

Executive Summary

Part 1: Reconnaissance

Using the initial starter code to verify socket and docker networking working properly, I was able to discover port 5000 on 172.20.0.10 was open.

```
[mar@archlinux port_scanner] (main)$ python main.py 172.20.0.10
[*] Starting port scan on 172.20.0.10
[*] Scanning 172.20.0.10 from port 1 to 10000
[*] This may take a while...
[+] Scan complete!
[+] Found 1 open ports:
    Port 5000: open
```

Figure 1: Basic socket test to find port 5000

After implementing some input handling with `argparse`, CIDR handling with `ipaddress`, and threading, I ran `python main.py --target 172.10.0.0/24 --ports 1-10000 --threads 10000` and got the results below.

```
[+] Scan complete!
[+] Found 6 open ports:
Target 172.20.0.1
    Port 5001: open
Target 172.20.0.10
    Port 5000: open
Target 172.20.0.11
    Port 3306: open
Target 172.20.0.20
    Port 2222: open
Target 172.20.0.21
    Port 8888: open
Target 172.20.0.22
    Port 6379: open
```

Figure 2: Open ports on the 172.10.0.0/24

Implementing some level of banner grabbing by going through some common probing techniques onto the same subnet and ports on Figure 3.

Part 2: MITM Attack

Part 3: Security Fixes

Port Knocking

Honeypot

Remediation Recommendations

Conclusion

```
[+] Scan complete!
[+] Found 7 open ports:
Target 172.20.0.1
    Port 2222: open
    Port 5001: open
        Banner: HTTP/1.1 200 OK
Server: Werkzeug/3.1.5 Python/3.11.14
Date: Sat, 07 Feb 2026 06:49:52 GMT
Content-Type: text/html; charset=ut
Target 172.20.0.10
    Port 5000: open
        Banner: HTTP/1.1 200 OK
Server: Werkzeug/3.1.5 Python/3.11.14
Date: Sat, 07 Feb 2026 06:50:03 GMT
Content-Type: text/html; charset=ut
Target 172.20.0.11
    Port 3306: open
        Banner: J
8.0.45c
*!H=UXmysql_native_password
Target 172.20.0.20
    Port 2222: open
        Banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13
Target 172.20.0.21
    Port 8888: open
        Banner: HTTP/1.1 200 OK
Server: Werkzeug/3.1.5 Python/3.11.14
Date: Sat, 07 Feb 2026 06:50:17 GMT
Content-Type: application/json
Con
Target 172.20.0.22
    Port 6379: open
        Banner: -ERR wrong number of arguments for 'get' command
```

Figure 3: Banner grabbing on 172.10.0.0/24