Minor Project II

SECURITY ANALYSIS OF METASPLOITABLE 2 USING NMAP AND NESSUS

Senselearner

-Team Euphorbia

Contents

Introduction

The purpose of this report is to present the activities conducted during Week 02 of the Cybersecurity Internship. The focus of this week's project was to set up and analyze the security of Metasploitable 2, a deliberately vulnerable virtual machine. We were tasked with installing Metasploitable 2, performing a network scan using Nmap, conducting a vulnerability assessment using Nessus, and generating a comprehensive report outlining the identified vulnerabilities and recommended remediation actions.

PROJECT OBJECTIVES AND METHODOLOGYS

The objectives of this project were to set up Metasploitable 2, perform a network scan using Nmap to identify open ports, running services, and potential vulnerabilities, conduct a vulnerability assessment using Nessus, and generate a comprehensive report. The methodology involved the following steps:

a) Downloading and installing Metasploitable 2 on a virtualization platform such as VMware or VirtualBox.

b) Executing a network scan using Nmap to identify open ports, running services, and potential vulnerabilities.

c) Utilizing Nmap scripts to gather additional information about the identified services and potential vulnerabilities.

d) Installing and configuring Nessus, a vulnerability scanner, on the host machine.

e) Conducting a comprehensive vulnerability assessment of Metasploitable 2 using Nessus.

f) Analyzing the Nessus scan results, including identified vulnerabilities, severity levels, and potential impacts.

g) Preparing a comprehensive report documenting the project findings, including an overview of the project objectives and methodology, the installation process and network configuration of Metasploitable 2, Nmap scan results, Nessus vulnerability assessment findings, recommended remediation actions for each identified vulnerability, and a conclusion with recommendations for improving the security posture of Metasploitable 2.

METASPLOITABLE 2 INSTALLATION AND NETWORK CONFIGURATION

The installation process of Metasploitable 2 involves the following steps:

1. **Download the Metasploitable 2 VM:** Metasploitable 2 is available for download as a pre-configured virtual machine. You can obtain the VM image from reliable sources such as the Metasploit website or trusted online repositories.
2. **Choose a Virtualization Platform:** Metasploitable 2 can be run on popular virtualization platforms such as VMware or VirtualBox. Select the platform of your choice and ensure it is installed on your system.
3. **Import Metasploitable 2 into the Virtualization Software:** Open the virtualization software (VMware or VirtualBox) and import the Metasploitable 2 VM image into the software. This process typically involves selecting the option to import an existing virtual machine and providing the path to the downloaded Metasploitable 2 VM image.
4. **Configure Network Settings:** Once the VM is imported, you need to configure the network settings to establish connectivity. Metasploitable 2 is usually set up with a default network configuration, but it's essential to ensure that it aligns with your virtualization software's networking setup.
5. **Start the Metasploitable 2 VM:** After the network settings are configured, you can start the Metasploitable 2 virtual machine within your virtualization software. The VM will boot up, and you will be provided with the login credentials for accessing the system.

Regarding network configuration, Metasploitable 2 is typically set up with a default network configuration that allows it to connect to the network and communicate with the host machine and other virtual machines. By default, Metasploitable 2 is configured

witha single network interface and may use NAT (Network Address Translation) or Bridged mode to establish connectivity.

NAT mode allows the virtual machine to access the network through the host machine's network interface, using the host's IP address for external communication. In Bridged mode, the virtual machine is directly connected to the network, obtaining its IP address and network connectivity independently.

It's crucial to ensure that the virtualization software's network settings are properly configured to establish connectivity between the host machine and the Metasploitable 2 VM. This will enable network scanning using tools like Nmap and conducting vulnerability assessments using Nessus as discussed in the project objectives.

NETWORK SCANNING USING NMAP

Nmap, a network scanning tool, was used to perform a network scan of Metasploitable 2. The objective was to identify open ports, running services, and potential vulnerabilities.

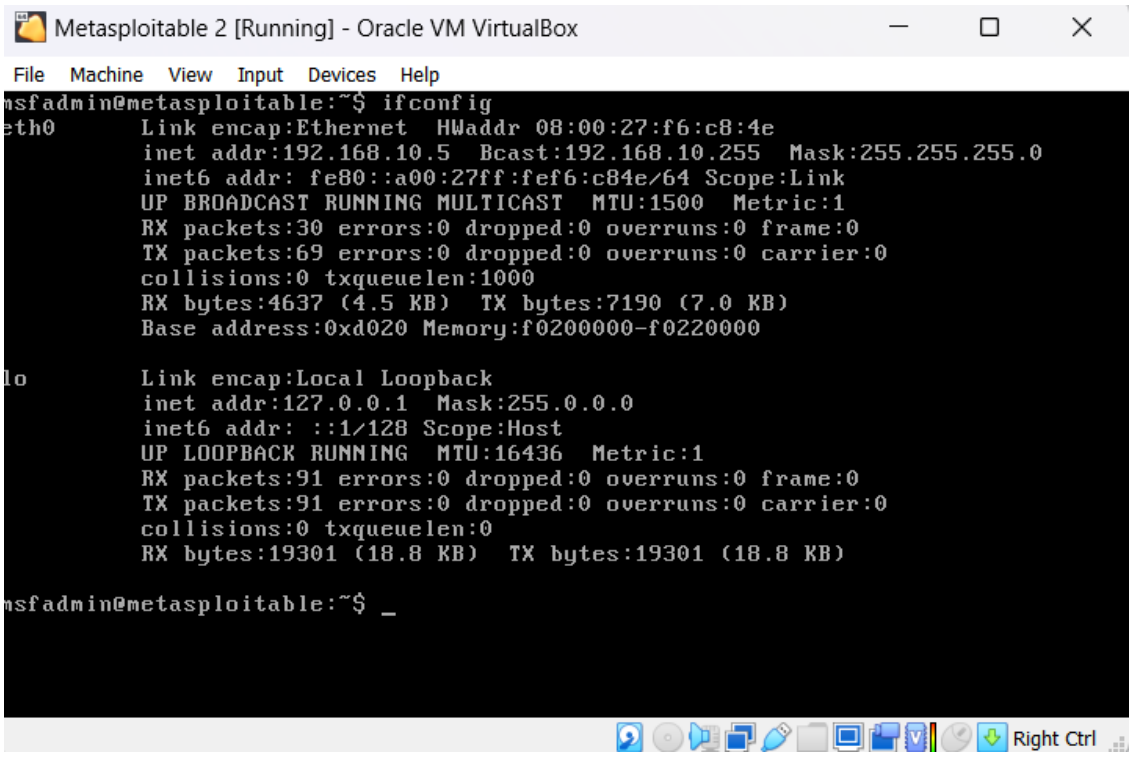
NMAP SCAN RESULTS

The Nmap scan yielded the following results:

Open Ports: List the open ports discovered during the scan and their associated services.

Running Services: Identify the services running on the open ports.

Finding the Ip address of linux machines



NETWORK SCANNING USING NMAP

Metasploitable 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:c8:4e
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:c84e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4637 (4.5 KB)  TX bytes:7190 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

Right Ctrl

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.4  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::efde:e5c3:bb1e:aa27  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 1890 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3700 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

NETWORK SCANNING USING NMAP

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sV -O 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-08 06:26 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00094s 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       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
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
MAC Address: 08:00:27:F6:C8:4E (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

OS and Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Default Scan

```
nmap -sV -script=default 192.168.10.5

Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-09 00:52 EDT

Nmap scan report for 192.168.10.5

Host is up (0.00017s 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 192.168.10.4

|      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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)

|_ 2048 5656240f211ddea72bae61b1243de8f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

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

| 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: 2023-07-09T04:52:33+00:00; +1s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC2_128_CBC_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

```
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_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-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      40281/udp   mountd
|   100005  1,2,3      55892/tcp   mountd
|   100021  1,3,4      41604/udp   nlockmgr
|   100021  1,3,4      46082/tcp   nlockmgr
```

```
|   100024  1         44922/tcp   status
|_  100024  1         52448/udp   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
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: Support41Auth, ConnectWithDatabase, SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumnFlag
```

```
|   Status: Autocommit
|_  Salt: '3i:$DjiR=zo@/h@E|_G
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-07-09T04:52:33+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
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, 0:03:49
|   source ident: nmap
|   source host: BAAF933C.554FE7D2.FFFA6D49.IP
|_  error: Closing Link: kqnepylav[192.168.10.4] (Quit: kqnepylav)
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-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:F6:C8:4E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h00m01s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
```

```
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-07-09T00:52:26-04:00
| 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: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.89 second
```

Vulnerability Scan

```
nmap --script=vuln -sV 192.168.10.5


Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-09 09:04 IST

Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 8.70% done; ETC: 09:04 (0:00:00 remaining)

Nmap scan report for 192.168.14.191

Host is up (0.054s latency).

Not shown: 977 filtered tcp ports (no-response)

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

| ssl-dh-params:

|   VULNERABLE:

|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability

|     State: VULNERABLE

|       Transport Layer Security (TLS) services that use anonymous

|       Diffie-Hellman key exchange only provide protection against passive

|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
```

```
|     which could completely compromise the confidentiality and integrity
|     of any data exchanged over the resulting session.
|   Check results:
|     ANONYMOUS DH GROUP 1
|          Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|          Modulus Type: Safe prime
|          Modulus Source: postfix builtin
|          Modulus Length: 1024
|          Generator Length: 8
|          Public Key Length: 1024
|   References:
|     https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE
|   IDs:  BID:74733  CVE:CVE-2015-4000
|     The Transport Layer Security (TLS) protocol contains a flaw that is
|     triggered when handling Diffie-Hellman key exchanges defined with
|     the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
```

```
|     to downgrade the security of a TLS session to 512-bit export-grade
|     cryptography, which is significantly weaker, allowing the attacker
|     to more easily break the encryption and monitor or tamper with
|     the encrypted stream.
|   Disclosure date: 2015-5-19
|   Check results:
|     EXPORT-GRADE DH GROUP 1
|         Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|         Modulus Type: Safe prime
|         Modulus Source: Unknown/Custom-generated
|         Modulus Length: 512
|         Generator Length: 8
|         Public Key Length: 512
|   References:
|     https://weakdh.org
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|     https://www.securityfocus.com/bid/74733
|
| Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
```

```
|     Transport Layer Security (TLS) services that use Diffie-Hellman groups
|     of insufficient strength, especially those using one of a few commonly
|     shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|     WEAK DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: postfix builtin
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|   References:
|_     https://weakdh.org
| ssl-poodle:
|  VULNERABLE:
|  SSL POODLE information leak
|   State: VULNERABLE
|   IDs:  BID:70574  CVE:CVE-2014-3566
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
```

```
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
53/tcp   open  domain      ISC BIND 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-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
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  tcpwrapped
1099/tcp open  java-rmi     GNU Classpath grmiregistry
|_rmi-vuln-classloader: ERROR: Script execution failed (use -d to debug)
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
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
```

```
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
```

```
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
```

```
|     References:
|_     https://weakdh.org
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
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache-Coyote/1.1
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-csrf:
|       Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.14.191
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.14.191:8180/admin/
|     Form id: username
|_                                                    Form action: j_security_check;jsessionid=843D54076336BF45FCD215D3D6231BA2
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: EOF

|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: EOF

|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

|_smb-vuln-ms10-054: false

| smb-vuln-cve2009-3103:

| VULNERABLE:

| SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)

| State: VULNERABLE

| IDs: CVE:CVE-2009-3103

| Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,

| Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a

| denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE

| PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,

| aka "SMBv2 Negotiation Vulnerability."

| Disclosure date: 2009-09-08

| References:

| http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 152.78 seconds

NMAP SCRIPT RESULTS

Nmap scripts were employed to gather additional information about the identified services and potential vulnerabilities. The following Nmap scripts were executed:

Script 1: The Metasploitable 2 machine has several open and vulnerable services, including an open FTP server (vsftpd 2.3.4) with anonymous login allowed, an outdated OpenSSH server (4.7p1 Debian 8ubuntu1), and an open Telnet service (Linux telnetd). These services could pose significant security risks if not properly secured and updated.

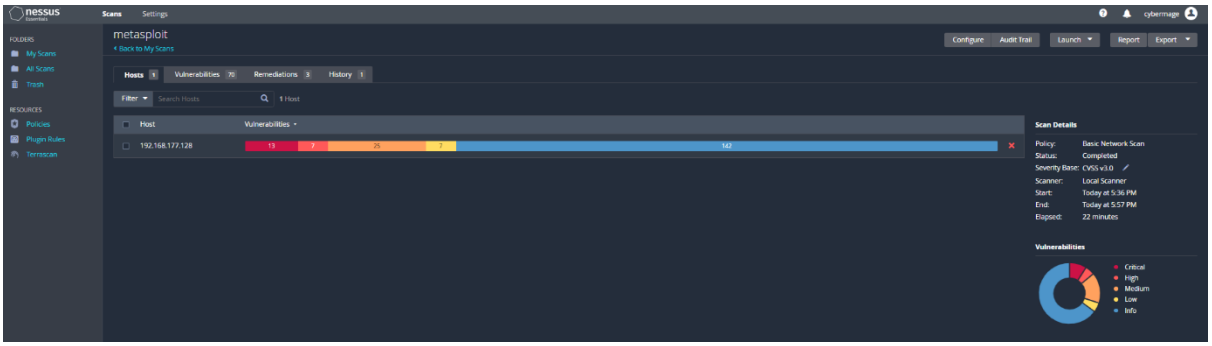
Script 2: The presence of open NetBIOS services (Samba smbd 3.X - 4.X) on ports 139 and 445 suggests potential vulnerabilities that could be exploited by attackers. It is crucial to ensure that proper security measures are implemented to protect against unauthorized access and data breaches.

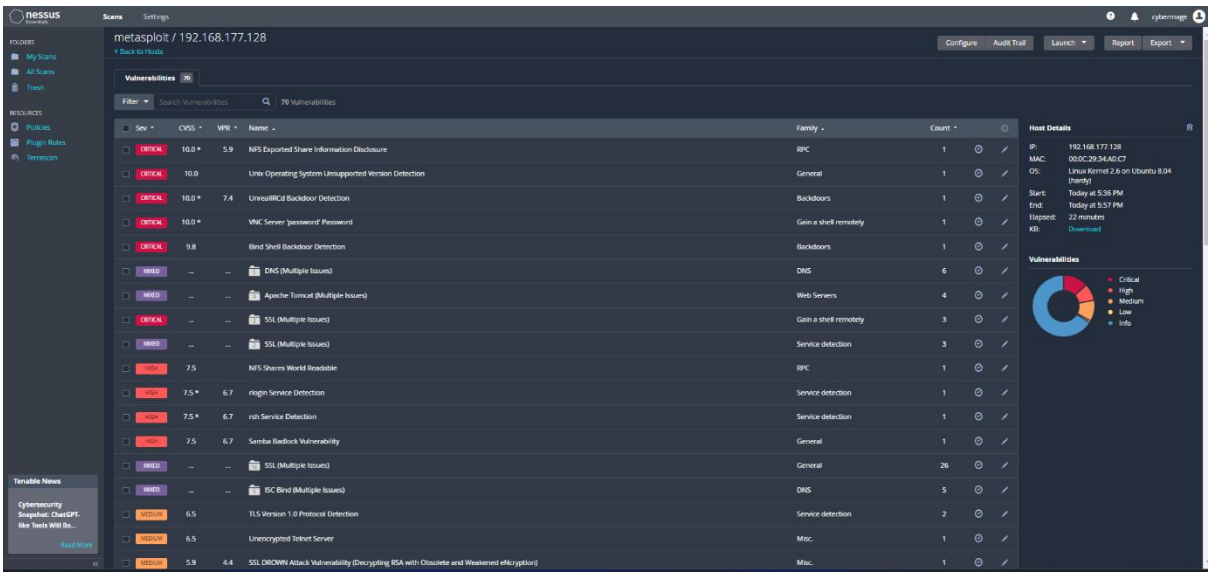
VULNERABILITY ASSESSMENT USING NESSUS

Nessus, a vulnerability scanner, was installed and configured on the host machine. A comprehensive vulnerability assessment of Metasploitable 2 was conducted using Nessus.

NESSUS SCAN RESULTS

The Nessus scan generated detailed results, including identified vulnerabilities, severity levels, and potential impacts. Notable findings include:





NESSUS SCAN RESULTS

nessus

Report generated by Nessus™

metasploit

Sun, 09 Jul 2023 17:57:42 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.177.128

11	6	19	6	79
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server

NESSUS SCAN RESULTS

LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection

1. **Vulnerability:** Unix OS Unsupported Version Detection

   Description: This vulnerability refers to the detection of an outdated and unsupported version of the Unix operating system on the target system.

   Severity Level: CRITICAL

   Potential Impact:

   Lack of security updates

   Exploitation of known vulnerabilities

   Compliance violations

2. **Vulnerability:** rlogin Service Detection

   Description: The rlogin service is detected on the target system, which poses security risks due to its lack of encryption and weak authentication.

   Severity Level: MEDIUM

   Potential Impact:

   Unauthorized access

   Data interception

   Credential compromise

3. **Vulnerability :** X Server Detection

   Description: The presence of Xserver, a component of the X Window System, is detected on the target system.

   Severity Level: LOW

   Potential Impact:

   Unauthorized access

   Session hijacking

   Information disclosure

RECOMMENDED REMEDIATION ACTIONS

- Upgrade the unsupported Unix OS version.
- Disable rlogin service and switch to SSH.
- Secure Xserver with proper configurations.
- Regularly update software and services.
- Implement network segmentation and access controls.
- Conduct regular security assessments.
- Provide training on secure practices.

These actions will help mitigate the identified vulnerabilities and enhance the overall security of the system.

CONCLUSION & RECOMMENDATIONS

In conclusion, the network scan using Nmap and vulnerability assessment using Nessus on Metasploitable 2 identified several vulnerabilities. It is crucial to address these vulnerabilities promptly to enhance the security posture of Metasploitable 2. The report concludes with recommendations for improving the security posture of Metasploitable 2, including implementing the recommended remediation actions and regularly conducting vulnerability assessments.

TEAM MEMBER'S

1. Jay
2. Niyati
3. Pawan
4. Aditya
5. Jiyanshu
6. Aasif Sudiwala
7. Mrunal
8. Piyush
9. Harsh
10. Prathamesh
11. Shubham
12. Ahmed
13. Ayaan
14. Prince
15. Kirti
16. Omkar
17. Sampada
18. Anubhav
19. Sakshee Jaiswal