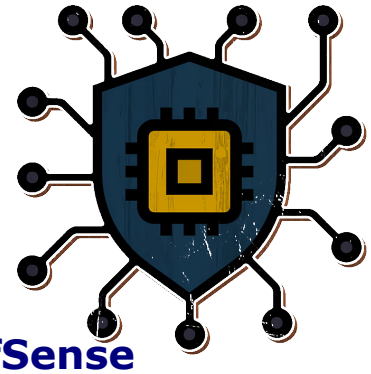


W10D4

Simulazione fase di raccolta

Info Gathering su Metasploitable 2 con pfSense

⋆ INDICE

1 Objective

Utilizzare i tool di scansione host per raccogliere informazioni sulla macchina Metasploitable2 192.168.51.101 da Kali Linux 192.168.50.100 in una rete interna con pfSense.

Produrre un report con screenshot delle esecuzioni e un report finale delle informazioni trovate.

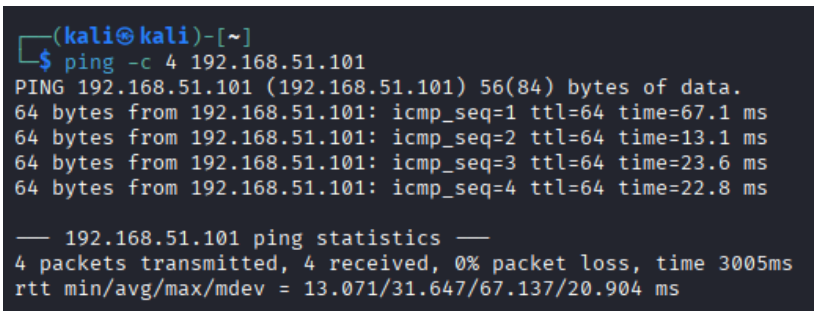
Approfondire i metodi di evasione firewall con Nmap.

1.1 Note sul contesto di rete

- Kali Linux 192.168.50.100 Attacker
- Metasploitable2 192.168.51.101 Target
- PfSense Firewall/Router tra le sottoreti 192.168.50.0/24 e 192.168.51.0/24
- Rete Interna

1.2 Verifica configurazione di rete

- Controllo che Kali e Metasploitable2 siano in esecuzione
- PfSene deve instradare il traffico tra 192.168.50.0/24 e 192.168.51.0/24
- Accedo all'interfaccia web di pfSense e verifico
  - Le regole firewall consentano ICMP, TCP/UDP da 192.168.50.100 a 192.168.51.101
  - NAT/Routing le due sottoreti devono comunicare
- Kali Veifico connettività ping -c 4 192.168.51.101



- Aggiorno Kali sudo apt update && sudo apt upgrade -y

```
┌──(kali㉿kali)-[~/esame-info-gathering]
└─$ sudo apt update && sudo apt upgrade -y
```

- Creo Directory di lavoro
  mkdir ~/esame-info-gathering && cd ~/esame-info-gathering

```
┌──(kali㉿kali)-[~]
└─$ mkdir ~/esame-info-gathering && cd ~/esame-info-gathering
```

- Installo Tool mancanti per quelli non presenti

  sudo apt install netdiscover unicornscan masscan crackmapexec -y

```
┌──(kali㉿kali)-[~/esame-info-gathering]
└─$ sudo apt install netdiscover unicornscan masscan crackmapexec -y
[sudo] password for kali:
```

- Verifico msfconsole ed exit

```
┌──(kali㉿kali)-[~/esame-info-gathering]
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
```

```
       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf6 >
```

2 Esecuzione dei Tool di scanning (14 Tool da YeahHub)

2.1 Nmap (Ping Scan per Host Attivi)

- Con nmap -sn -PE 192.168.51.101

```
┌──(kali㉿kali)-[~/esame-info-gathering]
└─$ nmap -sn -PE 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 04:50 EDT
Nmap scan report for 192.168.51.101
Host is up (0.12s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(kali㉿kali)-[~/esame-info-gathering]
└─$ nmap -sn -PE 192.168.51.101 > nmap_ping.txt
```

- Indica che l'host 192.168.51.101 Metasploitable2 è attivo con una latenza di 0.12 secondi, quidni indica che la connettività tra Kali 192.168.50.100 e Metasploitable2 funziona nonostante la presenza di pfSense.

2.2 Netdiscover (Scansione Passiva/Attiva)

- Con sudo netdiscover -r 192.168.51.0/24 mi darà gli host attivi nella rete tramite ARP, utile per mappaing rete

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 42
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.51.101  08:00:27:38:94:a5      1      42  PCS Systemtechnik GmbH
```

- Ho rilevato l'host 192.168.51.101 con indirizzo MAC 08:00:27:38:94:a5, tipico di una VM VirtualBox, questo conferma il mapping di rete

2.3 CrackMapExec (Test SMB)

- Con crackmapexec smb 192.168.51.101 proverò accesso SMB non AD ma utile per enumerazione servizi

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.51.101
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         192.168.51.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
```

- Ho conferma che la porta 445 (SMB) è aperta su Metasploitable2 con servizio Samba (Unix-Based) vulnerabile (SMBv1 abilitato noto per exploit come EternalBlue).
- Il nome METASPLOITABLE è coerente con la configurazione predefinita della VM.

2.4 Nmap (Top 10 Porte Aperte)

- Con nmap 192.168.51.101 --top-ports 10 --open effettuerò una scansione rapida per il mapping iniziale delle 10 porte più comuni

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.51.101 --top-ports 10 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 06:47 EDT
Nmap scan report for 192.168.51.101
Host is up (0.042s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

- Ho conferma della rilevazione di 7 delle 10 porte più comuni aperte, tra cui FTP (21)- SSH (22) - Telnet (23) - SMTP (25) HTTP (80) NetBIOS (139) - SMB (445), questo è coerente con Metasploitable2 che ha 21 porte aperte, molte delle quali vulnerabili

2.5 Nmap (Scansione Completa con Versioni)

- Con nmap 192.168.51.101 -p- -sV --reason --dns-servers 8.8.8.8
  Scansiono tutte le porte, uso DNS Google per risolvere nomi.
- Tempo più lungo di scansione

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.51.101 -p- -sV --reason --dns-servers 8.8.8.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 07:08 EDT
Stats: 0:11:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.47% done; ETC: 07:22 (0:02:09 remaining)
Stats: 0:22:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.63% done; ETC: 07:31 (0:00:47 remaining)
Nmap scan report for 192.168.51.101
Host is up, received echo-reply ttl 64 (0.014s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      REASON         VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?       syn-ack ttl 64
514/tcp   open  shell        syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi     syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell    syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp? syn-ack ttl 64
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack ttl 64 (access denied)
6667/tcp  open  irc          syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc          syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13        syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown      syn-ack ttl 64
8787/tcp  open  drb          syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
45423/tcp open  mountd       syn-ack ttl 64 1-3 (RPC #100005)
48679/tcp open  nlockmgr     syn-ack ttl 64 1-4 (RPC #100021)
55225/tcp open  status       syn-ack ttl 64 1 (RPC #100024)
60591/tcp open  java-rmi     syn-ack ttl 64 GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 1717.26 seconds
```

- Ho monitorato lo stato della scansione premendo invio, i dati dello stats

- Ho conferma dell'host 192.168.51.101 è attivo

- 30 porte TCP aperte più delle 21 attese per Metasploitable2, ma sono coerenti con la configurazione vulnerabile

- Elenco servizi e versioni
  - 21/TCP vsftpd 2.3.4 (vulnerabile, nota backdoor)
  - 22/tcp OpenSSH 4.7p1 (potenzialmente vulnerabile con credeziali deboli)
  - 80/TCP Apache 2.2.8 (vulnerabilità note, esempio directory traversal)
  - 139/445/tcp Samba 3.X-4.X (vulnerabilr, esempio exploit EternalBlue)
  - 1524/tcp Metasploitable2 root shell (bindshell, vulnerabilità critica)
  - Altri MySQL, PostgreSQL, VNC, IRC,...., molti con versioni obsolete

- PfSense
  - Nessun blocco presente nessun blocco evidente, tutte le porte rilevate, ICMP permesso
  - La scansione ha richiesto 28 minuti, normale per -p- -sV
- Service info conferma OS Linux (Unix, cpe:/o:linux:linux_kernel) e nomi host metasploitable.localdomain

⇒ Catturo lo screenschot con gnome-screenshot -f ~/esame-info-gathering/nmap_full.png

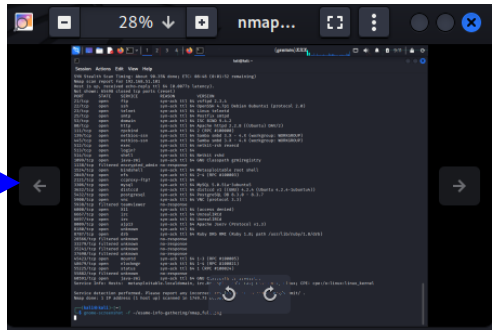
```
┌──(kali㉿kali)-[~]
└─$ gnome-screenshot -f ~/esame-info-gathering/nmap_full.png
** Message: 09:11:39.592: Unable to use GNOME Shell's builtin screenshot interface, resorting to fallback X11.
```

⇒ Verifico il file con file ~/esame-info-gathering/nmap_full.png

```
┌──(kali㉿kali)-[~]
└─$ file ~/esame-info-gathering/nmap_full.png
/home/kali/esame-info-gathering/nmap_full.png: PNG image data, 1160 x 915, 8-bit/color RGB, non-interlaced
```

⇒ Infine apro per controllare con eog ~/esame-info-gathering/nmap_full.png

```
┌──(kali㉿kali)-[~]
└─$ eog ~/esame-info-gathering/nmap_full.png
```



⇒ **Il file XML nmap_full.xml l'ho userò più avanti per Metasploit**

2.6 Unicornscan (TCP/UDP Veloce)

- Eseguo scansione TCP/UDP ad alta velocità
- Scansione TCP sudo us -mT -Iv 192.168.51.101:a -r 3000 -R 3 &&

```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT -Iv 192.168.51.101:a -r 3000 -R 3
adding 192.168.51.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.51.101:2121  ttl 64
TCP open 192.168.51.101:22  ttl 64
TCP open 192.168.51.101:445  ttl 64
TCP open 192.168.51.101:513  ttl 64
TCP open 192.168.51.101:3632  ttl 64
TCP open 192.168.51.101:55225  ttl 64
TCP open 192.168.51.101:111  ttl 64
TCP open 192.168.51.101:45423  ttl 64
TCP open 192.168.51.101:1524  ttl 64
TCP open 192.168.51.101:6667  ttl 64
TCP open 192.168.51.101:48679  ttl 64
TCP open 192.168.51.101:8180  ttl 64
TCP open 192.168.51.101:23  ttl 64
sender statistics 2825.1 pps with 196608 packets sent total
TCP open 192.168.51.101:6697  ttl 64
TCP open 192.168.51.101:1099  ttl 64
listener statistics 41160 packets recieved 0 packets droped and 0 interface drops
TCP open                     ssh[   22]         from 192.168.51.101  ttl 64
TCP open                  telnet[   23]         from 192.168.51.101  ttl 64
TCP open                  sunrpc[  111]         from 192.168.51.101  ttl 64
TCP open            microsoft-ds[  445]         from 192.168.51.101  ttl 64
TCP open                   login[  513]         from 192.168.51.101  ttl 64
TCP open             rmiregistry[ 1099]         from 192.168.51.101  ttl 64
TCP open               ingreslock[ 1524]         from 192.168.51.101  ttl 64
TCP open           scientia-ssdb[ 2121]         from 192.168.51.101  ttl 64
TCP open                  distcc[ 3632]         from 192.168.51.101  ttl 64
TCP open                     irc[ 6667]         from 192.168.51.101  ttl 64
TCP open                 unknown[ 6697]         from 192.168.51.101  ttl 64
TCP open                 unknown[ 8180]         from 192.168.51.101  ttl 64
TCP open                 unknown[45423]         from 192.168.51.101  ttl 64
TCP open                 unknown[48679]         from 192.168.51.101  ttl 64
TCP open                 unknown[55225]         from 192.168.51.101  ttl 64
```

- La scansione TCP ha rilevato numerose porte aperte, incluse
  - 22 (SSH), 23 (Telnet), 80(HTTP), 111 (rpcbind), 445 (SMB), 1099 (java-rmi), 1524 (ingreslock), 2121 (FTP), 3632 (distcc), 6667 (IRC), 8180 (unknown),....
  - E' risultata coerente con l'output precedente di nmap full scan (30bporte TCP aperte)
  - La scansione ha inviato 196.608 pacchetti a 2825 pps, completandosi in 72 secondi senza pacchetti persi.
  - PfSense: non ha rilevato nessun blocco TCP, questo significa che le regole firewall permettono il traffico

- Scansione UDP sudo us -mU -Iv 192.168.51.101:a -r 3000 -R 3

```
┌──(kali㉿kali)-[~]
└─$ sudo us -mU -Iv 192.168.51.101:a -r 3000 -R 3
adding 192.168.51.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
UDP open 192.168.51.101:137  ttl 64
UDP open 192.168.51.101:2049  ttl 64
UDP open 192.168.50.101:52288  ttl 64
UDP open 192.168.51.101:111  ttl 64
UDP open 192.168.51.101:53  ttl 64
UDP open 192.168.50.101:51391  ttl 64
sender statistics 2890.6 pps with 196635 packets sent total
listener statistics 16 packets recieved 0 packets droped and 0 interface drops
UDP open                 unknown[51391]         from 192.168.50.101  ttl 64
UDP open                 unknown[52288]         from 192.168.50.101  ttl 64
UDP open                  domain[   53]         from 192.168.51.101  ttl 64
UDP open                  sunrpc[  111]         from 192.168.51.101  ttl 64
UDP open              netbios-ns[  137]         from 192.168.51.101  ttl 64
UDP open                   shilp[ 2049]         from 192.168.51.101  ttl 64
```

- La scansione UDP ha rilevato porte aperte su 192.168.51.101
  - 53 (DN), 111 (sunrpc), 137 (netbios-ns), 2049 (NFS)
- Mi ha rilevato 2 errori nei risultati, due porte (51391, 52288) sono associate a 192.168.50.101 (Kali Linux), non al target Metasploitable2 (192.168.51.101).
  Ho dedotto che sicuramente è stato causato da un interferenza nell'ambiente virtuale oppure a pacchetti UDP riflessi da kali o pfSense (192.168.50.1)
- Le porte UDP rilevate (53,111,137,2049) sono coerenti con Metasplitable2 che ha pochi servizi UDP attivi
- La scansione ha inviato 196.635 pacchetti a 2890 pps, con solo 16 pacchetti ricevuti (questo è normale per UDP poichè molti pacchetti non ricevono risposta)
- PfSense anche qui nessun blocco UDP evidente, ma le porte su 192.168.50.101 mi suggeriscono un possibbile problema di rete, che ho verificato e non ho trovato criticità.
- Non ho ripetuto le scansioni perchè ho assodato che tutto è impostato in modo corretto senza riscontrare nessun problema d'instradamento di rete, confermado la mia analisi di interferenza nell'ambiente virtuale
- Proseguo con l'esame

2.7 Nmap (SYN Scan con Versioni)

- Scansione SYN stealth con con nmap -sS -sV -T4 192.168.51.101, -T4 per velocizzare

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -T4 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 10:13 EDT
Nmap scan report for 192.168.51.101
Host is up (0.020s 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?
514/tcp  open  shell       Netkit rshd
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  ccproxy-ftp?
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  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 174.73 seconds
```

- La scansione ha rilevato 22 porte TCP aperte su 192.168.51.101, leggermene meno delle 90 rilevate con nmap -p- -sV perhcè -sS -T4 sansionano solo le 1000 porte più comuni

- Vulnerabilità

- 21/tcp vsfpd 2.3.4 (conosciuto per backdoor)
- 139/445/tcp Samba 3.X-4.X (vulnerabile tipo EternalBlue)
- 1524/tcp Metasploitable2 root shell (bindshell, accesso critico)
- Altri come Apache 2.2.8 (HTTP), MySQL 5.0.51a, PostgreSQL 8.3.0-8.3-7,....

- pfSense anche qui nessun blocco TCP rilevato, confermatomi anche dai ping della scasnioni precedenti

- OS Linux 2.6.x confermato da Service info

- Durata scansione di 172 secondi circa 3 minuti grazie a -T4

2.8 Hping3 (Pacchetti Custom)

- Avvio Hping3 con pacchetti personalizzati TCP SYN con

sudo hping3 --scan known 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.51.101
Scanning 192.168.51.101 (192.168.51.101), port known
266 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (4 echo) (6 zip) (7 echo) (9 discard) (11 systat) (13 daytime) (15 netstat) (17 qotd) (19 chargen) (
20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (25 smtp) (37 time) (43 whois) (49 tacacs) (53 domain) (67 bootps) (68 bootpc) (69 tftp) (70 gophe
r) (79 finger) (80 http) (88 kerberos) (102 iso-tsap) (104 acr-nema) (106 poppassd) (110 pop3) (111 sunrpc) (113 auth) (119 nntp) (123 ntp) (
135 epmap) (137 netbios-ns) (138 netbios-dgm) (139 netbios-ssn) (143 imap2) (161 snmp) (162 snmp-trap) (163 cmip-man) (164 cmip-agent) (174 m
ailq) (177 xdmcp) (179 bgp) (199 smux) (209 qmtp) (210 z3950) (213 ipx) (319 ptp-event) (320 ptp-general) (345 pawserv) (346 zserv) (369 rpc2
portmap) (370 codaauth2) (371 clearcase) (389 ldap) (427 svrloc) (443 https) (444 snpp) (445 microsoft-d) (464 kpasswd) (465 submissions) (48
7 saft) (500 isakmp) (512 exec) (513 login) (514 shell) (515 printer) (517 talk) (518 ntalk) (520 route) (538 gdomap) (540 uucp) (543 klogin)
 (544 kshell) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (554 rtsp) (563 nntps) (587 submission) (607 nqs) (623 asf-rmcp) (628 qmqp
) (631 ipp) (636 ldaps) (646 ldp) (655 tinc) (706 silc) (749 kerberos-ad) (750 kerberos4) (751 kerberos-ma) (752 passwd-serv) (754 krb-prop)
(775 moira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (853 domain-s) (871 supfilesrv) (873 rsync) (989 ftps-data) (990 ftps) (992 tel
nets) (993 imaps) (995 pop3s) (1080 socks) (1093 proofd) (1094 rootd) (1099 rmiregistry) (1127 supfiledbg) (1178 skkserv) (1194 openvpn) (121
0 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw) (1352 lotusnote) (1433 ms-sql-s) (1434 ms-sql-m) (1524 ingreslock) (1645 datametrics) (1646
 sa-msg-port) (1649 kermit) (1677 groupwise) (1701 l2f) (1812 radius) (1813 radius-acct) (2000 cisco-sccp) (2049 nfs) (2086 gnunet) (2101 rtc
m-sc104) (2102 zephyr-srv) (2103 zephyr-clt) (2104 zephyr-hm) (2119 gsigatekeep) (2121 iprop) (2135 gris) (2401 cvspserver) (2430 venus) (243
1 venus-se) (2432 codasrv) (2433 codasrv-se) (2583 mon) (2600 zebrasrv) (2601 zebra) (2602 ripd) (2603 ripngd) (2604 ospfd) (2605 bgpd) (2606
 ospf6d) (2607 ospfapi) (2608 isisd) (2628 dict) (2792 f5-globalsi) (2811 gsiftp) (2947 gpsd) (3050 gds-db) (3130 icpv2) (3205 isns) (3260 is
csi-targe) (3306 mysql) (3389 ms-wbt-serv) (3493 nut) (3632 distcc) (3689 daap) (3690 svn) (4031 suucp) (4094 sysrqd) (4190 sieve) (4353 f5-i
query) (4369 epmd) (4373 remctl) (4460 ntske) (4500 ipsec-nat-t) (4557 fax) (4559 hylafax) (4569 iax) (4691 mtn) (4899 radmin-port) (4949 mun
in) (5060 sip) (5061 sip-tls) (5222 xmpp-client) (5269 xmpp-server) (5308 cfengine) (5353 mdns) (5432 postgresql) (5555 rplay) (5556 freeciv)
 (5666 nrpe) (5667 nsca) (5671 amqps) (5672 amqp) (5680 canna) (5683 coap) (5684 coaps) (6000 x11) (6001 x11-1) (6002 x11-2) (6003 x11-3) (60
04 x11-4) (6005 x11-5) (6006 x11-6) (6007 x11-7) (6346 gnutella-sv) (6347 gnutella-rt) (6379 redis) (6444 sge-qmaster) (6445 sge-execd) (6446
 mysql-proxy) (6514 syslog-tls) (6566 sane-port) (6667 ircd) (6696 babel) (6697 ircs-u) (7000 bbs) (7001 afs3-callba) (7002 afs3-prserv) (700
3 afs3-vlserv) (7004 afs3-kaserv) (7005 afs3-volser) (7007 afs3-bos) (7008 afs3-update) (7009 afs3-rmtsys) (7100 font-servic) (8021 zope-ftp)
 (8080 http-alt) (8081 tproxy) (8088 omniorb) (8140 puppet) (8990 clc-build-d) (9098 xinetd) (9101 bacula-dir) (9102 bacula-fd) (9103 bacula-
sd) (9418 git) (9667 xmms2) (9673 zope) (10000 webmin) (10050 zabbix-agen) (10051 zabbix-trap) (10080 amanda) (10081 kamanda) (10082 amandaid
x) (10083 amidxtape) (10809 nbd) (11112 dicom) (11371 hkp) (17001 sgi-cmsd) (17002 sgi-crsd) (17003 sgi-gcd) (17004 sgi-cad) (17500 db-lsp) (
22125 dcap) (22128 gsidcap) (22273 wnn6) (24554 binkp) (27374 asp) (30865 csync2) (57000 dircproxy) (60177 tfido) (60179 fido)
```

- Ma non ha rilevato porte aperte

- Ho rieffettuato la scansione con porte specifiche (21,22,80,445) con

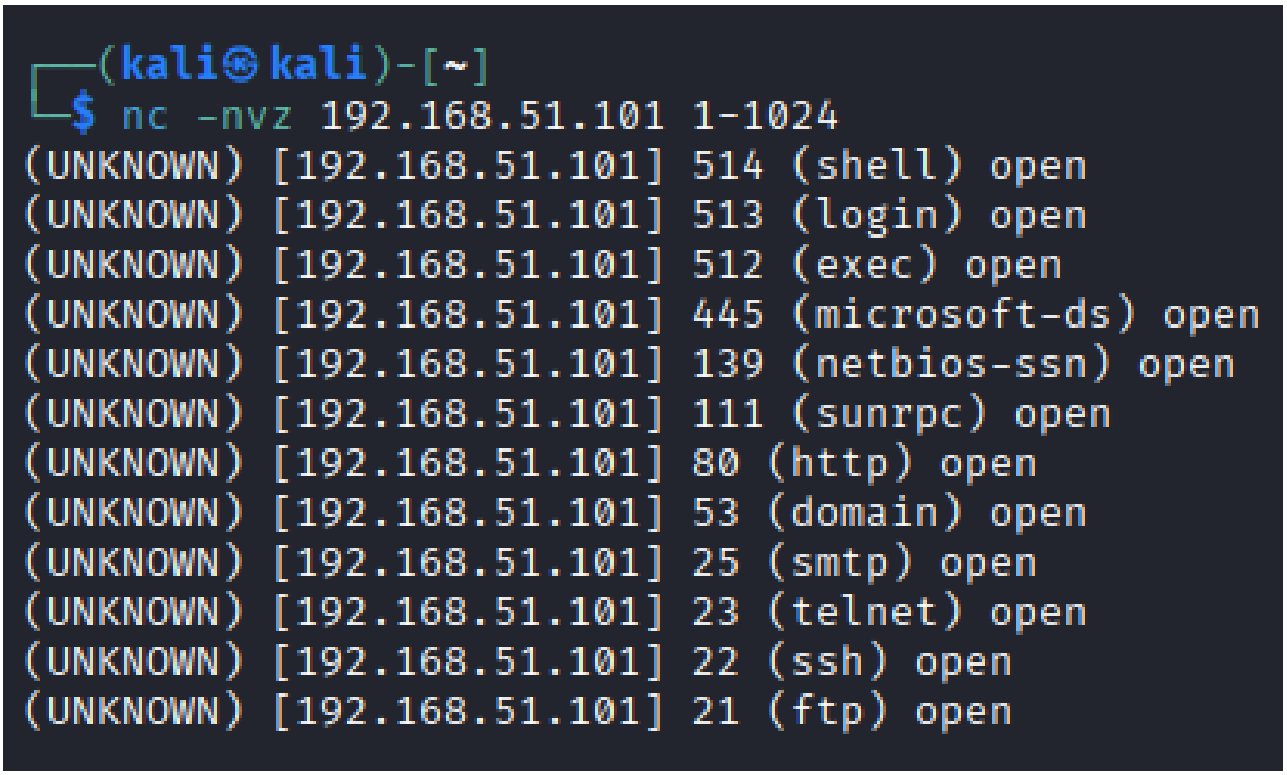
sudo hping3 --scan 21,22,80,445 -S --syn -c 10 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan 21,22,80,445 -S --syn -c 10 192.168.51.101
Scanning 192.168.51.101 (192.168.51.101), port 21,22,80,445
4 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  44
   22 ssh       : .S..A... 64    0     5840  44
   80 http      : .S..A... 64    0     5840  44
  445 microsoft-d: .S..A... 64    0     5840  44
All replies received. Done.
Not responding ports:
```

- Adesso ha rilevato correttamente le porte aperte
  - **21(FTP), 22(SSH), 80(HTTP), 445(SMB)**
  - L'outpout e coerente con nmap 5-7 e Unicornscan 6
  - PfSense nessun blocco TCP rilevato

2.9 Netcat (Scan Porte Base)

- Avvio scasione con nc -nvz 192.168.51.101 1-1024



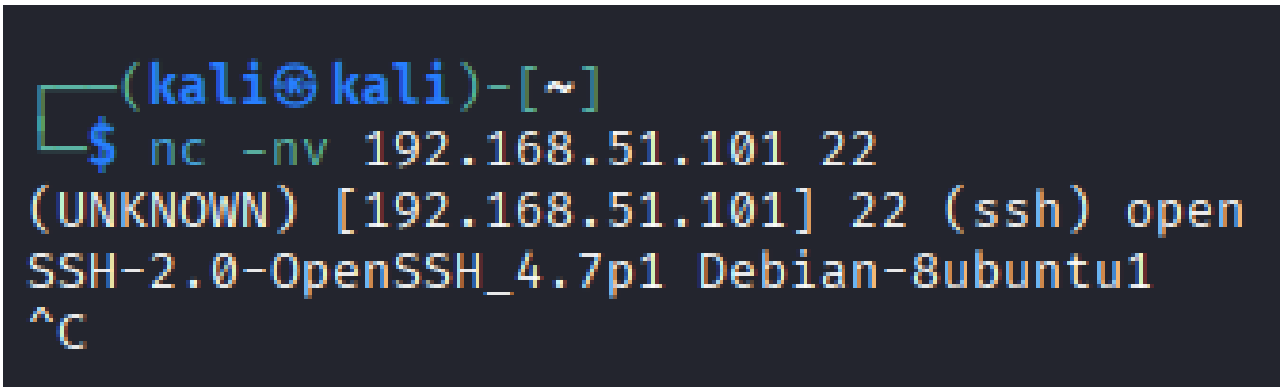
- La scansione ha rilevato **12 portte TCP aperte** nel rage 1-1024:21 (FTP), 22(SSH), 23(Telnet), 25(SMPT), 53(DNS), 80(HTTP), 111(rpc-bid), 139/445(SMB), 512(EXEC),513(login), 514(shell)

- In linea con nmap 5-7 e Unicornscan 6

- PfSense nessun blocco TCP

2.10 Netcat (Banner Grabbing)

- Avvio scansione nc -nv 192.168.51.101 22



- E' stato eseguito un banner grabbing sulla porta 22 (SSH) rilevando **OpenSSH 4.7p1 Debian-8ubuntu1**

- In linea con nmap 5 - 7

- PfSense porta 22 non bloccata

2.11 Nmap (Versioni Servizi)

- Avvio scansione con nmap -sV 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 10:38 EDT
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 10:40 (0:00:11 remaining)
Nmap scan report for 192.168.51.101
Host is up (0.068s 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?
514/tcp  open  shell        Netkit rshd
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  ccproxy-ftp?
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  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 175.44 seconds
```

- Ha rilebato **22 porte TCP aperte** nel range 1-1000, con versioni dei servizi come vsfpd 2.3.4 (FTP), OpenSSH 4.7p1 (SSH), Apache 2.2.8 (HTTP), Samba 3.X-4.X (SMB), Metaslploitable2 root shell (1524)

- In linea con il comando 7

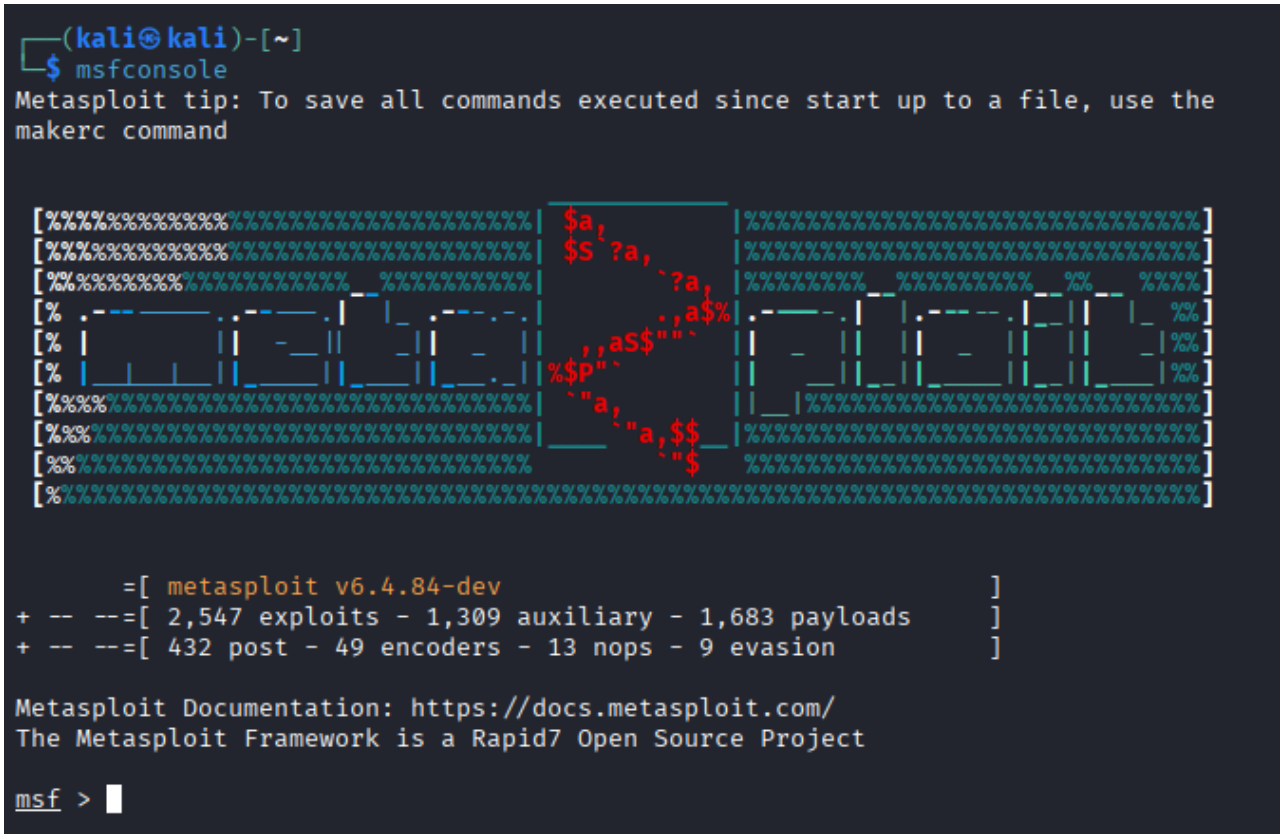
- PfSense nesun blocco TCP rilevato

- **Servizi Vulnerabili**

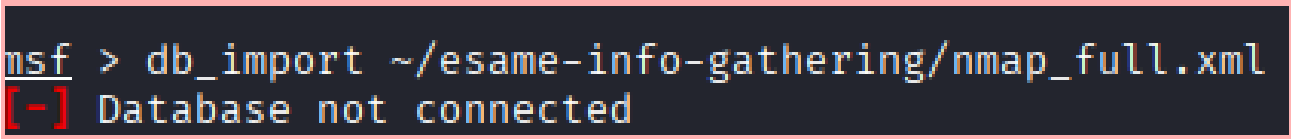
  - vsfpd (backdoor)
  - Samba (EternalBlue)
  - Bindshell (1524)

2.12 Metasploit (Import XML)

- Avvio con msfconsole



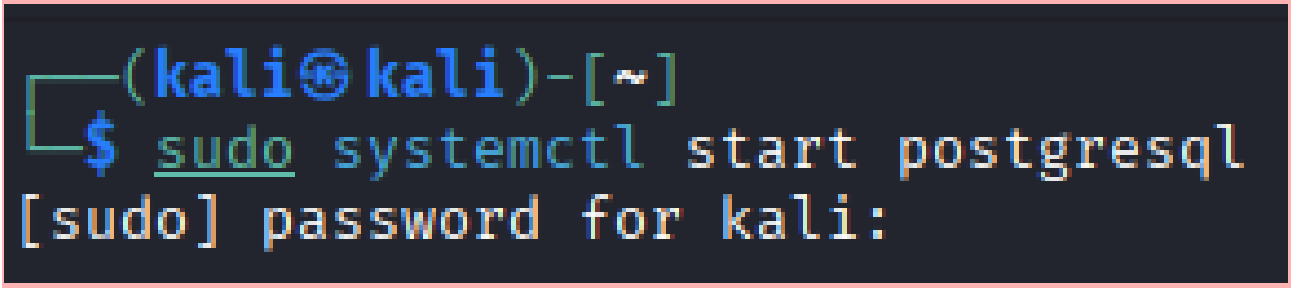
- Proseguo con l'importazione del file db_import ~/esame-info-gathering/nmap_full.xml



- Questo mi indica che il databese di Metasploit non è attivo o configurato correttamente.

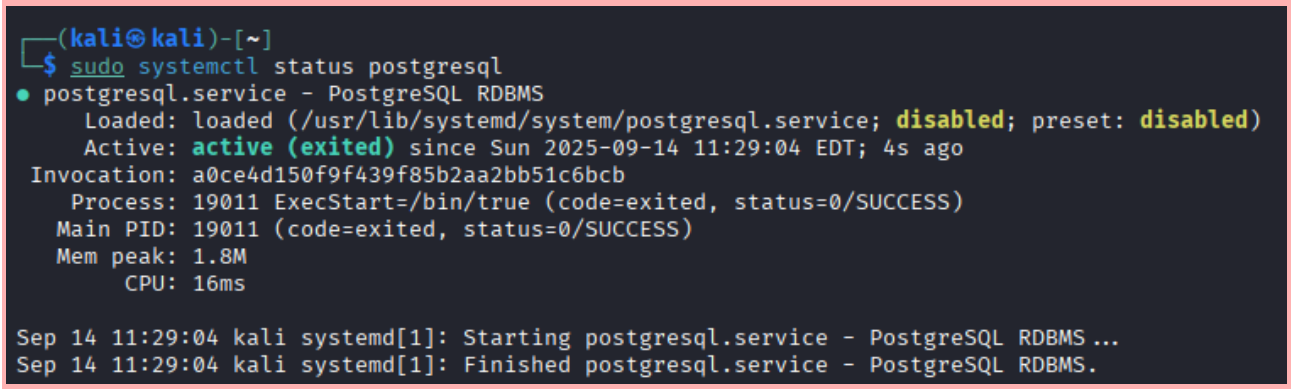
- Poichè Metasploit richiede un database attivo (**PostgreSQL**) per importare file XML e utilizzare i comandi come db_import o hosts, proseguo in questo modo

❍ Avvio il servizio con sudo systemctl start postgresql



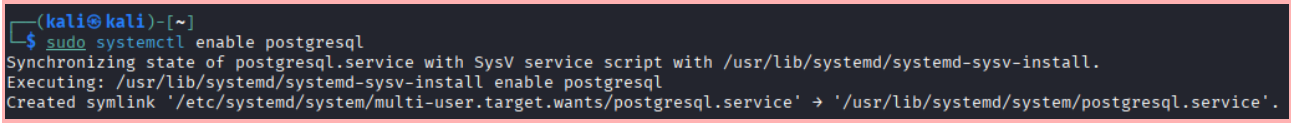
❍ Apro un terminle su Kali e verifico se è in esecuzione con

sudo systemctl status postgresql

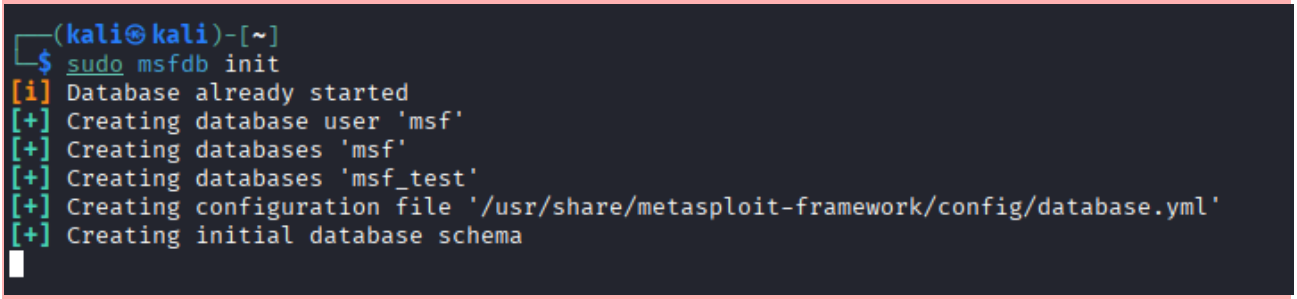


❍ Abilito il servizio all'avvio per evitare problemi futuri con

sudo systemctl enable postgresql



❍ Inizializzo il database di Metasploit configurandolo con sudo msfdb init



- Verifico il database con db_status

```
msf > db_status
[*] Connected to msf. Connection type: postgresql.
msf >
```

- Adesso dopo aver confermato l'attivazione del database proseguo importando il file

db_import ~/esame-info-gathering/nmap_full.xml

```
msf > db_import ~/esame-info-gathering/nmap_full.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.14.5'
[*] Importing host 192.168.51.101
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+
' and '?' was replaced with '*' in regular expression
[*] Successfully imported /home/kali/esame-info-gathering/nmap_full.xml
msf >
```

- Verifico i risultati con hosts

```
[*] Successfully imported /home/kali/esame-info-gathering/nmap_full.xml
msf > hosts

Hosts
=====

address         mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------  ---------  -----  -------  ----  --------
192.168.51.101             Linux                     server

msf >
```

- Elenco i servizi con services

```
msf > services
Services
========

host            port   proto  name            state     info
----            ----   -----  ----            -----     ----
192.168.51.101  21     tcp    ftp             open      vsftpd 2.3.4
192.168.51.101  22     tcp    ssh             open      OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.51.101  23     tcp    telnet          open      Linux telnetd
192.168.51.101  25     tcp    smtp            open      Postfix smtpd
192.168.51.101  53     tcp    domain          open      ISC BIND 9.4.2
192.168.51.101  80     tcp    http            open      Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.51.101  111    tcp    rpcbind         open      2 RPC #100000
192.168.51.101  139    tcp    netbios-ssn     open      Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.51.101  445    tcp    netbios-ssn     open      Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.51.101  512    tcp    exec            open      netkit-rsh rexecd
192.168.51.101  513    tcp    login           open
192.168.51.101  514    tcp    shell           open      Netkit rshd
192.168.51.101  1099   tcp    java-rmi        open      GNU Classpath grmiregistry
192.168.51.101  1138   tcp    encrypted_admin filtered
192.168.51.101  1524   tcp    bindshell       open      Metasploitable root shell
192.168.51.101  2049   tcp    nfs             open      2-4 RPC #100003
192.168.51.101  2121   tcp    ccproxy-ftp     open
192.168.51.101  3306   tcp    mysql           open      MySQL 5.0.51a-3ubuntu5
192.168.51.101  3632   tcp    distccd         open      distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
192.168.51.101  5432   tcp    postgresql      open      PostgreSQL DB 8.3.0 - 8.3.7
192.168.51.101  5900   tcp    vnc             open      VNC protocol 3.3
192.168.51.101  5938   tcp    teamviewer      filtered
192.168.51.101  6000   tcp    x11             open      access denied
192.168.51.101  6667   tcp    irc             open      UnrealIRCd
192.168.51.101  6697   tcp    irc             open      UnrealIRCd
192.168.51.101  8009   tcp    ajp13           open      Apache Jserv Protocol v1.3
192.168.51.101  8180   tcp                    open
192.168.51.101  8787   tcp    drb             open      Ruby DRb RMI Ruby 1.8; path /usr/lib/ruby/1.8/drb
192.168.51.101  28566  tcp                    filtered
192.168.51.101  33279  tcp                    filtered
192.168.51.101  35241  tcp                    filtered
192.168.51.101  37690  tcp                    filtered
192.168.51.101  45423  tcp    mountd          open      1-3 RPC #100005
192.168.51.101  48679  tcp    nlockmgr        open      1-4 RPC #100021
192.168.51.101  55225  tcp    status          open      1 RPC #100024
192.168.51.101  55882  tcp                    filtered
192.168.51.101  60591  tcp    java-rmi        open      GNU Classpath grmiregistry
```

- Infine esco con exit

```
msf > exit

┌──(kali㉿kali)-[~]
└─$
```

- L'output di hosts e services conferma che Metasploit ha correttamente importato i dati relativi all'host 192.168.51.101, mostrando un elenco dettagliato di porte aperte e servizi
- In linea con le scansioni precedneti 5 - 7
- Il database PostgreSQL è stato configurato correttamente risolvendo il problema.
- Proseguo con l'esame spiegando l'output di Metasploit

- Il File nmap_full.xml è stato importato con successo in Metasploit e l'output di hosts mi conferma che l'host 192.168.51.101 è stato aggiunto come server Linux (2.6.X)

- L'output di services elenca 30 porte TCP aperte, con servizi e versioni coerenti con le scansioni precedenti 5 - 7

  - 21/tcp vsfpd 2.3.4 (FTP, vulnerabile a backdoor)
  - 22/tcp OpenSSH 4.7p1 (SSH)
  - 80/TCP Apache 2.2.8 (HTTP)
  - 139/445/tcp Samba 3.X-4.X (vulnerabile a EternalBlue)
  - 1524/tcp Metasploitable2 root shell (bindshell, accesso critico)

- PfSense nessun blocco TCP rilevato

2.13 Nmap (Frammentazione per Firewall)

- Avvio la frammentizzazione dei pacchetti (-f –mtu=512) per eludere potenziali filtri firewall

```
┌──(kali㉿kali)-[~]
└─$ nmap -f --mtu=512 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 12:41 EDT
Nmap scan report for 192.168.51.101
Host is up (0.10s 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

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

- La scansione ha rilevato **23 porte TCP aperte** su 192.168.51.101
- Scansionando le 1000 porte più comuni (defoult di nmap senza -p-)
- Analizzando la scansione mi trovo in linea con le precedenti 7 - 5 che hanno identificato circa 22– - 30 porte aperte
- **Porte chiave**
  - 24/tcp FTP (vsfpd 2.3.4 vulnerabile a backdoor)

- 22/tcp SSH (OpenSSH 4.7p1)
- 80/tcp HTTP (Apache 2.2.8)
- 139/445/tcp SMB (Samba 3.X-4.X vulnerabile a EternalBlue)

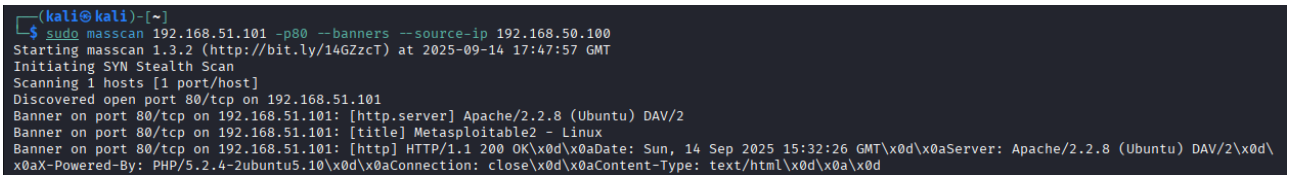
- La frammentazione (-f –mtu=512) no sembra aver influenzato i risultati in questo caso perchè pfSense non sta bloccando il traffico TCP

- La scansione è stata molto veloce 0.67 secondi, questo è stato possibile grazie al range limitato di porte e a –mtu=512

2.14 Masscan (Scan Veloce HTTP)

- Avvio Masscan per effettuare una scansione ultra-veloce della porta 80 con banner grabbing con

sudo masscan 192.168.51.101 -p80 --banners --source-ip 192.168.50.100



- Ho avuto conferma che la porta 80/tcp è aperta su 192.168.51.101, questo mi identifica il servizio come **Apache/2.2.8 (Ubuntu) DV/2** con PHP 5.2.4 -ubuntu 5.10

- L'output include informazioni aggiuntive come il titolo della pagina web (Metasploitable2 - Linux) in linea con la configurazione di Metasploitable2

- La scasnione è stata ultra-veloce, questo è tipico di Masscan che è progettato per scansioni da alta velocità

- PfSense anche qui non mi ha segnalato nessun blocco sulla porta 80/tcp, questo è in linea con le scansioni precedenti 7 - 11 - 13

3 In depth Firewall Evasion Analysis with nmap

⇒ Per questo esame Facoltativo procederò in questo modo:

- Configurero un blocco in pfSense per bloccare il traffico TCP verso la porta 80 (HTTP) o ICMP (Echo Request) da [Kali 192.168.50.100] a [Metassploitable2 1192.168.51.101] per simulare un firewall

- Ho valutato di iniziare con un blocco TCP sulla porta 80 perchè è un servizio chiave che mi è stato confermato aperto (Apache 2.2.8)

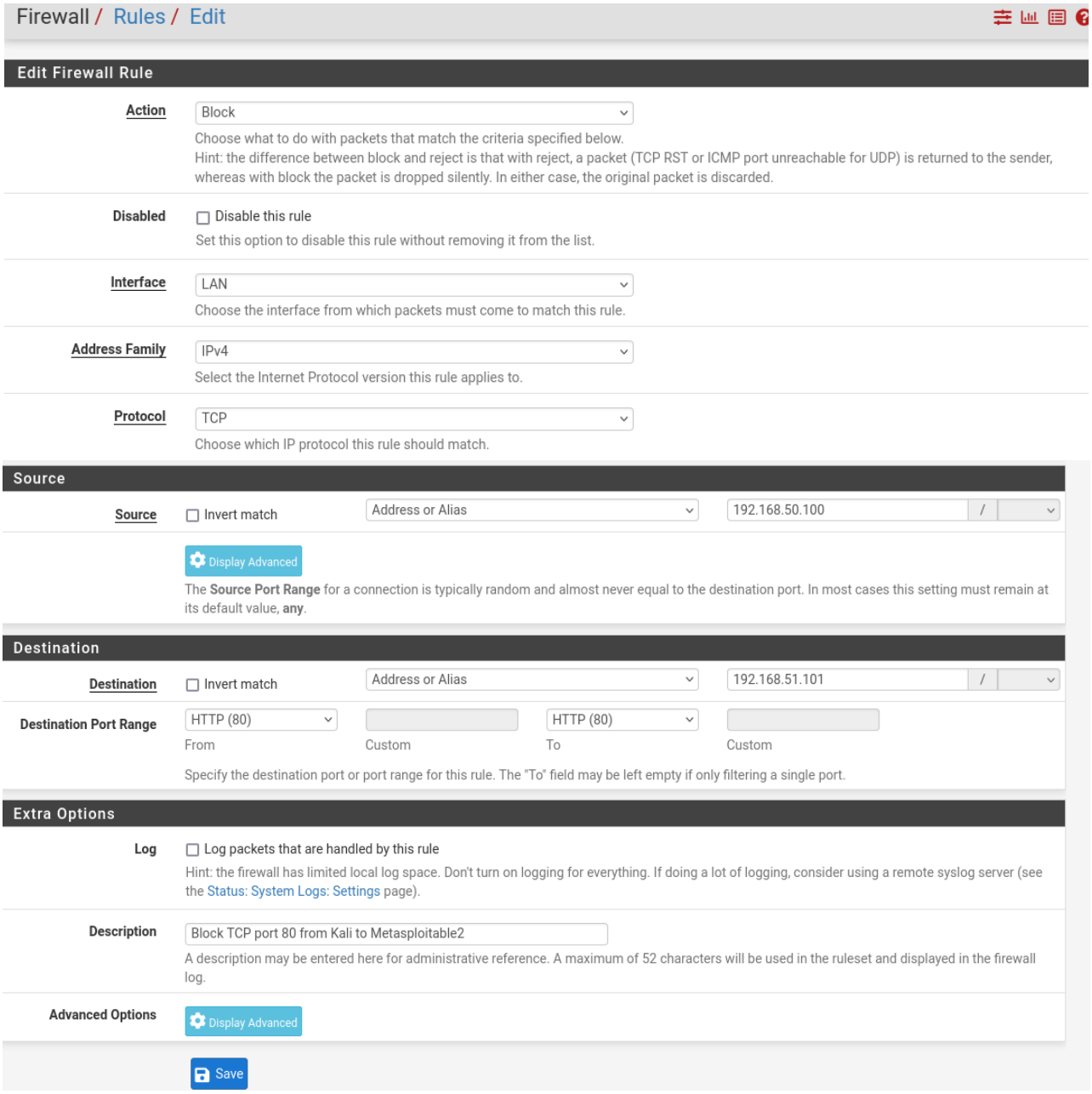
- Testerò i metodi di evasione di firewall con Nmap eseguendo ciscuno dei metodi indicati

  - FIN Scann
  - Source Port Manipulation
  - IPv6 Attacks
  - IP ID Idle Scannig
  - Idle Scan
  - Fragmentation
  - MAC Adress Spoofing
  - Source Routing
  - FTP Bounce Scan

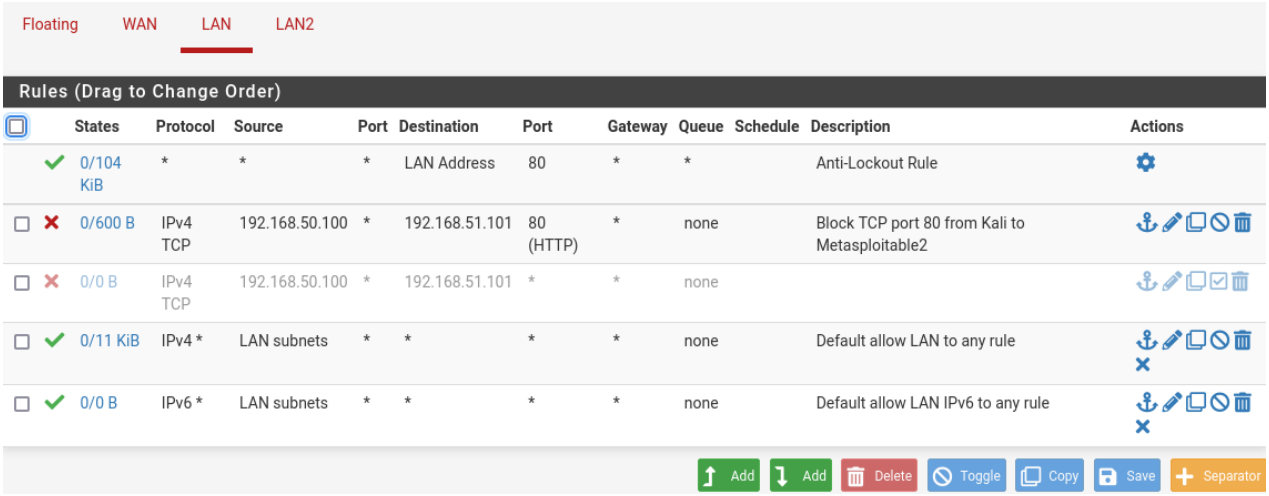
3.1 Setting up a Block in pfSense

- Apro pfSense con htt://192.168.50.1 loggandomi con le mie credenziali

- Aggiungo regola di blocco seguendo il percorso e configurando la regola con parametri che ho allegato nello screenshot di seguito

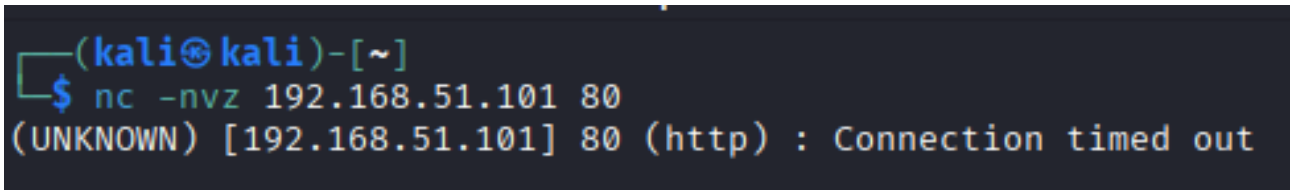


- Dopo aver salvato sposto in cima la regola per far si che pfSense la metta in atto e risalvo confermando

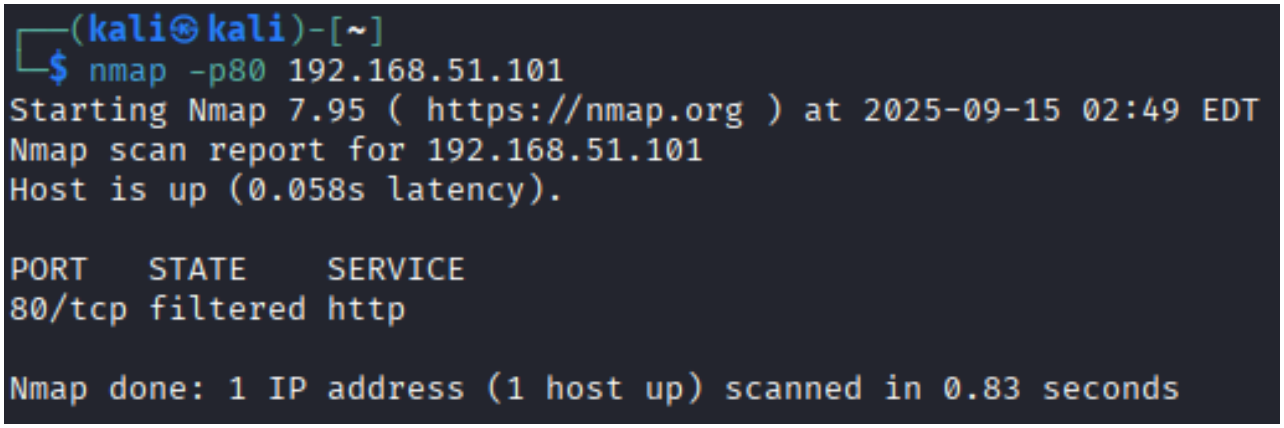


- Adesso verifico il blocco della porta 80 con 2 scansioni

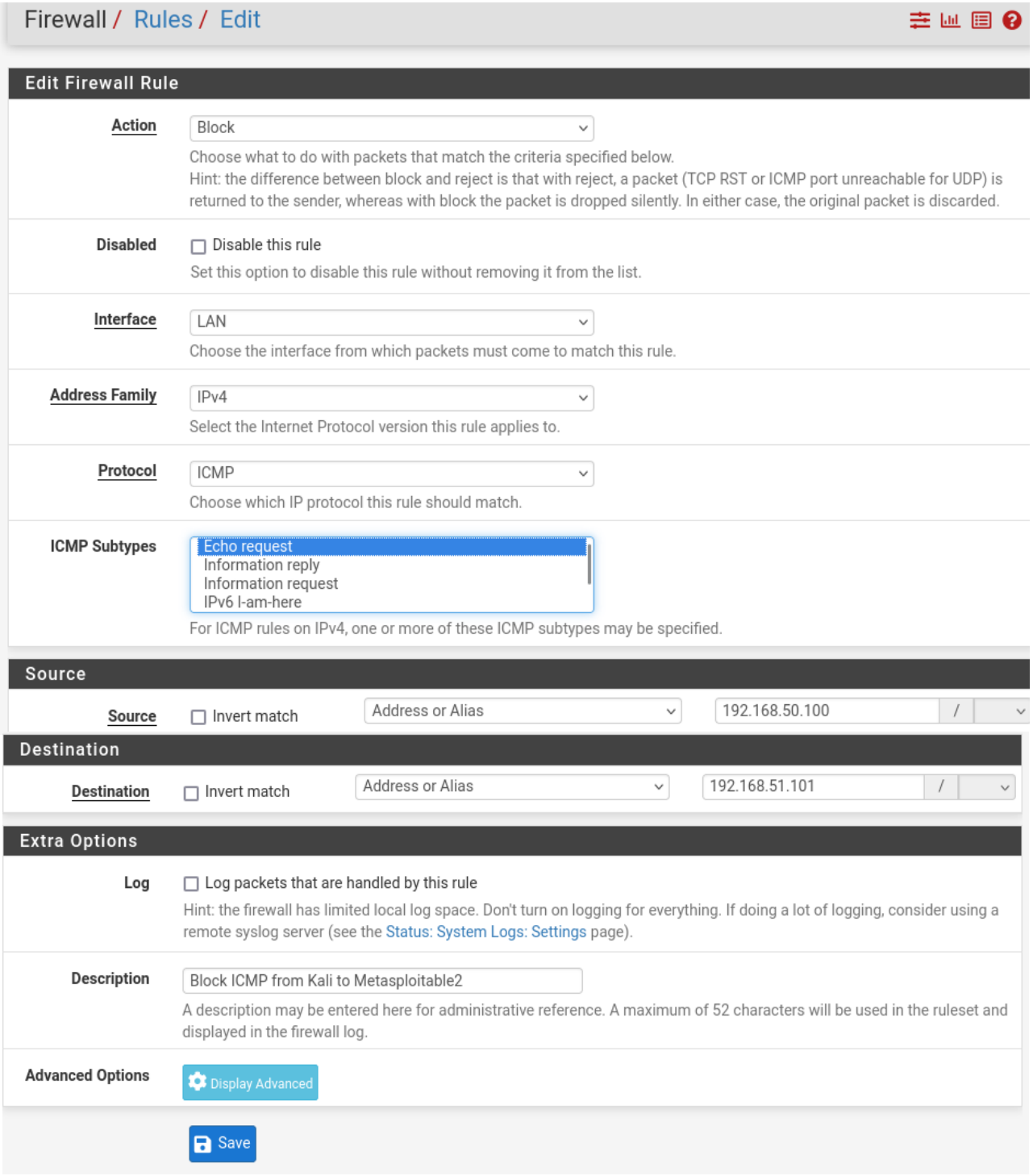
nc -nvz 192.168.51.101 80



nmap -p80 192.168.51.101



- Testo anche il blocco ICMP (Echo Request) per verificare l'evasione di ping, configurando la regola con parametri che allegato nello screeshot di seguito



- Stessa cosa anche qua, sposto in alto la regola per far si che funzioni e proseguo con il test da teminal con nmap -sn -PE 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 03:02 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.06 seconds
```

3.2 Evasione Methods

- Ora con entrambe le rogole di blocco attive (**ICMP Echo Request** e **TCP porta 80**) procedo ai test di evasione per bypassare i filtri

3.2.1 Exotic Scan Flags

- Consiste nell'uso di pacchetti FIN invece di SYN per baypassare filtri che bloccano pacchetti SYN, testo con

nmap -sF 192.168.51.101 -p80

```
┌──(kali㉿kali)-[~]
└─$ nmap -sF 192.168.51.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 03:45 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0093s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

- Esito la porta 80 è risultata open|filtered indicandomi che il filtro TCP di pfSense è efficace e la scansione FIN non ha completamente baypassato il blocco.

3.2.2 Source Port Manipulation

- Questo test usa una porta sorgente trusted (tipo 53 DNS) per baypassare filtri che permettono traffico da porte specifiche

nmap -sS --source-port 53 192.168.51.101 -p80

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS --source-port 53 192.168.51.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 03:46 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0017s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

- La porta 80 è riportata come filtered indicandomi che il blocco TCP configurato in pfSense ha impedito il rilevamento della porta come aperta quindi è risultato efficace

- L'uso della porta 53 (DNS) non ha baypassato il filtro TCP suggerendomi che pfSense non ha regole che permettono traffico da porte trusted come 53

- L'host rilevato come up nonostante il blocco ICMP, questo perchè nmap molto bobabilmente ha usato meccanismi alternativi per il rilevamento tipo pacchetti TCP

3.2.3 IPv6 Attacks Certifica IPv6

- Ho riscontrato un problema SSH per connettermi a Metasploitable2 192.168.51.101 per verificare la configurazione di rete con ifconfig.
- Procedo in questo modo per risolvere
- Quando inserivo il comando ssh msfadmin@192.168.51.101 ifconfig su terminale Kali

Ssh msfadmin@192.168.51.101 ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ssh msfadmin@192.168.51.101 ifconfig
Unable to negotiate with 192.168.51.101 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

- Riscontravo questo errore perchè Metasplitable2 utilizza **OpenSSH 4.7p1** che supporta algoritmi legacy ssh-rsa e ssh-dss
- OpenSSH su Kali rifiuta di default gli algoritmi (ssh-rsa usa SHA-1 insicuro) e (ssh-dss, obsoleto)
- Per risolvere il problema di abilitazione degli algoritmi legacy ho corretto la sintassi perchè mi dava diversi errori in questo modo
  - Nel file cat ~/.ssh/temp_config, ho rimosso il prefisso + e specificato solo ssh-rsa per HostKeyAlgorithms e PubkeyAcceptedAlgorithms, evitando ssh-dss (questo è più restrittivo e meno necessario)

```
┌──(kali㉿kali)-[~]
└─$ cat ~/.ssh/temp_config
Host 192.168.51.101
  HostKeyAlgorithms ssh-rsa
  PubkeyAcceptedAlgorithms ssh-rsa
```

- Comandi corretti

echo -e "Host 192.168.51.101\n HostKeyAlgorithms ssh-rsa\n PubkeyAcceptedAlgorithms ssh-rsa" > ~/.ssh/temp_config

e

ssh -F ~/.ssh/temp_config msfadmin@192.168.51.101 ifconfig

```
┌──(kali㉿kali)-[~]
└─$ echo -e "Host 192.168.51.101\n  HostKeyAlgorithms ssh-rsa\n  PubkeyAcceptedAlgorithms ssh-rsa" > ~/.ssh/temp_config

┌──(kali㉿kali)-[~]
└─$ ssh -F ~/.ssh/temp_config msfadmin@192.168.51.101 ifconfig
The authenticity of host '192.168.51.101 (192.168.51.101)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

- Accettazione della chiave host proseguendo digitando yes in modo da aggiungere la chiave RSA di Metaasplitable2, procedura allegata di sopra
- Ho ricevuto un conflitto al primo tentativo (Connection closed by 192.168.51.101 port 22) questo probabilmente è fallito a causa di un conflitto nella chiave host o di un problema temporaneo.

- Il tentativo 2 successivo è riuscito, sicuramente perché la chiave è stata aggiornata correttamente in ~/.ssh/known_hosts.

```
┌──(kali㉿kali)-[~]
└─$ ssh -F ~/.ssh/temp_config msfadmin@192.168.51.101 ifconfig
The authenticity of host '192.168.51.101 (192.168.51.101)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.51.101' (RSA) to the list of known hosts.
Connection closed by 192.168.51.101 port 22
```

- Quindi rieseguo

ssh -F ~/.ssh/temp_config msfamin@192.168.51.101 ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ssh -F ~/.ssh/temp_config msfadmin@192.168.51.101 ifconfig
msfadmin@192.168.51.101's password:
eth0      Link encap:Ethernet  HWaddr 08:00:27:38:94:a5
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe38:94a5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1374 (1.3 KB)  TX bytes:24777 (24.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

eth1      Link encap:Ethernet  HWaddr 08:00:27:54:62:9e
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe54:629e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10290 (10.0 KB)  TX bytes:12511 (12.2 KB)
          Base address:0xd240 Memory:f0820000-f0840000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:221821 (216.6 KB)  TX bytes:221821 (216.6 KB)
```

- Questa volta con successo risolvendo il problema proseguendo con l'esame

- Ho conferma come da foto allegata antecedentemente nel fine pagina 30 le interfacce di rete:

- **eth0**:
  IPv4: **192.168.50.101** (sottorete diversa da **192.168.51.0/24**, dovuta a una configurazione secondaria)
  IPv6: **fe80::a00:27ff:fe38:94a5/64**

- **eth1**:
  IPv4: **192.168.51.101** (indirizzo usato per tutte le scansioni precedenti, inlinea con nmap 7 - 11)
  IPv6: **fe80::a00:27ff:fe54:629e/64**

- **lo**:
  IPv4: **127.0.0.1** (loopback)
  IPv6: **::1/128** (loopback)

- **IPv6 configurato**: Metasploitable 2 ha indirizzi IPv6 link-local su **eth0** e **eth1**

- **Aggiunta sull'IPv4 di eth0**: L'indirizzo **192.168.50.101** su **eth0** è inaspettato, poiché tutte le scansioni precedenti hanno usato **192.168.51.101** su **eth1**
  Questo mi conferma che Metasploitable2 a due interfacce attive come sapevo già su sottoreti diverse rete interna **192.168.50.0/24** e una rete target **192.168.51.0/24**

- Test allegato di seguito

```
┌──(kali㉿kali)-[~]
└─$ nmap -6 -Pn fe80::a00:27ff:fe54:629e%eth0 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 11:17 EDT
Nmap done: 1 IP address (0 hosts up) scanned in 1.61 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -6 -Pn fe80::a00:27ff:fe54:629e%eth1 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 11:17 EDT
setup_target: failed to determine route to fe80::a00:27ff:fe54:629e
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
```

- L’output mi mostra host non rilevato **failed to determine route o 0 hosts up** a causa della separazione delle sottoreti **192.168.50.0/24 per Kali, 192.168.51.0/24 per Metasploitable 2** gestite da pfSense **vtnet1 e vtnet2** questo verificato con ip -6 addr che l'interfaccia corretta su Kali è eth0

- La scansione IPv6 non è stata completata poiché gli indirizzi link-local non sono instradabili, dimostrando che l'IPv6 non è utilizzabile per bypassare i filtri IPv4 in questa configurazione.

3.2.4 IP ID Idle Scanning

- Testerò l'IP ID Idle Scan per baypassare il filtro TCP sulla porta 80 (HTTP) di Metasploitable2 192.168.51.101 configurato in pfSesne con interfaccia **vtnet2** 19.168.51.1/24

- Ricerco **host zombie** con

nmap --script broadcast-ping 192.168.50.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap --script broadcast-ping 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 08:15 EDT
Nmap scan report for samaritan.samaritan.home.arpa (192.168.50.1)
Host is up (0.0016s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:A3:9A:EC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.101
Host is up (0.012s 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: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for epicode.internal (192.168.50.100)
Host is up (0.000012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 256 IP addresses (3 hosts up) scanned in 10.27 seconds
```

ed

nmap -sn 192.168.50.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 08:42 EDT
Nmap scan report for samaritan.samaritan.home.arpa (192.168.50.1)
Host is up (0.0010s latency).
MAC Address: 08:00:27:A3:9A:EC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.101
Host is up (0.0069s latency).
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for epicode.internal (192.168.50.100)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.91 seconds
```

- Tovando 3 host attivi
  - 192.168.50.1
  - 192.168.50.100
  - 192.168.50.101

- Procedo con la verifica **IP ID incrementale** con

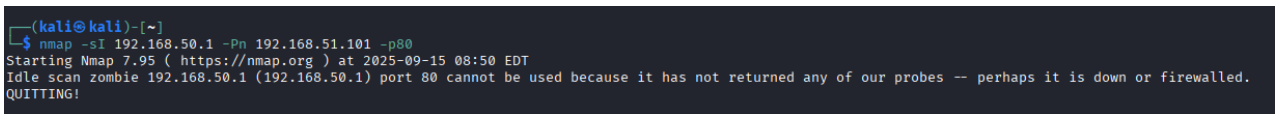
nmap --script ipidseq 192.168.50.1

```
┌──(kali㉿kali)-[~]
└─$ nmap --script ipidseq 192.168.50.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 08:17 EDT
Nmap scan report for samaritan.samaritan.home.arpa (192.168.50.1)
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:A3:9A:EC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_ipidseq: All zeros

Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds
```

- Ho ricevuto l'output **ipidseq: All zeros** indicandomi che pfSense non è valido come zombie

- Procedo con la verifica dell' **Idle Scan**

nmap -sI 192.168.50.1 -Pn 192.168.51.101 -p80



- Ho ricevuto output che mi dice (**Idle scan zombie 192.168.50.1 port 80 cannot be used because it has not returned any of our probes**) questo errore mi indica:

  - Che pfSense 192.168.50.1 non ha risposto ai probe di nmap sulla porta 80, molto probabilmente perchè la porta è filtrata o il firewall di pfSense blocca i pacchetti di test

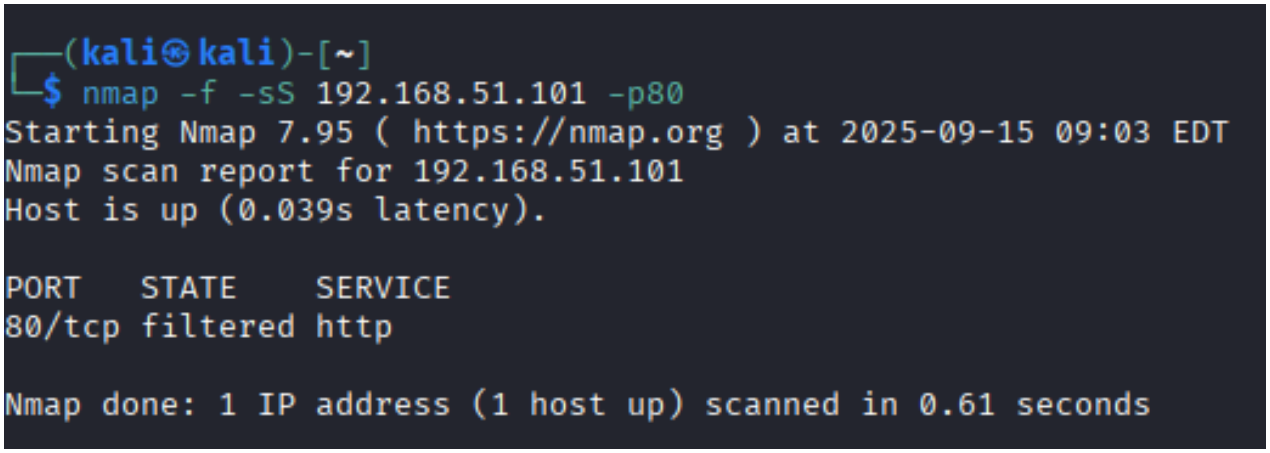
  - PfSense non è un candidato valiso come zombie perchè lo script **ipidseq** ha rilevato che l'IP ID non è incrementale **All zeros**, questà è una condizione necessaria per l'ildle Scan

  - Ho usato **-Pn** per baypassare il blocco ICMP di pfSense

3.2.5 Fragmentation

- La frammentazione TCP invia pacchetti TCP (SYN) frammentati in piccoli segmenti per baypassare filtri firewall che non gestiscono correttamente la frammentazione dei pachetti, verifico con

nmap -f -sS 192.168.51.101 -p80



- Analizzando l'output la porta 80 (HTTP) è risultata **filtered** indicando mi che il filtro TCP di pfSense corrispondente all'interfaccia **vtnet2** 192.168.51.1/24 ha bloccatto i pacchetti frammentati SYN inviati con l'opzione **-f**

- Il motivo e che pfSense ha gestito corretttamente la frammentazione TCP impedendo il baypass del filtro, coincide con i risultati di Source Port Manipulation **filtered** e indica che il firewall è configurato in modo robusto

3.2.6 MAC Adress Spoofing

- Proseguo con lo Spoofing dell'indirizzo MAC per anonimizzare la fonte e baypassare eventuali filtri basati su MAC con

nmap --spoof-mac 0 192.168.51.101 -p80

```
┌──(kali㉿kali)-[~]
└─$ nmap --spoof-mac 0 192.168.51.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 09:32 EDT
Spoofing MAC address 66:7B:59:7E:9B:02 (No registered vendor)
Nmap scan report for 192.168.51.101
Host is up (0.025s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

- Risulta **filtered** la porta 80 (HTTP) indicandomi che il filtro TCP di pfSense con interfaccia **vtnet2** 192.168.51.1/24 ha bloccato la scansione anche con spoofing dell'indirizzo MAC

- Il motivo e che pfSense non basa il filtro sull'indirizzo MAC ma su regole TCP/IP di conseguenza lo spoofing del MAC non ha influenzato il risultato

3.2.7 Source Routing

- Con

nmap --ip-options "L 192.168.50.1" 192.168.51.101 -p80

```
┌──(kali㉿kali)-[~]
└─$ nmap --ip-options "L 192.168.50.1" 192.168.51.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 09:33 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
```

- La scansione ha fallito con **Host seems down** suggerendomi di usare **-Pn** per baypassare il rilevamento dell'host tramite ping

- Il motivo è perchè pfSense blocca i pacchetti ICMP impedento a nmap di rilevare l'host 192.168.51.101, in aggiunta il source routing potrebbe non essere supportato da pfSesne o dalla rete rendendo la scasnione inefficace

- Rieseguo il comando con **-Pn** per baypassare il blocco ICMP con

nmap --ip-options "L 192.168.50.1" -Pn 192.168.51.101 -p80

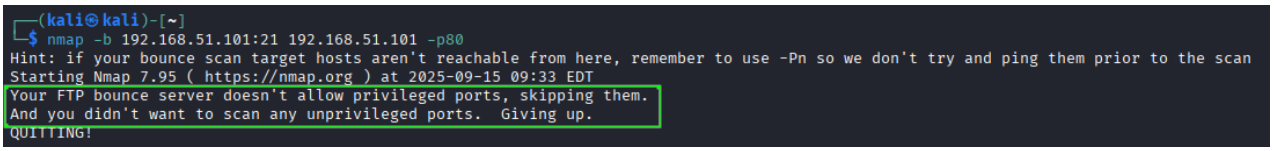
```
┌──(kali㉿kali)-[~]
└─$ nmap --ip-options "L 192.168.50.1" -Pn 192.168.51.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 09:44 EDT
Nmap scan report for 192.168.51.101
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
```

- Adesso ho conferma che la porta 80 (HTTP) su Metasploitable2 192.168.50.101 e risultata **filtered**, indicandomi che il filtro TCP di pfSense con interfaccia **vtnet2** 192.168.51.1/24 ha bloccato la scansione anche utilizzando il source routing tramite pfSene 192.168.50.1 con interfaccia **vtnet1**

3.2.8 FTP Brounce Scan

- Effettto scansione con

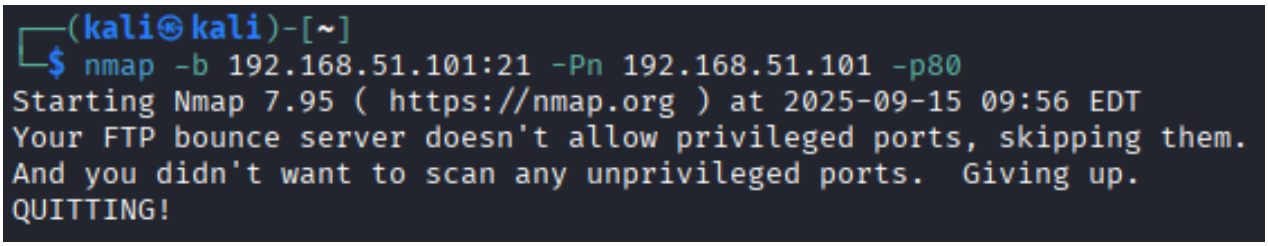
nmap -b 192.168.51.101:21 -Pn 192.168.51.101 -p80



- La scansione è fallita perchè il server FTP vsfdp 2.3.4 su Metasploitable2 192.168.51.101:21 non supporta il bounce scan per porte privilegiate tipo porta 80 che è < 1024

- Il comando **-b** di nmap tenta di sfruttare il comando FTP **PORT** per scansionare indirettamente ma vsftpd 2.3.4 non consente questa operazione per porte privilegiate.

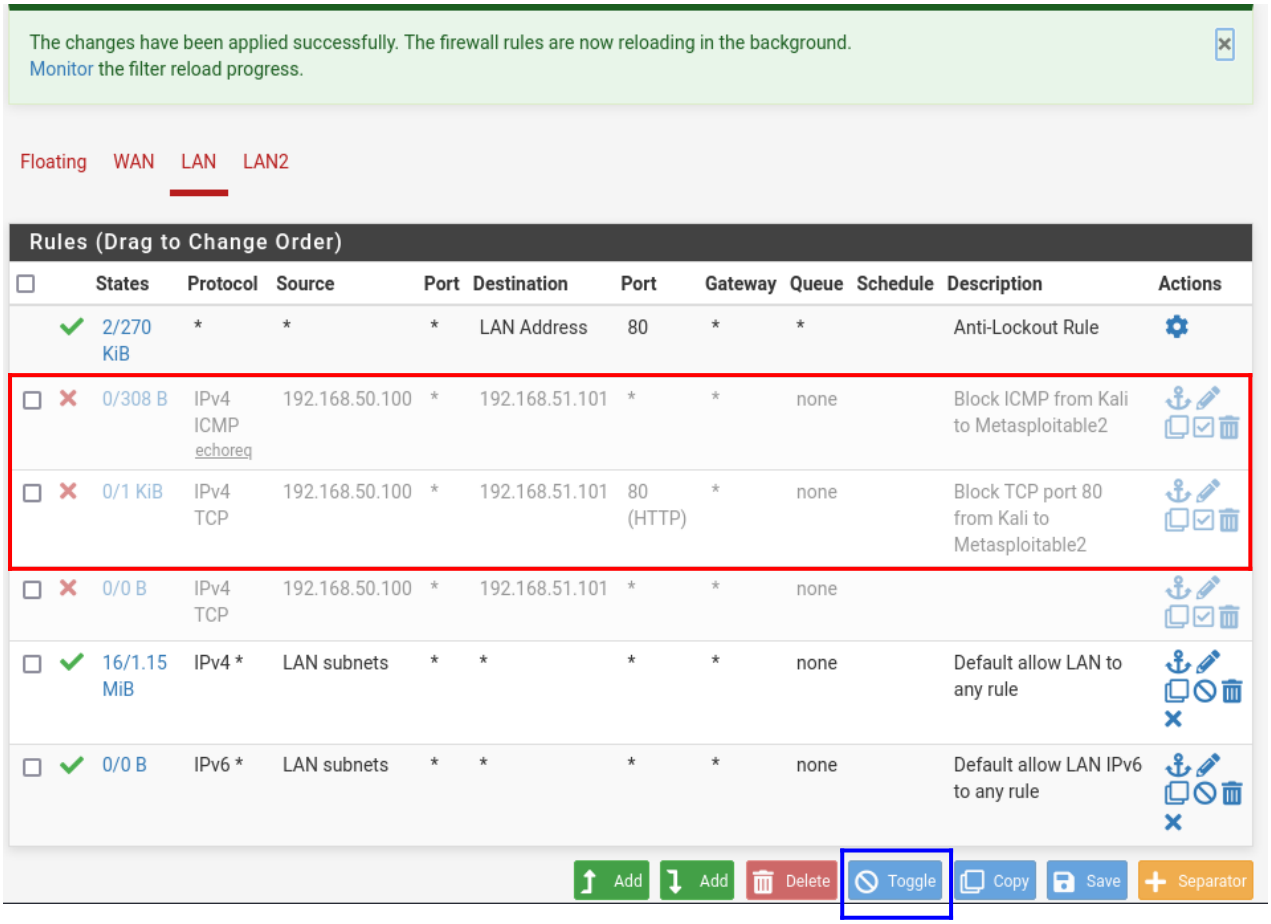
- Con l'inserimento di **-Pn** ha escluso il problema del blocco ICMP ma non ha risolto la limitazione delserver FTP



- Questo metodo FTB Brounce Scan non è applicabile in questa configurazione a causa dell limitazioni del server FTP di Metasploitable2

4 PfSense rules reset

- Accedo a pfSense e disabilito con Toggle le due regole create per svolgere l'esame, salvo e allego screeschot



- Verifico la **porta 80** con
  - nc -nvz 192.168.51.101 80
- Ho conferma

```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.51.101 80
(UNKNOWN) [192.168.51.101] 80 (http) open
```

- Verifico **ICMP** con
  - ping -c 4 192.168.51.101
- Ho conferma

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=64 time=9.91 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=64 time=3.86 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=64 time=1.67 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=64 time=18.1 ms

── 192.168.51.101 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.672/8.372/18.058/6.353 ms
```

- I test svolti di evasione firewall hanno confermato la robustezza delle regole di blocco TCP e ICMP di pfSense evidenzianto nessun metodo in grado di bypassare il filtro sulla porta 80, l'accesso è stato ripristinato con successo, come verificato tramite nc e ping allegati sopra.