Assessment 1 Details and Submission Guidelines	
Trimester	1
Unit Code	ICT306
Unit Title	Advanced Cyber Security
Assessment Type	Individual Assessment
Assessment Title	**Mastering Network Mapping and Enumeration**
Purpose of the assessment(with ULO Mapping)	a. Evaluate the different techniques used by attackers in cyber-attacks, employing both technical knowledge and ethical reasoning b Analyse IT Systems and their weaknesses
Objectives of Assignment	• Gain a solid understanding of Nmap • Learn modern techniques to map and scan the network • Learn how to generate outputs and reports with WebMap
Weight	Assignment 1 30 %
Total Marks	Assignment 1 30
Word limit	1500
Due Dates	Assignment 25/09/2022
Submission Guidelines	• All work must be submitted on Moodle by the due date along with a completed Assignment Cover Page. • The assignment must be in MS Word format, 1.5 spacing, 11-pt Calibri (Body) font and 2 cm margins on all four sides of your page with appropriate section headings. • Reference sources must be cited in the text of the report, and listed appropriately at the end in a reference list using IEEE referencing style.
Extension	• If an extension of time to submit work is required, a Special Consideration Application must be submitted. You must submit this application within four working days of the assessment due date. • Further information is available at: Microsoft Word - QA20 Student Assessment 2.0 (3).doc (filesusr.com)
Academic Misconduct	• Academic Misconduct is a serious offence. Depending on the seriousness of the case, penalties can vary from a written warning or zero marks to exclusion from the course or rescinding the degree. • Students should make themselves familiar with the full policy and procedure available at: Microsoft Word - Student Academic Integrity.docx (filesusr.com).

Assignment 1

Permeable:

Network scanning and enumeration have become an increasingly important aspect of penetration tests over the last couple of years. Organizations now have a complex network of assets storing sensitive and valuable data. To test the security posture of the organization, conducting effective network scanning and enumeration of the organization's network is mandatory. This assignment will help you become an expert in Nmap quickly and easily.

Objectives of the Assignment:

1. The Assignment starts by setting up the working and then highlights the importance of Nmap for network scanning.

2. Next, you will grasp the fundamental concepts of networking, such as port scanning, the Open Systems Interconnection (OSI) model, network layer, and transport layer.

3. Moving along, you will learn how to discover hosts using pings and understand advanced scanning that will help you to set up your own virtual hacking lab.

4. Next, you will learn techniques to detect and evade firewalls and become familiar with the Nmap Scripting Engine (NSE).

5. Finally, you will find out the role of enumeration services, such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Doman Name System (DNS), Hyper Text Transfer Protocol (HTTP), Server Message Block (SMB), and MySQL in network scanning.

6. By the end of this Assignment, you will have all the key skills needed to use Nmap for penetration testing**.**

Questions: (Total marks 40)

1.All questions carry equal marks.
2. Justify the document properly before submission.
3. Use the diagrams, images wherever necessary.
4. Provide the references in the description in the IEEE format
5. Word limit is 1500 words.
6. Upload the screen shots for every question on the Moodle.

Q1. What is NMAP? What is NMAP used for?

Q2. Type the command 'Nmap -A -T4 scanme.nmap.org' in the terminal and check results. Use the search function to answer the following questions.

a. What does the switch -A do?
b. What does the switch -T4 do?

Q3. Open NMAP and type the command *'nmap -A -T4 localhost'*. Depending on your local network and devices, the scan will take anywhere from a few seconds to a few minutes. Review the results and answer the following questions.

a. Which ports and services are opened?
b. For each of the open ports, record the software that is providing the services.

Q4. At the terminal command prompt, enter *'ip address'* to determine the IP address and subnet mask for your host.

a. Record the IP address and subnet mask of your machine.
b. Which networks your machine belongs to?

Q5. Locate other hosts on your LAN with command *'nmap -A -T4 network address/prefix'*. For example *'nmap -A -T4 10.0.0.0/24'* .The last octet of the your IP address should be replaced with a zero. For example, in the IP address 10.0.2.15, the .15 is the last octet. Therefore, the network address is 10.0.2.0. The /24 is called the prefix and is a shorthand for the netmask 255.255.255.0. If your network has a different netmask, search the internet for a "CIDR conversion table" to find your prefix. For example, 255.255.0.0 would be /16.

Note: This operation can take some time, especially if you have many devices attached to the network. In one test environment, the scan took about 4 minutes.

a. How many hosts are up?
b. From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your machine. List some of the services that are available on the detected hosts.

Q6. Open a web browser and navigate to 'scanme.nmap.org'. Please read the message posted. What is the purpose of this site?

Q7.

a. At the terminal prompt, enter *'nmap -A -T4 scanme.nmap.org'*
Review the results and answer the following questions.
b. Which ports and services are opened?
c. Which ports and services are filtered?
d. What is the IP address of the server?
e. What is the operating system?

Q8. Reflection Question.

Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can NMAP be used by a threat actor as a nefarious tool?

Marking Guide:

Criteria	Description	Marks
Q1	2 marks for description and 3 marks for screen shot	5
Q2	2 marks for description and 3 marks for screen shot	5
Q3	2 marks for description and 3 marks for screen shot	5
Q4	2 marks for description and 3 marks for screen shot	5
Q5	2 marks for description and 3 marks for screen shot	5
Q6	5 marks for description	5
Q7	2 marks for description and 3 marks for screen shot	5
Q8	5 marks for description	5

Marking Rubric for Exercise Answers:

Grade **Mark**	**HD** **80%+**	**D** **70%-79%**	**CR** **60%-69%**	**P** **50%-59%**	**Fail** **< 50%**
	Excellent	**Very Good**	**Good**	**Satisfactory**	**Unsatisfactory**
Q1	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q2	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q3	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q4	Explanation is clear and easy to follow with strong	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed

	arguments				
Q5	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q6	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q7	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed
Q8	Explanation is clear and easy to follow with strong arguments	Consistency logical and convincing	Mostly consistent and convincing	Adequate cohesion and conviction	Argument is confused and disjointed