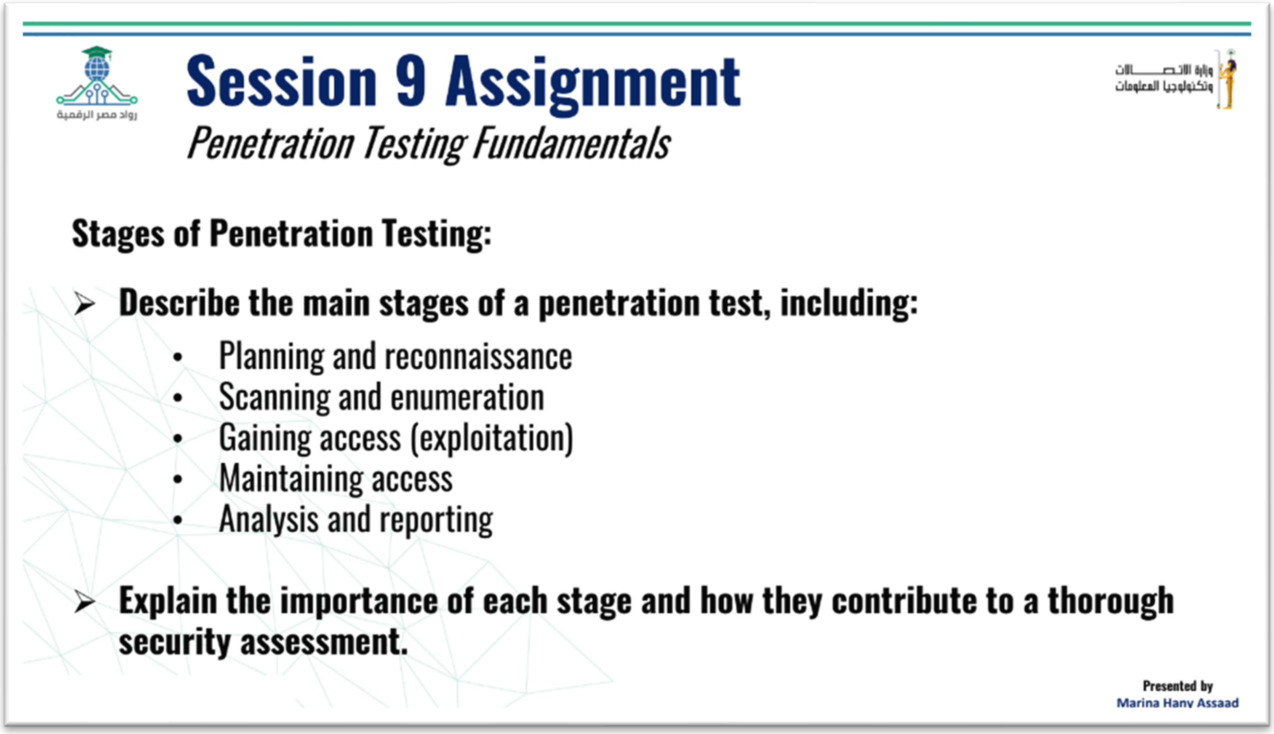
Suhaila Adel Ali

21063119



Session 9 Assignment

Penetration Testing Fundamentals

Stages of Penetration Testing:

- **Describe the main stages of a penetration test, including:**
  - Planning and reconnaissance
  - Scanning and enumeration
  - Gaining access (exploitation)
  - Maintaining access
  - Analysis and reporting
- **Explain the importance of each stage and how they contribute to a thorough security assessment.**

Presented by
Marina Hany Assaad

Understanding the Main Stages of Penetration Testing and its importance:

1. Planning and Reconnaissance

This is where everything begins. In this stage, we define the scope and goals of the test. We also gather as much information as possible about the target—things like network details, domain names, and possible entry points. This can be done actively (interacting with the target) or passively (observing without interaction).

Importance:
Good planning ensures the test stays on track and focuses on the right areas. Reconnaissance is like doing your homework before a big exam—it gives you valuable insights that will guide the next steps. Without this stage, the test could miss important details or even cross legal boundaries.

2. Scanning and Enumeration

Here, we identify live systems, open ports, and services running on the target network. We use tools like Nmap to map out the network and detect vulnerabilities. Enumeration goes a step further, gathering details about user accounts, shared resources, and more.

Importance:
This phase helps us pinpoint potential weaknesses. By understanding the network layout and the services in use, we can identify the best ways to approach an attack. It's like mapping out a building before trying to break in—you need to know where the doors and windows are.

3. Gaining Access (Exploitation)
This is the "action" phase. We try to exploit the vulnerabilities found in the previous step to gain access to systems or data. This could involve cracking passwords, exploiting software bugs, or even using social engineering.

Importance:
Gaining access shows how real-world attackers could breach the system. This phase reveals the potential impact of vulnerabilities and helps organizations understand how much damage could be done. It's like a dress rehearsal for a real attack.

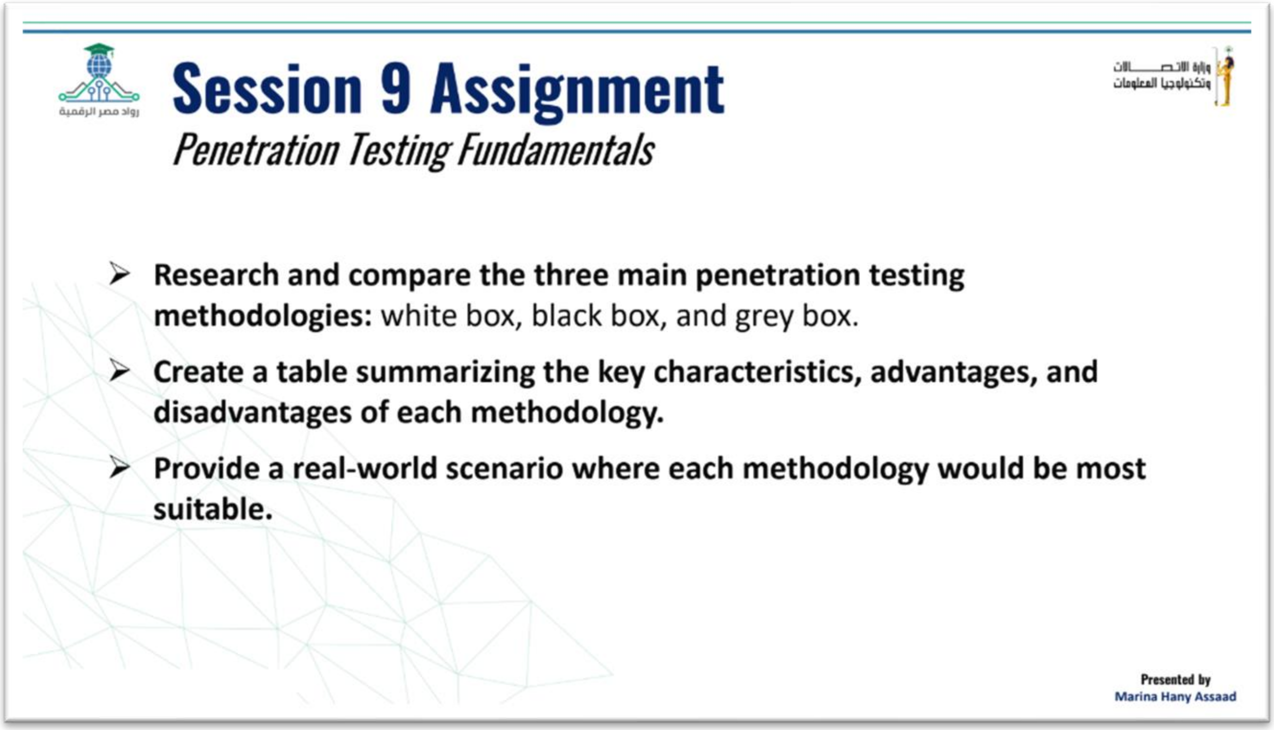
4. Maintaining Access

Once we've gained access, we try to maintain our foothold—just like a real attacker would. This might involve installing backdoors or creating hidden accounts to ensure continued access to the system.

Importance:
This phase demonstrates how long an attacker could stay hidden inside the system. It helps organizations understand if their monitoring tools would detect a persistent threat and how much damage could be done over time. Think of it as testing how well the security guards notice an intruder who doesn't leave.

5. Analysis and Reporting
This is where we put everything together. We document what we found, how we exploited the system, and what data we accessed. The final report includes risks, impacts, and, most importantly, recommendations for fixing the vulnerabilities.

Importance:
The report is the most valuable part of the process. It gives the organization a clear picture of its security strengths and weaknesses. It also provides actionable steps to improve security. Without this stage, the whole test would be pointless—like solving a mystery but never sharing the solution.



Session 9 Assignment

Penetration Testing Fundamentals

- **Research and compare the three main penetration testing methodologies:** white box, black box, and grey box.
- **Create a table summarizing the key characteristics, advantages, and disadvantages of each methodology.**
- **Provide a real-world scenario where each methodology would be most suitable.**

Presented by
Marina Hany Assaad

1. Overview of Penetration Testing Methodologies

White Box Testing

Description:
In white box testing, the tester has full knowledge of the system's internal architecture, source code, and network details. This method is also known as transparent or clear-box testing.

Advantages:

- Comprehensive assessment due to full access.
- Efficient identification of internal vulnerabilities.
- Ideal for testing complex systems and code.

Disadvantages:

- Time-consuming and resource intensive.
- Requires significant collaboration with the organization.
- May miss external attack vectors due to internal focus.

Black Box Testing

Description:
In black box testing, the tester has no prior knowledge of the system's internal workings. The test simulates an external hacker attempting to breach the system.

Advantages:

- Realistic simulation of an external attack.
- Provides an unbiased assessment of the system's perimeter security.
- Requires minimal information from the organization.

Disadvantages:

- May miss internal vulnerabilities.
- Time-consuming due to the need to discover system architecture.
- Limited by the tester's lack of internal knowledge.

Grey Box Testing

Description:
In grey box testing, the tester has partial knowledge of the system, such as network diagrams or user credentials. This method strikes a balance between white and black box testing.

Advantages:

- More focused testing compared to black box.
- Simulates an insider threat or an attacker with limited knowledge.
- Balances efficiency and realism.

Disadvantages:

- Might miss some vulnerabilities due to partial information.
- Requires accurate and up-to-date documentation.
- Can be less thorough than white box testing.

Real-World Scenarios

- **White Box:**
  An organization developing a new web application needs a thorough code review to ensure no vulnerabilities exist before launching. White box testing allows testers to dive deep into the code and identify any hidden issues.
- **Black Box:**
  A company wants to evaluate the security of its public-facing website from the perspective of an external attacker. Black box testing simulates a real-world hack attempt to assess perimeter security.
- **Grey Box:**
  A company suspects an insider threat and wants to simulate what a rogue employee with some access could achieve. Grey box testing provides insights into potential internal risks with limited insider information.