
**LAB 2**
BIS20303: WEB SECURITY
SEMESTER II 2024/2025
SECTION 1

# GROUP 1

| NAME | MATRIC NUMBER |
|---|---|
| KHALIEF HAZIEQ BIN RUHISYAM | DI220147 |
| MUHAMMAD ARIF AIMAN BIN MAZLAN | DI220103 |
| WAN AMIRUL HAKIM BIN WAN KAMARULFARID | DI220123 |
| MANOJJ KUMARR NAIDU A/L GANESAN | DI220043 |
| ARULVADIVELAN A/L SUBRAMANIAM | DI220087 |

**Lab 2: Understanding Hacker Mindset and the Cyber Kill Chain**

**Lab Objective**

- To expose students to real-world hacker strategies.
- To understand the **Cyber Kill Chain** model.
- To analyze and discuss how attacks are structured and mitigated in **web security**.

**Instructions**

1. **Form a group of five students.**
2. **Attend the following talk live** or **listen to the full recording** (link will be provided after the session).

   **Course:** Web Security
   **Date:** Tuesday, 25 March 2025
   **Duration:** 9.00 AM – 11.00 AM (During Industrial Talk)
   **Mode:** Online (Microsoft Teams)
   **Speaker:** Mr. Mohamed Iqbal Bin Tajol Azmi, CyberSecurity Malaysia
   **Talk Title:** *"How Hackers Think – The Cyber Kill Chains and Application"*

3. **Discuss as a group** to analyze key takeaways from the talk and complete the lab questions below.
4. **One group member** should compile the group's answers into a single document.
5. Submit your group's answers via the **e-learning platform** by **28 March 2025, 11:59 PM**.

**Lab Questions**

**Part A: Reflection and Conceptual Understanding**

1. As a group, summarize what the speaker means by *"How Hackers Think."*
   - What were the key takeaways?
     - Hackers have a method: they plan their attacks, do their research, and carry them out precisely rather than attacking at random.
     - One popular strategy is social engineering, in which hackers use human behavior manipulation to obtain access rather than simply depending on technological flaws.
     - Unpatched software is a major weakness: Many attacks exploit known vulnerabilities in outdated applications and systems.
     - Defensive strategies must be proactive: Security teams must anticipate hacker methods and take preventive measures early.
     - Attackers evolve constantly: As security measures improve, hackers adapt by finding new weaknesses or refining their techniques.

   - What stood out to your group the most?

     The way hackers plan and carry out assaults using the Cyber Kill Chain was one of the talk's most remarkable features. Cybersecurity experts can stop attacks

before they start by mastering this concept. Many attacks rely on deceiving users rather than only taking advantage of technical vulnerabilities, underscoring the significance of human factors in security.

2. Explain the **Cyber Kill Chain** model in your own words.
    - Briefly describe each of the seven phases.
        - **Reconnaissance**: The hacker checks out the target, looking for weaknesses or valuable information they can use.
        - **Weaponization**: The hacker creates a malicious tool (like a virus or malware) to attack the target.
        - **Delivery**: The hacker sends the harmful tool to the target, usually through email or a website.
        - **Exploitation**: Once the hacker's tool reaches the target, it uses a weakness in the system to break in.
        - **Installation**: The hacker sets up a way to stay in the system, even if the initial attack is discovered.
        - **Command and Control (C2)**: The hacker connects to the infected system and can now control it remotely.
        - **Actions on Objectives**: Finally, the hacker does what they wanted, like stealing data, causing damage, or disrupting the system.

**Part B: Application and Analysis**

3. Identify **one real-world example or case study** shared by the speaker.
    - Map it to the **Cyber Kill Chain stages**:

1. **Reconnaissance:**

- Hackers identified a vulnerability in Microsoft Windows called Eternal Blue, which was leaked from the NSA.
- They scanned networks worldwide to find computers that had not been patched with Microsoft's security update.

2. **Weaponization:**

- Attackers developed a wormable ransomware that exploited the EternalBlue vulnerability.
- The ransomware was designed to encrypt files and demand payment in Bitcoin.

3. **Delivery:**

- WannaCry spread automatically through networks, without requiring user interaction.
- It exploited open SMB (Server Message Block) ports to spread to connected computers.

4. **Exploitation:**

- Once on a system, WannaCry executed malicious code using the EternalBlue exploit.
- It bypassed security defenses in outdated Windows versions.

5. **Installation:**

- The ransomware installed itself on the infected system and encrypted critical files.
- It modified system settings to prevent easy removal.

6. **Command & Control (C2):**

- The malware connected to hardcoded domains, but a researcher accidentally stopped it by registering a "kill switch" domain.
- Hackers attempted to regain control by modifying the malware to remove the kill switch.

7. **Actions on Objectives:**

- The final goal was to extort money by locking users out of their files and demanding Bitcoin payments for decryption.
- Many victims, including hospitals and businesses, paid the ransom, but there was no guarantee of data recovery.

4. In the context of **web security**, choose **one stage** of the Cyber Kill Chain (e.g., *Exploitation* or *Delivery*) and discuss:
    - How it applies to a **web application attack**.
    - One hacking technique that might be used at this stage.
    - One defense mechanism to counter it.

    At the Exploitation stage of the Cyber Kill Chain is a critical phase, as many web applications utilize frameworks, libraries, and third-party software. If these components have known vulnerabilities and are not updated and not patch, attackers can exploit them to gain unauthorized access.

    One exploitation method is Remote Code Execution (RCE), where an attacker leverages vulnerabilities in unpatched software to execute arbitrary commands on the web server. One defense mechanism to counter this is to make sure do regularly patched and update to fix any vulnerable.

**Part C: Critical Thinking and Discussion**

5. If your team was responsible for securing a web application, at **which stage of the Cyber Kill Chain** would you focus most of your efforts to stop an attack?
    - Justify your answer with reasoning and examples.

    - If my team were to be responsible for securing a web application, we would concentrate most of our efforts on the reconnaissance and weaponization stages of the Cyber Kill Chain to intercept an attack before it goes too far. The reconnaissance stage is when attackers are gathering information about the web application, such as exposed services, API endpoints, and vulnerabilities. We can help limit the amount of

information an attacker can gather by implementing security best practices; this includes implementation of WAFs, rate limiting, and bot detection mechanisms. For example, we can limit the ability to search file indexing through proper configuration of robots.txt can prevent attackers from using Google Dorking to find sensitive files. In the weaponization stage, attackers create exploits based on vulnerabilities discovered during reconnaissance. To avoid this, we recommend secure coding techniques, regular security patching, and checking vulnerabilities with tools such as Burp Suite, OWASP ZAP, or Nessus. For example, using prepared statements and input validation can help prevent SQL injection attacks.

**Submission Format**

- One group member should submit a single **PDF or DOCX** file.
- File name: `Lab2_SessionX_GroupX_WebSecurity` (Replace **X** with your session and group number).
- List all **group members' names and student IDs** on the cover page.