

CISC 367 – Spring 2016

Port Scanning

1 Port Scanning with Nmap

Submit the nmap scanning reports (via Unix command `script` – make record of a terminal session) of running the following commands

- `nmap -O <IP address>`
- `nmap -sV <IP address>`
- `nmap -sT <IP address>`

to scan machine `128.4.31.225`

Note: It is the best to scan these machine while your are in the `128.4.0.0` subnet.

2 Port Scanning in Python

- Exame the Python code in **Port Scanner in Python**.
- Execute this Python code to generate scanning report of `128.4.31.225`. Submit the report (via command `script`).
- What do you need to change in this Python code to report status of **the same set of ports** as was reported by the above `nmap` commands? And why? Submit the scanning report from running your revised Python code.