Exercise 05

Esteban Calvo

2023-10-17

Contents

1 Attack Narrative

1.1 TCP Scan

To run an nmap scan on arts tailor shop, the following command was performed

```
sudo nmap -sV -O www.artstailor.com
```

and this yielded the following results:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-20 22:14 EDT
Nmap scan report for www.artstailor.com (172.70.184.133)
Host is up (0.00058s latency).
rDNS record for 172.70.184.133: ns.artstailor.com
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
53/tcp open  domain  ISC BIND 9.18.16-1~deb12u1 (Debian Linux)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
No exact OS matches for host (If you know what OS is running on it, see
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/20%OT=22%CT=1%CU=43456%PV=N%DS=2%DC=I%G=Y%TM=650B
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%II=I%TS=A)OPS(O
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11N
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 25.18 seconds
```

From this command, we can several open ports as well as their operating system. These ports are pretty standard ports and there was not much to observere here.

1.2 UDP Scan

To run nmap on the UDP ports, we used the command

```
sudo nmap -sU -p 1-256 -sV www.artstailor.com
```

and got the following results:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-20 22:35 EDT
Nmap scan report for www.artstailor.com (172.70.184.133)
Host is up (0.00066s latency).
rDNS record for 172.70.184.133: ns.artstailor.com
Not shown: 254 closed udp ports (port-unreach)
PORT   STATE         SERVICE VERSION
40/udp open|filtered unknown
53/udp open          domain  ISC BIND 9.18.16-1~deb12u1 (Debian Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http
Nmap done: 1 IP address (1 host up) scanned in 369.53 seconds
```

Here, the interesting port was port 40 which may be a threat if it is running tcp, but there was little to suggest that this port was a threat in the current state.

1.3 Comparison

From the scan, we can clearly see that TCP is much faster than UDP considering that tcp scanned 1000 ports and ran in 25 seconds while UDP scanned 256 ports and took 370 seconds. The reason for this lies in the protocol itself as a three-way handshake is much easier to establish using TCP and UDP's stateless protocol.

1.4 Searchsploit

Using Searchsploit on all the ports did not reveal any potential vulnerabilites. It is possible There previously some vulnerabilities that have been patched with recent updates, but there is no reason to belive that the current setup has any real risks.

1.5 Key

To find the key, wireshark was used to examine the packets sent to the suspicous UDP port 40. Here, some of the packets sent back and forth contained the key which turned out to combine to:

```
KEY007-52kyxvjHNa8SNF/s55JH0A
```

1.6 Findings

Running both the TCP and the UDP scan, there were no vulnerabilites found.

1.6.1 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance
T1595: Active Scanning
.002: Vulnerability Scanning

TA0043: Reconnaissance
T1592: Gather Victim Host Information
.001: Hardware

TA0043: Reconnaissance
T1592: Gather Victim Host Information
.002: Software