



CS 6411 – Fundamentals of Info Assurance

Vulnerability Scanning with Nmap

Final Project Report

Submitted by

Ashique Arman

Table of Contents

1.1 What is Nmap?	2
1.2 Objective	2
1.3 Applications of Nmap	2
2. Methodology	3
2.1 Use-Case.....	3
2.2 Tools	3
2.3 Target hosts/websites	3
3. Demonstration of some useful Nmap commands	4
3.1 Basic commands	4
4. Vulnerability Scan	9
5. Discussion	10
References.....	11

1. Introduction

In today's dynamic IT environment, securing networks and web applications is vital. This project focuses on using Nmap, a versatile network scanning tool, to conduct thorough scans, identify vulnerabilities, and boost cybersecurity. The aim is to proactively assess and fortify digital infrastructure in the face of evolving threats.

1.1 What is Nmap?

Nmap, short for Network Mapper, is a powerful and versatile open-source tool used for network exploration and security auditing. It helps users discover devices and services on a computer network, find open ports, and identify their characteristics. Nmap is widely used by network administrators, security professionals, and ethical hackers to assess the security of a network, detect vulnerabilities, and create a map of the network topology. It employs a variety of scanning techniques to gather information about hosts and services, making it a valuable tool for both defensive and offensive security purposes.

1.2 Objective

The primary objective of this project is to leverage the capabilities of Nmap to perform systematic and thorough examinations of networks and websites. Through a combination of active and passive scanning techniques, we aim to provide a detailed analysis of the target systems, unveiling potential security gaps and weaknesses. The project will extend its focus to vulnerable websites, employing Nmap to pinpoint vulnerabilities that could be exploited by malicious actors.

1.3 Applications of Nmap

Here are some of the applications of Nmap:

- **IP Address Analysis:** Delve into detailed information on an IP address in a network to assess potential compromises, distinguishing between legitimate services and potential external threats.
- **Full Network Examination:** We can scan through networks and gain insights into those networks. For instance, we can check hosts, open ports, and even operating systems of connected devices.
- **OS Scanning:** Nmap has the capability to discover details about the operating system in use on various devices. It furnishes comprehensive information, including OS versions, facilitating the planning of additional strategies in the context of penetration testing.

- **Server Vulnerability Identification:** We can also use Nmap to expose server vulnerabilities. If we know about these vulnerabilities, then we can take steps to prevent them. This can be useful to protect personal as well as business websites.
- **Scripting Engine:** We can use the Nmap Scripting Engine (NSE), which is a powerful Nmap tool that involves utilizing the Network Mapper (Nmap) tool to perform a series of predefined tasks without manual intervention.

2. Methodology

2.1 Use-Case

Our project will include the following use cases:

- Perform a ping scan on the website's URL to retrieve active IP information.
- Conduct port scanning to uncover open ports on the target website.
- Execute host scan to figure out suspicious hosts connected to the network.

2.2 Tools

We have used the following tools for this project:

- Nmap
- Linux operating system
- Wireshark

2.3 Target hosts/websites

We have used the following hosts/websites for the purpose of this project:

- www.hackthissite.org
- www.juice-shop.herokuapp.com

3. Demonstration of some useful Nmap commands

Here, we have shown some useful Nmap commands:

3.1 Basic commands

Port Scan: Initially, to conduct a TCP connect scan using `-sT` code in our target website `www.hackthissite.org` as illustrated in Fig. 1.

```
(kali@kali)~$ sudo nmap -sT www.hackthissite.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 16:46 AST
Nmap scan report for www.hackthissite.org (137.74.187.102)
Host is up (0.077s latency).
Other addresses for www.hackthissite.org (not scanned): 137.74.187.1
:187:104 2001:41d0:8:ccd8:137:74:187:102
rDNS record for 137.74.187.102: hackthissite.org
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 12.97 seconds
```

Fig. 1: Port Scanning using NMap in Kali Linux.

Nmap establishes a full TCP connection by completing a three-way handshake process. During this scan Nmap sends a SYN packet to start the TCP connection whenever the target network or website has open ports it responds with a SYN-ACK packet. Finally, the Nmap completes its connection with an ACK packet. However, this is not a stealthy scan. Fig. 2 illustrates how the TCP connect scan works. In this case, the scan took 12.97 seconds and it demonstrated that the IP is up for communication.

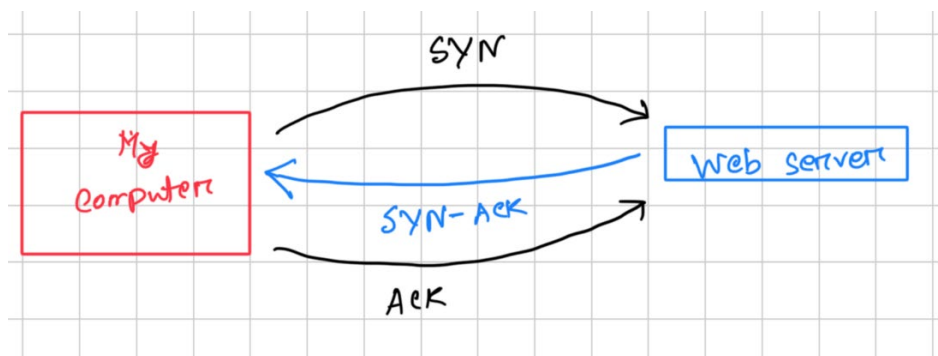
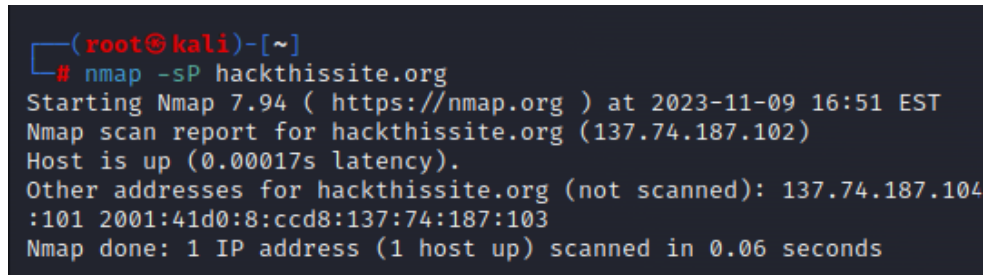


Fig. 2: Three-way handshake in TCP Connect scan.

Ping Scan: Ping scan shows all the active ip that are active on the scanned network. Fig. 3 illustrates the ping scanning script and output using Nmap in Linux environment. Here is the script:

nmap -sP hackthissite.org



```
(root@kali)-[~]
# nmap -sP hackthissite.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 16:51 EST
Nmap scan report for hackthissite.org (137.74.187.102)
Host is up (0.00017s latency).
Other addresses for hackthissite.org (not scanned): 137.74.187.104
:101 2001:41d0:8:ccd8:137:74:187:103
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

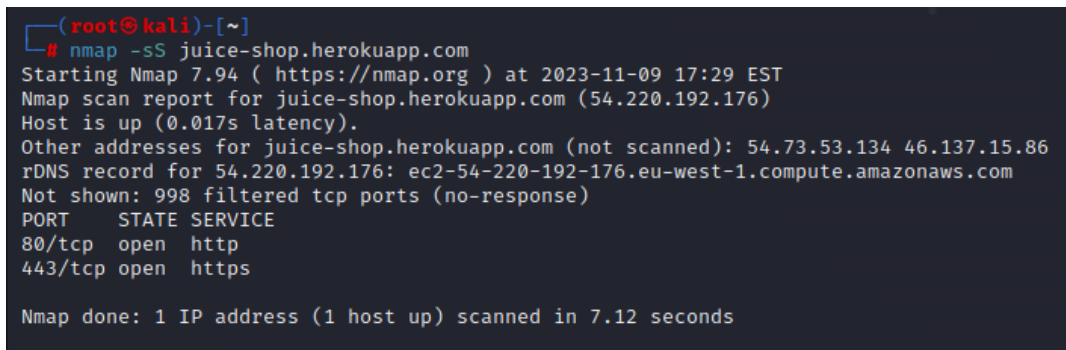
Fig. 3: Ping Scan using Nmap.

From this output, we get to know the following:

- Target scanned: "hackthissite.org" (IP: 137.74.187.102).
- Host is up with a low latency of 0.00017 seconds.
- Additional IP addresses for "hackthissite.org" are listed, but not scanned.
- Scan completed in 0.06 seconds, identifying 1 host as up.

Stealth Scan: Stealth scanning works by sending a SYN packet and checking the response. If you get a SYN/ACK, it means the port is open, and you can establish a TCP connection. The unique thing about a stealth scan is that they don't finish the 3-way handshake, making it tricky for the target to figure out the scanning system. In Fig. 4 we can observe a stealth scan conducted on our target website. Here is the script:

Nmap -sS juice-shop.herokuapp.com



```
(root@kali)-[~]
# nmap -sS juice-shop.herokuapp.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 17:29 EST
Nmap scan report for juice-shop.herokuapp.com (54.220.192.176)
Host is up (0.017s latency).
Other addresses for juice-shop.herokuapp.com (not scanned): 54.73.53.134 46.137.15.86
rDNS record for 54.220.192.176: ec2-54-220-192-176.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 7.12 seconds
```

Fig. 4: Stealth scan in Kali Linux using NMAP.

From this output, we can observe the following:

- Stealth Nmap scan executed on "juice-shop.herokuapp.com" (IP: 54.220.192.176).
- Host is up with a latency of 0.017 seconds.
- Additional IP addresses listed but not scanned.

- An rDNS record for the target's IP address is provided, linking it to "ec2-54-220-192-176.eu-west-1.compute.amazonaws.com." This information can aid in understanding the hosting environment without explicitly revealing the scanning intent.

OS Detection

Fig. 5 shows the conducted operating system detection in the website. However, the tool was unable to detect the exact match of the operating system the website was using.

```
(kali@kali)~$ sudo nmap -O www.hackthissite.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 18:02 AST
Nmap scan report for www.hackthissite.org (137.74.187.102)
Host is up (0.059s latency).
Other addresses for www.hackthissite.org (not scanned): 137.74.187.104 137.74.187.103 137.74.187.101 137.74.187.100 2001:41d0:8:ccd8:137:74:187:104 2001:41d0:8:ccd8:137:74:187:103 2001:41d0:8:ccd8:137:74:187:102
rDNS record for 137.74.187.102: hackthissite.org
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
Device type: bridge[general purpose]switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds
```

Fig. 5: Complete OS detection with Nmap.

This scan predicted that the OS can be oracle virtual box (95%) QEMU or Quick EMUlator (91%) or it can be Bay Networks (86%) from this we have the information the target website might be running in a simulation environment. Moreover, in the scan that we have conducted before we were unable to find any closed website but in this OS detection method we can see an SSH port 22/TCP which is closed. This can be important information for any attack or vulnerability check of the target website. Important information is revealed during this test which shows that the test condition is non ideal.

Possible reason for non-ideal test condition:

- Firewall that filters probes sent by Nmap so that it becomes difficult to acquire information about the host.
- Rate limiting techniques to mitigate the impact of scanning and save the website from DDOS attacks.
- The host configuration may have been hardened.
- Responsive Network protections can make the target to take adaptive security measures or feed false information.

By seeing the host does not provide ideal test conditions it will become a little bit harder for anyone to attack the website. However, there are some more vulnerabilities are there which will be discussed further in this report.

Removing Footstep from the target:

The use of the Decoy feature is an approach in Nmap to evade detection when proving a target network for vulnerabilities The `-D` option added in Nmap is used for using different decoys during a scan. If we mix it up with a stealth scan it makes it hard to track.

The way it works is:

- Nmap spreads the decoy IP addresses with the real IP address inside the packets sent to the target.

- It seems to the website or network you are observing that the scan is coming from multiple sources from the decoy IP.
- Resulting the tracking of your own IP address confusing for the target and it helps to anonymize the real source of scan.

This process is conducted on the hackthissite.org website whose IP address is 137.74.187.101 you the virtual machine that we are using for this case has an IP address of 10.0.2.15 during the scan we have monitored the network traffic using Wireshark to see the destination and source IP addresses to check if the decoy is working. One can use many decoy ip address to clock their identity however in this case we have used only one IP address 10.1.1.1 for understanding. The code for this process is as follows:

```
sudo nmap -sS -D 10.1.1.1 www.hackthissite.org
```

Fig.6 shows the terminal code of the decoy using Nmap followed by Fig. 7 which illustrates the network traffic observed through the Wireshark.

```
(kali㉿kali)-[~]
$ sudo nmap -sS -D 10.1.1.1 www.hackthissite.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 19:45 AST
Nmap scan report for www.hackthissite.org (137.74.187.101)
Host is up (0.10s latency).
Other addresses for www.hackthissite.org (not scanned): 137.74.187.104 137.
:187:104 2001:41d0:8:ccd8:137:74:187:100
rDNS record for 137.74.187.101: hackthissite.org
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 51.83 seconds
```

Fig. 6: Using decoy in Nmap.

No.	Time	Source	Destination	Protocol	Length	Info
19	0.176263157	10.0.2.15	137.74.187.101	TCP	58	45550 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.176278258	10.1.1.1	137.74.187.101	TCP	58	45550 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.176294039	10.0.2.15	137.74.187.101	TCP	58	45550 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.176312405	10.1.1.1	137.74.187.101	TCP	58	45550 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.176333634	10.0.2.15	137.74.187.101	TCP	58	45550 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	0.176347644	10.1.1.1	137.74.187.101	TCP	58	45550 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	0.176363995	10.0.2.15	137.74.187.101	TCP	58	45550 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	0.176378616	10.1.1.1	137.74.187.101	TCP	58	45550 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	0.176394217	10.0.2.15	137.74.187.101	TCP	58	45550 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	0.176429677	10.1.1.1	137.74.187.101	TCP	58	45550 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Fig. 7: Network traffic during decoy observed in Wireshark.

In Fig. 7 we can observe that the source IP address alters between two IP addresses one is our virtual machine 10.0.2.15 and another is 10.1.1.1 which is our decoy. The destination remains the same as our target IP address. We can modify the code so that instead of sending one decoy we will be able to send multiple decoys. The modification is provided;

```
sudo nmap -sS -D 10.1.1.1, 10.1.1.2, 10.1.1.3 www.hackthissite.org
```

We can add more IP addresses using a comma at the end to increase decoy.

Aggressive Scan: This scan can do OS detection, version detection, script scanning, and traceroute which is illustrated in Fig. 8 Here is the script:

`nmap -A hackthissite.org`

```
(root@kali)~# nmap -A hackthissite.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 16:39 EST
Nmap scan report for hackthissite.org (137.74.187.102)
Host is up (0.016s latency).
Other addresses for hackthissite.org (not scanned): 137.74.187.104 137.74.187.100 137.74.187.103 137.74.187.101 2001:41d0:8:ccd8:137:74:187:104 2001:41d0:8:101:2001:41d0:8:ccd8:137:74:187:103
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http-proxy     HAProxy http proxy 1.3.1 or later
|_http-open-proxy: Proxy might be redirecting requests
443/tcp   open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
|_ssl-cert: Subject: commonName=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
| Subject Alternative Name: DNS=hackthissite.org, DNS=www.hackthissite.org, DNS=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
|_Not valid before: 2023-04-03T06:47:49
|_Not valid after: 2024-04-02T06:47:49
|_http-title: Hack This Site
|_http-server-header: HackThisSite
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Device: load balancer

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.26 ms 10.0.2.2
2 0.30 ms hackthissite.org (137.74.187.102)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.89 seconds
```

Fig. 8: Aggressive Scanning script and output in Kali Linux using NMAP

From this result, we can interpret the following:

- Responsive host with low latency (IP: 137.74.187.102).
- Multiple IP addresses, but only one (137.74.187.102) was scanned.
- Open Ports and Services:
 - Port 80/tcp: HAProxy http proxy.
 - Port 443/tcp: SSL-enabled HAProxy http proxy with an onion domain certificate.
 - 998 filtered TCP ports (no response).
- Device and OS:
 - Identified as a load balancer.
 - Possible devices: Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%).
 - No exact OS match due to non-ideal conditions.
- Network:
 - Target is 2 hops away.
- Traceroute:
 - Two hops: 10.0.2.2 and hackthissite.org (137.74.187.102).
- Warning:
 - Unreliable OS Scan results.
- Scan Duration: Aggressive scan took 108.89 seconds.

4. Vulnerability Scan

We will do a vulnerability check using ‘Nmap vuln’ for the website: ‘www.juice-shop.herokuapp.com’. Here is the script required for this task:

```
nmap -Pn --script vuln www.juice-shop.herokuapp.com
```

```
(root@kali)~# nmap -Pn --script vuln juice-shop.herokuapp.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 18:14 EST
Nmap scan report for juice-shop.herokuapp.com (54.229.192.176)
Host is up (0.13s latency).
Other addresses for juice-shop.herokuapp.com (not scanned): 54.73.53.134 46.137.15.86
rDNS record for 54.229.192.176: ec2-54-229-192-176.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|   State: VULNERABLE
|   IDs:  BID:49303  CVE:CVE-2011-3192
|   The Apache web server is vulnerable to a denial of service attack when numerous
|   overlapping byte ranges are requested.
|   Disclosure date: 2011-08-19
|   References:
|   https://www.tenable.com/plugins/nessus/55976
|   https://seclists.org/fulldisclosure/2011/Aug/175
|   https://www.securityfocus.com/bid/49303
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|   State: UNKNOWN (unable to test)
|   IDs:  CVE:CVE-2005-3299
|   PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|   Disclosure date: 2005-10-nil
|   Extra information:
|   .. / .. / .. / .. / etc/passwd :
|
| --
| - Copyright (c) 2014-2023 Bjoern Kimminich & the OWASP Juice Shop contributors.
| - SPDX-License-Identifier: MIT
| -><!DOCTYPE html><html lang="en"><head>
| <meta charset="utf-8">
| <title>OWASP Juice Shop</title>
| <meta name="description" content="Probably the most modern and sophisticated insecure web application">
| <meta name="viewport" content="width=device-width, initial-scale=1">
| <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon.js.ico">
| <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">
| <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
| <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
| <script>
|   window.addEventListener("load", function(){
|     window.cookieconsent.initialise({
```

Fig. 9: Vulnerability scan of our target website.

Fig. 9 shows the whole output that we have found after we ran the beforementioned script for the vulnerability check on our target website.

The output exposes a huge number of vulnerabilities of the target website. Here are some of the vulnerabilities that are found:

- phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion (CVE-2005-3299). PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1.
Description: Allows remote attackers to include local files via the \$__redirect parameter, possibly involving the subform array.
- Apache byterange filter DoS (CVE-2011-3192).
Description: The Apache web server is vulnerable to a denial-of-service (DOS) attack when numerous overlapping byte ranges are requested.

5. Discussion

In this project, our goal was to learn how to use NMAP and how it can be used for network scanning and find potential security gaps and weaknesses of our target website. At first, we have done multiple types of port scanning which is required to understand the pathways to enter any website or network. By using scanning techniques, we can find the open port. While learning the tool it is essential to understand different types of scanning techniques so that we can use the proper technique that is required based on any cases. At first, we did port scanning which is a basic scanning technique used to discover open ports to identify the entry point of any Network. One might argue that why not use a stealth scan as it can make you invisible by any firewall? That is because the port scan can send faster and more amount packets in a shorter amount of time and it is more likely to provide a comprehensive list of open ports to a target system which cannot be provided by a stealth scan. Later, we have learned how to do a stealth scan on our target website. Whenever we want to enter any network undetected, we can use this scanning technique to gather information without alerting the target system security mechanism. We have found two open ports of our target website as well without the knowledge of the target security system.

While attacking any website it is essential to know the characteristics of the target to create a foolproof plan of attack. Among the important features of any network, the operating system is believed as a core characteristic. For that, we have learned OS detection using NMAP which is a very important feature required while scanning. However, while practicing it on the website we did not find the exact operating system but based on the characteristics of the website it provided the percentage of the operating system the website might run on.

To gather information from the target we do not want to let the target know about our location in that case the decoy scan of NMAP comes in handy. Using the decoy, you can send the same scan from many IP addresses which will confuse the target system security and any human who might check the network traffic. To prove that we have used Wireshark while deploying decoy code using NMAP.

Unlike other scanning techniques, we have an aggressive scanning technique that is differentiated from others by its thoroughness. It implements a group of techniques to find out ports, services, and weaknesses. It can provide us with an exhaustive analysis of the security system. The problem with this scanning is one must be cautious while using this technique as it can trigger a security alert as it tries to gather all the information aggressively from the target.

Finally, we have the vulnerability scan which is used particularly to find the weaknesses in the system. This scan was used to find valuable insights into the security posture of our target by examining open ports, services, and versions. By using this we have gathered information that our target website was vulnerable to DOS attack at the Apache web server and it allowed remote attackers to include files in the system.

In conclusion, these various techniques equip a person with a comprehensive toolkit to assess and fortify digital security. Together these methodologies empower security professionals to proactively identify, analyze, and mitigate risks, ultimately enhancing the resilience of systems and networks against evolving cybersecurity threats.

References

[1] K. Sen, “How to use nmap: Upguard,” RSS, <https://www.upguard.com/blog/how-to-use-nmap> (accessed Nov. 20, 2023).

[2] M. Shivanandhan, “What is nmap and how to use it – a tutorial for the greatest scanning tool of all time,” freeCodeCamp.org, <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/> (accessed Nov. 20, 2023).

[3] E. BORGES, “Securitytrails,” SecurityTrails, <https://securitytrails.com/blog/nmap-vulnerability-scan> (accessed Nov. 20, 2023).