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

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 vunerabilities. Penetration Testing has done within a controlled virtual environment with the vulnerable applications.

- ***Environment***
  - *Kali Linux-202(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

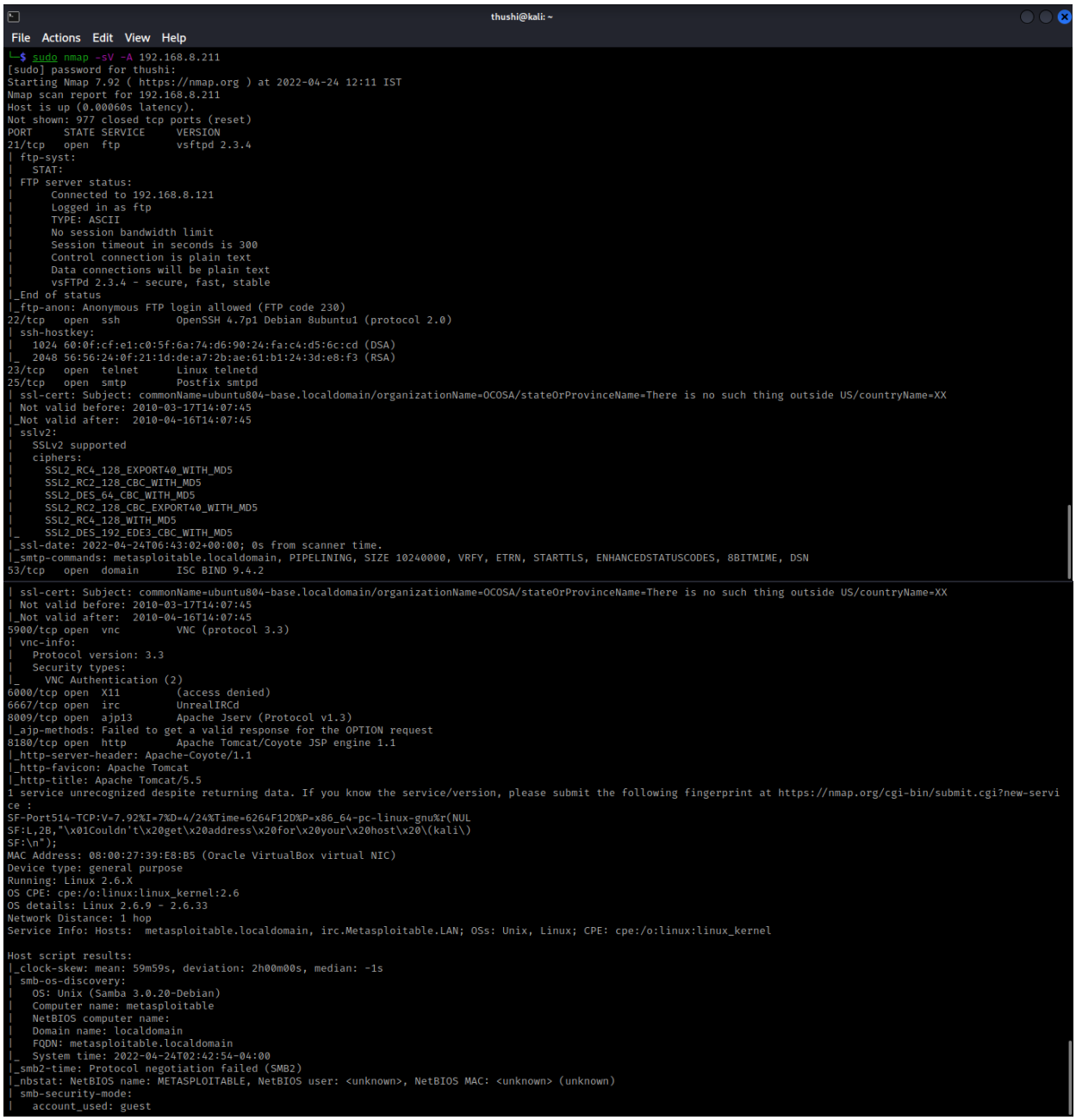
3.1. Nmap

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

Figure 2 : Nmap scan results of OWASP Virtual Machine

$ sudo nmap -sV -A 192.168.8.211



```
| 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      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-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: 24
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase, Support41Auth, SupportsCompression, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag
|   Status: Autocommit
|_  Salt: }m+*4f66/VF:1'mrvvpP
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-servi
ce :
SF-Port514-TCP:V=7.92%I=7%D=4/24%Time=6264F12D%P=x86_64-pc-linux-gnu%r(NUL
SF:L,2B,"\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: 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
```

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

┌──(thushi㉿kali)-[~]
└─$ sudo nmap -traceroute 192.168.8.211
[sudo] password for thushi:
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 (0.00071s 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  ccproxy-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
8180/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 Metasplitable 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.

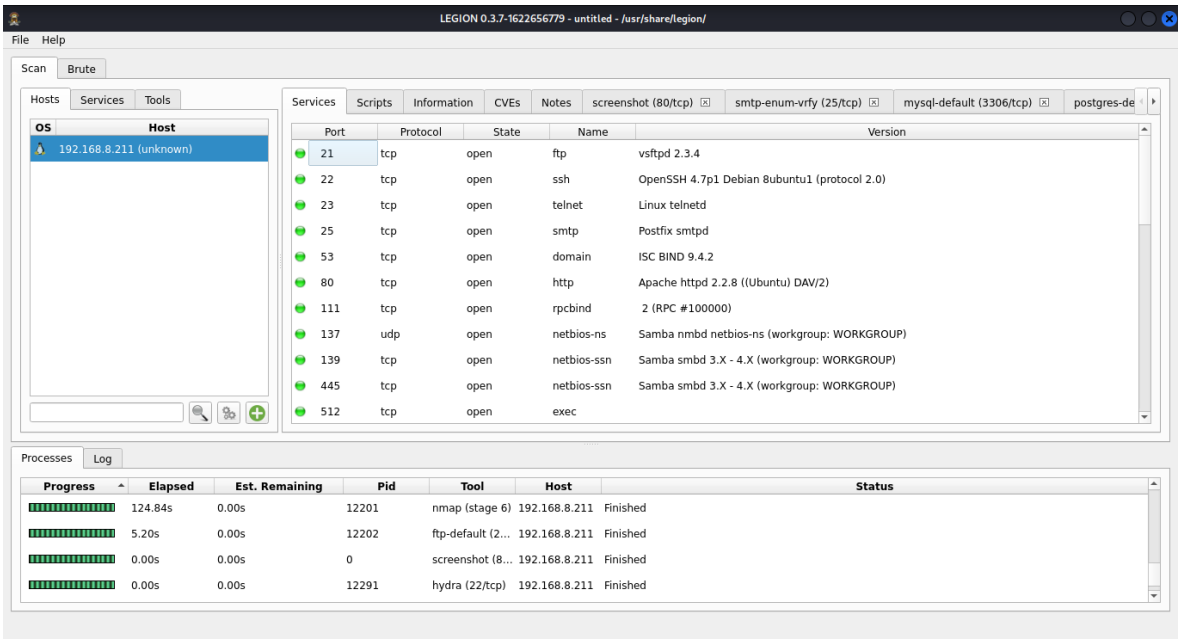


Figure 5 : Legion Scan Results of Metasploitable 2 VM

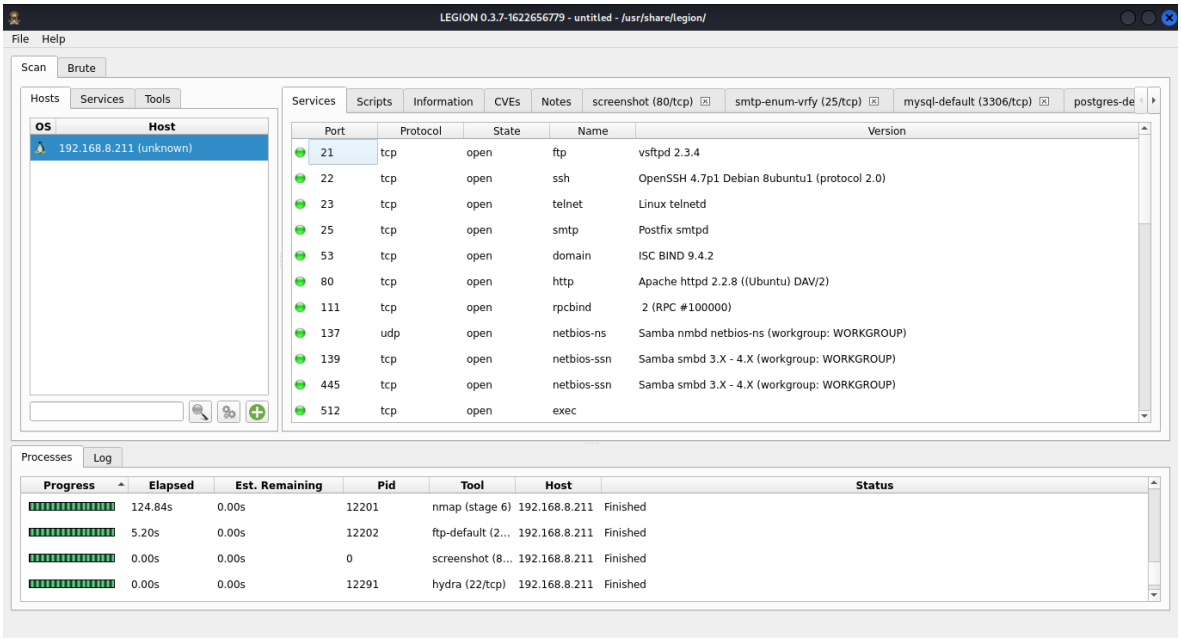


Figure 6 : Legion Scan Results of OWASP BWA VM

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

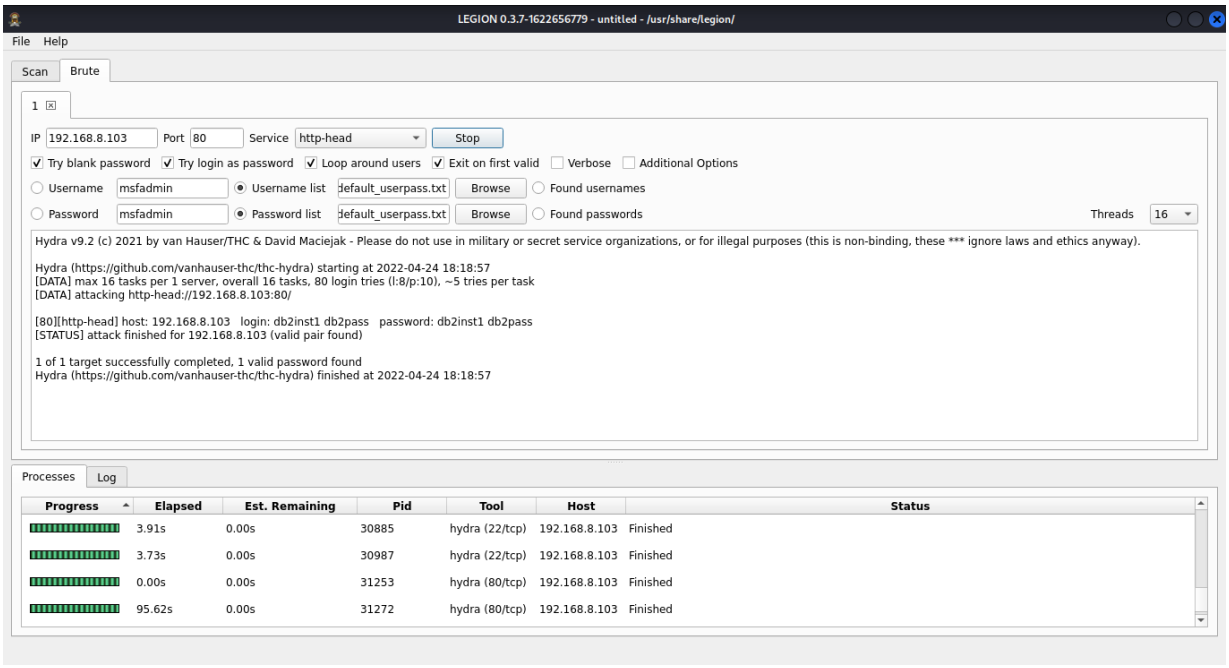
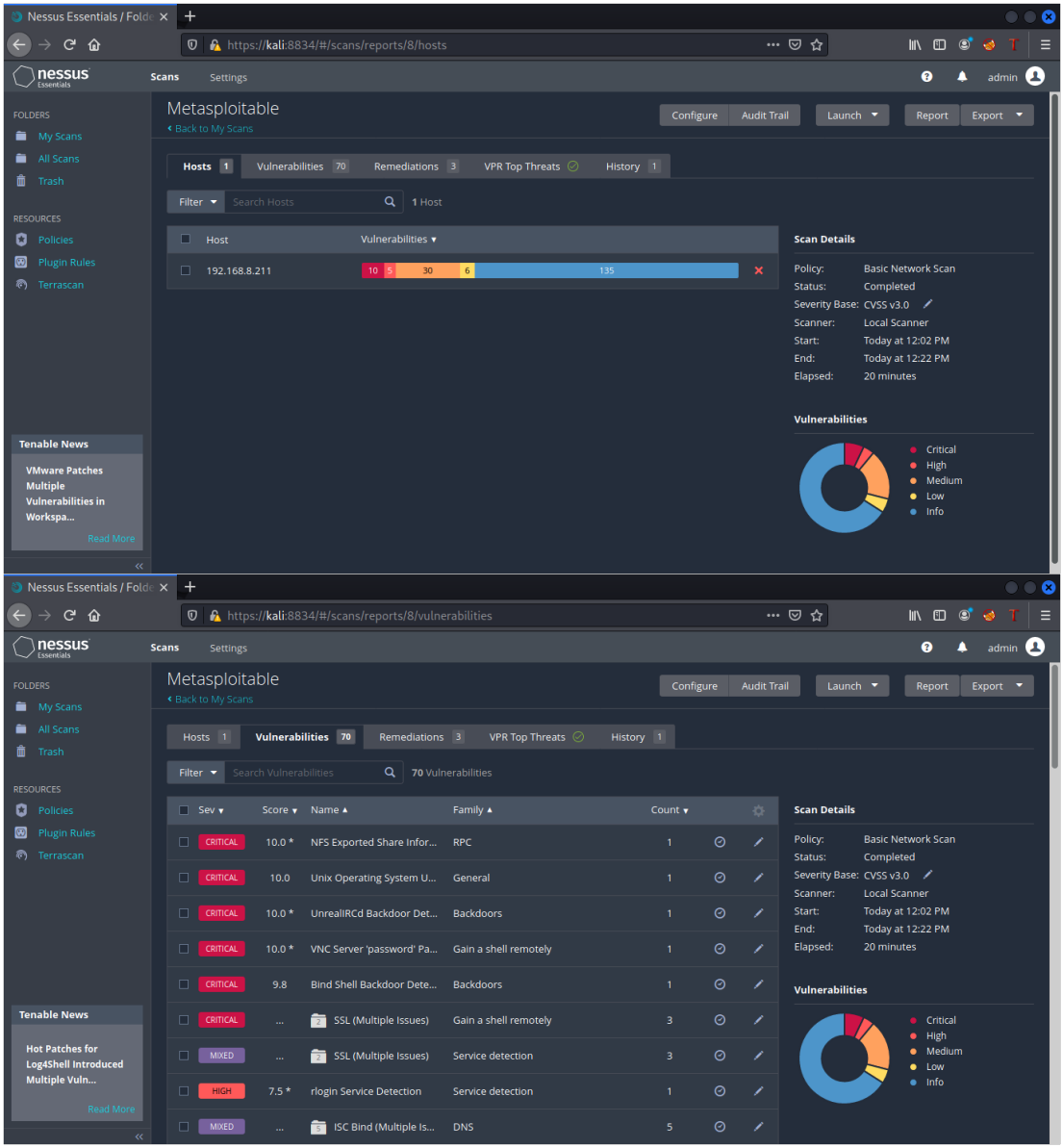


Figure 7 : http-header login credientials

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.



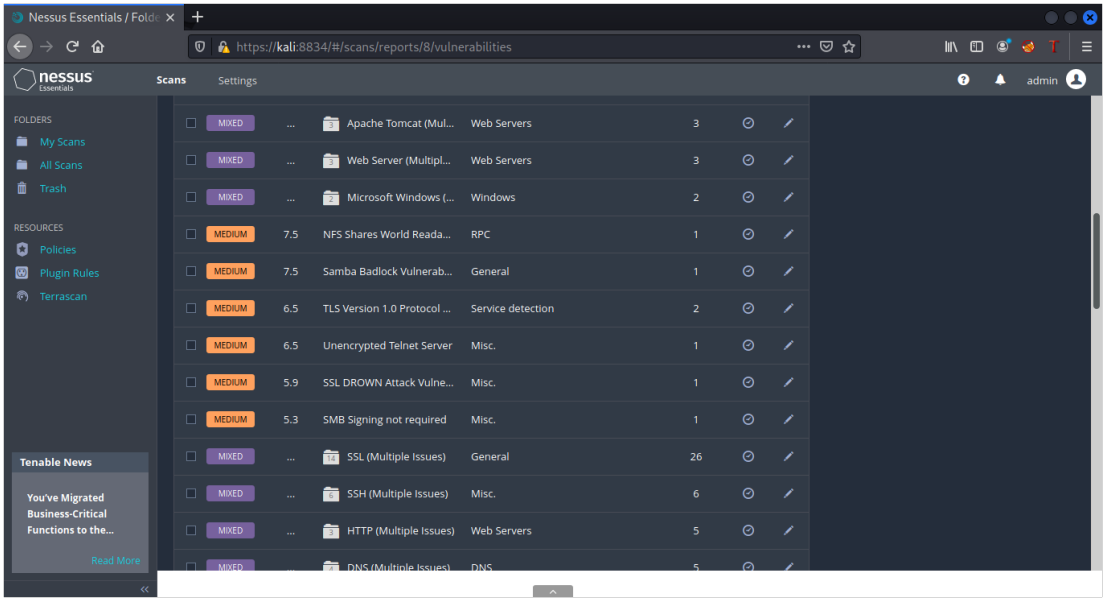


Figure 8 : Nessus Scan Results of Metasploitable

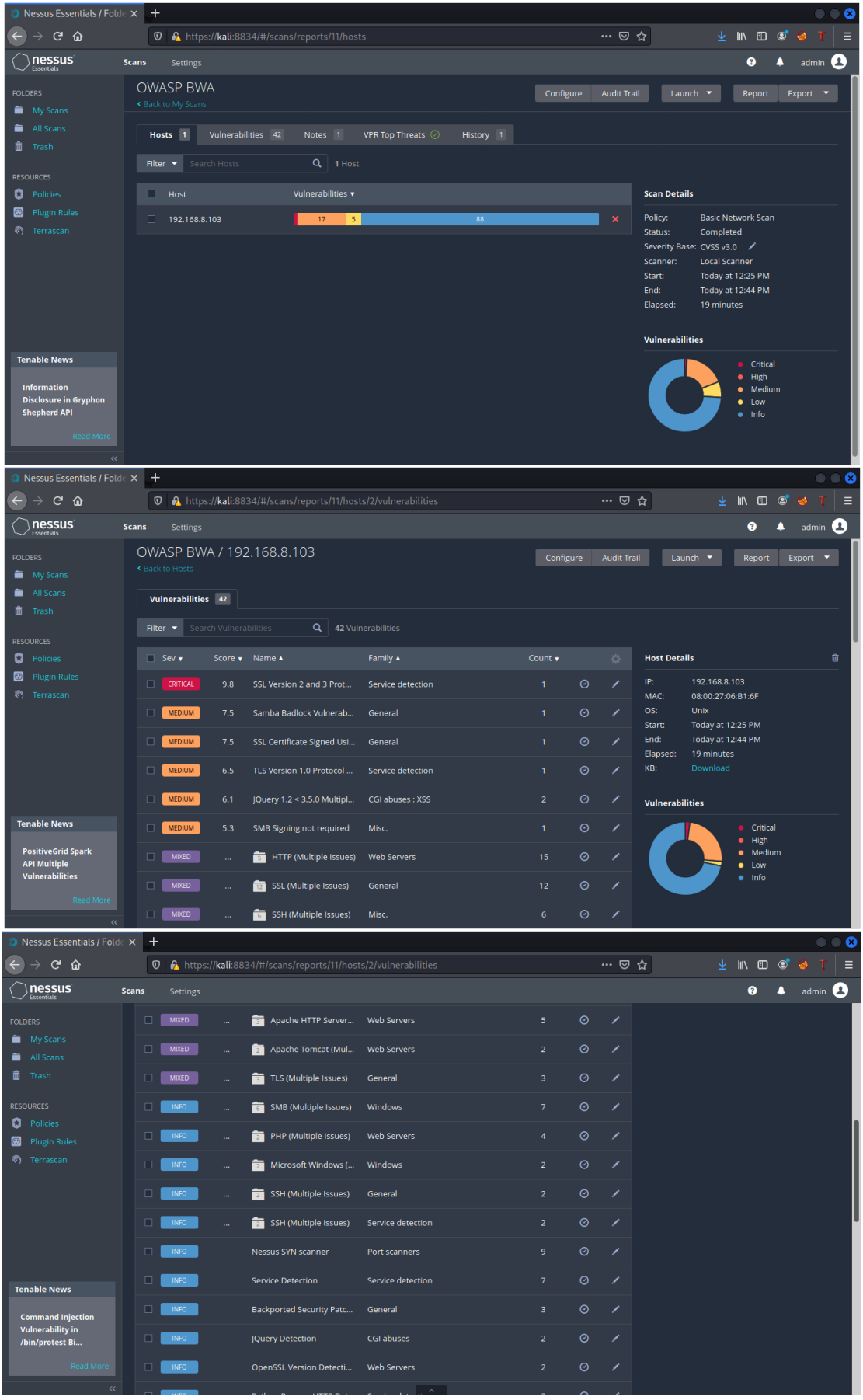


Figure 9 : Nessus Scan result for OWASP BWA VM

4. Vulnerability Analysis, Exploitation and Mitigation

4.1. Exploit openSSH Random Number Generator weakness – Metasploitable 2

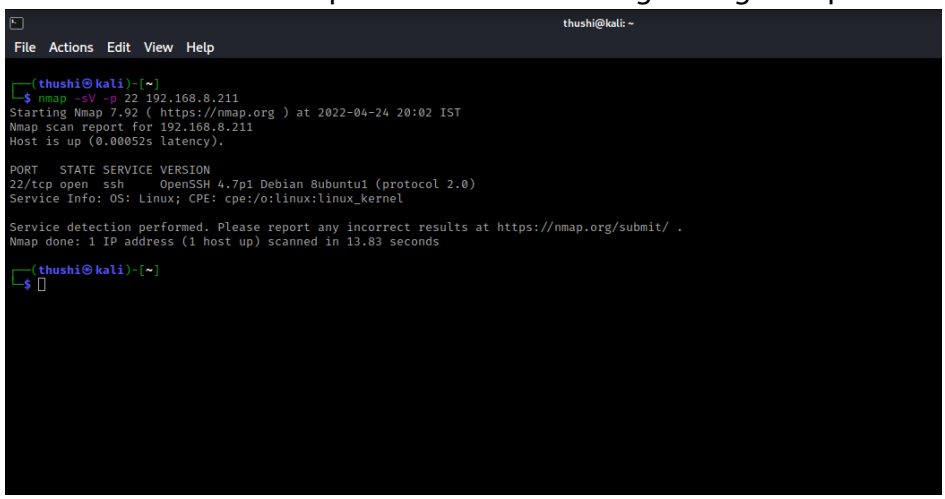
Severity – **Critical**

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.

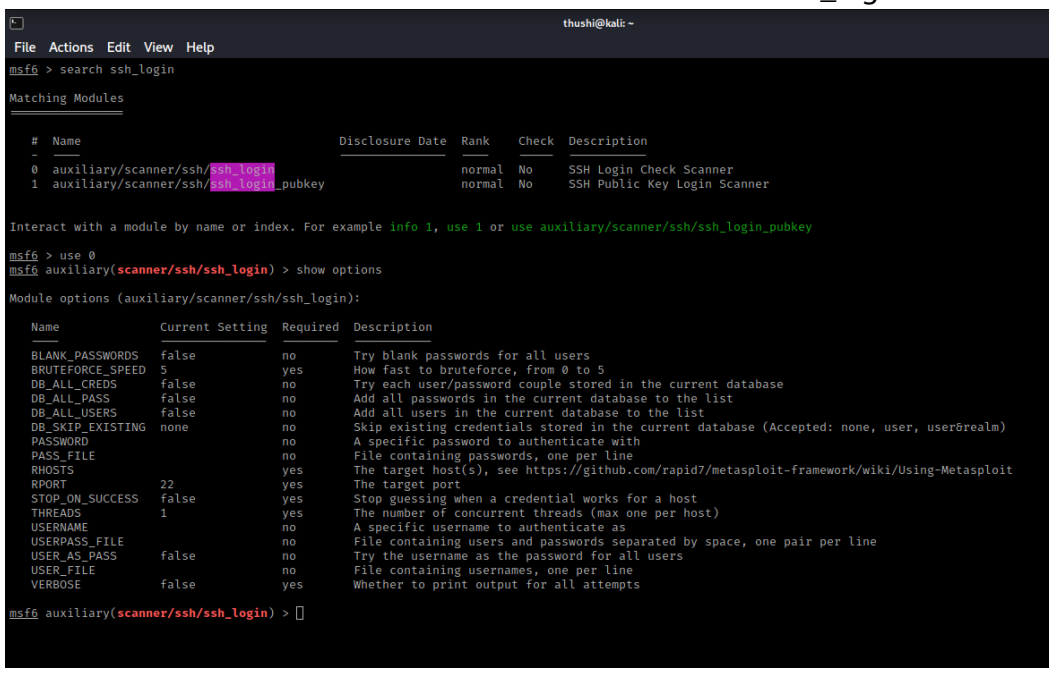
Solution **-** Consider all cryptographic material generated on the remote host to be guessable. All SSH, SSL and OpenVPN key material should be re-generated.

Exploitation –

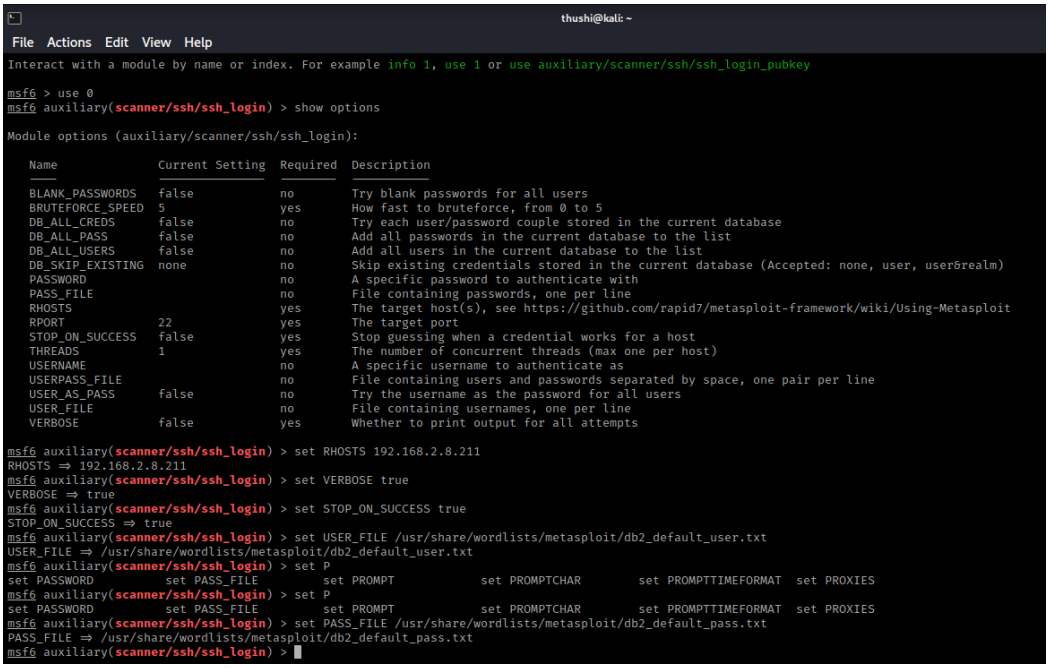
- Find the version of the open SSH service running through the port.



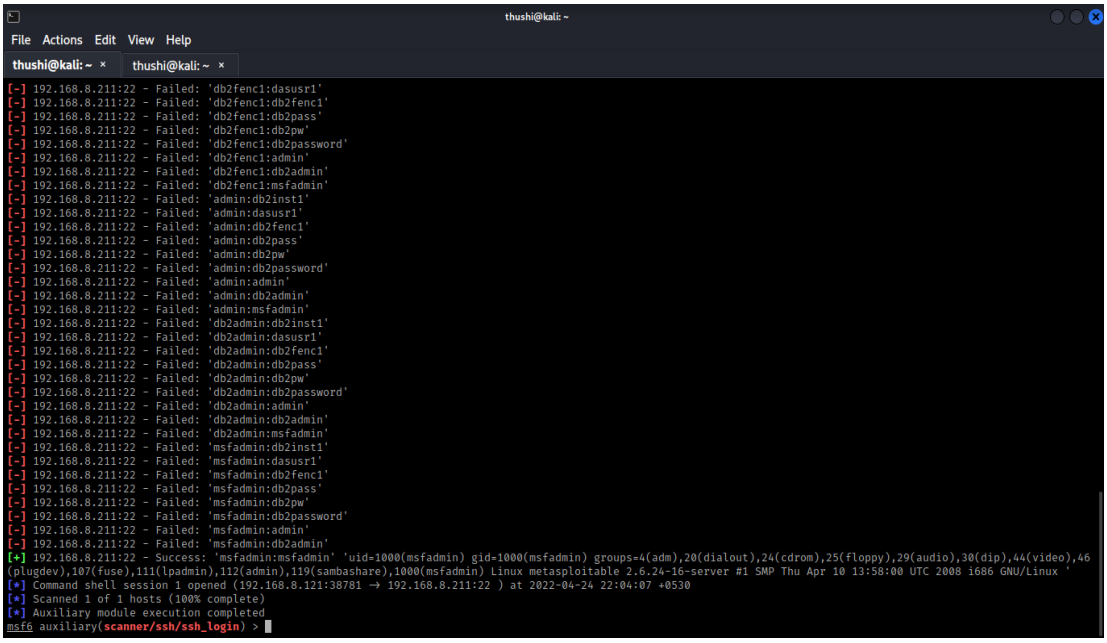
- The red team launched the msfconsole and search for the ssh_login module.



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



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



- 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

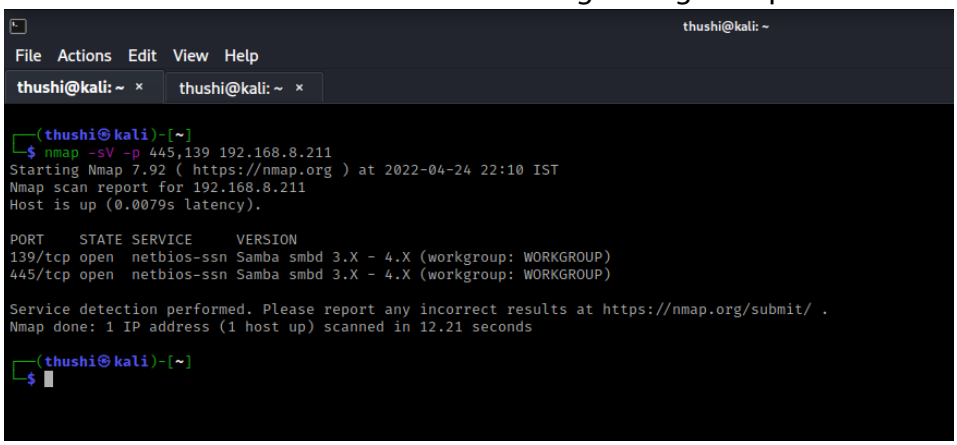
Severity – **High**

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.

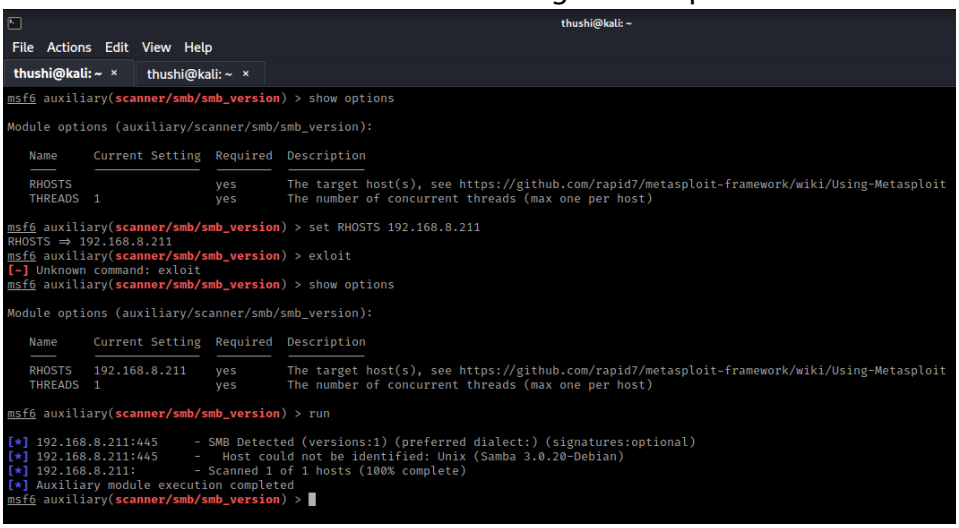
Solution – Upgrade to Samba Version 4.2.11 / 4.3.8/ 4.4.2 or later.

Exploitation –

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



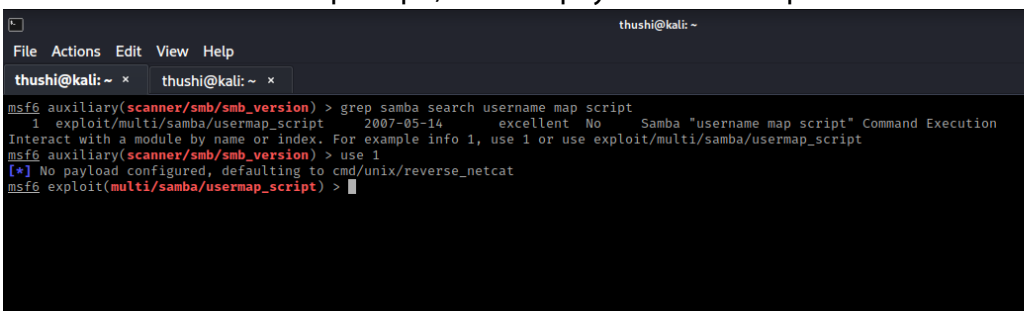
- Launch the msfconsole and search through the modules and auxiliary scanners available for the SMB service. Then, an auxiliary scanner. After setting the necessary options, the auxiliary scanner was launched. Result yielded and re-affirmed version of SMB service running on both port 139 and 445.



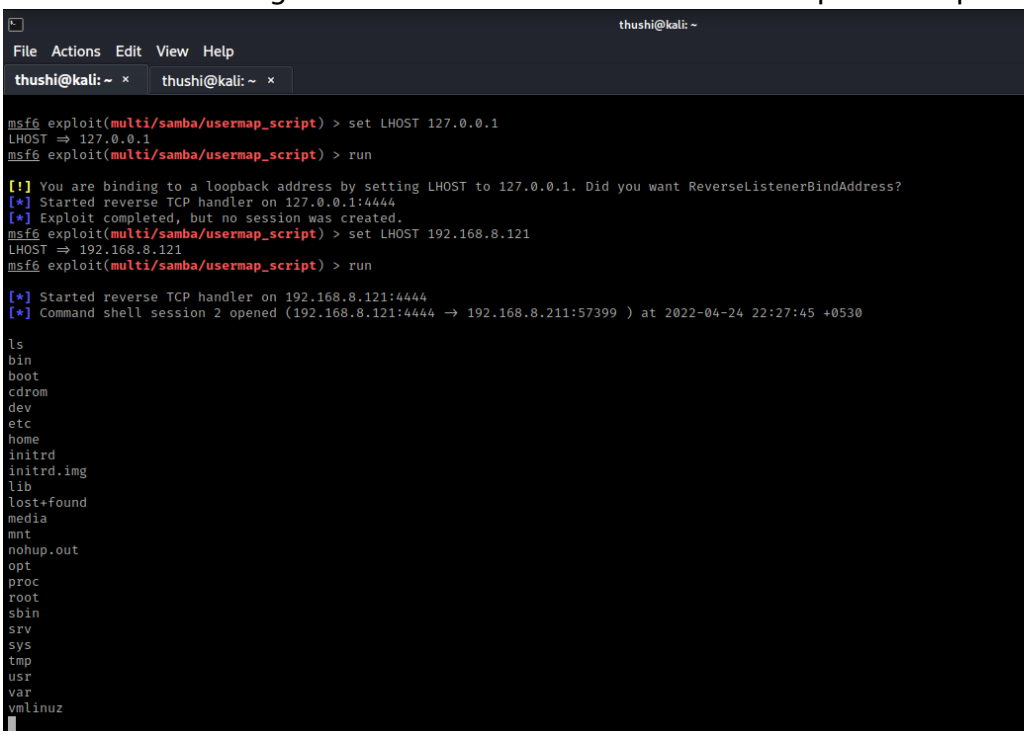
- Next step is to identify the matching exploits for the current samba version. And there are two exploits found.

```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)          | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
```

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



- 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.



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*

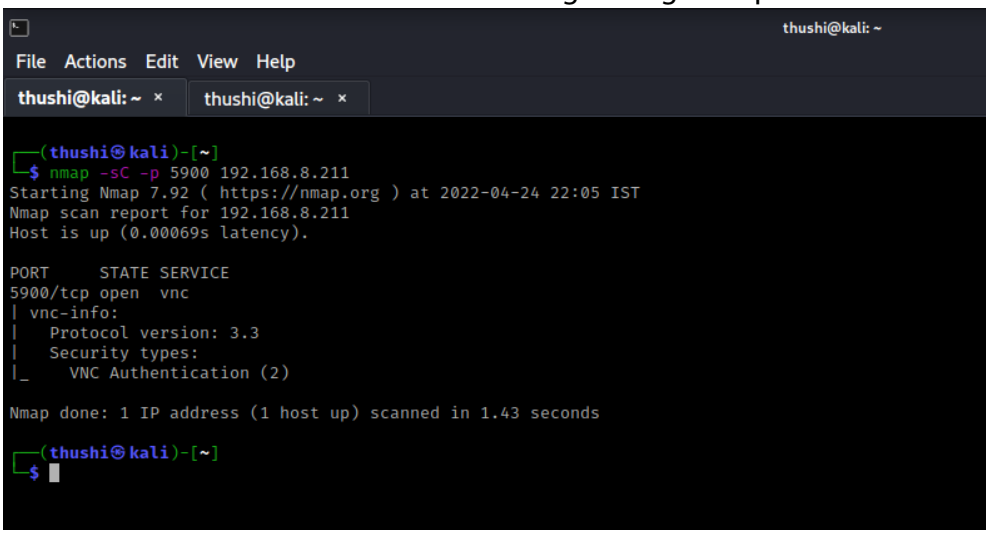
Severity – **Critical**

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.

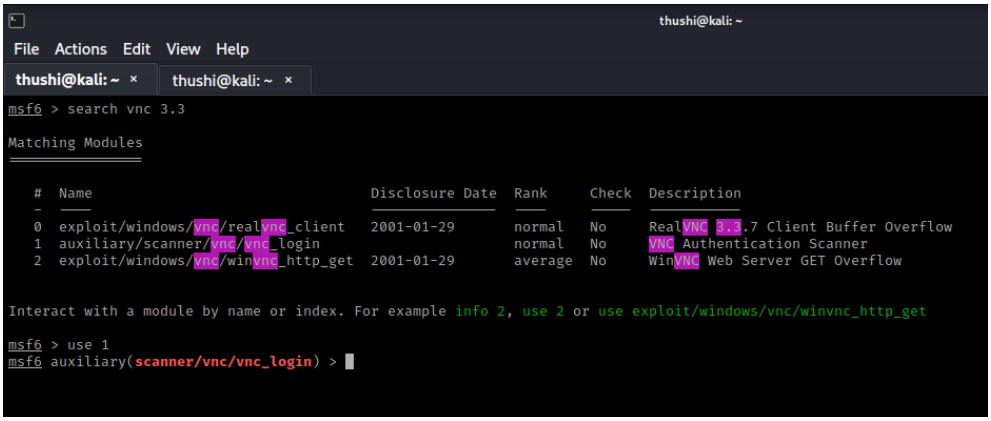
Solution - Use Strong password pattern mechanism to secure the VNC service.

Exploitation –

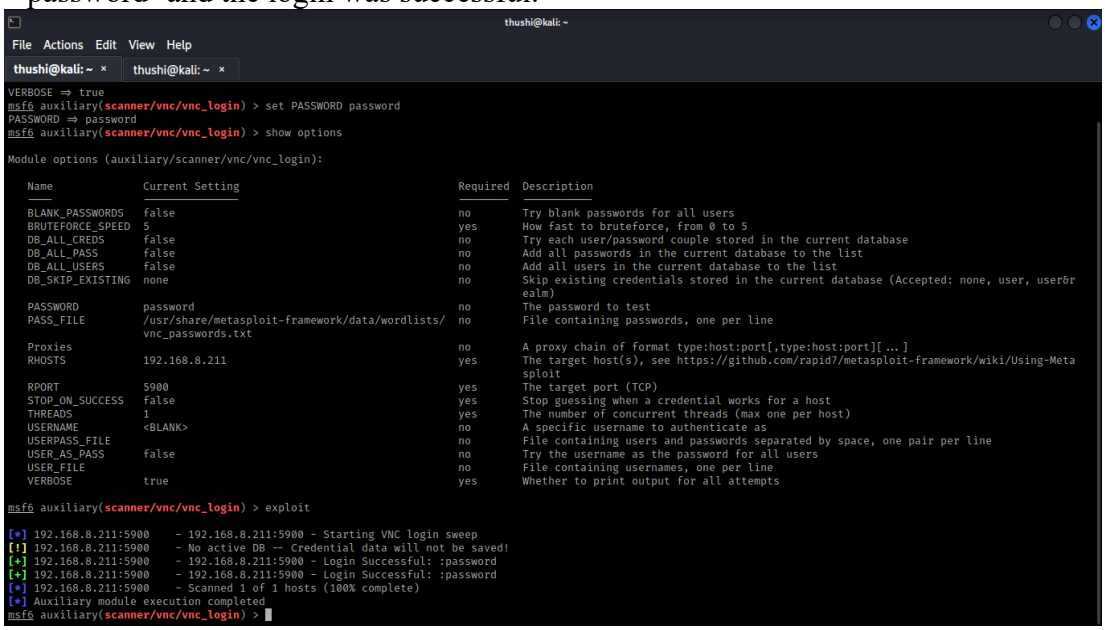
- Find the version of the VNC service running through the port.



- 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.



- 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.



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.