Ex050 - Nmap

Simon Tobon

2021-07-08

Contents

Executive Summary

For this exercise we were tasked to use nmap to explore the services available on the machine www.f4rmc0rp.com. Using this list of services we then explore any vulnerabilities.

Technical Report

Finding: Description of finding

Vulnerability Description

- **OpenSSH 7.9:** "due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred."
- **Debian Linux 10:** "Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash." Exim is a message transfer agent, i.e., email.
- **ISC BIND 9.11.5:** "buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query." There is also a METASPLOIT module available for this vulnerability.
- **Apache 2.4.38:** "In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected." This version of Apache is also full of exploits such as a Local Privilege escalation exploit that can be found here: https://www.exploit-db.com/exploits/46676

Attack Narrative

To begin the Exercise I opened up Wireshark and prepared it for listening. I then ran an nmap TCP version scan on www.f4rmc0rp.com with the following command: **nmap -sV www.f4rmc0rp.com**. This command listed 5 open ports and several service and OS INFO, as can be seen below.

```
kali@kali:~$ nmap -sV www.f4rmc0rp.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:42 EDT
Nmap scan report for www.f4rmc0rp.com (172.30.0.128)
Host is up (0.00026s latency).
rDNS record for 172.30.0.128: ns.f4rmc0rp.com
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp   open  domain  ISC BIND 9.11.5-P4-5.1+deb10u1 (Debian Linux)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
443/tcp  open  ssl/ssl Apache httpd (SSL-only mode)
2121/tcp open  ftp     vsftpd 2.3.4
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
```

From Wireshark I saw that the majority of packets were TCP as expected since we ran a TCP version scan. I could not find a KEY from any ICMP packets for this domain.

Then a nmap UDP version scan on the same machine was run, this time only for ports 1-256, with the following command: **sudo nmap -sU -sV -p 1-256 www.f4rmc0rp.com**. This scan was also monitored by Wireshark. As expected many of the packets were UDP and of course others ICMP. nmap was able to find 2 open ports and other information as seen below.

```
kali@kali:~$ sudo nmap -sU -sV -p 1-256 www.f4rmc0rp.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 12:25 EDT
Nmap scan report for www.f4rmc0rp.com (172.30.0.128)
Host is up (0.00065s latency).
rDNS record for 172.30.0.128: ns.f4rmc0rp.com
Not shown: 254 closed ports
PORT   STATE         SERVICE VERSION
40/udp open|filtered unknown
53/udp open          domain  ISC BIND 9.11.5-P4-5.1+deb10u1 (Debian Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 371.68 seconds
```

Out of the 2 scans the UDP version scan took significantly longer. It took about 6 minutes as opposed to the TCP scan taking about 13 seconds. The TCP version scan even scanned more ports than the UDP did. This can be easily explained however, in a TCP scan if the other server is responds saying "no one is home" it terminates and moves on. While in a UDP scan there's no such response, so nmap kinda waits and lingers there for a while then finally gives up. Something interesting to me was that port 40 was both open and filtered.

Using this information several security vulnerabilities were researched for each of the services, they are described in greater detail in the Vulnerability Description section.

Finally, through both the use of nmap and Wireshark a KEY was found. This occured in an ICMP packet that wireshark picked up when running the nmap UDP version scan. The key is as follows: **KEY007:lYk6V+e8i1mYqtSZRk42xA==**.

References

- exploit-db.com
- cvedetails.com