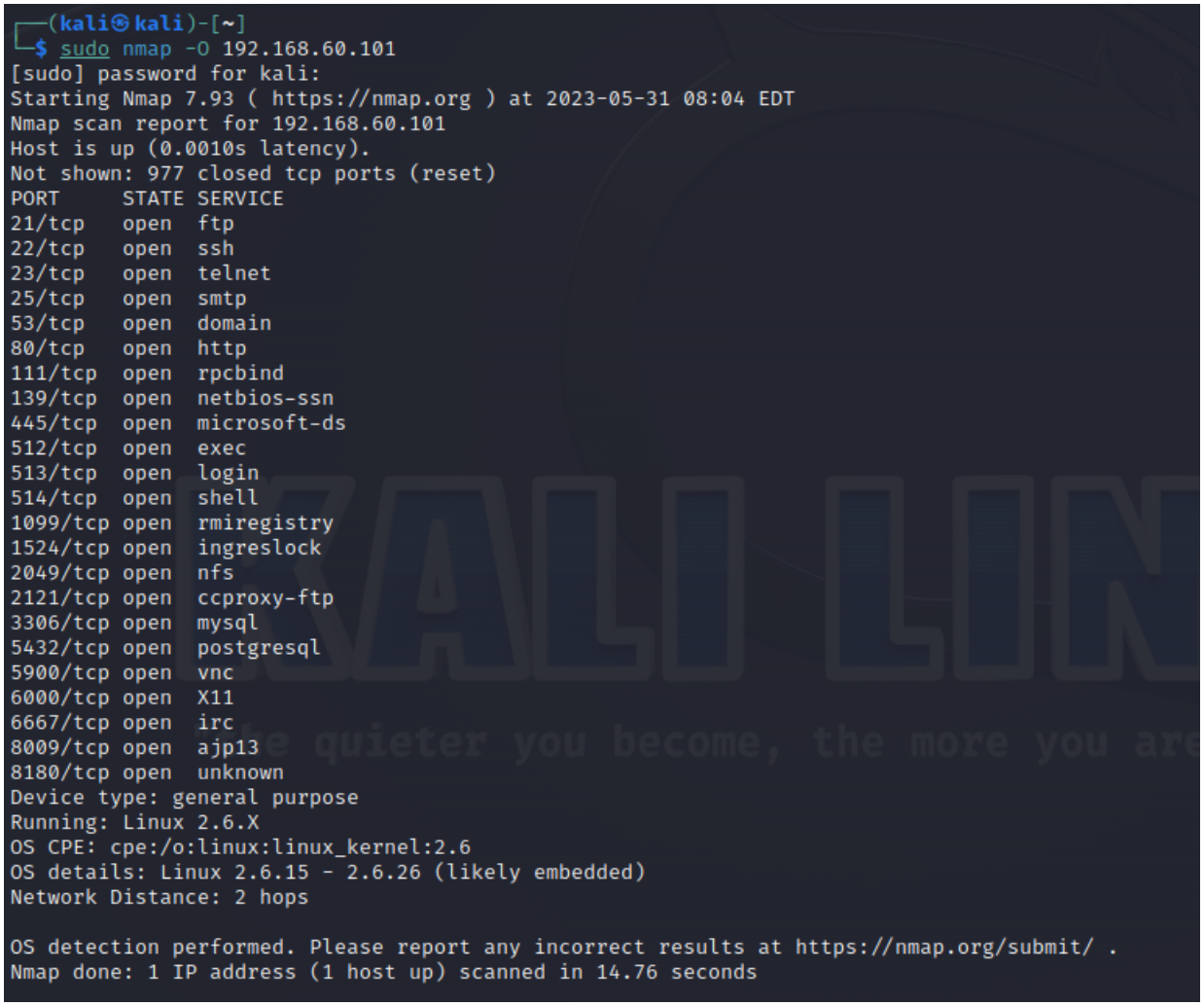
TECNICHE DI SCANSIONE CON NMAP

METASPOITTABLE

OS fingerprint



Da qua capisco le tcp porte aperte

Che ci sono 2 host ed è una machina linux

Per cui disabilito l’ost discovery ma il risultato è identico

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.60.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:23 EDT
Nmap scan report for 192.168.60.101
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
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 15.71 seconds
```

Syn scan per rimanere nascosti

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.60.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:26 EDT
Nmap scan report for 192.168.60.101
Host is up (0.00059s 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  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 65.55 seconds
```

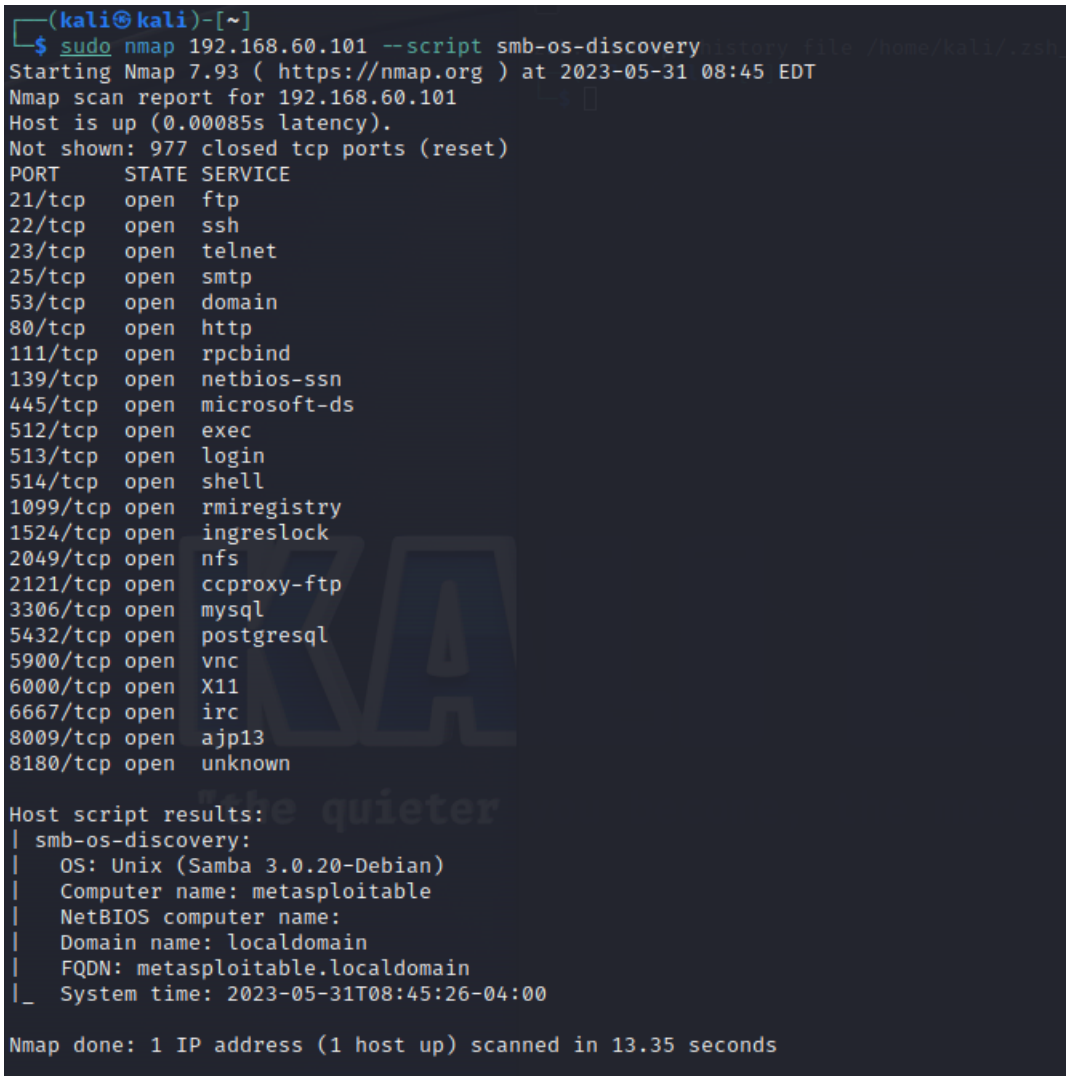
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sT 192.168.60.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:29 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql?
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 186.17 seconds
```

Noto che in modalita stelt la porta 973 è in restart

Per trovare l'hots

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sO 192.168.60.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:37 EDT
Stats: 0:03:31 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 08:40 (0:00:00 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 99.99% done; ETC: 08:40 (0:00:00 remaining)
Nmap scan report for 192.168.60.101
Host is up (0.00097s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open|filtered tcp
17       open          udp
58       open|filtered ipv6-icmp
136      open|filtered udplite

Nmap done: 1 IP address (1 host up) scanned in 290.09 seconds
```

Per trovare il sistema operativo



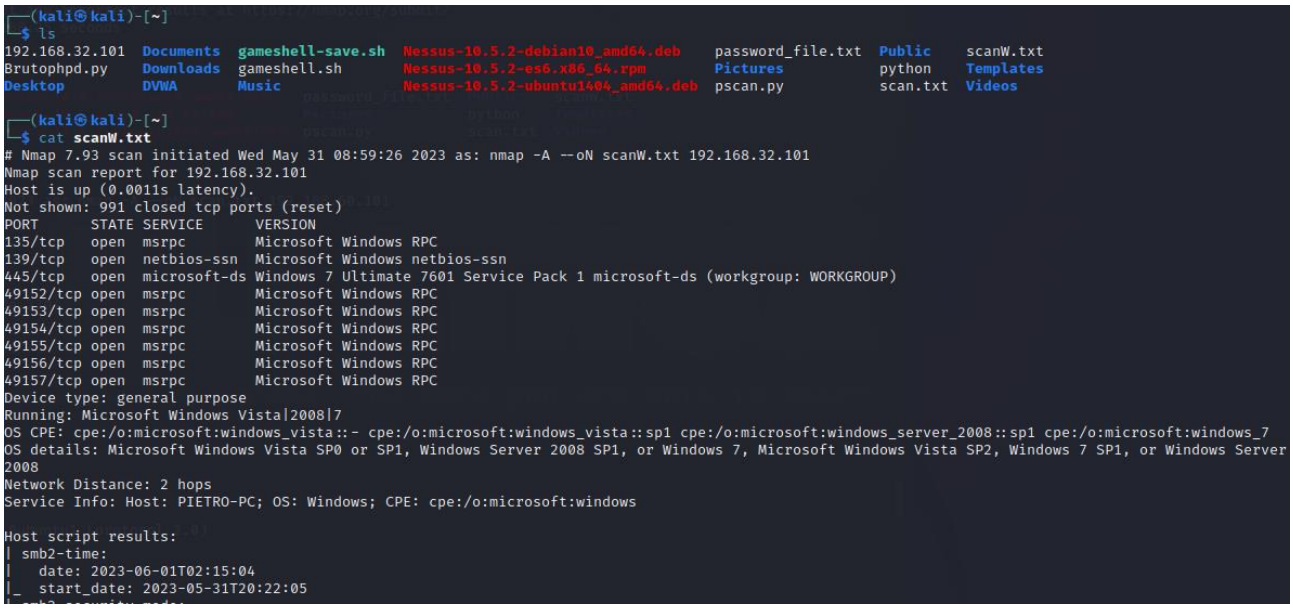
Nmap report

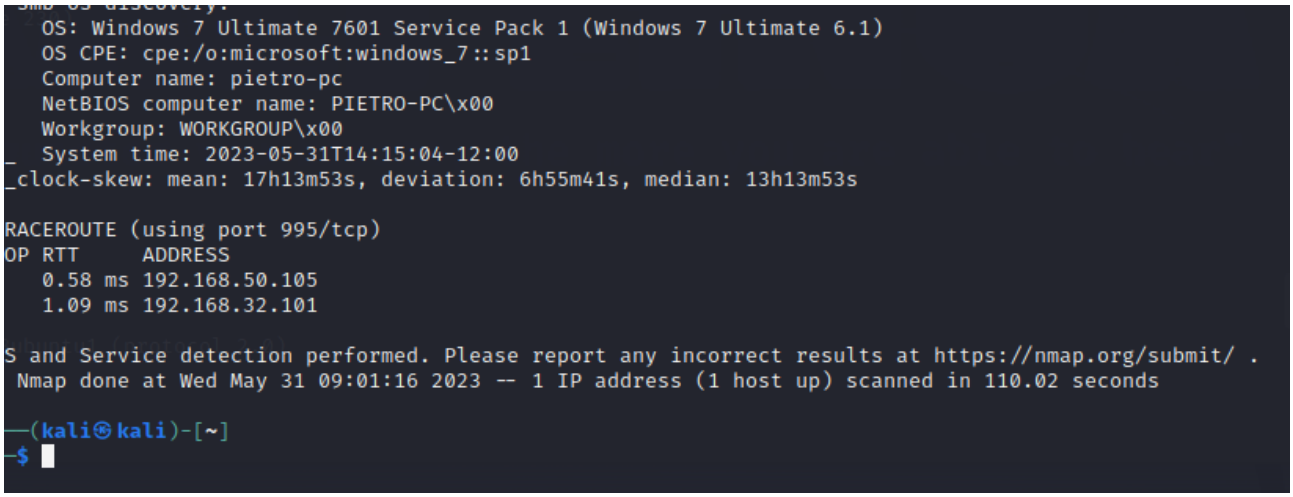
Metaspit

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.60.101 --oN scan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:57 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0011s 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      33072/tcp   mountd
|   100005  1,2,3      53321/udp   mountd
```

```
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   0.55 ms 192.168.50.105
2   1.08 ms 192.168.60.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 168.25 seconds

┌──(kali㉿kali)-[~]
└─$ ls
192.168.32.101  Documents  gameshell-save.sh  Nessus-10.5.2-debian10_amd64.deb    password_file.txt  Public     scanW.txt
Brutophpd.py    Downloads  gameshell.sh       Nessus-10.5.2-es6.x86_64.rpm       Pictures           python     Templates
Desktop         DVWA       Music              Nessus-10.5.2-ubuntu1404_amd64.deb  pscan.py           scan.txt   Videos

┌──(kali㉿kali)-[~]
└─$ cat scan.txt
# Nmap 7.93 scan initiated Wed May 31 08:57:21 2023 as: nmap -A --oN scan.txt 192.168.60.101
Nmap scan report for 192.168.60.101
Host is up (0.0011s 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
```

Windows





Windows

1. IP: L'indirizzo IP del dispositivo scansionato è 192.168.32.101.
2. Porte TCP aperte:

- Porta 135: msrpc (Microsoft Windows RPC)
- Porta 139: netbios-ssn (Microsoft Windows netbios-ssn)
- Porta 445: microsoft-ds (Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds)
- Porte 49152-49157: msrpc (Microsoft Windows RPC)
- Modalità di sicurezza SMB: Viene utilizzato l'account "guest", il livello di autenticazione è "user", il challenge-response è supportato e la firma dei messaggi è disabilitata (impostazione predefinita ma pericolosa).
- SMB2 time: La data è il 1° giugno 2023 alle 02:25:31 e l'orario di inizio è il 31 maggio 2023 alle 20:22:05.
- Modalità di sicurezza SMB2: La firma dei messaggi è abilitata ma non richiesta.

- Rilevamento SMB OS: L'host sta eseguendo Windows 7 Ultimate 7601 Service Pack 1, con il nome del computer "pietro-pc", il nome del computer NetBIOS "PIETRO-PC" e appartiene al gruppo di lavoro "WORKGROUP".
- Ora di sistema: L'ora di sistema è il 31 maggio 2023 alle 14:25:31.

Risultati del traceroute:

- HOP 1: Tempo di andata e ritorno (RTT) di 0,23 millisecondi per l'indirizzo 192.168.50.105.
- HOP 2: Tempo di andata e ritorno (RTT) di 0,45 millisecondi per il dispositivo scansionato all'indirizzo 192.168.32.101.

Metaspoit

1. FTP (vsftpd 2.3.4): La porta 21 è aperta e il servizio FTP è in esecuzione. La versione del server FTP è vsftpd 2.3.4. Inoltre, è consentito l'accesso FTP anonimo (FTP code 230).
2. SSH (OpenSSH 4.7p1 Debian 8ubuntu1): La porta 22 è aperta e il servizio SSH è in esecuzione. La versione del server SSH è OpenSSH 4.7p1 Debian 8ubuntu1 e il protocollo supportato è il 2.0.
3. Telnet (Linux telnetd): La porta 23 è aperta e il servizio Telnet è in esecuzione. Si tratta di un demone Telnet per Linux.
4. SMTP (Postfix smtpd): La porta 25 è aperta e il servizio SMTP è in esecuzione. Il server SMTP è Postfix smtpd.
5. DNS (ISC BIND 9.4.2): La porta 53 è aperta e il servizio DNS è in esecuzione. Il server DNS è ISC BIND 9.4.2.
6. HTTP (Apache httpd 2.2.8): La porta 80 è aperta e il servizio HTTP è in esecuzione. Il server HTTP è Apache httpd 2.2.8 su un sistema operativo Ubuntu. La pagina di benvenuto mostra "Metasploitable2 - Linux" come titolo.
7. RPCbind (RPC #100000): La porta 111 è aperta e il servizio RPCbind è in esecuzione. È un servizio di registrazione e mappatura dei protocolli di remote procedure call (RPC).
8. Samba (Samba smbd 3.X - 4.X): Le porte 139 e 445 sono aperte e il servizio Samba è in esecuzione. Si tratta di un'implementazione open source del protocollo SMB/CIFS per la condivisione di file e stampanti tra sistemi Windows e Unix.
9. MySQL (MySQL 5.0.51a-3ubuntu5): La porta 3306 è aperta e il servizio MySQL è in esecuzione. La versione del database MySQL è 5.0.51a-3ubuntu5.
10. PostgreSQL (PostgreSQL DB 8.3.0 - 8.3.7): La porta 5432 è aperta e il servizio PostgreSQL è in esecuzione. La versione del database PostgreSQL è compresa tra la 8.3.0 e la 8.3.7.

clock-skew: Il risultato mostra la discrepanza di orario tra il tuo sistema e l'host scansionato. La media è di 1 ora, 19 minuti e 59 secondi, con una deviazione di 2 ore e 18 minuti.

smb-os-discovery: Questo script ha rilevato che il sistema operativo dell'host è Unix, con Samba 3.0.20-Debian installato. Il nome del computer è "metasploitable", il nome NetBIOS è vuoto, il dominio è

"localdomain", e l'FQDN (Fully Qualified Domain Name) è "metasploitable.localdomain". L'orario di sistema dell'host è impostato al 2023-05-31T09:10:31-04:00.

nbstat: Questo script ha rilevato il nome NetBIOS dell'host come "METASPLOITABLE" e l'indirizzo MAC associato è "000000000000" (Xerox).

smb-security-mode: Questo script mostra alcune informazioni sulla modalità di sicurezza SMB (Server Message Block) del sistema. Non è specificato l'account utilizzato, il livello di autenticazione è "user", la risposta alla sfida è supportata e la firma dei messaggi è disabilitata (pericolosa, ma predefinita). Inoltre, la negoziazione del protocollo SMB2 non è riuscita.

Si tratta di informazioni rilevate dagli script specifici di Nmap, che forniscono dettagli aggiuntivi sullo stato del sistema e delle connessioni di rete dell'host scansionato.