NETWORK SCANNING USING NMAP

A PROJECT REPORT

Submitted by

Sai Charitesh [Reg No: RA21110300010171]

Sai Vardhan [Reg No: RA2111030010186]

Jaini Eswar [Reg No: RA2111030010190]

Under the Guidance of

DR B SOWMIYA

Assistant Professor, Department of Computing Technologies

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTING TECHNOLOGIES

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR– 603 203

NOV 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR–603 203

BONAFIDE CERTIFICATE

Certified that 18CSE412J/OFFENCIVE SECURITY project report titled "**Title of the project : NETWORK SCANNING USING NMAP**" is the bonafide work of **Sai charitesh [RegNo: RA2111030010171]** and **Sai Vardhan [RegNo: RA2111030010186] and Jaini Eswar[RA2111030010190]** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion for this or any other candidate.

signature

Faculty name

DR B SOWMIYA
Assistant Professor
Department of Computing Technologies

signature

HEAD OF THE DEPARTMENT

Dr.M .PUSHPALATHA
Department of Computing Technologies

Department of Computing Technologies

SRM Institute of Science and Technology

Own Work Declaration Form

Degree/Course :B.Tech in Computer Science and Engineering

Student Names : Sai Charitesh, Sai Vardhan, Jaini Eswar

Registration Number: RA2111030010171, RA2111030010186, RA2111030010190

Title of Work : **Network Scanning using NMAP**

I/We here by certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism, as listed in the University Website, Regulations, and the Education Committee guidelines.

I / We confirm that all the work contained in this assessment is our own except where indicated, and that we have met the following conditions:

- Clearly references / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web,etc.)
- Given the sources of all pictures, data etc that are not my own.

DECLARATION:
I am aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above. **Student 1 Signature:** **Student 2 Signature:** **Student 3 Signature:** **Date:**
If you are working in a group, please write your registration numbers and sign with the date for every student in your group.

- No made any use of the report(s) or essay(s) of any other student(s)either past or present
- Acknowledged in appropriate places any help that I have received from others (e.g fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course hand book / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

ABSTRACT

NMAP, a versatile and powerful open-source tool, operates by sending packets to target hosts and meticulously analyzing the responses. Its multifaceted functionality encompasses diverse scanning techniques, such as port scanning, version detection, OS fingerprinting, and vulnerability detection, allowing for a granular understanding of network configurations and potential security loopholes.This abstract explores the practice of network scanning through the lens of Nmap, a versatile and powerful open-source tool. Delving into the fundamentals of network reconnaissance, the paper elucidates Nmap's capabilities in discovering hosts, services, and vulnerabilities within a network. The discussion encompasses various scanning techniques, scripting, and advanced features that empower security professionals and network administrators to assess and fortify their systems. Additionally, the abstract highlights the ethical considerations and best practices associated with Nmap usage in the context of cybersecurity.

TABLE OF CONTENTS

1.INTRODUCTION

Network scanning plays a fundamental role in assessing the security posture of an organization's digital infrastructure. NMAP, an open-source network scanning tool, offers comprehensive capabilities for probing network hosts, identifying available services, and potential vulnerabilities. This report aims to provide an in-depth analysis of the methodology, significance, and ethical considerations associated with network scanning using NMAP.

In the contemporary landscape of cybersecurity, the need for robust network security measures is paramount. NMAP serves as a versatile tool in this domain, enabling network administrators and security professionals to conduct thorough scans to identify weaknesses, potential threats, and areas for improvement within their network architecture.

2.OBJECTIVE

The primary objective of this report is to outline the methodologies, benefits, and ethical considerations associated with employing NMAP for network scanning.

.The objective of network scanning using Nmap is to identify all hosts and services on a network. This information can be used for a variety of purposes, such as:

- Network inventory: Nmap can be used to create a complete inventory of all devices on a network, including their IP addresses, operating systems, and services. This information can be used to track network assets and identify potential security vulnerabilities.
- Security auditing: Nmap can be used to identify security vulnerabilities on a network. For example, Nmap can be used to find open ports that are not needed or services that are running insecure versions.
- Network troubleshooting: Nmap can be used to troubleshoot network problems. For example, Nmap can be used to identify why a particular host is unreachable or why a particular service is not working.

Nmap can be used to scan networks of any size, from small home networks to large enterprise networks. It is also available for a variety of operating systems, including Linux, Windows, and macOS.

3.REQUIREMENTS

- NMAP Software
- Permission and Authorization
- Knowledge and Understanding
- Network Access
- System Resources

4.METHODOLOGY

Find Devices connected to your Network

Command used : nmap -sP [IP ADDRESS]

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 20:45 UTC
Nmap scan report for 192.[redacted]
Host is up (0.022s latency).
Nmap scan report for 192.[redacted]
Host is up (0.029s latency).
Nmap scan report for 192.[redacted]
Host is up (0.00041s latency).
Nmap scan report for 192.[redacted]
Host is up (0.026s latency).
Nmap scan report for 192.[redacted]
Host is up (0.047s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.87 seconds
```

Find Open Ports of Devices

Command used : sudo nmap -sT [IP ADDRESS]

```
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
8654/tcp  filtered unknown
33354/tcp filtered unknown
MAC Address: 18:[redacted]

Nmap scan report for 192.[redacted]
Host is up (0.020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
1011/tcp filtered unknown
4848/tcp filtered appserv-http
MAC Address: 1A:[redacted]
```

```
Nmap scan report for 192.[redacted]
Host is up (0.0068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 30:[redacted]
```

Search For Specific Ports

Command used : sudo nmap -sT -p [PORT NUMBERS] [IP ADDRESS]

```
Nmap scan report for 192.[redacted]
Host is up (1.0s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address:[redacted]

Nmap scan report for 192.[redacted]
Host is up (0.27s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address:[redacted]
```

Use NMAP's Stealth mode

Command used : sudo nmap -sS [PORT NUMBERS] [IP ADDRESS]

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 80,443 192.[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 22:09 UTC
```

Detect the OS of a Device

Command used : nmap -O [IP ADDRESS]

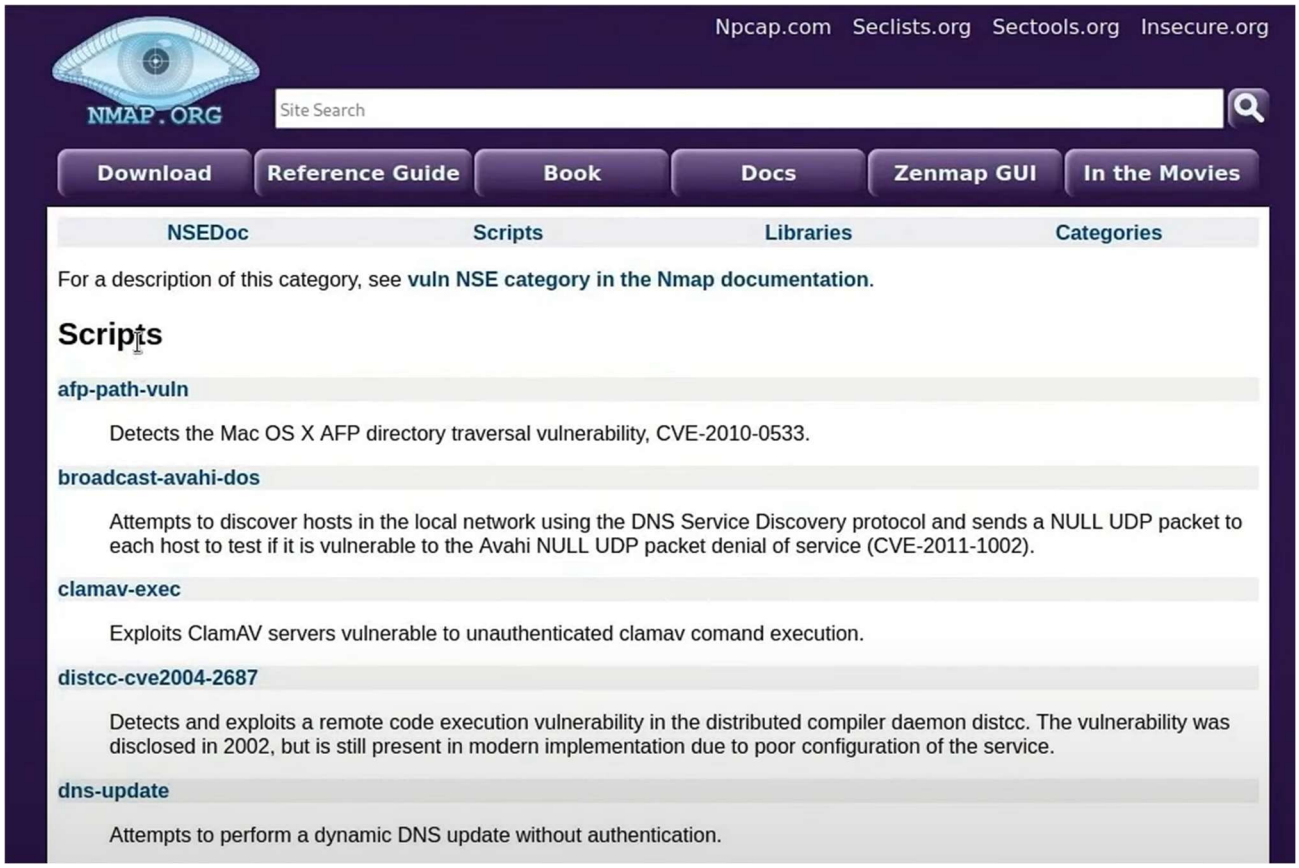
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 22:25 UTC
Nmap scan report for 192[redacted]
Host is up (0.057s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 30:14:4A:[redacted]
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (92%), AVtech embedded (87%), FreeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (92%), AVtech Room Alert 26W environmental monitor (87%), Micro
soft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

NMAP's Aggressive mode

Command used : sudo nmap -A [IP ADDRESS]

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 22:34 UTC
Nmap scan report for 192.[redacted]
Host is up (0.19s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 30:14:4A:[redacted]
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (91%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (91%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

NMAP in Scripts



ftp-vuln-cve2010-4221

Checks for a stack-based buffer overflow in the ProFTPD server, version between 1.3.2rc3 and 1.3.3b. By sending a large number of TELNET_IAC escape sequence, the proftpd process miscalculates the buffer length, and a remote attacker will be able to corrupt the stack and execute arbitrary code within the context of the proftpd process (CVE-2010-4221). Authentication is not required to exploit this vulnerability.

http-adobe-coldfusion-apsa1301

Attempts to exploit an authentication bypass vulnerability in Adobe Coldfusion servers to retrieve a valid administrator's session cookie.

http-aspnet-debug

Determines if a ASP.NET application has debugging enabled using a HTTP DEBUG request.

http-avaya-ipoffice-users

Attempts to enumerate users in Avaya IP Office systems 7.x.

http-awstatstotals-exec

Exploits a remote code execution vulnerability in Awstats Totals 1.0 up to 1.14 and possibly other products based on it (CVE: 2008-3922).

http-axis2-dir-traversal

Exploits a directory traversal vulnerability in Apache Axis2 version 1.4.1 by sending a specially crafted request to the parameter `xsd` (BID 40343). By default it will try to retrieve the configuration file of the Axis2 service `'/conf/axis2.xml'` using the path `'/axis2/services/'` to return the username and password of the admin account.

http-cookie-flags

Examines cookies set by HTTP services. Reports any session cookies set without the httponly flag. Reports any session cookies set over SSL without the secure flag. If http-enum.nse is also run, any interesting paths found by it will be checked in addition to the root.

5.Significance

The use of NMAP holds significant importance in network security:

- **Network Visibility:** Provides a detailed view of network architecture, aiding in network documentation and management.
- **Security Enhancement:** Identifies potential security loopholes, allowing for proactive security measures.
- **Access Control:** Helps in understanding open ports, allowing for better access control.

6.Ethical and Legal Considerations

- **Authorization:** Scanning networks should only be performed with explicit permission or for systems owned by the user conducting the scan.
- **Legal Compliance:** Unauthorized scanning can infringe upon privacy laws and the rights of system owners.
- **Responsible Use:** Adherence to ethical guidelines and legal frameworks is crucial to avoid legal consequences.

7.Advanced Nmap topics

- Scanning for specific services and versions: Nmap can be used to scan for specific services and versions on a network. This can be useful for identifying potential security vulnerabilities or troubleshooting network problems. For example, you can use the following command to scan for the SSH service running on all hosts on the 192.168.1.0/24 network:

```
nmap -sS -p 22 192.168.1.0/24
```

- Using Nmap to scan remote networks: Nmap can be used to scan remote networks by tunneling through a bastion host. This is useful for scanning networks that are not directly accessible from your network. For example, you can use the following command to scan the 192.168.2.0/24 network through the bastion host 192.168.1.1:

```
nmap -sS -p 22 192.168.2.0/24 -Pn 192.168.1.1
```

- The Nmap Scripting Engine (NSE): The NSE is a powerful scripting engine that can be used to extend Nmap's functionality. NSE scripts can be used to perform a variety of tasks, such as detecting security vulnerabilities, enumerating services, and gathering information about hosts and networks. For example, you can use the following command to run the NSE script `vulscan.nse` on all hosts on the 192.168.1.0/24 network:

```
nmap -sS -A -script vulscan.nse 192.168.1.0/24
```

Example NSE scripts:

Here are some example NSE scripts that you can use to perform advanced network scanning tasks:

- `vulscan.nse`: This script scans hosts for security vulnerabilities.
- `smb-enum-users.nse`: This script enumerates the users on a Windows host.
- `ssh-brute.nse`: This script attempts to brute-force SSH logins.
- `http-enum.nse`: This script enumerates the resources on a web server.
- `ftp-brute.nse`: This script attempts to brute-force FTP logins.

Best practices for advanced Nmap scanning:

- Be careful when using NSE scripts. Some scripts can be disruptive or even destructive.
- Be aware of the legal and ethical implications of advanced Nmap scanning.
- Only scan networks that you have permission to scan.
- Use Nmap's stealth scanning techniques to avoid detection.
- Be careful not to overload the network with traffic.
- Monitor your own network for unauthorized scans.

8.Recommendations

- Encourage regular network scans using NMAP to uphold network security.
- Ensure strict adherence to authorization protocols and legal guidelines in all scanning practices.
- Conduct training sessions to educate security professionals on responsible tool usage and compliance with laws and regulations.

9.Conclusion

The use of NMAP for network scanning is an indispensable practice for fortifying network security. It enables the identification of vulnerabilities and provides insights into network architecture. However, responsible and ethical utilization of this tool is paramount to prevent legal ramifications and maintain integrity within the cybersecurity domain.