PROJECT REPORT: SCANNING

OWASP BWA PENTESTING USING NMAP

BY AURA SHANAGONDA

TABLE OF CONTENTS

1. ROLE IN MY COMPANY

I ,Aura Shanagonda , as a dedicated Vulnerability Assessment and Penetration Tester (VAPT) and be at the forefront of securing cutting-edge educational technology. In this pivotal role, I will conduct thorough assessments of our web applications, networks, and systems to identify and mitigate potential security risks. Collaborate closely with our development teams, providing real-time feedback and assisting in implementing robust security measures. Stay ahead of cybersecurity threats, contributing to the company's proactive defense strategy.

My responsibilities are extend to creating and maintaining detailed security documentation, ensuring a comprehensive understanding of our security posture. Actively participate in incident response, investigating and resolving security incidents promptly.

2. PROJECT SCOPE

A. IN SCOPE

I am performing the Network scanning on OWASP (BWA) Using Nmap. I am going to check all the ports , OS detection and services running on OWASP . If I found something , I will document it.

3. THREAT ASSESSMENT :

1. Scope Definition:

- **System:** OWASP BWA vulnerable application.
- **Components:** Whole vulnerable application
- **Assessment Tools:** Nmap

2. Data Collection:

- **Network Scan:** Using Nmap to identify ports and services running on the application.

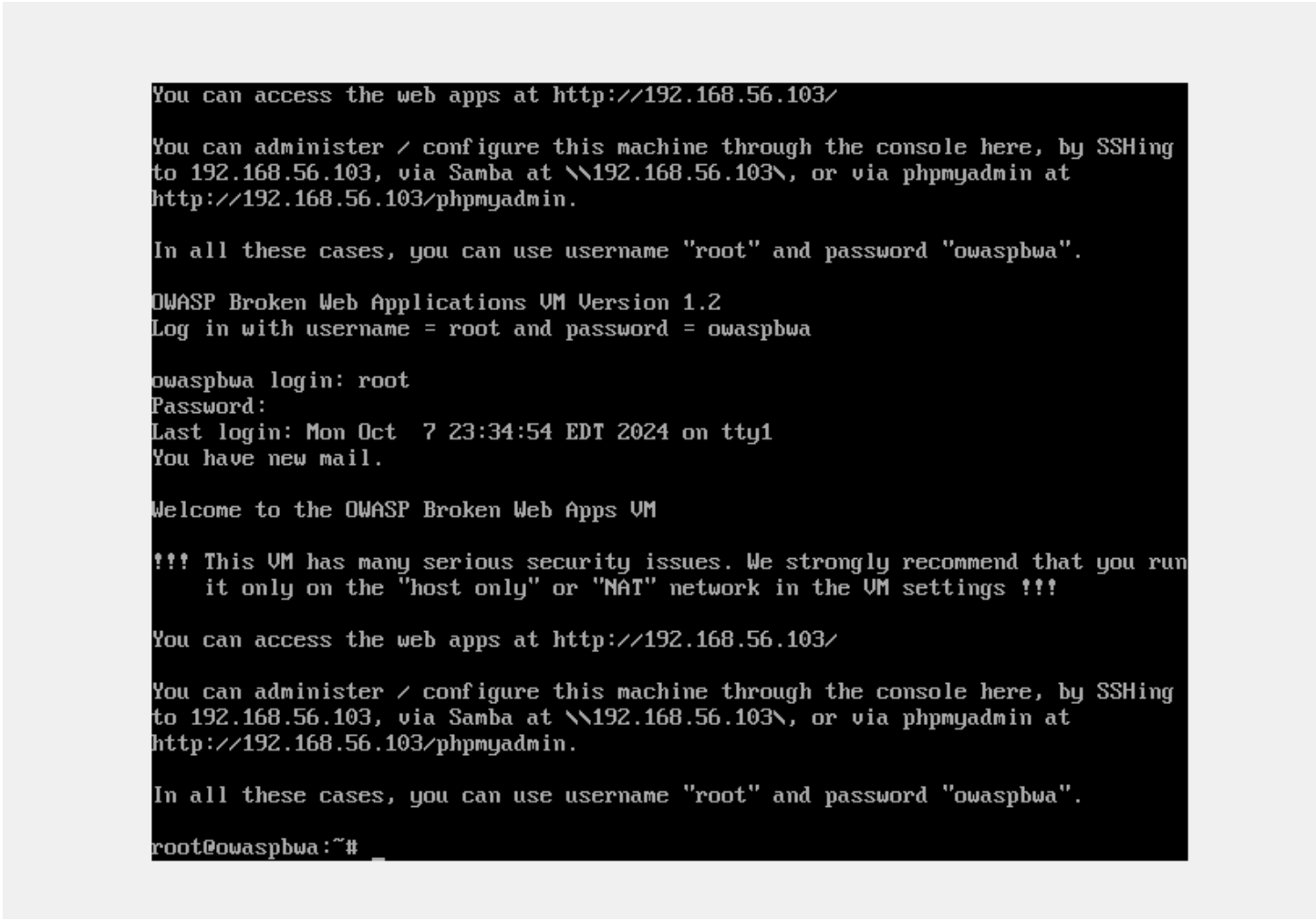
3. Introduction of Target Machine :

This project report outlines the process of conducting network scan operations on the OWASP Broken Web Applications (BWA) virtual machine using Nmap. The OWASP BWA is a valuable resource for security professionals and enthusiasts, designed to help identify and exploit vulnerabilities in various web applications. This project aims to demonstrate how Nmap can be utilized to assess the security posture of the applications hosted within this environment.

4. Installation Steps:

- **Download the OWASP BWA:** Obtain the latest version of the OWASP BWA in a compressed format.
- **Install VirtualBox:** Ensure that VirtualBox is installed and configured on your system.
- **Unzip the Downloaded File:** Extract the contents of the downloaded ZIP file.
- **Create a New Virtual Machine:** In VirtualBox, create a new VM for OWASP BWA, specifying appropriate settings for memory and network interfaces.
- **Network Configuration:** Ensure that the correct network interface is designated for the VM to allow communication with other devices on the network.
- **Start the VM:** Boot up the OWASP BWA virtual machine and log in using the credentials (username: root, password: owaspbwa).

- **Obtain an IP Address:** Confirm that the VM is receiving an IP address via DHCP by using commands like ifconfig.



5. Performing the Assessment:

Nmap, short for Network Mapper, is a powerful open-source tool widely used for network exploration and security auditing. It enables users to discover hosts and services on a computer network by sending packets and analyzing the responses.

With capabilities such as port scanning, OS detection, and service version identification, Nmap helps administrators assess the security posture of their systems.

The tool is highly versatile, supporting various scanning techniques and can be utilized in both small networks and large enterprise environments. Its extensive features make Nmap an essential asset for penetration testers and network security professionals alike.

Network Scan with Nmap :

- **Scan using -sV:**

The -sV flag enables version detection, allowing Nmap to probe open ports and gather information about the services running on them. This is useful for identifying potential vulnerabilities associated with specific service versions. When you run a scan with -sV, Nmap sends a series of probes to each open port.

These probes are designed to elicit responses that can reveal the service name and version.It uses a database of service probes (nmap-service-probes) that defines how to interact with various services to retrieve version information.

The output will include the service name and its version for each port detected, which helps in assessing the security posture of the target system.

Command: sudo nmap -sV 192.168.56.103

Results:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 23:13 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0067s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; proto
col 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-1ubuntu4.30 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/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
2.6.5 mod_ssl/2.2.14 OpenSSL ... )
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/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port5001-TCP:V=7.94SVN%I=7%D=10/28%Time=672052E8%P=x86_64-pc-linux-gnu%
SF:r(NULL,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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.97 seconds
```

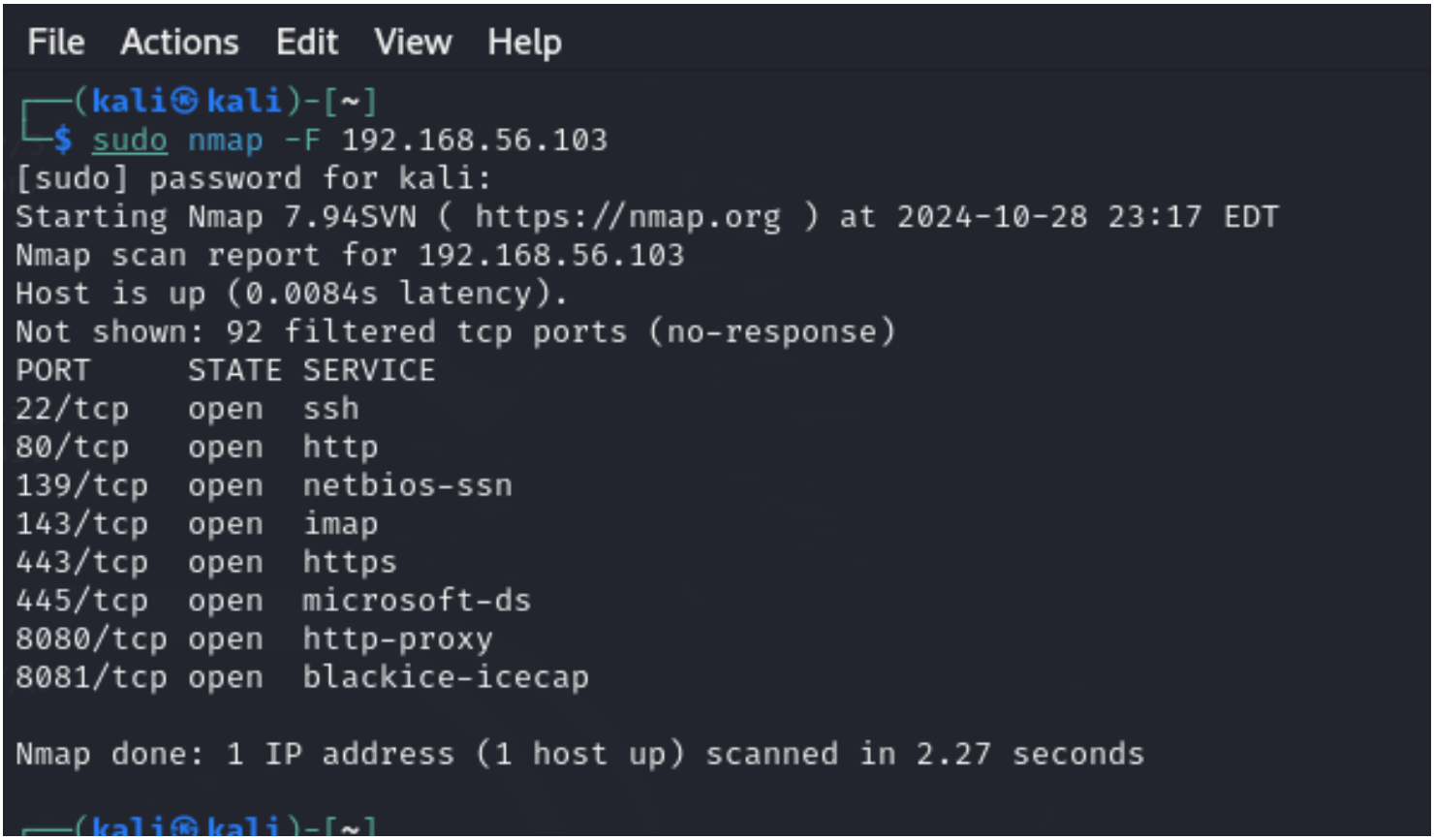
- **Scan using -F :**

The -F option in Nmap is used for performing a fast scan. The -F flag allows users to quickly scan the top 100 most commonly used ports instead of scanning all 65535 ports. This is useful for quickly assessing the services running on a target without taking too much time.

It provides a balance between speed and information gathering, allowing for rapid assessments without overwhelming detail.

Command: sudo nmap -F 192.168.56.103

Results:



- **Scan using -p-:**

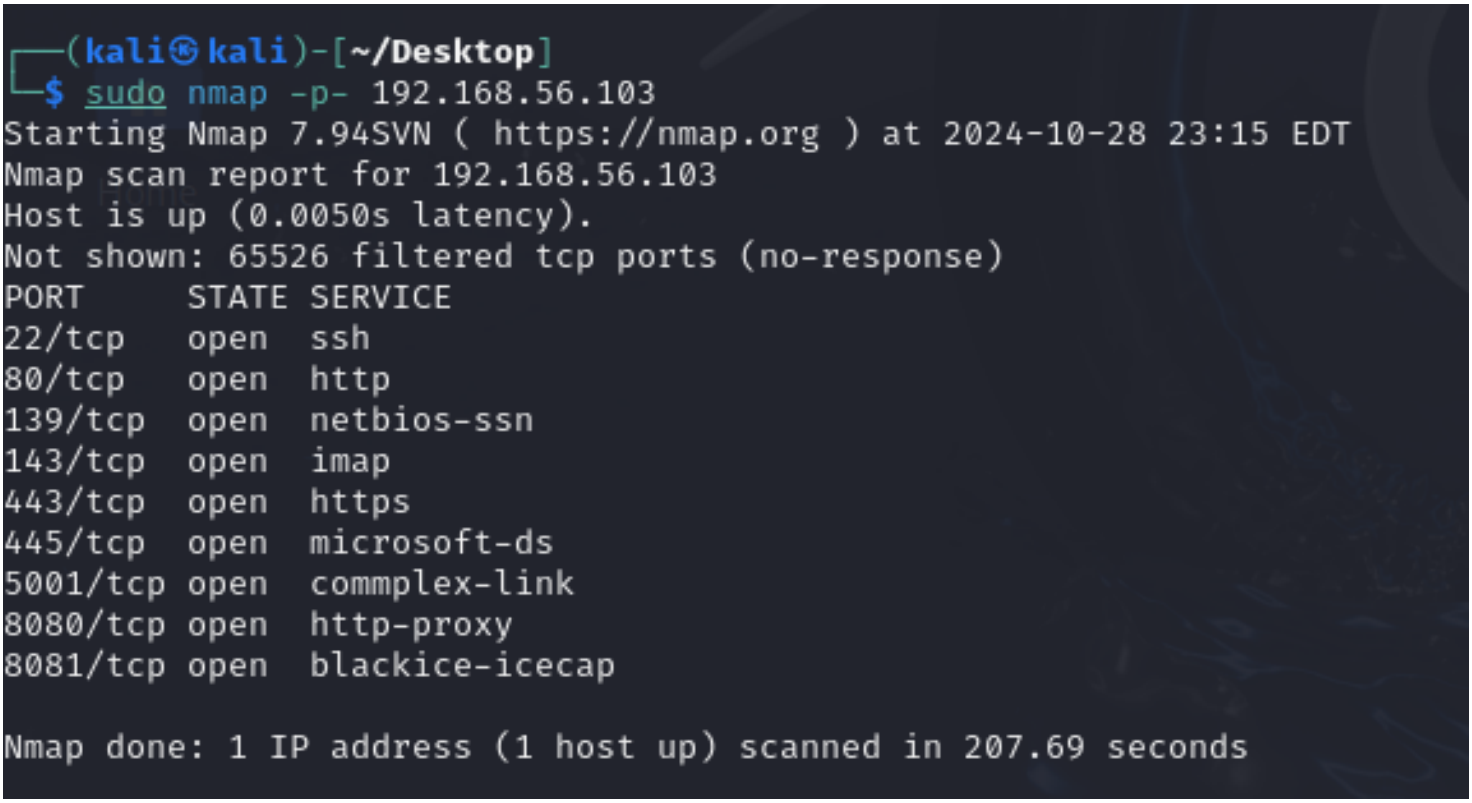
The -p- option in Nmap is used to scan all 65,535 TCP ports on a target. The -p- flag instructs Nmap to scan every port from 1 to 65535. This is useful for comprehensive assessments of services running on a target, ensuring that no ports are overlooked.

Use Cases:

- **Security Audits:** Comprehensive scans to identify all open ports and potential vulnerabilities.
- **Network Inventory**: Understanding what services are running on devices within a network.
- **Penetration Testing:** Gathering information for further exploitation by identifying all accessible services.

Command: sudo nmap -p- 192.168.56.103

Results:



- **Scan using -O:**

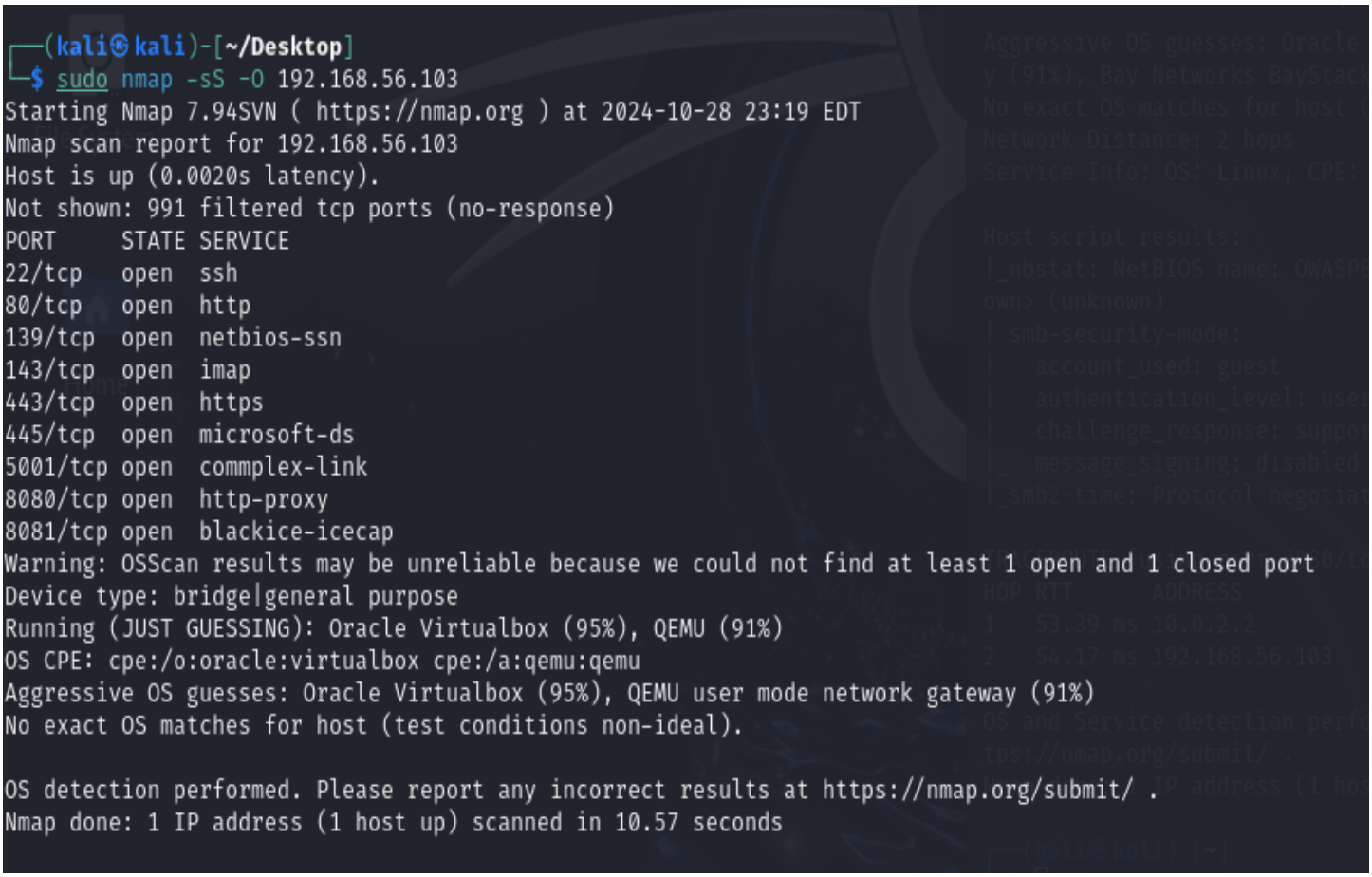
The -O option in Nmap is used for Operating System Detection. This feature allows Nmap to determine the operating system running on a target host by analyzing the TCP/IP stack fingerprint. Nmap sends a series of specially crafted packets to the target and analyzes the responses.

By examining various characteristics such as TCP options, IP header fields, and other protocol-specific details, Nmap can match the observed behavior against a database of known operating system fingerprints.

The -sS option in Nmap is used for performing a SYN scan, which is one of the most popular and stealthy scanning techniques available

Command: sudo nmap -sS -O 192.168.56.103

Results:



- **Scan using -A:**

The -A option in Nmap is used to enable Aggressive Scan mode. This option combines several useful features that provide a comprehensive overview of the target system.

When you use the -A option, Nmap performs the following actions:

- **OS Detection:** Identifies the operating system running on the target.
- **Version Detection:** Determines the versions of services running on open ports.
- **Script Scanning:** Executes Nmap scripts (NSE) that can perform additional checks and gather more information.

- **Traceroute:** Maps the path packets take to reach the target, providing insight into the network topology.

- **Command: sudo nmap -A 192.168.56.103**

Results:

Nmap scan report for 192.168.56.103
Host is up (0.0089s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_ 2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp open http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: owaspbwa OWASP Broken Web Applications
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap Courier Imapd (released 2008)
|_imap-capabilities: NAMESPACE CHILDREN UIDPLUS completed ACL IDLE IMAP4rev1 CAPABILITY OK THREAD=ORDEREDSUBJECT SORT THREAD=REFERENCES ACL2=UNIONA0001 QUOTA
443/tcp open ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_ssl-date: 2024-10-29T03:19:10+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=owaspbwa
| Not valid before: 2013-01-02T21:12:38
|_Not valid after: 2022-12-31T21:12:38
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1

|_http-title: owaspbwa OWASP Broken Web Applications
| http-methods:
|_ Potentially risky methods: TRACE
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open java-object Java Object Serialization
8080/tcp open http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open http   Jetty 6.1.25
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
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=7.94SVN%I=7%D=10/28%Time=67205415%P=x86_64-pc-linux-gnu%
SF:r(NULL,4,"\xac\xed\0\x05");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: OWASPBWA, 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)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 8080/tcp)
HOP RTT   ADDRESS

1 53.39 ms 10.0.2.2
2 54.17 ms 192.168.56.103

Nmap done: 1 IP address (1 host up) scanned in 41.75 seconds

6. Reporting :

Summary : Using nmap I scanned the vulnerable application called OWASP BWA. I performed various basic scanning operations on the vulnerable machine.

Detailed Report :

- **OS Detection :** In this scan, Actually the machine is running in Oracle virtual box . So it shows OS as Oracle Virtual Box.
- **Aggressive Scan:** In aggressive scan, It has done OS detection, ports and other operation like Traceroute.
- **Port Scan using -F and -p-:** In port scan , Nmap scanned all the 65535 ports and gave all the open ports which are opened in Vulnerable machine,
- **Service Scan:** In the service scan , I came to know that a lot services are running on the machine and I documented it .

Conclusion:

This is a basic project using Nmap . This project demonstrates how Nmap can be effectively utilized to perform various network scan operations on a vulnerable machine like OWASP BWA. By leveraging different Nmap options, security professionals can gain valuable insights into potential vulnerabilities within web applications, ultimately aiding in strengthening security measures.