Skill Area	Cyber Security
Title	Conduct basic cybersecurity tasks such as network scanning and vulnerability identification
Aim	To evaluate students' ability to perform essential cybersecurity tasks, including network scanning, vulnerability identification, and incident analysis.
Competencies Tested	• Network scanning • Vulnerability identification • Incident identification and analysis • Time management
Duration	30 - 45 mins
Task	**Section 1: Network Scanning (12 minutes)** Use a network scanning tool to perform a scan on the IP range 192.168.1.0/24. Identify and list all active devices. Note any open ports for the first two discovered devices. **Deliverable:** List of active devices with IP addresses. Open ports for the first two devices. **Section 2: Vulnerability Identification (10 minutes)** You are provided with scan results for one device (IP: 192.168.1.5). Review the scan results and identify one potential vulnerability. Provide a brief description of the identified vulnerability. **Deliverable:** Identified vulnerability. Description of the vulnerability. **Section 3: Basic Incident Identification (8 minutes)** Analyse the provided sample network traffic snapshot. Identify one unusual activity or potential security incident. Write a brief note describing the unusual activity. **Deliverable:** Description of the unusual activity
Resources	• Network scanning tool • Vulnerability assessment tool

	• Sample network traffic snapshot • Access to a computer or virtual machine with necessary software installed

Marking

Competency	M/J	3 Marks	2 Marks	1 Mark	0 Marks
Network scanning	M	Accurately identifies all active devices and lists correct open ports for the first two devices.	Identifies most active devices and lists correct open ports for at least one device.	Identifies some active devices but lists incorrect or partial open ports.	Fails to identify active devices or list any open ports.
Vulnerability identification	J	Correctly identifies a potential vulnerability and provides a clear, accurate description.	Identifies a potential vulnerability with a mostly accurate description.	Identifies a vulnerability but provides an unclear or inaccurate description.	Fails to identify a vulnerability or provide any description.
Incident identification	J	Clearly identifies unusual activity, providing a well-explained and accurate description.	Identifies unusual activity with a mostly accurate description.	Identifies unusual activity but provides an unclear or partially inaccurate description.	Fails to identify any unusual activity or provide any description.
Time management	M	Completes all tasks within the allocated time efficiently.	Completes most tasks within the allocated time.	Completes some tasks but exceeds the allocated time.	Fails to complete tasks within the allocated time.