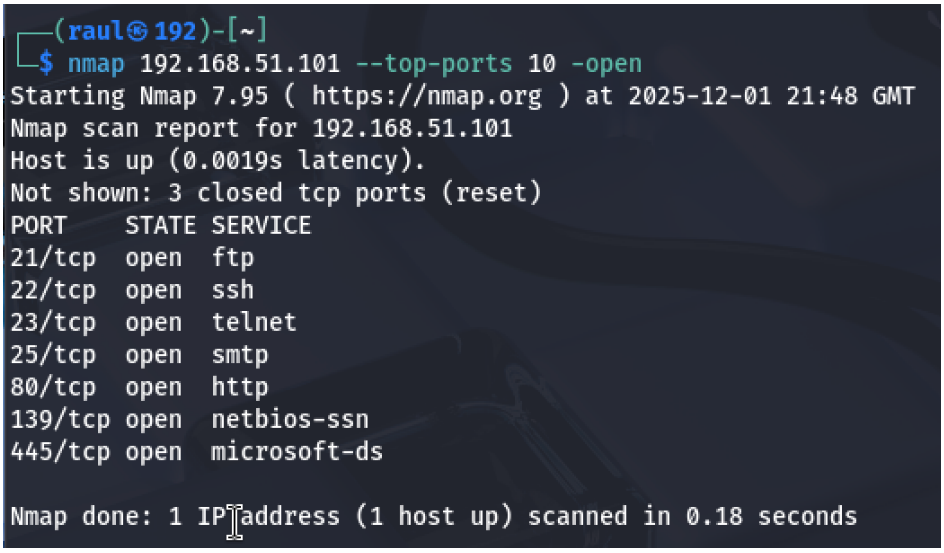
Raul Pastor

Comandi Linux

L’esercizio di oggi riguarda l’utilizzo di alcuni dei 15 comandi riguardante lo scan delle porte su un target (nel nostro caso sempre Meta), presi dalla pagina https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/.
In particolare ho utilizzato:

- nmap 192.168.51.101 -top-ports 10 -open



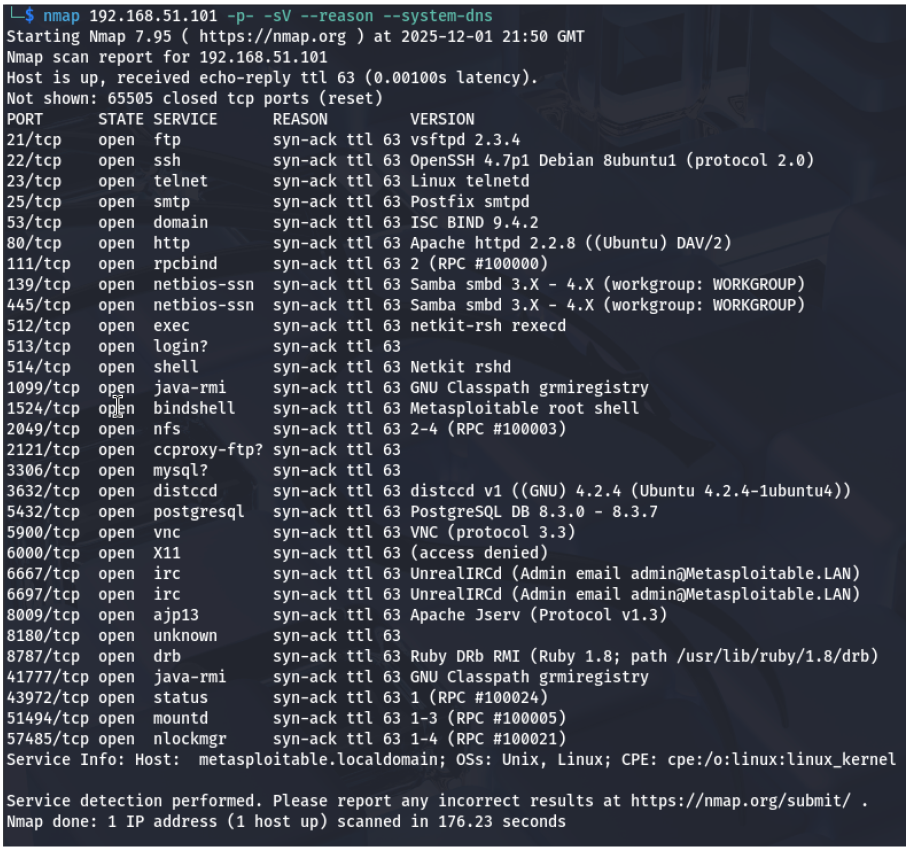
```
┌──(raul㉿192)-[~]
└─$ nmap 192.168.51.101 --top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 21:48 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0019s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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 0.18 seconds
```

Questo comando serve per trovare lo stato delle 10 porte piu utilizzate e il servizio su quella porta su un determinato target.

Raul Pastor

- nmap 192.168.51.101 -p- -sV –reason –system-dns

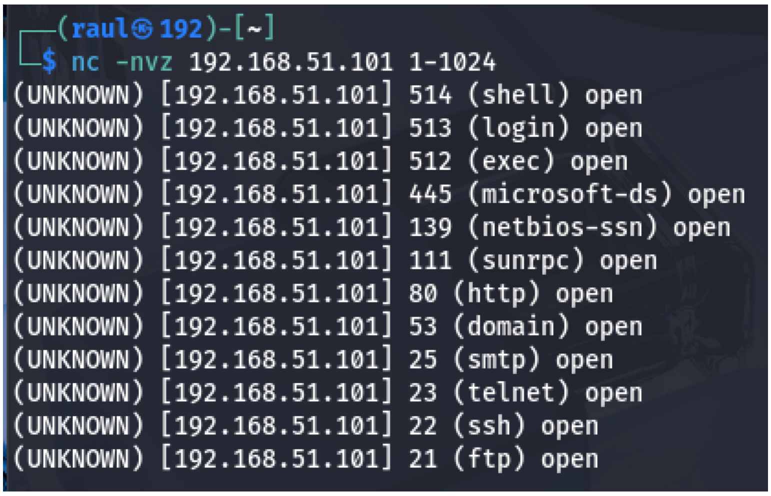


```
└─$ nmap 192.168.51.101 -p- -sV --reason --system-dns
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 21:50 GMT
Nmap scan report for 192.168.51.101
Host is up, received echo-reply ttl 63 (0.00100s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      REASON         VERSION
21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 63 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 63 Postfix smtpd
53/tcp    open  domain       syn-ack ttl 63 ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 63 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack ttl 63 2 (RPC #100000)
139/tcp   open  netbios-ssn  syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack ttl 63 netkit-rsh rexecd
513/tcp   open  login?       syn-ack ttl 63
514/tcp   open  shell        syn-ack ttl 63 Netkit rshd
1099/tcp  open  java-rmi     syn-ack ttl 63 GNU Classpath grmiregistry
1524/tcp  open  bindshell    syn-ack ttl 63 Metasploitable root shell
2049/tcp  open  nfs          syn-ack ttl 63 2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp? syn-ack ttl 63
3306/tcp  open  mysql?       syn-ack ttl 63
3632/tcp  open  distccd      syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack ttl 63 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 63 VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack ttl 63 (access denied)
6667/tcp  open  irc          syn-ack ttl 63 UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc          syn-ack ttl 63 UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13        syn-ack ttl 63 Apache Jserv (Protocol v1.3)
8180/tcp  open  unknown      syn-ack ttl 63
8787/tcp  open  drb          syn-ack ttl 63 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41777/tcp open  java-rmi     syn-ack ttl 63 GNU Classpath grmiregistry
43972/tcp open  status       syn-ack ttl 63 1 (RPC #100024)
51494/tcp open  mountd       syn-ack ttl 63 1-3 (RPC #100005)
57485/tcp open  nlockmgr     syn-ack ttl 63 1-4 (RPC #100021)
Service Info: Host:  metasploitable.localdomain; 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 176.23 seconds
```

Questo comando fa uno scan su un target e mostra lo stato di tutte le porte aperte oltre al servizio su quella porta, inoltre la ragione per cui quel servizio è in quello stato e la versione presente del servizio.

- nc -nvz 192.168.51.101 1-1024

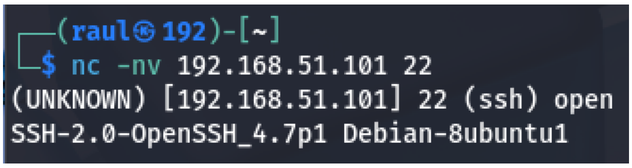


```
┌──(raul㉿192)-[~]
└─$ nc -nvz 192.168.51.101 1-1024
(UNKNOWN) [192.168.51.101] 514 (shell) open
(UNKNOWN) [192.168.51.101] 513 (login) open
(UNKNOWN) [192.168.51.101] 512 (exec) open
(UNKNOWN) [192.168.51.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.51.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.51.101] 111 (sunrpc) open
(UNKNOWN) [192.168.51.101] 80 (http) open
(UNKNOWN) [192.168.51.101] 53 (domain) open
(UNKNOWN) [192.168.51.101] 25 (smtp) open
(UNKNOWN) [192.168.51.101] 23 (telnet) open
(UNKNOWN) [192.168.51.101] 22 (ssh) open
(UNKNOWN) [192.168.51.101] 21 (ftp) open
```

Questo comando esegue uno scan delle prime 1024 porte su un target attraverso il comando netcat (abbreviato con nc) e l’opzione -nvz riportando il nome del servizio su quella porta e lo stato della porta.

Raul Pastor

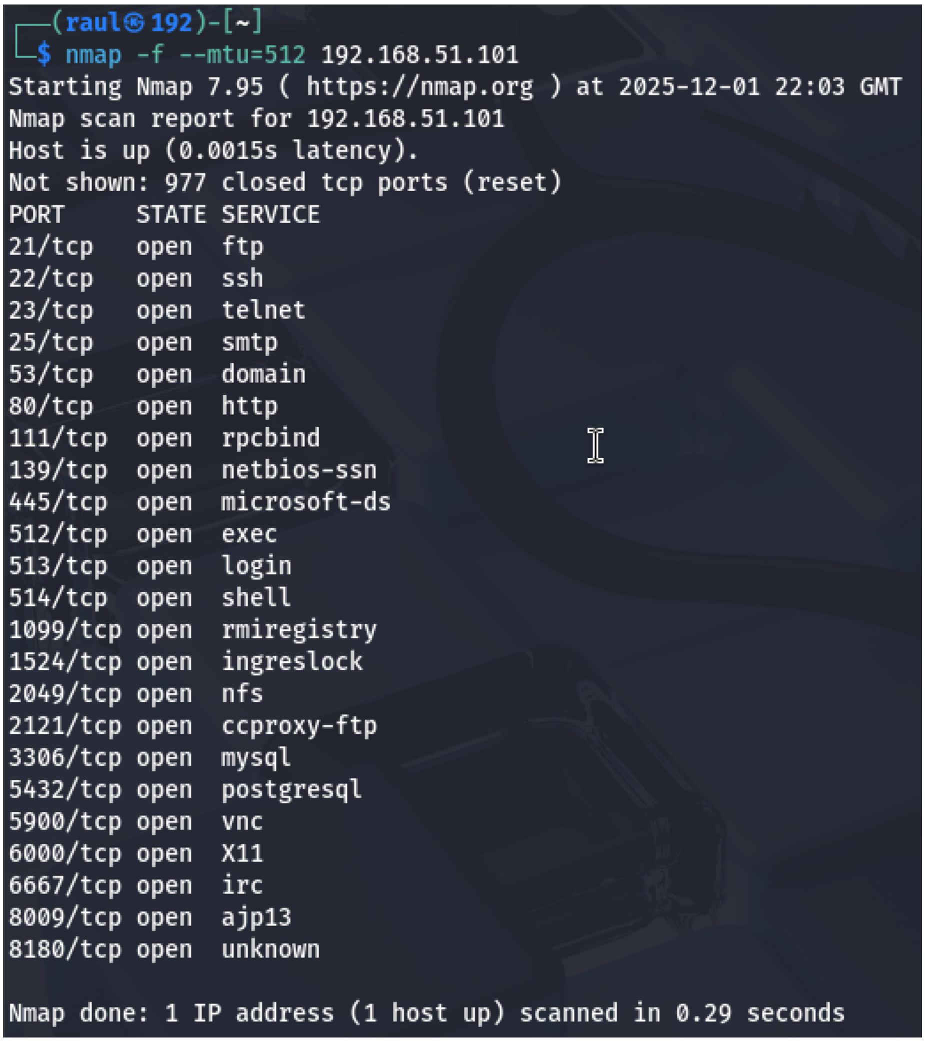
- nc -nv 192.168.51.101 22



```
┌──(raul㉿192)-[~]
└─$ nc -nv 192.168.51.101 22
(UNKNOWN) [192.168.51.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Questo comando esegue uno scan della porta 22 su un target attraverso il comando netcat (abbreviato con nc) e con l'opzione -nv per riportare informazioni sulla versione ssh.

- Nmap -f –mtu=512 192.168.51.101



```
┌──(raul㉿192)-[~]
└─$ nmap -f --mtu=512 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 22:03 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0015s 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 0.29 seconds
```

Questo comando viene spesso usato per eseguire scan delle porte bypassando le regole di firewall con l'opzione -f, frammentando i pacchetti in 512 parti cercando di eseguire le richieste "a pezzi".