# 21CY683 - Cybersecurity Lab Experiment– 2

[CYS 2022 - 2024] 16-03-2023

**(Note: Total 20 marks for this lab assignment which includes 15 marks + 5 marks for report) For each of the following steps describe your results, give the syntax of the command you used, and, where appropriate, the output produced. Include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and answer each question in your report.**

Use the tool **NMAP [Command line only]** to perform the below task. Run Wireshark in the background and capture only the necessary packets to showcase for the corresponding question.

a) Explain the subnet and use the NMAP Command to scan the services for the whole subnet.

b) What is a firewall and mention its types. Use the NMAP command to detect that a firewall protects the host.

c) Use the NMAP command to scan a network and determine which devices are up and running.

d) What are vertical and horizontal scanning?

e) Use the NMAP command to scan multiple hosts. [HINT: Add hosts into a file and scan it].

f) Use NMAP commands to export the output in XML format.

g) Use the NMAP command to get OS information about a host.

h) Explain ping sweeping and Perform ping sweeping using Nmap

***Also, learn other scans of NMAP using the man page or –help option.***

**Try these below questions after completing the above commands.**

1. What is a web application firewall? How do you use Nmap to detect a WAF? Perform WAF fingerprint detection using NMAP.
2. What is EXIF data? Try to find EXIF data of images on a website using NMAP NSE.
3. Use NMAP NSE to find all subdomains of the website.
4. Perform a vulnerability scan on the target host using NMAP NSE.

NMAP Download: https://nmap.org/

NMAP Reference: https://nmap.org/book/man.html