**Penetration Testing Report**

**Objective**

The primary objective of this penetration testing project was to assess the security posture of the network hosted at **http://scanme.nmap.org**. This included identifying live hosts, open ports, running services, operating systems, and potential vulnerabilities.

**Scope**

* **Target:** http://sunstone.in
* **Scans Performed:** Ping Scan, TCP SYN Scan, Service Version Scan, OS Detection, Nmap Scripting Engine (NSE) Scans

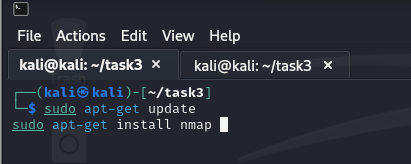
**Initial Setup**

**Network Scan**

The target network was scanned using Nmap, a powerful network scanning tool.

**Nmap Installation**

Nmap was installed on a Linux system using the following command:



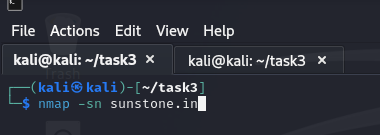
A screenshot of a computer

Description automatically generated

**Basic Scans**

**Ping Scan**

A ping scan was performed to identify live hosts on the network.



Output:

A computer screen shot of numbers

Description automatically generated

TCP SYN Scan

A basic TCP SYN scan was conducted to discover open ports on the identified hosts.

A screenshot of a computer

Description automatically generated

Output:

A computer screen shot of a computer code

Description automatically generated

**Task 2: Detailed Scanning**

**Service Version Scan**

A service version scan was performed to identify the services running on open ports.

A screenshot of a computer

Description automatically generated

Output:

A screenshot of a computer

Description automatically generated

**OS Detection**

OS detection was used to determine the operating systems of the live hosts.

A screenshot of a computer

Description automatically generated

Output:

A screen shot of a computer

Description automatically generated

**Task 3: NSE Scans**

**Running NSE Scripts**

Nmap Scripting Engine (NSE) scripts were used to gather additional information about the network

**CMD**

**A screenshot of a computer

Description automatically generated**

**Output:**

**A screenshot of a computer program

Description automatically generated**

**Task 4: Report Creation**

**Summary of the Scanned Network**

* **Target:**sunstone.in
* **Scans Performed:** Ping Scan, TCP SYN Scan, Service Version Scan, OS Detection, NSE Scripts

Open ports

|  |  |  |
| --- | --- | --- |
| Port | state | service |
| 80/tcp | open | http |
| 443/tcp | open | https |

**OS Information**

|  |  |
| --- | --- |
| Host | OS |
| Sunstone.in | Linux 2.4.37 |

* **Host is up:** The target host is reachable and responded to the Nmap ping.
* **Open Ports:**
  + 80/tcp: HTTP service running.
  + 443/tcp: HTTPS service running.
* **Vulnerability Scans:**
  + **Stored XSS:** No stored cross-site scripting vulnerabilities were found on either port 80 or 443.
  + **CSRF:** No cross-site request forgery vulnerabilities were found on either port 80 or 443.
  + **DOM-based XSS:** No DOM-based cross-site scripting vulnerabilities were found on either port 80 or 443.
  + **CVE-2014-3704:** The script for checking this vulnerability failed to execute.
  + **ASP.NET Debug:** The script for checking this vulnerability failed to execute.

**HTTP Service Enumeration:**

* The following resources were identified on the HTTP service:
  + /wiki/Main\_Page: Wiki
  + /cgi-bin/mj\_wwusr: Majordomo2 Mailing List
  + /majordomo/mj\_wwwusr: Majordomo2 Mailing List
  + /reg\_1.htm: Polycom IP phone
  + /adr.htm: Snom IP Phone
  + /line\_login.htm?l=1: Snom IP Phone
  + /tbook.csv: Snom IP Phone
  + /globalSIPsettings.html: Aastra IP Phone
  + /SIPsettingsLine1.html: Aastra IP Phone
  + /login.stm: Belkin G Wireless Router

**Recommendations:**

* **Remediate Failed Scripts:** Investigate and address the errors encountered during the execution of the vulnerability scripts (CVE-2014-3704 and ASP.NET Debug).
* **Review HTTP Resources:** Analyze the enumerated HTTP resources to identify any potential misconfigurations or vulnerabilities.
* **Regular Security Assessments:** Conduct periodic security assessments to identify and address any emerging threats or vulnerabilities.