

MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

NETWORK SERVICE SCANNING WITH NMAP IN
XML AND HTML FORMAT

ASSIGNMENT 4

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 21, 2024

Contents

| | | |
|----------|--|----------|
| 1 | Aim | 1 |
| 2 | Objectives | 1 |
| 3 | Theory | 1 |
| 3.1 | XML Format | 1 |
| 3.2 | Uses | 1 |
| 3.3 | Advantages | 1 |
| 3.4 | Disadvantages | 2 |
| 4 | Implementation | 2 |
| 4.1 | Scanning all ports with nmap Aggresively and verbosely to get an xml format output | 2 |
| 4.2 | Installing xsltproc | 4 |
| 4.3 | Report Generated opened in the Browser | 6 |
| 5 | Platform | 7 |
| 6 | FAQs | 7 |
| 7 | Conclusion | 8 |

1 Aim

To Discover Network service to Organize and sort through Nmap scan output

2 Objectives

1. To Discover Network service
2. To Organize and sort through Nmap scan output
3. To Generate Nmap scan output in XML and HTML format

3 Theory

3.1 XML Format

XML stands for eXtensible Markup Language. It was designed to store and transport data. It was designed to be both human- and machine-readable. XML plays an important role in many different IT systems. It is used to store data, to configure programs, and to create user interfaces. XML is often used for distributing data over the Internet. It is important to note that XML is not a replacement for HTML. XML and HTML were designed with different goals.

3.2 Uses

- Storing and transporting data in a structured format.
- Configuring programs and defining settings in a readable manner.
- Creating user interfaces and defining document structures.
- Exchanging data between different systems and platforms.
- Representing data hierarchies and relationships in a standardized format.

3.3 Advantages

- Human-readable format, making it easy to understand and modify by developers and users.
- Machine-readable format, allowing for automated processing and interoperability between systems.
- Platform-independent, enabling data exchange between different operating systems and software applications.
- Extensibility, allowing users to define custom tags and structures to meet specific requirements.
- Well-defined syntax and rules, ensuring consistency and reliability in data representation.

3.4 Disadvantages

- Verbosity, as XML documents can become large and complex due to the use of tags and attributes.
- Overhead, as XML parsing and processing may require additional computational resources compared to other data formats.
- Lack of native support for complex data types and structures, leading to the need for custom solutions or additional standards (e.g., XML Schema).
- Limited support for binary data, as XML is primarily designed for text-based data representation.
- Potential security risks, such as XML External Entity (XXE) attacks, if not properly validated and sanitized.

4 Implementation

4.1 Scanning all ports with nmap Aggressively and verbosely to get an xml format output

Syntax

```
$ nmap -p 1-65535 -A -v <IP Address> -oX <Output File Name>
```

Command

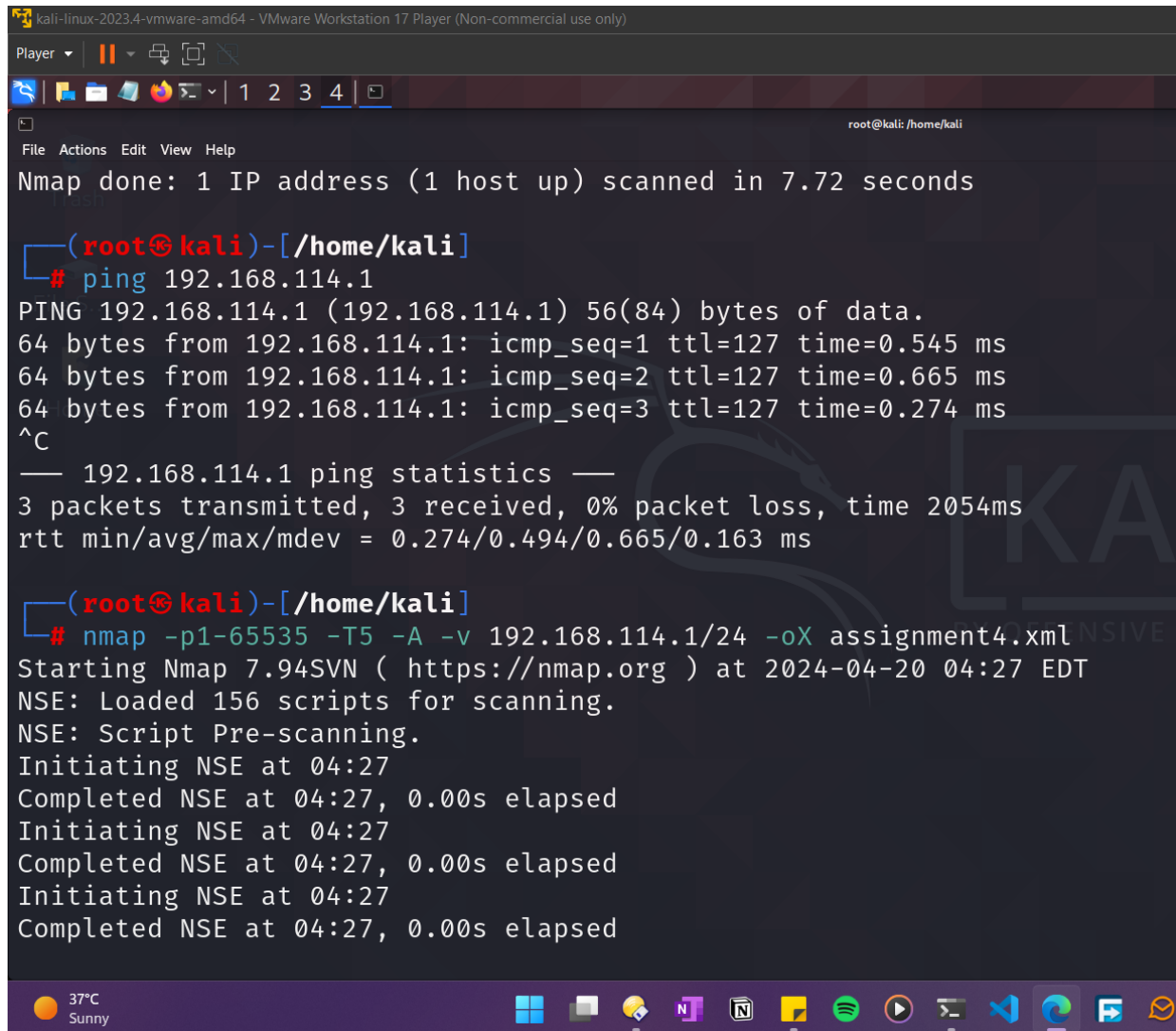
```
$ nmap -p 1-65535 -A -v 192.168.114.1 -oX scan.xml -T5 -oX assignment4.xml
```

Purpose

This command will

1. Scan all ports (1-65535) on the target IP address.
2. Perform an aggressive scan with OS detection, version detection, script scanning, and traceroute.
3. Display verbose output to provide detailed information about the scan process.
4. Save the scan results in XML format to the specified output file.
5. Use the -T5 timing template for faster scanning.

Output



The screenshot shows a Kali Linux terminal window running in a VMware Workstation 17 Player. The terminal displays the output of an Nmap scan and a ping command. The Nmap scan is for the IP address 192.168.114.1/24, using port 65535, with the output saved to a file named assignment4.xml. The ping command is for the IP address 192.168.114.1, showing 3 packets transmitted, 3 received, 0% packet loss, and a round trip time of 0.274 ms. The terminal also shows the Nmap version 7.94SVN and the date and time of the scan.

```
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 7.72 seconds

(root@kali)-[/home/kali]
# ping 192.168.114.1
PING 192.168.114.1 (192.168.114.1) 56(84) bytes of data.
64 bytes from 192.168.114.1: icmp_seq=1 ttl=127 time=0.545 ms
64 bytes from 192.168.114.1: icmp_seq=2 ttl=127 time=0.665 ms
64 bytes from 192.168.114.1: icmp_seq=3 ttl=127 time=0.274 ms
^C
— 192.168.114.1 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.274/0.494/0.665/0.163 ms

(root@kali)-[/home/kali]
# nmap -p1-65535 -T5 -A -v 192.168.114.1/24 -oX assignment4.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 04:27 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
Initiating NSE at 04:27
Completed NSE at 04:27, 0.00s elapsed
```

[illegible]

```
NSE: Script Post-scanning.
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results.
Nmap done: 256 IP addresses (1 host up) scanned in 192.66 seconds
Raw packets sent: 133216 (5.851MB) | Rcvd: 83 (4.960KB)
```

4.2 Installing xsltproc

Syntax

```
$ sudo apt-get install xsltproc
```

Command

```
$ sudo apt-get install xsltproc
```

Purpose

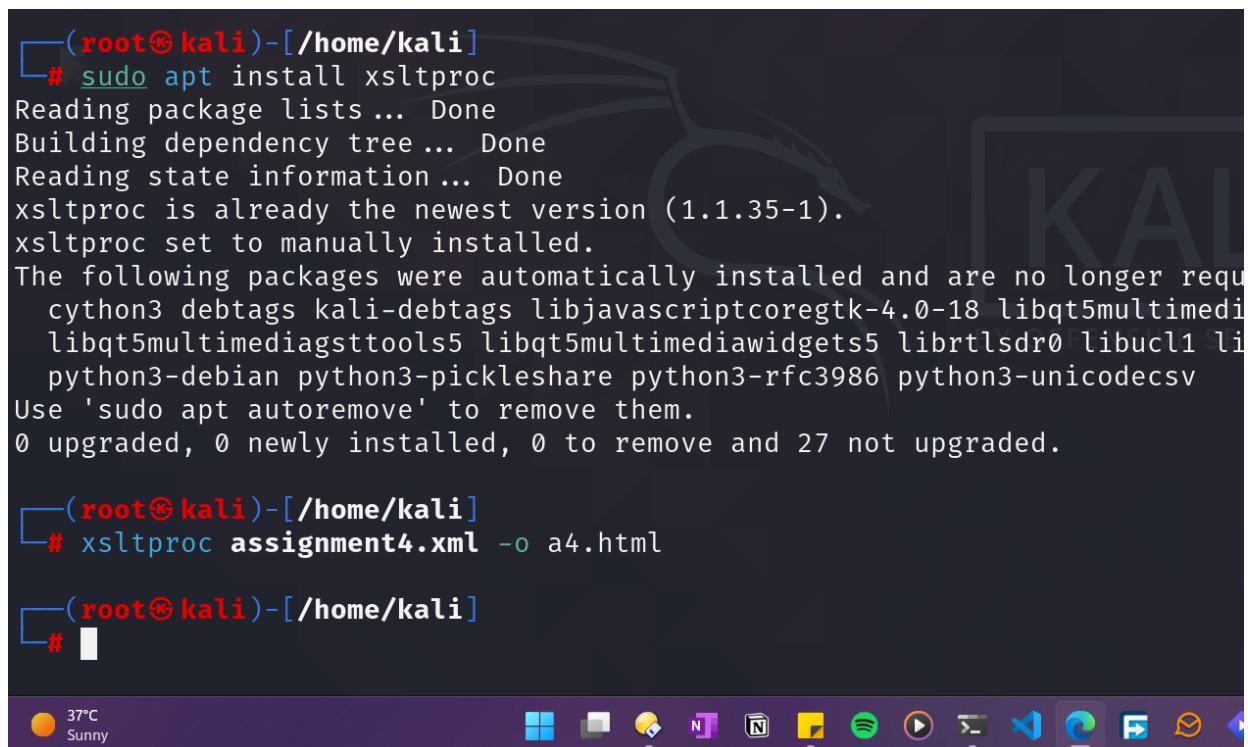
This command will install the xsltproc package on the system, which is required for transforming XML documents using XSLT stylesheets.

Output

```
(root@kali)-[/home/kali]
# sudo apt install xsltproc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xsltproc is already the newest version (1.1.35-1).
xsltproc set to manually installed.
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18 libqt5multimedia5
  libqt5multimedia5gsttools5 libqt5multimedia5widgets5 librtlsdr0 libucl1 libucl1-dev
  python3-debian python3-pickleshare python3-rfc3986 python3-unicodedcsv
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.

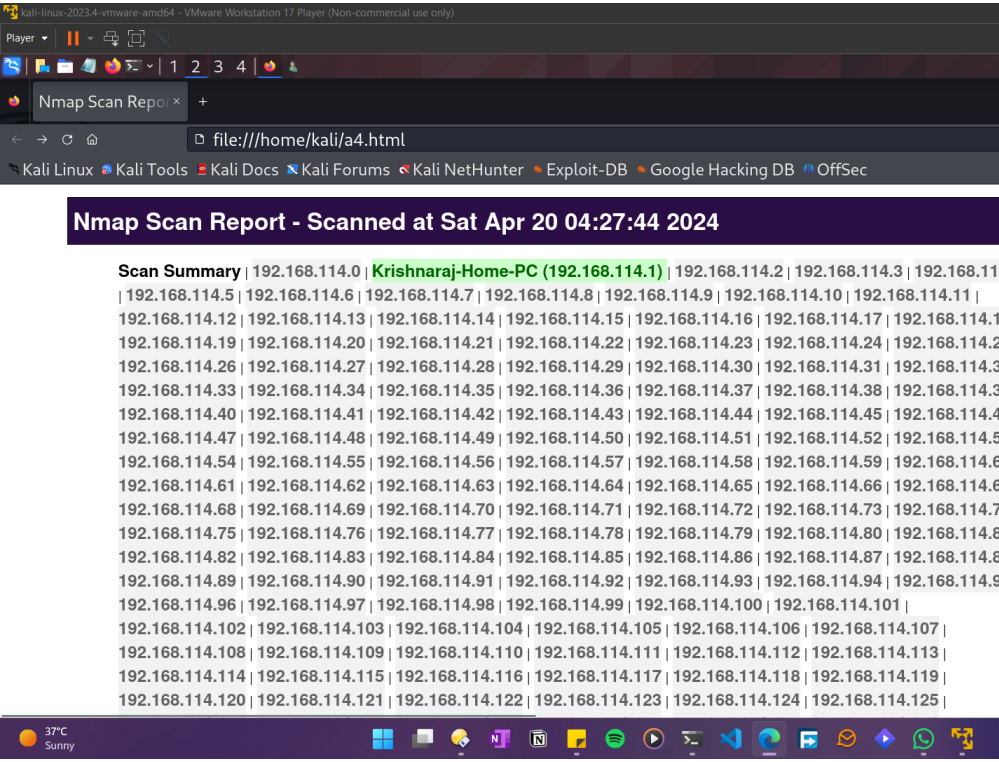
(root@kali)-[/home/kali]
# xsltproc assignment4.xml -o a4.html

(root@kali)-[/home/kali]
#
```



4.3 Report Generated opened in the Browser

Output



Nmap Scan Report - Scanned at Sat Apr 20 04:27:44 2024

Scan Summary | 192.168.114.0 | **Krishnaraj-Home-PC (192.168.114.1)** | 192.168.114.2 | 192.168.114.3 | 192.168.114.4 | 192.168.114.5 | 192.168.114.6 | 192.168.114.7 | 192.168.114.8 | 192.168.114.9 | 192.168.114.10 | 192.168.114.11 | 192.168.114.12 | 192.168.114.13 | 192.168.114.14 | 192.168.114.15 | 192.168.114.16 | 192.168.114.17 | 192.168.114.18 | 192.168.114.19 | 192.168.114.20 | 192.168.114.21 | 192.168.114.22 | 192.168.114.23 | 192.168.114.24 | 192.168.114.25 | 192.168.114.26 | 192.168.114.27 | 192.168.114.28 | 192.168.114.29 | 192.168.114.30 | 192.168.114.31 | 192.168.114.32 | 192.168.114.33 | 192.168.114.34 | 192.168.114.35 | 192.168.114.36 | 192.168.114.37 | 192.168.114.38 | 192.168.114.39 | 192.168.114.40 | 192.168.114.41 | 192.168.114.42 | 192.168.114.43 | 192.168.114.44 | 192.168.114.45 | 192.168.114.46 | 192.168.114.47 | 192.168.114.48 | 192.168.114.49 | 192.168.114.50 | 192.168.114.51 | 192.168.114.52 | 192.168.114.53 | 192.168.114.54 | 192.168.114.55 | 192.168.114.56 | 192.168.114.57 | 192.168.114.58 | 192.168.114.59 | 192.168.114.60 | 192.168.114.61 | 192.168.114.62 | 192.168.114.63 | 192.168.114.64 | 192.168.114.65 | 192.168.114.66 | 192.168.114.67 | 192.168.114.68 | 192.168.114.69 | 192.168.114.70 | 192.168.114.71 | 192.168.114.72 | 192.168.114.73 | 192.168.114.74 | 192.168.114.75 | 192.168.114.76 | 192.168.114.77 | 192.168.114.78 | 192.168.114.79 | 192.168.114.80 | 192.168.114.81 | 192.168.114.82 | 192.168.114.83 | 192.168.114.84 | 192.168.114.85 | 192.168.114.86 | 192.168.114.87 | 192.168.114.88 | 192.168.114.89 | 192.168.114.90 | 192.168.114.91 | 192.168.114.92 | 192.168.114.93 | 192.168.114.94 | 192.168.114.95 | 192.168.114.96 | 192.168.114.97 | 192.168.114.98 | 192.168.114.99 | 192.168.115.0 | 192.168.115.1 | 192.168.115.2 | 192.168.115.3 | 192.168.115.4 | 192.168.115.5 | 192.168.115.6 | 192.168.115.7 | 192.168.115.8 | 192.168.115.9 | 192.168.116.0 | 192.168.116.1 | 192.168.116.2 | 192.168.116.3 | 192.168.116.4 | 192.168.116.5 | 192.168.116.6 | 192.168.116.7 | 192.168.116.8 | 192.168.116.9 | 192.168.117.0 | 192.168.117.1 | 192.168.117.2 | 192.168.117.3 | 192.168.117.4 | 192.168.117.5 | 192.168.117.6 | 192.168.117.7 | 192.168.117.8 | 192.168.117.9 | 192.168.118.0 | 192.168.118.1 | 192.168.118.2 | 192.168.118.3 | 192.168.118.4 | 192.168.118.5 | 192.168.118.6 | 192.168.118.7 | 192.168.118.8 | 192.168.118.9 | 192.168.119.0 | 192.168.119.1 | 192.168.119.2 | 192.168.119.3 | 192.168.119.4 | 192.168.119.5 | 192.168.119.6 | 192.168.119.7 | 192.168.119.8 | 192.168.119.9 | 192.168.120.0 | 192.168.120.1 | 192.168.120.2 | 192.168.120.3 | 192.168.120.4 | 192.168.120.5 | 192.168.120.6 | 192.168.120.7 | 192.168.120.8 | 192.168.120.9 | 192.168.121.0 | 192.168.121.1 | 192.168.121.2 | 192.168.121.3 | 192.168.121.4 | 192.168.121.5 | 192.168.121.6 | 192.168.121.7 | 192.168.121.8 | 192.168.121.9 | 192.168.122.0 | 192.168.122.1 | 192.168.122.2 | 192.168.122.3 | 192.168.122.4 | 192.168.122.5 | 192.168.122.6 | 192.168.122.7 | 192.168.122.8 | 192.168.122.9 | 192.168.123.0 | 192.168.123.1 | 192.168.123.2 | 192.168.123.3 | 192.168.123.4 | 192.168.123.5 | 192.168.123.6 | 192.168.123.7 | 192.168.123.8 | 192.168.123.9 | 192.168.124.0 | 192.168.124.1 | 192.168.124.2 | 192.168.124.3 | 192.168.124.4 | 192.168.124.5 | 192.168.124.6 | 192.168.124.7 | 192.168.124.8 | 192.168.124.9 | 192.168.125.0 | 192.168.125.1 | 192.168.125.2 | 192.168.125.3 | 192.168.125.4 | 192.168.125.5 | 192.168.125.6 | 192.168.125.7 | 192.168.125.8 | 192.168.125.9 |

Scan Summary

Nmap 7.94SVN was initiated at Sat Apr 20 04:27:44 2024 with these arguments:
`nmap -p1-65535 -T5 -A -v -oX assignment4.xml 192.168.114.1/24`

Verbosity: 1; Debug level 0

Nmap done at Sat Apr 20 04:30:56 2024; 256 IP addresses (1 host up) scanned in 192.66 seconds

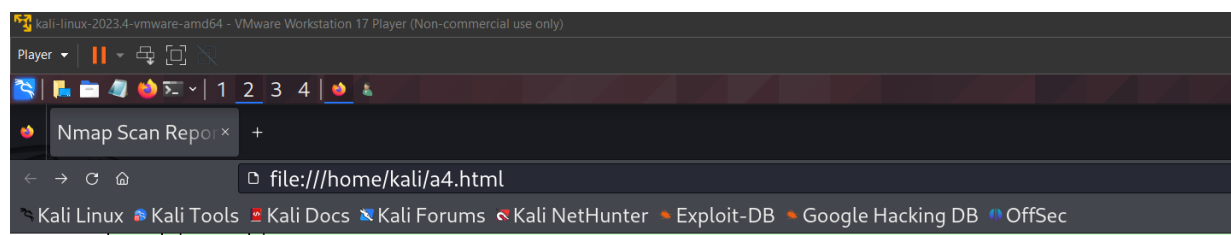
192.168.114.0 (click to expand)

192.168.114.1 / Krishnaraj-Home-PC

Address

- 192.168.114.1 (ipv4)

Hostnames



Remote Operating System Detection

- Used port: **135/tcp (open)**
- Used port: **38238/udp (closed)**
- OS match: **Microsoft Windows 11 21H2 (90%)**
- OS match: **Microsoft Windows 10 (87%)**
- OS match: **Microsoft Windows Server 2022 (86%)**
- OS match: **Microsoft Windows Server 2008 R2 (86%)**

Host Script Output

| Script Name | Output |
|--------------------|---|
| nbstat | NetBIOS name: KRISHNARAJ-HOME, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:01 (VMware) Names: KRISHNARAJ-HOME<20> Flags: <unique><active> KRISHNARAJ-HOME<00> Flags: <unique><active> WORKGROUP<00> Flags: <group><active> |
| smb2-security-mode | 3:1:1: Message signing enabled but not required |
| smb2-time | date: 2024-04-20T08:30:25 start_date: N/A |



5 Platform

Operating System: Arch Linux X8664

IDEs or Text Editors Used: Visual Studio Code

6 FAQs

1. What is the meaning of subnet?

- Subnet: Division of an IP network for efficient resource management.
- Facilitates organization and management of network devices and addresses.

2. Explain subnet mask? Meaning of /8, /16, /24, /32?

- Subnet Mask: Binary pattern dividing IP address into network and host portions.
- /8, /16, /24, /32 denote network size, representing the number of bits in the subnet mask.

3. What is NSE? Explain it.

- NSE (Nmap Scripting Engine): Automates Nmap's functionality for network reconnaissance and exploitation.

- Provides a framework for writing and executing scripts to enhance scanning capabilities.

4. Different flags for output supported by nmap.

- Nmap Output Flags: Include -oN (normal), -oG (grepable), -oX (XML), and -oA (all formats).
- Allow users to customize the format and content of Nmap scan results for analysis and reporting.

5. What is xsltproc? Explain it.

- xsltproc: Command-line tool for transforming XML documents using XSLT stylesheets.
- Facilitates conversion of XML data into different formats such as HTML, text, or other XML formats.

6. Why to see the output in HTML format than XML?

- HTML Output: Provides visually appealing presentation of Nmap scan results compared to XML.
- Allows for easier interpretation and analysis of scan data through structured formatting and styling.

7 Conclusion

In this assignment, we learned about the importance of network service scanning and organizing Nmap scan output. We explored the generation of Nmap scan results in XML and HTML formats to facilitate data analysis and reporting. By leveraging the capabilities of Nmap and related tools, we can enhance our understanding of network vulnerabilities and security risks. This assignment provided valuable insights into the practical aspects of vulnerability identification and penetration testing, which are essential skills for cybersecurity professionals.