

Report per 192.168.50.101 (Metasploitable):

- **IP:** 192.168.50.101
- **Sistema Operativo:** Linux 2.6.9 - 2.6.33
- **Porte Aperte:**
- 21/tcp (ftp)
- 22/tcp (ssh)
- 23/tcp (telnet)
- 25/tcp (smtp)
- 53/tcp (domain)
- 80/tcp (http)
- 111/tcp (rpcbind)
- 139/tcp (netbios-ssn)
- 445/tcp (microsoft-ds)
- 512/tcp (exec)
- 513/tcp (login)
- 514/tcp (shell)
- 1099/tcp (rmiregistry)
- 1524/tcp (ingreslock)
- 2049/tcp (nfs)
- 2121/tcp (ccproxy-ftp)
- 3306/tcp (mysql)
- 5432/tcp (postgresql)
- 5900/tcp (vnc)
- 6000/tcp (X11)
- 6667/tcp (irc)
- 8009/tcp (ajp13)
- 8180/tcp (unknown)
- **Servizi in Ascolto con Versione:**
- ftp: vsftpd 2.3.4
- ssh: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- telnet: Linux telnetd
- smtp: Postfix smtpd
- domain: ISC BIND 9.4.2
- http: Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- rpcbind: 2 (RPC #100000)
- netbios-ssn: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- microsoft-ds: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- exec: netkit-rsh rexecd
- login?: Netkit rshd
- shell: Netkit rshd

- rmiregistry: GNU Classpath grmiregistry
- ingreslock: Metasploitable root shell
- nfs: 2-4 (RPC #100003)
- ccproxy-ftp: ProFTPD 1.3.1
- mysql: MySQL 5.0.51a-3ubuntu5
- postgresql: PostgreSQL DB 8.3.0 - 8.3.7
- vnc: VNC (protocol 3.3)
- X11: (access denied)
- irc: UnrealIRCd
- ajp13: Apache Jserv (Protocol v1.3)
- unknown: (servizio sconosciuto)

Potrebbe essere necessario eseguire la scansione con privilegi più elevati o esaminare le configurazioni di sicurezza come firewall su Windows 7 per ottenere risultati più completi.

Report per 192.168.50.102 (Windows 7):

- **IP:** 192.168.50.102
- **Sistema Operativo:** Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
- **Porte Aperte:**
 - 135/tcp (msrpc)
 - 139/tcp (netbios-ssn)
 - 445/tcp (microsoft-ds)
 - 5357/tcp (wsdapi)
 - 49152/tcp (unknown)
 - 49153/tcp (unknown)
 - 49154/tcp (unknown)
 - 49155/tcp (unknown)
 - 49156/tcp (unknown)
 - 49157/tcp (unknown)
- **Servizi in Ascolto con Versione:**
 - msrpc: Microsoft Windows RPC
 - netbios-ssn: Microsoft Windows NetBIOS
 - microsoft-ds: Microsoft Windows file sharing
 - wsdapi: Microsoft Windows Web Services API
 - unknown: (servizio sconosciuto)

SOLUZIONE:

Blocco delle Scansioni:

Il firewall di Windows 7 potrebbe essere configurato per bloccare le scansioni da parte di strumenti come Nmap. In questo caso, la scansione potrebbe non essere in grado di rilevare tutte le porte aperte o i servizi in esecuzione.

Autorizzazioni delle Regole:

Le regole del firewall potrebbero non essere configurate per consentire la comunicazione con lo strumento di scansione. Verificare che ci siano regole specifiche che consentano il traffico in ingresso e in uscita per gli strumenti di scansione come Nmap.

Modifica delle Regole del Firewall:

Accedere alle impostazioni del firewall su Windows 7 e modificare le regole per consentire la comunicazione con Nmap. Assicurarsi che le porte utilizzate da Nmap siano aperte e che ci siano regole specifiche per permettere il traffico.

Disabilitazione Temporanea del Firewall:

Se necessario, si possono disabilitare temporaneamente i firewall per condurre la scansione. Tuttavia, questo processo può essere effettuato solo se la rete sia sicura e non esposta a potenziali minacce esterne. Dopo la scansione, riabilitare il firewall.

Esecuzione di Nmap con Privilegi Elevati:

Assicurarsi di eseguire Nmap con privilegi elevati (ad esempio, eseguendo il prompt dei comandi come amministratore). Questo potrebbe consentire una scansione più approfondita, superando eventuali restrizioni imposte da Windows.

Esame degli Eventi del Firewall:

Controllare gli eventi del firewall su Windows 7 per individuare eventuali blocchi o avvisi relativi alla scansione. Questi eventi potrebbero fornire indicazioni su eventuali problemi di comunicazione.

Autorizzazioni Adeguatamente Configurate:

Assicurati che le autorizzazioni del firewall siano configurate in modo adeguato per evitare aperture non necessarie, mantenendo allo stesso tempo un ambiente sicuro.

Consenso dell'Amministratore:

Per modificare le impostazioni del firewall, potrebbe essere necessario l'accesso con privilegi di amministratore. Verificare di avere le autorizzazioni necessarie.



```
root@luxme: /home/kali
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds

(root@luxme)-[/home/kali]
# nmap -sT 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 10:59 CET
Nmap scan report for 192.168.50.101
Host is up (0.0020s 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    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
3040/tcp  open  nfs
```


```
root@luxme: /home/kali

5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:99:EC:DB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.73 seconds

(root@luxme)-[/home/kali]
# nmap -sV 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 10:59 CET
Nmap scan report for 192.168.50.101
Host is up (0.0015s 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)
```



```

root@luxme: /home/kali
nmap done: 1 IP address (1 host up) scanned in 10.100 seconds

(root@luxme)-[/home/kali]
# nmap -O 192.168.50.102

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-27 11:03 CET
Nmap scan report for 192.168.50.102
Host is up (0.0017s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:07:71:A4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7:sp1 cpe:/o:microsoft:windows_server_2008:sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_server_2008:r3

```