Sri Lanka Institute of Information Technology

Penetration Testing Report- Assignment 02

IE3022– Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT 20228880	K.K.K.P.Kumara

Table of Contents

Executive Summary

Wayne Industries hired the SecureX security team to conduct an extensive penetration test on their systems in order to identify any weaknesses or vulnerabilities that could be exploited by cybercriminals. The Penetration Testing was carried out by simulating a real-world attack scenario against the Wayne Industrial Corporation. The team responsible for penetration testing was divided into three groups: the Red Team, the Blue Team, and the Purple Team. The Red Team was in charge of identifying system vulnerabilities and launching attacks against those vulnerabilities that were discovered. In order to assess the Red Team's attacks, their business impact, and the resilience of current controls to such attacks, the Blue Team was tasked with performing an analysis of the attacks. It was the Purple Team's responsibility to keep track of the entire pen testing process, making recommendations and verifying the defensive controls proposed by the Blue Team against the vulnerabilities discovered. The primary objectives of the penetration testing were to determine, among other things,attacks on Wayne Industries' critical infrastructure and the effectiveness of the company's existing defensive controls against attacks. the impact of attacks on Wayne Industries' sensitive data confidentiality, availability of information systems, and other critical infrastructure.

The penetration testing was done out from a black-box viewpoint, with just the general user access level to Wayne Industries' local area network (LAN) being provided. After scanning the local area network of the Wayne Industries Group, the Red Team discovered and targeted two Vulnerable Applications/Systems that were in use inside the Wayne Industries Group. Two virtual computers in the virtual box were considered to be two targeted applications/systems of the Wayne Industries group and were used in the simulation.

Targeted Virtual computers are ,

1. Metaspoitable machine
2. OWASP BWA machine

In this case, it was presumed that the evaluation was carried out in accordance with the guidelines given in NIST SP 800-115. Aside from that, the following industry-standard tools were used for information collecting, vulnerability analysis, and exploitation of Critical Vulnerabilities.

Used tools for the Assessment

- Nmap Scanner : Used for Reconnaissance, Network and Ports Scanning, An open-source program for network scanning and discovery, Nmap stands for Network Mapper. Network administrators use Nmap to discover what devices are operating on their systems, locate open ports, and uncover security threats.

- Angry IP Scanner : Used to Scan the Network and detect live hosts. It's a highly quick IP address and port scanner called Angry IP scanner It is capable of scanning any IP address range and any associated port. It may run on a variety of operating systems and is quite little in size. It may be copied and used elsewhere without the need for installation.

- Nessus Scanner : Network security scanning tool Nessus examines a computer and issues an alert if it detects any vulnerabilities that malevolent hackers may exploit in order to obtain access to any other machine on the network to which it has been connected.

The identified vulnerabilities at Wayne Industries were classified based on the severity grading methodology obtained from the CVSS score. A total of 04 categories have been identified as risk factors for vulnerabilities.

Critical Vulnerabilities

Because the attacker does not need any prior knowledge about the victim, exploiting this sort of vulnerability is simple. Exploitation might result in a root-level breach as well as a significant loss of data. This sort of vulnerability necessitates the use of an urgent solution or patch.

High

This sort of vulnerability is tough to take advantage of and attack. Exploitation may result in privilege escalation as well as partial or complete exposure of information. exploitation Countermeasures and enhancements must be implemented immediately.

Medium

In order to properly exploit this sort of vulnerability, the attacker must be located on the same local area network as the victim. Limited access to sensitive information might be provided as a result of exploitation. It is not necessary to apply patches right away.

Low

When it comes to organizational operations, this form of vulnerability provides minimal danger. It is necessary to have physical access in order to attack this sort of vulnerability.

This classification of vulnerabilities assisted the blue team in identifying and allocating more attention to vulnerabilities with the highest risk levels. As a result, in order to make the best possible use of available resources, the blue team's vulnerability analysis and defensive measures were primarily focused on high- to critical-level vulnerabilities.

The values of danger, consequence, and vulnerability combine to form the concept of risk. The goal of risk management is to provide a degree of protection that reduces vulnerabilities to threats and the possible repercussions of those threats, so lowering the level of risk to an acceptably low threshold. It is possible to quantify risk using a number of mathematical models, and to see the influence of increasing preventive measures on the risk equation by using different models.

Summary of Methodology

Red team was responsible for conducting network and application evaluations, both inside and outside the Wayne Industries. First They wanted to identified IP addresses of the network ,After that red team could identified two live systems were running in the network,Two remote targeted systems could be identified as Metaspoitable and OWASP BWA.After identifying these ,team had to use Nmap scans on each targeted systems for enumerate the running services on systems, Operating Systems on each and Nmap scans helped to get more information about open and closed ports. As part of their analysis of the target system, the red team was able to identify certain potentially susceptible services that were operating on system ports.

The vulnerability analysis performed using the Nessus scan assisted in reaffirming and highlighting the most severe vulnerabilities of two targeted systems, which were previously identified. The results of the Nessus scan report highlighted the vulnerabilities of the targeted systems, which were ranked according to their relative risk level. Vulnerabilities identified by red team and blue team were analyzed them as well as purple team got the mitigations for them.

Methodology

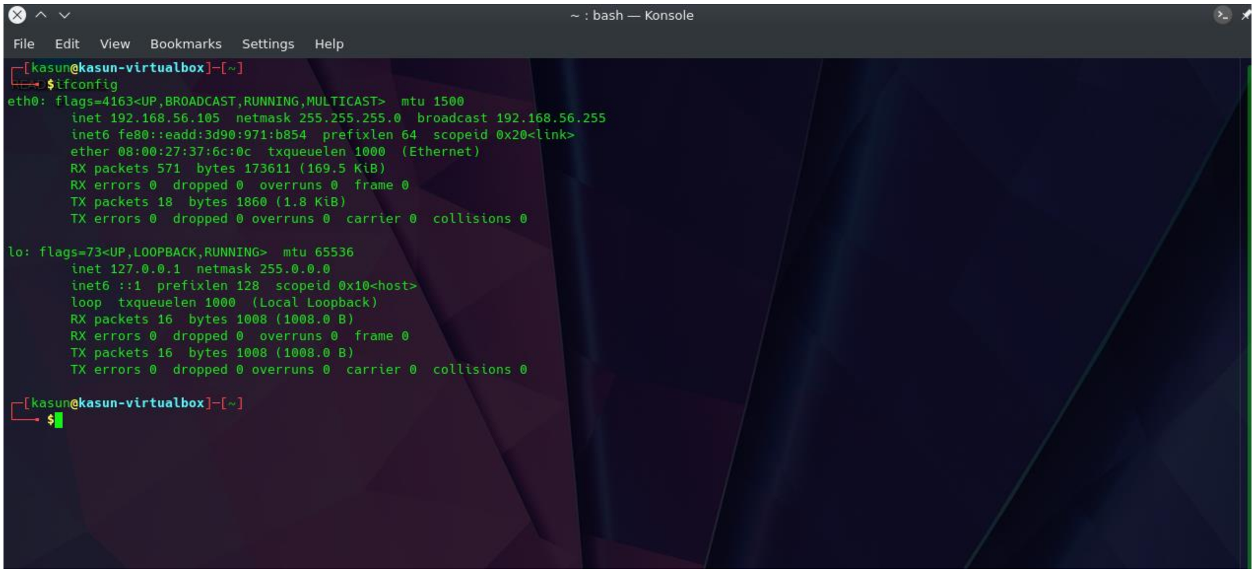
Footprinting and Reconnaissance

The red team did not have any previous knowledge of the targeted systems or applications of Wayne Industries since the penetration testing methodology was carried out from a black-box viewpoint. They had to start from the very beginning of the project. Consequently, they used a step-by-step strategy similar to an external attacker to gather knowledge on the host systems they were targeting. During the Footprinting Process, the red team made use of network scanning and enumeration tools such as Nmap and Angry IP Scanner.

Nmap Scans for Gathering Information

An open-source program for network scanning and discovery, Nmap stands for Network Mapper. Network administrators use Nmap to discover what devices are operating on their systems, locate open ports, and uncover security threats. Red team had to use Nmap for gather information such as Operating systems ,ports ,services which running on systems of Wayne Industries .

First step is ,The **ifconfig** command was used by the red team to determine the IP address of the Wayne Industries Local Area Network. The IP address of the Wayne LAN that was discovered was 192.168.56.105.



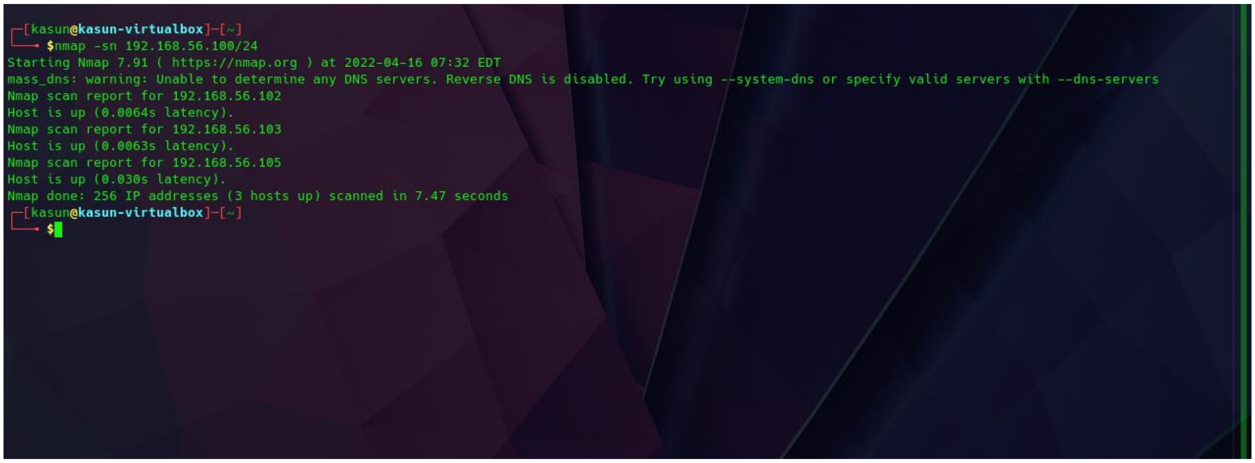
```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.105  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::eadd:3d90:971:b854  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:37:6c:0c  txqueuelen 1000  (Ethernet)
        RX packets 571  bytes 173611 (169.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1860 (1.8 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 16  bytes 1008 (1008.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 1008 (1008.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌─[kasun@kasun-virtualbox]─[~]
└──╼ $
```

Figure 1 Ip address of Wayne Lan

Second Step : Red team wanted to identify devices which connected to Wayne Local Area Network.For that They carried out a Nmap scan in order to identify any active hosts or systems that were linked to the neTwork. The IP addresses of two linked systems / hosts were retrieved as a result of the scan. The IP addresses of two systems that have been found are 192.168.56.102 and 192.168.56.103.



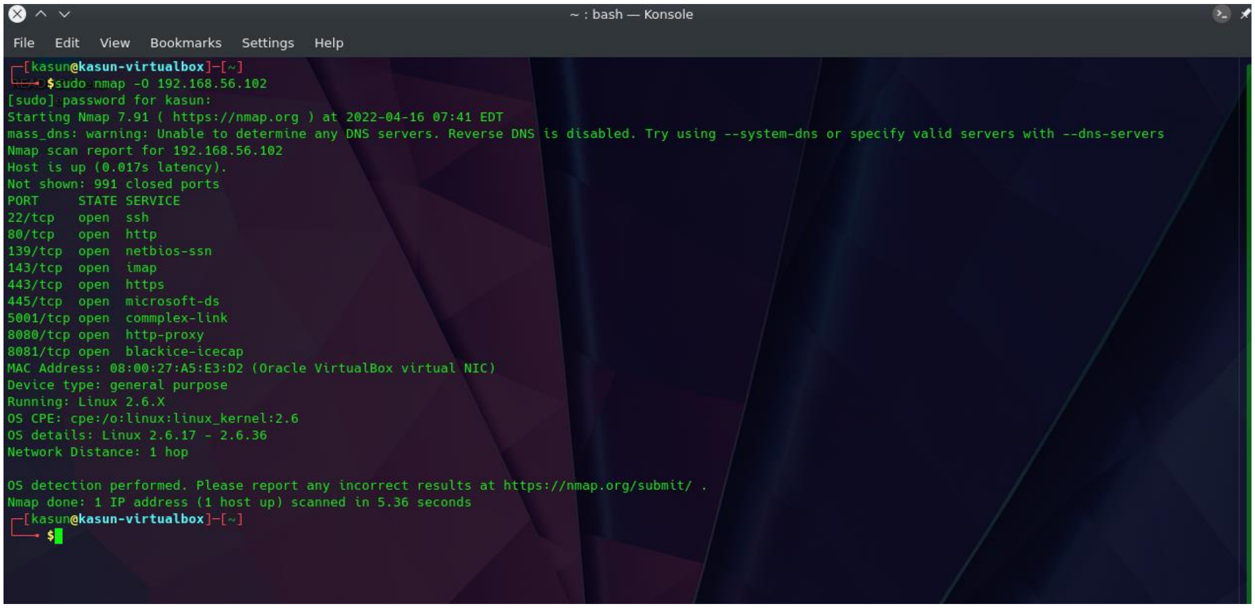
```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $nmap -sn 192.168.56.100/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 07:32 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0064s latency).
Nmap scan report for 192.168.56.103
Host is up (0.0063s latency).
Nmap scan report for 192.168.56.105
Host is up (0.030s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 7.47 seconds
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $
```

Figure 2 Seaeching Ip addresses which connected to network

Despite the fact that the IP addresses of two host systems were discovered, this information was insufficient for the exploitations. A greater amount of information regarding these two systems was requested by the Red team. To obtain information on the operating system, host names, and services that were running on these two linked computers, they performed another version of the nmap scan. Metasploitable 2.0 and Owaspbwa were the host names of the two targeted systems, respectively. The team discovered that Linux was the operating system running on both of the linked PCs once the scan had been completed and analyzed. Additionally, the results of the scan showed information on the open ports and the services that were operating on them. The material that was made public gave more compelling proof in support of the red team assault. The number of very essential ports such as FTP, SSH, and SMTP that were open on each of the targeted host systems was significant. This information served as an excellent starting point for the red team's attacks on two target systems.

For get more information such as port details (open ports),services regarding identified 1st ip address

192.168.56.102 by using advanced Nmap scan.

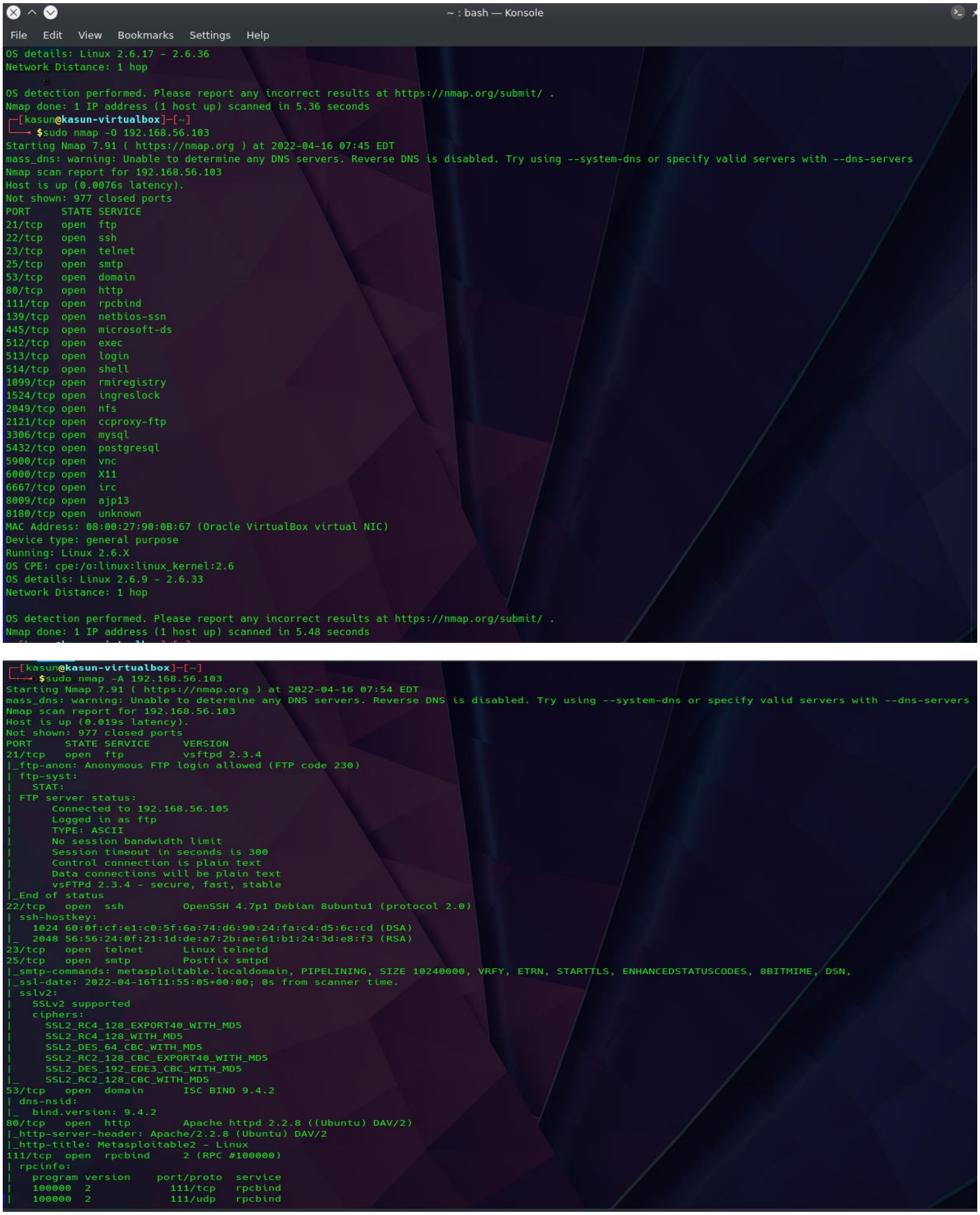


```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $sudo nmap -O 192.168.56.102
[sudo] password for kasun:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 07:41 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.017s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:A5:E3:D2 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $
```

Figure 3 nmap results of owasp bwa machine

After that need to same scan for 2nd Identified IP address 192.168.56.103



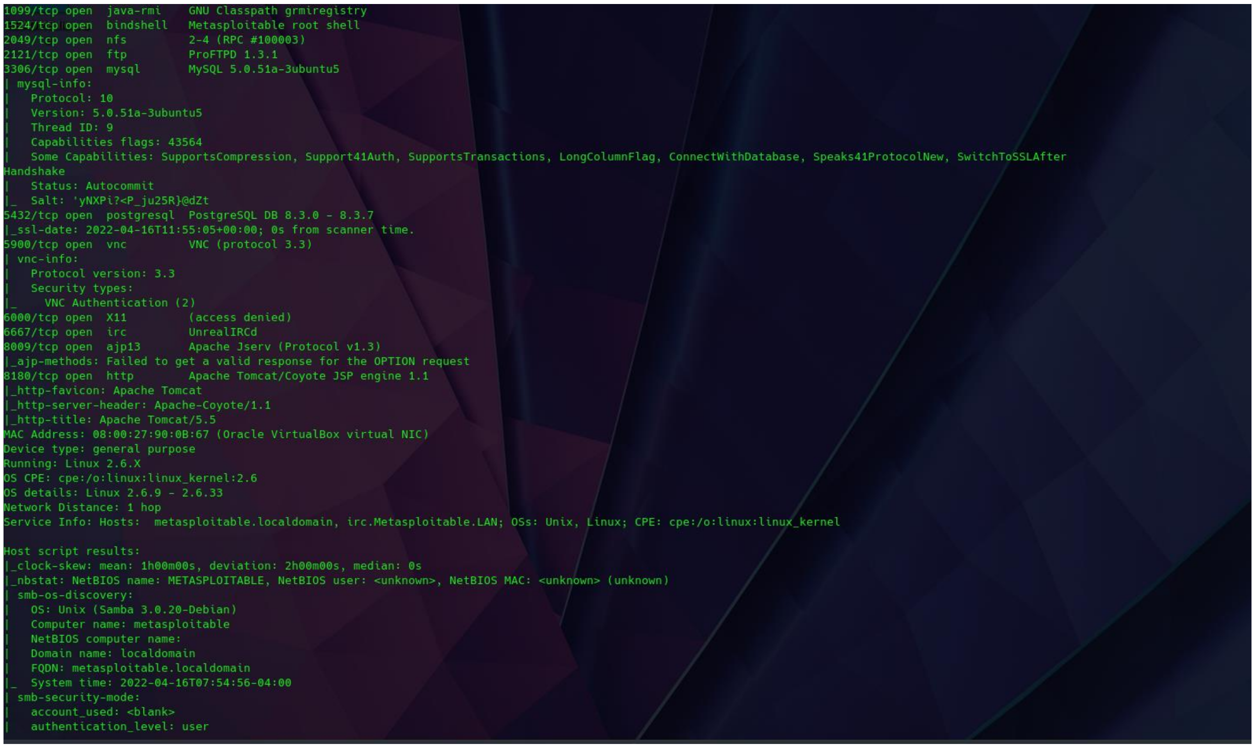
```
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $sudo nmap -O 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 07:45 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0076s latency).
Not shown: 977 closed ports
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: 08:00:27:90:0B:67 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.48 seconds
```

```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $sudo nmap -A 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 07:54 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.019s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.105
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2022-04-16T11:55:05+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```

Figure 4 nmap results of metaspoitable machine



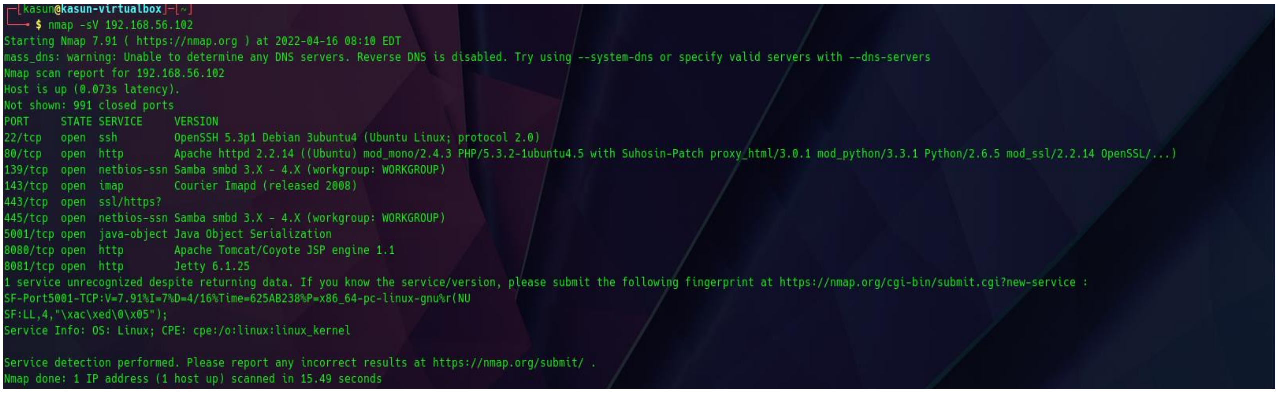
```
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, Support41Auth, SupportsTransactions, LongColumnFlag, ConnectWithDatabase, Speaks41ProtocolNew, SwitchToSSLAfter
Handshake
|   Status: Autocommit
|_  Salt: 'yNXPi?<P_ju25R}@dZt
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-04-16T11:55:05+00:00; 0s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:90:0B:67 (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: 1h00m00s, deviation: 2h00m00s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-04-16T07:54:56-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
```

Using another nmap scan, the red team was able to identify the service version that was executing on the specified ports. An instance is the discovery of a vulnerable service version of vsftpd 2.3.4 operating on port 21 of the metasploitable 2.0 system, which was outdated and susceptible.

The vulnerable samba service version was running on the tcp port 139 on the Owaspbwa system.

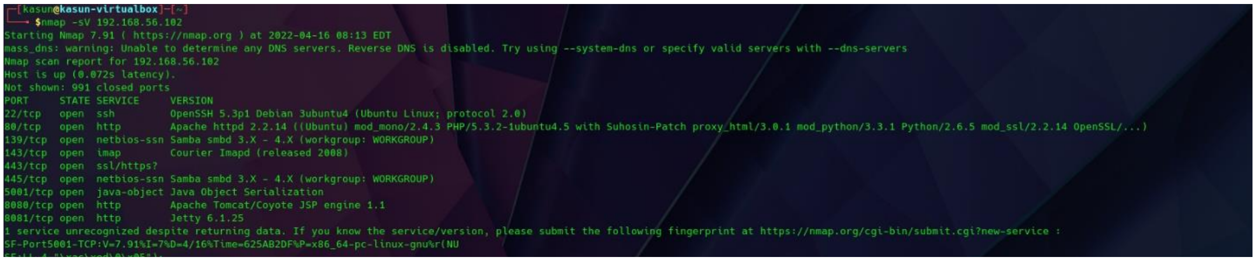
This obtained information provided important proof for the red team, which enabled them to launch their attacks on two systems of Wayne Industries that had been identified as targets.



```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $ nmap -sV 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 08:10 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.073s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
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/...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
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
8081/tcp open  http        Jetty 6.1.25
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:V=7.91%I=7%D=4/16%Time=625AB238%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
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 15.49 seconds
```

Figure 5 Details of service which running on owasp bwa machine



```
┌─[kasun@kasun-virtualbox]─[~]
└──╼ $nmap -sV 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-16 08:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.072s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
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/...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
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
8081/tcp open  http        Jetty 6.1.25
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:V=7.91%I=7%D=4/16%Time=625AB2DF%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
```

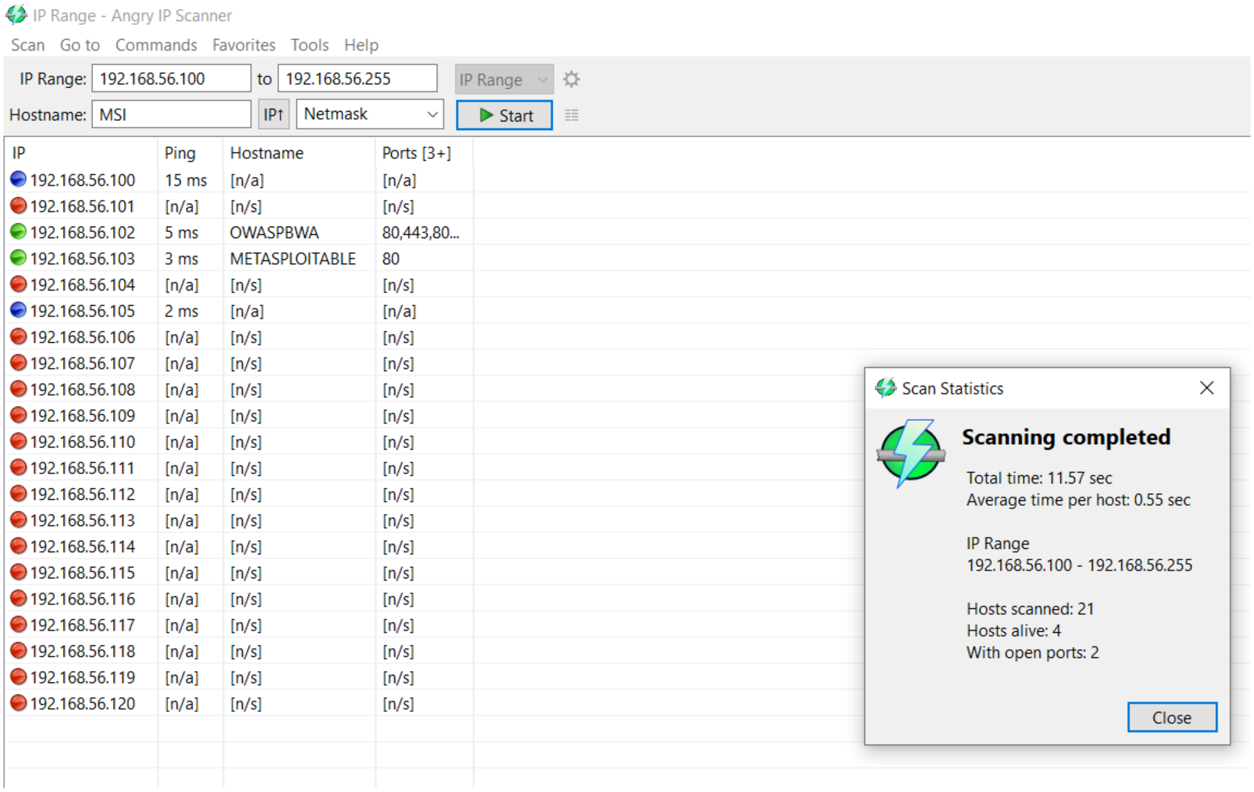
Figure 6 Details of service which running on metaspoitable machine

Scanning with Angry Ip scanner for gather information

In order to validate the findings of Nmap scan, red team applied open-source Angry IP Scanner tool to locate the active host systems in Network range of Wayne Industries and other vital information of connected IP addresses. Angry IP Scanner. After supplying the IP range of Network of Wayne Industries.

The results of the scan indicated the presence of two active host systems and their IP addresses inside ABC's local area network. The

Metasploitable and Owaspbwa were discovered to be running on live computers linked to the ABC network.These pieces of evidence contributed to the verification of the probable targets of the red team's strike.



IP Range: 192.168.56.100 to 192.168.56.255

Hostname: MSI

Netmask

IP	Ping	Hostname	Ports [3+]
🔵 192.168.56.100	15 ms	[n/a]	[n/a]
🔴 192.168.56.101	[n/a]	[n/s]	[n/s]
🟢 192.168.56.102	5 ms	OWASPBWA	80,443,80...
🟢 192.168.56.103	3 ms	METASPLOITABLE	80
🔴 192.168.56.104	[n/a]	[n/s]	[n/s]
🔵 192.168.56.105	2 ms	[n/a]	[n/a]
🔴 192.168.56.106	[n/a]	[n/s]	[n/s]
🔴 192.168.56.107	[n/a]	[n/s]	[n/s]
🔴 192.168.56.108	[n/a]	[n/s]	[n/s]
🔴 192.168.56.109	[n/a]	[n/s]	[n/s]
🔴 192.168.56.110	[n/a]	[n/s]	[n/s]
🔴 192.168.56.111	[n/a]	[n/s]	[n/s]
🔴 192.168.56.112	[n/a]	[n/s]	[n/s]
🔴 192.168.56.113	[n/a]	[n/s]	[n/s]
🔴 192.168.56.114	[n/a]	[n/s]	[n/s]
🔴 192.168.56.115	[n/a]	[n/s]	[n/s]
🔴 192.168.56.116	[n/a]	[n/s]	[n/s]
🔴 192.168.56.117	[n/a]	[n/s]	[n/s]
🔴 192.168.56.118	[n/a]	[n/s]	[n/s]
🔴 192.168.56.119	[n/a]	[n/s]	[n/s]
🔴 192.168.56.120	[n/a]	[n/s]	[n/s]

Scanning completed

Total time: 11.57 sec
Average time per host: 0.55 sec

IP Range
192.168.56.100 - 192.168.56.255

Hosts scanned: 21
Hosts alive: 4
With open ports: 2

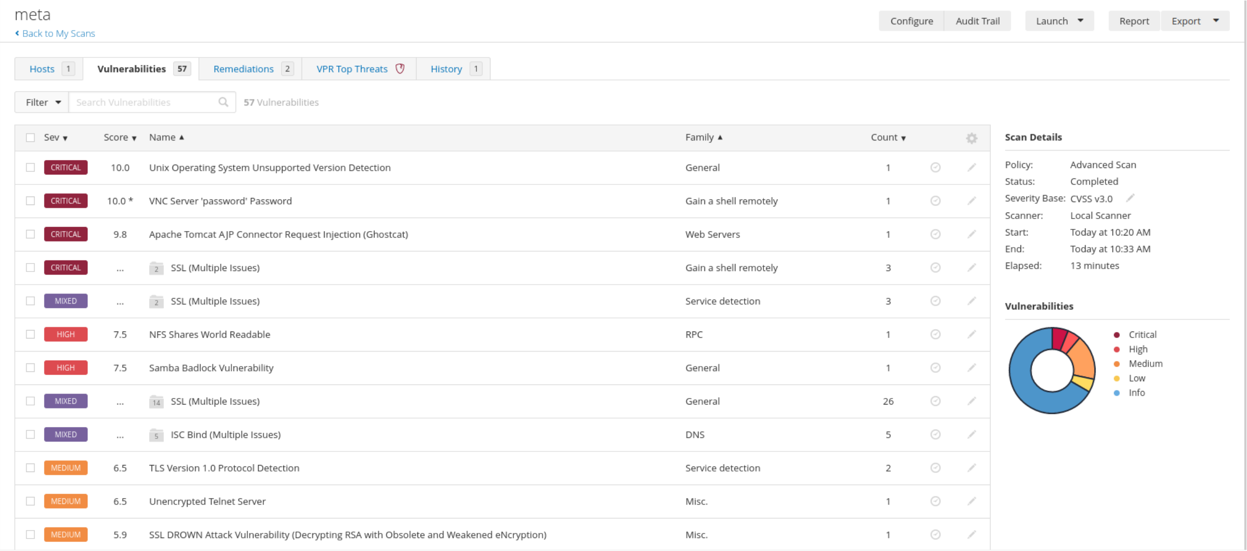
Figure 7 angry Ip scanner results which search of 192.168.56 Ip range

Vulnerability Analysis and Mitigation

After foot printing ,Red team were launching vulnerability assessment and attacks against the Wayne network as well as Blue team analyze red team's attacks and determine the readiness of the company to such attacks. Vulnerability is a fault or weakness in a computer system which gives rise to the threats for hackers to exploit. The exploitation of system vulnerabilities would damage the CIA of information systems and other key infrastructures.

After determining that two active systems of the Wayne Industry firm were vulnerable to being attacked, members of the red team began the process of identifying, categorizing, and defining vulnerabilities in the metasploitable and owaspbwa domains. Following the conclusion of the vulnerability study, the red team performed the exploitation of the critical level vulnerabilities that had been discovered. Following the Exploitation, the Blue team was tasked with determining the business impact and effectiveness of the newly implemented security procedures. The Purple team then offered the suggestions and enhancements that were required to fix the vulnerabilities of two associated systems, which were then implemented.

Using the Nessus Vulnerability scanner, the Red Team was able to identify and assess potential vulnerabilities in the Metasploitable and Owaspbwa live host systems in wayne network. Following the conclusion of the vulnerability scan, the Nessus vulnerability scanner gave a comprehensive list of vulnerabilities, along with a risk assessment for each vulnerability. The following are the vulnerabilities that were discovered in the Metasploitable and Owaspbwa systems.



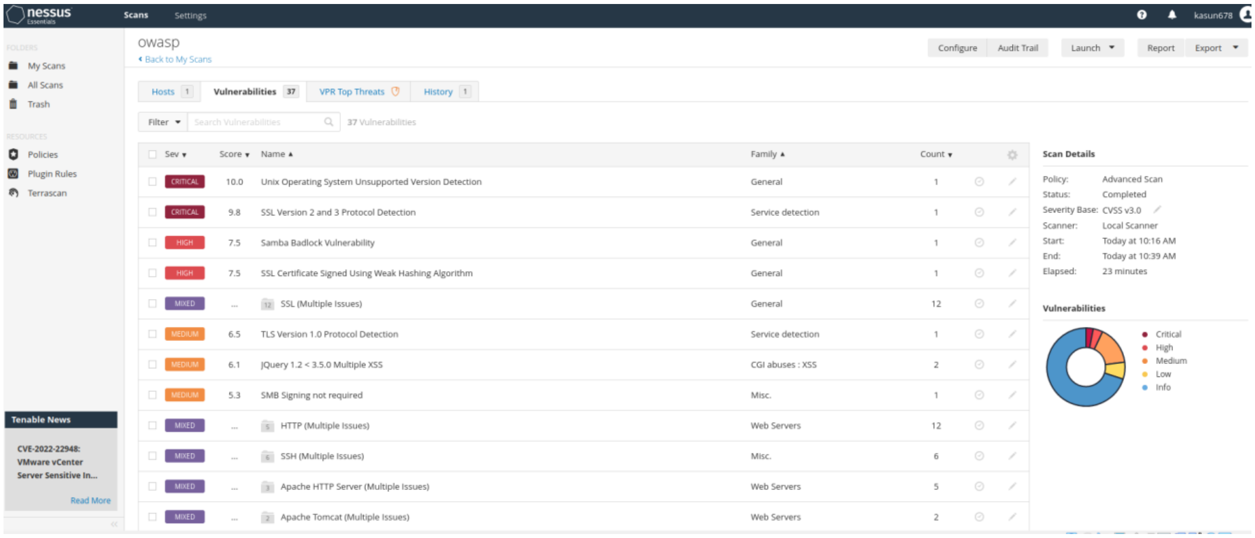
Sev	Score	Name	Family	Count
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	2 SSL (Multiple Issues)	Service detection	3
HIGH	7.5	NFS Shares World Readable	RPC	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	14 SSL (Multiple Issues)	General	26
MIXED	...	5 ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:20 AM
End: Today at 10:33 AM
Elapsed: 13 minutes

Figure 8 Nessus vulnerability report of metaspotable machine

According to Nessus red team identified 4 critical vulnerabilities on metaspoitable system on Wayne Industries.



Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
HIGH	7.5	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MIXED	...	12 SSL (Multiple Issues)	General	12
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	6.1	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	2
MEDIUM	5.3	SMB Signing not required	Misc.	1
MIXED	...	5 HTTP (Multiple Issues)	Web Servers	12
MIXED	...	6 SSH (Multiple Issues)	Misc.	6
MIXED	...	3 Apache HTTP Server (Multiple Issues)	Web Servers	5
MIXED	...	2 Apache Tomcat (Multiple Issues)	Web Servers	2

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:16 AM
End:	Today at 10:39 AM
Elapsed:	23 minutes

Vulnerabilities

Figure 9 Nessus vulnerability report of owasp bwa machine

Next Nessus scan for owasp system in Wayne Industries .The red team identified 02 critical vulnerabilities from that system after getting results from nessus scan.

Identified Vulnerabilities and Mitigations

1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- Severity : Critical
- Description: A file read/inclusion vulnerability in the AJP connection has been discovered. This vulnerability might allow a remote, unauthenticated attacker to access web application files from a vulnerable server by abusing the flaw. An attacker might upload malicious JavaServer Pages (JSP) code to a susceptible server in situations where the host supports file uploads.A range of file formats, as well as the ability to acquire remote code execution (RCE).
- Mitigation : Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

2. OpenSSH/OpenSSL Package Random Number Generator Weakness

- Severity : Critical

- Description: The remote SSH host key was created on a Debian or Ubuntu system that includes a fault in the random number generator of the OpenSSL library, which is used by the system's SSH client. An openSSL packager for the Debian distribution removed practically all sources of entropy from the remote version of OpenSSL, which caused the issue.Obtaining the private portion of the remote key is rather simple, and using it to interpret the remote session or launch a man in the middle attack is relatively simple as well.
- Mitigation : Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

3. VNC Server 'password' Password

- Severity : Critical

- Description: The VNC server operating on the remote machine is protected by a password that is too easy to guess. Nessus was able to log in using VNC authentication and the password 'password', which was provided by the user. An unauthenticated remote attacker might take advantage of vulnerability to gain complete control of the system.

- Mitigation : Secure the VNC service with a strong password.

4. Samba Badlock Vulnerability

- Severity : Medium

- Description: Due to improper authentication level negotiation over Remote Procedure Call (RPC) channels, the version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is vulnerable to a flaw known as Badlock, which exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols. Attackers with the ability to intercept traffic between clients and servers hosting SAM databases can take advantage of this flaw to force a downgrade in authentication level, allowing them to perform 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, as well as disabling critical services.

- Mitigation : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later

5. SSL Certificate Signed Using Weak Hashing Algorithm

- Severity : Medium

- Description: The remote service makes use of an SSL certificate chain that has been signed with a hashing method that is cryptographically vulnerable (e.g. MD2, MD4, MD5, or SHA1). Collision attacks on these signature techniques are well-known to exist in the cryptographic community. An attacker can take advantage of this to issue another certificate with the same digital signature as the original, allowing the attacker to pose as the service that was compromised. It should be noted that this plugin flags as vulnerable all SSL certificate chains that are certified with SHA-1 and that expire after January 1, 2017. This is in conformity with Google's plan to phase out the SHA-1 cryptographic hash method over the course of many years.

- Mitigation : Contact the Certificate Authority to have the SSL certificate reissued.

6. Unencrypted Telnet Server

- Severity : Medium

- Description: The remote host is operating a Telnet server via an unencrypted channel, which is being used by the client. If you are using Telnet over an unencrypted connection, it is not advised since all information such as login credentials, passwords, and instructions is sent in cleartext. The ability to intercept and edit Telnet communication allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet connection and gain credentials or other sensitive information, as well as to modify traffic transmitted between a client and a server SSH is preferable to Telnet because it protects passwords from eavesdropping and may tunnel other data streams, such as an X11 session, via the network connection.
- Mitigation : Disable the Telnet service and use SSH instead.

7. SSL Certificate Cannot Be Trusted

- Severity : Medium

- Description: The X.509 certificate issued by the server cannot be trusted. This predicament can arise in three distinct ways, each of which has the potential to break the trust chain, as detailed below: To begin, it is possible that the top of the certificate chain given by the server is not descended from a publicly recognized certificate authority. Depending on the circumstances, this can occur when the top of the certificate chain is an unrecognized, self-signed certificate, or when intermediate certificates that would connect the top of the certificate chain to a known public certificate authority are absent. - Second, it is possible that the certificate chain contains a certificate that is no longer valid at the time of scanning. If a scan happens before one of the certificate's "notBefore" dates, or after one of the certificate's "notAfter" dates, this might result in a certificate being rejected. - Third, the certificate chain may contain a signature that either did not match the certificate's information or could not be validated by the issuing certificate authority. Faulty signatures can be rectified by requesting that the certificate with the bad signature be re-signed by the issuer of the certificate. Signatures that were unable to be validated were the consequence of the certificate's issuer employing a signature method that Nessus either does not support or does not recognize as a valid signing algorithm. If the remote host is a public host that is being used in production, any break in the chain makes it more difficult for users to authenticate the validity and identity of the web server that is hosting the website. Man-in-the-middle attacks against the remote host may become easier as a result of this change.

- Mitigation : Purchase or generate a proper SSL certificate for this service.

Conclusion

The SecureX security team was tasked with conducting this penetration testing for Wayne Industries, and they were successful. The SecureX security team's red, blue, and purple teams worked together to complete this ethical hacking exercise in a well-coordinated and professional manner. Their job was so intertwined that the red team was tasked with identifying the weaknesses in both remote targeted systems and the Wayne Network's internal systems. The red team then reduced their possibilities and focused only on exploiting the most critical to high-risk vulnerabilities, while the blue team participated in an analysis of the red team assaults and their impact on the company's operations. Purple team, on the other hand, was hard at work developing recommendations and making enhancements in order to avoid critical to high-risk vulnerabilities from occurring. As a result, Wayne Group should concentrate its efforts on mitigating and removing the vulnerabilities identified in this report, which are regarded to constitute a significant risk and have significant consequences for the systems, data, and operations.