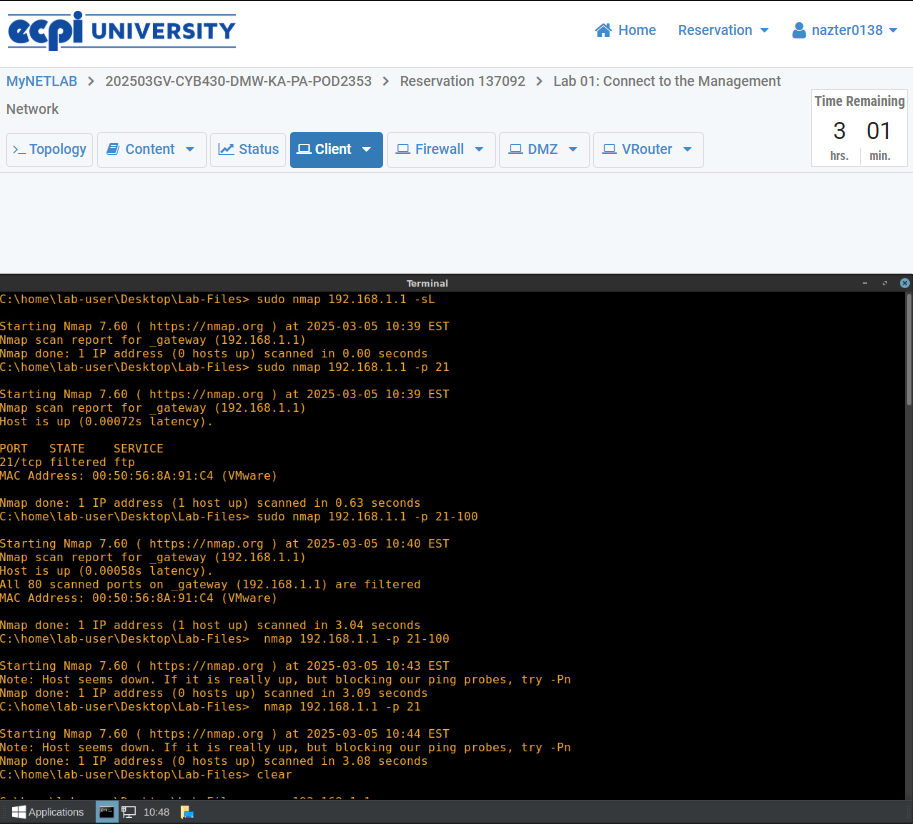
Complete the following Nmap Commands:

|  |  |  |
| --- | --- | --- |
| Switch | Example | Description |
|  | nmap 192.168.1.1 | Scan a single IP |
|  | nmap 192.168.1.1 192.168.1.2 | Scan specific IPs |
|  | nmap 192.168.1.1-254 | Scan a range |
|  | nmap example.org | Scan a domain |
|  | Nmap 192.168.1.0/24 | Scan a network with a CIDR |

Target Specification

**Target Specification Results**: What do you observe about the results?

The single and multi IP scans only scan if the host is up and were completed within the shortest amount of time while the range scan checked all IP’s from 1-254 giving open ports and the services related to the ports. The domain scan gives the host status, other address for the domain and the state and service of the ports captured. The CIDR scan like the range scan captured all IPS on the network in a shorter time with less detail

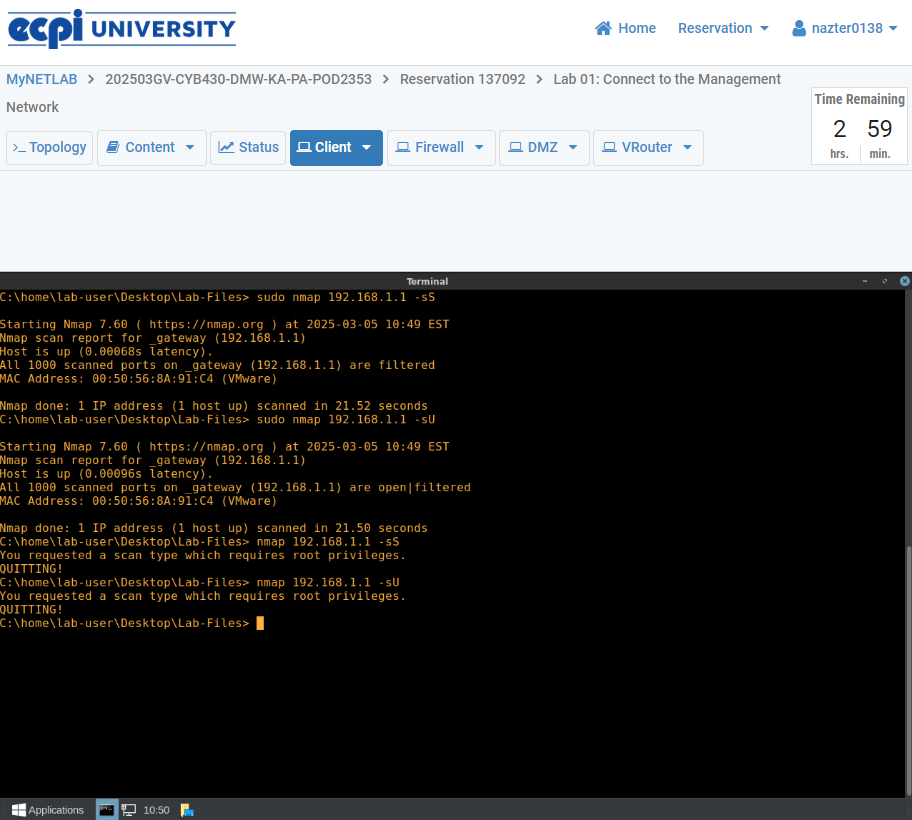


|  |  |  |
| --- | --- | --- |
| Switch | Example | Description |
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
|  |  |  |
|  |  |  |
|  |  |  |

Scan Techniques

**Scan Techniques Results**: What do you observe about the results?

The results from the UDP scan were recieved slightly faster than the TCP scan as expected. The UDP scan also implied that the 1000 scanned ports are open or filtered while the TCP scan only implied filtered



|  |  |  |
| --- | --- | --- |
| Switch | Example | Description |
| -sL | nmap 192.168.1.1 -sL | No Scan. List targets only |
| -p | nmap 192.168.1.1 -p 21 | Port scan for port X |
| -p | nmap 192.168.1.1 -p 21-100 | Port scan range |
|  |  |  |

Host Discovery

**Scan Techniques Results**: What do you observe about the results?

The no scan was easily the fastest scan thus far taking no time and simply checked the state of the host of the given IP address. This would explain why it is said that the scan is performed during reconnaissance since it does not appear to send or receive anything from the scanned target. The port scan simply checked the port protocol, state, and provided service. The port scan range surprisingly did not list out the ports but instead simply stated that all scanned ports on the IP were filtered. Interestingly if the port scans are performed without using escalated privileges then the result instead states that the host appears to be down or possibly blocking the pings being sent

