**Report di sicurezza**

- Prima scansione *(port 0 to 1024)* TCP:

La scansione eseguta con nmap dalla macchina Kali Linux ha scansionato tutte le porte well-know, di quetste 1013 snon risultate come chiuse e la conessione verso di esse è stata rifiutata.

Le porte trovate come aperte sono le seguenti:

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

La scansione è stata eseguta verso un solo host (*192.168.50.101*), in questo caso analizzando Wireshark si possono notare chimate di tipo SYN verso l’ip di destinazione e risposte (ACK) con richiesta di rest della conessione (RST).

- Seconda scansione *(port 0 to 1024)* SYN:

Come la precedente scansione anche qui ho usato nmap, da questo risultato posso sapere: la latenza, le port non “mostrate”, il MAC adddress e il suo nome.

Nmap scan report for 192.168.50.101

Host is up (0.000094s latency).

All 1025 scanned ports on 192.168.50.101 are in ignored states.

Not shown: 1025 unfiltered tcp ports (reset)

MAC Address: 08:00:27:EA:CD:BB (Oracle VirtualBox virtual NIC)

- Terza scansione: questo tipo di scansione risulta come la più completa poichè effettua chiamate utliazzando diversi protocolli a differnza delle precedenti dove veiva utliazzato solo TCP, questa scansione sono stati utlizzati i protocolli SSHv2, TCP, RPC, HTTP, Portmap, FTP, DNS, UDP, ICMP, SMB.

Nmap mostra nell’output tutti i dettagli dei servizi aperti come FTP che permette il login e non ha limiti di banda.

Questa scansione riporta anche altre informazioni utili come il system time, il tipo di BIOS in questo caso: *METASPLOITABLE*.

Nmap riporta come output:

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 09:39 EST

Nmap scan report for 192.168.50.101

Host is up (0.00029s latency).

Not shown: 1013 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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|\_ssl-date: 2023-12-21T14:40:16+00:00; -1s from scanner time.

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

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 34967/udp mountd

| 100005 1,2,3 42752/tcp mountd

| 100021 1,3,4 36042/tcp nlockmgr

| 100021 1,3,4 54885/udp nlockmgr

| 100024 1 47725/udp status

|\_ 100024 1 50330/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login OpenBSD or Solaris rlogind

514/tcp open shell Netkit rshd

MAC Address: 08:00:27:EA:CD:BB (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|\_clock-skew: mean: 1h39m55s, deviation: 2h53m15s, median: -1s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2023-12-21T09:39:58-05:00

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE

HOP RTT ADDRESS

1 0.29 ms 192.168.50.101

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 44.65 seconds