Alaimo Alessandro
10/11/2022

Scanning con Nmap

Tipo di scan
nmap 192.168.50.101 -sT

	Fonte dello scan	Target dello scan	Risultato Ottenuto
1	192.168.50.100	192.168.50.101	Port: 45098 → 80 [SYN] Seq= 0
1	192.168.50.101	192.168.50.100	Port: 80 → 45098 [SYN, ACK] Seq= 0 Ack=1
1	192.168.50.100	192.168.50.101	Port: 45098 → 80 [ACK] Seq= 1 Ack=1
2	192.168.50.100	192.168.50.101	Port: 37288 → 445 [SYN] Seq= 0
2	192.168.50.101	192.168.50.100	Port: 445 → 37288 [SYN, ACK] Seq= 0 Ack=1
2	192.168.50.100	192.168.50.101	Port: 37288 → 445 [ACK] Seq= 1 Ack=1
3	192.168.50.100	192.168.50.101	Port: 49774 → 53 [SYN] Seq= 0
3	192.168.50.101	192.168.50.100	Port: 53 → 49774 [SYN, ACK] Seq= 0 Ack=1
3	192.168.50.100	192.168.50.101	Port: 49774 → 53 [ACK] Seq= 1 Ack=1
4	192.168.50.100	192.168.50.101	Port: 43342 → 22 [SYN] Seq= 0
4	192.168.50.101	192.168.50.100	Port: 22 → 43342 [SYN, ACK] Seq= 0 Ack=1
4	192.168.50.100	192.168.50.101	Port: 43342 → 22 [ACK] Seq= 1 Ack=1
5	192.168.50.100	192.168.50.101	Port: 55674 → 25 [SYN] Seq= 0
5	192.168.50.101	192.168.50.100	Port: 25 → 55674 [SYN, ACK] Seq= 0 Ack=1
5	192.168.50.100	192.168.50.101	Port: 55674 → 25 [ACK] Seq= 1 Ack=1
6	192.168.50.100	192.168.50.101	Port: 54340 → 111 [SYN] Seq= 0
6	192.168.50.101	192.168.50.100	Port: 111 → 54340 [SYN, ACK] Seq= 0 Ack=1
6	192.168.50.100	192.168.50.101	Port: 54340 → 111 [ACK] Seq= 1 Ack=1
7	192.168.50.100	192.168.50.101	Port: 39484 → 21 [SYN] Seq= 0
7	192.168.50.101	192.168.50.100	Port: 21 → 39484 [SYN, ACK] Seq= 0 Ack=1
7	192.168.50.100	192.168.50.101	Port: 39484 → 21 [ACK] Seq= 1 Ack=1
8	192.168.50.100	192.168.50.101	Port: 58396 → 139 [SYN] Seq= 0
8	192.168.50.101	192.168.50.100	Port: 139 → 58396 [SYN, ACK] Seq= 0 Ack=1
8	192.168.50.100	192.168.50.101	Port: 58396 → 139 [ACK] Seq= 1 Ack=1
9	192.168.50.100	192.168.50.101	Port: 35502 → 23 [SYN] Seq= 0
9	192.168.50.101	192.168.50.100	Port: 23 → 35502 [SYN, ACK] Seq= 0 Ack=1
9	192.168.50.100	192.168.50.101	Port: 35502 → 23 [ACK] Seq= 1

			Ack=1
10	192.168.50.100	192.168.50.101	Port: 49916 → 514 [SYN] Seq= 0
10	192.168.50.101	192.168.50.100	Port: 514 → 49916 [SYN, ACK] Seq= 0 Ack=1
10	192.168.50.100	192.168.50.101	Port: 49916 → 514 [ACK] Seq= 1 Ack=1
11	192.168.50.100	192.168.50.101	Port: 54844 → 512 [SYN] Seq= 0
11	192.168.50.101	192.168.50.100	Port: 512 → 54844 [SYN, ACK] Seq= 0 Ack=1
11	192.168.50.100	192.168.50.101	Port: 54844 → 512 [ACK] Seq= 1 Ack=1
12	192.168.50.100	192.168.50.101	Port: 41642 → 513 [SYN] Seq= 0
12	192.168.50.101	192.168.50.100	Port: 513 → 41642 [SYN, ACK] Seq= 0 Ack=1
12	192.168.50.100	192.168.50.101	Port: 41642 → 513 [ACK] Seq= 1 Ack=1
		Totale Servizi:	12 Servizi Attivi nelle Well-Know Port

Tipo di scan
nmap 192.168.50.101 -sS

	Fonte dello scan	Target dello scan	Risultato Ottenuto
1	192.168.50.100	192.168.50.101	Port: 45098 → 80 [SYN] Seq= 0
1	192.168.50.101	192.168.50.100	Port: 80 → 45098 [SYN, ACK] Seq= 0 Ack=1
1	192.168.50.100	192.168.50.101	Port: 45098 → 80 [RST] Seq= 1 Ack=1
2	192.168.50.100	192.168.50.101	Port: 37288 → 445 [SYN] Seq= 0
2	192.168.50.101	192.168.50.100	Port: 445 → 37288 [SYN, ACK] Seq= 0 Ack=1
2	192.168.50.100	192.168.50.101	Port: 37288 → 445 [RST] Seq= 1 Ack=1
3	192.168.50.100	192.168.50.101	Port: 49774 → 53 [SYN] Seq= 0
3	192.168.50.101	192.168.50.100	Port: 53 → 49774 [SYN, ACK] Seq= 0 Ack=1
3	192.168.50.100	192.168.50.101	Port: 49774 → 53 [RST] Seq= 1 Ack=1
4	192.168.50.100	192.168.50.101	Port: 43342 → 22 [SYN] Seq= 0
4	192.168.50.101	192.168.50.100	Port: 22 → 43342 [SYN, ACK] Seq= 0 Ack=1
4	192.168.50.100	192.168.50.101	Port: 43342 → 22 [RST] Seq= 1 Ack=1
5	192.168.50.100	192.168.50.101	Port: 55674 → 25 [SYN] Seq= 0
5	192.168.50.101	192.168.50.100	Port: 25 → 55674 [SYN, ACK] Seq= 0 Ack=1
5	192.168.50.100	192.168.50.101	Port: 55674 → 25 [RST] Seq= 1 Ack=1
6	192.168.50.100	192.168.50.101	Port: 54340 → 111 [SYN] Seq= 0
6	192.168.50.101	192.168.50.100	Port: 111 → 54340 [SYN, ACK] Seq= 0 Ack=1
6	192.168.50.100	192.168.50.101	Port: 54340 → 111 [RST] Seq= 1

			Ack=1
7	192.168.50.100	192.168.50.101	Port: 39484 → 21 [SYN] Seq= 0
7	192.168.50.101	192.168.50.100	Port: 21 → 39484 [SYN, ACK] Seq= 0 Ack=1
7	192.168.50.100	192.168.50.101	Port: 39484 → 21 [RST] Seq= 1 Ack=1
8	192.168.50.100	192.168.50.101	Port: 58396 → 139 [SYN] Seq= 0
8	192.168.50.101	192.168.50.100	Port: 139 → 58396 [SYN, ACK] Seq= 0 Ack=1
8	192.168.50.100	192.168.50.101	Port: 58396 → 139 [RST] Seq= 1 Ack=1
9	192.168.50.100	192.168.50.101	Port: 35502 → 23 [SYN] Seq= 0
9	192.168.50.101	192.168.50.100	Port: 23 → 35502 [SYN, ACK] Seq= 0 Ack=1
9	192.168.50.100	192.168.50.101	Port: 35502 → 23 [RST] Seq= 1 Ack=1
10	192.168.50.100	192.168.50.101	Port: 49916 → 514 [SYN] Seq= 0
10	192.168.50.101	192.168.50.100	Port: 514 → 49916 [SYN, ACK] Seq= 0 Ack=1
10	192.168.50.100	192.168.50.101	Port: 49916 → 514 [RST] Seq= 1 Ack=1
11	192.168.50.100	192.168.50.101	Port: 54844 → 512 [SYN] Seq= 0
11	192.168.50.101	192.168.50.100	Port: 512 → 54844 [SYN, ACK] Seq= 0 Ack=1
11	192.168.50.100	192.168.50.101	Port: 54844 → 512 [RST] Seq= 1 Ack=1
12	192.168.50.100	192.168.50.101	Port: 41642 → 513 [SYN] Seq= 0
12	192.168.50.101	192.168.50.100	Port: 513 → 41642 [SYN, ACK] Seq= 0 Ack=1
12	192.168.50.100	192.168.50.101	Port: 41642 → 513 [RST] Seq= 1 Ack=1
		Totale Servizi:	12 Servizi Attivi nelle Well-Know Port

```
└─$ sudo nmap 192.168.50.101 -A
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 09:51 EST
Nmap scan report for 192.168.50.101
Host is up (0.00019s latency).
Not shown: 977 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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, E
NHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=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
|_ssl-date: 2022-11-10T14:52:14+00:00; +3s from scanner time.
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
```

```
|_  100003  2,3,4       2049/udp   nfs
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
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 18
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHan
dshake, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: 9~3~DxPe-N"[&I}Z+fC[
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-11-10T14:52:14+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=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
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:29:CA:6A (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: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-10T09:52:06-05:00
```

```
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xer
ox)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h15m06s, deviation: 2h30m06s, median: 2s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.19 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.09 seconds
```