Task 1:

Security Audits and Vulnerability Scanning

Project Scope: Network Scanning and Vulnerability Assessment

Objective

- **Primary Goal:** To evaluate the security posture of a network by identifying vulnerabilities and weaknesses.
- **Secondary Goal:** To provide recommendations for enhancing network security based on the findings.

Using Nmap:

Host Discovery:

In this section, we present the results of the host discovery phase conducted using Nmap. This phase's main objective was to identify which devices are active on the network within the specified IP range. We employed Nmap's Ping Scan and TCP SYN Ping techniques to determine the presence of hosts. The scan was performed on subnet 192.168.100.0/24, covering all IP addresses within this range. The findings revealed several active hosts, each responding to our probes with varying latency and response types. These results provide a foundational understanding of the network's active devices, setting the stage for further detailed analysis and security assessments.

nmap –sn scan which no port scan in nmap and only discovers hosts.

```
┌──(root㉿Lt-GH0ST)-[/home/lt-gh0st/Downloads]
└─# nmap -sn 192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 15:22 PKT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Sca
n
ARP Ping Scan Timing: About 73.92% done; ETC: 15:22 (0:00:01 remaining)
Nmap scan report for 192.168.100.1
Host is up (0.0025s latency).
MAC Address: 6C:E8:74:59:25:86 (Huawei Technologies)
Nmap scan report for 192.168.100.5
Host is up (0.097s latency).
MAC Address: E4:FD:A1:34:63:7B (Huawei Technologies)
Nmap scan report for 192.168.100.6
Host is up (0.016s latency).
MAC Address: 5C:E0:C5:A8:AE:F8 (Intel Corporate)
Nmap scan report for 192.168.100.25
Host is up (0.0035s latency).
MAC Address: 58:D9:D5:20:41:78 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for 192.168.100.78
Host is up (0.075s latency).
MAC Address: C2:4A:45:AD:7B:04 (Unknown)
Nmap scan report for 192.168.100.89
Host is up (0.058s latency).
MAC Address: 24:EE:9A:3D:0A:D6 (Intel Corporate)
Nmap scan report for 192.168.100.8
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.91 seconds
```

Now we have listed all the devices that are in my network. Let's check for the open ports of the devices in my networks by using the following command.

Ports Scanning:

```
┌──(root㉿Lt-GH0ST)-[/home/lt-gh0st/Downloads]
└─# nmap --top-ports 1000 192.168.100.0/24
```

```
SYN Stealth Scan Timing: About 98.55% done; ETC: 15:34 (0:00:02 remaining)
Nmap scan report for 192.168.100.1
Host is up (0.0057s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
8022/tcp filtered oa-system
MAC Address: 6C:E8:74:59:25:86 (Huawei Technologies)

Nmap scan report for 192.168.100.5
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.100.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E4:FD:A1:34:63:7B (Huawei Technologies)

Nmap scan report for 192.168.100.6
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.100.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 5C:E0:C5:A8:AE:F8 (Intel Corporate)

Nmap scan report for 192.168.100.25
Host is up (0.033s latency).
All 1000 scanned ports on 192.168.100.25 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 58:D9:D5:20:41:78 (Tenda Technology,Ltd.Dongguan branch)

Nmap scan report for 192.168.100.40
Host is up (0.0043s latency).
All 1000 scanned ports on 192.168.100.40 are in ignored states.
Not shown: 829 filtered tcp ports (no-response), 171 closed tcp ports (reset)
MAC Address: EC:1F:72:24:02:03 (Samsung Electro-mechanics(Thailand))

Nmap scan report for 192.168.100.72
Host is up (0.076s latency).
All 1000 scanned ports on 192.168.100.72 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 26:3E:E0:DD:E7:BA (Unknown)

Nmap scan report for 192.168.100.78
Host is up (0.033s latency).
All 1000 scanned ports on 192.168.100.78 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: C2:4A:45:AD:7B:04 (Unknown)
```

```
Nmap scan report for 192.168.100.89
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.100.89 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 24:EE:9A:3D:0A:D6 (Intel Corporate)

Nmap scan report for 192.168.100.8
Host is up (0.000019s latency).
All 1000 scanned ports on 192.168.100.8 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (9 hosts up) scanned in 145.78 seconds
```

All devices in my network have no open ports except my router (192.168.100.1).

```
Nmap scan report for 192.168.100.1
Host is up (0.0057s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
23/tcp   filtered telnet
53/tcp   open     domain
80/tcp   open     http
8022/tcp filtered oa-system
MAC Address: 6C:E8:74:59:25:86 (Huawei Technologies)
```

In the above screenshots my router has HTTP port 80 let's check for known vulnerabilities in it using nmap.

Vulnerability scanning command for nmap is:

┌──(root㉿Lt-GH0ST)-[/home/lt-gh0st/Downloads]

└─# nmap -p 80 --script vuln 192.168.100.1

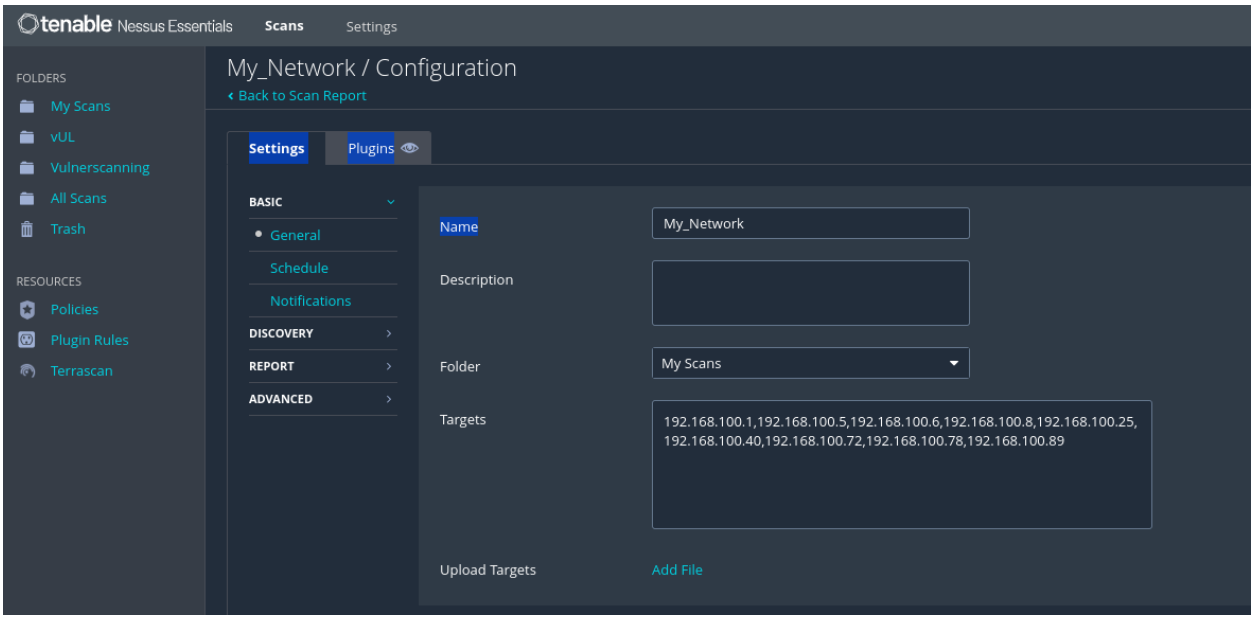
```
PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-fileupload-exploiter:
|
|      Couldn't find a file-type field.
|
|_     Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| 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:
|        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_       http://ha.ckers.org/slowloris/
MAC Address: 6C:E8:74:59:25:86 (Huawei Technologies)

Nmap done: 1 IP address (1 host up) scanned in 67.48 seconds
```

My router which means my network is Vulnerable to DOS attack. Slowloris is Type of DOS attack and my network is vulnerable to Slowloris. 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 the connection to the target web server and sending a partial request. By doing so, it starves the http server's resources causing DOS (Denial of Services).

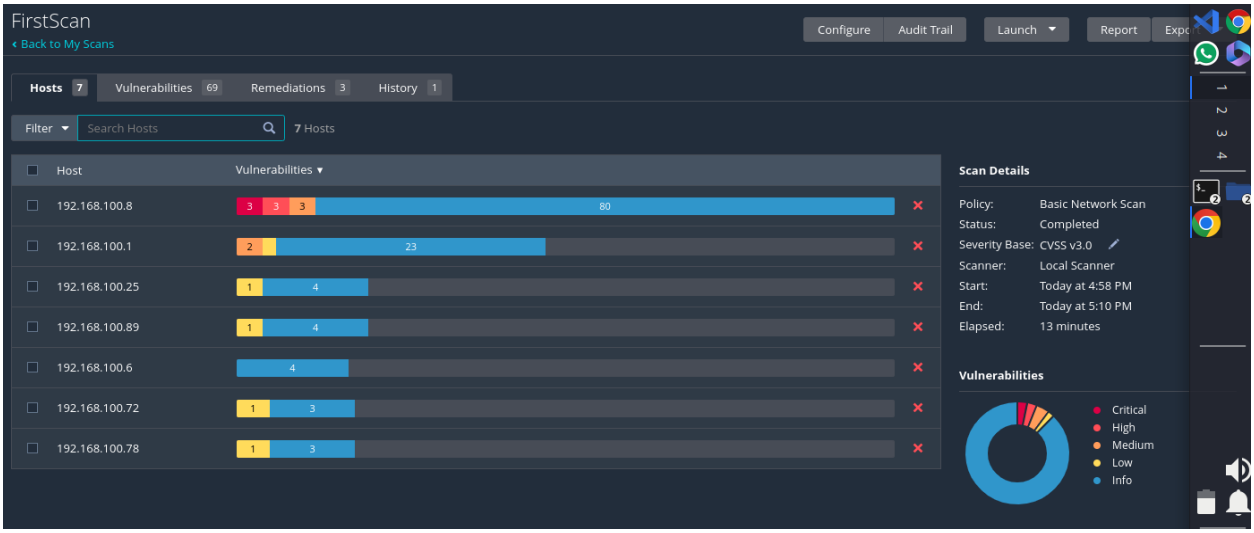
How can I save my Network from Slowloris DOS attack?

- Implement rate limiting and connection management techniques to mitigate Slowloris attacks.
- Configure the web server to handle incomplete or slow HTTP requests more robustly.
- Consider using web application firewalls (WAFs) or other security appliances to protect against DoS attacks.

Now let's Checks check network vulnerabilities with Nessus:



After the complete Vulnerability Scanning:



Hosts 7 | Vulnerabilities 69 | Remediations 3 | History 1

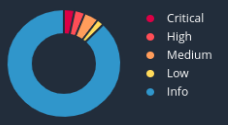
Filter | Search Vulnerabilities | 69 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	Nodejs Node.js (Multiple Issues)	Misc.	5
MIXED	...	...	...	Apache Log4j (Multiple Issues)	Misc.	4
MEDIUM	6.5			IP Forwarding Enabled	Firewalls	1
MEDIUM	4.4			urllib3 Python Library < 1.26.19, < 2.2.2 (...	Misc.	1
MIXED	...	...	...	SSL (Multiple Issues)	General	10
MIXED	...	...	...	Intel Media Sdk (Multiple Issues)	Misc.	2
LOW	3.3 *			DHCP Server Detection	Service detection	1
LOW	2.1 *			ICMP Timestamp Request Remote Date ...	General	4
INFO	...	...	...	SSH (Multiple Issues)	General	6
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	4
INFO	...	...	...	TLS (Multiple Issues)	General	3

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:58 PM
End:	Today at 5:10 PM
Elapsed:	13 minutes

Vulnerabilities



INFO	...	...	...	TLS (Multiple Issues)	General	3
INFO	...	...	...	TLS (Multiple Issues)	Service detection	3
INFO	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO				Ethernet MAC Addresses	General	7
INFO				Nessus Scan Information	Settings	7
INFO				Traceroute Information	General	6
INFO				Ethernet Card Manufacturer Detection	Misc.	5
INFO				Netstat Portscanner (SSH)	Port scanners	4
INFO				Service Detection	Service detection	4
INFO				OpenJDK Java Detection (Linux / Unix)	General	3
INFO				Common Platform Enumeration (CPE)	General	2
INFO				Device Type	General	2
INFO				Host Fully Qualified Domain Name (FQD...	General	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				OS Identification	General	2

Modify

Actions to be taken:

Action	Vulns	Hosts
Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).: Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.	14	1
Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104): Upgrade to Apache Log4j version 2.16.0 or later since 1.x is end of life. Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.	1	1
urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891): Upgrade to urllib3 version 1.26.19, 2.2.2 or later.	0	1

IP forwarding Vulnerability Solutions given by Nessus:

MEDIUM IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Output

```
IP forwarding appears to be enabled on the remote host.

 Detected local MAC Address        : 50b7c363eb0c
 Response from local MAC Address   : 50b7c363eb0c

 Detected Gateway MAC Address      : 6ce874592586
 Response from Gateway MAC Address : 6ce874592586
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.100.1

Python Library Vulnerability Solution by Nessus:

FirstScan / Plugin #200807

‹ Back to Vulnerabilities

Configure

Hosts 7 | Vulnerabilities 69 | Remediations 3 | History 1

MEDIUM urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891)

Description

urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with 'ProxyManager', the 'Proxy-Authorization' header is only sent to the configured proxy, as expected. However, when sending HTTP requests without using urllib3's proxy support, it's possible to accidentally configure the 'Proxy-Authorization' header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the 'Proxy-Authorization' HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to urllib3 version 1.26.19, 2.2.2 or later.

See Also

http://www.nessus.org/u?7b44847c

Output

```
Path              : /urllib3
Installed version : 2.0.7
Fixed version     : 2.2.2
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.100.8

DHCP Server Vulnerability Solution by Nessus:

FirstScan / Plugin #10663

‹ Back to Vulnerabilities

Configure | Audit Tra

Hosts 7 | **Vulnerabilities 69** | Remediations 3 | History 1

LOW **DHCP Server Detection**

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Output

```
Nessus gathered the following information from the remote DHCP server :

  Master DHCP server of this network : 0.0.0.0
  IP address the DHCP server would attribute us : 192.168.100.8
  DHCP server(s) identifier : 192.168.100.1
  Netmask : 255.255.255.0
  Router : 192.168.100.1
  Domain name server(s) : 192.168.100.1
```

To see debug logs, please visit individual host

Port ▲	Hosts
67 / udp	192.168.100.1

ICMP Time stamp request remote Data disclose Vulnerability Solution by Nessus:

FirstScan / Plugin #10114

‹ Back to Vulnerabilities

Config

Hosts 7 | **Vulnerabilities 69** | Remediations 3 | History 1

LOW **ICMP Timestamp Request Remote Date Disclosure**

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Output

```
The difference between the local and remote clocks is 12746 seconds.
```

To see debug logs, please visit individual host

Port ▲	Hosts
0 / icmp	192.168.100.25

```
The remote clock is synchronized with the local clock.
```

To see debug logs, please visit individual host

Port ▲	Hosts
0 / icmp	192.168.100.89