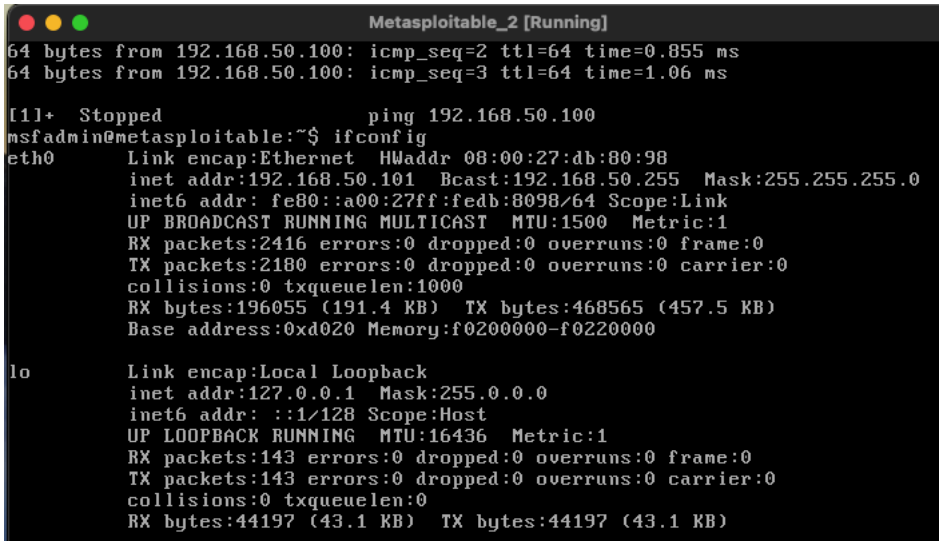
Modulo 3 Esercitazione 6 Parte 2 – Alessio Russo

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

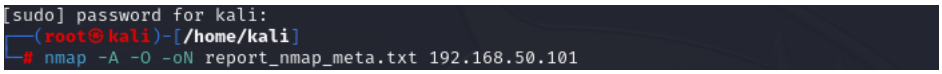
- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

Effettuo una scansione completa attraverso: nmap -A -O -oN {nomereport} IP_target:

IP target



comando nmap:



Report completo:

Nmap 7.94SVN scan initiated Sun Jan 21 16:32:29 2024 as: nmap -A -O -oN report_nmap_meta.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: 2024-01-21T15:33:00+00:00; +10s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| 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_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| 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
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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     35593/tcp   mountd
|   100005  1,2,3     36902/udp   mountd
|   100021  1,3,4     48342/tcp   nlockmgr
|   100021  1,3,4     49379/udp   nlockmgr
```

| 100024 1 33457/udp status
|_ 100024 1 46727/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 tcpwrapped
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: 8
| Capabilities flags: 43564
| Some Capabilities: Speaks41ProtocolNew, SupportsTransactions, Support41Auth, SupportsCompression, LongColumnFlag, SwitchToSSLAfterHandshake, ConnectWithDatabase
| Status: Autocommit
|_ Salt: |Rd"xW+prkDROrrd}j{K
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| 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
|_ssl-date: 2024-01-21T15:33:00+00:00; +10s from scanner time.
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
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:05:19
| source ident: nmap
| source host: C96903AF.85216C96.FFFA6D49.IP
|_ error: Closing Link: ifjtbfjfh[192.168.50.100] (Quit: ifjtbfjfh)
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-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:DB:80:98 (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: 2024-01-21T10:32:51-05:00
|_clock-skew: mean: 1h15m09s, deviation: 2h29m59s, median: 9s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT   ADDRESS
1   0.61 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done at Sun Jan 21 16:32:51 2024 -- 1 IP address (1 host up) scanned in 22.08
seconds

Da queste info possiamo ricavare tutti I quesiti richiesti nella traccia.