

Praktikum 2

Vulnerabilities in FortifyTech Company by Applying Ethical Hacking Principles

Assessment Overview

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka. Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

Assessment Note

Menggunakan wifi/VPN ITS

Scoping

- 10.15.42.36
- 10.15.42.7

Testing Summary

Belum ditemukan celah untuk mencari informasi

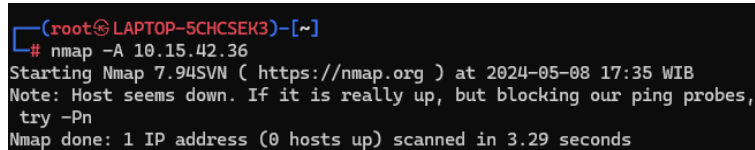
Technical Finding

Nmap

Dalam penggunaan nmap saya masih belum menemukan port yang terbuka

Documentation :

```
`nmap -A 10.15.42.36`
```



```
(root@LAPTOP-5CHCSEK3)~# nmap -A 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:35 WIB
Note: Host seems down. If it is really up, but blocking our ping probes,
try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.29 seconds
```

```
`nmap -T4 -A -v 10.15.42.36`
```

```

(root@LAPTOP-5CHCSEK3)~# nmap -T4 -A -v 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:36 WIB
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating Ping Scan at 17:36
Scanning 10.15.42.36 [4 ports]
Completed Ping Scan at 17:36, 2.06s elapsed (1 total hosts)
Nmap scan report for 10.15.42.36 [host down]
NSE: Script Post-scanning.
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Initiating NSE at 17:36
Completed NSE at 17:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes,
try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.29 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)

```

`nmap -sU -p- 10.15.42.36`

```

(root@LAPTOP-5CHCSEK3)~# nmap -sU -p- 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:38 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds

```

`nmap -p 80,443,8080 10.15.42.36`

```

(root@LAPTOP-5CHCSEK3)~# nmap -p 80,443,8080 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:39 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

```

`nmap -Pn 10.15.42.7`

```

(root@LAPTOP-5CHCSEK3)~# nmap -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:43 WIB
Nmap scan report for 10.15.42.7
Host is up (0.019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds

```

```
`nmap -p 21-1337 -T1 10.15.42.7`
```

```
(root@LAPTOP-5CHCSEK3)~# nmap -p 21-1337 -T1 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:46 WIB
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 1
  undergoing Ping Scan
Ping Scan Timing: About 12.50% done; ETC: 17:50 (0:
03:30 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (0 up), 1
  undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 17:48 (0:
01:16 remaining)
Note: Host seems down. If it is really up, but bloc
king our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 136
.23 seconds
```

```
`nmap -Pn --script vuln 10.15.42.36`
```

```
(root@LAPTOP-5CHCSEK3)~# nmap -Pn --script vuln 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:51 WIB
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1
  undergoing Script Scan
NSE Timing: About 88.35% done; ETC: 17:51 (0:00:01
remaining)
Nmap scan report for 10.15.42.36
Host is up (0.021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 30.0
4 seconds
```

Probs :

Belum memahami sepenuhnya untuk mencari kerentanan