Port Knocking

Code can be found here: https://github.com/c2003-tamu/413

Environment Setup

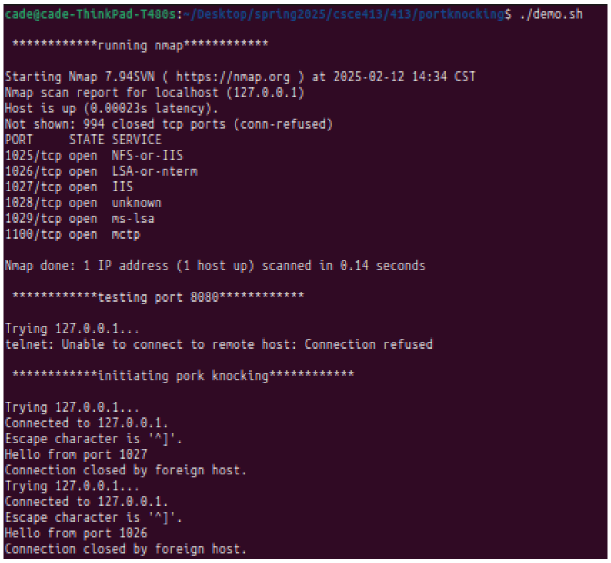
- Ensure python is installed
- Ensure telnet is installed

Running the Project

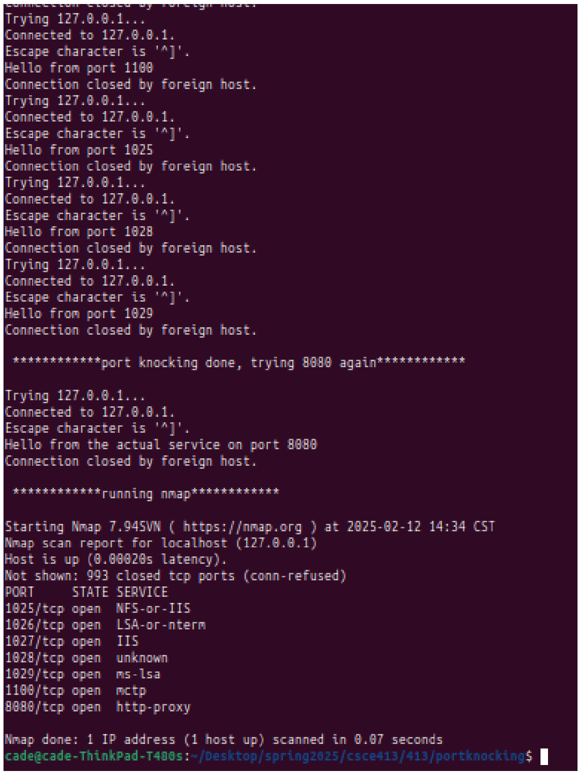
- Clone git repo
- Navigate to 413/portknocking directory
- Open 2 terminal tabs
- In one tab, run command: python3 server.py
- In other tab, run command: ./demo.sh

Explanation

There is a predefined “combination” of ports that need to be connected to in order for the real service to open up on port 8080.
The output from the script ./demo.sh shows the following output:



```
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/portknocking$ ./demo.sh

 ************running nmap************

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-12 14:34 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00023s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1100/tcp open  mctp

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

 ************testing port 8080************

Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

 ************initiating pork knocking************

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1027
Connection closed by foreign host.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1026
Connection closed by foreign host.
```



```
Connection closed by foreign host.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1100
Connection closed by foreign host.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1025
Connection closed by foreign host.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1028
Connection closed by foreign host.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from port 1029
Connection closed by foreign host.

 ************port knocking done, trying 8080 again************

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Hello from the actual service on port 8080
Connection closed by foreign host.

 ************running nmap************

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-12 14:34 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00020s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1100/tcp open  mctp
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
cade@cade-ThinkPad-T480s:~/Desktop/spring2025/csce413/413/portknocking$
```

From this output, we can see that:

- Port 8080 is not initially open
- Ports are knocked in correct order: 1027, 1026, 1100, 1025, 1028, 1029
- Port 8080 is then open and able to be connected to