National Forensic Sciences University
School of Cyber Security and Digital Forensics

M.Sc. Cyber Security, Semester - 1, Dec – 2025
Semester End Examination (LPW)

Subject: Essentials of Cyber Security and Cyber Warfare

Subject Code: CTMSCS SI L1 Date: 26/12/25

Time: 11:30 AM to 01:30 PM | Marks: 100

Instructions:

1. Attempt any ten (10) questions from the given set.
2. Each question must be properly documented.
    - Capture and attach a clear screenshot for every question attempted.
3. For theory and logical explanations, students must use a document editing tool such as Microsoft Word, WPS Office, or any equivalent software.
    - *Use of Microsoft Word is recommended for uniform formatting.*
4. After completing all answers, compile a single combined file that includes:
    - All attempted questions
    - Detailed explanations
    - Proof of Concept (PoC) wherever applicable
5. The first page of the document must clearly mention the following details:
    - Student Name
    - Enrolment Number
    - Course Name
    - Semester
    - Title of the Examination
    - Date of the Examination
6. Ensure that the document is well-formatted, properly aligned, and clearly readable before final submission.

National Forensic Sciences University
School of Cyber Security and Digital Forensics

Scenario 1: You are appointed as a **Security Analyst** in a government office. A Windows 10 workstation shows unusual behaviour:

- System slowdown
- Unknown services running
- Automatic updates are disabled
- Sensitive files are accessible by non-admin users

You are asked to **investigate, secure, and harden the system** without reinstalling the OS.

Questions

Q1. Identify **two suspicious processes or services** using any tools. Explain how you decide they are suspicious.

Q2. Check whether the system is **fully patched**.

- Identify missing updates
- Explain the security risk of not applying them

Q3. Examine **NTFS permissions** on a sensitive folder (e.g., C:\anyfolder which is available in drive).

- Identify misconfigurations
- Propose corrected permissions

Q4. Verify whether **BitLocker Drive Encryption** is enabled.

- If disabled, explain the steps of enabling and **why enabling BitLocker is important** in this scenario

Q5. Apply **one Local Group Policy** that improves system security and justify your choice.

Scenario:2 A Linux server hosting internal applications has shown **unauthorized login attempts**.
You are tasked to **secure and identify attack traces**.

Questions

Q1. Identify **which services start automatically at boot** and justify whether all are required.

Q2. Analyse authentication logs to detect **failed login attempts**.

Q3. Restrict **unused ports** on the system and explain the security impact.

Q4. Demonstrate how **log monitoring helps in attack detection** using any one command.

Q5. Propose **two hardening measures** to prevent future attacks.

Scenario: 3 During a geopolitical conflict, a country experiences:

- Website defacement
- Social media panic campaigns
- Network outages in public services

You are part of a **Cyber Defence Think-Tank** analysing the situation.

Questions

Q1. Identify whether the situation qualifies as **Cyber Warfare or Information Warfare**. Justify your answer.

Q2. Classify the attacks into **tactical or operational cyber actions**.

Q3. Explain how **psychological operations (PSYOPS)** are being conducted digitally.

Q4. Propose **two defensive cyber strategies** to counter such attacks.

Q5. Explain the role of **Information Assurance** in restoring public trust.

Scenario: 4 Users complain of **slow internet and intermittent connectivity**.
You suspect internal misuse or reconnaissance activity.

Questions

Q1. Capture live network traffic and identify if any **abnormal traffic pattern is there.**

Q2. Determine whether the traffic indicates **scanning, flooding, or normal communication**.

Q3. Identify the **source and destination** of suspicious packets.

Q4. Explain how this activity could impact system availability.

Q5. Propose two **preventive controls** to stop such activity.

Scenario 5 During elections, a country faces:

- Fake government advisories
- Website defacement
- Coordinated social media narratives

Questions

Q1. Distinguish between **Cyber Warfare and Information Operations** in this case.

Q2. Identify the **primary objective** of the attacker.

Q3. Classify actions into **psychological warfare or technical warfare**.

Q4. Propose two **non-technical countermeasures**.

Q5. Explain how **Information Superiority** helps mitigate damage.

Scenario 6 An organization operates a **Windows client system**, a **Linux application server**, and a **shared internal network**. During routine monitoring, the SOC observes the following:

- Multiple **authentication failures** from one internal IP
- Temporary **network congestion** without service outage
- A **Windows system** where security updates are delayed
- A **Linux server** where logs are growing unusually fast

No malware has been detected, and systems remain operational.

You are assigned to **analyse, correlate, and recommend corrective controls** without assuming a breach.

Questions

Q1. Identify whether the observed behaviour represents a **security incident, security weakness, or normal operational anomaly**.
Justify your classification using reasoning.

Q2. On the **Windows system**, How to identify **security misconfigurations** that could indirectly contribute to this situation.

Q3. On the **Linux server**, explain how log growth itself can become a **security risk**, even if no attack is confirmed.

Q4. Using a **network-level perspective**, explain what type of activity could cause authentication failures and congestion *without being a full attack*.

Q5. Propose **three corrective actions** (one each for Windows, Linux, and Network) that improve security **without disrupting services**.

Scenario:7 An academic institution operates a mixed environment consisting of **Windows-based user endpoints** and **Linux-based backend servers**.

A recent internal compliance review reports **no recorded security incidents**, no malware alerts, and no service downtime. However, the following operational characteristics are observed:

- Multiple users routinely access systems through **shared credentials**
- Authentication secrets are **static and infrequently rotated**
- Linux servers follow an **ad-hoc patching cycle** rather than a structured update policy
- System and authentication logs are generated but **remain unanalyzed**
- Several network services are accessible beyond their functional necessity

Senior management concludes that the absence of incidents indicates an *adequate security posture*.

You are asked to **critically evaluate this conclusion** using security principles, not attack signatures.

Questions

Q1. Assess the managerial conclusion that *"absence of incidents implies security sufficiency."*
Determine whether this represents **sound security reasoning or a conceptual fallacy**, and justify your assessment.

Q2. How to Identify **Windows security-policy deficiencies** that, while not immediately exploitable, substantially **increase the probability of future compromise**.
Explain the risk propagation mechanism for each.

Q3. Explain how **irregular and unscheduled patch management** on Linux systems constitutes a **latent security liability**, even in the absence of an active adversary.

Q4. From a network security design perspective, analyse why **excessive service reachability** should be treated as a **risk amplifier rather than a mere configuration choice**.

Scenario: 8 An organization reports zero cyber incidents over three years. As a result, senior leadership has **deferred security policy reviews**, reduced training budgets, and relaxed enforcement of controls.

Questions

1. Analyse whether **historical stability** is a valid indicator of **future security**.
2. Identify two **policy blind spots** created by deferring reviews.
3. Explain how **human behaviour** can undermine technical controls in this scenario.
4. Distinguish between **compliance** and **actual security effectiveness**.
5. Propose one **non-technical policy change** with high security impact.

Scenario: 9 Management decides not to implement certain security controls due to cost constraints but documents no formal risk acceptance.

Questions

1. Differentiate **risk acceptance** from **risk negligence**.
2. Explain why undocumented risk decisions are dangerous.
3. Identify one **long-term governance risk** in this approach.
4. Propose a **simple risk acceptance framework**.
5. Explain how transparency improves organizational security.

National Forensic Sciences University
School of Cyber Security and Digital Forensics

Scenario: 10 You are assigned as a **network security assessor** for an organization that suspects **unnecessary exposure of internal services**, but no breach or malware activity has been reported.

Management authorizes **only reconnaissance-level assessment**, explicitly prohibiting exploitation or disruption.

You are provided **temporary access to an internal network segment** and are asked to use **Nmap strictly as an observational tool** to support **security policy decisions**, not penetration testing.

Questions

Q1. Explain why **Nmap-based scanning**, even without exploitation, is considered a **powerful security decision-support activity** rather than an attack.

Q2. Using Nmap results, how would you **logically differentiate between essential services and policy violations**, without knowing the business context of each system?

Q3. If Nmap reveals multiple open ports across several hosts, explain why this finding represents a **risk condition**.

Q4. Describe how **service version detection** from Nmap output can influence **patch management and risk prioritization**, without confirming any vulnerability.

Scenario: 11 A Linux server hosts an internal web application and provides remote administrative access. There is no evidence of intrusion, but a recent audit highlights that the server is overexposed at the network layer.

Questions

Q.1 Design iptables rules that:

- Allow SSH access **only from a specific trusted network**
- Allow HTTP/HTTPS access to all users
- Block all other unsolicited inbound traffic

Scenario: 12 In a controlled laboratory network consisting of multiple client machines and a gateway, users report that:

- Network connectivity remains active
- Websites load normally, but login sessions intermittently fail
- No alerts are triggered by the firewall or antivirus

You are informed that one internal system may be manipulating network trust relationships rather than exploiting software vulnerabilities.

You are authorized to perform a **demonstrative ARP poisoning attack** in a lab environment using standard tools, strictly for educational analysis and defensive understanding.

Questions

Q1. Using a practical ARP poisoning setup, describe how an attacker can position themselves as a **Man-in-the-Middle** *without disrupting network connectivity*.

Q2. Explain why **encrypted protocols (HTTPS)** do not prevent ARP poisoning, yet still limit the attacker's capability.

Scenario: 13 A Linux computer is connected to a network.
The administrator wants to:

- Allow only **SSH access** to the system
- Block **all other incoming connections**
- Ensure the system works normally for outgoing connections

You are asked to **configure and explain a simple firewall rule set** using iptables.

Questions

Q1. Why is a firewall needed on a Linux system?

Q2. What should be the **default policy** for incoming traffic to make the system secure?

Q3. Write or explain a rule that allows **SSH (port 22)** access to the system.

Q4. Why should **established connections** be allowed?

Q5. What happens if all incoming traffic is allowed?
