

W10D4 – NICHOLAS DI ANGELO –

- Con il comando `nmap -sV <indirizzo_IP>` si esegue una scansione delle porte aperte sul target specificato e si tenta di determinare le versioni dei servizi in esecuzione su tali porte. Questo comando fornisce informazioni sulle versioni dei servizi rilevati, come ad esempio i server web, i server FTP, i server SSH, e così via

- Con il comando `nmap -p 21 -Pn -sT <indirizzo_IP>`, si effettua una scansione delle porte aperte escludendo la porta 21 (FTP) e mostrando solo le porte aperte, senza inviare il ping per determinare se l'host è raggiungibile e utilizzando una scansione TCP. In sostanza, si otterranno informazioni sulle porte aperte escluse la porta 21, senza effettuare un ping preliminare sull'host.

- Il comando corretto per eseguire una scansione SYN con Nmap è `nmap -sS <indirizzo_IP>`. Con questo comando, Nmap invia pacchetti SYN al target e ascolta le risposte per determinare lo stato delle porte. La scansione SYN è una delle tecniche di scansione più comuni ed efficaci utilizzate per scoprire le porte aperte su un host.

- Il comando corretto per eseguire una scansione UDP con Nmap è `nmap -sU <indirizzo_IP>`. Con questo comando, Nmap invia pacchetti UDP al target e ascolta le risposte per determinare lo stato delle porte UDP aperte. La scansione UDP è utile per individuare servizi e applicazioni che utilizzano il protocollo UDP anziché TCP.

- Il comando `nmap ip -p- -sV -r -e -a -ss --dns-server ns` esegue diverse azioni con Nmap:
 - `ip`: Specifica l'indirizzo IP del target da scansionare.
 - `-p-`: Specifica di scansionare tutte le porte, da 1 a 65535.
 - `-sV`: Attiva il rilevamento del servizio per determinare le versioni dei servizi in esecuzione sulle porte aperte.
 - `-r`: Esegue una scansione casuale delle porte anziché una scansione sequenziale.
 - `-e`: Abilita la modalità di identificazione dell'interfaccia di rete utilizzata.
 - `-a`: Esegue la scansione delle porte ACK per determinare se una porta è aperta, filtrata o chiusa.
 - `-ss`: Specifica di utilizzare la tecnica di scansione SYN per determinare lo stato delle porte.
 - `--dns-server ns`: Specifica il server DNS da utilizzare per le risoluzioni DNS durante la scansione.

In sintesi, con questo comando, Nmap esegue una scansione approfondita sul target, inclusi tutti i porti, determina le versioni dei servizi in esecuzione, esegue una scansione casuale delle porte e utilizza un server DNS specifico per le risoluzioni DNS.

- Con il comando `nmap -sS -sV -T4 ip`, stai eseguendo una scansione utilizzando le seguenti opzioni:
 - `-sS`: Specifica di utilizzare la tecnica di scansione SYN per determinare lo stato delle porte. Questo è un tipo di scansione stealth che non completa la connessione TCP, ma invia solo il pacchetto di SYN e aspetta una risposta.
 - `-sV`: Attiva il rilevamento del servizio per determinare le versioni dei servizi in esecuzione sulle porte aperte.
 - `-T4`: Specifica il livello di aggressività della scansione. In questo caso, è impostato su T4, che è una velocità di scansione media e aggressiva.

Quindi, con questo comando, stai eseguendo una scansione SYN per determinare lo stato delle porte aperte e, contemporaneamente, stai cercando di identificare le versioni dei servizi in esecuzione su tali porte. La scansione è impostata su un livello di aggressività medio.

- Il comando `crackmapexec` è uno strumento utilizzato per l'analisi e l'esecuzione di attacchi di forza bruta su sistemi Windows. Con `crackmapexec ip`, si esegue uno scan per individuare le vulnerabilità sui sistemi Windows presenti all'indirizzo IP specificato. Il tool tenta di eseguire l'accesso ai servizi di rete utilizzando varie tecniche di attacco, inclusi attacchi di forza bruta per scoprire credenziali deboli o predefinite.
- Il comando `nc -nvz ip` esegue una scansione delle porte aperte su un determinato indirizzo IP utilizzando Netcat. Ecco cosa significano i singoli parametri:
 - `-n`: Imposta Netcat in modalità "non-risoluzione DNS", il che significa che non verranno effettuate risoluzioni DNS per gli indirizzi IP o i nomi host.
 - `-v`: Attiva la modalità "verbose", che mostra output dettagliato durante l'esecuzione del comando.
 - `-z`: Imposta Netcat in modalità "scansione delle porte", che esegue solo la scansione delle porte senza inviare alcun dato.
 - `ip`: Rappresenta l'indirizzo IP del sistema target su cui si desidera eseguire la scansione delle porte.

In sintesi, eseguendo questo comando, verranno elencate le porte aperte sul sistema corrispondente all'indirizzo IP specificato.

- Con il comando `nmap ip --top-port 10 --open`, stai eseguendo una scansione utilizzando Nmap sull'indirizzo IP specificato. Ecco cosa significano i singoli parametri:
 - `ip`: Rappresenta l'indirizzo IP del sistema target su cui si desidera eseguire la scansione.
 - `--top-port 10`: Specifica di scansionare solo le prime 10 porte più comuni. Questo riduce il tempo necessario per completare la scansione, concentrandosi solo sulle porte più utilizzate.
 - `--open`: Specifica di mostrare solo le porte aperte durante la scansione.

Quindi, eseguendo questo comando, Nmap eseguirà una scansione delle prime 10 porte più comuni sull'indirizzo IP specificato e mostrerà solo le porte aperte durante la scansione.

- Con il comando `nc -nvz ip`, stai utilizzando il comando `nc` (netcat) per eseguire un controllo di connettività verso l'indirizzo IP specificato. Ecco cosa significano i singoli parametri:
 - `-nvz`: Questi sono i parametri di `nc`:
 - `-n`: Specifica di non risolvere simbolicamente gli indirizzi IP e i nomi di host.
 - `-v`: Specifica la modalità verbosa, che mostra output dettagliato durante l'esecuzione.
 - `-z`: Specifica di eseguire una scansione di tipo "zero-I/O", che significa che nc non invierà alcun dato dopo la connessione.
 - `ip`: Rappresenta l'indirizzo IP del sistema target verso cui si sta eseguendo il controllo di connettività.

Quindi, eseguendo questo comando, `nc` cercherà di connettersi all'indirizzo IP specificato, mostrando output dettagliato sulla connessione durante l'esecuzione. La modalità "zero-I/O" assicura che nc non invii dati dopo la connessione, ma mostra solo se la connessione è possibile.

data
18.17.04

data
0.47.03

● ● ●

o

sfadmin@metasploitable:~\$ _



metasploitable2 [Running]

```
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:24:01:f5
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:1f5/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
             RX packets:2861 errors:0 dropped:0 overruns:0 frame:0
             TX packets:2659 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:210499 (205.5 KB)  TX bytes:176422 (172.2 KB)
             Base address:0xd020  Memory:f0200000-f0220000

          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:126 errors:0 dropped:0 overruns:0 frame:0
             TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:35929 (35.0 KB)  TX bytes:35929 (35.0 KB)

sfadmin@metasploitable:~$ _
```

kali linux 1 [Running]



Trash, File System, Home, wireshark, putty.exe

File Actions Edit View Help

```
(root@kali)-[~]
# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 09:06 CE
ST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00057s 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?
513/tcp   open  login
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
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: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```





data
18.17.04



data
0.47.03



o

sfadmin@metasploitable:~\$

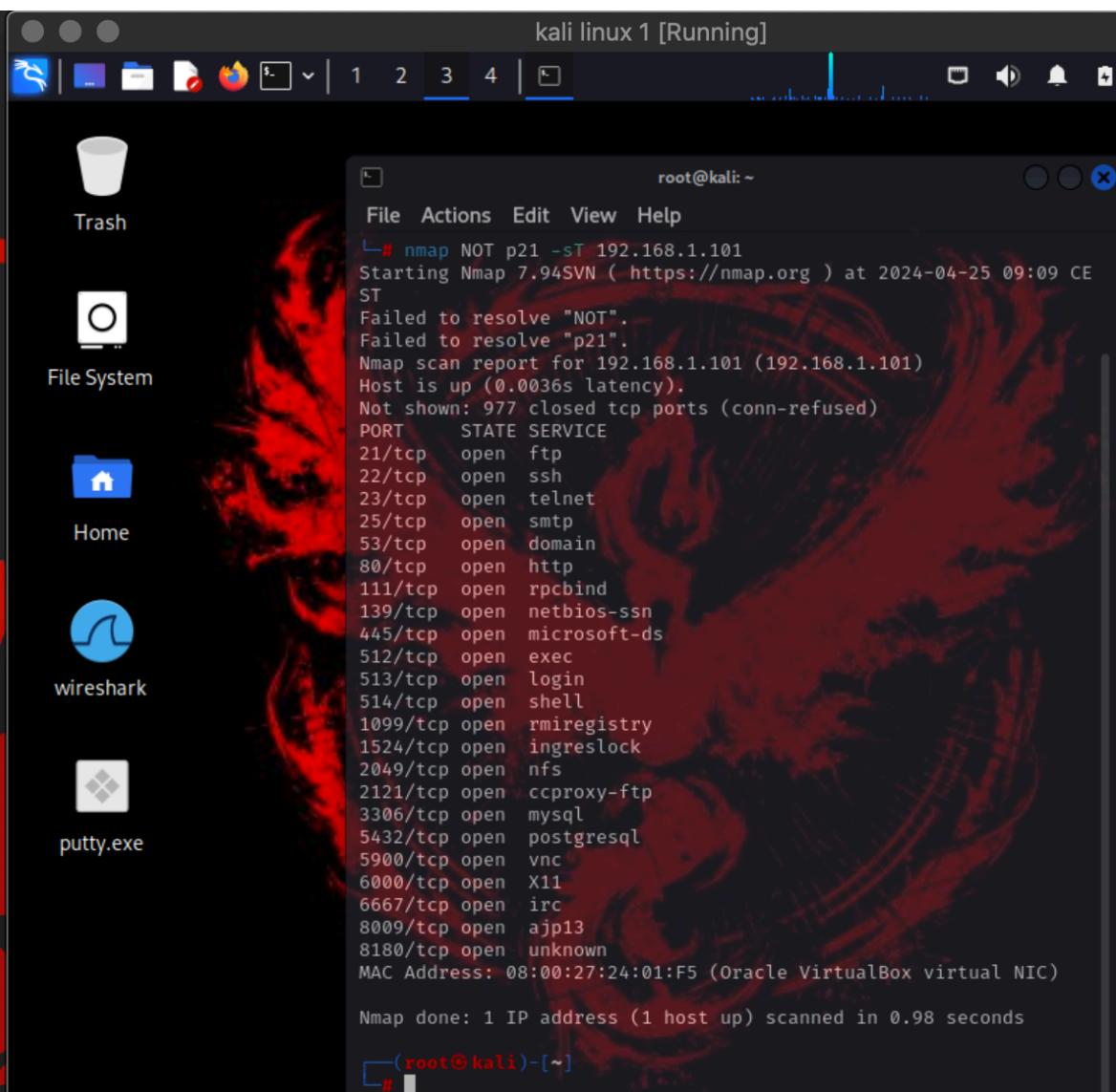


metasploitable2 [Running]

```
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:24:01:f5
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:1f5/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:2861 errors:0 dropped:0 overruns:0 frame:0
             TX packets:2659 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:210499 (205.5 KB)  TX bytes:176422 (172.2 KB)
             Base address:0xd020  Memory:f0200000-f0220000

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:126 errors:0 dropped:0 overruns:0 frame:0
             TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:35929 (35.0 KB)  TX bytes:35929 (35.0 KB)
```

sfadmin@metasploitable:~\$





data
18.17.04



data
0.47.03



metasploitable2 [Running]

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

Metasploitable login: msfadmin
Password:
Last login: Wed Apr 24 16:15:19 EDT 2024 on ttym1
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/
To mail:
msfadmin@metasploitable:~$
```



kali linux 1 [Running]

Trash

File System

Home

wireshark

putty.exe

```
root@kali:~# nmap -sT 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 08:58 CE
ST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.005s 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
MAC Address: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

(root@kali)-[~]

#





data
18.17.04



data
0.47.03



metasploitable2 [Running]

```
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:24:01:f5
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:1f5/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
             RX packets:6477 errors:0 dropped:0 overruns:0 frame:0
             TX packets:5964 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:493620 (482.0 KB)  TX bytes:434495 (424.3 KB)
             Base address:0xd020 Memory:f0200000-f0220000

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:210 errors:0 dropped:0 overruns:0 frame:0
             TX packets:210 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:77177 (75.3 KB)  TX bytes:77177 (75.3 KB)

sfadmin@metasploitable:~$ _
```

Left ☰

kali linux 1 [Running]

Trash

File System

Home

wireshark

putty.exe

File Actions Edit View Help

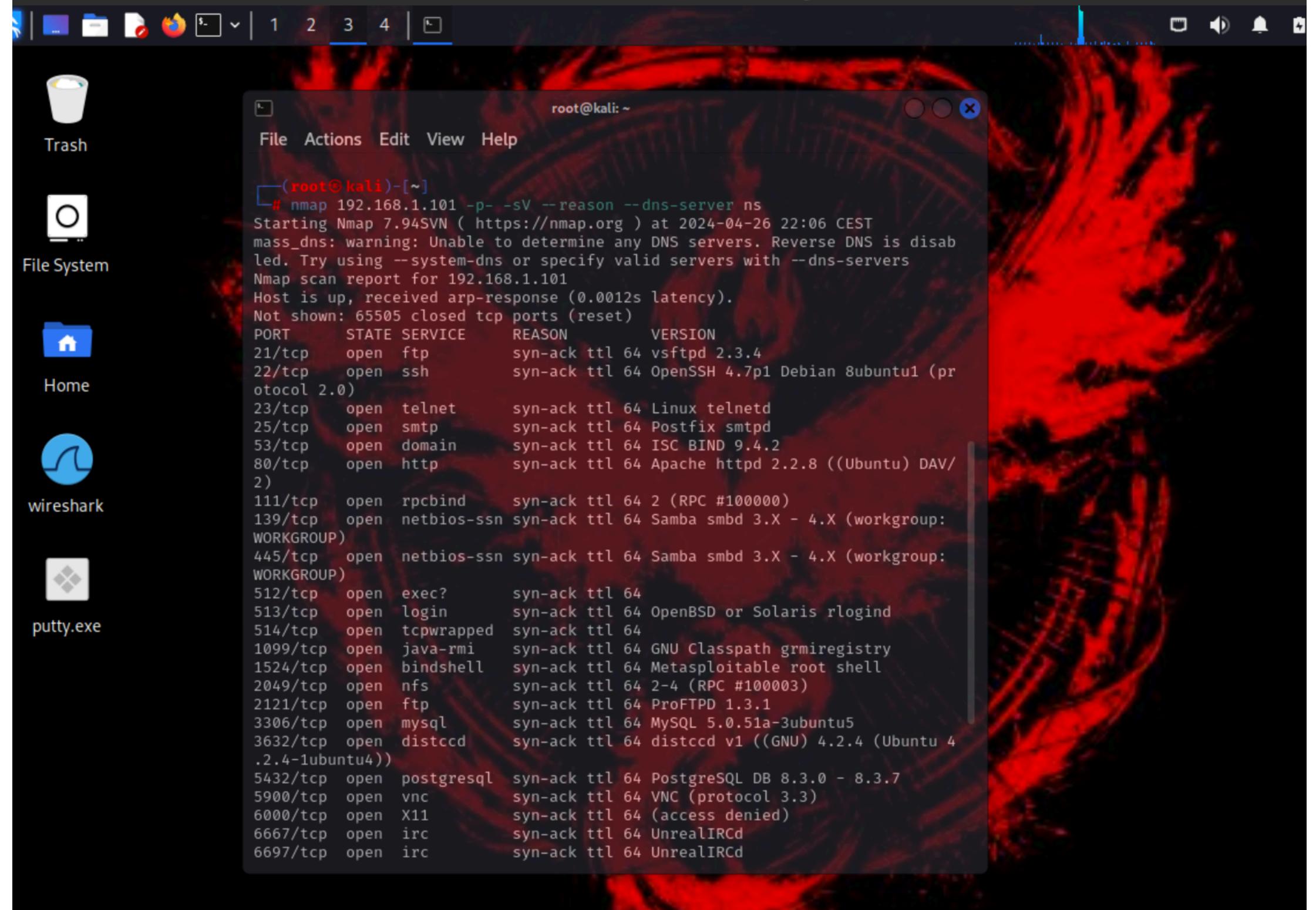
```
(root@kali)-[~]
# nmap -sU 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 09:10 CE
ST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00088s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
MAC Address: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

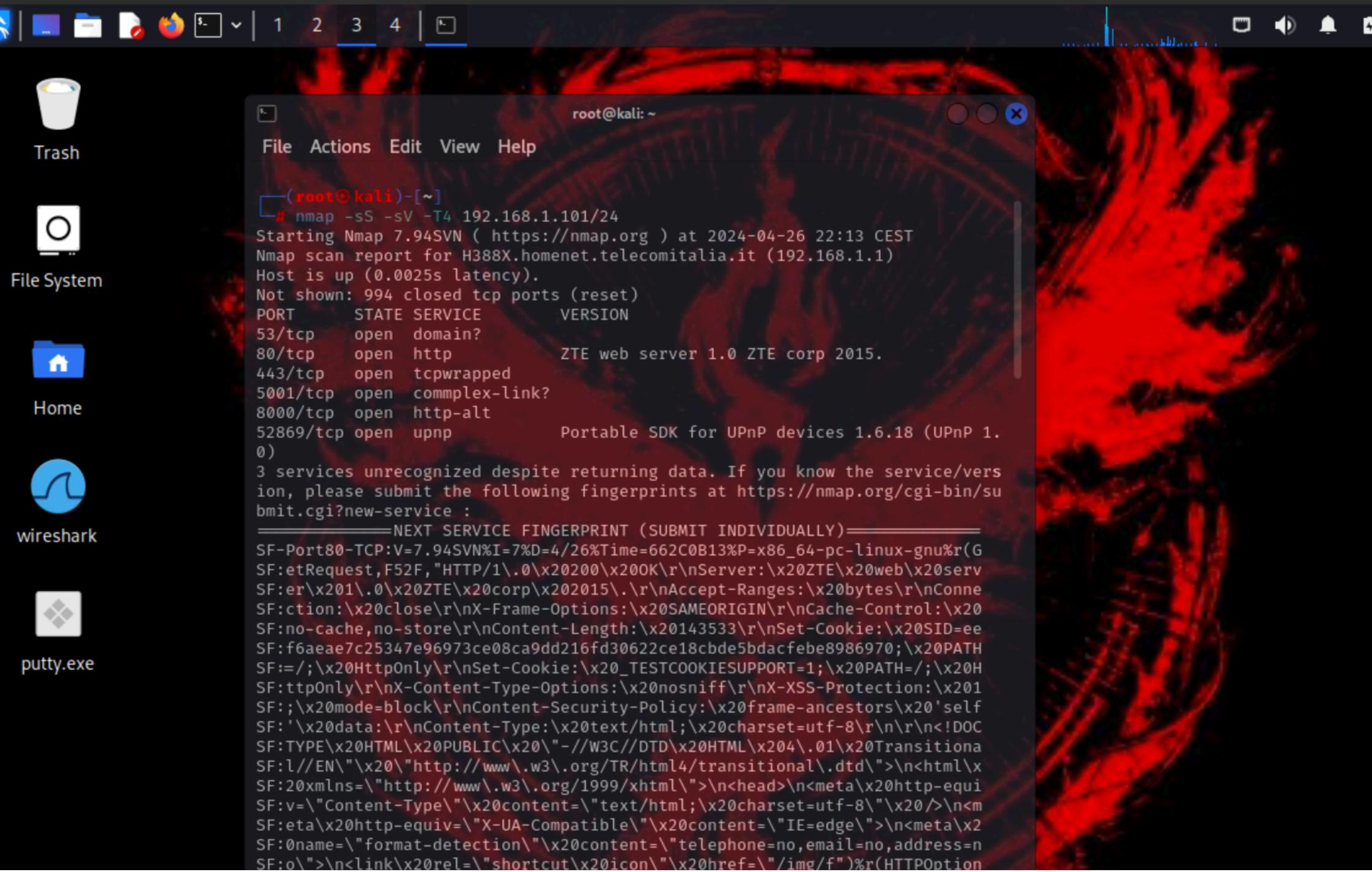
Nmap done: 1 IP address (1 host up) scanned in 1119.26 seconds

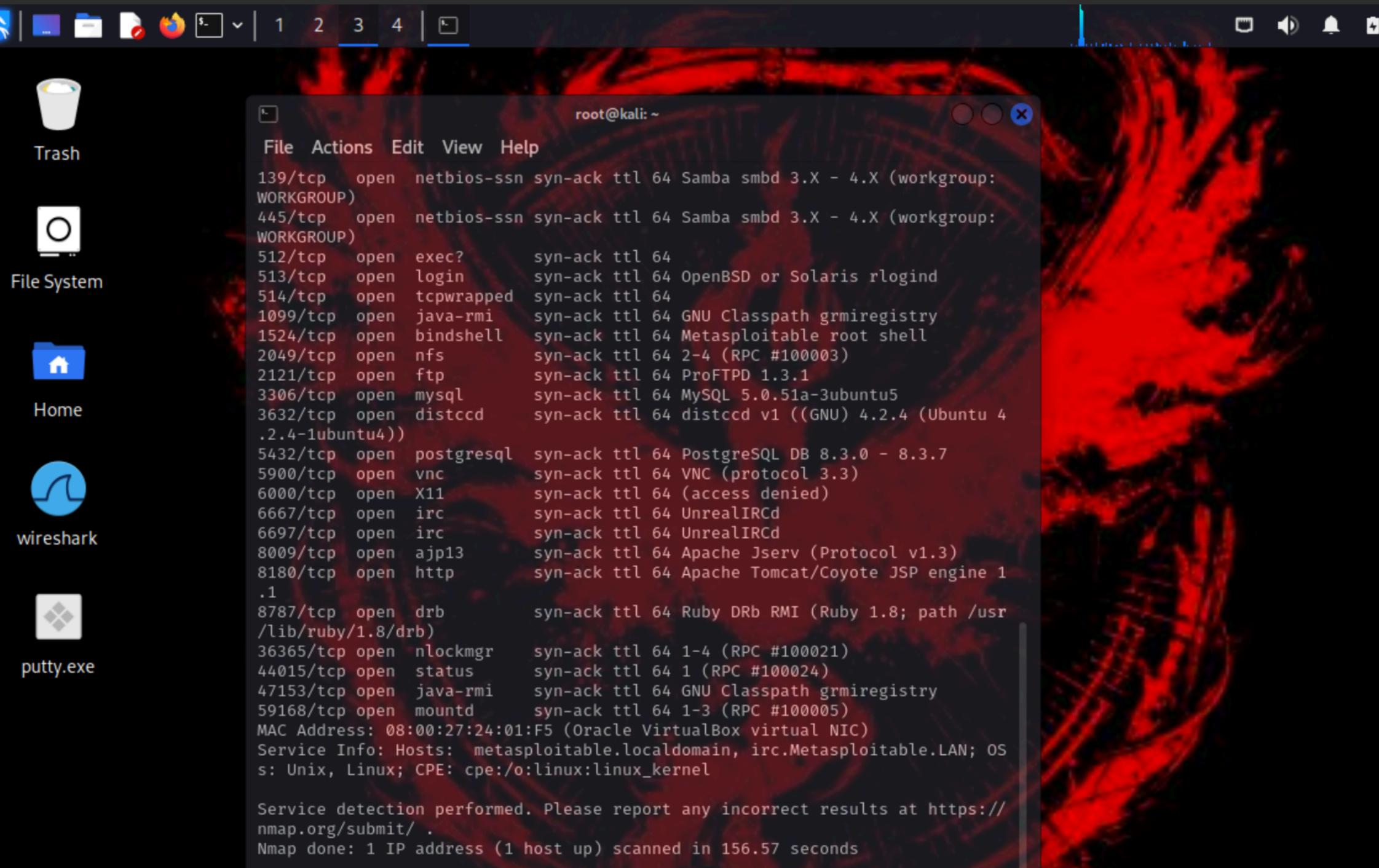
(root@kali)-[~]
#
```

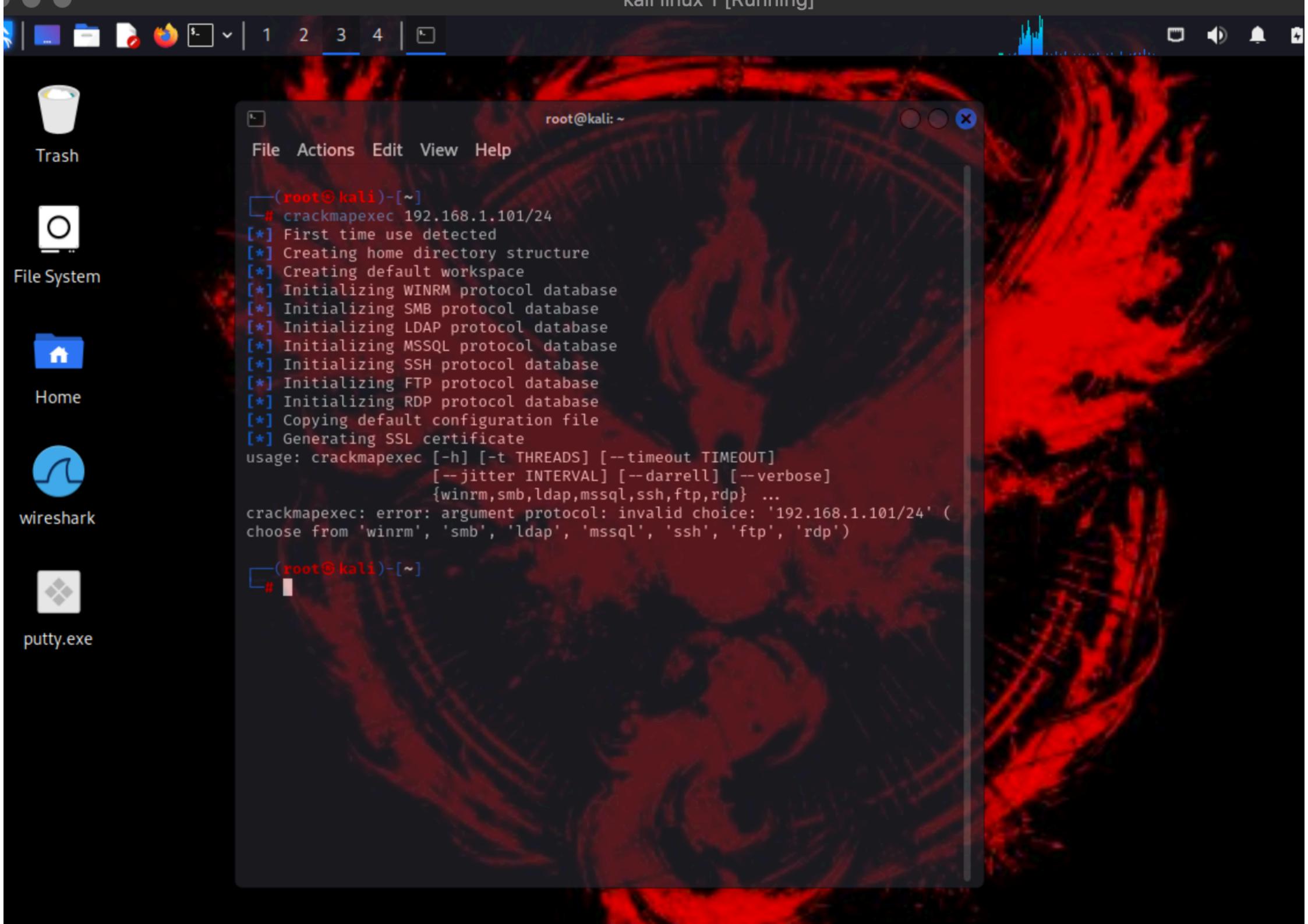
Left ☰

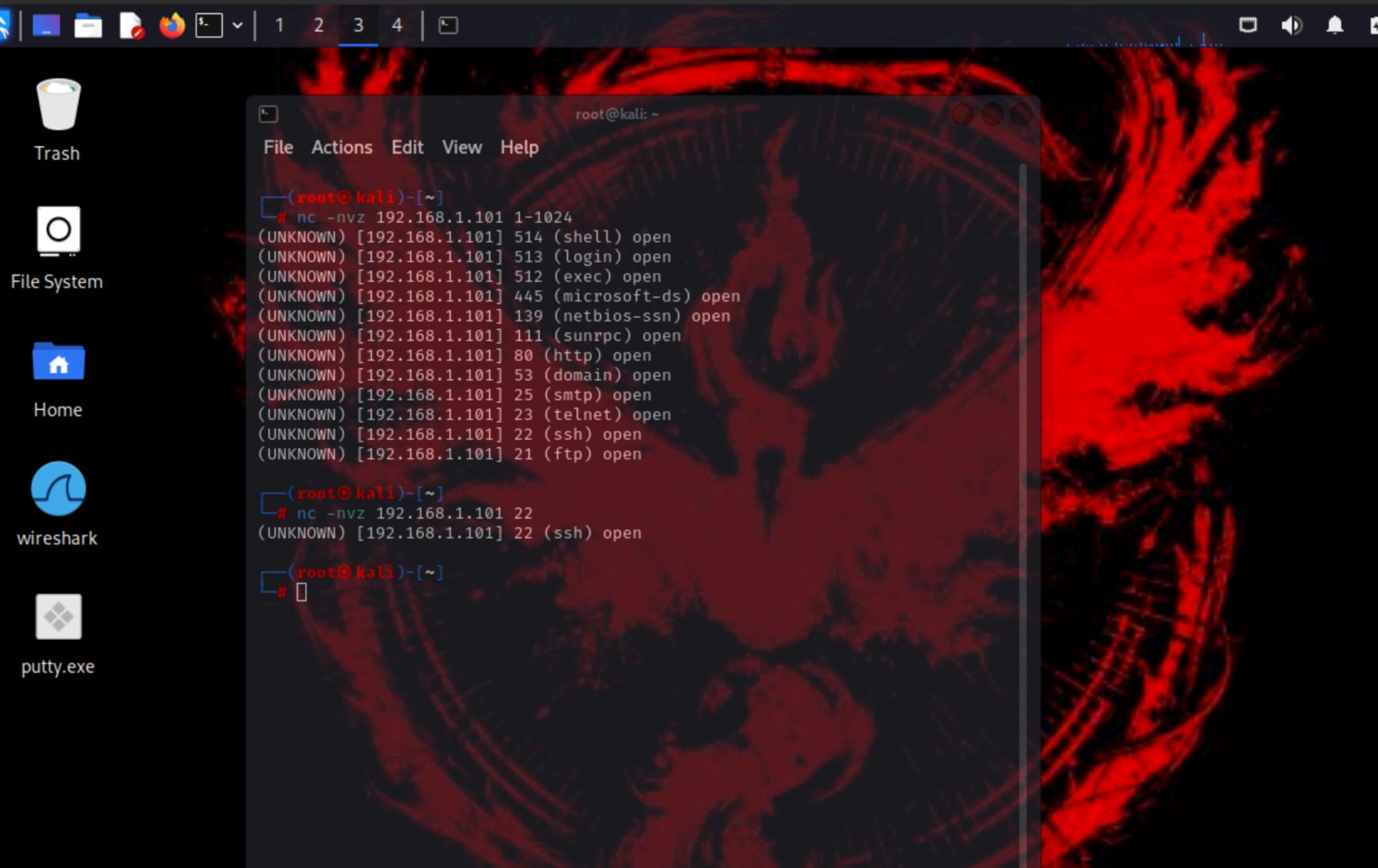


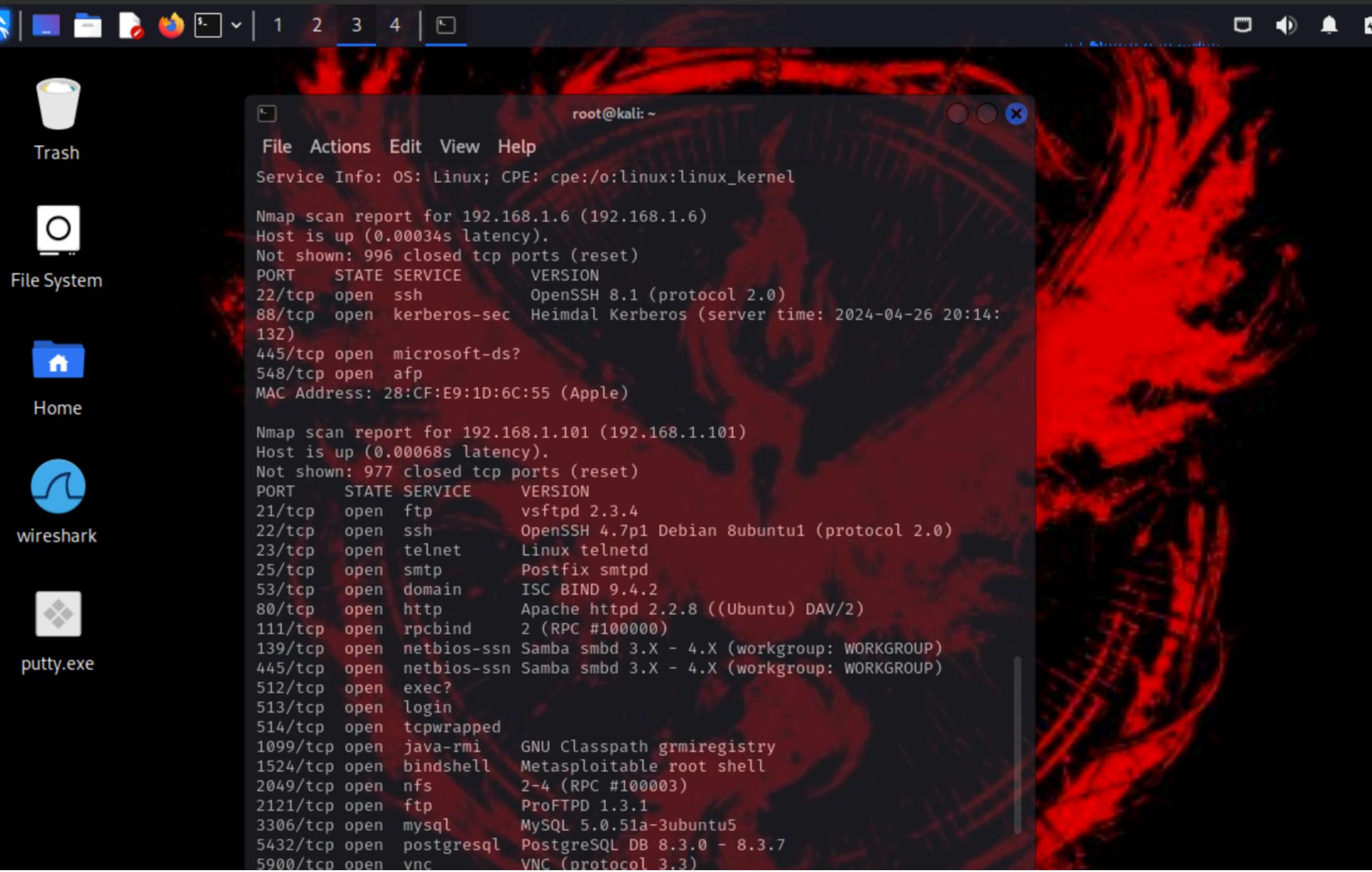












wireshark



putty.exe

```
[root@kali) [~]
# nmap 192.168.1.101 --top-port 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 22:05 CEST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00078s 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
MAC Address: 08:00:27:24:01:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

[root@kali) [~]
#
```

kali linux 1 [Running]

