Report Host Scanning

Il target dell'attività è variabile, infrastruttura composta da 2 LAN. Tutte le scansioni sono state effettuate da Kali nella subnet 50.0/24, la seconda subnet è su 51.0/24 in cui è presente l'host Metaslpoitable, entrambe le LAN hanno regole firewall *Pass* reciproche verso entrambe.

1. ***nmap -sn -PE 192.168.51.101*** (Metasploitable)
   Ha la stessa funzionalità del comando *ping*.
   -sn → no port scanning
   -PE → ping echo request

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:08 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.51.101
Host is up (0.0035s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

2. ***netdiscover -r 192.168.50.0*** (LAN1)
   esegue una scansione attiva della rete locale, inviando richieste ARP per ogni possibile IP nel range specificato.
   -r → specifica il range di indirizzi ip

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

255 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 15300

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.50.1    08:00:27:85:76:9b    255   15300  PCS Systemtechnik GmbH
```

3. ***nmap --top-ports 10 --open 192.168.51.101***
   controlla solo le 10 porte statisticamente più usate al mondo, mostrando solo le open

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --top-ports 10 --open 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:48 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.51.101
Host is up (0.0078s 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 13.19 seconds
```

4. ***nmap 192.168.51.101 -sV –reason***

scansiona le porte, riporta in output le open con versione del service e ragione per cui sono state decretate open (riporta le response delle request)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.51.101 -sV --reason
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:55 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.51.101
Host is up, received echo-reply ttl 63 (0.029s latency).
Not shown: 977 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
25/tcp   open  smtp?        syn-ack ttl 63
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
513/tcp  open  login?       syn-ack ttl 63
514/tcp  open  shell?       syn-ack ttl 63
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
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
8009/tcp open  ajp13        syn-ack ttl 63 Apache Jserv (Protocol v1.3)
8180/tcp open  unknown      syn-ack ttl 63
Service Info: Host: 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 195.76 seconds
```

5. ***us -mT -lv 192.168.51.101:a -r 3000 -R 3 && us -mU -lv 192.168.51.101:a -r 3000 -R 3***

unione di due comandi (con operatore logico &&→AND)

us → UnicornScan, effettua scansioni asincrone, a differenza di nmap non aspetta che le request abbiano una risposta, lui manda numerose request e ha un thread separato che ascolta le risposte.

-mT / -mU → scan ports TCP / scan ports UDP

-lv → Immediate Verbose, mostra i risultati non appena vengono trovati fornendo dettagli aggiuntivi nell'output

<IP>:a → All ports (da 0 a 65535), l'equivalente di -p- di nmap

-r 3000 → Imposta la velocità a 3000 pacchetti al secondo

-R 3 → ogni pacchetto lo invia 3 volte, aumenta la certezza di trovare porte aperte, con la scansione UDP è meglio data la possibile perdita di pacchetti in UDP

```
┌──(root㉿kali)-[/home/kali]
└─# us -mT -Iv 192.168.51.101:a -r 3000 -R 3 && us -mU -Iv 192.168.51.101:a -r 3000 -R 3
adding 192.168.51.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.51.101:8180  ttl 63
TCP open 192.168.51.101:36343  ttl 63
TCP open 192.168.51.101:2049  ttl 63
TCP open 192.168.51.101:6000  ttl 63
TCP open 192.168.51.101:5900  ttl 63
TCP open 192.168.51.101:1099  ttl 63
TCP open 192.168.51.101:6667  ttl 63
TCP open 192.168.51.101:23  ttl 63
TCP open 192.168.51.101:8787  ttl 63
TCP open 192.168.51.101:53  ttl 63
TCP open 192.168.51.101:40845  ttl 63
TCP open 192.168.51.101:22  ttl 63
TCP open 192.168.51.101:5432  ttl 63
TCP open 192.168.51.101:2121  ttl 63
TCP open 192.168.51.101:514  ttl 63
TCP open 192.168.51.101:3632  ttl 63
TCP open 192.168.51.101:111  ttl 63
TCP open 192.168.51.101:445  ttl 63
TCP open 192.168.51.101:40766  ttl 63
TCP open 192.168.51.101:21  ttl 63
TCP open 192.168.51.101:53221  ttl 63
TCP open 192.168.51.101:25  ttl 63
TCP open 192.168.51.101:3306  ttl 63
TCP open 192.168.51.101:139  ttl 63
TCP open 192.168.51.101:6697  ttl 63
TCP open 192.168.51.101:80  ttl 63
TCP open 192.168.51.101:512  ttl 63
TCP open 192.168.51.101:1524  ttl 63
TCP open 192.168.51.101:513  ttl 63
TCP open 192.168.51.101:8009  ttl 63
sender statistics 1572.8 pps with 196608 packets sent total
listener statistics 162017 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.51.101  ttl 63
TCP open                     ssh[   22]         from 192.168.51.101  ttl 63
TCP open                  telnet[   23]         from 192.168.51.101  ttl 63
TCP open                    smtp[   25]         from 192.168.51.101  ttl 63
TCP open                  domain[   53]         from 192.168.51.101  ttl 63
TCP open                    http[   80]         from 192.168.51.101  ttl 63
TCP open                  sunrpc[  111]         from 192.168.51.101  ttl 63
TCP open             netbios-ssn[  139]         from 192.168.51.101  ttl 63
TCP open            microsoft-ds[  445]         from 192.168.51.101  ttl 63
TCP open                    exec[  512]         from 192.168.51.101  ttl 63
TCP open                   login[  513]         from 192.168.51.101  ttl 63
TCP open                   shell[  514]         from 192.168.51.101  ttl 63
TCP open             rmiregistry[ 1099]         from 192.168.51.101  ttl 63
TCP open              ingreslock[ 1524]         from 192.168.51.101  ttl 63
TCP open                   shilp[ 2049]         from 192.168.51.101  ttl 63
TCP open           scientia-ssdb[ 2121]         from 192.168.51.101  ttl 63
TCP open                   mysql[ 3306]         from 192.168.51.101  ttl 63
TCP open                  distcc[ 3632]         from 192.168.51.101  ttl 63
TCP open              postgresql[ 5432]         from 192.168.51.101  ttl 63
TCP open                  winvnc[ 5900]         from 192.168.51.101  ttl 63
TCP open                     x11[ 6000]         from 192.168.51.101  ttl 63
TCP open                     irc[ 6667]         from 192.168.51.101  ttl 63
TCP open                 unknown[ 6697]         from 192.168.51.101  ttl 63
TCP open                 unknown[ 8009]         from 192.168.51.101  ttl 63
TCP open                 unknown[ 8180]         from 192.168.51.101  ttl 63
TCP open                 msgsrvr[ 8787]         from 192.168.51.101  ttl 63
TCP open                 unknown[36343]         from 192.168.51.101  ttl 63
TCP open                 unknown[40766]         from 192.168.51.101  ttl 63
TCP open                 unknown[40845]         from 192.168.51.101  ttl 63
TCP open                 unknown[53221]         from 192.168.51.101  ttl 63
adding 192.168.51.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
UDP open 192.168.51.101:2049  ttl 63
UDP open 192.168.51.101:57411  ttl 63
UDP open 192.168.51.101:137  ttl 63
sender statistics 2845.3 pps with 196635 packets sent total
listener statistics 4 packets recieved 0 packets droped and 0 interface drops
UDP open              netbios-ns[  137]         from 192.168.51.101  ttl 63
UDP open                   shilp[ 2049]         from 192.168.51.101  ttl 63
UDP open                 unknown[57411]         from 192.168.51.101  ttl 63
```

6. *nmap -sS -sV -T4 192.168.51.101*

esegue una scansione stealth, mostrando le versioni dei service, riducendo il tempo di attesa

-sS → scan SYN, non completa il 3-way-handshake, rendendo la scansione più stealth

-sV → stampa le service versions

-T4 → dice ad nmap di aspettare 1.25s per ogni request e le esegue in parallelo, ha 6 livelli (da T0 a T5, il default è T3) ognuno varia la RTT Timeout

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 12:30 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.51.101
Host is up (0.027s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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?
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  unknown
Service Info: Host: 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 195.15 seconds
```

7. *nmap --script=ftp-anon 192.168.51.101*

oltre a scansionare le porte interagisce con il servizio **FTP** (Porta 21) e verifica se è configurato per accettare connessioni anonime.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=ftp-anon 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 14:37 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.51.101
Host is up (0.088s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
23/tcp   open  telnet
```

8. ***nmap --script=smb-enum-shares 192.168.51.101***

   oltre a scansionare le porte interroga il servizio **SMB** (Server Message Block, porte 445/139) per ottenere la lista delle Shares disponibili sul target, con i relativi permessi.

```
Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.51.101\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.51.101\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.51.101\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.51.101\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.51.101\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 24.16 seconds
```

9. ***nmap --script=smb-enum-users 192.168.51.101***

   oltre a scansionare le porte interroga il servizio **SMB** (Server Message Block, porte 445/139) per ottenere un elenco di tutti gli utenti definiti sulla macchina target.

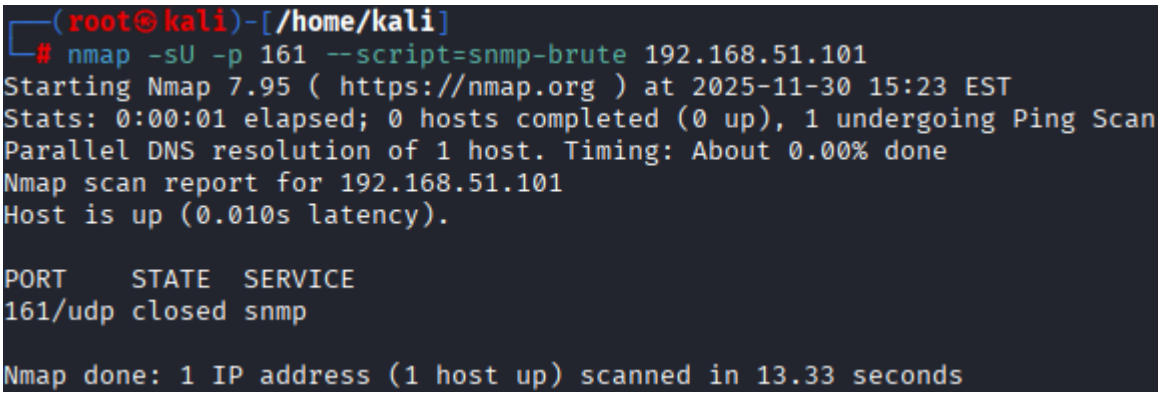
```
Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Account disabled, Normal user account
```

```
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Account disabled, Normal user account
```

10. *nmap --script=snmp-brute 192.168.51.101*

Questo script esegue una scansione UDP sulla porta 161 in modo da effettuare un attacco di **Brute-Force** contro il servizio **SNMP** (porta 161) per trovare la parola chiave, se si trovasse si potrebbe leggere (talvolta modificare) ogni dettaglio della configurazione del server.

--script=snmp-brute → utilizza un file interno di Nmap (nmap.lst o liste specifiche) contenente le Community String più comuni al mondo.



Nel caso riportato in figura la porta 161 è closed perciò lo script non è entrato in funzione.

Riepilogo delle vulnerabilità:

Oltre alle numerose porte open scansionate si possono distinguere diverse gravi vulnerabilità, sfruttabili con comandi base del sistema:

- **Ingreslock Backdoor (Porta 1524)**
  Durante la scansione *nmap -sV*, alla riga della porta 1524, risultante open, il servizio è descritto esplicitamente come Metasploitable root shell. Chiunque si connetta a questa porta (con netcat o telnet) ottiene immediatamente accesso come utente root senza dover inserire alcuna password.
- **Permessi read/write pubblici (SMB)**
  Lo script *smb-enum-shares* mostra per la cartella condivisa *\\192.168.51.101\tmp* la dicitura: *Anonymous access: READ/WRITE.* La configurazione della cartella è impostata in modo da permettere a chiunque di scrivere. Un attaccante può usare questo accesso per caricare virus o script malevoli direttamente nel server.
- **Enumerazione users non bloccata**
  Lo script smb-enum-users è riuscito a scaricare l'intera lista degli utenti (es. backup, msfadmin, root). Il server non è configurato contro ricognizioni fatte da estranei. Questo dimezza il lavoro per un attacco brute-force, perché l'attaccante conoscerebbe già tutti i nomi utente validi.
- **Accesso FTP senza password**
  Lo script *ftp-anon* riporta *Anonymous FTP login allowed.* Ciò significa che è stata lasciata attiva l'opzione che permette l'ingresso con l'utente "anonymous".
- **Telnet open**
  La Telnet (porta 23) trasmette tutto (inclusa la password di root) in chiaro. Chiunque "ascolti" la rete (sniffing) può rubare le credenziali.

Oltre a queste vulnerabilità se ne possono scoprire altre, sfruttabili con l'utilizzo di codici specifici, queste vulnerabilità sono causate dall'obsolescenza di molti software installati sulla macchina (*Apache 2.2.8, OpenSSH 4.7p1, PostgreSQL 8.3.0, MySQL, ISC BIND 9.4.2*)