CHAMELEON

FOR OUR SMARTER WORLD

Port Scan (MOP)

Adam Sarin
217342706

Contents

Introduction:

This goal of this report is to conduct a port scan on the MOP site, both the site being hosted that was provided to us for testing purposes: https://react-test-6najyje5cq-uc.a.run.app/
As well as the MOP site that is linked on the official Github: https://melbourne-open-playground.vercel.app/
Most of the information on how we will run these port scans is provided by the nmap official book about port scanning.

Tools used:

- Kali Linux
- Nmap

Scope of Testing

The scope of our testing will be solely the MOP site, which we will not have any prior knowledge of the inner workings of the site, nor GCP access to the site, all tests will be performed as an outsider with no permissions with the intention of identifying open ports and potential vulnerabilities of the network the website is hosted on.

Methodology

Firstly we are going to be running basic entry scans on both MOP sites, which as outlined in the documentation for nmap is as simple as calling nmap with the url you want to scan.

Example 4.2. Simple scan: nmap scanme.nmap.org

```
# nmap scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  closed smtp
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

After we will run nmap with more advanced flags also provided in the nmap tutorial which will use:
“-p0-“ – making nmap scan every possible TCP port
“-v” – run nmap in verbose mode to provide us more information with each scan
“-A” – enable aggressive tests such as remote OS detection
“-T4” – enables a more aggressive timing policy which speeds up the scan.

Results

Firstly the simple scans on both MOP sites:

```
┌──(kali㉿kali)-[~]
└─$ nmap react-test-6najyje5cq-uc.a.run.app
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 07:52 EDT
Nmap scan report for react-test-6najyje5cq-uc.a.run.app (216.239.36.53)
Host is up (0.0059s latency).
Other addresses for react-test-6najyje5cq-uc.a.run.app (not scanned): 216.239.38.53 216.239.32
.53 216.239.34.53 2001:4860:4802:38::35 2001:4860:4802:32::35 2001:4860:4802:34::35 2001:4860:
4802:36::35
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 4.82 seconds
```

Other then port 80 and port 443, nothing else identified, which is normal.

```
┌──(kali㉿kali)-[~]
└─$ nmap melbourne-open-playground.vercel.app
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 07:53 EDT
Nmap scan report for melbourne-open-playground.vercel.app (76.76.21.164)
Host is up (0.0072s latency).
Other addresses for melbourne-open-playground.vercel.app (not scanned): 76.76.21.9
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 5.12 seconds
```

Once again nothing found other then port 80 and port 443, so both sites are looking secure on the open port front, but let's run our advanced tests to identify maybe something the simple scan missed:

```
Completed NSE at 07:56, 0.00s elapsed
Initiating NSE at 07:56
Completed NSE at 07:56, 0.00s elapsed
Initiating Ping Scan at 07:56
Scanning react-test-6najyje5cq-uc.a.run.app (216.239.34.53) [2 ports]
Completed Ping Scan at 07:56, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:56
Completed Parallel DNS resolution of 1 host. at 07:56, 0.20s elapsed
Initiating Connect Scan at 07:56
Scanning react-test-6najyje5cq-uc.a.run.app (216.239.34.53) [65536 ports]
Discovered open port 80/tcp on 216.239.34.53
Discovered open port 443/tcp on 216.239.34.53
Increasing send delay for 216.239.34.53 from 0 to 5 due to 11 out of 17 dropped probes since l
ast increase.
Connect Scan Timing: About 4.10% done; ETC: 08:08 (0:12:05 remaining)
Connect Scan Timing: About 8.15% done; ETC: 08:10 (0:13:09 remaining)
Connect Scan Timing: About 12.49% done; ETC: 08:10 (0:12:23 remaining)
Connect Scan Timing: About 20.03% done; ETC: 08:10 (0:11:39 remaining)
Connect Scan Timing: About 26.48% done; ETC: 08:10 (0:10:52 remaining)
Connect Scan Timing: About 31.96% done; ETC: 08:10 (0:10:02 remaining)
Connect Scan Timing: About 37.07% done; ETC: 08:10 (0:09:17 remaining)
Connect Scan Timing: About 43.09% done; ETC: 08:11 (0:08:29 remaining)
Connect Scan Timing: About 48.64% done; ETC: 08:11 (0:07:40 remaining)
Connect Scan Timing: About 53.82% done; ETC: 08:11 (0:06:53 remaining)
Connect Scan Timing: About 59.12% done; ETC: 08:11 (0:06:06 remaining)
Connect Scan Timing: About 64.52% done; ETC: 08:11 (0:05:21 remaining)
Connect Scan Timing: About 69.92% done; ETC: 08:11 (0:04:31 remaining)
Connect Scan Timing: About 75.30% done; ETC: 08:11 (0:03:43 remaining)
Connect Scan Timing: About 80.47% done; ETC: 08:11 (0:02:56 remaining)
Connect Scan Timing: About 85.60% done; ETC: 08:11 (0:02:10 remaining)
Connect Scan Timing: About 90.83% done; ETC: 08:11 (0:01:23 remaining)
Connect Scan Timing: About 96.08% done; ETC: 08:11 (0:00:36 remaining)
Completed Connect Scan at 08:11, 905.33s elapsed (65536 total ports)
Initiating Service scan at 08:11
Scanning 2 services on react-test-6najyje5cq-uc.a.run.app (216.239.34.53)
Service scan Timing: About 50.00% done; ETC: 08:13 (0:00:58 remaining)
Completed Service scan at 08:12, 67.16s elapsed (2 services on 1 host)
NSE: Script scanning 216.239.34.53.
Initiating NSE at 08:12
Completed NSE at 08:12, 5.46s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 1.44s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Nmap scan report for react-test-6najyje5cq-uc.a.run.app (216.239.34.53)
Host is up (0.0100s latency).
Other addresses for react-test-6najyje5cq-uc.a.run.app (not scanned): 216.239.36.53 216.239.38
.53 216.239.32.53 2001:4860:4802:36::35 2001:4860:4802:38::35 2001:4860:4802:32::35 2001:4860:
4802:34::35
Not shown: 65532 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach), 1 filt
ered tcp ports (net-unreach)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Google Frontend
```

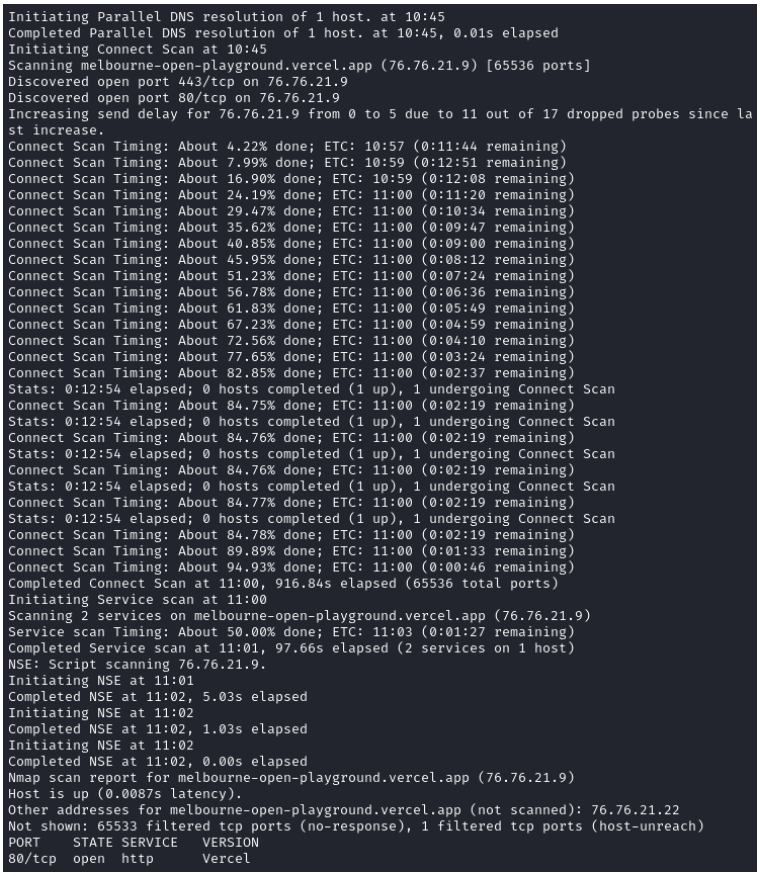
The advanced scan took over 16 minutes and yet unfortunately for us, but fortunately for the MOP site no additional open ports were detected.

This was using the MOP site we were provided: https://react-test-6najyje5cq-uc.a.run.app/

Once again, the advanced test took a little extra, and despite deep dive it attempted, no other ports other then 80 and 443 were identified.

This was using the MOP site identified on the GitHub:

https://melbourne-open-playground.vercel.app/



Recommendations & Conclusions

Using the results of our testing it is clear to see that when it comes to open ports there are no vulnerabilities on either MOP site, with only port 80 and port 443 being open, for standard and encrypted traffic respectively which is the normal for a website, and as such there are no recommendations I can offer regarding this matter.

In conclusion the security of the network might be vulnerable via other methods but an attack using an open port other then 80 or 443 is just not possible as they all seem to be closed, so MOP passes the port vulnerability test.

References:

Chapter 15. nmap reference guide (no date) *Chapter 15. Nmap Reference Guide | Nmap Network Scanning*. Available at: https://nmap.org/book/man.html (Accessed: 1 April 2024).

A quick port scanning tutorial: Nmap network scanning (no date) *A Quick Port Scanning Tutorial | Nmap Network Scanning*. Available at: https://nmap.org/book/port-scanning-tutorial.html (Accessed: 1 April 2024).