Report W10D4

Tramite la VM Kali (192.168.50.100) vengono eseguite delle scansioni sulla VM Meta (192.168.51.101)

Con il comando

nmap -sV 192.168.51.101 si ottengono questi risultati, mostrando sia le porte aperte sia i relativi servizi con le versioni in uso:

```
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 ccproxy-ftp?
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
```

Con il comando

Nmap -sn -PE 192.168.51.101 viene mostrato se l'host è attivo sulla rete:

```
└─# nmap -sn -PE 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 05:01 EST
Nmap scan report for 192.168.51.101
Host is up (0.017s latency).
Nmap done: 1 IP address (1 host up) scanned in 17.30 seconds
```

Con il comando

Nmap -sS -Sv -T4 192.168.51.101 andiamo ad eseguire una scansione SYN, quindi più leggera, ed una scansione che, come sopra, mostra le versioni dei servizi in uso. Il flag -T4 aumenta l'aggressività della scansione:

```
└─# nmap -sS -sV -T4 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 05:05 EST
Nmap scan report for 192.168.51.101
Host is up (0.0036s 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  ccproxy-ftp?
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
```

Con il comando

Nc -nvz 192.168.51.101 1-1024 si esegue una scansione TCP/IP mediante un'altra utility chiamata netcat, il quale scansione le porte dalla 1 alla 1024: