Using NMAP to find Vulnerabilities in TCP and UDP Ports

Zachary Kein – 220277143

Contents

Discovering the IP for further analysis

Finding server's IP:

```
user@Ubuntu1804:~$ nslookup master-mop-busaytgm.ts.gateway.dev
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   master-mop-busaytgm.ts.gateway.dev
Address: 216.239.36.56
Name:   master-mop-busaytgm.ts.gateway.dev
Address: 2001:4860:4802:36::38
```

Pinging to see if running correctly:

```
user@Ubuntu1804:~$ ping 216.239.36.56
PING 216.239.36.56 (216.239.36.56) 56(84) bytes of data.
64 bytes from 216.239.36.56: icmp_seq=1 ttl=57 time=22.7 ms
64 bytes from 216.239.36.56: icmp_seq=2 ttl=57 time=25.9 ms
64 bytes from 216.239.36.56: icmp_seq=3 ttl=57 time=26.3 ms
64 bytes from 216.239.36.56: icmp_seq=4 ttl=57 time=25.1 ms
64 bytes from 216.239.36.56: icmp_seq=5 ttl=57 time=26.8 ms
64 bytes from 216.239.36.56: icmp_seq=6 ttl=57 time=28.5 ms
64 bytes from 216.239.36.56: icmp_seq=7 ttl=57 time=49.1 ms
64 bytes from 216.239.36.56: icmp_seq=8 ttl=57 time=17.6 ms
64 bytes from 216.239.36.56: icmp_seq=9 ttl=57 time=18.2 ms
64 bytes from 216.239.36.56: icmp_seq=10 ttl=57 time=29.7 ms
^C
--- 216.239.36.56 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 17.693/27.030/49.159/8.298 ms
user@Ubuntu1804:~$
```

Finding that the IP for the MOP website is 216.239.36.56, it allows us to use NMAP to find information on the ports for the website.

Performing TCP Scans

Performing OS detection & finding which TCP ports are open:

```
user@Ubuntu1804:~$ sudo nmap -O 216.239.36.56

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-30 16:00 AEDT
Nmap scan report for 216.239.36.56
Host is up (0.0099s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
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 20.94 seconds
user@Ubuntu1804:~$
```

Scanning all 65535 TCP ports in case there are more than the 1000 in normal scan:

```
user@Ubuntu1804:~$ sudo nmap -sT -p  1-65535 216.239.36.56

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-30 16:44 AEDT
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.91% done; ETC: 16:50 (0:05:34 remaining)
Stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 8.29% done; ETC: 17:00 (0:14:23 remaining)
Stats: 0:04:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 20.43% done; ETC: 17:04 (0:15:35 remaining)
Stats: 0:06:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 29.51% done; ETC: 17:04 (0:14:22 remaining)
Stats: 0:10:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 51.78% done; ETC: 17:05 (0:10:13 remaining)
Stats: 0:21:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.66% done; ETC: 17:06 (0:00:17 remaining)
Nmap scan report for 216.239.36.56
Host is up (0.024s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1298.21 seconds
user@Ubuntu1804:~$
```

Examination of TCP Scan Results

Ports 80 and 443 can be susceptible to an attack. They are commonly targeted by attackers due to them being used for web traffic. This makes it a common entry point when attackers are looking to breach a web server. This port is essential for communication between web servers and clients, but it is also a prime target for attackers who want to compromise systems or steal sensitive information.

Examples of the different attacks that may be used to exploit the open ports are:

- HTTP Request Smuggling
- SQL injections
- Man-in-the-middle attacks
- Cross-site scripting (XSS)
- DDoS attacks

To mitigate the risk of attacks on ports 80 and 443, it is important to have measures in place that ensure these ports remain secure as they are seen as a significant security risk as they need to remain open. Some steps to take to keep these ports as secure as possible are:

1. Using encryption (HTTPS) to ensure traffic remains encrypted
2. Keeping software up to date with automatic updates and regular manual checks
3. Setting up and using a firewall
4. Implementing strong access controls
5. Regularly auditing the web server
6. Testing security to prepare for attacks

TCP Port Attacks and Prevention

HTTP Request Smuggling:

HTTP Request Smuggling is a technique used to bypass security measures such as firewalls and load balancers. Attackers use this technique to split HTTP requests into smaller packets, each of which can be processed by the server in different ways, leading to unexpected behaviour.

To mitigate HTTP Request Smuggling, organizations should implement the latest versions of web servers that can detect and prevent this kind of attack. They should also use a Web Application Firewall (WAF) to filter out suspicious traffic.

Cross-Site Scripting (XSS):

Cross-site scripting (XSS) is a type of attack that injects malicious scripts into web pages viewed by other users. This attack is possible when a web application fails to properly sanitize user input.

To mitigate XSS attacks, organizations should implement input validation and output sanitization in their web applications. Additionally, they should use a Content Security Policy (CSP) to restrict the types of content that can be loaded by their web pages.

Man-in-the-Middle (MitM) Attacks:

Man-in-the-Middle (MitM) attacks are a type of attack where an attacker intercepts communication between two parties to steal data or modify messages. In the context of

port 443, an attacker could intercept HTTPS traffic to steal sensitive information or inject malware into web pages.

To mitigate MitM attacks, organizations should use SSL/TLS certificates from trusted certificate authorities (CAs) to ensure that the communication is encrypted and not tampered with. They should also use modern cipher suites to ensure the strongest encryption possible. Additionally, implementing HTTP Strict Transport Security (HSTS) ensures that the website can only be accessed through HTTPS.

SQL Injection:

SQL Injection is a type of attack that exploits vulnerabilities in web applications that use SQL databases. Attackers use this technique to inject malicious SQL commands into web forms or other inputs, allowing them to access or modify sensitive data.

To mitigate SQL Injection attacks, organizations should implement input validation and parameterized SQL queries in their web applications. They should also use a WAF to detect and prevent SQL Injection attacks.

Distributed Denial of Service (DDoS):

A Distributed Denial of Service (DDoS) attack is a type of attack in which a large number of computers, typically compromised by malware, flood a target server with traffic, rendering it unavailable to legitimate users.

To mitigate DDoS attacks, organizations should use a content delivery network (CDN) to distribute traffic and absorb attacks. They should also implement rate limiting and traffic filtering to prevent traffic from known malicious IP addresses.

Performing UDP Scan

Performing scan to see what UDP ports are open:

```
user@Ubuntu1804:~$ sudo nmap -sU 216.239.36.56

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-30 17:27 AEDT
Nmap scan report for 216.239.36.56
Host is up (0.00049s latency).
All 1000 scanned ports on 216.239.36.56 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
```

Scan attempted to see all 65535 UDP ports, however due to its ETA being 2+ hours to complete and seeing that the normal 1000 port scan showed all were open | filtered, it is not necessary to see all UDP ports.

Examination of UDP Scan Results

The MOP website currently has all of its UDP ports open which is not necessary. It is generally not recommended to have any unnecessary ports open due to the inherent security risk of many different pathways to unlawful entry.

There are quite a few security risks that having all UDP ports open can have on the website. Some of these security risks can include:

1. Attackers may use the open ports to gain access to the system via brute force
2. Vulnerable DNS and SNMP services may be exploited
3. There is an increased risk of DoS attacks
4. Open UDP ports may lead to sensitive data being intercepted, leading to a data leakage

A way to minimise these risks is to find out which UDP ports should remain open on the system. Only certain UDP ports need to remain open which depends on the requirements of the system and the applications that are running on it. There are some common UDP ports that generally remain open on any website if the specific services are used. These can be:

- Port 53: DNS (Domain Name System)
- Port 68: DHCP (Dynamic Host Configuration Protocol)
- Port 69: TFTP (Trivial File Transfer Protocol)
- Port 123: SNMP (Simple Network Management Protocol)
- Port 169: NTP (Network Time Protocol)

Not every website will need to make use of all the common ports listed, however it is important to check what the website uses before closing certain ports to prevent the website crashing.

It is important to only have the necessary ports open on your website to limit potential attack vectors for malicious actors. You should consult with your web hosting provider or a cybersecurity expert to determine which ports are necessary for your website's specific needs and ensure that only those ports are open.