ENAC

TLS-SEC

Hacking réseau éthique

L. HAJNAL / N. LARRIEU

2017

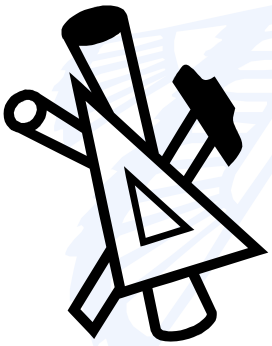
ENAC

Objectifs

A la fin du cours l'étudiant saura:

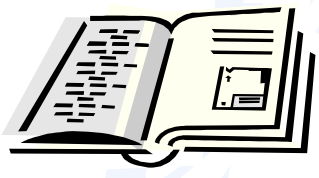
- Apprécier comment lister, quantifier et limiter l'ensemble des vulnérabilités inhérentes aux architectures système et réseau.
- Connaître les grandes techniques de tentatives d'intrusions système ou réseau et les contremesures à déployer dans le système pour s'en prémunir.
- Connaître la problématique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



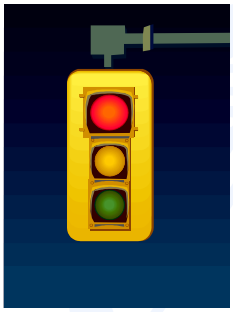
- ✓ Introduction
  - ✓ Rappels
  - ✓ Stratégies d'intrusion
  - ✓ Outils d'Intrusion
  - ✓ En cas d'incident
  - ✓ Conclusion

Livre Blanc de la défense

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

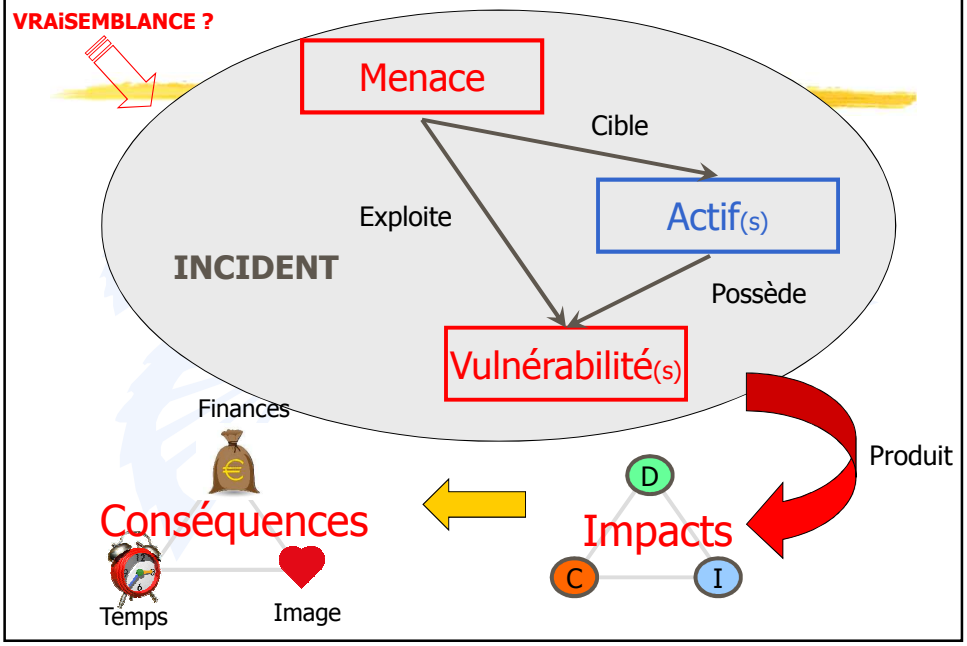
- LA loi de programmation militaire de décembre 2013 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale.

Le PLAN



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

Dynamique du risque



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 : Faille 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

ENAC

Stratégies d'intrusion

-. Idées générales

-. Recueil d'informations

-. Exploitation de vulnérabilités

-. Pivot

ENAC

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

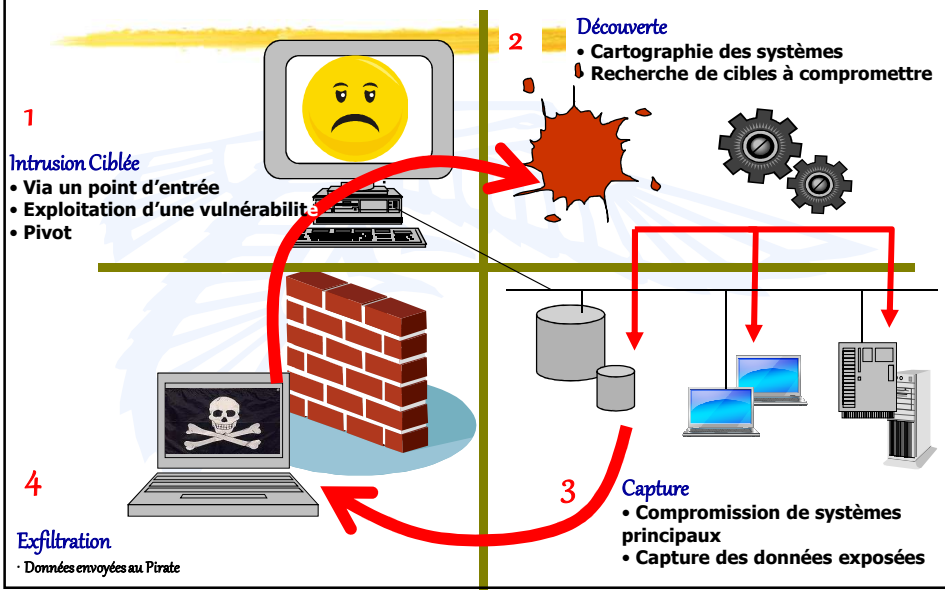
ENAC

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)

ENAC

Intrusion Logique



ENAC

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)

ENAC

Stratégies d'intrusion

-.Idées générales

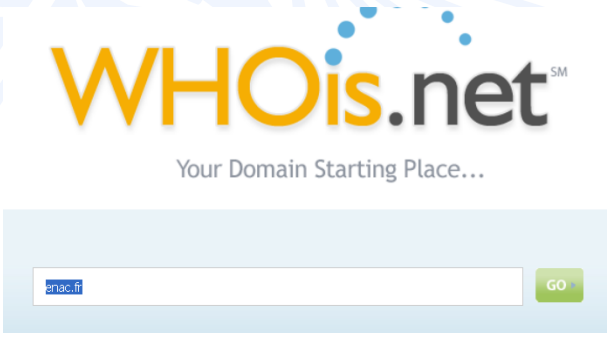
-. Recueil d'informations

-. 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.houalla@enac.fr
registrar:   GIP 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
registrar:   GIP 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

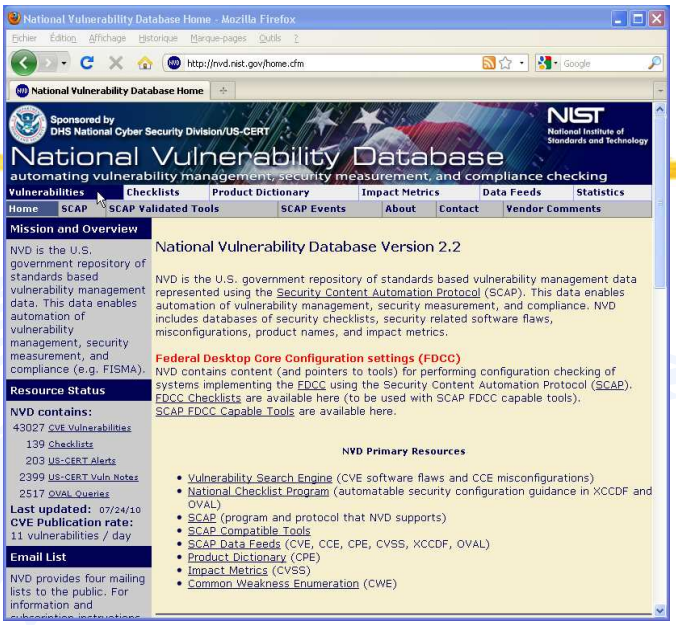
- Cartographie du réseau
  - Balayage des @ IP
- Cartographie des services
  - Balayage de ports
- savoir quels systèmes sont présents
  - Noyau, distrib, service pack ?
- savoir quels logiciels assurent les services
  - version ?

ENAC

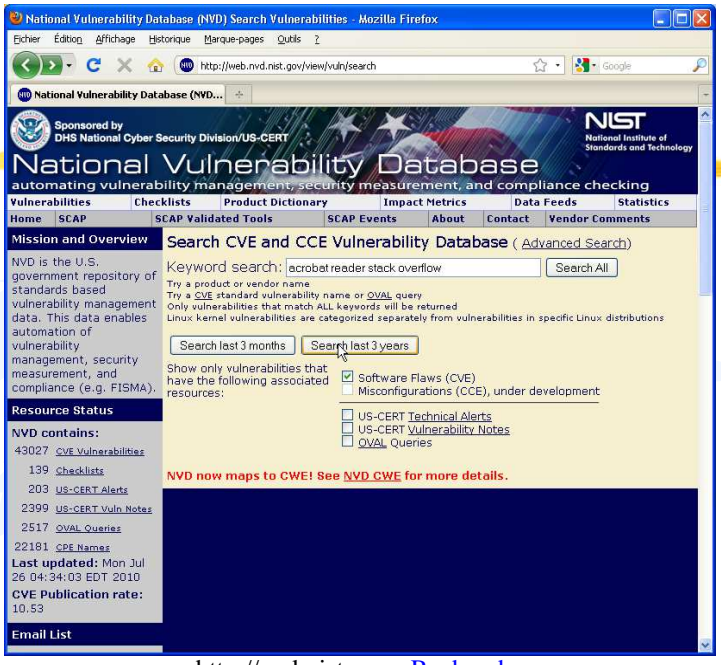
Répertoriage des Vulnérabilités Logiques

- 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.

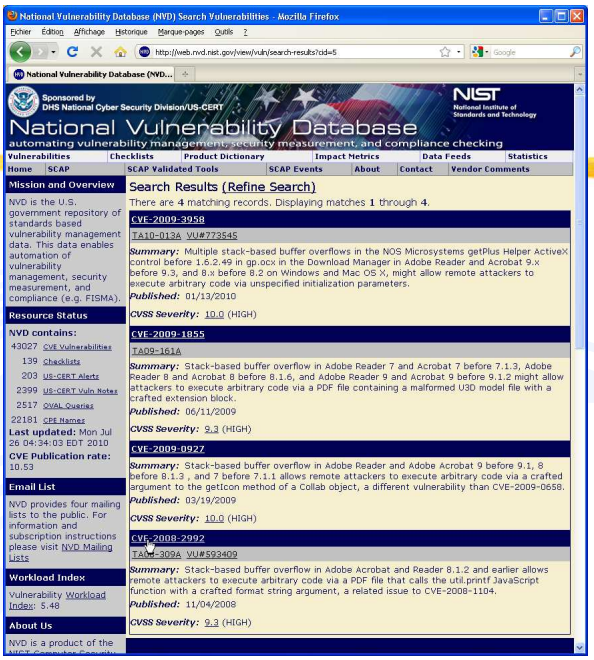
ENAC



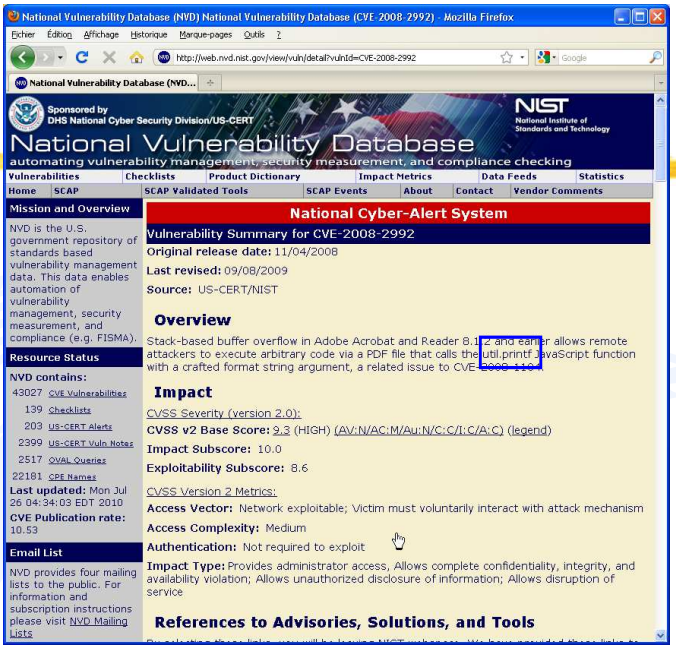
http://nvd.nist.gov
Accueil



http://nvd.nist.gov Recherche



http://nvd.nist.gov Résultats



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

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

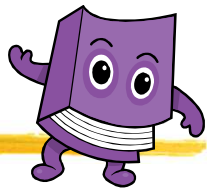
- A partir de la liste des utilisateurs on essaye une séries de combinaisons: permutation, substitutions + ou - simples
- Ex: pour l'utilisateur *administrateur on essaye*

'	(pas de mot de passe)
administrateur	(mdp=nom de login)
rdministrateua	(permutations en tous genres)
admin123456	(subtitutions)
AdminIstraTeur	(subtitutions avec des lettres majuscules)

ENAC

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 une fonction de dérivation (algorithme de Hellman)

ENAC

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[])

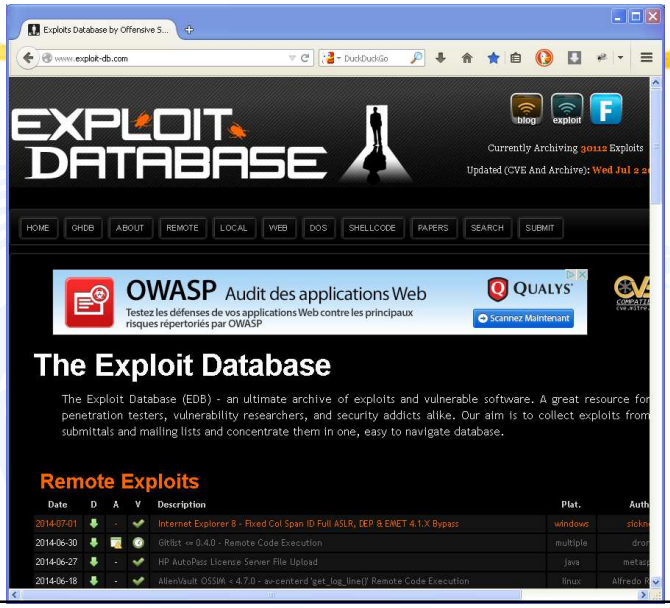
- Unix(s), Microsoft, Adobe, Oracle, open source… beaucoup d'exploits
- Quelques sites parmi d 'autres

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

  http://packetstormsecurity.org
- Cadriciel d'exploitation: Metasploit

Exploit Database

Main (int argc ,char* argv[])



ENAC

Stratégies d'intrusion

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

-. Pivot

ENAC

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.

ENAC

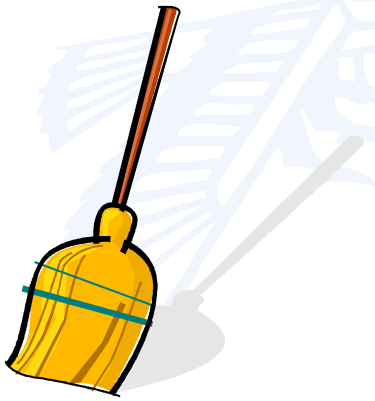
TD Hacking Éthique:
environnement de travail

ENAC

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

ENAC

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

ENAC

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).

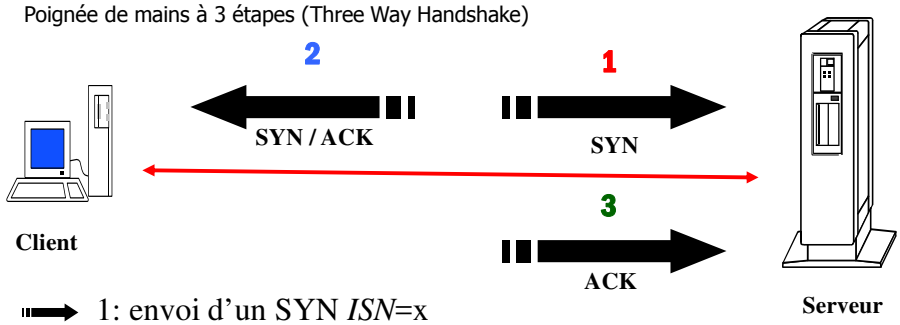
-P0 Permet de scanner les machines qui n'autorisent pas les ICMP echo request.

NMAP

principe de fonctionnement (port TCP actif)

⌘ TCP – Etablissement de Connexion

Poignée de mains à 3 étapes (Three Way Handshake)



1: envoi d'un SYN *ISN*=x

2: envoi SYN *ISN*=y, ACK x+1

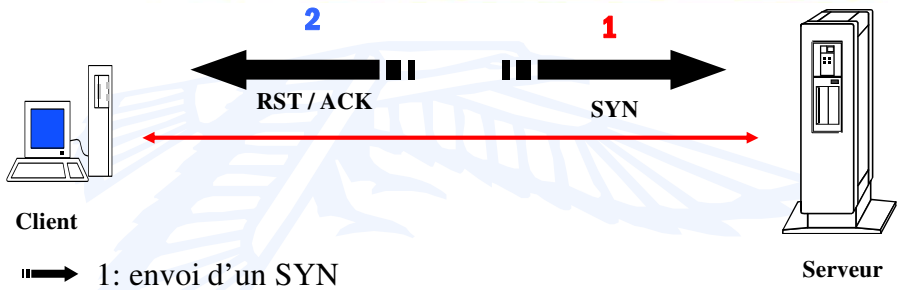
3: Send ACK *ISN* y+1

4: La connexion est établie

ISN = numéro de séquence initial

NMAP

principe de fonctionnement (port TCP inactif)



1: envoi d'un SYN

2: envoi RST, ACK

3: Le port n'est pas actif sur le serveur

ISN = numéro de séquence initial

ENAC

NMAP

scan de port UDP (1)

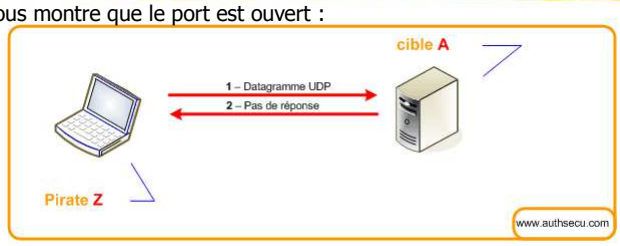
- Le protocole UDP est ne requiert pas de connexions. Il y 2 manières d'énumérer les services UDP sur notre cible :
  - Envoyer des paquets UDP sur les 65535 ports et attendre un "ICMP destination port unreachable" qui signifie que le port est fermé, inaccessible ou que la machine est hors service.
  - 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)

ENAC

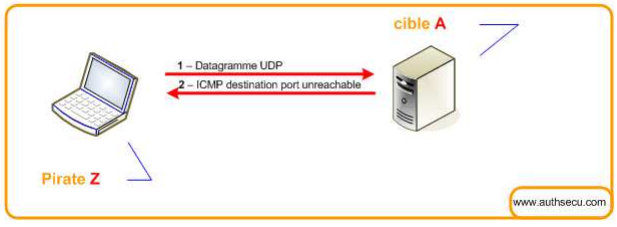
NMAP

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 :



ENAC

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).

ENAC

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'echo 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

ENAC

TD Hacking Éthique:
étape1 jusqu'au 4.4

ENAC

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

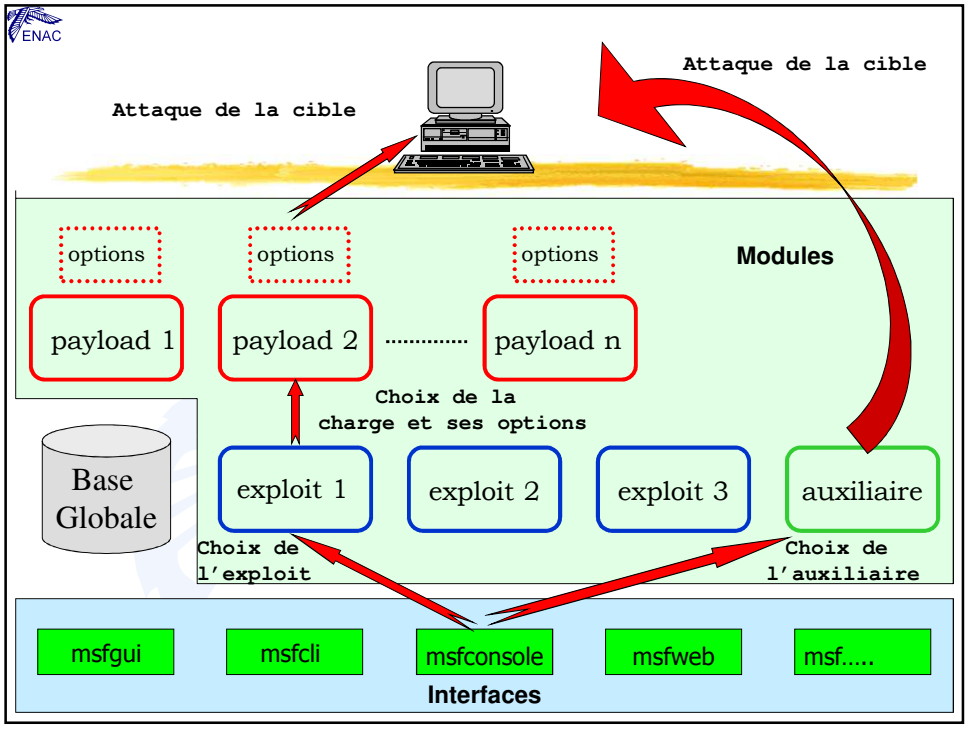

```
Fichier  Édition  Affichage  Terminal  Aide
root@incs22:/etc/init.d# msfconsole

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

msf >
```

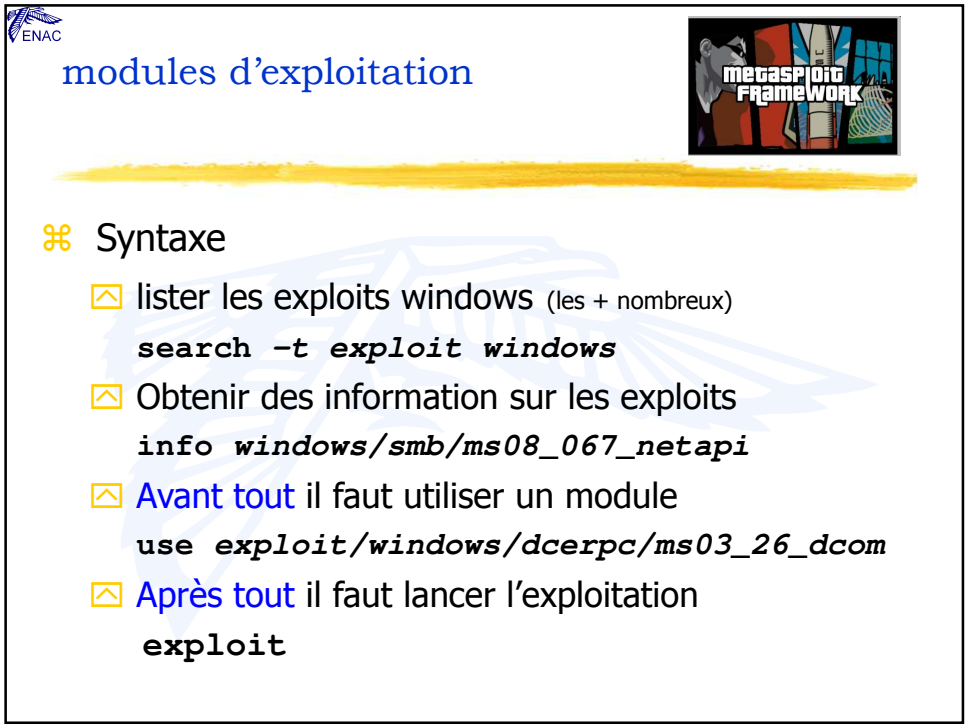
Architecture modulaire
3 Modules principaux

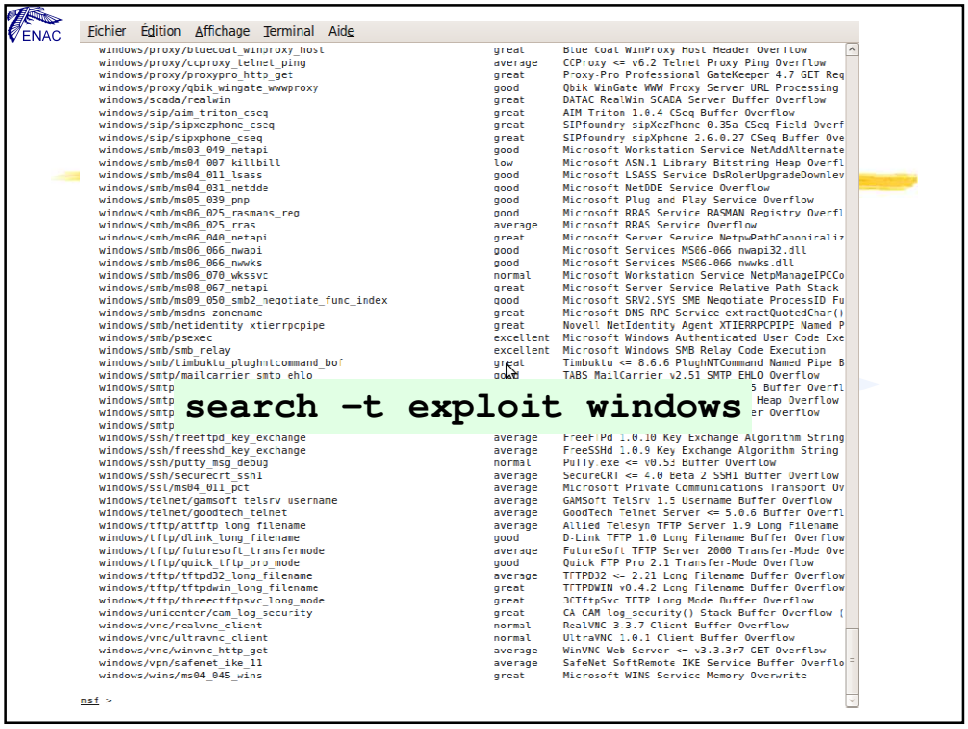
- Code d'exploitation (exploit)
- Charge utile (payload)
  - associé au code d'exploitation choisi
  - permet d'assurer la communication entre Metasploit et la victime
- Auxiliaire (auxiliary)
  - actions arbitraires telles que le scan de ports,
  - le déni de services entre autres

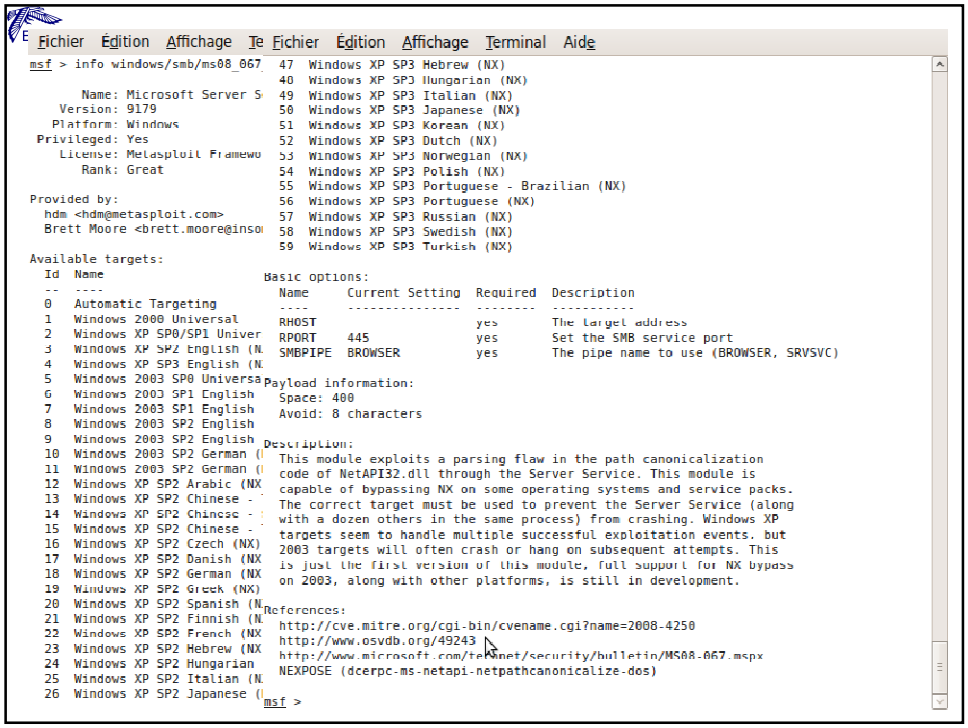
Architecture modulaire
Avantage

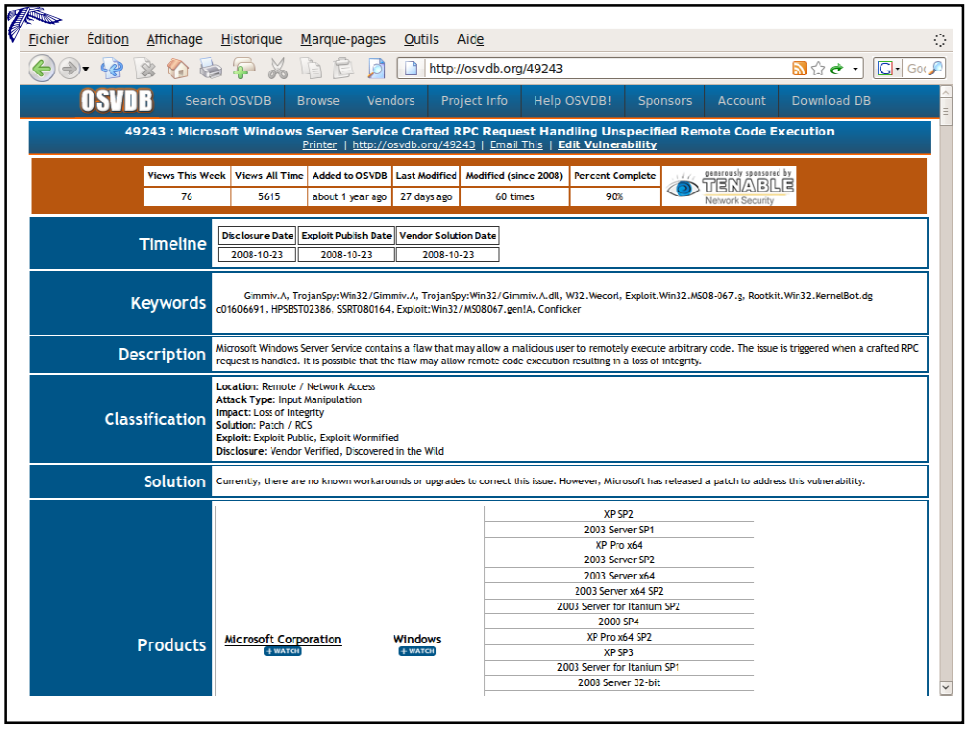
- utiliser plusieurs charges utiles pour un même code d'exploitation
- et vice-versa.


ENAC
Attaque de la cible
Attaque de la cible
options
options
options
Modules
payload 1
payload 2
payload n
Choix de la
charge et ses options
Base
Globale
exploit 1
exploit 2
exploit 3
auxiliaire
Choix de
l'exploit
Choix de
l'auxiliaire
msfgui
msfcli
msfconsole
msfweb
msf.....
Interfaces


ENAC
modules d'exploitation
metasploit
FRAMEWORK
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 Édition Affichage Terminal Aide
search -t exploit windows
msf >


Fichier Édition Affichage Terminal Aide
msf > info windows/smb/ms08_067
Name: Microsoft Server S
Version: 9179
Platform: Windows
Privileged: Yes
License: Metasploit Framewo
Rank: Great
Provided by:
hdm <hdm@metasploit.com>
Brett Moore <brett.moore@inso
Available targets:
Id Name
0 Automatic Targeting
1 Windows 2000 Universal
2 Windows XP SP0/SP1 Univer
3 Windows XP SP2 English (N
4 Windows XP SP3 English (N
5 Windows 2003 SP0 Universa
6 Windows 2003 SP1 English
7 Windows 2003 SP1 English
8 Windows 2003 SP2 English
9 Windows 2003 SP2 English
10 Windows 2003 SP2 German (
11 Windows 2003 SP2 German (
12 Windows XP SP2 Arabic (NX
13 Windows XP SP2 Chinese -
14 Windows XP SP2 Chinese -
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 (N
21 Windows XP SP2 Finnish (N
22 Windows XP SP2 French (NX
23 Windows XP SP2 Hebrew (NX
24 Windows XP SP2 Hungarian
25 Windows XP SP2 Italian (N
26 Windows XP SP2 Japanese (
47 Windows XP SP3 Hebrew (NX)
48 Windows XP SP3 Hungarian (NX)
49 Windows XP SP3 Italian (NX)
50 Windows XP SP3 Japanese (NX)
51 Windows XP SP3 Korean (NX)
52 Windows XP SP3 Dutch (NX)
53 Windows XP SP3 Norwegian (NX)
54 Windows XP SP3 Polish (NX)
55 Windows XP SP3 Portuguese - Brazilian (NX)
56 Windows XP SP3 Portuguese (NX)
57 Windows XP SP3 Russian (NX)
58 Windows XP SP3 Swedish (NX)
59 Windows XP SP3 Turkish (NX)
Basic options:
Name Current Setting Required Description
RHOST yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload information:
Space: 400
Avoid: 8 characters
Description:
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.
The correct target must be used to prevent the Server Service (along
with a dozen others in the same process) from crashing. Windows XP
targets seem to handle multiple successful exploitation events, but
2003 targets will often crash or hang on subsequent attempts. This
is just the first version of this module, full support for NX bypass
on 2003, along with other platforms, is still in development.
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 >



ENAC

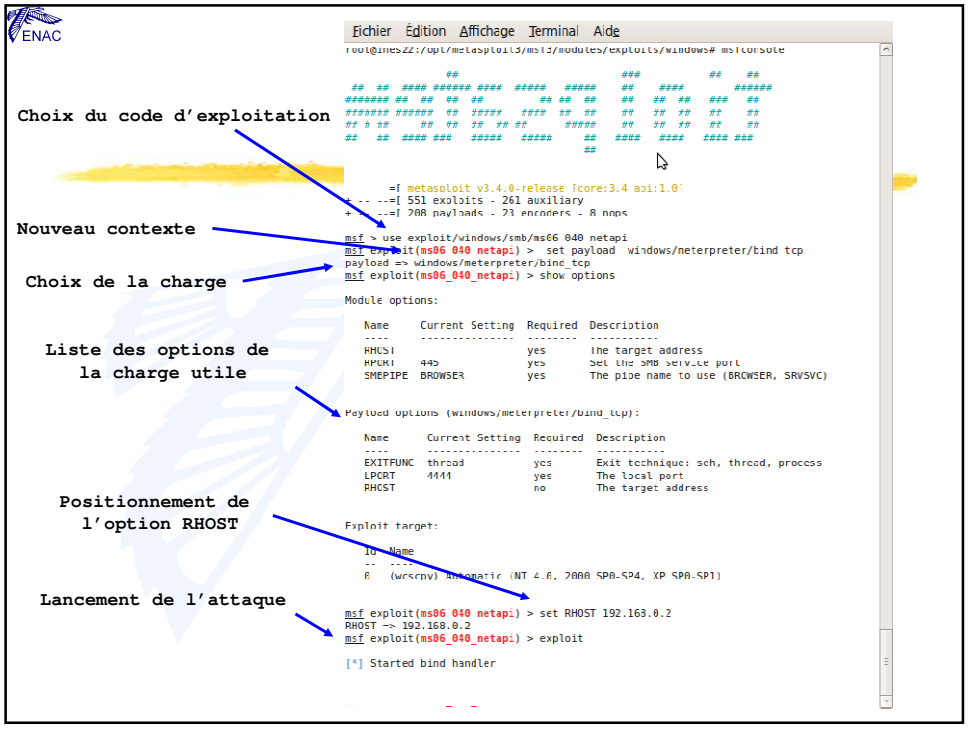
Modules payload

- 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 »***



Modules auxiliaire

- Module sweep_udp (scan)

  msf > **use auxiliary/scanner/discovery/udp_sweep**

  msf auxiliary (udp_sweep)> **set RHOSTS 192.168.0.0/24**

  RHOSTS => 192.168.0.0/24

  Pour lancer la découverte d'hôte :

  msf auxiliary (udp_sweep)> **run**

- Module smb/version

  msf > **use auxiliary/scanner/smb/smb_version**

  msf auxiliary (smb_version)> **set RHOSTS 192.168.0.12**

  msf auxiliary(smb_version) > **run**

  [*] 192.168.0.12 is running Windows XP Service Pack 2+

  [*] Auxiliary module execution completed

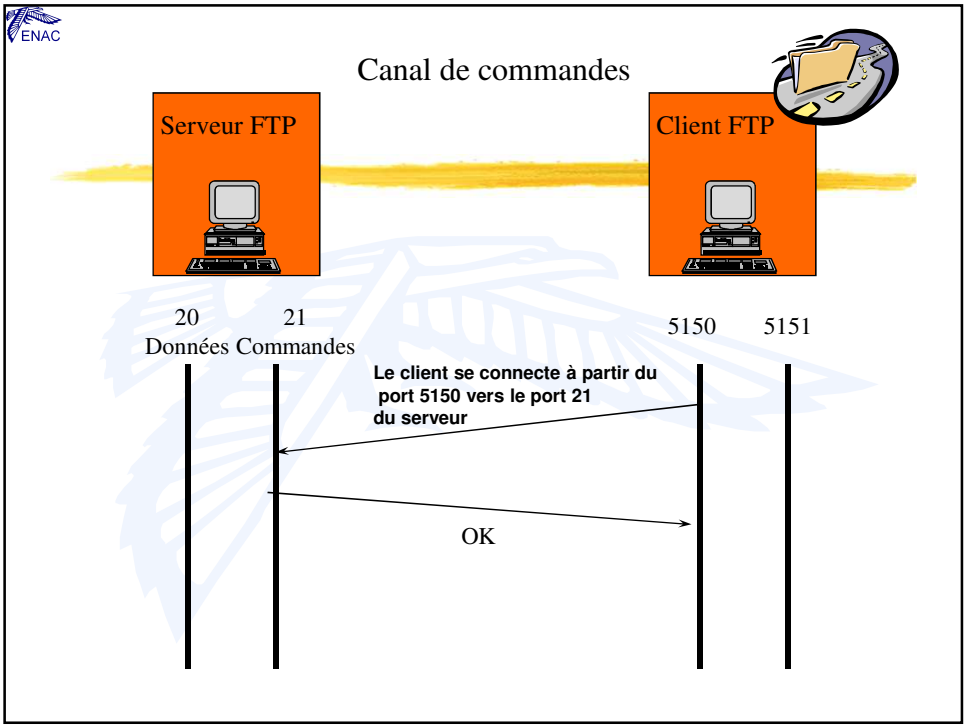
TD Hacking Éthique: 4.5 et 4.6

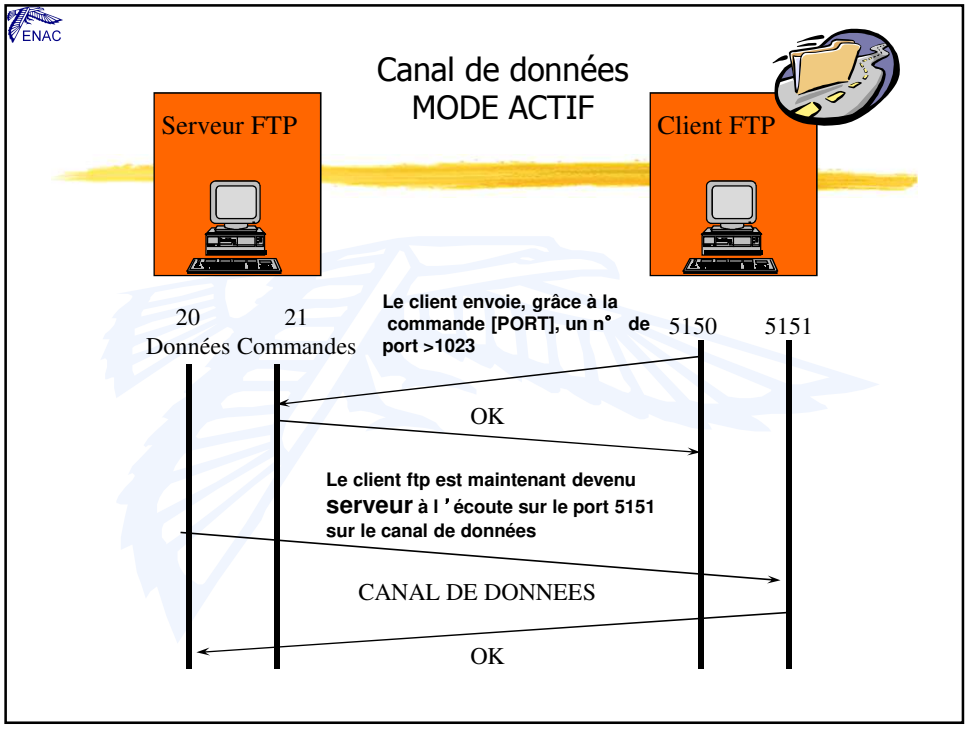
TRANSFERT DES FICHIERS

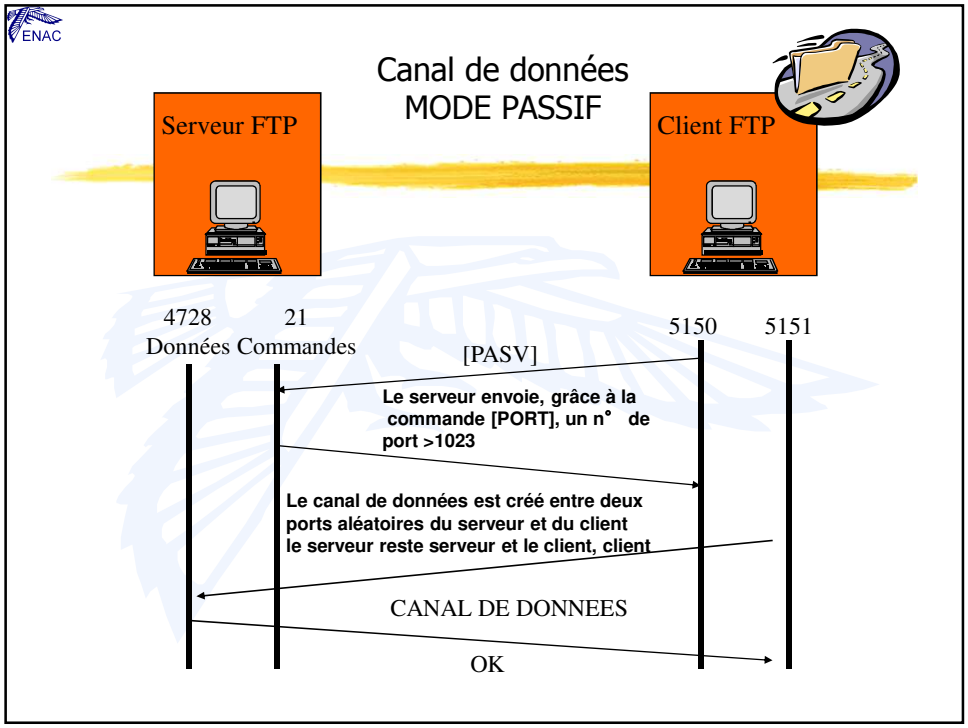
- Le protocole FTP présente les particularités suivantes:
  - Il y a un canal de commandes (port 21)
  - et un canal de données (port 20 ou > 1023)
  - Deux modes de fonctionnement
    - le mode actif
    - le mode passif
- Ftp tourne au dessus de TCP

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 peut suivant que le serveur est en mode actif ou passif

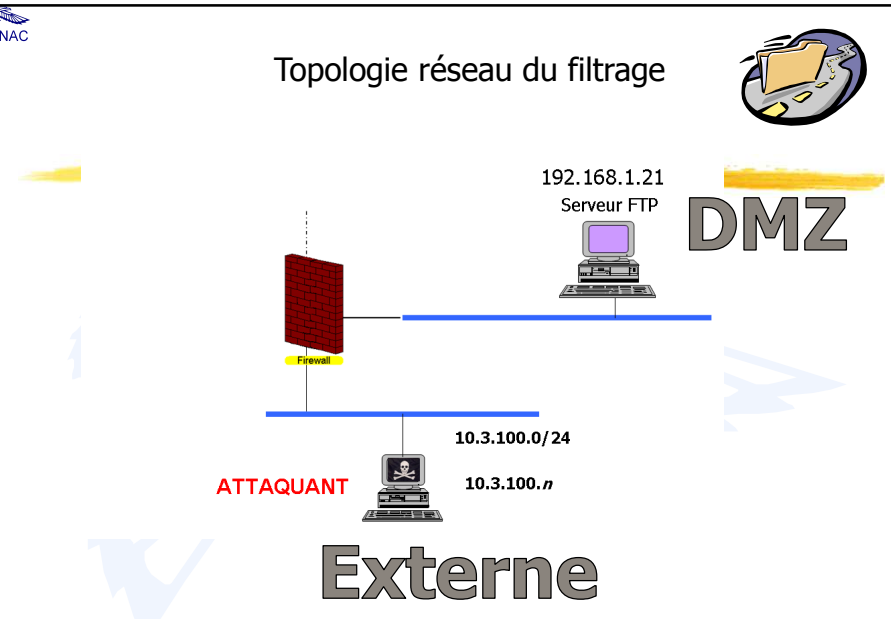



ENAC
Canal de données
MODE ACTIF
Serveur FTP
Client FTP
20
Données
21
Commandes
Le client envoie, grâce à la commande [PORT], un n° de port >1023
5150
5151
OK
Le client ftp est maintenant devenu serveur à l 'écoute sur le port 5151 sur le canal de données
CANAL DE DONNEES
OK


ENAC
Canal de données
MODE PASSIF
Serveur FTP
Client FTP
4728
Données
21
Commandes
5150
5151
[PASV]
Le serveur envoie, grâce à la commande [PORT], un n° de port >1023
Le canal de données est créé entre deux ports aléatoires du serveur et du client
le serveur reste serveur et le client, client
CANAL DE DONNEES
OK

ENAC

Topologie réseau du filtrage



ENAC

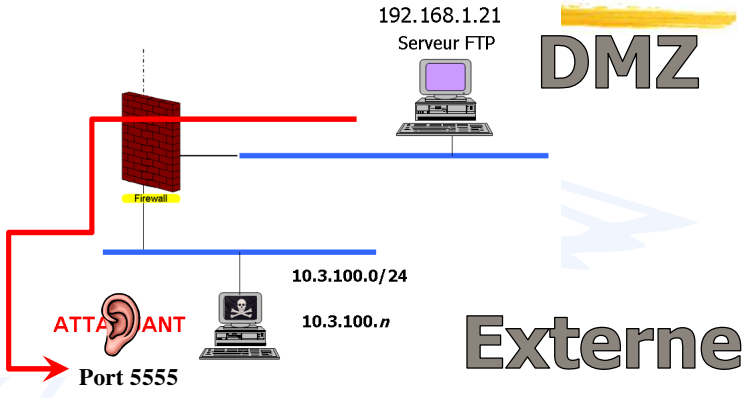
Règles de filtrage FTP: externe -> DMZ

- ✓ 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

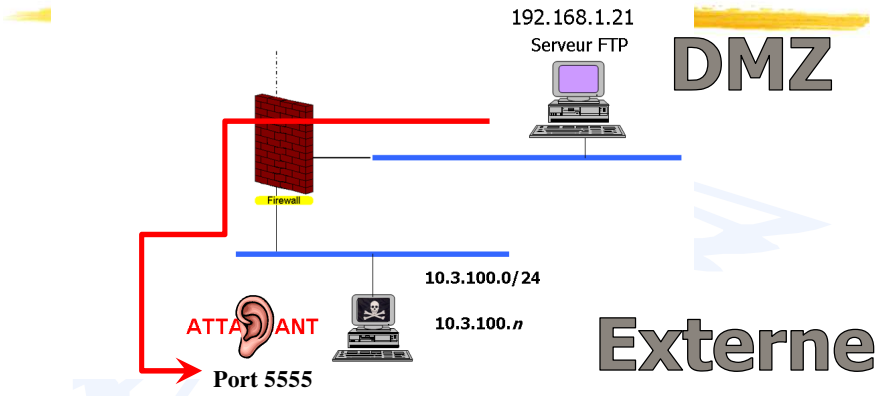
Rappel sur la charge Finale Metasploit



PAYLOAD meterpreter en reverse TCP:
Contact initié par 192.168.1.21 vers le port 5555 de l'attaquant positionné en écoute (mode serveur)

ENAC

OÙ EST l'ERREUR ?



Observons de plus près les règles de filtrage du FireWall

ENAC

Faille-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 --dport1024:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT

ENAC

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

ENAC

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

ENAC

Faille-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

ENAC

TD Hacking Éthique:
étape1 jusqu'au 4.7.1

ENAC

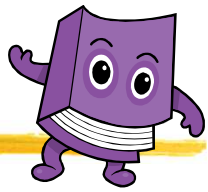
Le PLAN

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

ENAC

Les outils de craquage

Constituer un dictionnaire



⌘Crunch

- http://sourceforge.net/projects/crunch-wordlist/files/

⌘WYD (Who's Your Daddy?)

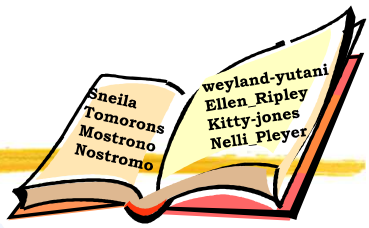
- Infos: http://www.socialengineer.org/framework/Computer_Based_Social_Engineering_Tools:_Who's_Your_Daddy_Password_Profiler_(WYD)
- Télécharger: http://www.remote-exploit.org/content/wyd-0.2.tar.gz

⌘Cupp (Common User Passwords Profiler)

- Infos: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Common_User_Passwords_Profiler_(CUPP)
- Télécharger: http://www.remote-exploit.org/articles/misc_research__amp_code/index.html

ENAC

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 chaines 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

ENAC

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

ualpha                          = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                    = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
ualpha-numeric                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space            = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
                                                                4,1           1%
```

Constituer un dictionnaire

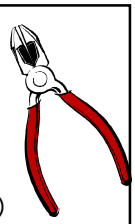
Crunch: charset persos

- Il est possible de personnaliser le fichier charset.lst
- Ici je créée 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           1%
```

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
49 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 5764801
100%
root@bt:/pentest/passwords/crunch#
```

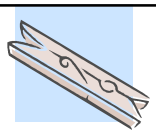
- Taille du

```
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     5657 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 51883209 2014-06-24 17:55 test1
root@bt:/pentest/passwords/crunch#
                                                      1,1           Top
```

ENAC

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: 362880 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 40320
100%
root@bt:/pentest/passwords/crunch#

0226eoth
0226etho
0226etoh
0226heot
0226heto
0226hoet
0226hote
0226hteo
0226htoe
0226uhil
0226oeth
0226ohet
0226ohte
0226oteh
0226othe
0226teho
0226toeh
0226theo
0226thoe
                                                22,1          Top
```

s)

ENAC

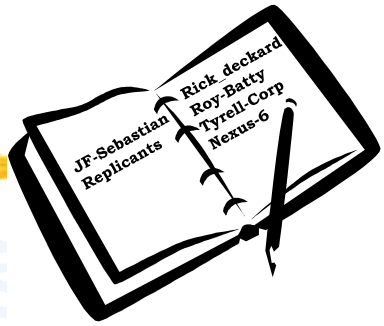
Constituer un dictionnaire

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

ENAC

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

ENAC

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/

ENAC

Les outils de craquage

John the ripper

- deux modes en force brute:
  - « single crack », incremental
- un mode dictionnaire
  - Wordlist
- RainbowCrack
- Hydra

ENAC

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 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
# Very slow stuff...
l Az"[1-90][0-9][0-9]" <+
-c (?a c Az"[1-90][0-9][0-9]" <+
<[\-9] l A\p[z0]"[a-z][a-z]"
<- l ^[a-z] $[a-z]

# Wordlist mode 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" -> "CRaCK96"
```

ENAC

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

ENAC

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…..

ENAC

TD Hacking Éthique:
étape1 jusqu'au chapitre 5

ENAC

Le PLAN

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

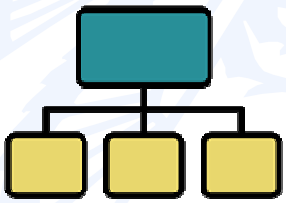
ENAC

Pour pivoter

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

ENAC

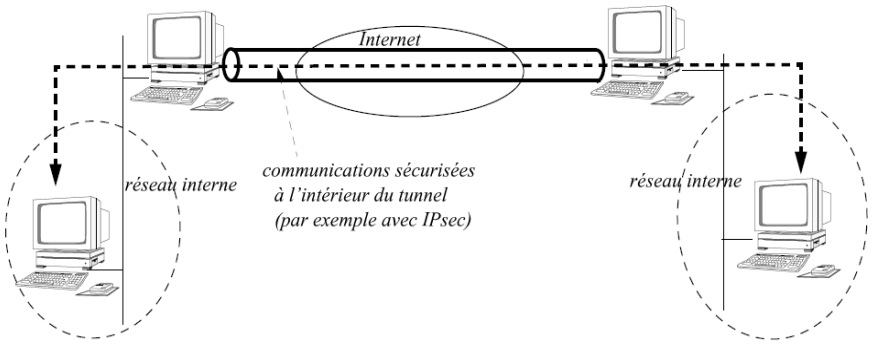
Pour pivoter



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

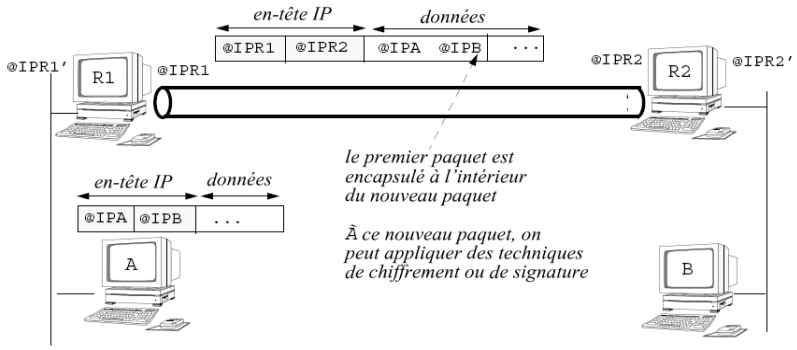
Rôle d'un VPN

- Rôle d'un VPN
  - permet à 2 réseaux d'entreprise 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) :



ENAC

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

ENAC

Pour pivoter

-. VPN

-. Redirection de port SSH

-.Firewalls

-.Proxychains

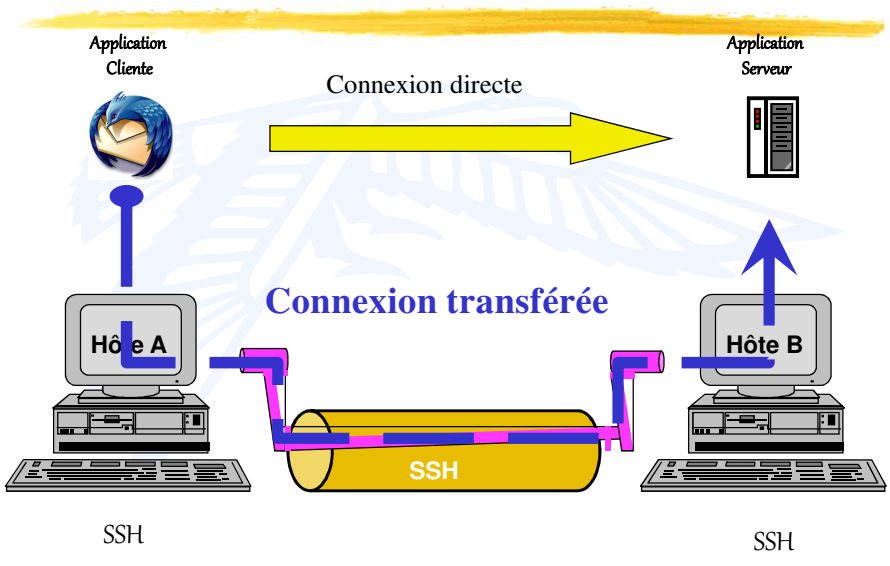
ENAC

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.

ENAC

Redirection de Port TCP



ENAC

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'envoie les données dans ce tunnel
  - Redirection distante

ENAC

Redirection de port TCP
Redirection Locale

- C'est la machine qui crée le tunnel qui initie l'envoie les 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

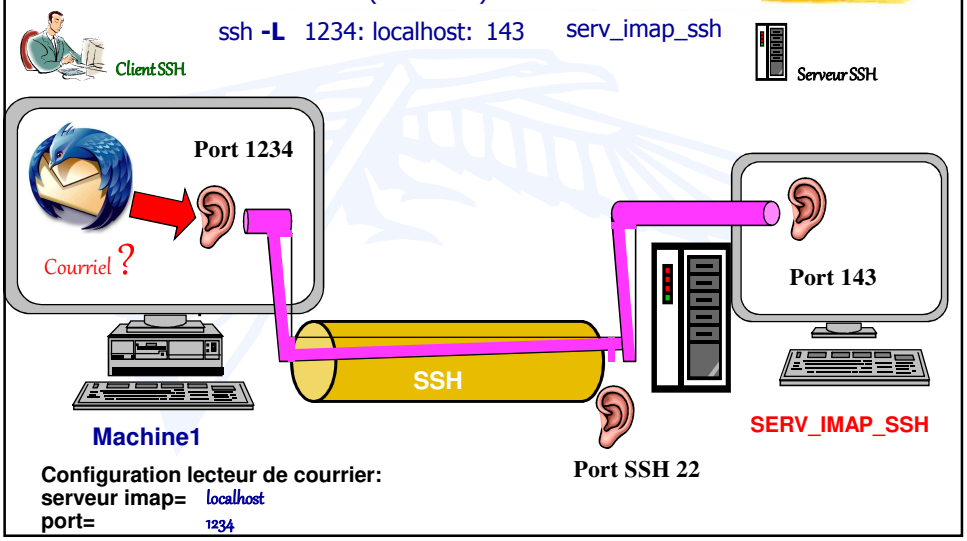
Redirection Locale
Exemple 1

- 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 :

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



Configuration lecteur de courrier:
serveur imap= localhost
port= 1234

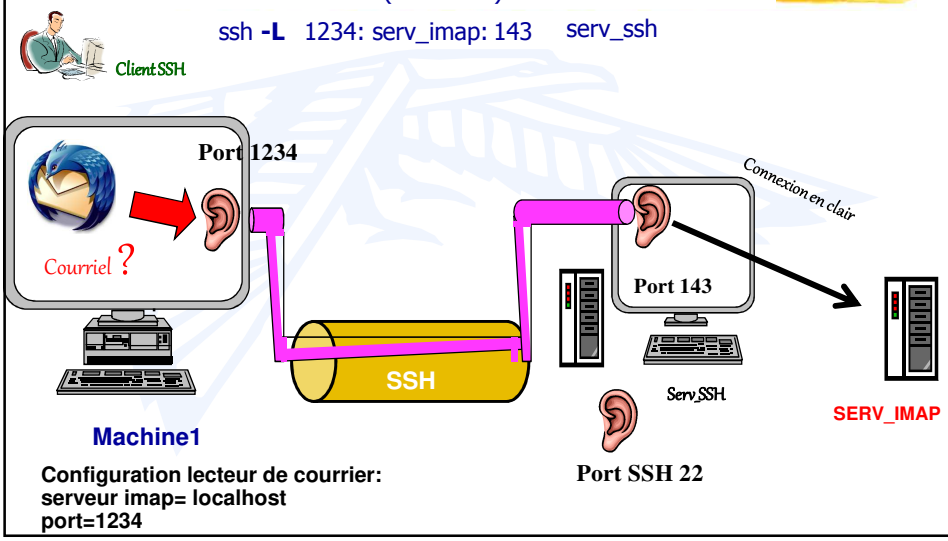
Redirection Locale
Exemple 2

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



Configuration lecteur de courrier:
serveur imap= localhost
port=1234

ENAC

TD Hacking Éthique:
chapitre 5 Étape2: premier pivot

ENAC

Pour pivoter

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

ENAC

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)**

ENAC

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)

ENAC

Caractéristiques d'un firewall (2/2)

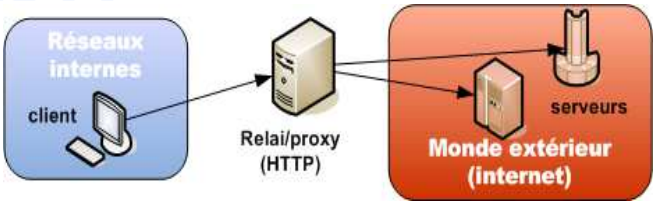
Différents modes de fonctionnement

2. Fonctions de **relais et de masque (ie. proxy)**
   - Application-level gateway (ALG)
   - Circuit-level gateway (CLG)

ENAC

Fonctions de relais et de masque en ALG (1)

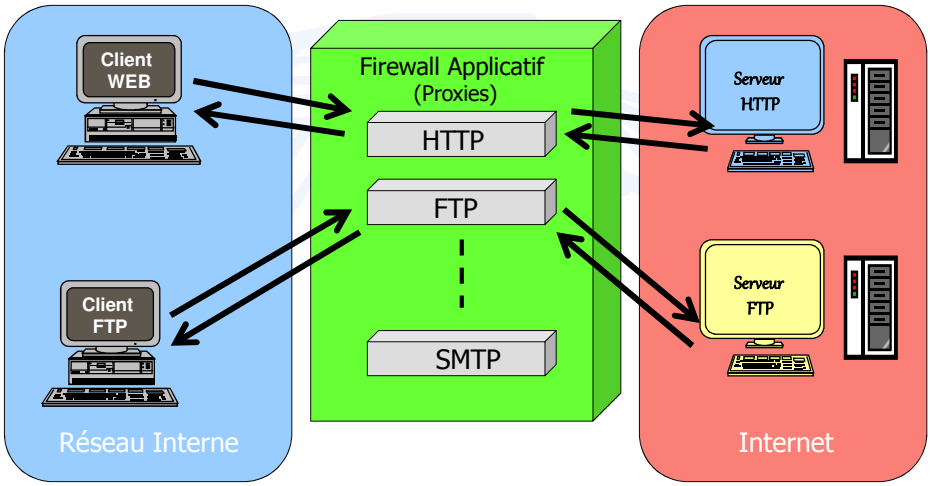
- Principe
  - Permet d'établir un relai entre le réseau interne et le réseau externe en se basant sur le contenu des messages au niveau applicatif,
  - Un utilisateur externe demande une connexion TCP/IP à la passerelle, qui authentifie et qui, en cas de succès, contacte l'application que l'utilisateur 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 utiliser le serveur http interne.



118

ENAC

Fonctions de relais et de masque en ALG (2)



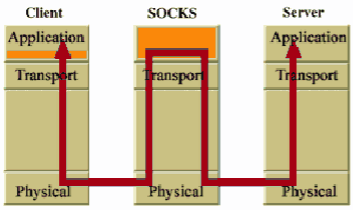
ENAC

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 server 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'authentication, 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 librarie 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
```

ENAC

Pour pivoter

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

ENAC

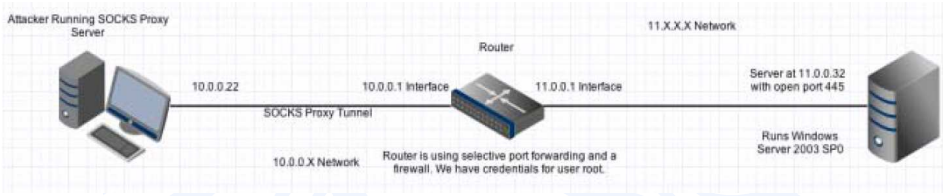
PROXYCHAINS : principes

- Proxychains est un outil qui permet de faire sortir le traffic d'une application à travers un tunnel SOCKS précédemment configuré et ouvert
- Etant donné que le tunnel SOCKS peut être ouvert vers n'importe qu'elle autre machine, Proxychains permet de faire éxecuter une application sur n'importe qu'elle machine distante (i.e. la sortie du tunnel SOCKS)

⇨ Contournement aisé de la politique de sécurité d'un Firewall

ENAC

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)

ENAC

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)

ENAC

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 -Nf  -D 127.0.0.1:7777 root@192.168.1.21
root@bt:~/proxychains1# netstat  an | 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 deuxieme serveur SOCKS)

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

ENAC

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'utilisaiton de deux redirections proxychain nécessite deux configurations différentes de proxychains c'est la raison pour laquelle le **nmap est executé dans le répertoire proxychains2**

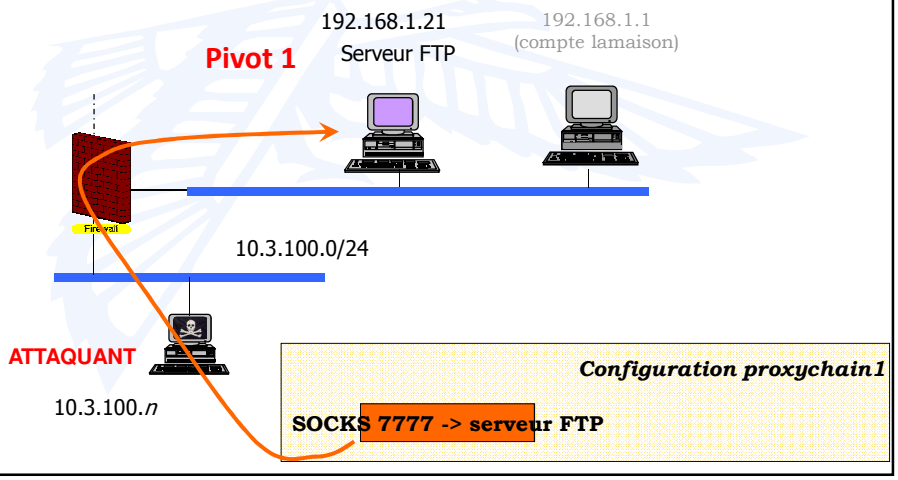
  Fichier /etc/proxychains.conf
  socks4 127.0.0.1 8888

  et les deux pivots précédents dans le répertoire proxychain1

  Fichier /etc/proxychains.conf
  socks4 127.0.0.1 7777

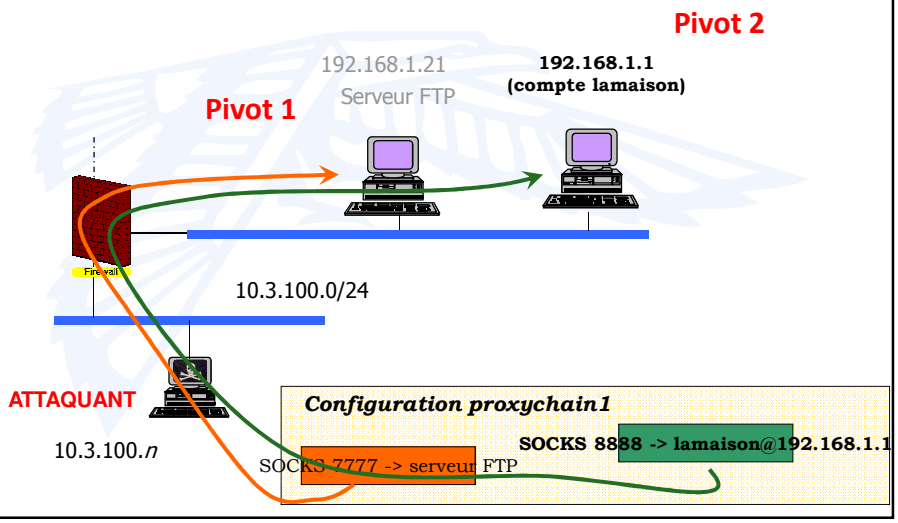
ENAC

PROXYCHAINS : résumé des tunnels SOCKS utilisés



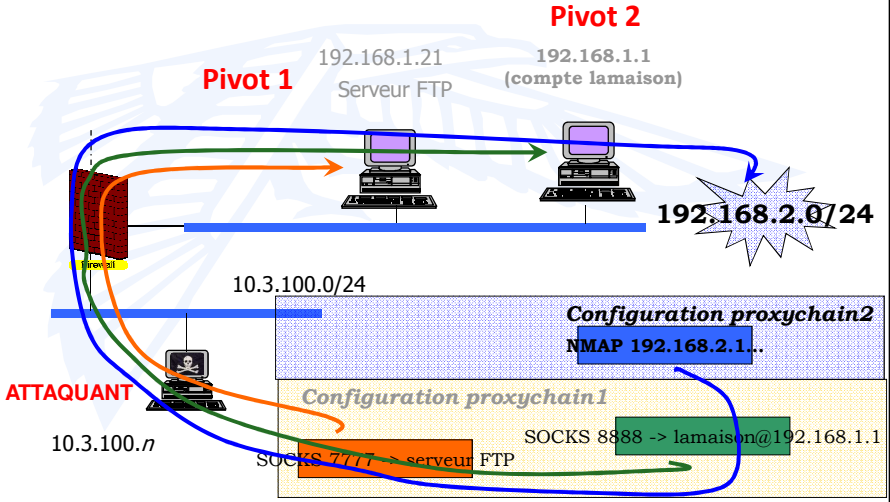
ENAC

PROXYCHAINS : résumé des tunnels SOCKS utilisés



ENAC

PROXYCHAINS : résumé des tunnels SOCKS utilisés



ENAC

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