

# CS470

## Computer Security

### Laboratory Project Due Date:

## System Reconnaissance

The objective of this project is to understand the methods of invasive probing of system ports on the transport and network protocol layers of a network stack. These methods are used by both legitimate and illegitimate (hackers) users of the system to test for system vulnerability. You are required to enumerate live or accessible Internet services as well as the operating system used by each node in a network segment using **nmap**, which is an open source utility program for port scanning.

You need to accomplish each of the following tasks and to briefly answer the question that is related to the task. You need to document the command(s) you used to accomplish each and a partial snapshot of each of the results.

- 1) Task: Discover all hosts (hostnames and IP addresses) in the 192.168.100.0 network. Why is this useful in vulnerability assessment/analysis?
- 2) Task: Send ICMP echo requests. Use two other options that will expand/verify your scanning capability. Why do some computers prevent/disallow ICMP requests?
- 3) Task: Modify the nmap configuration of its default service enumeration by creating a new service list that is composed only of the following: ftp, telnet, ssh, http, https, tftp, and smtp (all with udp and tcp). Speed-up the scanning process by using the “Insane” mode of scanning. Why do hackers limit the service enumeration list? Why do they mostly choose the “Paranoid” option as the speed of the scanning process?
- 4) Task: Scan a range of IP addresses using at least 5 decoy IP addresses. In a hacker’s point of view, what is the purpose of using decoys?
- 5) Task: Determine the operating system used by each computer in the network segment. Why do hacker’s need to know the target machine’s operating system? How does **nmap** determine the operating system used by a particular machine?
- 6) Task: Scan an IP address using a) TCP SYN, b) TCP FIN, c) TCP Xmas Tree, d) TCP ACK, and e) TCP Null. What is the purpose/goal of each type of scan?