



TLS-SEC

Hacking réseau éthique

L. HAJNAL / N. LARRIEU
2017

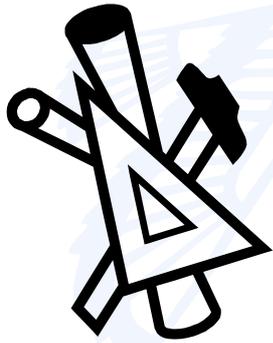
Objectifs



A la fin du cours l'étudiant saura :

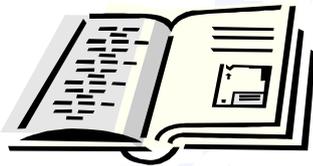
- ⌘ Apprécier comment lister, quantifier et limiter l'ensemble des vulnérabilités inhérentes aux architectures système et réseau.
- ⌘ Connaître les grandes techniques de tentatives d'intrusions système ou réseau et les contremesures à déployer dans le système pour s'en prémunir.
- ⌘ Connaître la problématique de la réaction en cas d'incident et les techniques d'investigation numérique

Le PLAN



- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'Intrusion
- ✓ Outils d'intrusion
- ✓ En cas d'incident
- ✓ Conclusion

Le PLAN



- ✓ **Introduction**
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ Outils d'Intrusion
- ✓ En cas d'incident
- ✓ Conclusion

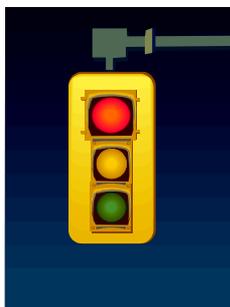
Livre Blanc de la défense



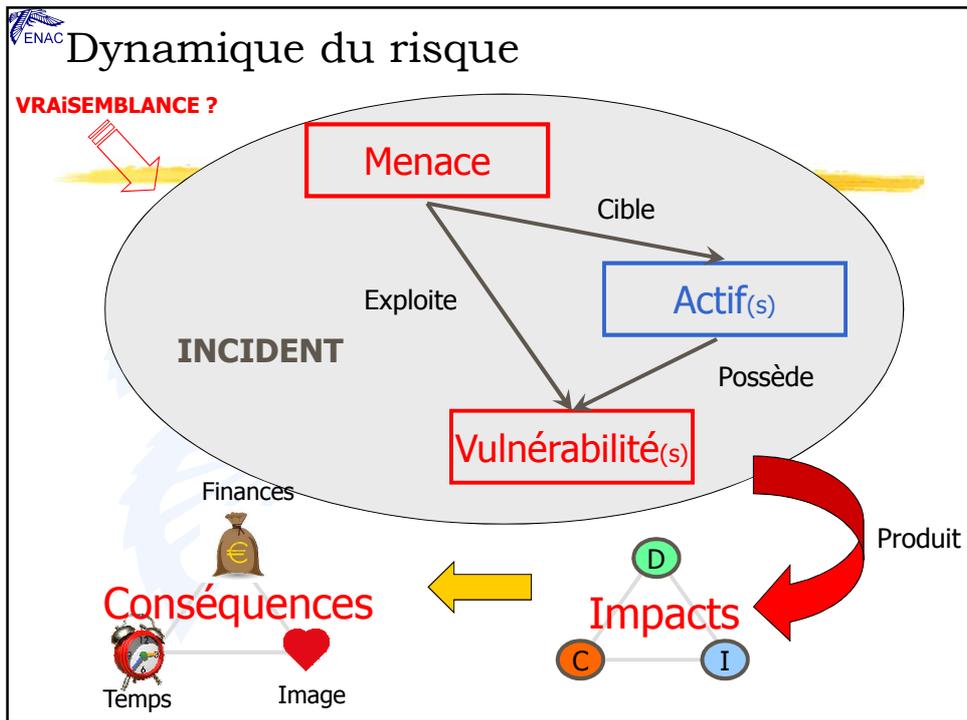
« Les *cyber-attaques* constituent une menace majeure, à forte probabilité et à fort impact potentiel. »

- ⌘ LA loi de programmation militaire de décembre 2013 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale.

Le PLAN



- ✓ Introduction
- ✓ **Rappels**
- ✓ Stratégies d'intrusion
- ✓ Outils d'intrusion
- ✓ En cas d'incident
- ✓ Conclusion



ENAC **Menace: Définition**

Menace : [ISO/CEI 27000] Cause potentielle d'un incident indésirable, qui pourrait provoquer des dommages à un système ou une organisation.

Vulnérabilité: Définition



Vulnérabilité : **Faible** ou faiblesse dans
un **actif** (pouvant être exploité par une
menace)

Le PLAN

- ✓ Introduction
- ✓ Rappels

✓ Stratégies d'intrusion

- ✓ Détection d'intrusion
- ✓ En cas d'incident
- ✓ Conclusion



Stratégies d'intrusion



- Idées générales
- Recueil d'informations
- Exploitation de vulnérabilités
- Pivot

Stratégies d'intrusion



- Idées générales
- Recueil d'informations
- Exploitation de vulnérabilités
- Pivot

Même si.....



- ✓ Même si toutes les entreprises n'ont pas de PSSI
- ✓ Même si, quand elles en ont une, elle est parfois difficile à appliquer
- ✓ Même si, la défense en profondeur n'est pas simple
- ✓ Même si, l'amélioration continue requiert des efforts,

- ✓ bon nombre de SI sont protégés par des systèmes de sécurité.

Porte d'entrée



- ✓ Les SI « *rendent service* »
 - Portails web
 - Messagerie
 - dns
 - FTP.....

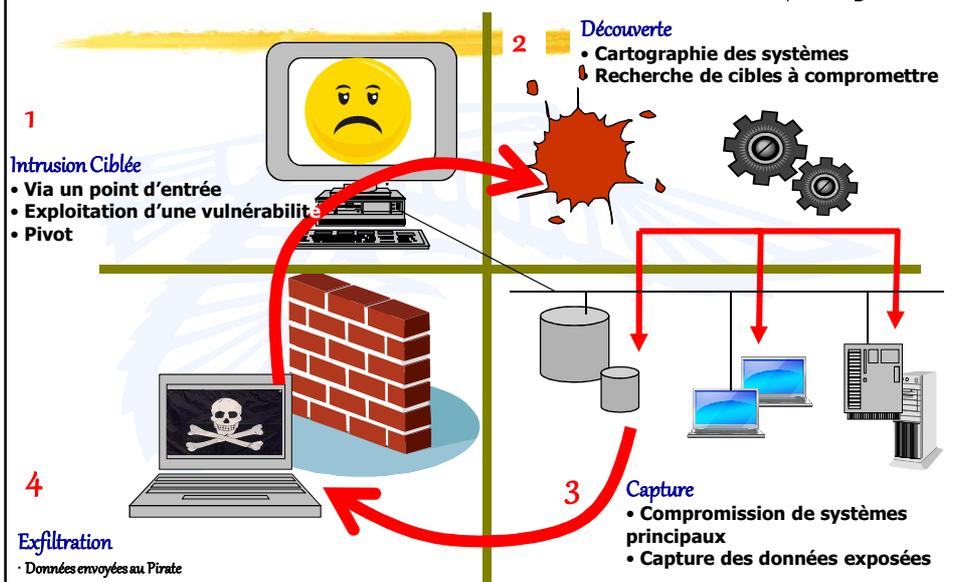
- ✓ Ces services sont des points d'entrée

Pivot



- ✓ L'intrusion d'une machine publique peut constituer l'objectif
 - ✓ Constitution de réseaux malveillants (botnets)
 - ✓ Relais de spam
 - ✓ Relais d'anonymisation
- ✓ Mais le point d'entrée **n'est pas toujours la cible**
- ✓ Nécessité d'aller plus loin pour atteindre les données sensibles (notion de **pivot**)

Intrusion Logique



Intrusion ciblée :

3 Phases



1. **L'approche** : récupération d'un maximum d'informations sur la cible.
2. **L'analyse** des informations récupérées
 - ❑ définir les **vulnérabilités** de la cible
 - ❑ choisir son **angle d'attaque**.
3. **L'exploitation** de(s) la vulnérabilité(s)

Stratégies d'intrusion



- Idées générales
- **Recueil d'informations**
- Exploitation de vulnérabilités
- Pivot

Les ressources humaines:

⌘ Qui fait quoi ?

⌘ Internet est votre complice

☑ Whois



Whois

WHOIS information for enac.fr:**

```
[Querying whois.nic.fr]
[whois.nic.fr]
%%
%%
domain:      enac.fr           /MM
status:     ACTIVE           2.5
%%
%%
contact:    ECOLE NATIONALE DE L AVIATION CIVILE
address:    7, avenue Edouard Belin
address:    B.P. 4005
address:    31055 Toulouse
country:    FR
phone:      +33 5 62 17 40 01
e-mail:     marc.houalle@enac.fr
registrant: SIP RENATER
%%
%%
type:       PERSON
contact:    Didier Magre
address:    Ecole nationale de l'Aviation Civile
address:    7, avenue Edouard Belin
address:    31055 Toulouse Cedex
country:    FR
phone:      +33 5 62 17 41 57
fax-no:     +33 5 62 17 41 58
e-mail:     didier.magre@enac.fr
registrant: SIP RENATER
changed:    26/07/2004 domaine@renater.fr
anonymous: NO
obsoleted:  NO
source:     FRNIC
nic-hdl:    AC952-FRNIC
type:       PERSON
contact:    Alexandre Cohen
address:    Ecole nationale de l'Aviation Civile
...
%%
%%
```

Les ressources humaines:

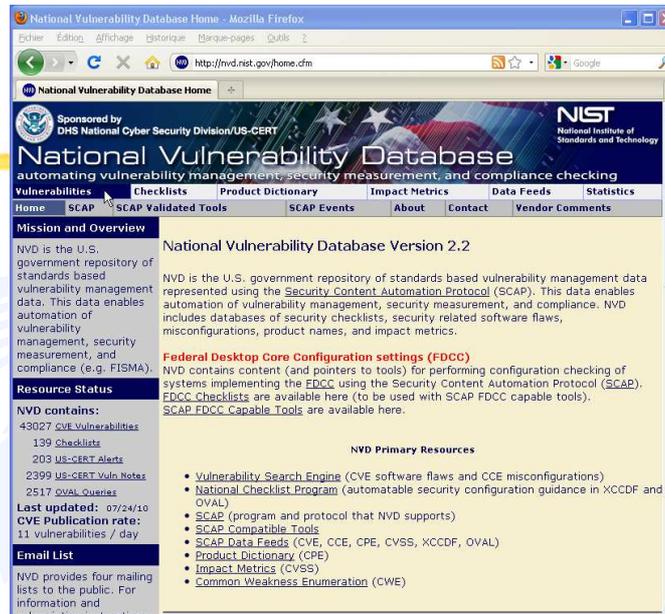
- ⌘ Qui fait quoi ?
- ⌘ Internet est votre complice
 - ☒ Whois
 - ☒ Portail de l'entreprise
 - ☒ Blogs
 - ☒ Réseaux sociaux
 - ☒ Copains d'avant, twitter, facebook etc...
- ⌘ L'ingénierie sociale est un atout pour l'attaquant

Ressources Logiques

- ⌘ Cartographie du **réseau**
 - ☒ Balayage des @ IP
- ⌘ Cartographie des **services**
 - ☒ Balayage de **ports**
- ⌘ savoir **quels systèmes** sont présents
 - ☒ Noyau, distrib, service pack ?
- ⌘ savoir **quels logiciels** assurent les services
 - ☒ version ?

Répertoire des Vulnérabilités Logiques

- ⌘ Les erreurs logiques sont nomenclaturées dans différentes bases de données.
- ⌘ Le classement de référence est probablement celui assuré par le MITRE sous la houlette du CERT US (United states computer emergency readiness team)
- ⌘ Le classement cve est accessible à partir de différents sites
 - ⊗ <http://cve.mitre.org>
 - ⊗ <http://nvd.nist.gov> (national Vulnerability database)
 - ⊗ <http://www.osvdb.org>
- ⌘ En France le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques <http://www.certa.ssi.gouv.fr/>) effectue notamment un travail de veille ainsi qu'un classement des vulnérabilités.



<http://nvd.nist.gov>
Accueil

ENAC

National Vulnerability Database (NVD) Search Vulnerabilities - Mozilla Firefox

http://web.nvd.nist.gov/view/vuln/search

National Vulnerability Database (NVD...)

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists Product Dictionary Impact Metrics Data Feeds Statistics

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 43027 CVE Vulnerabilities
- 139 Checklists
- 203 US-CERT Alerts
- 2399 US-CERT Vuln Notes
- 2517 OVAL Queries
- 22181 CPE Names

Last updated: Mon Jul 26 04:34:03 EDT 2010
 CVE Publication rate: 10.53

Email List

Search CVE and CCE Vulnerability Database (Advanced Search)

Keyword search:

Try a product or vendor name
 Try a CVE standard vulnerability name or OVAL query
 Only vulnerabilities that match ALL keywords will be returned
 Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:

- Software Flaws (CVE)
- Misconfigurations (CCE), under development
- US-CERT Technical Alerts
- US-CERT Vulnerability Notes
- OVAL Queries

NVD now maps to CWE! See NVD CWE for more details.

http://nvd.nist.gov Recherche

ENAC

National Vulnerability Database (NVD) Search Vulnerabilities - Mozilla Firefox

http://web.nvd.nist.gov/view/search/results?td=5

National Vulnerability Database (NVD...)

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists Product Dictionary Impact Metrics Data Feeds Statistics

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 43027 CVE Vulnerabilities
- 139 Checklists
- 203 US-CERT Alerts
- 2399 US-CERT Vuln Notes
- 2517 OVAL Queries
- 22181 CPE Names

Last updated: Mon Jul 26 04:34:03 EDT 2010
 CVE Publication rate: 10.53

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#).

Workload Index

Vulnerability Workload Index: 9.49

About Us

NVD is a product of the

Search Results (Refine Search)

There are 4 matching records. Displaying matches 1 through 4.

CVE-2009-3958
 TAD-013A VU#773545
 Summary: Multiple stack-based buffer overflows in the NOS Microsystems getPlus Helper ActiveX control before 1.6.2.49 in gp.ocx in the Download Manager in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow remote attackers to execute arbitrary code via unspecified initialization parameters.
 Published: 01/13/2010
 CVSS Severity: 10.0 (HIGH)

CVE-2009-1855
 TAD9-161A
 Summary: Stack-based buffer overflow in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow attackers to execute arbitrary code via a PDF file containing a malformed U3D model file with a crafted extension block.
 Published: 06/11/2009
 CVSS Severity: 9.3 (HIGH)

CVE-2009-0927
 Summary: Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1.9 before 9.1.2, and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getIcon method of a collab object, a different vulnerability than CVE-2009-0658.
 Published: 03/19/2009
 CVSS Severity: 10.0 (HIGH)

CVE-2008-2992
 TAD-309A VU#593409
 Summary: Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104.
 Published: 11/04/2008
 CVSS Severity: 9.3 (HIGH)

http://nvd.nist.gov Résultats

ENAC

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2008-2992) - Mozilla Firefox

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2992

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

National Cyber-Alert System

Vulnerability Summary for CVE-2008-2992
Original release date: 11/04/2008
Last revised: 09/08/2009
Source: US-CERT/NIST

Mission and Overview
NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status
NVD contains:
43027 CVE Vulnerabilities
139 Checklists
203 US-CERT Alerts
2399 US-CERT Vuln Notes
2517 OVAL Overies
22181 CPE Names
Last updated: Mon Jul 26 04:34:03 EDT 2010
CVE Publication rate: 10.53

Email List
NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#)

Overview
Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the `util.print()` JavaScript function with a crafted format string argument, a related issue to CVE-2008-4146

Impact
CVSS Severity (Version 2.0):
CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/AU:N/C:C/L:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6
CVSS Version 2 Metrics:
Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

References to Advisories, Solutions, and Tools

http://nvd.nist.gov CVE-2008-2992

ENAC

Stratégies d'intrusion

- Idées générales
- Recueil d'informations
- Exploitation de vulnérabilités
- Pivot



Exploitation de Vulnérabilités Craquage



- ⌘ Lorsque la vulnérabilité à exploiter est une absence ou une mauvaise gestion des mots de passe, le craquage peut être un moyen d'exploitation efficace.
- ⌘ Ce n'est toutefois pas le seul moyen pour récupérer des mots de passe:
 - ☒ écoute du réseau
 - ☒ Utilisation de **logiciels malveillant** (keyloggers...)
 - ☒ **Ingénierie sociale** (phishing)



Craquage enjeux



- ⌘ Recueillir des identifiants/mots de passe revêt un intérêt stratégique majeur:
 - ☒ Les utilisateurs ont parfois des comptes sur plusieurs machines avec les mêmes couples identifiants/mots de passe.
 - ☒ Si des annuaires ou du Single Sign On sont en place un mot de passe est un **sésame vers beaucoup de machines**
 - ☒ L'acquisition d'une seul couple Id/mdp peut rendre possible des **pivots successifs**



Craquer les Mots de Passe Comment ?



⌘ Force brute

⌘ Dictionnaires



Craquage Méthode Force Brute



⌘ A partir de la liste des utilisateurs on essaye une série de combinaisons: permutation, substitutions + ou - simples

⌘ Ex: pour l'utilisateur *administrateur* on essaye

^ (pas de mot de passe)

administrateur (mdp=nom de login)

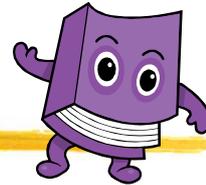
rdministrateura (permutations en tous genres)

admin123456 (substitutions)

AdminIstraTeur (substitutions avec des lettres majuscules)

Craquage

Méthode Attaque par dictionnaires



⌘ traditionnel :

- ☒ L'outil de craquage va chiffrer chaque mot du dictionnaire et comparer avec la valeur contenue dans la base jusqu'à obtenir correspondance.
- ☒ Le fichier dictionnaire contient les mots de passe les plus usités
 - 123456, Admin, les prénoms etc
- ☒ et ceux qu'on veut bien y ajouter suite à un recueil d'infos

⌘ dictionnaires pré-calculés (rainbow tables)

- ☒ Compromis temps-mémoire
- ☒ seules sont conservées certaines de ces empreintes (typiquement une sur 4000) et le complément est déduit grâce à une fonction de dérivation (algorithme de Hellman)

Exploitation de Vulnérabilité

Trouver les codes d'exploitation



Exploits: programmes qui exploitent les failles

- ☒ des systèmes d'exploitation,
- ☒ des logiciels
- ☒ des protocoles.

Exploits

Main (int argc ,char* argv[])

⌘ Unix(s), Microsoft, Adobe, Oracle, open source...
beaucoup d'exploits

⌘ Quelques sites parmi d'autres

<http://www.exploit-db.com/>

<http://packetstormsecurity.org>

⌘ Cadriciel d'exploitation: **Metasploit**

Exploit Database

Main (int argc ,char* argv[])

The screenshot shows the Exploit Database website interface. At the top, there's a navigation menu with links for HOME, CHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT. Below the menu, there are several banners, including one for OWASP (Audit des applications Web) and another for QUALYS. The main heading is "The Exploit Database" with a sub-heading "Remote Exploits". Below this, there is a table listing various exploits with columns for Date, D, A, V, Description, Plat., and Auth.

Date	D	A	V	Description	Plat.	Auth
2014-07-01	-	-	✓	Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & ENET 4.1.X Bypass	windows	stok
2014-06-30	-	-	✓	GRoll - 6.4.0 - Remote Code Execution	multiple	droit
2014-06-27	-	-	✓	HP AutoPass License Server File Upload	java	metasp
2014-06-18	-	-	✓	AbenVault OSIM - 4.7.0 - ax-centered (get_log_line) Remote Code Execution	linux	Alfredo

Stratégies d'intrusion



- Idées générales
- Recueil d'informations
- Exploitation de vulnérabilités
- **Pivot**

Pivot



- vous avez posé votre ancre de pirate dans un des réseaux de l'entreprise cible, mais.....
 - ❑vous voulez investiguer plus loin et hélas la machine victime ne possède pas les outils nécessaires et vous n'avez pas les droits suffisants pour les installer.
 - ❑un FW vous empêche d'aller plus loin et vous avez bon espoir qu'un hôte accessible, car sur le même réseau que le vôtre, est autorisé à le traverser.
- **Pivoter est la solution**
Le calculateur sur lequel vous êtes va vous servir d'**appui** pour continuer l'attaque.



TD Hacking Éthique: environnement de travail

Le PLAN



- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ **Outils d'Intrusion**
 - ✓ Nmap
 - ✓ Metasploit
 - ✓ Craqueurs
 - ✓ Pour pivoter
- ✓ En cas d'incident
- ✓ Conclusion

Le PLAN



- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ Outils d'Intrusion
 - ✓ Nmap
 - ✓ Metasploit
 - ✓ Craqueurs
 - ✓ Pour pivoter
- ✓ Investigation numérique
- ✓ Conclusion

NMAP balai High Tech



- ⌘ Principe : outil pour scanner les ports ouverts sur une machine distante.
- ⌘ Mais aussi outil **multifonction**:
 - ☒ Permet la **reconnaissance** d'OS (OS fingerprinting)
 - ☒ **mode furtif** disponible...
- ⌘ Pour la défense comme pour l'attaque

NMAP

scanner de port



⌘ Utilisation basique

- ☒ Ex : pour scanner une machine :
\$ nmap 192.168.0.1
- ☒ Ex : pour scanner les machines se trouvant dans le plan d'adressage 192.168.0.0/24 :
\$ nmap 192.168.0.0/24

- ⌘ **option -v** pour avoir plus d'informations.
- ⌘ On peut choisir le ou les protocoles à balayer,
- ⌘ par défaut le protocole scanné est TCP.
- ⌘ Pour scanner TCP **et** UDP :
\$ nmap -v -sU -sT 192.168.0.1

NMAP

Quelques Options



- sT** Scanne les ports TCP **-sU** pour UDP (attention cela est inscrit dans les fichiers de log de la machine cible).
- sP** En fait un ping.
- p 20-140** Ne scanne que les ports entre 20 et 140 ;
- p 1024-** scanne tous les ports à partir de 1024 ;
- O** Permet de connaître l'OS (voir aussi `-osscan_guess`).
- P0** Permet de scanner les machines qui n'autorisent pas les ICMP echo request.

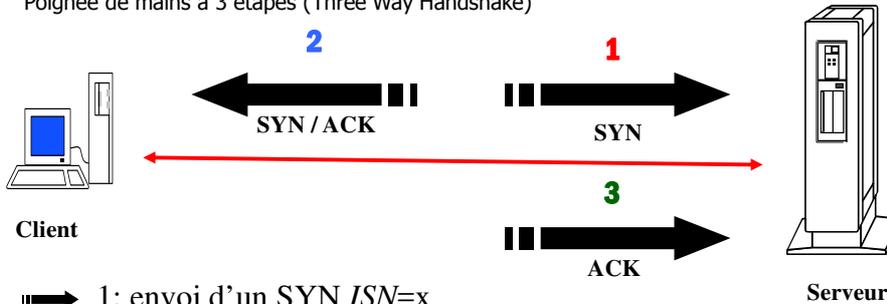


NMAP

principe de fonctionnement (port TCP actif)

⌘ TCP – Etablissement de Connexion

Poignée de mains à 3 étapes (Three Way Handshake)

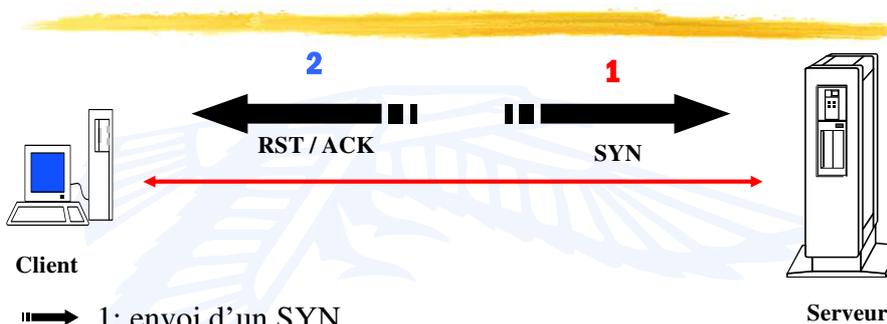


ISN = numéro de séquence initial



NMAP

principe de fonctionnement (port TCP inactif)



ISN = numéro de séquence initial

NMAP

scan de port UDP (1)

- ⌘ Le protocole UDP est ne requiert pas de connexions. Il y 2 manières d'énumérer les services UDP sur notre cible :
 - ☒ Envoyer des paquets UDP sur les 65535 ports et attendre un "ICMP destination port unreachable" qui signifie que le port est fermé, inaccessible ou que la machine est hors service.
 - ☒ Utiliser un client UDP tel que Snmpwalk, Dig ou Tftp pour envoyer un datagramme à la cible et d'attendre une réponse positive.
- ⌘ La plupart des réseaux filtrent les messages ICMP, il est donc souvent difficile d'évaluer quel service UDP est accessible par un simple scan de port.
- ⌘ Le temps de diagnostic est généralement assez long (cf. TP NMAP)

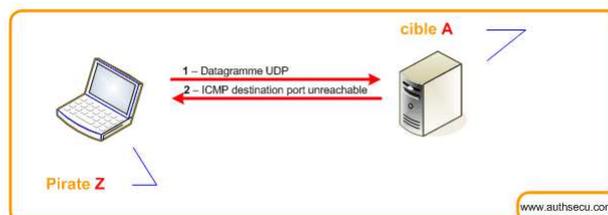
NMAP

scan de port UDP (2)

- ⌘ Le schéma ci-dessous montre que le port est ouvert :



- ⌘ Et le schéma ci-dessous montre que le port est fermé :





NMAP déroulement du scan

```
[root@G17-15]# nmap -v -sU -sT 192.168.200.1
Starting nmap V. x.x by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host (192.168.200.1) appears to be up ... good.
Initiating TCP connect() scan against (192.168.200.1)
Adding TCP port 139 (state Open).
Adding TCP port 25 (state Open).
Adding TCP port 110 (state Open).
Adding TCP port 21 (state Open).
Adding TCP port 135 (state Open).
Adding TCP port 80 (state Open).
Adding TCP port 1026 (state Open).
```



NMAP résultat de scan

```
The TCP connect scan took 1 seconds to scan 1534 ports.
Initiating FIN, NULL, UDP, or Xmas stealth scan against (192.168.200.1)
The UDP or stealth FIN/NULL/XMAS scan took 4 seconds to scan 1534 ports.
Interesting ports on (192.168.200.1):
Port State Service
21/tcp open ftp
25/tcp open smtp
80/tcp open http
110/tcp open pop-3
135/tcp open loc-srv
137/udp open netbios-ns
138/udp open netbios-dgm
139/tcp open netbios-ssn
1026/tcp open nterm
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
```



NMAP

Dans un contexte d'intrusion



⌘ Découverte du réseau

- ☒ Un scan sans option comme `nmap 10.3.100.1` envoie un paquet TCP ACK sur le port 80 ainsi qu'une requête d'écho ICMP à chaque machine cible
- ☒ Cela s'avère insuffisant dans un contexte de test d'intrusion
- ☒ Si présence de système filtrant **proscrire les scans ICMP**
`nmap -PN 10.3.100.1`



NMAP

Temps de réponse



- ⌘ + le scan est complexe (stealth scan, reconnaissance d'OS) + on attend.
- ⌘ + les hôtes scannés sont nombreux, + c'est long
- ⌘ + le nombre de ports scannés par hôte est élevé et + long c'est
- ⌘ Si un système filtrant est présent (FW, routeur...) C + long

- ⌘ possibilité de réduire les coups de balai
 - ☒ En jouant avec les masques: `nmap 10.3.10.1/24`
 - ☒ Ou avec ce genre de syntaxe: `nmap 10.0.0,1,3-7.0-255`
 - ☒ Certaines options (-PS,-PU,-PA) permettent de restreindre les ports à scanner: `nmap -PS25,80,445,139,3306 192.168.2-20.1-20`



TD Hacking Éthique:
étape1 jusqu'au 4.4

Le PLAN

- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ **Outils d'Intrusion**
 - ✓ Nmap
 - ✓ **Metasploit**
 - ✓ Craqueurs
 - ✓ Pour pivoter
- ✓ En cas d'incident
- ✓ Conclusion



Metasploit



⌘ Framework (**cadriciel**) **open source** débuté en 2003

- ☒ Écrit en perl puis ruby depuis la version 3
- ☒ Environnement de développement
- ☒ Très actif

⌘ Outil **d'aide** aux test d'intrusion

- ☒ Utilisation **facile** de codes d'exploitation de vulnérabilités
- ☒ Codes d'exploitation **nombreux** ciblant **plusieurs plate formes**

Metasploit



```
Fichier Édition Affichage Terminal Aide
root@incs22:/ctc/init.d# msfconsole

          01
  metasploit

=[ metasploit v3.4.0-release [core:3.4 api:1.0]
+ -- --=[ 551 exploits - 261 auxiliary
+ -- --=[ 208 payloads - 23 encoders - 8 nops

msf >
```

Architecture modulaire

3 Modules principaux



⌘ **Code d'exploitation** (exploit)

⌘ **Charge utile** (payload)

☑ associé au code d'exploitation choisi

☑ permet d'assurer la communication entre Metasploit et la victime

⌘ **Auxiliaire** (auxiliary)

☑ actions arbitraires telles que le scan de ports,

☑ le déni de services entre autres

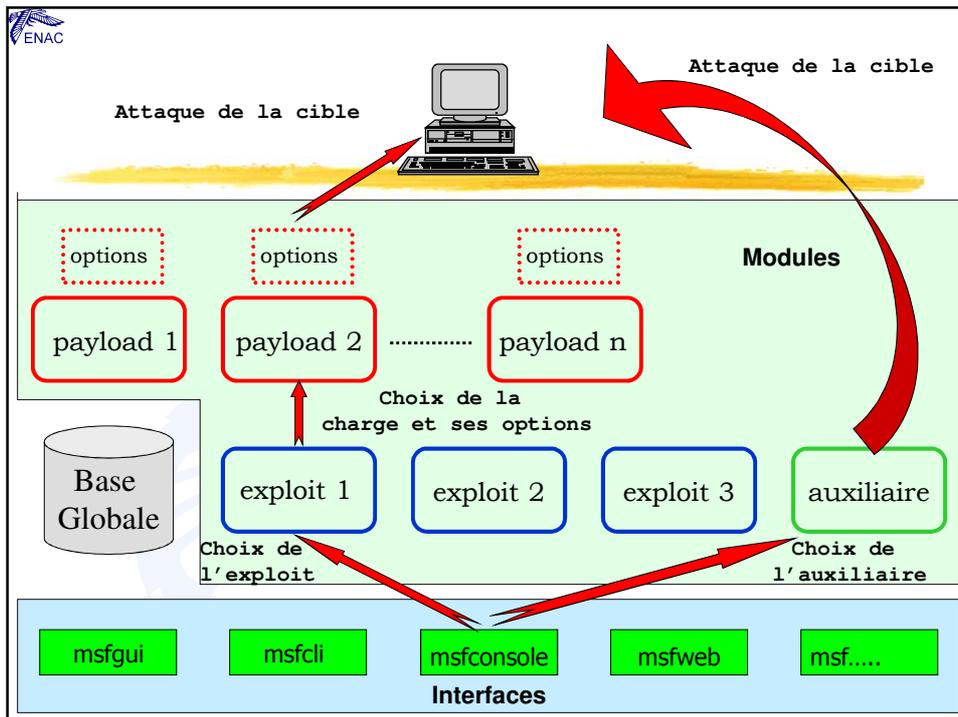
Architecture modulaire

Avantage



⌘ utiliser plusieurs charges utiles pour un même code d'exploitation

⌘ et vice-versa.



ENAC

modules d'exploitation



⌘ Syntaxe

- ☒ lister les exploits windows (les + nombreux)
`search -t exploit windows`
- ☒ Obtenir des information sur les exploits
`info windows/smb/ms08_067_netapi`
- ☒ Avant tout il faut utiliser un module
`use exploit/windows/dcerpc/ms03_26_dcom`
- ☒ Après tout il faut lancer l'exploitation
`exploit`

```

Fichier Edition Affichage Terminal Aide
windows/proxy/luetool_winproxy_host great Blue Coat WinProxy Host Header Overflow
windows/proxy/luetool_telnet_ping average CCP Proxy <= v6.2 Telnet Proxy Ping Overflow
windows/proxy/proxypro http_get great Proxy-Pro Professional Gatekeeper 4.7 GET Req
windows/proxy/qbik_wingate_wwwproxy good Qbik WinGate WWW Proxy Server URL Processing
windows/scada/realwin great DATAC RealWin SCADA Server Duffer Overflow
windows/sip/aim_triton_cscc great AIM Triton 1.6.4 CScc Buffer Overflow
windows/sip/sipxphone_cscc great SIPfoundry sipXPhone 0.35a CScc Field Overf
windows/sip/sipxphone_cscc great SIPfoundry sipXPhone 2.6.0.27 CScc Buffer Ove
windows/smb/ms03_049_netapi good Microsoft Workstation Service NetAddAlternate
windows/smb/ms04_007_killbill low Microsoft ASN.1 Library Bitstring Heap Overfl
windows/smb/ms04_011_lsass good Microsoft LSASS Service DsRolerUpgradeDownlev
windows/smb/ms04_031_netdde good Microsoft NetDDE Service Overflow
windows/smb/ms05_039_pnp good Microsoft Plug and Play Service Overflow
windows/smb/ms06_075_rasman_rpc onnd Microsoft RRAS Service RASMAN Registry Overfl
windows/smb/ms06_075_rras average Microsoft RRAS Service Overflow
windows/smb/ms06_080_netapi great Microsoft Remote Service NetPathCanonicaliz
windows/smb/ms06_066_nwks good Microsoft Services MS66-066 nwap32.dll
windows/smb/ms06_066_nwks good Microsoft Services MS66-066 nwks.dll
windows/smb/ms06_070_wkssvc normal Microsoft Workstation Service NetManageIPCCom
windows/smb/ms08_067_netapi great Microsoft Server Service Relative Path Stack
windows/smb/ms09_050_smb2_negotiate_func_index good Microsoft SV2.SYS SMB Negotiate ProcessID Fu
windows/smb/msdns_zoncnac great Microsoft DNS RPC Service extractQuotedChar()
windows/smb/netidentity_xtierrpcpipe great Novell NetIdentity Agent XTERRPCPIPE Named P
windows/smb/psexec excellent Microsoft Windows Authenticated User Code Exe
windows/smb/smb_relay excellent Microsoft Windows SMB Relay Code Execution
windows/smb/linDukku_pluginCommand_buf great Timbuktu <= 8.6.6 PluginCommand Named Pipe B
windows/smb/mailcarrier_smt ehlo ockw TABS MailCarrier v2.51 SMTP EHLO Overflow
windows/smb/3 Buffer Overfl
windows/smb/Heap Overfl
windows/smb/er Overflow
search -t exploit windows
windows/smb/FreeFIP 1.0.10 Key Exchange Algorithm String
windows/smb/FreeSSH 1.0.9 Key Exchange Algorithm String
windows/smb/Fullly exe <= v0.52 buffer Overfl
windows/smb/SecureRLI <= 4.0 beta 2 SSH1 Buffer Overfl
windows/smb/Microsoft Private Communications Transport Ov
windows/smb/GAMSoft TelSrv 1.5 Username Buffer Overflow
windows/smb/goodtech_telnet average goodtech Telnet Server <= 5.0.0 Buffer Overfl
windows/smb/allied_telsyn_fttp_server_1.9 Long Filename average Allied Telsyn FTP Server 1.9 Long Filename
windows/smb/D-Link TFTP 1.0 Long Filename Buffer Overflow good
windows/smb/FutureSoft TFTP Server 2000 Transfer-Mode Ove average
windows/smb/Quick FTP Pro 2.1 Transfer-Mode Overflow good
windows/smb/TFTPD32 <= 2.11 Long Filename Buffer Overflow average
windows/smb/TFTPDWIN v0.4.2 Long Filename Buffer Overflow great
windows/smb/3Tftpsvc TFTP Long Mode Buffer Overflow great
windows/smb/CA CAR log_security() Stack Buffer Overflow ( great
windows/smb/RealVNC 3.2.7 Client Buffer Overflow normal
windows/smb/ULtraVNC 1.6.1 Client Buffer Overflow normal
windows/smb/WinVNC Web Server <= v3.2.3.7 GET Overflow average
windows/smb/SafeNet SoftRemote IKE Service Buffer Overflo average
windows/smb/Microsoft WINS Service Memory Overwrite great
msf >

```

```

Fichier Edition Affichage Terminal Aide
msf > info windows/smb/ms08_067 47 Windows XP SP3 Hebrew (NX)
40 Windows XP SP3 Hungarian (NX)
Name: Microsoft Server S 49 Windows XP SP3 Italian (NX)
Version: 9179 50 Windows XP SP3 Japanese (NX)
Platform: Windows 51 Windows XP SP3 Korean (NX)
Privileged: Yes 52 Windows XP SP3 Dutch (NX)
License: Metasploit Framework 53 Windows XP SP3 Norwegian (NX)
Rank: Great 54 Windows XP SP3 Polish (NX)
55 Windows XP SP3 Portuguese - Brazilian (NX)
Provided by: 56 Windows XP SP3 Portuguese (NX)
hdm <hdm@metasploit.com> 57 Windows XP SP3 Russian (NX)
Brett Moore <brett.moore@infosec.sans.org> 58 Windows XP SP3 Swedish (NX)
59 Windows XP SP3 Turkish (NX)

Available targets:
Id Name Basic options:
-- ---- Name Current Setting Required Description
0 Automatic Targeting
1 Windows 2000 Universal RHOST yes The target address
2 Windows XP SP0/SP1 Univer RPORT 445 yes Set the SMB service port
3 Windows XP SP2 English (N SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
4 Windows XP SP3 English (N
5 Windows 2003 SP0 Universal
6 Windows 2003 SP1 English Payload information:
7 Windows 2003 SP1 English Space: 400
8 Windows 2003 SP2 English Avoid: 8 characters
9 Windows 2003 SP2 English
10 Windows 2003 SP2 German ( Description:
11 Windows 2003 SP2 German ( This module exploits a parsing flaw in the path canonicalization
code of NetAPI32.dll through the Server Service. This module is
capable of bypassing NX on some operating systems and service packs.
12 Windows XP SP2 Arabic (NX The correct target must be used to prevent the Server Service (along
with a dozen others in the same process) from crashing. Windows XP
13 Windows XP SP2 Chinese - targets seem to handle multiple successful exploitation events, but
2003 targets will often crash or hang on subsequent attempts. This
14 Windows XP SP2 Chinese - is just the first version of this module, full support for NX bypass
is still in development.
15 Windows XP SP2 Chinese -
16 Windows XP SP2 Czech (NX)
17 Windows XP SP2 Danish (NX)
18 Windows XP SP2 German (NX)
19 Windows XP SP2 Greek (NX)
20 Windows XP SP2 Spanish (NX)
21 Windows XP SP2 Finnish (NX)
22 Windows XP SP2 French (NX)
23 Windows XP SP2 Hebrew (NX)
24 Windows XP SP2 Hungarian (NX)
25 Windows XP SP2 Italian (N)
26 Windows XP SP2 Japanese (L)
References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4250
http://www.osvdb.org/49243
http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
NEXPOSE (dcerpc-ms-netapi-netpathcanonicalize-dos)
msf >

```

Fichier Édition Affichage Historique Marque-pages Outils Aide

http://osvdb.org/49243

OSVDB Search OSVDB Browse Vendors Project Info Help OSVDB! Sponsors Account Download DB

49243 : Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution
 Printer | <http://osvdb.org/49243> | [Email This](#) | [Edit Vulnerability](#)

Views This Week	Views All Time	Added to OSVDB	Last Modified	Modified (since 2008)	Percent Complete
76	5615	about 1 year ago	27 days ago	60 times	90%

generously sponsored by **TENABLE** Network Security

Timeline	Disclosure Date	Exploit Publish Date	Vendor Solution Date
	2008-10-23	2008-10-23	2008-10-23

Keywords Gimmiv.A, TrojanSpy:Win32/Gimmiv.A, TrojanSpy:Win32/Gimmiv.A.dll, W32.Wecort, Exploit.Win32.M508-067.g, Rootkit.Wir32.KernelBot.dg, c01606491, HPSBST02386, SSRTO80164, Exploit:Win32/M508067_gen1A, Conficker

Description Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that this flaw may allow remote code execution resulting in a loss of integrity.

Classification
 Location: Remote / Network Access
 Attack Type: Input Manipulation
 Impact: Loss of Integrity
 Solution: Patch / RCS
 Exploit: Exploit Public, Exploit Wormified
 Disclosure: Vendor Verified, Discovered in the Wild

Solution Currently, there are no known workarounds or upgrades to correct this issue. However, Microsoft has released a patch to address this vulnerability.

Products

Microsoft Corporation
Windows
XP SP2
2003 Server SP1
XP Pro x64
2003 Server SP2
2003 Server x64
2003 Server x64 SP2
Z003 Server for Itanium SP2
2003 SP4
XP Pro x64 SP2
XP SP3
2003 Server for Itanium SP1
2003 Server 32-bit

ENAC

Modules payload



⌘ Syntaxe

- ☑ Une fois l'exploit choisi :
 - `show payloads` liste les charges possibles dans le contexte
- ☑ sélectionner une charge utile
 - `set payload « nom_du_payload »`
- ☑ Afficher les options possibles
 - `show options`
- ☑ Renseigner les options
 - ☑ `set «nom_de_l_option» « paramètre »`



TD Hacking Éthique: 4.5 et 4.6

TRANSFERT DES FICHIERS



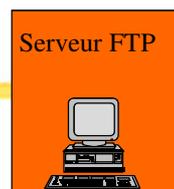
- Le protocole FTP présente les particularités suivantes:
 - ❑ Il y a un canal de commandes (port 21)
 - ❑ et un canal de données (port 20 ou > 1023)
 - ❑ Deux modes de fonctionnement
 - le mode actif
 - le mode passif
- Ftp tourne au dessus de TCP

TRANSFERT DES FICHIERS



- Le canal de commandes sert à envoyer un ensemble de commandes
- Le canal de données sert au transfert des fichiers
- Le client se connecte à partir d'un port aléatoire > 1023 vers le port 21 (élémentaire)
- Mais quand des données doivent être transférées ça se complique un peu suivant que le serveur est en mode actif ou passif

Canal de commandes

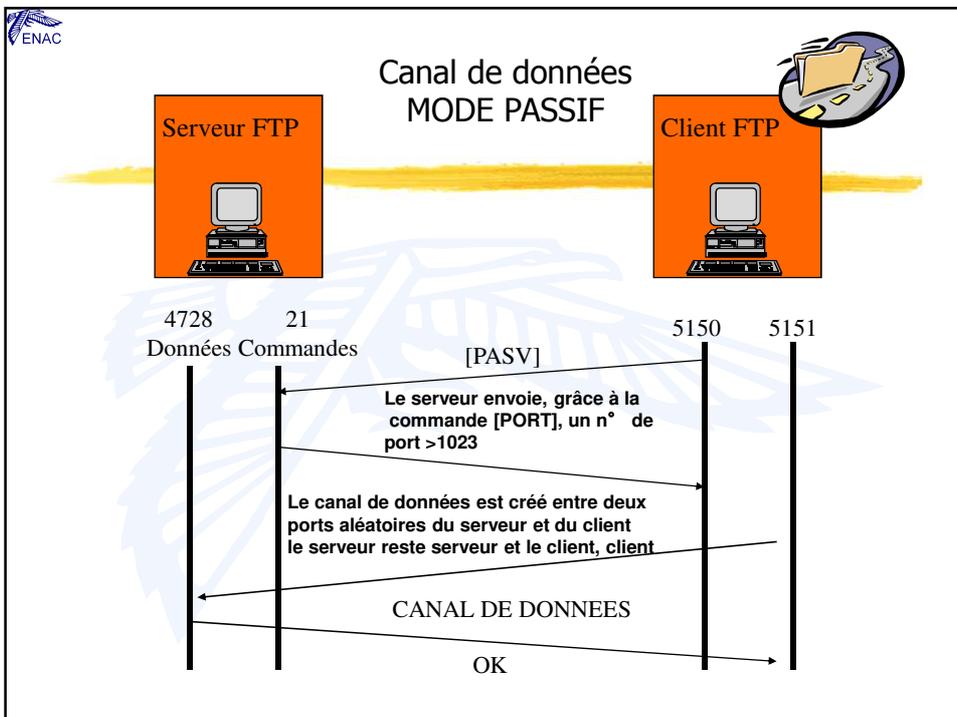
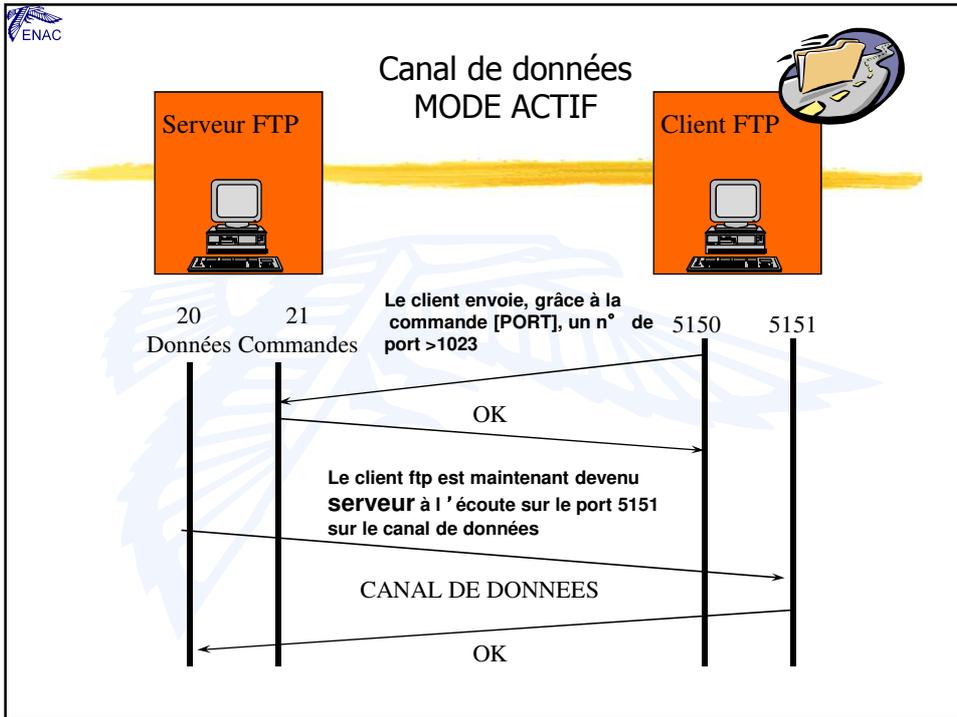


20 21
Données Commandes

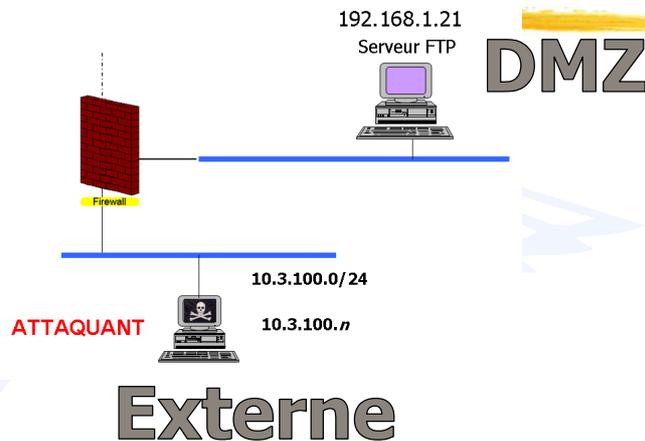
5150 5151

Le client se connecte à partir du port 5150 vers le port 21 du serveur

OK



Topologie réseau du filtrage



Règles de filtrage FTP: externe -> DMZ

✓ Canal de Cmd :

- Iptables -A ext-dmz -s @reseau_externe -p tcp --sport 1024:65535 -d @serveur_ftp --dport 21 -m state --state NEW, ESTABLISHED -j ACCEPT

✓ Canal de données (mode Actif) :

- Iptables -A ext-dmz -s @reseau_externe -p tcp --sport 1024:65535 -d @serveur_ftp --dport 20 -m state --state ESTABLISHED -j ACCEPT

✓ Canal de données (mode Passif) :

- Iptables -A ext-dmz -s @reseau_externe -p tcp --sport 1024:65535 -d @serveur_ftp --dport 1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT

Règles de filtrage FTP: DMZ -> externe

✓ Canal de Cmd :

- `Iptables -A dmz-ext -s @serveur_ftp -p tcp --sport 21 -d @reseau_externe --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT`

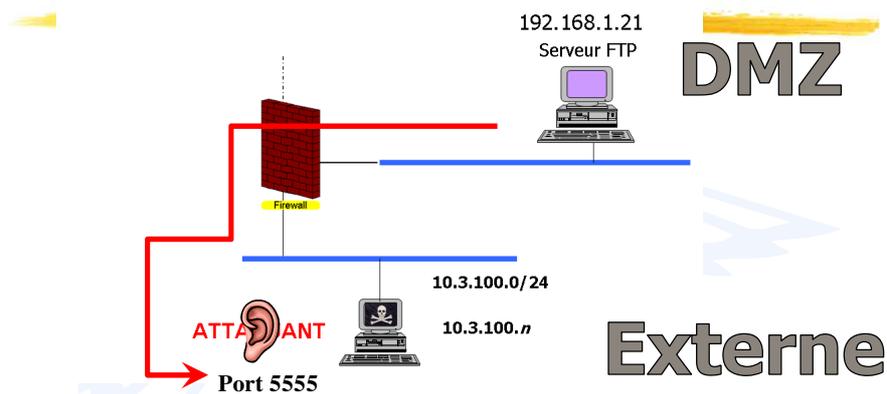
✓ Canal de données (mode Actif) :

- `Iptables -A dmz-ext -s @serveur_ftp -p tcp --sport 20 -d @reseau_externe --dport 1024:65535 -m state --state RELATED, ESTABLISHED -j ACCEPT`

✓ Canal de données (mode Passif) :

- `Iptables -A dmz-ext -s @serveur_ftp -p tcp --sport 1024:65535 -d @reseau_externe --dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT`

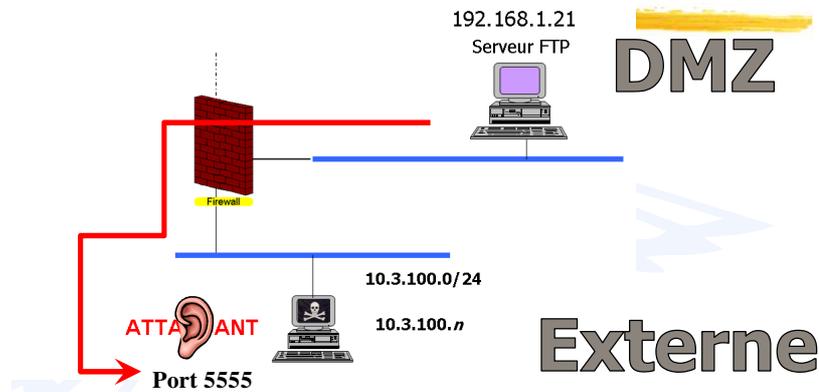
Rappel sur la charge Finale Metasploit



PAYLOAD meterpreter en reverse TCP:

Contact initié par 192.168.1.21 vers le port 5555 de l'attaquant positionné en écoute (mode serveur)

OÙ EST L'ERREUR ?



Observons de plus près les règles de filtrage du FireWall

Faible-RWall: externe -> DMZ

```
$IPTABLES -A externe-dmz -p tcp -s 0/0 -d $FTP --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
```

canal des données pour lequel il faut prendre en compte le ftp actif et le ftp passif
1 FTP actif : notre serveur ftp a initié une connexion (outbound) vers le client externe sur un port choisi (envoyé au serveur grâce à la commande PORT), à partir de son port 20. On traite ici les réponses du client.

```
$IPTABLES -A externe-dmz -p tcp -s 0/0 -d $FTP --dport 20 -m state --state ESTABLISHED -j ACCEPT
```

2 FTP passif : Ici c'est la machine cliente sur le réseau externe qui initie une connexion (inbound) d'un port local >1023 vers un port distant > 1023 de notre serveur ftp

```
$IPTABLES -A externe-dmz -p tcp -s 0/0 --sport 1024:65535 -d $FTP --dport 1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Faille-RWall: DMZ -> externe

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 21 -m state --state ESTABLISHED -j ACCEPT
```

le canal des données pour lequel il faut prendre en compte le ftp actif et le ftp passif

1 **FTP actif** : notre serveur FTP qui a été contacté par une machine du réseau externe initie une connexion (outbound) vers le client sur un port choisi (envoyé au serveur grâce a la commande PORT), à partir de son port 20

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2 **FTP passif** : Ici c'est la machine cliente distante sur le réseau externe qui initie une connexion (inbound) d'un port local >1023 vers un port distant > 1023 de notre machine serveur qui a été contacté. on traite ici les réponses.

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 1024:65535 --dport 1024:65535 -j ACCEPT
```

Faille-RWall: DMZ -> externe

La faille est là.....(?)

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 21 -m state --state ESTABLISHED -j ACCEPT
```

le canal des données pour lequel il faut prendre en compte le ftp actif et le ftp passif

1 **FTP actif** : notre serveur FTP qui a été contacté par une machine du réseau externe initie une connexion (outbound) vers le client sur un port choisi (envoyé au serveur grâce a la commande PORT), à partir de son port 20

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2 **FTP passif** : Ici c'est la machine cliente distante sur le réseau externe qui initie une connexion (inbound) d'un port local >1023 vers un port distant > 1023 de notre machine serveur qui a été contacté. on traite ici les réponses.

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 1024:65535 --dport 1024:65535 -j ACCEPT
```

Faible-RWall:

Il aurait fallu écrire ?

2 **FTP passif** : Ici c'est la machine cliente distante sur le réseau externe qui initie une connexion (inbound) d'un port local >1023 vers un port distant > 1023 de notre machine serveur qui a été contacté. on traite ici les réponses.

```
$IPTABLES -A dmz-externe -p tcp -s $FTP --sport 1024:65535  
--dport 1024:65535 ..... -j ACCEPT
```

Ainsi 192.168.1.21 ne peut plus initier
une nouvelle connexion vers le pirate



TD Hacking Éthique:
étape1 jusqu'au 4.7.1

Le PLAN



- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ **Outils d'Intrusion**
 - ✓ Nmap
 - ✓ Metasploit
- ✓ **Craqueurs**
 - ✓ Pour pivoter
- ✓ En cas d'incident
- ✓ Conclusion

Les outils de craquage Constituer un dictionnaire



⌘ Crunch

☒ <http://sourceforge.net/projects/crunch-wordlist/files/>

⌘ WYD (Who's Your Daddy?)

☒ Infos: [http://www.socialengineer.org/framework/Computer_Based_Social_Engineering_Tools:_Who's_Your_Daddy_Password_Profiler_\(WYD\)](http://www.socialengineer.org/framework/Computer_Based_Social_Engineering_Tools:_Who's_Your_Daddy_Password_Profiler_(WYD))

☒ Télécharger: <http://www.remote-exploit.org/content/wyd-0.2.tar.gz>

⌘ Cupp (Common User Passwords Profiler)

☒ Infos: [http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Common_User_Passwords_Profiler_\(CUPP\)](http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Common_User_Passwords_Profiler_(CUPP))

☒ Télécharger: http://www.remote-exploit.org/articles/misc_research__amp_code/index.html

Constituer un dictionnaire Crunch



⌘ Crunch

- ☒ générateur de listes de mots
- ☒ basé sur un jeu de caractères fixé par l'utilisateur
- ☒ génère toutes les combinaisons et permutations possibles
- ☒ Attention à la taille des fichiers générés !

☒ Exemple :

```
./crunch 1 4 abc123 -b 1mb -o mondico
```

Génère toutes les chaînes de 1 à 4 caractères possibles (min=1 et max vaut 4) parmi l'ensemble abc123, avec une taille du fichier mondico produit inférieure à 1mb

- ⌘ Wyd
- ⌘ Cupp

Constituer un dictionnaire Crunch: jeux de caractères



- ☒ un jeu de caractères est disponible dans le fichier charset.lst

☒ Exemple (à partir du répertoire /pentest/passwords/crunch):

```
./crunch 8 8 -f ./charset.lst numeric -o mondico
```

Crunch génère une liste de mots de passe longs 8 caractères composés de chiffres.

```
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>
hex-lower      = [0123456789abcdef]
hex-upper      = [0123456789ABCDEF]
numeric        = [0123456789]
numeric-space  = [0123456789 ]
symbols14      = [!@#%^&*()_+~]
symbols14-space = [!@#%^&*()_+~ ]
symbols-all   = [!@#%^&*()_+~`~[]{}|\:;'"<.>/?]
symbols-all-space = [!@#%^&*()_+~`~[]{}|\:;'"<.>/? ]
ua1pha        = [BCDEFGHIJKLMNOPQRSTUVWXYZ]
ua1pha-space   = [BCDEFGHIJKLMNOPQRSTUVWXYZ ]
ua1pha-numeric = [BCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ua1pha-numeric-space = [BCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
```

4, 1

13



Constituer un dictionnaire

Crunch: charset persos

- Il est possible de **personnaliser** le fichier **charset.lst**
- Ici je crée un jeu de caractères baptisé lamaison et contenant les caractères [260theo]

```
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>
lamaison = [260theo]
hex-lower = [0123456789abcdef]
hex-upper = [0123456789ABCDEF]

numeric = [0123456789]
numeric-space = [0123456789 ]

symbols14 = [!@#%&*()_-=]
symbols14-space = [!@#%&*()_-= ]

symbols-all = [!@#%&*()_-=^~`{|}:;'"<.,?/]
symbols-all-space = [!@#%&*()_-=^~`{|}:;'"<.,?/ ]

alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
```

4,1

18



Constituer un dictionnaire

Crunch: jeux de caractères persos

- Utilisation du jeu de caractères (au nombre de 7) lamaison
- Liste de mots de passes ($7^8 = 5\,764\,801$ de mots de passe générés)

```
root@bt:/pentest/passwords/crunch# ./crunch 8 8 -f charset.lst lamaison -o test1
Crunch will now generate the following amount of data: 51883209 bytes
0 GB
0 TB
Crunch will now generate the following number of lines: 5764801
100%
root@bt:/pentest/passwords/crunch# █

0000002v
00000022
00000026
0000002t
0000002h
0000002e
0000002p
00000060
00000062
00000066
0000006t
0000006h

root@bt:/pentest/passwords/crunch# ll
total 50820
drwxr-xr-x  2 root root   4096 2014-06-24 17:56 ./
drwxr-xr-x 35 root root   4096 2012-08-08 19:19 ../
-rwxr-xr-x  1 root root   5857 2014-06-24 17:51 charset.lst*
-rwxr-xr-x  1 root root   53280 2012-02-16 04:48 crunch*
-rw-r--r--  1 root root   18982 2012-02-16 04:48 CPL.TXT
-rw-r--r--  1 root root 51883209 2014-06-24 17:55 test1
root@bt:/pentest/passwords/crunch# █
```

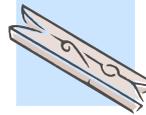
000000h2

1,1

Top

Constituer un dictionnaire

Crunch: option -p



- ☒ L'option `-p` suivi du jeu de caractères permet d'éviter de répéter chaque caractère dans le mdp

```
root@bt:/pentest/passwords/crunch# ./crunch 8 8 -o test2 -p 2602theo
Crunch will now generate approximately the following amount of data: 368000 bytes
0 MB
☒ 0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10320
100%
root@bt:/pentest/passwords/crunch#
```

```
☒ 0226e0th
0226e0tho
0226e0toh
-0226he0t
0226he0ta
0226he0te
0226he0t0
0226he0t1
0226he0t2
0226he0t3
0226he0t4
0226he0t5
0226he0t6
0226he0t7
0226he0t8
0226he0t9
0226he0t0a
0226he0t0b
0226he0t0c
0226he0t0d
0226he0t0e
```

22,1 Top

Constituer un dictionnaire

Wyd



⌘ Crunch

⌘ **Wyd**

- ☒ Outil de **profilage** de mots de passe
- ☒ **Extrait des chaînes de caractères** à partir de fichiers ou de répertoires.
- ☒ Analyse les fichiers en fonction de leur nature et extrait les **informations utiles** (titres de morceaux, compositeur pour des mp3 ou descriptions et titres d'images).
- ☒ **Exemple:**

```
mkdir /site-victime
cd site-victime/
wget -r http://www.site-victime.fr
perl wyd.pl -o liste-victime.txt -t -b -e /home/pirate/site-victime/
```

⌘ Cupp

Constituer un dictionnaire Cupp



⌘ Crunch

⌘ Wyd

⌘ Cupp

- ☑ Profilage automatique de mots de passe **communs**
- ☑ Recommandé de l'utiliser **à la suite de Wyd**
- ☑ **prédire des mots de passe simples** en exploitant les failles de l'humain

☑ Exemple:

```
python cupp.py -w /home/pirate/site-victime/liste-victime.txt
```

Les outils de craquage



⌘ John the ripper

☑ <http://www.openwall.com/john/>

⌘ RainbowCrack

☑ <http://www.antsight.com/zsl/rainbowcrack/>

⌘ Hydra

☑ <https://www.thc.org/thc-hydra/>

⋮

Les outils de craquage

John the ripper



⌘ deux modes en force brute:

☑ « single crack », incremental

⌘ un mode dictionnaire

☑ Wordlist

⌘ RainbowCrack

⌘ Hydra

Les outils de craquage

John: --rules



⌘ En mode dictionnaire, l'option --rules permet d'utiliser des règles de « trituration » (substitutions et permutations de caractères) des mots de passe candidats

⌘ Extrait du fichier john.conf:

```

-c 14 Q M T[z0] T[z1] T[z2] T[z3] Q
-c 15 Q M T[z0] T[z1] T[z2] T[z3] T[z4] Q
-c 16 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] Q
-c 17 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] T[z6] Q
# Very slow stuff...
1 Az-[1-90][0-9][0-9]" <+
-c (?a c Az [1-90][0-9][0-9]" <+
<[1-9] 1 A\p{L0}"[a-z][a-z]" <+
<- 1 ^[a-z] $[a-z]

# Wordlist: word rules
[List.Rules:Wordlist]
# Try words as they are
:
# Toggle case everywhere (up to length 8), assuming that certain case
# combinations were already tried.
-c T1 Q M T0 Q
-c T2 Q M T[z0] T[z1] Q
-c T3 Q M T[z0] T[z1] T[z2] Q
-c T4 Q M T[z0] T[z1] T[z2] T[z3] Q
-c T5 Q M T[z0] T[z1] T[z2] T[z3] T[z4] Q
-c T6 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] Q
-c T7 Q M T[z0] T[z1] T[z2] T[z3] T[z4] T[z5] T[z6] Q
# lowercase vowels, uppercase consonants: "Crack96" -> "CRaDk96"

```

Les outils de craquage

RainbowCrack



⌘ John the ripper

⌘ RainbowCrack

- ☒ Génération de **dictionnaires pré-calculés**
- ☒ Compromis entre % de résolution et taille du dictionnaire
- ☒ table disponibles publiquement ou non

⌘ Hydra

Les outils de craquage



⌘ John the ripper

⌘ RainbowCrack

⌘ Hydra

- ☒ Craquage de mots de passe en réseau
- ☒ Supporte une grande quantité de services réseaux
 - ☒ Ssh, imap, ftp, http, mysql etc.....



TD Hacking Éthique:
étape1 jusqu'au chapitre 5

Le PLAN



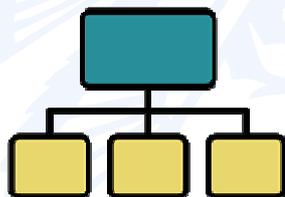
- ✓ Introduction
- ✓ Rappels
- ✓ Stratégies d'intrusion
- ✓ **Outils d'Intrusion**
 - ✓ Nmap
 - ✓ Metasploit
 - ✓ Craqueurs
- ✓ **Pour pivoter**
 - ✓ En cas d'incident
 - ✓ Conclusion

Pour pivoter

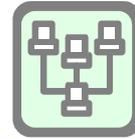


- . VPN
- .Redirection de Ports SSH
- .Firewalls
- .Proxchains

Pour pivoter

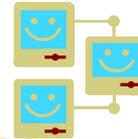
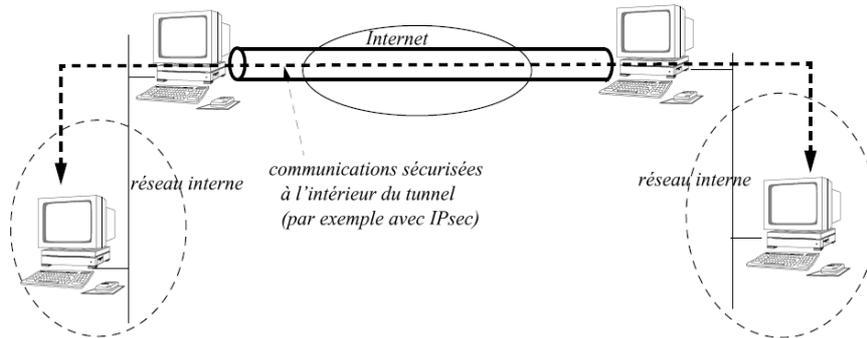


- . VPN
- .Redirection de Ports SSH
- .Firewalls
- .Proxchains



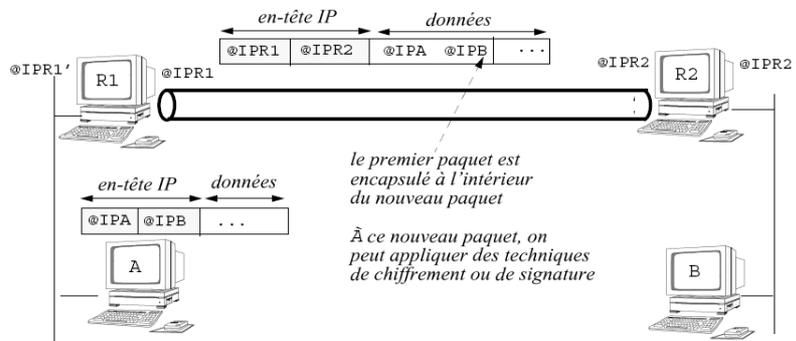
Rôle d'un VPN

- Rôle d'un VPN
 - permet à 2 réseaux d'**palier** se distribués géographiquement de constituer un seul réseau logique sûr et privé (chiffrement à l'intérieur du tunnel)
 - permet également de palier à un déficit d'adresses routables



Principe d'un VPN

- Principe
 - L'*encapsulation (ou tunneling)* de paquets dans d'autres paquets
 - Exemple avec IP (A envoie un paquet à B) :





Exemples de mise en oeuvre d'un VPN

- ⌘ Niveau **liaison** : **PPTP** (Point-to-Point Tunneling Protocol), **L2TP** (Layer 2 Tunneling Protocol)
- ⌘ Niveau **réseau** : **IPSec** (service ESP) en mode **tunnel**
- ⌘ Niveau **applicatif** : SSH, DNS2TCP

Pour pivoter



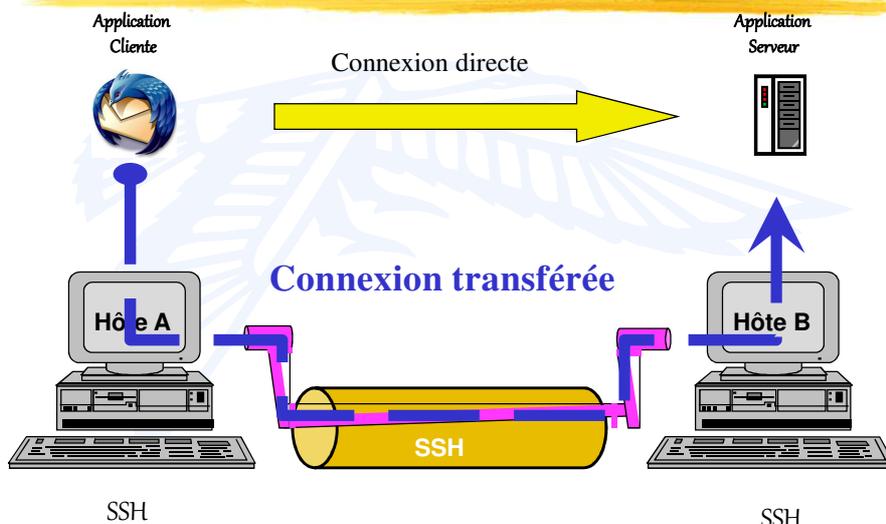
- . VPN
- . Redirection de port SSH
- . Firewalls
- . Proxychains

SSH : Redirection de port TCP



- ⌘ La redirection de port consiste à **encapsuler** un autre service TCP/IP (par exemple IMAP) dans une session SSH afin de leur apporter les bénéfices du tunnel de transport.

Redirection de Port TCP



Redirection de port TCP



- ⌘ La commande SSH est lancée, comme à l'accoutumée, à partir du client SSH.
 - ☒ Le référentiel local/distant est le client SSH
- ⌘ Deux types de redirection:
 - ☒ Redirection Locale:
 - C'est la machine qui crée le tunnel qui initie l'envoi des données dans ce tunnel
 - ☒ Redirection distante

Redirection de port TCP

Redirection Locale



- ⌘ C'est la machine qui crée le tunnel qui initie l'envoi des données dans ce tunnel .
- ⌘ le client imap et le client SSH sont sur la même machine
- ⌘ Syntaxe
 - `ssh -L port-local:machine-distante:port-distant serv_SSH`

Redirection Locale Exemple 1



- ⌘ le client imap et le client SSH sont sur la même machine
- ⌘ le serveur imap et le le serveur SSH sont sur la même machine

Redirection Locale Application



Machine1 veut lire ses nouveaux messages courriels :
sur le client SSH (machine1) on lance la commande :

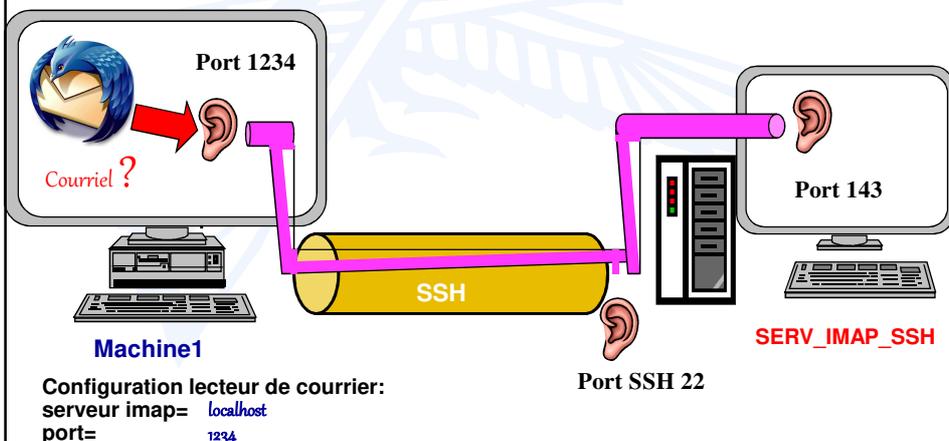


Client SSH

```
ssh -L 1234:localhost:143 serv_imap_ssh
```



Serveur SSH



Redirection Locale Exemple 2



- ⌘ le client imap et le client SSH sont sur la même machine
- ⌘ le serveur imap et le serveur SSH sont sur une machine différente

Redirection Locale Application

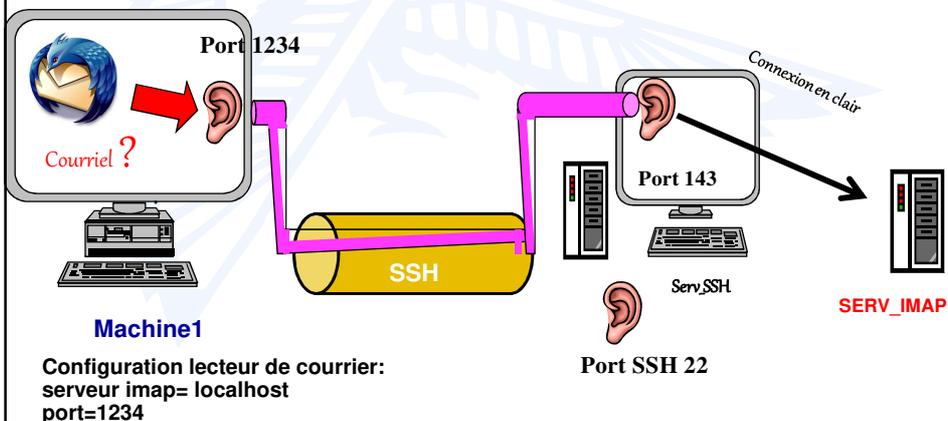


Machine1 veut lire ses nouveaux messages courriels :
sur le client SSH (machine1) on lance la commande :

```
ssh -L 1234: serv_imap: 143 serv_ssh
```



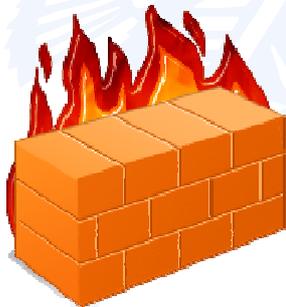
Client SSH





TD Hacking Éthique:
chapitre 5 Étape2: premier pivot

Pour pivoter



- . VPN
- .Redirection de Ports SSH
- **.Firewalls**
- .Proxchains

Caractéristiques d'un firewall (1/3)

Différents modes de fonctionnement

1. Fonctions de **filtre et de cloisonnement**
2. Fonctions de **relais et de masque (ie. proxy)**

Caractéristiques d'un firewall (1/2)

Différents modes de fonctionnement

1. Fonctions de **filtre et de cloisonnement**

- ☒ Concept simple, complètement transparent pour l'utilisateur interne ou externe, rapide
- ☒ Difficulté de paramétrer la configuration de façon cohérente, pas de mécanisme d'authentification
- ☒ Différents types
 - ☒ **Firewall routeur** (stateless firewall) : analyse chaque paquet selon un ensemble de règles déterminées qui constituent le filtre et les informations contenues dans le paquet
 - ☒ **Statefull firewall** : permet de filtrer les paquets en se basant sur la couche transport (ports de communication UDP-TCP)

Caractéristiques d'un firewall (2/2)

Différents modes de fonctionnement

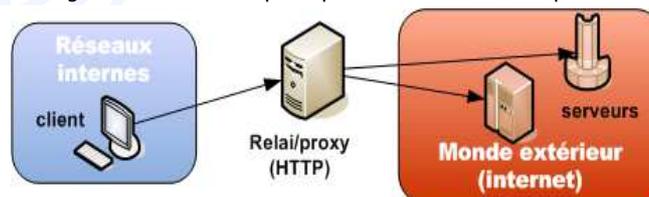
2. Fonctions de relais et de masque (ie. proxy)

- ☒ Application-level gateway (ALG)
- ☒ Circuit-level gateway (CLG)

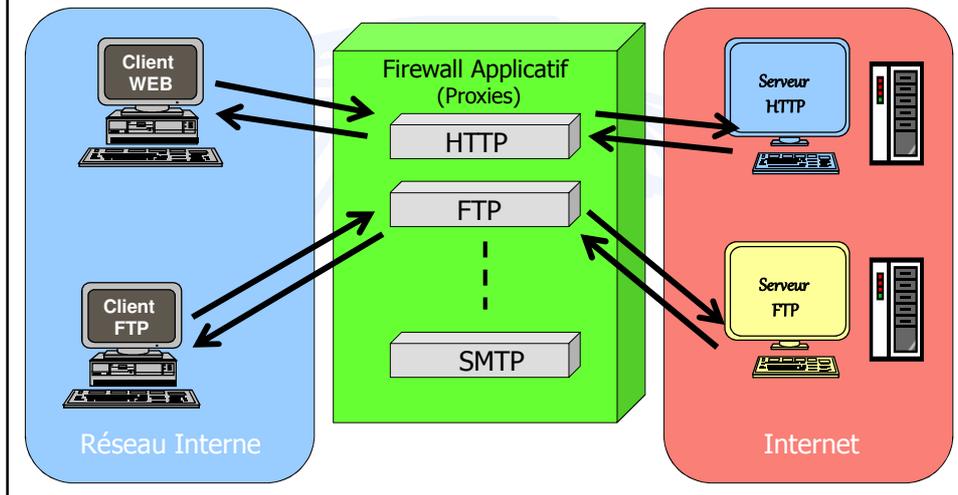
Fonctions de relais et de masque en ALG (1)

⌘ Principe

- ☒ Permet d'établir un relai entre le réseau interne et le réseau externe en se basant sur le contenu des messages au niveau applicatif,
- ☒ Un utilisateur externe demande une connexion TCP/IP à la passerelle, qui authentifie et qui, en cas de succès, contacte l'application que l'utilisateur demande,
- ☒ Nécessite la collaboration de la part des systèmes finaux.
 - **Exemple** : utilisation d'un serveur proxy cache *http* pour sortir sur internet depuis un réseau interne; il est nécessaire sur le poste client de modifier la configuration du browser pour qu'il utilise le serveur http interne.



Fonctions de relais et de masque en ALG (2)



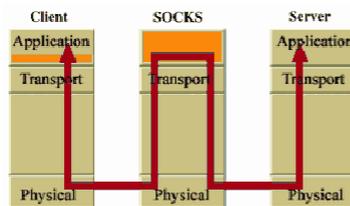
Fonctions de relais et de masque en CLG (1)

- Principe
 - permet d'établir un relai au niveau transport
 - empêche l'établissement d'une connexion TCP (ou UDP) point à point
 - ⇒ établissement de deux connexions différentes : la première dans le réseau protégé avec la machine interne et la seconde avec la machine externe
- Avantages
 - pas spécifique à une application : est donc plus "générique" a priori
- Inconvénients
 - effectue des contrôles moins précis que l'application-level gateway
 - ⇒ fonctionnellement équivalent à un packet-filter

Fonctions de relais et de masque en CLG (2)

- Exemple (1)

- SOCKS (<http://www.socks.permeo.com>)
- SOCKSv5 est un standard IETF (rfc1928) et un outil associé
- 2 composants : le serveur et client
 - + le serveur est implémenté au niveau de la couche application
 - + le client est implémenté entre la couche transport et la couche application



Fonctions de relais et de masque en CLG (3)

- Exemple (2)

- configuration du serveur
 - => effectue de l'authentification, du relai (UDP, TCP)
 - => `/etc/sockd.conf`

```

permit ... ← accès autorisés
deny ... ← accès refusés

```

- configuration du client

- + les applicat librairie ielles (`telnet`, `ftp`, ...) doivent être modifiées de façon à ce qu'elles utilisent la librairie de SOCKS : cette librairie permet d'effectuer des accès au serveur SOCKS si nécessaire de façon transparente pour les utilisateurs
- + dans le fichier `/etc/socks.conf`, on indique quels accès extérieurs doivent passer par le serveur SOCKS, quels accès extérieurs ne sont pas relayés


```

direct ... ← accès non relayés
sockd ... ← accès relayés

```

Pour pivoter

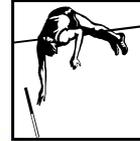


- . VPN
- .Redirection de Ports SSH
- .Firewalls
- .Proxychains

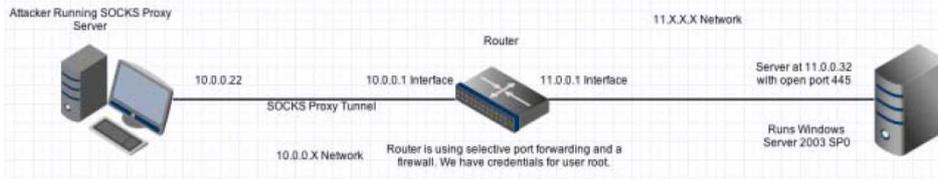
PROXYCHAINS : principes



- ⌘ Proxychains est un outil qui permet de faire sortir le trafic d'une application à travers un tunnel SOCKS précédemment configuré et ouvert
- ⌘ Etant donné que le tunnel SOCKS peut être ouvert vers n'importe quelle autre machine, Proxychains permet de faire exécuter une application sur n'importe quelle machine distante (i.e. la sortie du tunnel SOCKS)
- ⇒ Contournement aisé de la politique de sécurité d'un Firewall



PROXYCHAINS : exemple (1)



⌘ Le firewall n'autorise que le trafic SSH

⌘ L'attaquant veut contacter le serveur Windows (situé derrière le routeur) sur le port 445 (Microsoft Directory Services aka Netbios)



PROXYCHAINS : exemple (2)

1. Mettre en place le tunnel SOCKS (via SSH) entre l'attaquant et le Firewall
`root@bt: ssh -NfD 9050 root@10.0.0.1`
2. Configurer proxychains (fichier /etc/proxychains.conf) sur la machine de l'attaquant :

```
[ProxyList]
# add proxy here ...
socks4 127.0.0.1 9050
```
3. Utilisation de proxychains depuis la machine de l'attaquant :
`root@bt: proxychains msfconsole`

*L'attaquant peut maintenant utiliser metasploit pour exploiter une vulnérabilité du serveur Windows (port 445) qui se situe derrière le routeur
 ⇒ Tout le trafic généré par Metasploit sera directement redirigé vers l'interface de sortie du routeur (sur le réseau privé)*



PROXYCHAINS : utilisation avancée (1)

- ⌘ Le nombre de redirection que l'on peut concatener dans proxychain n'est pas limité
- ⌘ Dans le TP vous utiliserez deux chainages successifs :
 1. Premier tunnel SOCKS (traverser le Firewall et arriver sur le serveur FTP)
 2. Deuxième tunnel SOCKS (rebondir du FTP vers la machine dont le compte lamaison a été trouvé @192.168.1.1)
- ⌘ Vous utiliserez ainsi NMAP en local mais il sera exécuté sur le réseau distant à travers un premier pivot (atteignable via le premier serveur SOCKS)

```
root@bt:~/proxychains1# ssh -f -D 127.0.0.1:7777 root@192.168.1.21
root@bt:~/proxychains1# netstat -en | grep 7777
tcp        0      0 127.0.0.1:7777      0.0.0.0:*           LISTEN
root@bt:~/proxychains1#
```

- ⌘ puis un deuxième pivot (atteignable via le deuxième serveur SOCKS)

```
root@bt:~/proxychains1# proxychains ssh -f -D 127.0.0.1:8888 lamaison@192.168.1.1
ProxyChains-3.1 (http://proxychains.sf.net)
[S-chain]->-127.0.0.1:7777-<->-192.168.1.1:22-<->-OK
lamaison@192.168.1.1's password:
root@bt:~/proxychains1#
```

PROXYCHAINS : utilisation avancée (2)

- ⌘ Il est maintenant possible de pouvoir utiliser un outil comme NMAP depuis la machine de l'attaquant :

proxychains nmap -v -sT-PN -n 192.168.2.1-10 -p 25-80

```
root@bt:~/proxychains2# proxychains nmap -v -sT -PN -n 192.168.2.1-10 -p 25-80
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 6.01 ( http://nmap.org ) at 2014-06-25 15:25 CEST
Initiating Connect Scan at 15:25
Scanning 10 hosts [56 ports/host]
[S-chain]->-127.0.0.1:8888-<->-192.168.2.2:53-<--timeout
[S-chain]->-127.0.0.1:8888-<->-192.168.2.5:53-channel 1: open failed: connect fai
: Connection timed out
```

- ⇒ La commande sera lancée depuis la machine de l'attaquant, pivotera sur le serveur FTP, puis sur la machine dont vous avez précédemment trouvé le compte lamaison pour finalement scanner le réseau 192.168.2.1 – 192.168.2.10

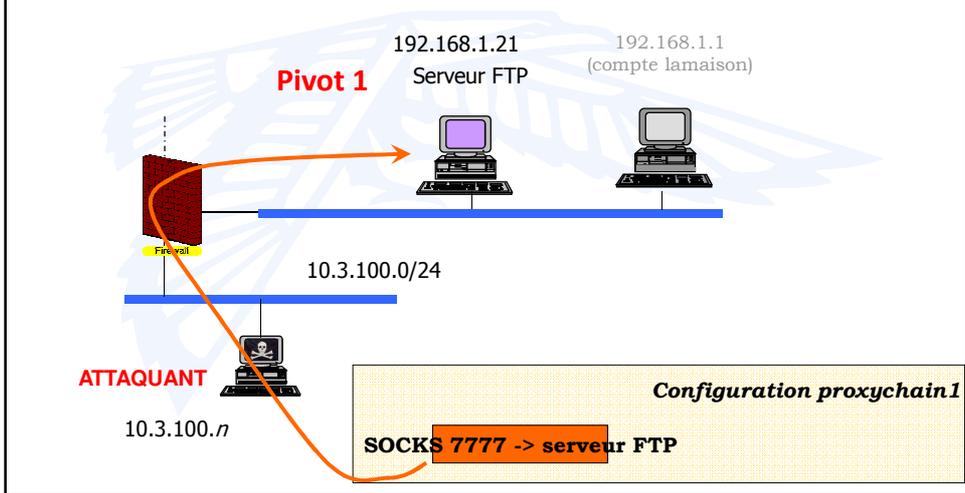
- **Remarque de configuration :** l'utilisation de deux redirections proxychain nécessite deux configurations différentes de proxychains c'est la raison pour laquelle le **nmap est exécuté dans le répertoire proxychains2**

Fichier /etc/proxychains.conf
socks4 127.0.0.1 8888

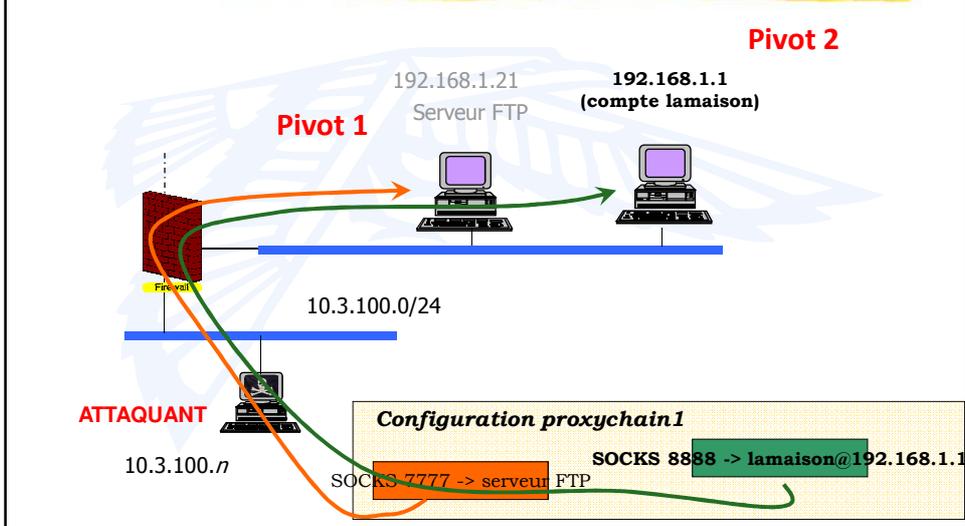
et les deux pivots précédents dans le répertoire proxychain1

Fichier /etc/proxychains.conf
socks4 127.0.0.1 7777

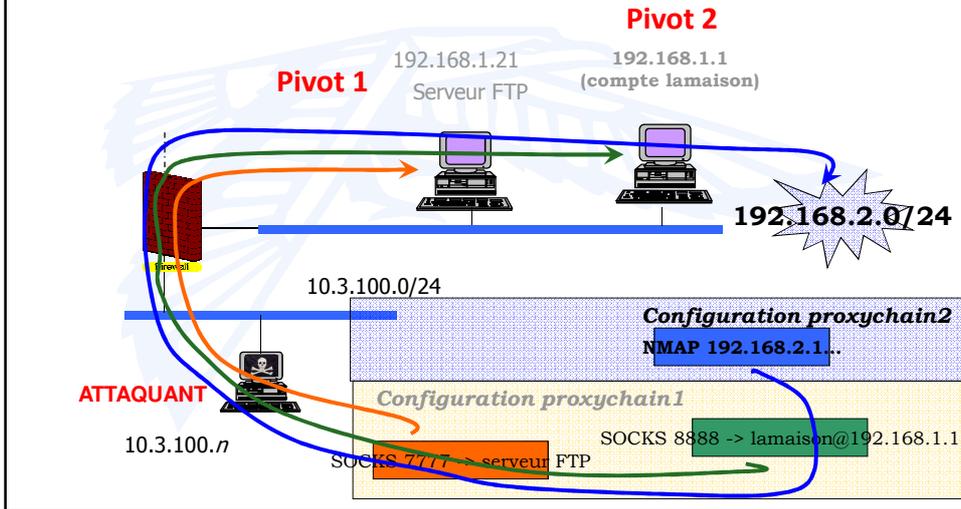
PROXYCHAINS : résumé des tunnels SOCKS utilisés



PROXYCHAINS : résumé des tunnels SOCKS utilisés



PROXYCHAINS : résumé des tunnels SOCKS utilisés



TD Hacking Éthique: Chapitres 6 et 7
(étapes 3 et 4)