Network Security Assessment Report

1. Introduction This report documents the results of a network security assessment conducted using port scanning and network service enumeration techniques. The goal of this assessment was to identify active services on a target system and perform a vulnerability scan to uncover potential security risks.

General Port Scan Results

```
sh-3.2# nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 17:17 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 5.61 seconds
```

2. Tools Used

- **Port Scanning Tool:** Nmap (Network Mapper)
- **Network Service Enumeration:** Nmap Service Version Detection
- **Vulnerability Scanning:** Nmap NSE Vulnerability Scripts

3. Port Scanning Results A standard Nmap scan was performed to identify open ports and active services on the target host (scanme.nmap.org). The results revealed the following open ports:

Port Scanning Details

Port	State	Service
22/tcp	open	SSH
80/tcp	open	HTTP
9929/tcp	open	Nping Echo
31337/tcp	open	Elite

4. Network Service Enumeration To gather further details about active services, a service version scan was conducted. The identified services include:

Service Enumeration Scan

```
[sh-3.2# nmap -sS -sV -p- scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 15:51 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
68/tcp    filtered dhcpc
80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))
546/tcp   filtered dhcpv6-client
9929/tcp  open     nping-echo    Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- **SSH (Port 22):** OpenSSH 6.6.1p1 running on Ubuntu Linux
- **HTTP (Port 80):** Apache HTTPD 2.4.7 running on Ubuntu
- **Nping Echo (Port 9929):** Used for testing network latency
- **31337/tcp:** Listed as "tcpwrapped," indicating possible access control mechanisms

5. Vulnerability Scan Results An Nmap vulnerability scan was performed using NSE scripts, identifying the following security risks:

Vulnerability Scan Results

```
sh-3.2# nmap --script vuln scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 15:59 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:02:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.21% done; ETC: 16:01 (0:00:01 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-head-search
|     Form action: /search/
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-foot-search
|_    Form action: /search/
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 550.26 seconds
```

Vulnerability	Risk Level	Description and Impact
Slowloris DoS Attack (CVE-2007-6750)	High	The Apache web server is vulnerable to a Slowloris attack, which allows an attacker to exhaust server resources by maintaining multiple open connections. This can lead to denial of service.

Cross-Site Request Forgery (CSRF) on HTTP (Port 80)	Medium	The web application was found to be vulnerable to CSRF, which could allow attackers to perform unauthorized actions on behalf of an authenticated user.
SSH Service Exposure	Low	The SSH service is running with an older version (6.6.1p1), which may contain vulnerabilities if not properly configured or patched.

6. Risk Analysis and Mitigation Strategies

1. **Slowloris DoS Attack:**
    - **Risk Level:** High
    - **Impact:** Can cause denial of service by consuming server resources.
    - **Mitigation:** Implement rate limiting, increase the `Timeout` directive in Apache, and use a reverse proxy such as Nginx.
2. **Cross-Site Request Forgery (CSRF) Vulnerability:**
    - **Risk Level:** Medium
    - **Impact:** Allows an attacker to trick users into executing unwanted actions.
    - **Mitigation:** Implement anti-CSRF tokens and enforce user authentication validation.
3. **SSH Service Exposure:**
    - **Risk Level:** Low
    - **Impact:** Older SSH versions may contain unpatched security flaws.
    - **Mitigation:** Upgrade to the latest version of OpenSSH and enforce strong authentication policies.

7. Conclusion This assessment identified multiple security risks that could be exploited by attackers. While the Slowloris vulnerability poses the highest risk, proper security configurations and mitigations can significantly reduce the likelihood of exploitation. It is recommended that the target system implement the suggested security measures to enhance its overall security posture