### 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:

```
vsftpd 2.3.4
OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
           open
22/tcp
           open
                 ssh
23/tcp
                  telnet
                                   Postfix smtpd
ISC BIND 9.4.2
                  smtp
53/tcp
           open
                  domain
80/tcp
                                   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
           open
                  rpcbind
                                    2 (RPC #100000)
           open
          open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
445/tcp
                                   netkit-rsh rexecd
           open
513/tcp open
514/tcp open
                  login?
                  shell
                                   Netkit rshd
1099/tcp open
                                   GNU Classpath grmiregistry
                  java-rmi
1524/tcp open
2049/tcp open
                                   Metasploitable root shell
2-4 (RPC #100003)
                  bindshell
                 nfs
2121/tcp open
                 ccproxy-ftp?
3306/tcp open
                                   MySQL 5.0.51a-3ubuntu5
5432/tcp open
                  postgresql PostgreSQL DB 8.3.0 - 8.3.7 vnc VNC (protocol 3.3)
5900/tcp open
6000/tcp open
                                    (access denied)
6667/tcp open
8009/tcp open
                                   UnrealIRCd
                  ajp13
http
                                   Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open
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:

```
Starting Nmap 7.945VN ( 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
                                             vsftpd 2.3.4
                                             OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
 22/tcp
             open ssh
open telnet
23/tcp
25/tcp
53/tcp
                                             Linux telnetd
Postfix smtpd
                        smtp
domain
              open
                                             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #100000)
80/tcp
111/tcp
139/tcp
445/tcp
                        http
rpcbind
                        netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
              open
 512/tcp
513/tcp
                        exec
login?
                                             netkit-rsh rexecd
             open
                                             Netkit rshd
GNU Classpath grmiregistry
514/tcp open
1099/tcp open
                        java-rmi
1524/tcp open
2049/tcp open
                                             Metasploitable root
2-4 (RPC #100003)
                        bindshell
                        nfs
2121/tcp open
3306/tcp open
                        ccproxy-ftp?
                       mysql
postgresql
                                              MySOL 5.0.51a-3ubuntu5
 5432/tcp open
5900/tcp open
                                             PostgreSQL DB 8.3.0
VNC (protocol 3.3)
                        vnc
X11
 5000/tcp open
6667/tcp open
8009/tcp open
                                              UnrealIRCd
                                   Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
8180/tcp open http
Service Info: Hosts:
```

## 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:

```
(UNKNOWN) [192.168.51.101] 514 (shell) open (UNKNOWN) [192.168.51.101] 513 (login) open (UNKNOWN) [192.168.51.101] 512 (exec) open (UNKNOWN) [192.168.51.101] 512 (exec) open (UNKNOWN) [192.168.51.101] 445 (microsoft-ds) open (UNKNOWN) [192.168.51.101] 139 (netbios-ssn) open (UNKNOWN) [192.168.51.101] 111 (sunrpc) open (UNKNOWN) [192.168.51.101] 80 (http) open (UNKNOWN) [192.168.51.101] 53 (domain) open (UNKNOWN) [192.168.51.101] 25 (smtp) open (UNKNOWN) [192.168.51.101] 25 (smtp) open (UNKNOWN) [192.168.51.101] 23 (telnet) open (UNKNOWN) [192.168.51.101] 22 (ssh) open (UNKNOWN) [192.168.51.101] 21 (ftp) open
```