

CSCE 413: Software Security
PoC 8: Port Knocking

Create a Network Application

For this assignment, I created a simple Python application that accepts UDP requests through several sockets. A demo script presenting all major requirements can be found as `demo.sh`. To run the demo script;

1. Enter the PoC8 directory.
`cd PoC8`
2. Run the script.
`./demo.sh`

Application Behavior

The python server can be ran via `python3 ./knockknock.py`.

This program offers a class called `KnockingServer`. This class accepts a sequence of ports (in the order that they should be knocked) and a timeout for the intervals between knocking. If a knock is received more than that many seconds later, the sequence is reset before evaluating the new knock.

The `run()` function starts running the server after it has been instantiated. The server will first create individual threads hosting sockets that listen for incoming UDP requests for each port in the sequence. More directly, the `start_listeners()` function is called that runs a thread for each port, calling the `listener()` function. Once all threads have been created, they will monitor all ports and call a handler function `handle_knock()` for their respective port if a UDP request is made.

The `handle_knock()` first checks the time of the incoming request compared to the last request, and ensures that the knocks occurred within the timeout range. If the newest knock occurs at a time beyond the timeout period, it will reset the sequence and continue to check the knock. Next, the function then compares the incoming knock with the expected knock, as tracked by an index `expected_knock_index`. If the knocks are the same, it traverses the sequence, otherwise, it resets the sequence. The sequence is complete when the `expected_knock_index` matches the length of the knock sequence array.

Once the sequence is complete, the application will close all ports and open port 8080 for its main service. It should be noted that a real-world application of this will not need to close all other ports, but I am doing this just to demonstrate a change in the available sockets.

Scan with NMAP

Once the program is running a scan can be performed with nmap. Since the program is opening UDP ports, some modifications will be made to the nmap scan,

```
nmap -sU -p- 127.0.0.1
```

Where the `-sU` flag specifies to scan for all UDP ports, `-p-` scans for all ports from range 1-65535, and `127.0.0.1` specifies the localhost. Running this scan reveals,

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo python3 ./knockknock.py
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
.
.

user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo nmap -sU -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:39 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65530 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp    open|filtered ntp
456/udp    open|filtered macon
789/udp    open|filtered unknown
5353/udp   open|filtered zeroconf
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

As seen here, ports 123, 456, and 789 are open. Other dummy ports could also be added to this script for decreasing the change of brute force knocking. Note that port 8080, the main service, has not been opened as the correct sequence of knocks has not been implemented yet.

Implement Port Knocking Logic

The port knocking logic can be found on lines 45-73 of `knockknock.py`. As explained earlier, the service only traverses the sequence of knocks if the received knock matches the expected knock. if a timeout or incorrect knock occurs, the sequence is reset.

What follows is a demonstration of an incorrect order of knocks being performed,

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo python3 ./knockknock.py
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (789) does not match expected knock (456). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
.
.

user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 123
0.1 123
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 789
0.1 789
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 456
0.1 456
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

What follows is a series of correct knocks interrupted by a timeout,

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo python3 ./knockknock.py
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
[Valid Knock] New knock (123) matches expected knock (123).
[Valid Knock] New knock (456) matches expected knock (456).
[Knock Timeout] Previous knock was sent 14.864318370819092 seconds ago!
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
.
.

user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 123
0.1 123
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 456
0.1 456
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sleep 6
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 789
0.1 789
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

As seen in these examples, inputting an incorrect sequence of knocks or waiting too long will result in the sequence being reset.

Before and After Knock Sequence

First we will run the nmap scan as discussed earlier to reveal that port 8080 is not open.

We will then make the series three correct knocks.

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo python3 ./knockknock.py
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.

user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo nmap -sU -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:43 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65530 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp    open|filtered ntp
456/udp    open|filtered macon
789/udp    open|filtered unknown
5353/udp   open|filtered zeroconf
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

We will now run nmap again to view all opened ports.

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo python3 ./knockknock.py
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Knock Timeout] Previous knock was sent 30.6251699924469 seconds ago!
[Valid Knock] New knock (123) matches expected knock (123).
[Valid Knock] New knock (456) matches expected knock (456).
[Valid Knock] New knock (789) matches expected knock (789).
[Knocking Complete] Correct knock sequence detected.
[Main Service] Knocking successful, opening service on port 8080

user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo nmap -sU -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:43 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65530 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp    open|filtered ntp
456/udp    open|filtered macon
789/udp    open|filtered unknown
5353/udp   open|filtered zeroconf
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 123
echo "knock" | nc -u -w1 127.0.0.1 456
echo "knock" | nc -u -w1 127.0.0.1 789
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

It is seen that, after the correct sequence of knocks, the server has opened port 8080 for communication.

```
[Running] Waiting for knocks...
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (123) does not match expected knock (456). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting..
.
[Knock Timeout] Previous knock was sent 30.6251699924469 seconds ago!
[Valid Knock] New knock (123) matches expected knock (123).
[Valid Knock] New knock (456) matches expected knock (456).
[Valid Knock] New knock (789) matches expected knock (789).
[Knocking Complete] Correct knock sequence detected.
[Main Service] Knocking successful, opening service on port 8080
[Main Service] Received message from port 8080.
[Main Service] Received message from port 8080.

PORT      STATE      SERVICE
123/udp    open|filtered ntp
456/udp    open|filtered macon
789/udp    open|filtered unknown
5353/udp   open|filtered zeroconf
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ echo "knock" | nc -u -w1 127.0.0.1 123
echo "knock" | nc -u -w1 127.0.0.1 456
echo "knock" | nc -u -w1 127.0.0.1 789
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo nmap -sU -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:44 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65532 closed udp ports (port-unreach)
PORT      STATE      SERVICE
5353/udp   open|filtered zeroconf
8080/udp   open|filtered http-alt
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
user@user-VirtualBox:~/Documents/csce_413/PoC_8$
```

Demo Script

What follows is screenshots of the demonstration script.

```
user@user-VirtualBox:~/Documents/csce_413/PoC_8$ sudo ./demo.sh
~~~~~ RUNNING SERVER ~~~~~
We will first run the python server. We will then use Nmap to view which ports are exposed.
Press Enter to start the server...
Starting Python server...
~~~~~ server logs ~~~~~
[Startup] Opening ports: 123 456 789
[Running] Waiting for knocks...
~~~~~

We will now run Nmap on all exposed UDP ports with: nmap -sU -p- 127.0.0.1
Press Enter to view the Nmap scan...
~~~~~ nmap scan ~~~~~
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:45 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000000s latency).
Not shown: 65530 closed udp ports (port-unreach)
PORT      STATE      SERVICE
123/udp    open|filtered ntp
456/udp    open|filtered macon
789/udp    open|filtered unknown
5353/udp   open|filtered zeroconf
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
~~~~~
It is seen that the ports 123, 456, and 789 are open for knocking.
~~~~~

~~~~~ ATTEMPTING KNOCKS ~~~~~
We will now attempt knocking on the server. The correct order of knocks is 123, 456, 789.
We will first try to access the server via an incorrect sequence of knocks; 123, 789, 456.
Press Enter for netcat to send the incorrect sequence...
~~~~~ server logs ~~~~~
[Valid Knock] New knock (123) matches expected knock (123).
[Invalid Knock] New knock (789) does not match expected knock (456). Resetting...
[Invalid Knock] New knock (456) does not match expected knock (123). Resetting...
~~~~~
It is seen that entering ports in the incorrect sequence will not reveal the main service.

We will next attempt to access the server with the correct sequence, but exceeding the 5 second timeout buffer.
Press Enter for netcat to send the sequence...
~~~~~ server logs ~~~~~
[Valid Knock] New knock (123) matches expected knock (123).
[Valid Knock] New knock (456) matches expected knock (456).
[Invalid Knock] New knock (789) does not match expected knock (123). Resetting...
~~~~~
It is seen that taking too long to input a knock will result in a timeout and reset the sequence.
~~~~~

~~~~~ FULL KNOCK ~~~~~
We will now attempt a full correct knock to open the main service.
Press Enter to perform a full knock...
~~~~~ server logs ~~~~~
[Valid Knock] New knock (123) matches expected knock (123).
[Valid Knock] New knock (456) matches expected knock (456).
[Valid Knock] New knock (789) matches expected knock (789).
[Knocking Complete] Correct knock sequence detected.
[Main Service] Knocking successful, opening service on port 8080
~~~~~

We can now send requests to the main service hosted at port 8080.
Press Enter to send a request to port 8080...
~~~~~ server logs ~~~~~
[Main Service] Received message from port 8080.
~~~~~

We can also now run Nmap to view that all other ports have been closed, and port 8080 has been exposed.
NOTE: For port knocking, we don't need to close the other ports, but I've done it here just to display that the ports have changed.
Press Enter to view the Nmap scan...
~~~~~ nmap scan ~~~~~
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 12:45 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 65532 closed udp ports (port-unreach)
PORT      STATE      SERVICE
5353/udp   open|filtered zeroconf
8080/udp   open|filtered http-alt
47362/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
~~~~~
It is seen that port 8080 has been opened.
~~~~~
```