Diploma Programme
Programme du diplôme
Programa del Diploma

Computer science
Case study: An ethical approach to hacking

For use in May and November 2026

Instructions to students

- Case study booklet required for higher level paper 3.

5526 – 4410

7 pages

Scenario

CyberHealth Security is a company that specializes in cybersecurity analysis. A team from this company has recently been hired to review the cybersecurity systems at *MedTechPro Hospital* (*MTPH*). The hospital is heavily reliant on technology, specifically electronic health records (EHRs), internal communications, and medical devices that utilize the Internet of Things (IoT).

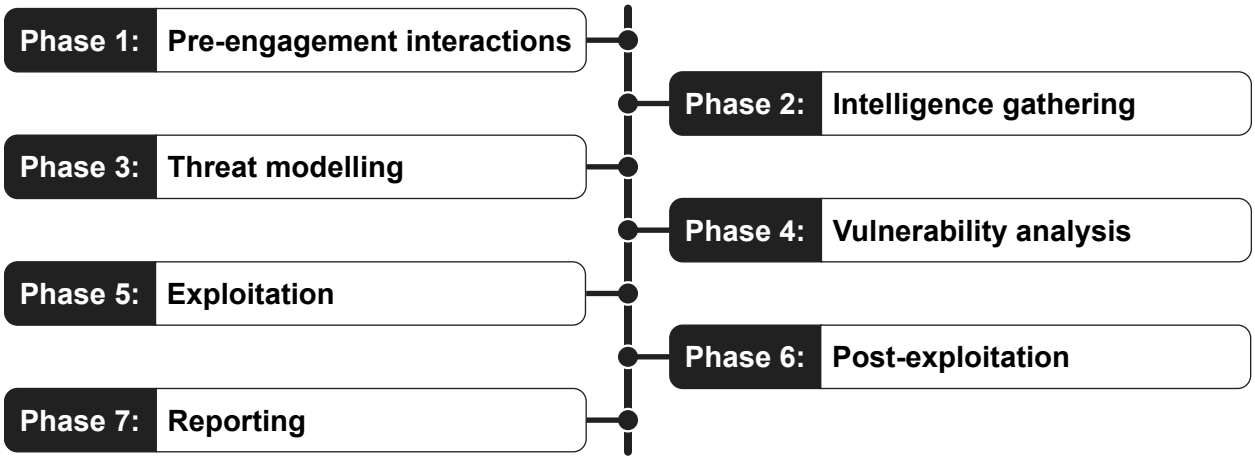
Problems to be addressed

The *CyberHealth Security* team's task is to conduct in-depth *penetration testing* to uncover any vulnerabilities within the hospital's network. They will need to navigate *MTPH*'s network, assessing system security and the privacy of patient data across all departments. To do this, they will use the penetration testing execution standard (PTES).

The penetration testing execution standard

The PTES is a comprehensive framework for conducting penetration testing. It is designed to provide a structured approach to performing tests and reporting results. The PTES process consists of seven phases (see **Figure 1**).

Figure 1: The seven phases of the PTES process



1. **Pre-engagement interactions.** The process begins with preparation, securing document approvals, and assembling the necessary tools.
2. **Intelligence gathering.** Data is collected from external sources, such as social media and official records, and then analysed, which is categorized as *open-source intelligence (OSINT)*.
3. **Threat modelling.** Potential threats and vulnerabilities are identified, and strategies to mitigate them are developed.
4. **Vulnerability analysis.** Vulnerabilities that could be exploited by a *hacker* are identified and confirmed.
5. **Exploitation.** An attempt is made to breach the system using the previously identified and confirmed vulnerabilities.
6. **Post-exploitation.** If access is gained, the focus shifts to maintaining control of the system and extracting data from it.
7. **Reporting.** The entire testing process is documented, and the findings are presented in a report to the client.

Phase 1: Pre-engagement interactions

In this phase, the *CyberHealth Security* team will collaborate with *MTPH* to define the penetration test's goals, scope, rules of engagement, logistics and *testing* approaches, and overall timeline. This collaborative process is crucial in ensuring that the testing aligns with the hospital's operational requirements and security concerns while adhering to professional ethical standards, particularly given the sensitive nature of healthcare data.

Goal setting and target identification

- Clear objectives for the test will be established after identifying *MTPH*'s key concerns. These key concerns may include patient data integrity, uninterrupted service delivery, and compliance with health sector regulations.
- Specific targets within the hospital's network will be identified. Any high-risk areas requiring special attention, such as patient record databases or IoT-enabled medical devices, will be determined.

Defining the scope and rules of engagement

- The test's boundaries will be confirmed to avoid any unintended disruption to critical hospital operations. This includes the systems to be tested and the limits of the testing.
- The rules of engagement will be agreed upon to ensure that both the *CyberHealth Security* team and *MTPH* administrators understand the methods and extent of the penetration testing activities.

Testing approaches

The *CyberHealth Security* team will need to consider the implications of three different approaches to testing—*black box* testing, *white box* testing, and *grey box* testing—and evaluate the potential risks and benefits of each in a healthcare environment.

- **Black box testing**. In this approach, the team would simulate an attack from the perspective of an uninformed external hacker and consider the immediately apparent vulnerabilities.
- **White box testing**. In this approach, the team would perform an in-depth analysis with full knowledge of the hospital's IT infrastructure. This approach would require access to network diagrams, system configurations, and known vulnerabilities.
- **Grey box testing**. A mixture of black box testing and white box testing, this approach would use partial knowledge of the hospital's systems, simulating an insider threat or an external hacker with partial inside information.

Phase 2: Intelligence gathering

This phase involves collecting all publicly available information on *MTPH* to identify potential vulnerabilities. The *CyberHealth Security* team will employ various open-source intelligence (OSINT) techniques, utilizing tools and sources such as search engines, social media, forums, and other internet-facing resources to gather actionable data about the hospital's digital footprint. This information will help the team create a map of the hospital's external presence and will be used to find weaknesses that could be exploited.

Examples of information that the team could gather using OSINT techniques include:

- **Employee details**. Gained through analysis of the social media presence of staff, particularly those in IT and administrative roles.
- **Technology usage**. Insights into the hospital's software and hardware solutions derived from public sources.
- **Security policies**. Examination of the hospital's publicly available security policies and procedures.

The *CyberHealth Security* team also intend to employ other reconnaissance techniques to gain a deeper understanding of *MTPH*'s network:

- **Gathering targeted information**. The team will use advanced search techniques, such as *search engine dorking*, to find exposed sensitive files or login portals.
- ***Network scanning* and *network mapping***. The team will employ advanced network mapping tools to identify *network topologies*, including internal and external servers, firewalls, and other network devices. Some of the key network mapping and network scanning activities include *port scanning*, *OS detection*, and network topology mapping. During network scanning and network mapping, the *IP addresses* of all devices on the hospital's network will be catalogued for a comprehensive understanding of the network's scope.
- **Social engineering reconnaissance**. The team will use *vishing (voice phishing)* or *pretexting* to gather information from employees that could aid in the penetration test.

The intelligence gathering phase helps the team conduct *security posture assessment* of the hospital from an external perspective, providing insight into how to approach the penetration testing.

Phase 3: Threat modelling

In this phase, the *CyberHealth Security* team will conduct a detailed threat analysis for *MTPH*'s cybersecurity. The process involves:

1. **Identifying potential adversaries**. The team will determine who might target the hospital, such as cybercriminals seeking valuable patient data or insiders with access to the network.
2. **Assessing hacker capabilities and intentions**. The team will analyse what these potential adversaries are capable of and how they might intend to use the accessed data or systems.
3. **Methods of exploitation**. The team will document how these adversaries might exploit vulnerabilities, considering tactics like *malware* deployment, *social engineering attacks*, and network attacks.
4. **Valuable asset evaluation**. The team will determine which assets are most critical to the hospital, such as EHRs, and assess the potential impact of their compromise.
5. **Prioritization of security efforts**. The team will use this analysis to guide the focus of the penetration testing, ensuring the most valuable and vulnerable areas receive the most attention.

This structured approach will enable the team to tailor their penetration testing strategies effectively, aligning them with the hospital's unique threat landscape.

Phase 4: Vulnerability analysis

In this phase, the *CyberHealth Security* team will employ automated tools and manual techniques to conduct a thorough vulnerability analysis of *MTPH*'s network. This process involves:

1. **Scanning for vulnerabilities**. The team will use automated tools to quickly identify known vulnerabilities across the network, such as unpatched software or insecure configurations.
2. **Manual examination**. The team will combine automated scans with manual checks to detect subtler security flaws or complex vulnerabilities that require expert analysis.
3. **Assessment of weaknesses**. The team will evaluate the identified vulnerabilities to understand their potential impact and how they could be exploited by hackers.
4. **Prioritization**. The team will determine which vulnerabilities are most critical based on factors like the ease of exploitation and potential damage to the hospital's operations and patient safety.

The outcome of this analysis will be crucial in guiding the subsequent steps of the penetration testing, allowing the team to focus their efforts on the most significant security gaps.

Phase 5: Exploitation

When the vulnerabilities in *MTPH*'s network are identified, the *CyberHealth Security* team will initiate the exploitation phase. This crucial stage involves the following considerations:

- **Targeted breaching attempts**. The team will use specific techniques to exploit the identified vulnerabilities, testing the hospital's defences.
- ***Exploit development***. The team will craft custom scripts or tools tailored to the specific vulnerabilities identified in the hospital's network.
- **Employing various techniques**. Depending on the vulnerabilities, the team will use some or all of several possible techniques, including *SQL injection*, *cross-site scripting (X-SS)*, *buffer overflow attacks*, and *password cracking tools*.
- **Assessing the impact**. The team will seek to understand the potential damage or access that could be achieved through successful exploitation, which is vital for evaluating the hospital's security resilience.

This phase is crucial in demonstrating how actual hackers could exploit weaknesses and will help the team formulate defensive strategies.

Phase 6: Post-exploitation

In this phase, the *CyberHealth Security* team will assess the consequences of the exploited vulnerabilities in *MTPH*'s network. Key activities include:

- **Data access and analysis**. The team will investigate the types of sensitive data accessible post-breach, such as patient records, administrative data, or confidential information.
- **Privilege escalation**. The team will examine the extent to which access within the network can be increased by escalating user privileges.
- **Establishing persistence**. The team will evaluate methods by which hackers might maintain long-term access to the network, which is critical for understanding the severity of a breach.
- **Operational impact assessment**. The team will assess the potential impact of the breach on hospital services and patient safety.
- ***System forensics* and malware analysis**. The team will analyse any traces left by the exploitation process by examining system logs, detecting malware implants, or identifying any changes made to system configurations.

This phase will help the team comprehend the full scope and scale of a potential cyberattack on the hospital.

Phase 7: Reporting

In this final phase, the *CyberHealth Security* team will compile a comprehensive report of the penetration testing conducted at *MTPH*. Key components of this report include:

- **Vulnerability and exploitation details**. These will provide an overview of the vulnerabilities discovered, the methods used for exploitation, and the potential impact of each.
- **Actionable recommendations**. Suggestions will be given and prioritized for the mitigation of the identified security risks, allowing the hospital to strengthen its defences.
- ***Security posture assessment***. This will provide a holistic analysis of the hospital's overall cybersecurity strengths and weaknesses, offering insights into areas for improvement and future focus.

This report will enable the IT team at *MTPH* to develop a *response plan* that includes incident detection, response strategies, and recovery processes. This will guide the hospital's efforts to enhance its cybersecurity measures, respond to threats, and protect against future threats.

Ethical considerations

Before conducting any form of penetration testing, it is essential to address ethical considerations, especially in a healthcare environment like *MTPH*. This includes:

- proper authorization
- data confidentiality and integrity
- non-disruption of services
- reporting and responsiveness.

This focus on ethical considerations underscores the responsibility of cybersecurity professionals to balance thorough testing with the welfare of the institution and its stakeholders.

Challenges faced

To ensure that *MTPH*'s cybersecurity framework is secure, the *CyberHealth Security* team will face the following challenges:

- Evaluating black box, white box, and grey box penetration testing approaches.
- Explaining how the hospital can maintain operational continuity and protect sensitive patient data while carrying out vulnerability testing.
- Investigating how network scanning, network mapping, and OSINT tools can be used to discover active devices and information about *MTPH*'s network.
- Developing a response plan that includes incident detection, response strategies, and recovery processes.
- Discussing the ethical implications of conducting penetration testing at *MTPH*.

Candidates are not expected to research how medical devices work or review legal compliance.

Additional terminology

Buffer overflow attacks
Cross-site scripting (X-SS)
Exploit development
Hacker
IP address
Malware
Network mapping
Network scanning
Network topology
Open-source intelligence (OSINT)
OS detection
Password cracking tool
Penetration testing
Port scanning
Pretexting
Response plan
Search engine dorking
Security posture assessment
Social engineering attacks
SQL injection
System forensics
Testing
    Black box
    Grey box
    White box
Vishing (voice phishing)

Some companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.