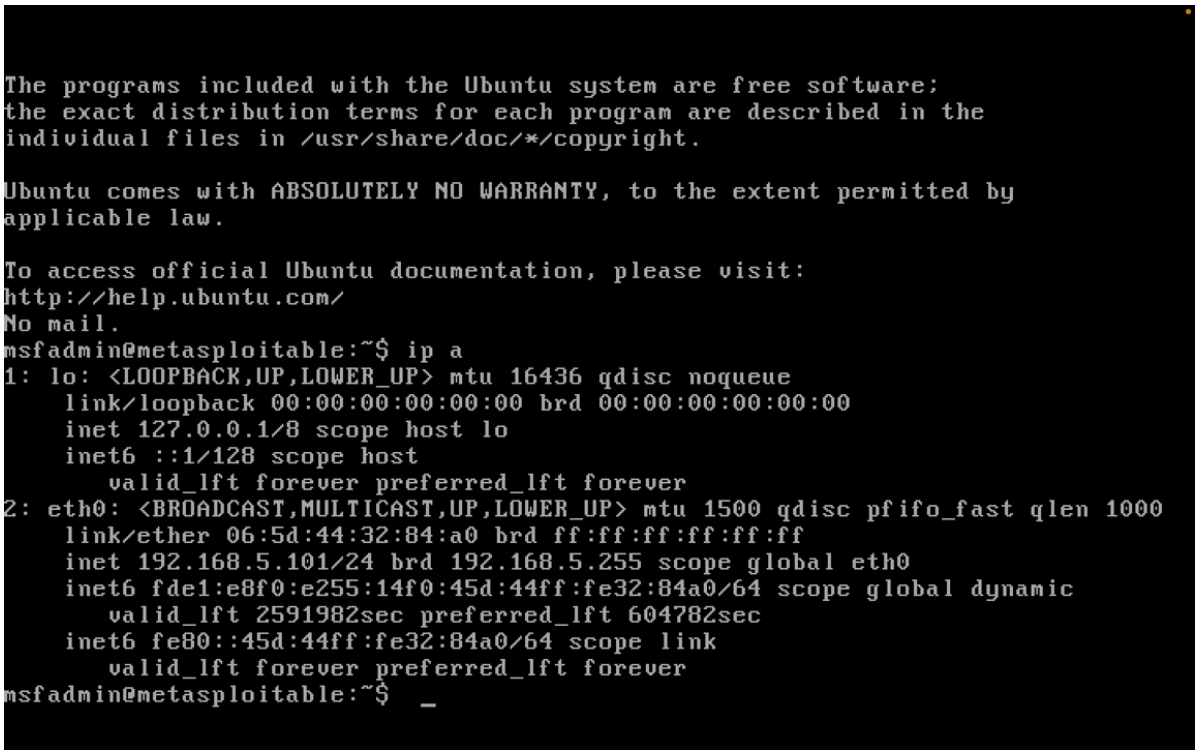
S5/L3

NMAP

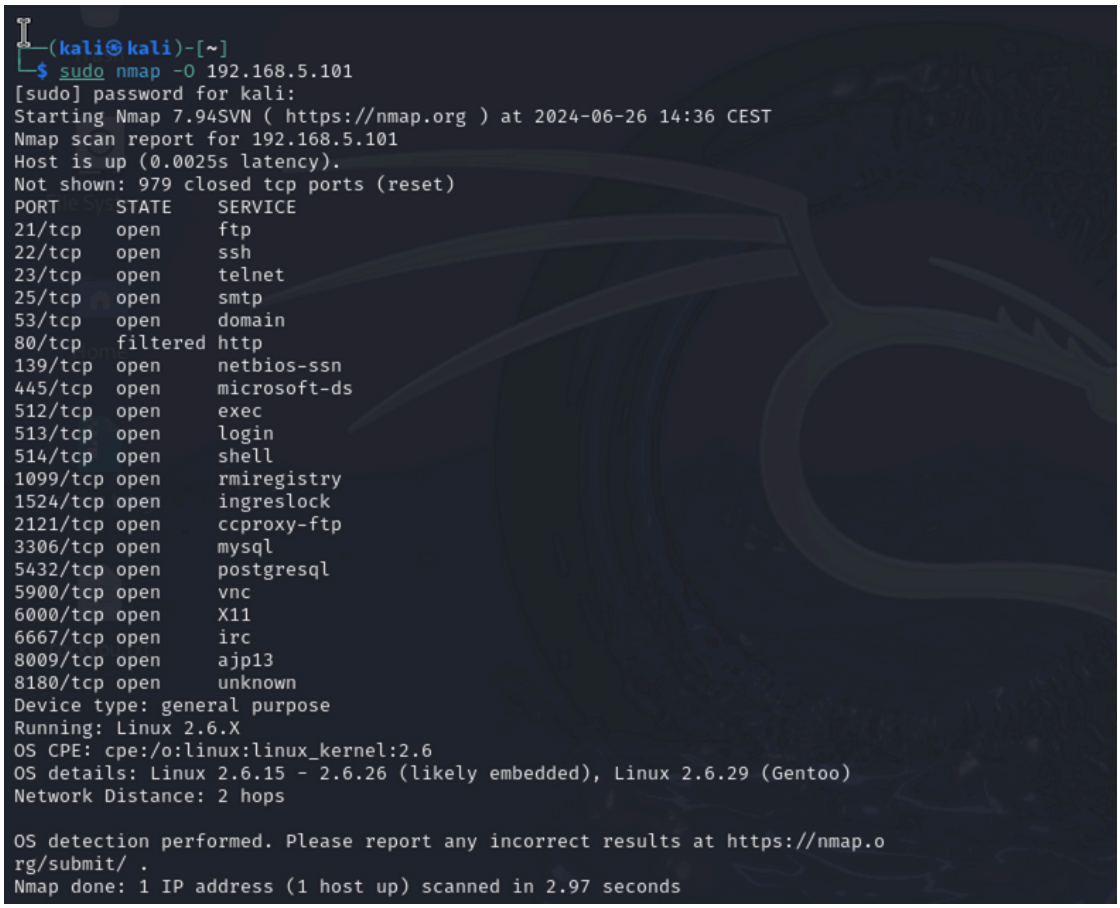
INTRODUZIONE

In questo report si illustra l’utilizzo del tool di NMAP per scan di vario tipo.

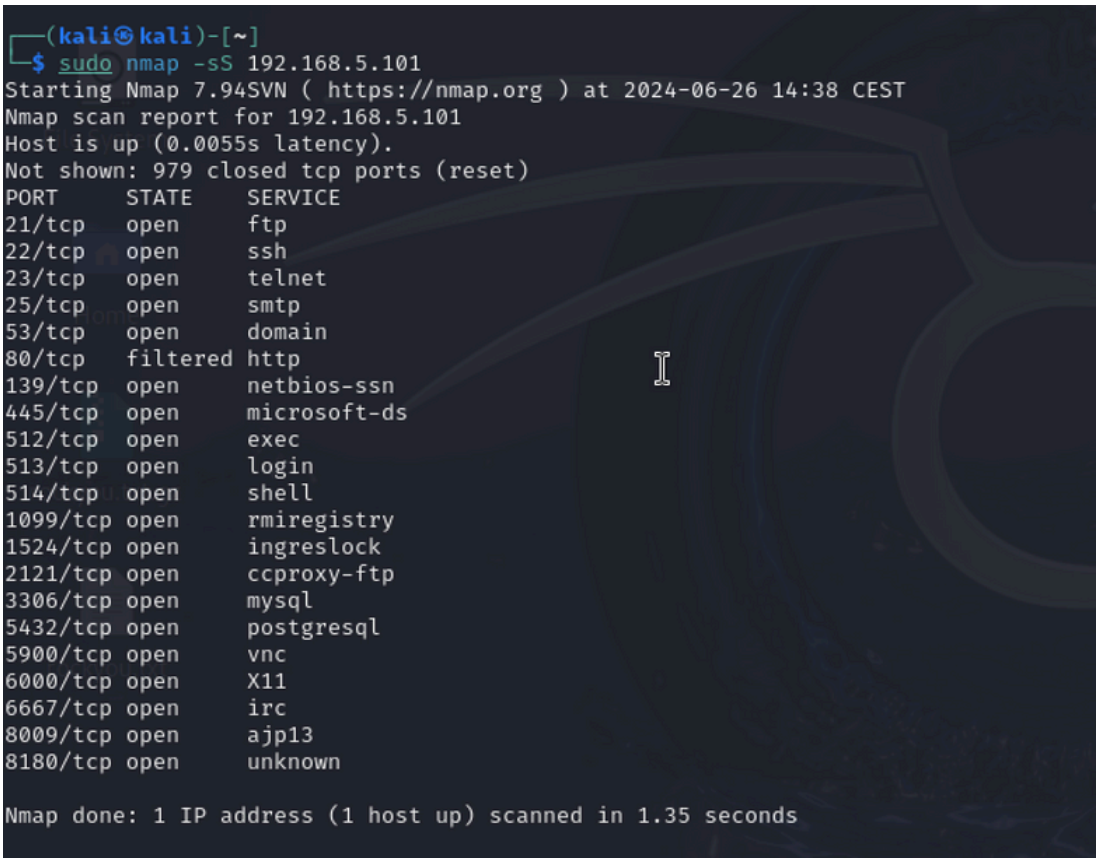
Configurazione METASLOITABLE



OS fingerprinting - Meta



SYN SCAN - META



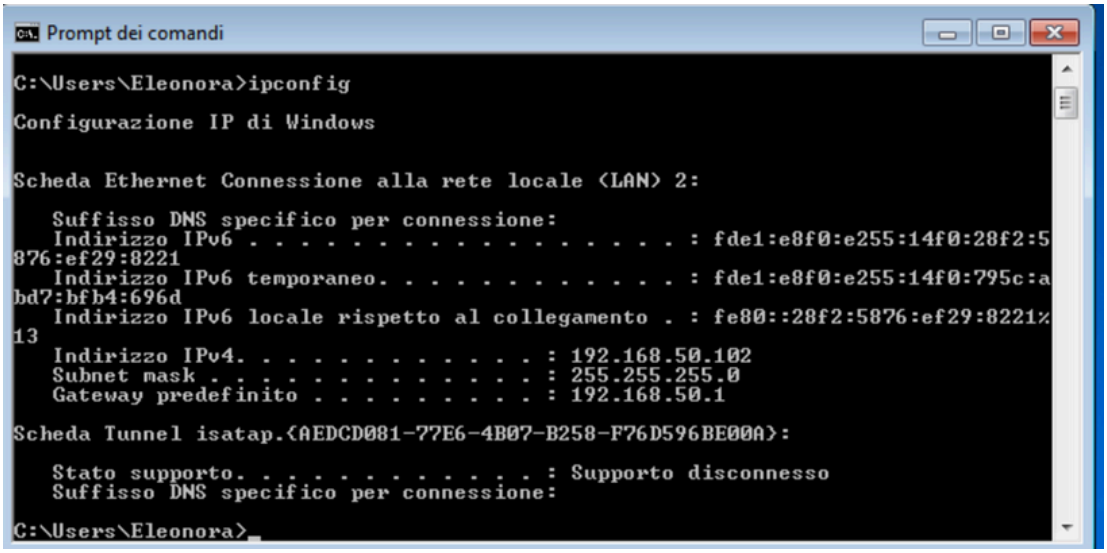
TCP connect - Metasploitable

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:45 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0045s latency).
Not shown: 979 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
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
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 1.30 seconds
```

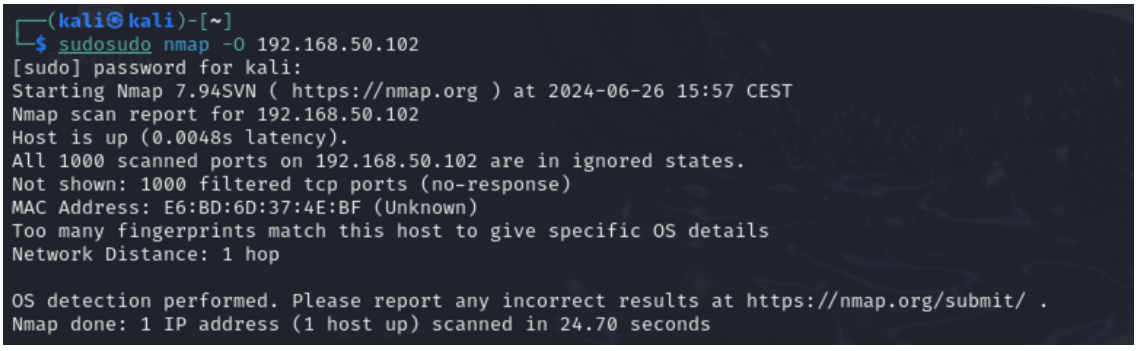
VERSION DETECTION

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:48 CEST
Nmap scan report for 192.168.5.101
Host is up (0.0073s latency).
Not shown: 979 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
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       OpenBSD or Solaris rlogind
514/tcp  open     tcpwrapped
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp open     bindshell   Metasploitable root shell
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds
```

CONFIGURAZIONE WINDOWS 7



OS FINGERPRINTING FIREWALL ATTIVO



FIREWALL SPENTO