

# MCAST

## Computer Security Laboratory Projects

### Project #1—Network and 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 TCP/IP protocol 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 and **UMIT**, a GUI front-end for nmap.

#### Goal 1 Produce a plan to perform network and system reconnaissance

**Task 1: Read the documentation on nmap and UMIT**

**Task 2: Install nmap and UMIT.**

**Task 3: Implement a reconnaissance procedure to check the hardware and software components using the scanning process capability of nmap.**

#### Assessment and Grading Criteria:

##### Task 1: (20%)

- What is the primary function of nmap?
- What is the primary function of UMIT?
- What is the purpose of the decoy option?
- How do you scan multiple IPs? Multiple ports?
- How do you output the results in XML format?

##### Task 2: (20%)

**Successful installation of nmap and UMIT**

##### Task 3: (60%)

- Completion of the following subtasks:

- 1) Identify all hosts (hostnames and IP addresses) in the 192.168.X.0 network. Why is this useful for a network or system administrator?
- 2) Send ICMP echo requests. Use two other options that will expand/verify your scanning capability. How can you prevent/disallow ICMP requests? Why do you have to do this?

3) Identify all the open ports and services offered by a host (IP 192.168.X.7). Identify the target's operating system. How does **nmap** determine the operating system used by a particular machine?

4) Scan the host (IP 192.168.X.7) 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?

5) Scan the same host using a spoofed IP address. Scan the same host using a spoofed MAC address. What IP and MAC addresses did you use? Are random IP and MAC addresses possible?