

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

Part 2: MITM Attack

Part 3: Security Fixes

Port Knocking

Honeypot

Remediation Recommendations

Conclusion