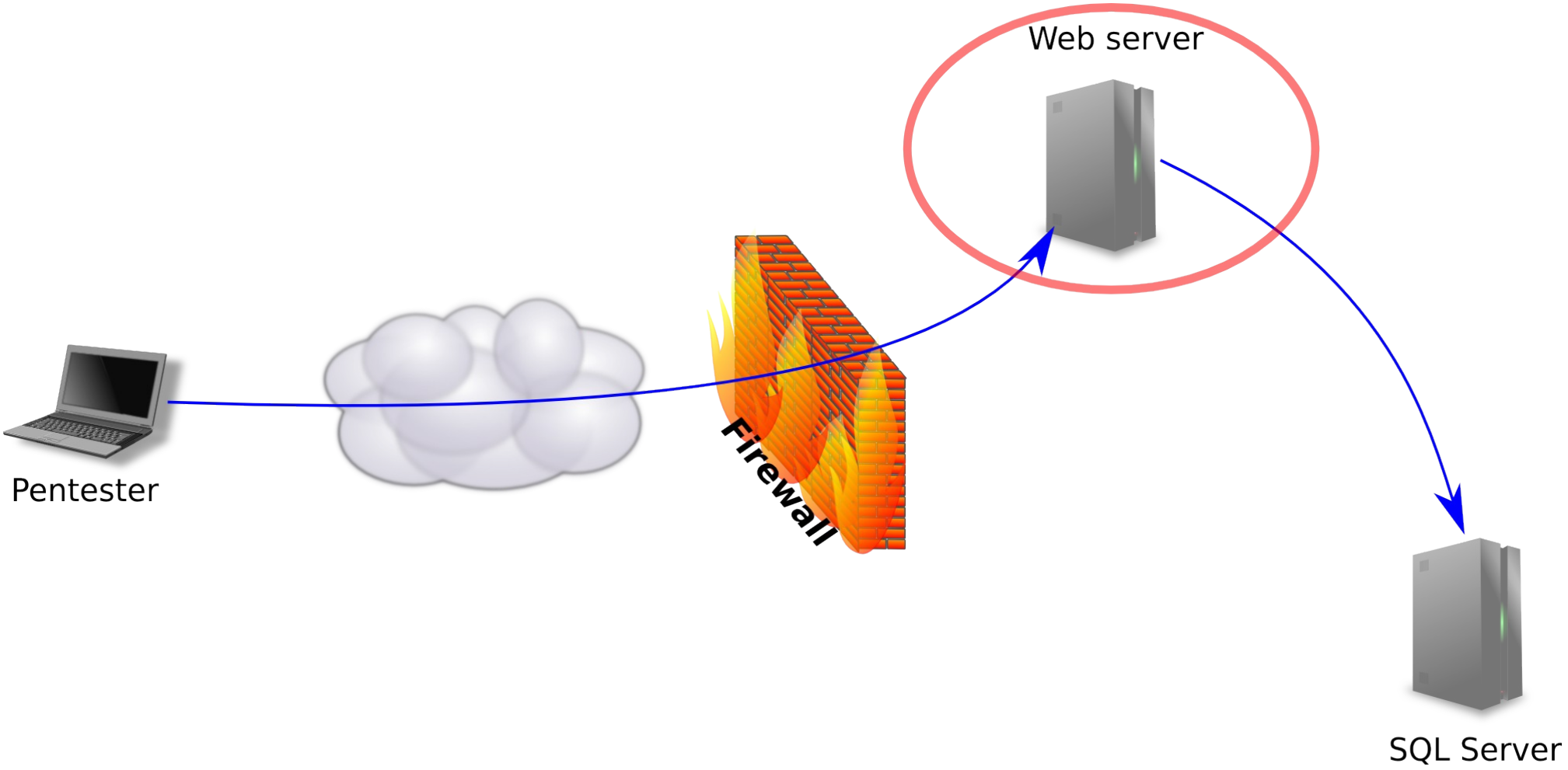
- **Instead of uploading an image:**
  - Let's upload an executable ASP script
- **Which can act as an interface to the operating system**
  - Public webshells are easy to found (c99.php, r57.php, …)
  - HSC consultants developed their own webshell

Demonstration

In the vulnerabilities summary...

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

Where are we now?



Bounce to the SQL Server

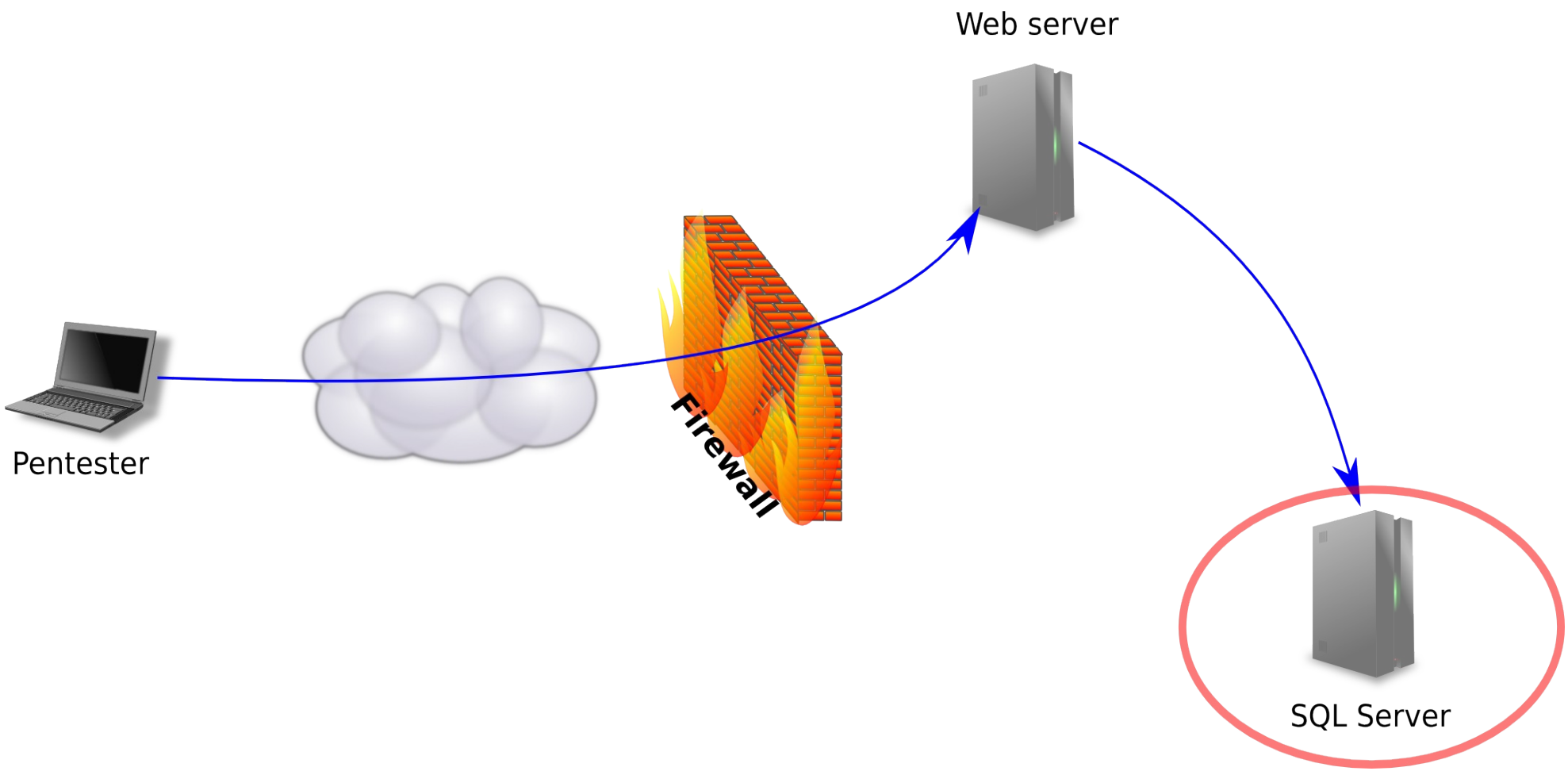
- **LocalSystem user can extract hashes from the system**
  - Public tools exist (fgdump.exe)
  - But also private tools (forestdump for HSC)
- **Such hashes can be broken**
  - Using 'Rainbow tables'
- **If a local account is shared accross servers:**
  - We can bounce to them !

Demonstration

In the vulnerabilities summary...

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

Where are we now?



Compromising the Active Directory

- **Domain controllers can be identified by querying a DNS record**

```
$ dig SRV @192.168.111.110 _ldap._tcp.dc._msdcs.hsc.local
[...]
;; ANSWER SECTION:
_ldap._tcp.dc._msdcs.hsc.local.      600 IN  SRV     0 100 389 win2003-ad.hsc.local.

;; ADDITIONAL SECTION:
win2003-ad.hsc.local. 3600    IN      A       192.168.111.110
```

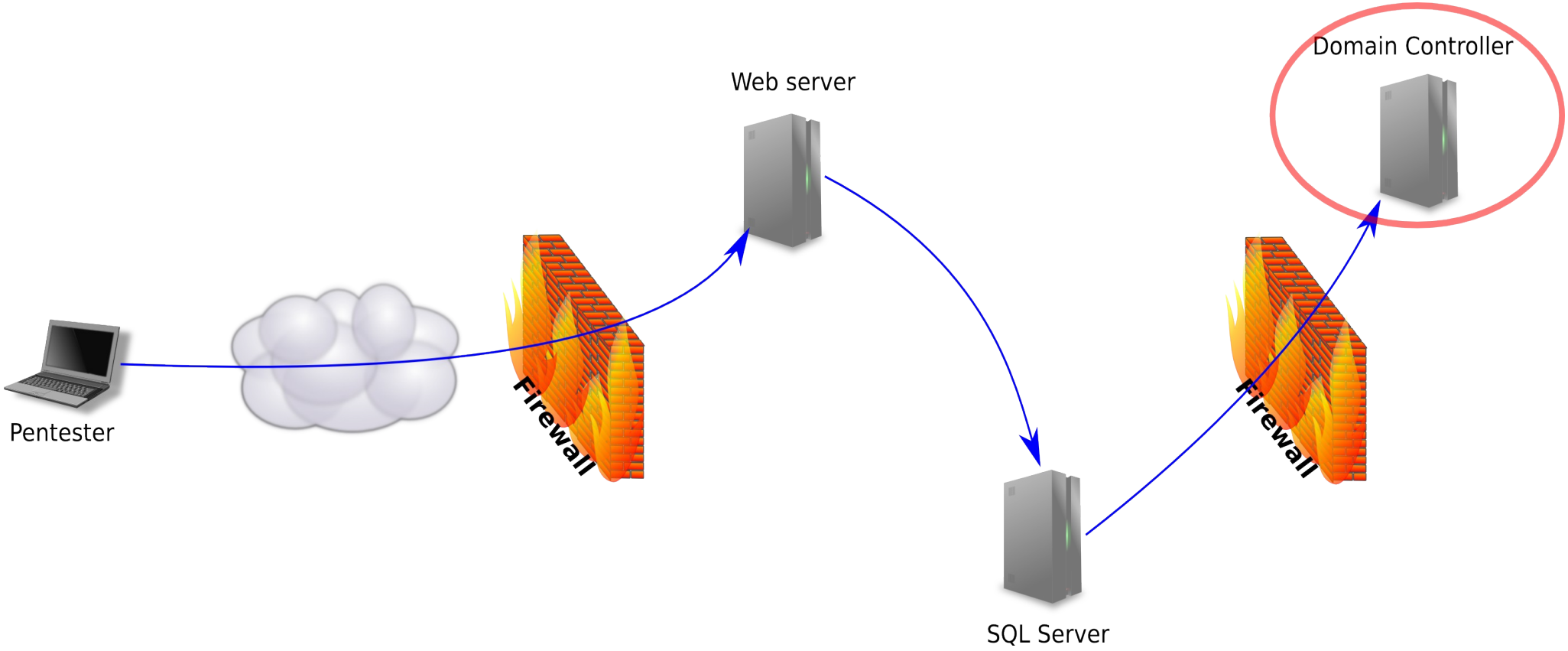
- **If a critical vulnerability hasn't yet been patched:**
  - It can be exploited to take control of the system
  - MS06-040 (netapi), MS08-067 (netapi) , MS10-46 (LNK), ...

Demonstration

In the vulnerabilities summary...

Vulnerability or significant element		Exploitation complexity	Associated risk	Criticity	Recommendation
Patch policy	Server out of date	2	Server takeover	B	Keep servers up to date
Web Application	Wrong parameters filtering	3	Information leaks	R	Filter user inputs
Web Application	No file extension filtering	2	Server takeover	R	Perform whitelist filtrering on uploaded files
User management	Accounts share the same password	1	Bounce accross servers	O	Use unique passwords
Passwords policy	Weak user password	2	User account thief	O	Force users to use strong passwords
Network filtering	Weak DMZ filtering	N/A	Compromized servers may reach unnecessary services on some hosts	O	Review firewall rules
Web application	Debug messages shown to user	N/A	Technical information leak	Y	Do not use debug mode on production applications

Where are we now?



Conclusion

- **Increasing number of attacks against web applications**
  - A vulnerability can be created by mistake very quickly :
    - Unfiltered user inputs, weak passwords, unpatched software…
  - Exploitation techniques are now mature
  - Impact can be disastrous :
    - Leak of confidential data
    - Servers and applications compromised or vandalized
    - …
- **Pentests make you aware of the issues before the real hackers...**