**Ethical Hacking Project Report**  
**Completed by:** Luswepo Daniel Sinyinza  
  
 PHASE 1: Network and Port Scanning

For my initial ethical hacking practice, I used Kali Linux installed on a virtual machine via the VirtualBox hypervisor. My goal was to scan my host device (a Mac) to identify open ports and running services using Nmap.

1. Basic Network Scan

To begin, I verified connectivity between my Kali Linux VM and the host device.

- Step 1: Ping the Host

I ran the following command to ensure my host (IP: `172.20.10.4`) was reachable:

**ping 172.20.10.4**

- Step 2: Install Nmap (if not pre-installed)

**sudo apt update**

**sudo apt install nmap**

- Step 3: Ping Sweep to Discover Live Devices

I scanned my network to identify active devices:

**nmap -sn 172.20.10.1/24**

My host device (`172.20.10.4`) appeared in the list of live devices.

2. Port Scan on the Host (Mac)

Next, I conducted a port scan to identify open ports on my host.

- Step 1: Basic Port Scan

To scan common ports (1-1024):

**nmap 172.20.10.4**

- Step 2: Full Port Scan

To scan all 65,535 ports:

**nmap -p- 172.20.10.4**

- Step 3: Service Enumeration

To identify services running on the open ports:

**nmap -sV 172.20.10.4**

PHASE 2: Results of Port Scans

The scans revealed the following open ports on my host:

1. Port 80 (HTTP)

2. Port 5000 (UPnP)

3. Port 7000 (AFS3 Fileserver)

1. Exploring Port 80 (HTTP)

- Goal: Enumerate the HTTP service and identify potential vulnerabilities.

- Step 1: Access the Web Service

**curl http://172.20.10.4**

Alternatively, I visited `http://172.20.10.4` in a browser.

- Step 2: HTTP Service Enumeration with Nmap

**nmap -p 80 --script http-enum 172.20.10.4**

- Step 3: Directory Bruteforcing (Optional)

Using Gobuster to find hidden directories:

**gobuster dir -u http://172.20.10.4 -w /usr/share/wordlists/dirb/common.txt**

2. Exploring Port 5000 (UPnP)

- Goal: Investigate potential misconfigurations in the UPnP service.

- Step 1: UPnP Enumeration with Nmap

**nmap -p 5000 --script upnp-info 172.20.10.4**

3. Exploring Port 7000 (AFS3 Fileserver)

- Goal: Probe the AFS3 file server for vulnerabilities.

- Step 1: AFS3 Service Scan with Nmap

**nmap -p 7000 --script afs3-info 172.20.10.4**

PHASE 3: Analysis and Next Steps

Port 80 (HTTP)

The scans indicated:

- A directory listing under `/icons/` suggesting misconfigured access.

- Files like `.htaccess` and `index.html` with accessible (200) and restricted (403) statuses.

Next Steps:

1. Explore the `/icons/` directory:

**curl http://172.20.10.4/icons/**

2. Check the contents of `index.html`:

**curl http://172.20.10.4/index.html**

3. Research vulnerabilities related to the web server software.

Port 5000 (UPnP)

- The UPnP service may expose network configurations if misconfigured.

Next Steps:

1. Perform deeper UPnP enumeration:

**sudo upnpc -l**

2. Investigate known UPnP vulnerabilities.

Port 7000 (AFS3 Fileserver)

- The AFS3 scan revealed limited information.

Next Steps:

1. Further probe using Nmap scripts:

**nmap -p 7000 --script banner 172.20.10.4**

2. Research AFS3 vulnerabilities and potential exploits.

PHASE 4: Summary of Findings

1. Port 80 (HTTP)

- Directory listing under `/icons/` may expose sensitive files.

- Potential misconfigurations or outdated web server software.

2. Port 5000 (UPnP)

- UPnP service may present security risks if misconfigured.

3. Port 7000 (AFS3 Fileserver)

- Limited information; further investigation needed.

Next Steps:

Based on these findings, I will focus on exploiting potential vulnerabilities related to the HTTP service, investigate UPnP misconfigurations, and explore AFS3 weaknesses.

This structured approach provided a clear roadmap for ethical hacking and vulnerability assessment on my host device.

Below are some of the screenshots from the project:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated