ESERCIZIO GIORNO 3PT

Identificazione servizi e scansione

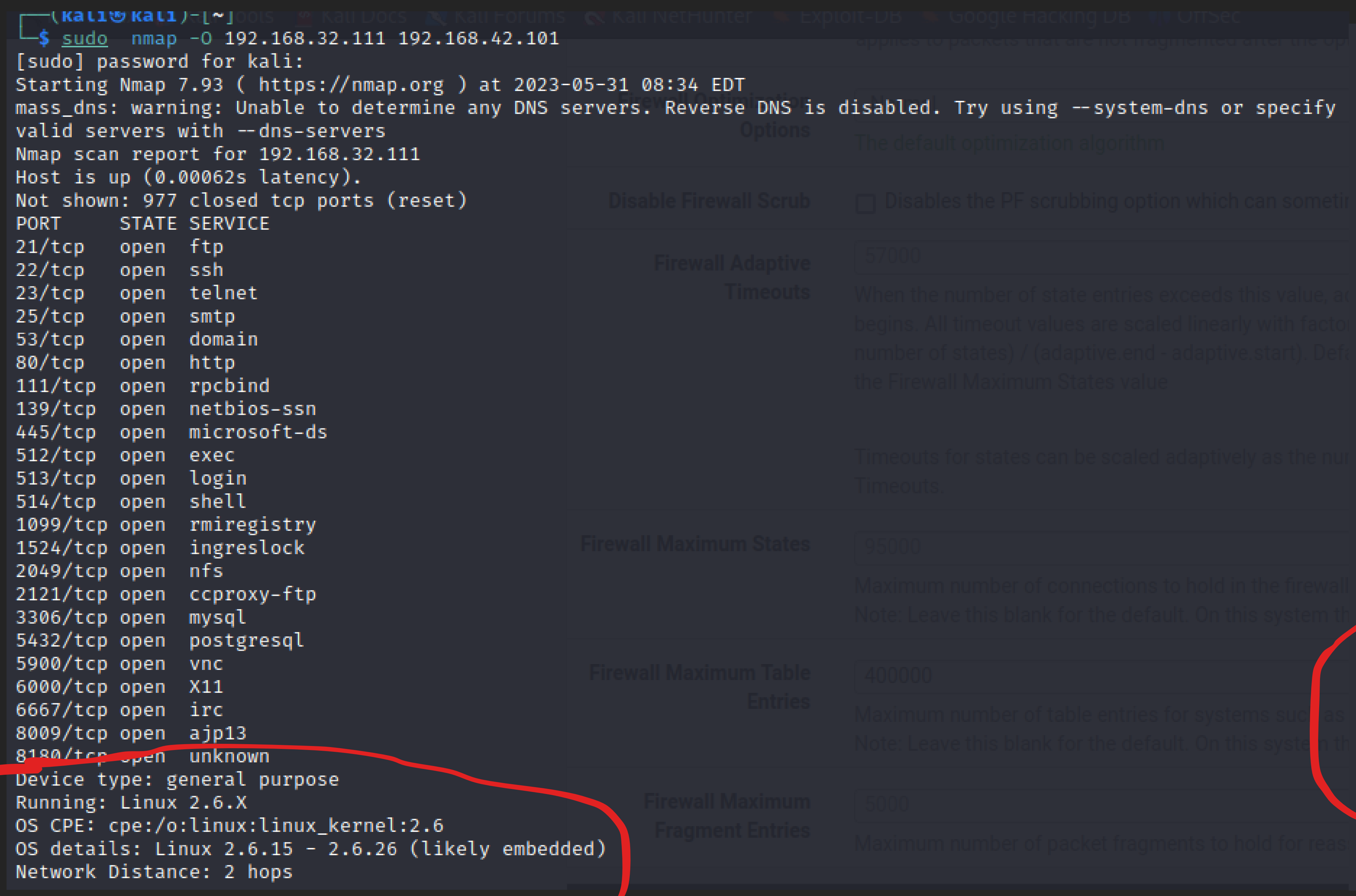
EPICODE

Giovanni Pisapia

SCANSIONE OS FINGERPRINT

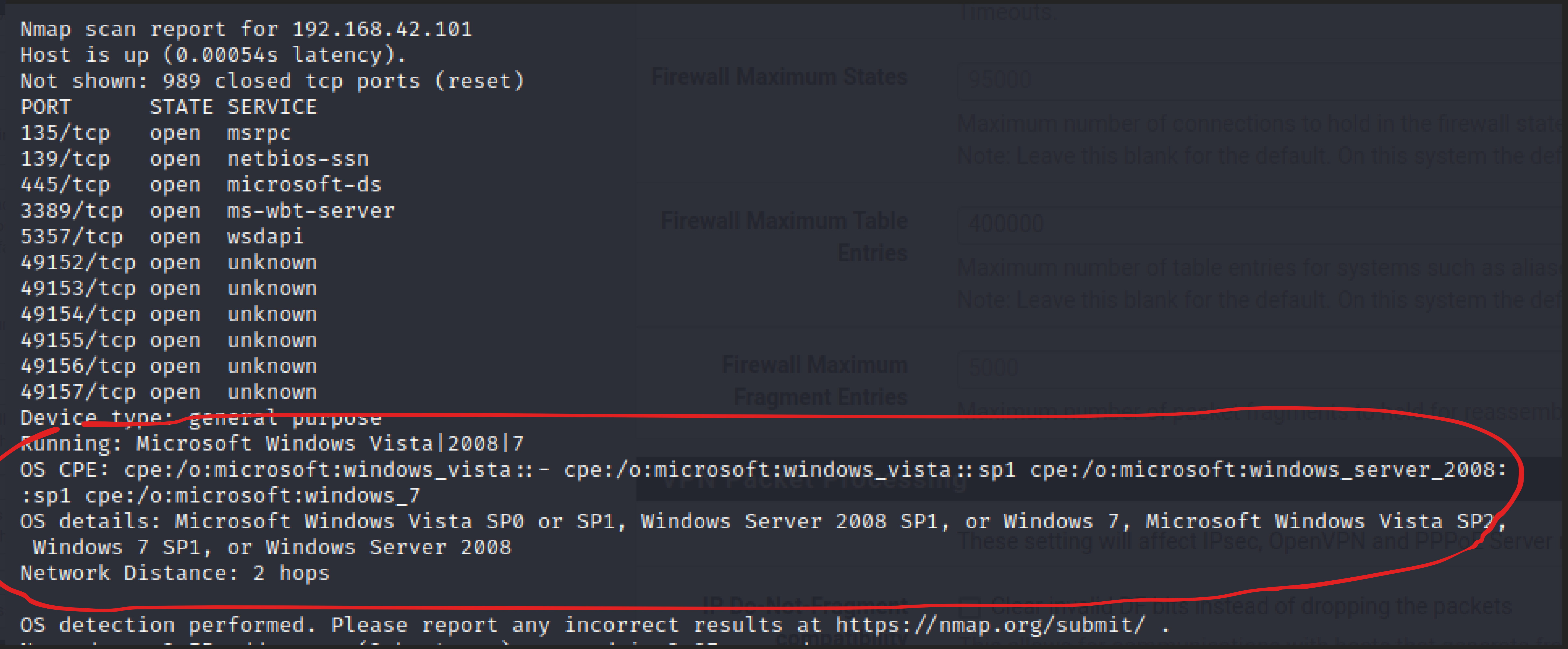
La scansione OS fingerprint, o rilevazione del sistema operativo, serve per determinare il sistema operativo presente su un determinato host. Questo processo coinvolge la consultazione di un database di firme conosciute per confrontare le risposte dei pacchetti inviati all'host e identificare in modo accurato il sistema operativo in uso. e si fa partire con il comando Nmap -O

KALI



```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap -O 192.168.32.111 192.168.42.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:34 EDT
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 192.168.32.111
Host is up (0.00062s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
```

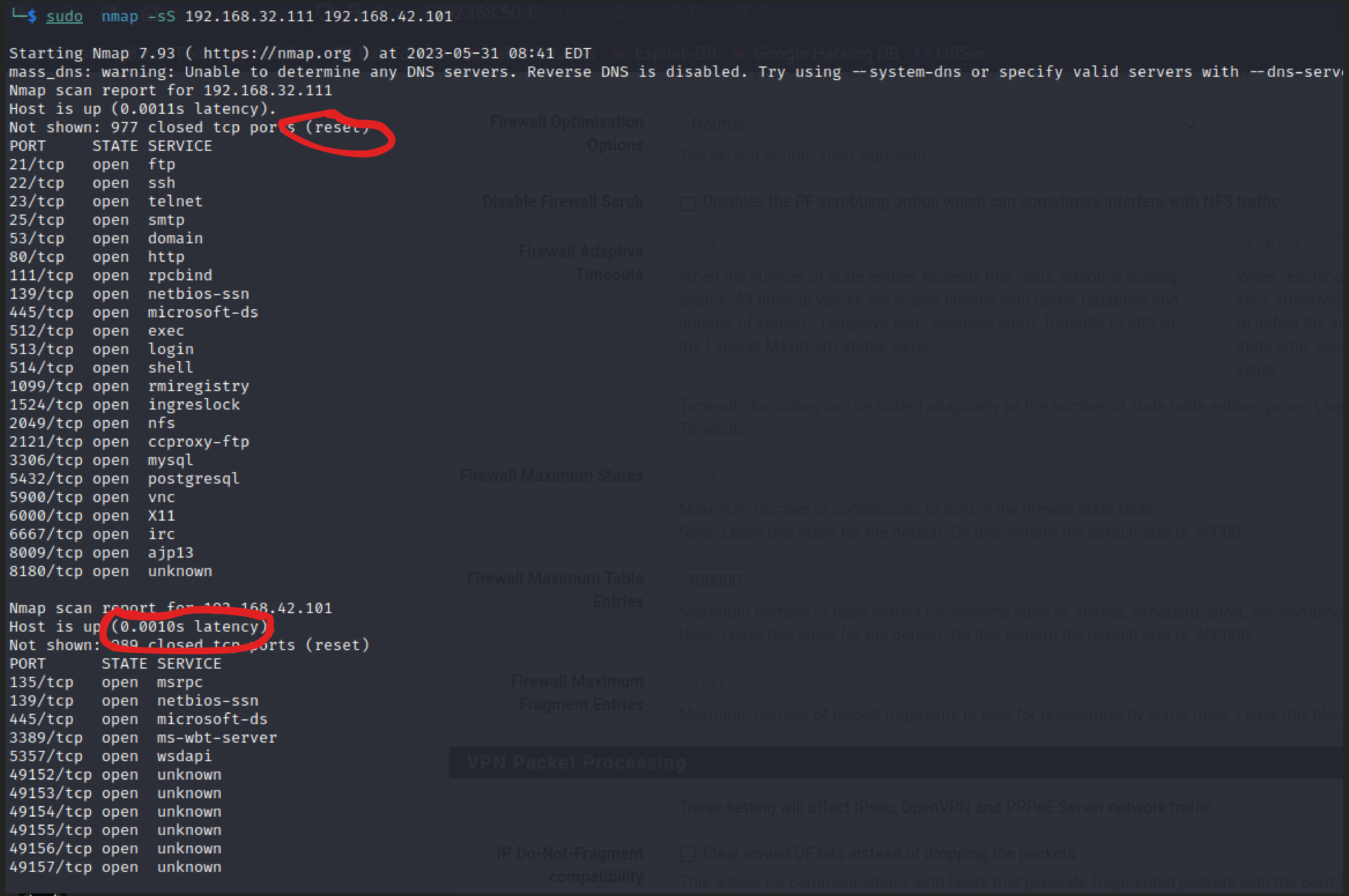
WINDOWS



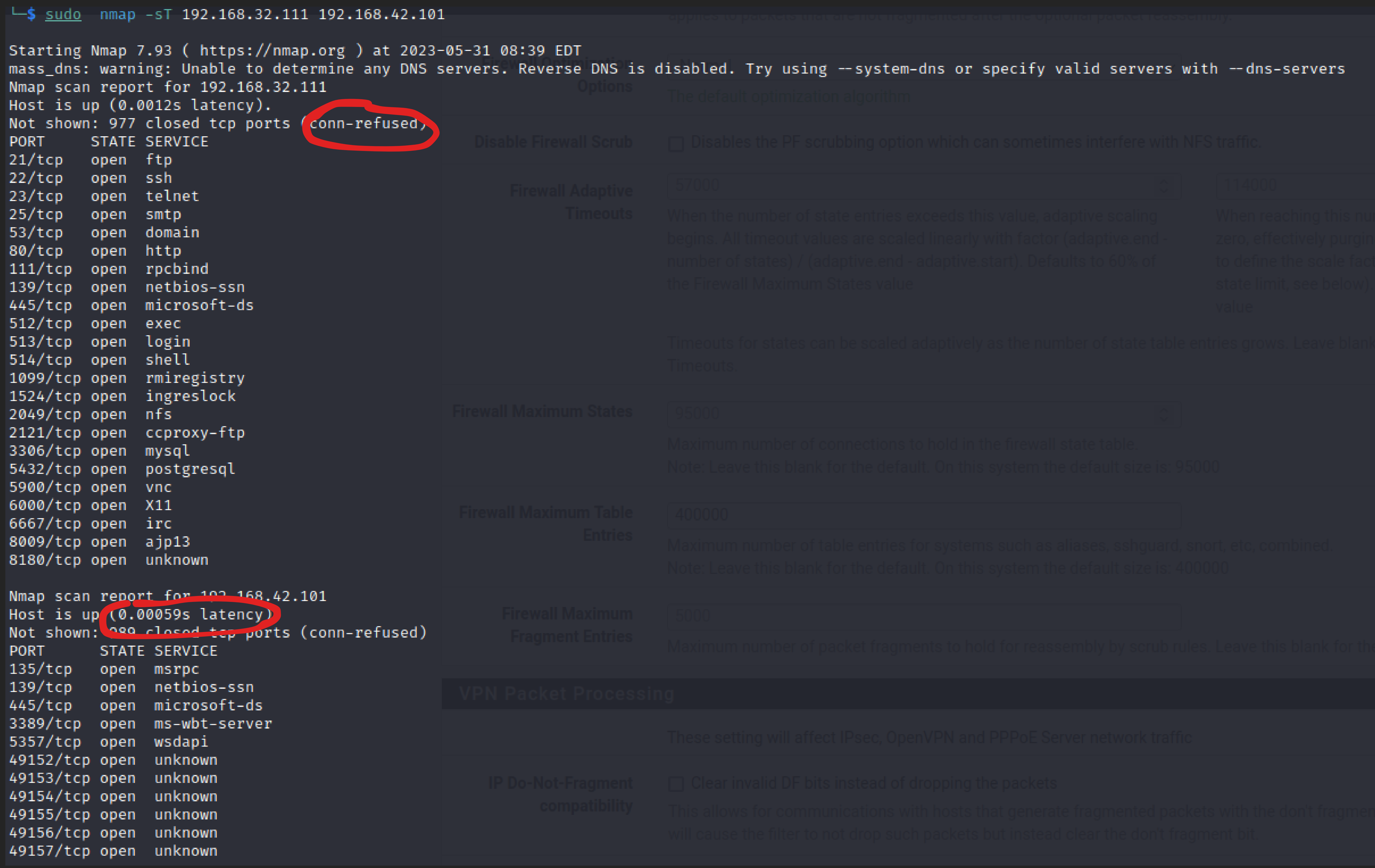
```
Nmap scan report for 192.168.42.101
Host is up (0.00054s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008:
:sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2,
 Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

STEALTH SCANNING- TCP

La differenza tra le scansioni TCP connect e SYN in Nmap riguarda il modo in cui vengono contattate le porte di destinazione. La scansione TCP connect stabilisce una connessione completa inviando più pacchetti, mentre la scansione SYN invia solo un pacchetto e termina immediatamente la connessione inviando un pacchetto rst. La scansione TCP connect è più accurata ma richiede più tempo, mentre la scansione SYN è più veloce ma potrebbe non fornire tutti i risultati desiderati in alcune situazioni. La scansione viene eeguita con nmap -sS per la SYN e per la TCP con nmap -sT



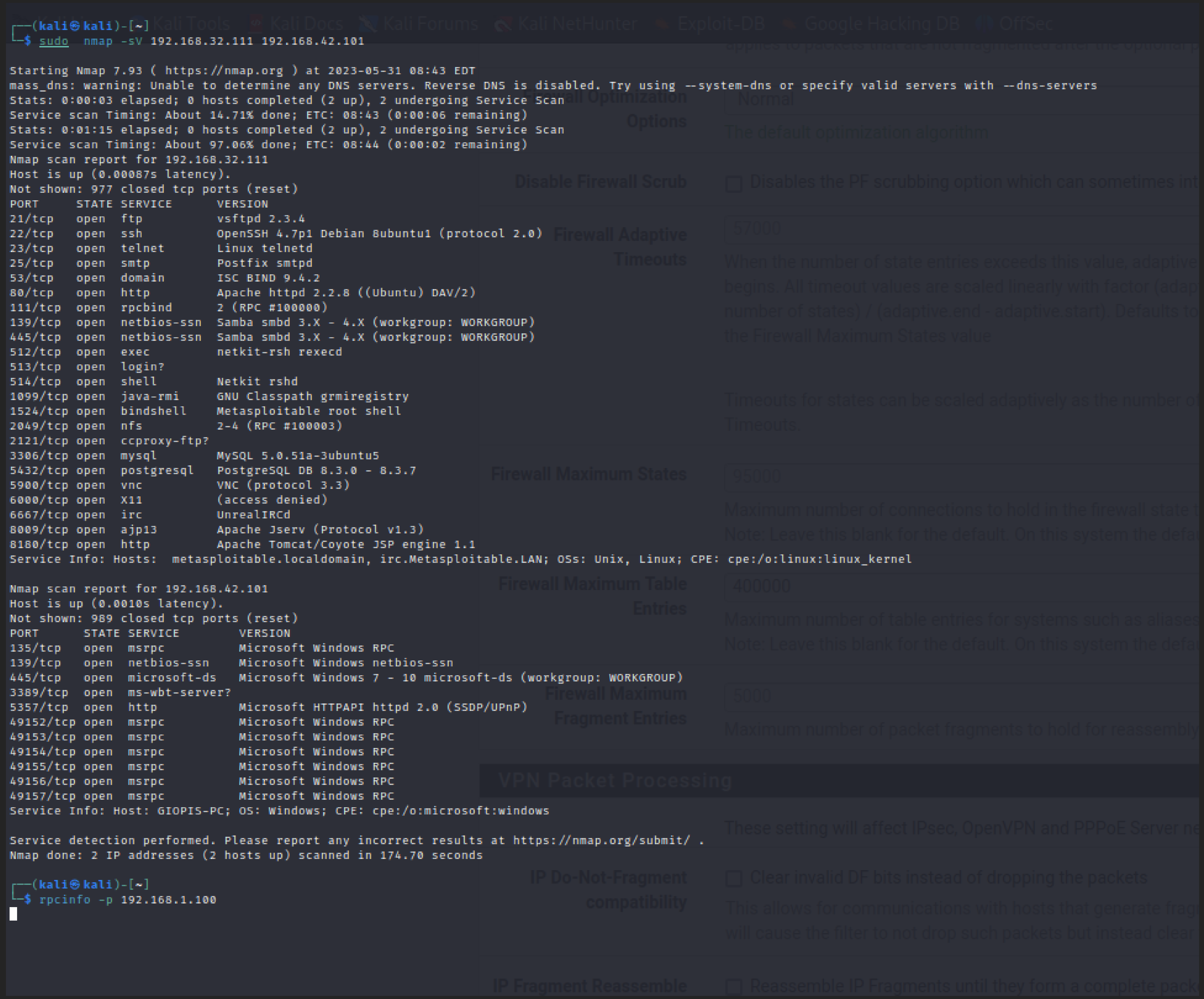
```
└─$ sudo  nmap -sS 192.168.32.111 192.168.42.101

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:41 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-serv
Nmap scan report for 192.168.32.111
Host is up (0.0011s 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 scan report for 192.168.42.101
Host is up (0.0010s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```



```
└─$ sudo  nmap -sT 192.168.32.111 192.168.42.101

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:39 EDT
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 192.168.32.111
Host is up (0.0012s 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 scan report for 192.168.42.101
Host is up (0.00059s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

Scanner Version Detection

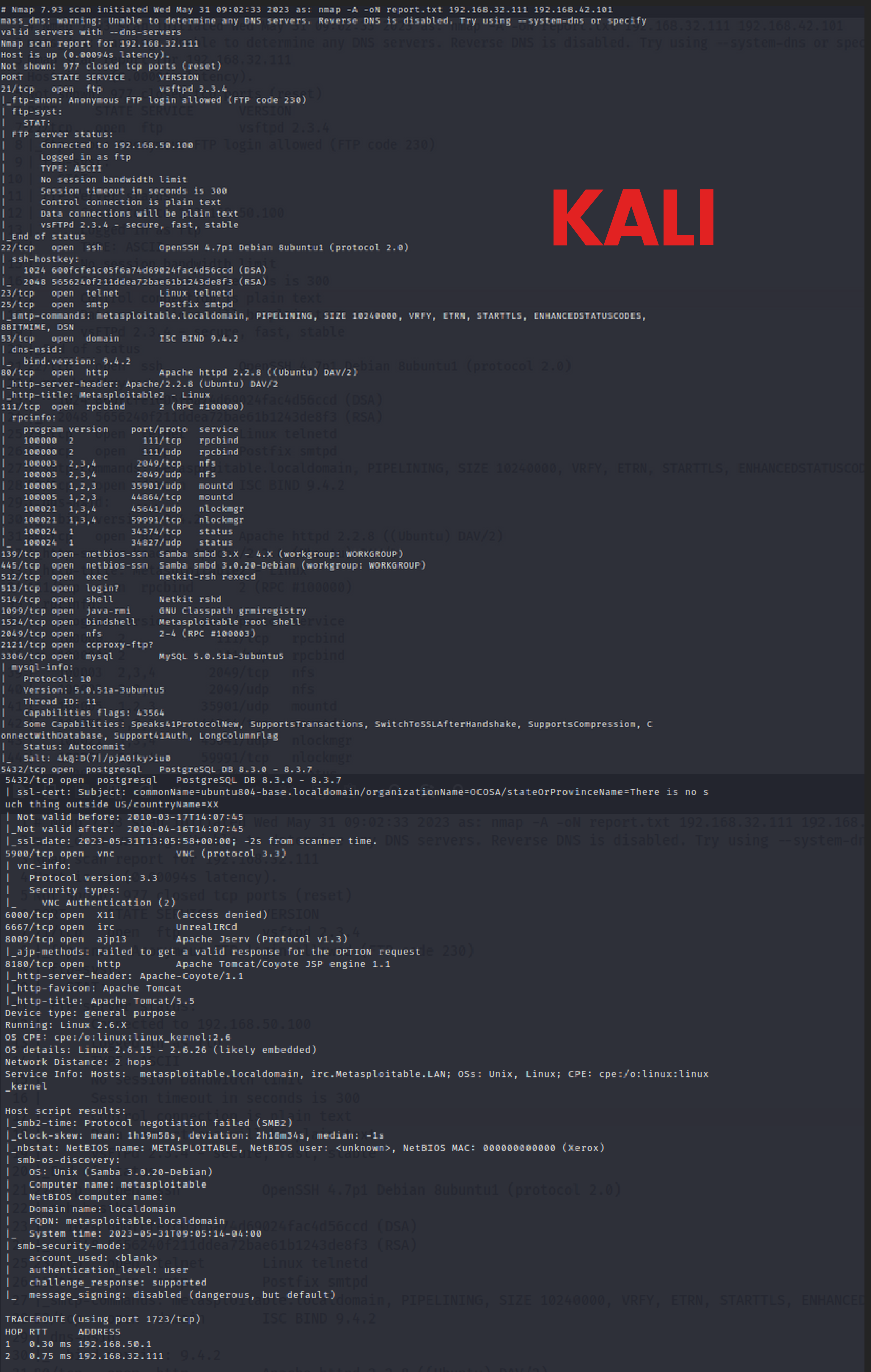
Con il cmando nmap-sV consente di eseguire una scansione di rilevamento delle versioni dei servizi. In poche parole, Nmap cercherà di identificare le versioni dei servizi che sono in ascolto sulle porte aperte su un determinato host.



```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap -sV 192.168.32.111 192.168.42.101

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:43 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:03 elapsed; 0 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 14.71% done; ETC: 08:43 (0:00:06 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 97.06% done; ETC: 08:44 (0:00:02 remaining)
Nmap scan report for 192.168.32.111
Host is up (0.00087s 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  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.42.101
Host is up (0.0010s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: Host: GIOPIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 174.70 seconds

┌──(kali㉿kali)-[~]
└─$ rpcinfo -p 192.168.1.100
```

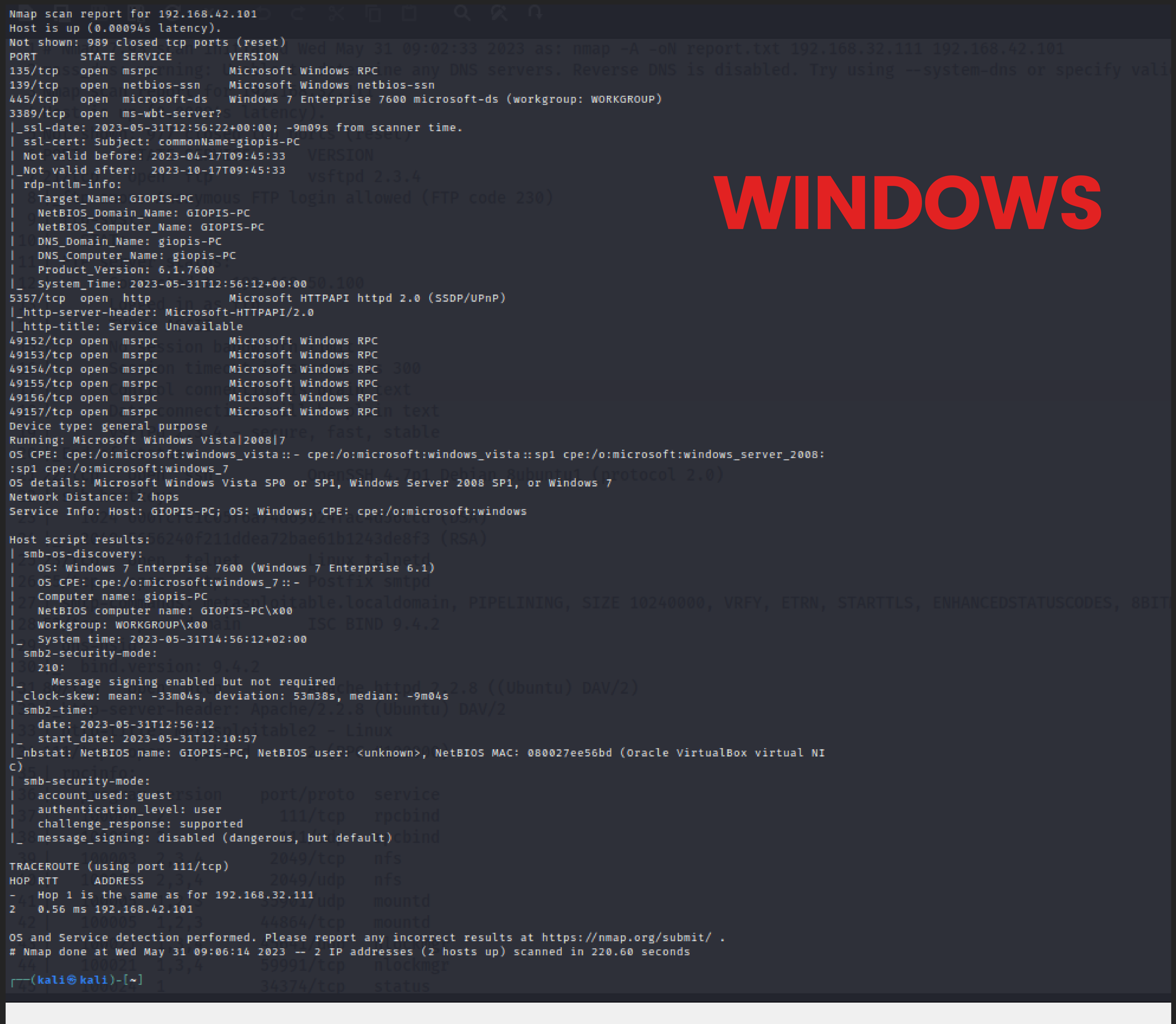
REPORT

Infine il report è stato generato utilizzando l'opzione "-A" (aggressiva) per ottenere informazioni dettagliate e successivamente è stato esportato in un file di testo con il comando "nmap -oN report.txt"



KALI

```
# Nmap 7.93 scan initiated Wed May 31 09:02:33 2023 as: nmap -A -oN report.txt 192.168.32.111 192.168.42.101
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 192.168.32.111
Host is up (0.00094s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35901/udp   mountd
|   100005  1,2,3      44864/tcp   mountd
|   100021  1,3,4      45641/udp   nlockmgr
|   100021  1,3,4      59991/tcp   nlockmgr
|   100024  1          34374/tcp   status
|_  100024  1          34827/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, SupportsTransactions, SwitchToSSLAfterHandshake, SupportsCompression, C
onnectWithDatabase, Support41Auth, LongColumnFlag
|   Status: Autocommit
|_  Salt: 4k@:D(7|/pjAG!ky>iu0
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-05-31T13:05:58+00:00; -2s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h19m58s, deviation: 2h18m34s, median: -1s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-31T09:05:14-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   0.30 ms 192.168.50.1
2   0.75 ms 192.168.32.111
```



WINDOWS

```
Nmap scan report for 192.168.42.101
Host is up (0.00094s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server?
|_ssl-date: 2023-05-31T12:56:22+00:00; -9m09s from scanner time.
| ssl-cert: Subject: commonName=giopis-PC
| Not valid before: 2023-04-17T09:45:33
|_Not valid after:  2023-10-17T09:45:33
| rdp-ntlm-info:
|   Target_Name: GIOPIS-PC
|   NetBIOS_Domain_Name: GIOPIS-PC
|   NetBIOS_Computer_Name: GIOPIS-PC
|   DNS_Domain_Name: giopis-PC
|   DNS_Computer_Name: giopis-PC
|   Product_Version: 6.1.7600
|_  System_Time: 2023-05-31T12:56:12+00:00
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008:
:sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 2 hops
Service Info: Host: GIOPIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: giopis-PC
|   NetBIOS computer name: GIOPIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-05-31T14:56:12+02:00
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
|_clock-skew: mean: -33m04s, deviation: 53m38s, median: -9m04s
| smb2-time:
|   date: 2023-05-31T12:56:12
|_  start_date: 2023-05-31T12:10:57
|_nbstat: NetBIOS name: GIOPIS-PC, NetBIOS user: <unknown>, NetBIOS MAC: 080027ee56bd (Oracle VirtualBox virtual NI
C)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 111/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.32.111
2   0.56 ms 192.168.42.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 31 09:06:14 2023 -- 2 IP addresses (2 hosts up) scanned in 220.60 seconds

┌──(kali㉿kali)-[~]
```