

Séquences d'une attaque



Prise d'empreinte

- Rechercher un maximum d'informations sur les équipements, les applications et les personnels de la cible par le biais de sources ouvertes



« Google Hacking »

Rechercher des informations dans :

- les articles de blog, les réseaux sociaux, des communiqués de presse, etc...
- les fichiers (pdf, docx, logs...) indexés
- les messages d'erreur qui permettraient de caractériser les moyens techniques en place.

« Google Hacking »

Opérateurs de base

- (-) : recherche en excluant un terme
apple pie VS apple -pie
- (" ") recherche d'une expression exacte
Jean lachose VS "Jean lachose"
- (~) recherche en fonction des synonymes du terme
~voiture
- (.) recherche avec un caractère joker dans le mot
m.téo

« Google Hacking »

- Un « Google Dork » est une signature typique d'une technologie Web parmi tout ce qui est indexé par Google.

Site de référence:

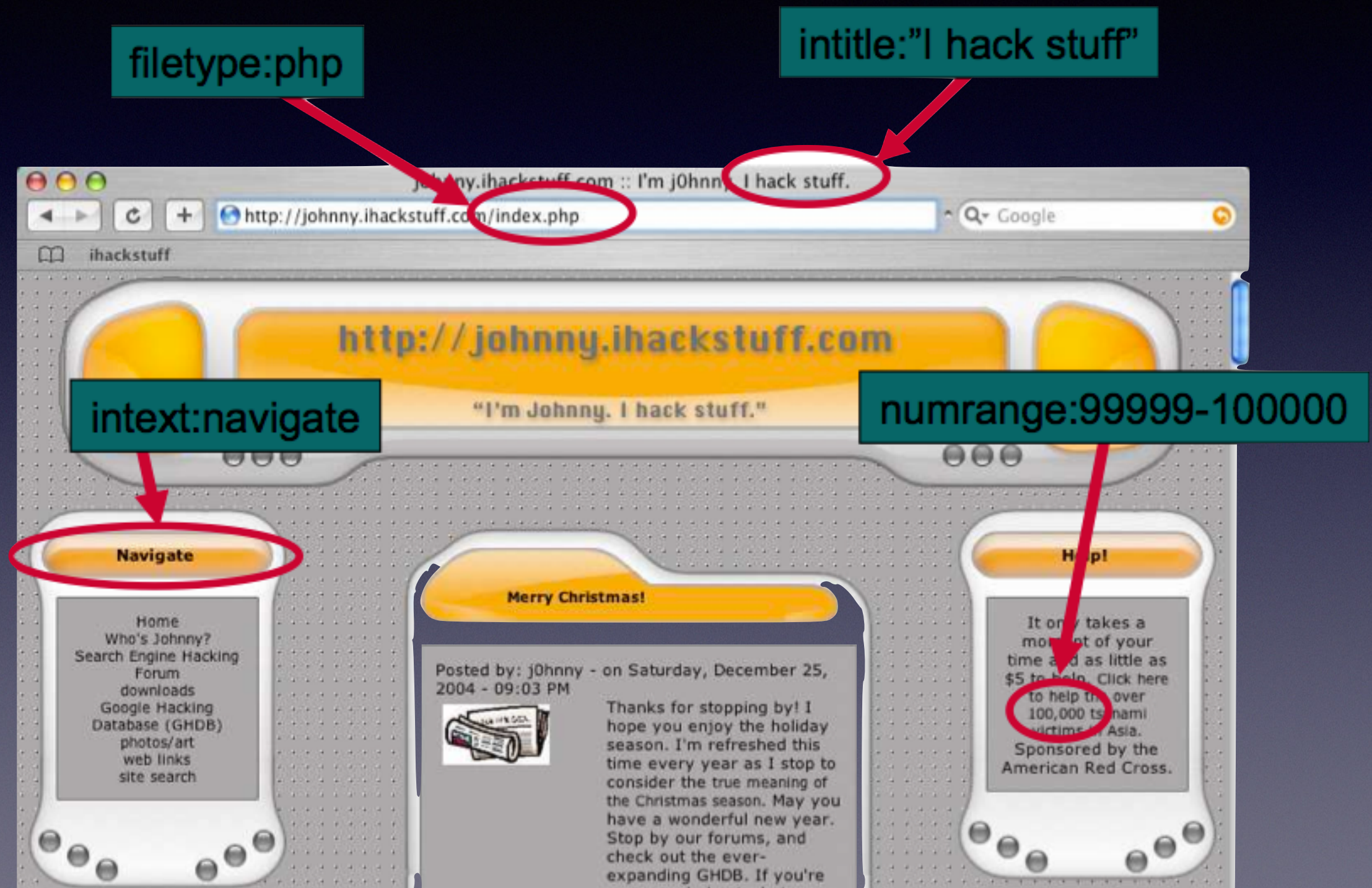
<https://www.exploit-db.com/google-hacking-database/>

« Google Hacking »

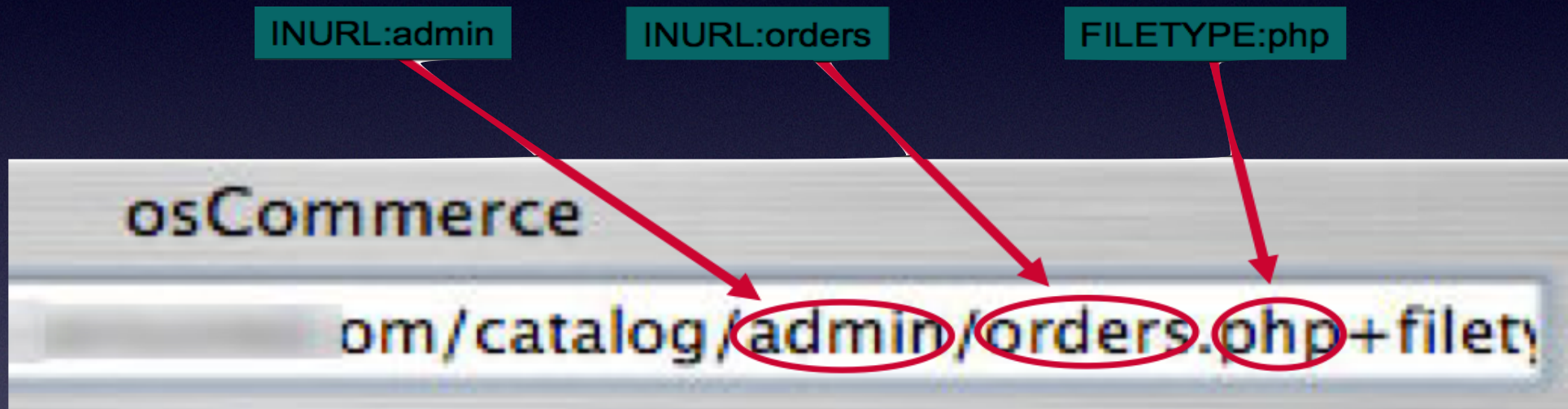
Opérateurs avancés

- allintext:
- allintitle:
- allinurl:
- bphonebook:
- cache:
- define:
- filetype:
- info:
- intext:
- intitle:
- inurl:
- link:
- phonebook:
- related:
- rphonebook:
- site:
- numrange:
- daterange

« Google Hacking »



« Google Hacking »



« Google Hacking »

- **intitle:hacking** : recherche les pages web contenant le mot « hacking » dans leur titre
- **inurl:login** : recherche les pages contenant l'occurrence « login » dans leur url
- **intext:"md5 reverse hash"** : recherche les pages contenant la phrase « md5 reverse hash » dans leur corps
- **link:www.blackhat.com** : recherche les pages web contenant un lien vers www.blackhat.com
- **filetype:log** : recherche les fichiers dont le type ou l'extension est « log »

« Google Hacking »

- `site:www.sans.org` : fourni l'ensemble des pages indexées du site `www.sans.org`
- `intitle:"index of" inurl:admin` : permet de rechercher l'ensemble des répertoires visités par Google ayant le mot « admin » dans leur url
- `intext: "enable password 7"`
- `Filetype:sql "insert into" (pass|passwd|password)`
- `inurl:viewer_index.shtml`



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Search

SEARCH

Date	Title	Category
2016-07-20	site:static.ow.ly/docs/ intext:@gmail.com Password	Files containing passwords
2016-07-15	inurl:DiGIR.php	Files containing juicy info
2016-07-07	filetype:sql intext:wp_users phpmyadmin	Files containing juicy info
2016-07-07	intext:"Dumping data for table `orders`"	Sensitive Online Shopping Info
2016-07-04	"Index of /wp-content/uploads/backupbuddy_backups" zip	Files containing juicy info
2016-07-04	"index of" bigdump.php	Advisories and Vulnerabilities
2016-07-01	intext: "/LM/W3SVC/" ext:asp	Files containing juicy info
2016-07-01	intext: "/showme.asp" HTTP_ACCEPT	Files containing juicy info
2016-06-29	inurl:top.htm inurl:currenttime	Various Online Devices
2016-06-23	intext: "Hello visitor from" ext:asp	Advisories and Vulnerabilities

Footholds (49)

Examples of queries that can help a hacker gain a foothold into a web server

Sensitive Directories (118)

Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to uber-secret!

Vulnerable Files (62)

HUNDREDS of vulnerable files that Google can find on websites...

Vulnerable Servers (83)

These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Error Messages (93)

Really retarded error messages that say WAY too much!

Network or vulnerability data (63)

These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!

Various Online Devices (307)

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Web Server Detection (77)

These links demonstrate Google's awesome ability to profile web servers..

Files containing usernames (17)

These files contain usernames, but no passwords... Still, google finding usernames on a web site..

Files containing passwords (199)

PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Sensitive Online Shopping Info (11)

Examples of queries that can reveal online shopping info like customer data, suppliers, orders, creditcard numbers, credit card info, etc

Files containing juicy info (366)

No usernames or passwords, but interesting stuff none the less.


Pages containing login portals (372)

These are login pages for various services. Consider them the front door of a website's more sensitive functions.

Advisories and Vulnerabilities (1995)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

inurl:"NetworkConfiguration" cisco



Device Information

Network Configuration

Network Statistics

Ethernet

Port 1 (Network)

Port 2 (Access)

Port 3 (Phone)

Device Logs

Debug Display

Stack Statistics

Status Messages

Streaming Statistics

Stream 1

Stream 2

Network Configuration


Cisco Systems, Inc. IP Phone CP-7960 (SEP0007EBBA6208)

DHCP Server	255.255.255.255
BOOTP Server	No
MAC Address	0007EBBA6208
Host Name	SEP0007EBBA6208
Domain Name	
IP Address	207.235.20.26
Subnet Mask	255.255.255.224
TFTP Server 1	69.26.218.218
Default Router 1	207.235.20.1
Default Router 2	
Default Router 3	
Default Router 4	
Default Router 5	
DNS Server 1	207.235.20.7
DNS Server 2	207.235.20.9
DNS Server 3	
DNS Server 4	
DNS Server 5	
Operational VLAN Id	
Admin. VLAN Id	
CallManager 1	69.26.218.218 Active
CallManager 2	0.0.0.0
CallManager 3 SRST	207.235.20.1 Standby
CallManager 4	
CallManager 5	
Information URL	http://66.226.209.123/ciscoportal/InformationServlet
Directories URL	http://66.226.209.123/ciscoportal/DirectoriesServlet

inurl:"8080/jmx-console"

inurl:"8080/jmx-console" - ... JBoss JMX Management C...

66.194.51.227:8080/jmx-console/index.jsp



JMX Agent View orscheduler

ObjectName Filter (e.g. "jboss:*", "*:service=invoker,*") :

Catalina

- [type=Server](#)
- [type=StringCache](#)

JMImplementation

- [name=Default,service=LoaderRepository](#)
- [type=MBeanRegistry](#)
- [type=MBeanServerDelegate](#)

jboss

- [database=localDB,service=Hypersonic](#)
- [service=ClientUserTransaction](#)
- [service=DynamicLoginConfig](#)
- [service=JNDIView](#)
- [service=Mail](#)
- [service=Naming](#)
- [service=TransactionManager](#)
- [service=WebService](#)
- [service=XidFactory](#)
- [service=invoker,type=jrmp](#)
- [service=invoker,type=local](#)
- [service=invoker,type=pooled](#)
- [service=proxyFactory,target=ClientUserTransaction](#)
- [service=proxyFactory,target=ClientUserTransactionFactory](#)

jboss.aop

- [service=AspectDeployer](#)
- [service=AspectManager](#)

jboss.bean

- [service=JBossBeanDeployer](#)

Interrogation des bases de données Internet

Whois

- Service de recherche fourni par les registres Internet permettant d'obtenir des informations sur une adresse IP, un nom de domaine ou sur des AS Numbers ;
- Fournissent des informations contextuelles intéressantes ;
- Permet de vérifier la cible.

Interrogation des bases de données Internet

Interrogation Whois

```
% whois clear.fr
...
domain:      clear.fr
status:      ACTIVE
hold:        NO
holder-c:    N2591-FRNIC
admin-c:     ACN385-FRNIC
tech-c:      ER507-FRNIC
zone-c:      NFC1-FRNIC
nsl-id:      NSL9131-FRNIC
registrar:   EURODNS S.A.
anniversary: 08/01
created:     08/01/2008
last-update: 22/09/2011
source:      FRNIC

ns-list:     NSL9131-FRNIC
nserver:     ns1.sedoparking.com
nserver:     ns2.sedoparking.com
source:      FRNIC

nic-hdl:     ER507-FRNIC
type:        ROLE
contact:     EDNS ROLE
address:     EuroDNS S.A.
address:     41, z.a. am Bann
address:     3372 Leudelange
address:     LU
e-mail:      dnsfr@admin.eurodns.com
admin-c:     MM2096-FRNIC
tech-c:      PYG1-FRNIC
changed:     15/05/2006 dnsfr@admin.eurodns.com
source:      FRNIC
```

```
...
nic-hdl:     N2591-FRNIC
type:        ORGANIZATION
contact:     NetTraffic.fr
address:     5, avenue albert durand Aeropole
address:     batiment 1
address:     31700 Blagnac
country:     FR
phone:       +33 9 70 46 73 11
e-mail:      contact@nettraffic.fr
changed:     23/12/2009 nic@nic.fr
anonymous:   NO
obsoleted:   NO
idstatus:    ok
source:      FRNIC

nic-hdl:     ACN385-FRNIC
type:        PERSON
contact:     Admin-C Nettraffic. Fr
address:     5, avenue albert durand Aeropole
address:     batiment 1
address:     31700 Blagnac
country:     FR
phone:       +33 9 70 46 73 11
e-mail:      contact@nettraffic.fr
...
```


Interrogation des bases de données Internet

Fuite d'information DNS

- Recherche de serveurs types (NS, MX, ...)

```
dig -t MX <zone>
```

- Transfert de zone

```
host -l <zone>
```

```
dig @server_dns <zone> axfr
```

- Attaque par dictionnaire sur nom dns (pop, smtp, ns, smtp, dc, db, fw ...)

```
dnsenum.pl <zone> -f dns.txt
```

```
./fierce.pl -dns <zone>
```

- Résolution inverse de noms

```
dig -x <ip>
```

```
for ((i=1;i<255;i++)) do host 192.134.105.$i; done >>reverse_host.txt 2>&1
```

```
Nmap -sL 192.134.105.0/24
```

Outils

dig, host, nslookup, dnsenum, fierce

Interrogation des bases de données Internet

Types de requêtes et enregistrements DNS

A : adresse IP

PTR : nom de machine

MX : serveur de messagerie

NS : serveur DNS

CNAME : alias de noms

TXT : autres informations

AXFR : transfert de zone

Interrogation des bases de données Internet

Interrogation DNS

```
root@bt: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# dig -t MX free.fr

; <<>> DiG 9.5.0-P2.1 <<>> -t MX free.fr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47928
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 6

;; QUESTION SECTION:
;free.fr.                IN      MX

;; ANSWER SECTION:
free.fr.                40124   IN      MX      20 mx2.free.fr.
free.fr.                40124   IN      MX      10 mx1.free.fr.

;; AUTHORITY SECTION:
free.fr.                40124   IN      NS      freens2-g20.free.fr.
free.fr.                40124   IN      NS      freens1-g20.free.fr.

;; ADDITIONAL SECTION:
mx1.free.fr.            25757   IN      A        212.27.48.6
mx1.free.fr.            25757   IN      A        212.27.48.7
mx2.free.fr.            30429   IN      A        212.27.42.58
mx2.free.fr.            30429   IN      A        212.27.42.59
freens2-g20.free.fr.    82629   IN      A        212.27.60.20
freens1-g20.free.fr.    30925   IN      A        212.27.60.19

;; Query time: 32 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: Mon Dec 5 03:35:59 2011
```


Prise d'empreinte

- Rechercher un maximum d'informations sur les équipements, les applications et les personnels de la cible par le biais de sources ouvertes
- Utiliser des techniques de « Google Hacking » qui mettent en oeuvre des mots-clés spéciaux aussi appelés opérateurs de recherche
- Réaliser la prise d'empreinte du réseau, des systèmes et des services

Réaliser la prise d'empreinte du réseau, des systèmes et des services

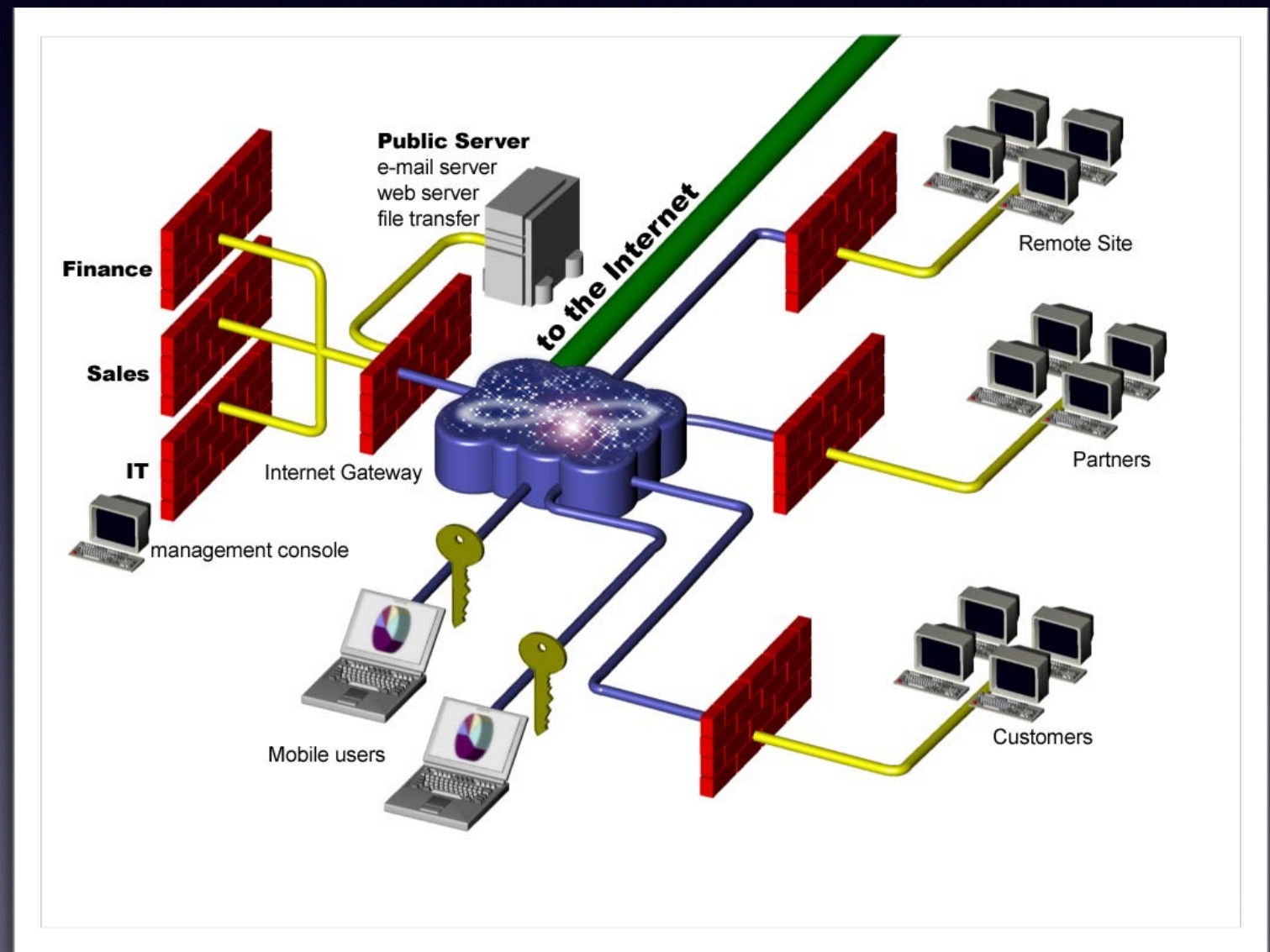
Cartographie du réseau

Identification des systèmes

Identification des services

Cartographie du réseau

- Objectifs
 - Découvrir les machines d'un réseau donné
 - Découvrir les services réseau fournis par ces machines
- Principe
 - Envoyer des paquets à toutes les adresses
 - Analyser les paquets retour



Découverte des hôtes présents

Scan ARP

- Principe

- Envoyer des requêtes ARP (en diffusion) pour demander les adresses MAC de toutes les adresses IP du réseau et détecter les hôtes qui répondent

- Outils

- nmap :

```
nmap -PR 192.168.0.1/24 (réseau local)
```

- arp-scan :

```
arp-scan -interface=eth0 -localnet
```

```
arp-scan -interface=eth0 10.0.0.0/24
```


Découverte des hôtes présents

Balayage ICMP (Ping Sweep)

- Principe

- Envoyer des requêtes ICMP (echo, netmask, timestamp et request) et détecter les hôtes qui répondent

- Outils

- `ping`
- `hping3 : option —icmptype`

Découverte des hôtes présents

Connexions TCP et UDP

- Principe
 - Envoyer un paquet de debut de connexion (TCP SYN) ou un paquet valide UDP sur un port potentiellement ouvert (139, 445, 22...) et observer la réponse.
- Outils
 - `hping3` :
 - TCP : options `-s` et `-p`
 - UDP : options `-udp` et `-p`
 - `nmap` : options `-sP` et `-PS` ou `-PU`

Découverte des hôtes présents

Scan des ports TCP

- Objectifs
 - Détecter l'ensemble des ports TCP ouverts/fermés/filtrés sur les machines cibles
- Principe
 - Envoi d'un segment TCP SYN sur l'ensemble des ports TCP
- Analyse de la réponse
 - TCP RST : port fermé
 - TCP SYN/ACK : port ouvert
 - Pas de réponse ou ICMP : port filtré

Découverte des hôtes présents

Scan des ports UDP

- Objectifs
 - Détecter l'ensemble des ports UDP ouverts/fermés/filtrés sur les machines cibles
- Principe
 - Envoi de datagrammes sur l'ensemble des ports UDP
- Analyse de la réponse
 - Message ICMP Destination Unreachable / Port Unreachable : port fermé
 - Réponse générée par l'équipement de filtrage (ICMP) : port filtré
 - Pas de réponse : port ouvert ou filtré
 - réponse applicative (ou erreur) : port ouvert
- Les scans UDP sont non fiables et très lents
 - Aucune réponse de certains services si les messages UDP ne sont pas formatés correctement.
 - Message ICMP (type 3, code 3) indiquant un port fermé sont souvent filtrés
- Nécessite d'utiliser des outils dédiés pour les port UDP
 - DNS (53), RPC(111), SNMP(161), NTP(123), IKE(500), SYSLOG(514)

Découverte de l'architecture du réseau

Découverte de la route

- Objectifs
 - découvrir l'architecture du réseau, la façon dont les différents réseaux sont interconnectés
- Méthodes
 - Envoi de paquets via traceront (UDP, ICMP et TCP)
- Outils
 - `traceroute` / `tracer` (Linux / Windows)
 - `tcptraceroute`
 - permet la découverte des redirections de port (TTL+1) et de découvrir certaines IP internes des équipements de routage
 - `hping3`
 - `ping`
 - `scapy`
 - `mtr`

Découverte de l'architecture du réseau

Découverte des répartiteurs de charge

- Scan de ports
 - Identifier les adresses IP de tous les serveurs
 - `nmap -sS -p 80 35.35.35.1/24`
 - Identifier les services offerts par ces serveurs (différences possibles)
- Analyse des timestamps
 - analyse des réponses
- Evolution de l'entête ID du champ IP
 - `hping3 -S -faster www.victim.com`

Réaliser la prise d'empreinte du réseau, des systèmes et des services

Cartographie du réseau

Identification des systèmes

Identification des services

Identification des systèmes

Prise d'empreinte de pile TCP/IP

- Objectifs
 - Détecter le type et la version du système d'exploitation installé sur les machines cibles
- Méthodes
 - Prise d'empreinte active : analyse de la réaction de la pile TCP/IP de la machine via des requêtes diverses
 - Prise d'empreinte passive
 - écoute du réseau (Ex: broadcast Netbios, CDP...)

Identification des systèmes

Prise d'empreinte TCP/IP active

- Chaque pile TCP/IP (Linux, Windows...) dispose d'une signature unique.
- Chaque système devrait implémenter de la même façon tous les types de requêtes, réponses, traitement d'erreurs définis dans les RFC, mais dans les faits, il n'en est rien.
- Le principe du fingerprinting actif est de transmettre des « sondes » correspondant à des paquets mal formés et d'écouter les réponses associées.
- Outils
 - `nmap -O <ip>`
 - Xprobe
 - SinFP

Identification des systèmes

Prise d'empreinte TCP/IP passive

- La prise d'empreinte passive consiste à **intercepter des paquets** transitants sur une interface d'écoute (sniffing). Cela **évite d'émettre** des paquets mal formés à destination du système cible et permet d'**échapper aux IDS**.
- **Outils**
 - P0f
 - Ettercap
 - SinFP
 - tcpdump

Réaliser la prise d'empreinte du réseau, des systèmes et des services

Cartographie du réseau

Identification des systèmes

Identification des services

Identification des services

Identification basique des applications

- Objectifs
 - Détecter les applications tournant sur les hôtes par des techniques simples
- Méthodes
 - Récupération des bannières des applications accessibles via un port ouvert ;
 - provocation d'erreur (404 par exemple).
- Outils
 - nmap : option -sV
 - netcat
 - openssl...

Banner Grabbing

- telnet, nc

```
%nc linux-attitude.fr 80
```

```
GET / HTTP/1.0
```

HTTP/1.0 200 OK

Date: Wed, 03 Aug 2016 20:43:25 GMT

Server: Apache/2.4.10

Set-Cookie: PHPSESSID=c2phkmn9fgjk621pnl2fu2k202; path=/

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

X-Pingback: http://linux-attitude.fr/xmlrpc.php

X-Powered-By: W3 Total Cache/0.9.3

X-W3TC-Minify: On

Vary: Accept-Encoding,User-Agent

Connection: close

Content-Type: text/html; charset=UTF-8

```
<html xmlns="http://www.w3.org/1999/xhtml" lang="fr-FR">
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

```
<title>Linux Attitude - Le libre est un état d'esprit</title>
```

```
<meta name="generator" content="WordPress 3.8" />
```

```
<meta name="robots" content="follow, all" />
```

```
...
```


Identification des services

• FTP

```
%ftp ftp.free.fr
```

```
Trying 212.27.60.27...
```

```
Connected to ftp.proxad.net.
```

```
220 Welcome to ProXad FTP server
```

```
Name (ftp.free.fr:john): anonymous
```

```
331 Please specify the password.
```

```
Password: anonymous
```

```
230 Login successful.
```

```
Remote system type is UNIX.
```

```
Using binary mode to transfer files.
```

```
ftp> ls
```

```
229 Entering Extended Passive Mode (|||26877|).
```

```
150 Here comes the directory listing.
```

lrwxrwxrwx	1	ftp	ftp	28 Jun 14	2011	MPlayer -> mirrors/mplayerhq.hu/ MPlayer
drwxr-xr-x	2	ftp	ftp	4096 May 07	2008	awstats
drwx-----	2	ftp	ftp	4096 Mar 08	2006	lost+found
drwxr-xr-x	3	ftp	ftp	4096 Jun 22	10:23	mirrors
drwxr-xr-x	2	ftp	ftp	4096 Dec 24	2008	nzb
drwxr-xr-x	9	ftp	ftp	4096 Oct 23	2014	pub
drwxr-xr-x	2	ftp	ftp	81920 Aug 02	22:30	stats
drwxr-xr-x	2	ftp	ftp	4096 Aug 03	16:58	tmp

```
226 Directory send OK.
```

```
ftp> quit
```

```
221 Goodbye.
```


Identification des services

- SNMP (161/UDP)
 - Protocole d'administration réseau très intéressant
 - La communauté « **public** » est généralement la communauté par défaut pour la lecture des objets SNMP.
- Outils pour la lecture/écriture de configurations
 - `snmpwalk`, `snmpget`, `snmpset`

Identification des services

Identification avancée des applications

- Objectifs
 - Identifier avec précision les applications tournant sur les hôtes sans se fier aux bannières
- Outils
 - Messagerie : `smtpmap`
 - Web : `httpprint`
 - scripts en mode découverte de version :
 - `Metasploit`
 - `Nmap`

Cartographie depuis
un poste interne

Découverte des hôtes présents

Analyser son environnement

- Réalisable à partir d'un accès interne (local, remote)
 - information (dhcp, dns, wins, ntp)
 - `netstat`
 - configuration réseau
- Capture et analyse réseau
 - `tcpdump` / `windump`
 - `wireshark`, `tshark`

Découverte des hôtes présents

Analyser son environnement

- Réalisable à partir d'un accès interne (local, remote)
 - information (dhcp, dns, wins, ntp)
 - `netstat`
 - configuration réseau
 - `netcat (*X)`
- Capture et analyse réseau
 - `tcpdump` / `windump`
 - `wireshark`, `tshark`

Quelques outils

- Wireshark
- tcpdump / windump
- nmap
- netcat
- hping3
- outils snmp

Séquences d'une attaque



Préparation à l'exploitation

- Identification des vulnérabilités
 - Analyse des versions des services
 - Scan de vulnérabilités
- Recherche de vulnérabilités
 - Recherche des exploits
 - Recherche des vulnérabilités dans les base de données d'exploit
 - Ecriture d'exploit

Préparation à l'exploitation

- **Objectif** : déterminer les failles présentes sur les systèmes cibles
- **Sources d'informations**
 - Sites Web : www.cvedetails.com, www.secunia.com, www.securityfocus.com, www.securiteam.com, isc.sans.org, cve.mitre.org, packetstormsecurity.nl ...
 - Organismes : CERT (CERTA, CERT-Renater, CERT-IST)
 - Listes de diffusion
 - Générales : Full Disclosure, BugTraq, etc.
 - Constructeurs : Microsoft, Solaris, Cisco ...
 - Applicatifs : Apache, Bind ...
 - Blogs
 - Services de veilles sociétés tierces (XMCO, HSC, Vupen ...)
 - Codes d'exploitation : <http://www.exploit-db.com/>, Metasploit ...

Préparation à l'exploitation

- Facteurs limitant : temps et quantité d'informations
- Il faut se focaliser sur les cibles les plus prometteuses
 - Contrôleurs de domaine ;
 - Applicatifs sensibles (messagerie, SGBD, serveurs WEB) ;
 - Postes clients.

Outils de recherche de vulnérabilités

Principe

- détection des machines vivantes sur le réseau ;
- « scan » des ports avec un des quatre ports scanners internes, ou un scanner externe (nmap ou amap) ;
- récupération d'informations ;
- type et version des divers services ;
- connexion (SSH, Telnet ou rsh) pour récupérer la liste des packages installés ;
- attaques simples, peu agressives. Par exemple, directory traversal, test de relais de messagerie ouverts, etc. ;
- attaques susceptibles d'être destructrices ;
- dénis de service (contre les logiciels visés) ;
- dénis de service contre la machine ou les équipements réseaux intermédiaires.

Questions ?