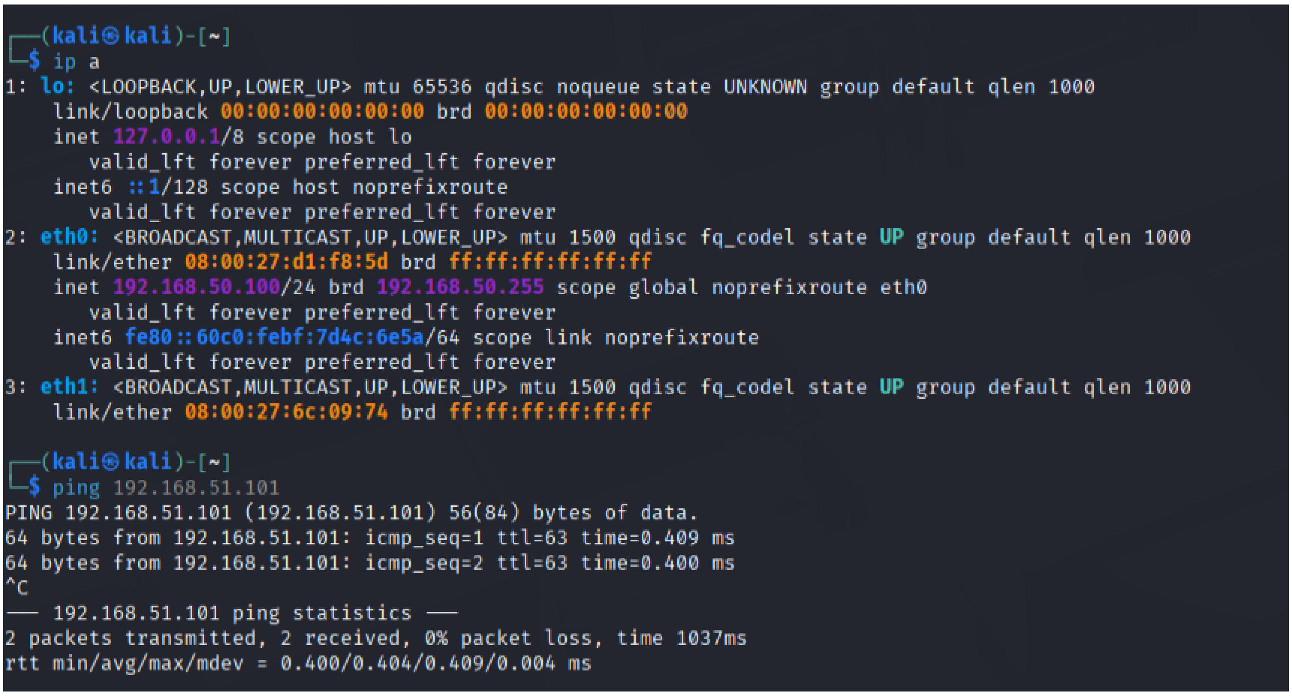
Report Tecnico – Analisi di Sicurezza su Rete Locale

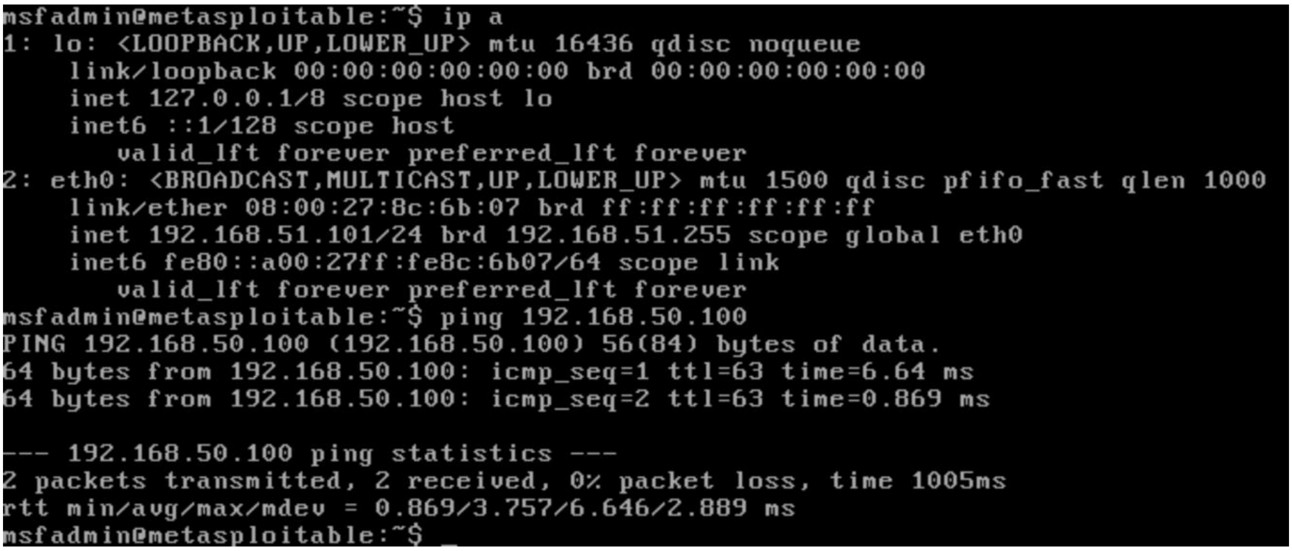
Ambiente di test:

- Macchina attaccante: Kali Linux (192.168.50.100)



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::60c0:febf:7d4c:6e5a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6c:09:74 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ ping 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=63 time=0.409 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=0.400 ms
^C
── 192.168.51.101 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1037ms
rtt min/avg/max/mdev = 0.400/0.404/0.409/0.004 ms
```

- Macchina bersaglio: Metasploitable (192.168.51.101)



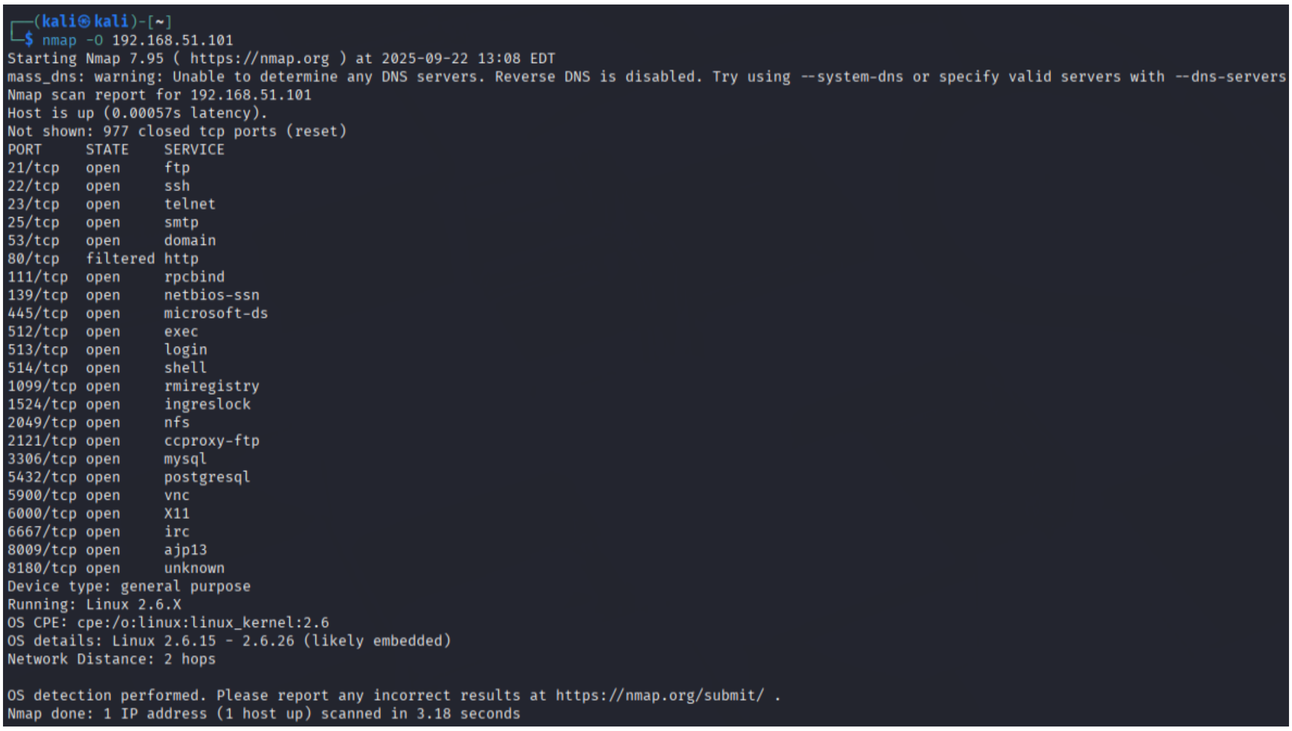
```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8c:6b:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
    inet6 fe80::a00:27ff:fe8c:6b07/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=6.64 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=0.869 ms

--- 192.168.50.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.869/3.757/6.646/2.889 ms
msfadmin@metasploitable:~$ _
```

- Obiettivo: Identificare i servizi esposti e valutare la superficie di attacco tramite scansioni Nmap

Verifica della Connettività

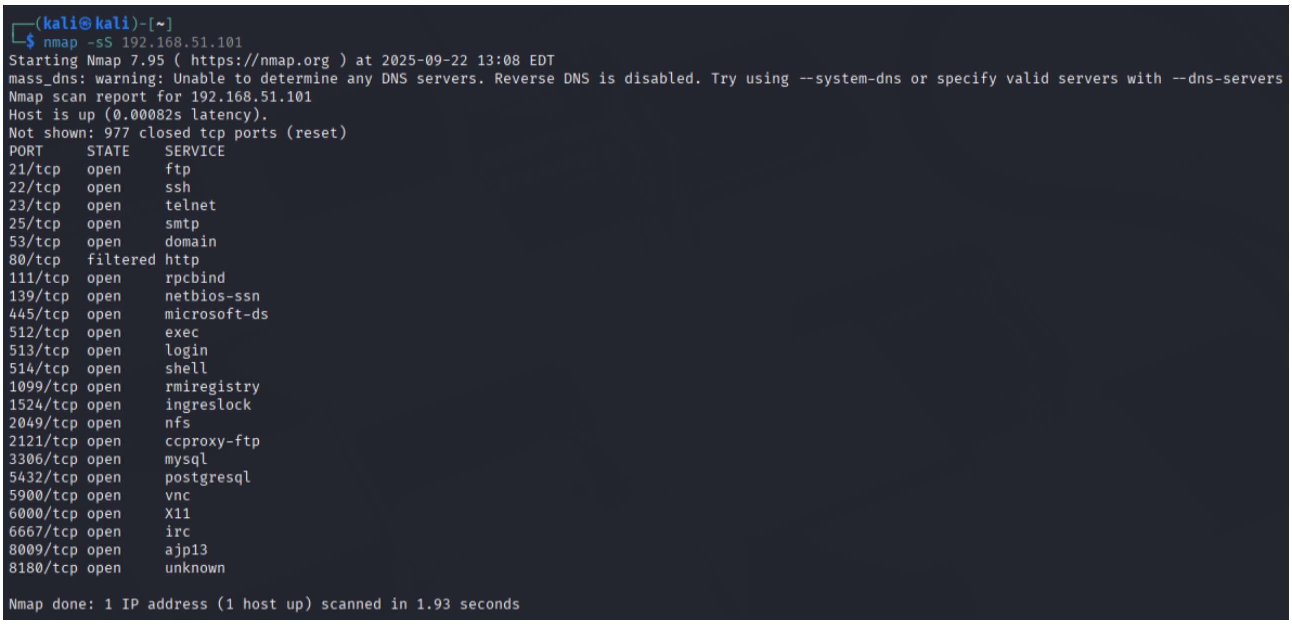
- Le due macchine si trovano su subnet diverse (192.168.50.0/24 e 192.168.51.0/24)
- Esecuzione di ping da Kali verso Metasploitable e viceversa: risposta positiva ambo i lati, connettività confermata tra i due host

Scansione Nmap -O: OS Detection, tenta di identificare il sistema operativo della macchina target analizzando le risposte ai pacchetti TCP/IP



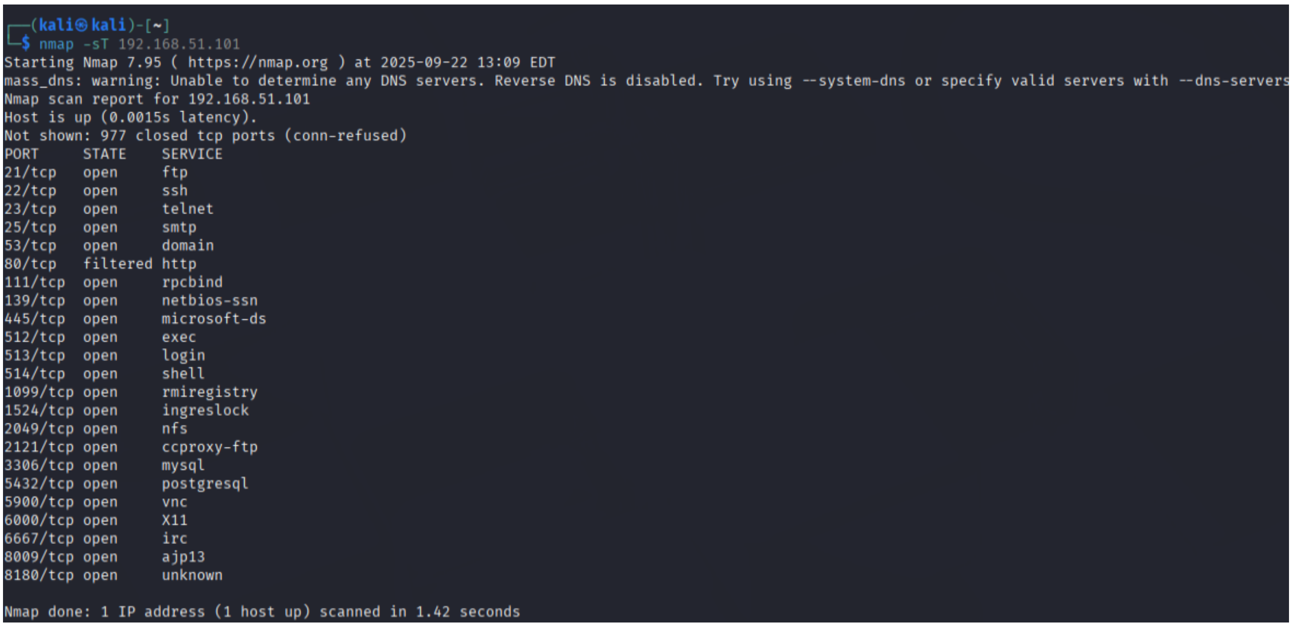
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 13:08 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.51.101
Host is up (0.00057s 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   filtered 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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

Scansione Nmap -sS: TCP SYN Scan, invia pacchetti SYN senza completare la connessione TCP. È veloce e discreto, spesso non rilevato dai sistemi di logging



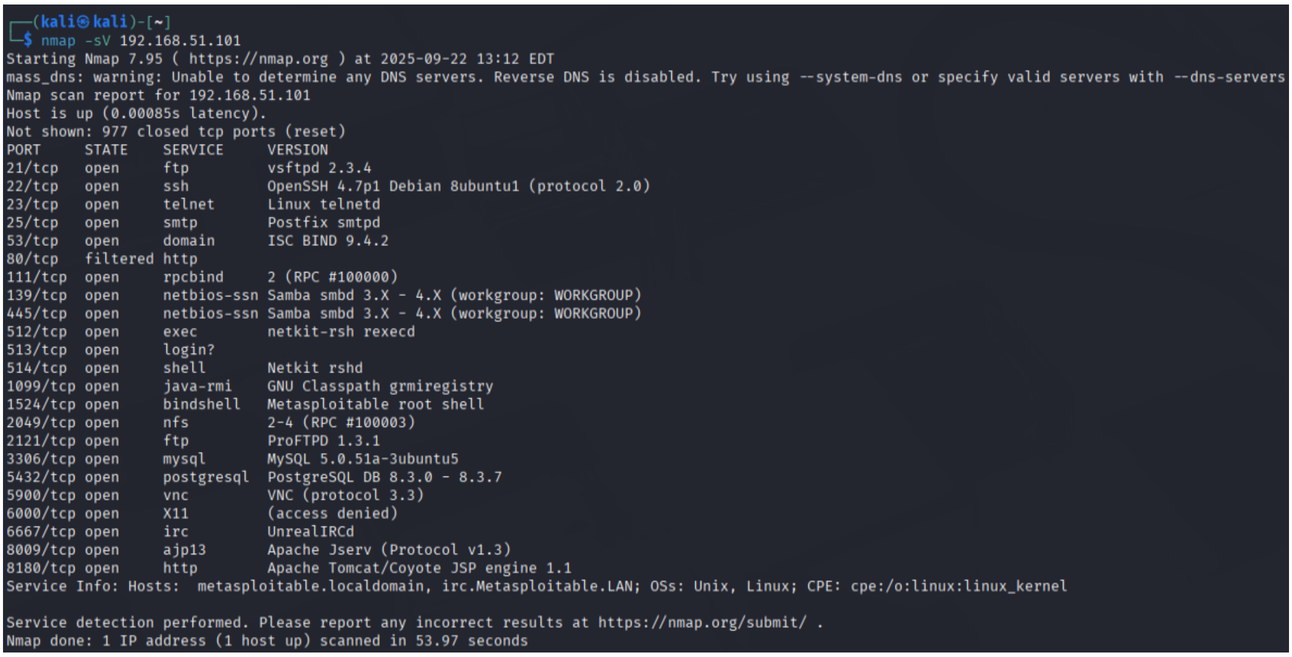
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 13:08 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.51.101
Host is up (0.00082s 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   filtered 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 1.93 seconds
```

Scansione Nmap -sT: TCP Connect Scan, effettua una connessione TCP completa (SYN, SYN-ACK, ACK). È più facile da rilevare ma funziona anche se non si hanno privilegi root.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 13:09 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 192.168.51.101
Host is up (0.0015s 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   filtered 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 1.42 seconds
```

Scansione Nmap -sV: Version Detection, identifica il software e la versione dei servizi in ascolto sulle porte aperte. Fondamentale per valutare vulnerabilità note.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 13:12 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 192.168.51.101
Host is up (0.00085s 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   filtered http
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     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
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 53.97 seconds
```

Scansione Nmap – Metasploitable (192.168.51.101)

Sistema operativo: Linux kernel 3.2 – 4.9

MAC Address 00:0C:29:2D:11:6A

Porte aperte: 31TCP

Distanza di rete: 1 hop

Servizi rilevati

- SSH (porta 22): OpenSSH 7.4p1 Debian – accesso remoto sicuro, da testare per brute-force e chiavi deboli
- SMTP (porta 25): Postfix smtpd – servizio email, verifica configurazione relay e autenticazione
- DNS (porta 53): dnsmasq 2.76 – DNS leggero, potenzialmente vulnerabile a cache poisoning
- HTTP (porta 80): Apache httpd 2.4.25 – web server, da analizzare per directory esposte e vulnerabilità note
- RPC (porta 111): rpcbind 2-4 – servizio RPC, possibile vettore di escalation locale
- NetBIOS (porta 139): Samba smbd 3.X–4.X – condivisione file, vulnerabile a enumerazione e attacchi SMB
- SMB (porta 445): Samba smbd 4.5.16 – noto per exploit come EternalBlue
- IPP (porta 631): CUPS 2.2 – servizio di stampa, da testare per accessi non autenticati
- MySQL (porta 3306): versione 5.5.60 – database relazionale, rischio di credenziali deboli e SQL injection
- PostgreSQL (porta 5432): versione 8.3.7 – database obsoleto, potenziale vulnerabilità
- ProFtpd (porta 8000): versione 1.3.5 – server FTP, da testare per accesso anonimo e directory traversal
- Apache HTTP (porte 8080 e 8888): versione 2.4.25 – web server su porte non standard, spesso usato per ambienti di test o interfacce di gestione

Descrizione dei servizi

La macchina espone servizi critici e obsoleti, tra cui:

Database vulnerabili (MySQL 5.5, PostgreSQL 8.3)

Web server su porte non convenzionali (8000, 8080, 8888)

Servizi SMB e NetBIOS noti per exploit come EternalBlue

RPC e CUPS potenzialmente sfruttabili per escalation locale