

Prepared by Dr. Nermin Hamza

CYB740

Penetration test and Ethical hacking

Lecture 10



Physical Penetration Testing Post-Exploitation

Lecture 10

CYB740

Penetration test and Ethical hacking

Prepared by
Dr. Nermin Hamza

- Physical Penetration Testing
- Post-Exploitation
- Penetration Testing Report

Physical Penetration Testing

- **A physical penetration test** is a type of security assessment that evaluates the physical security measures of an organization's facilities, assets, and personnel.
- It is conducted to simulate real-world attacks and identify vulnerabilities in the physical security controls of a target environment.
- The goal is to identify weaknesses in physical security controls such as access controls, surveillance systems, alarm systems, environmental controls , locks, cameras, sensors, and barriers, that may lead to a breach.

- Map The Entrances And Perimeter
- Lock Picking
- Test Server Rooms, Wires And Cables
- Test Fire And Cooling Systems
- Dumpster Diving

Map The Entrances And Perimeter

- By mapping all possible entrances, such as doors, windows, and fire exits, unsecured entry points can be identified and secured.
- Mapping the perimeter involves conducting an in-depth analysis of the surroundings and buildings, which is equivalent to a reconnaissance phase in other types of penetration testing.
- This step is crucial for ensuring the security of the premises and preventing attackers from gaining unauthorized access.
- Thoroughly mapping the perimeter helps in determining the direction of the entire physical penetration testing process, identifying doors, windows, roof type, basement access, physical access policy, and lock types.

Camera Blind Spots – Finding areas not covered by CCTV.

CCTV : Closed-Circuit Television.

Testing **camera blind spots** is a standard part of a physical penetration test, and it's done in a **controlled, legal, and documented** way so the security team can see where surveillance coverage fails.

1. **Survey the site** – note all camera positions, angles, and heights.
2. **Identify possible obstacles** (walls, furniture, vehicles, plants).
3. **Send a tester to move through these areas** while:
 - An **observer watches the CCTV feed** in real time, or
 - Recordings are reviewed later to see if movement is captured.
4. **Test in different conditions** – daytime, nighttime, and poor lighting.
5. **Mark confirmed blind spots** on the map.

Lock Picking

- The lock-picking techniques in gaining unauthorized access through doors and exits, especially with the use of mechanical locks that have not undergone significant advancements.
- Many businesses nowadays use electromagnetic locks to prevent lock picking, but scanning and duplicating ID cards used for such locks require equal effort.
- In order to avoid intrusions, consider using electromagnetic locks with PIN authorization access.

Test Server Rooms, Wires And Cables

- Servers represent the most critical part of any network and are thus usually given a higher level of attention when it comes to security.
- If an attacker gains access to your server room, your entire network is compromised. With such access, an attacker can infect your system, completely disable it, or steal your most sensitive data.
- Most businesses host their data and systems in cloud environments or own their infrastructure, which is typically stored in data centers.
- Because data centers host valuable websites and company data, they often require several layers of authentication including biometric scans, identification badges, and PIN numbers to access.
- In addition, servers are stored in rack cages that require a key or PIN to gain physical access to the server.

Test Fire And Cooling Systems

- Checking your fire and cooling systems is important in order to ensure the physical safety of your server equipment if a fire or overheating occurs inside the server room.
- Without these systems, you run the risk of having your servers becoming unavailable, which is worse than being a victim of a major distributed denial of service (DDoS) attack.

Dumpster Diving

- As the name suggests, dumpster diving involves looking through the business or its employee's trash in search of any information that can be used to further penetrate the business's defenses.
- Paper documents, books, manuals, invoices, and bank statements are some of the things an attacker would look for in order to retrieve useful information. It is therefore important to use paper shredders for all documents that are being discarded. In some cases, you may wish to consider burning sensitive documents as software exists to reconstruct shredded documents.

Post Exploitation



- **The post-exploitation process** in penetration testing refers to the phase of the assessment where an attacker maintains access to a compromised system and extracts additional information and data from it.
- The post-exploitation is used to determine the capabilities and base value of the target system.
- The main purpose of post-exploitation is to gain access to all parts of the target system without knowing the user or without being detected.
- If the attacker is detected, it will make all the effects useless and everything null.

The post-exploitation process typically consists of the following steps:

- **Maintaining access:** After gaining access to a system, the attacker needs to maintain access to it. This can be done by creating backdoors or persistent access points that allow the attacker to return to the system.
- **Privilege escalation:** Once access is maintained, the attacker will try to escalate their privileges to gain greater control over the system.
- **Reconnaissance:** Once the attacker has gained access and escalated privileges, they will start gathering intelligence about the system and the network.

- Data exfiltration: The attacker will then begin to extract valuable data from the compromised system.
- Covering tracks: Finally, the attacker will attempt to cover their tracks and erase any evidence of their presence on the system. This includes deleting logs, removing any backdoors or other access points, and obscuring any signs of their activity.
- It is important to note that post-exploitation is illegal without proper authorization and consent. Therefore, it should only be performed by authorized and certified professionals as part of a legitimate penetration testing engagement.

Rules of Engagement

- The post-exploitation consists of the set of rules which is used to protect the client and penetration tester.
- By using these rules, the unnecessary conflicts between the client and tester can be avoided.
- If anything does not need to be exploited, the tester will not exploit this. Using these engagement rules, we can avoid any unnecessary actions at all costs.

There are two types of set of rules, which are as follows:

- Protecting Ourselves
- Protecting the client

Protecting Ourselves

- Before making any attack, the penetration tester should learn all the necessary details about the victim or victim system. It is really important for a penetration tester to protect their identity anyhow. When the required operation is done, the tester should avoid the risk of leaving traces.
- A tester should perform all the operations under strict confidentiality. If a tester is detected, due to this, the whole operation will be terminated.

If the tester wants to ensure the safety of digital foot-printing or personal information or information of the client, the penetration tester should perform the following steps:

- If the client is a company or business, we should sign a service level agreement or contract. This contract is used to break the security of company assets.
- If we want to store the extracted information for a confidential purpose, we should use strong encryption methods.
- If we want to store the information or data of the client, we tester should avoid personal devices.

Protecting the client

- If the client is an individual user or a company or business, the safety of their information and data is upon us.
- Before the initiation of an attack, the penetration tester should have to follow the proper steps.
- The tester may also have analyzed the attack method's capabilities and effect and determined the best suitable method for the job.

- Suppose the client is a company or business. In that case, the tester should not use attack methods as SSL stripping, DDoS (distributed denial of service), network packet sniffing, SQL injection without the client's proper permission. Due to these attacks, daily operators may be disturbed or halted.

Penetration Testing Report

- The pen-test process is not limited to executing various test cases to identify security vulnerabilities.
- It is a multi-step process that, at a high level, includes: planning, initialization, execution, documentation, and wrap-up. It is essential to provide details on what you have identified, convey how you approached the pentest, communicate blockers, offer remediation plans, and share all relevant information.
- For most pentest engagements, a report is the ultimate deliverable to a customer. So, you must ensure that your report is clean, clear, and effective.

What Is a Penetration Testing Report?

- Penetration testing involves assessing the security of a system, network, or application. Although pen-testers use the same techniques as malicious attackers, the process is legal, because it is performed with the consent of the tested organization.
- A pentester must provide a detailed report on the testing process and the vulnerabilities discovered. A penetration testing report is the only tangible product of a pentest.
- The whole purpose of a penetration test is to identify vulnerabilities and security issues the organization can remediate—and these are communicated via the report. Thus, a penetration tester must ensure they create the best possible report.

A good penetration testing report provides an executive summary of finding, summarizes the vulnerabilities and their business impact, and provides recommendations to fix them.

Successful penetration testers use a methodical approach, and document their methodology as part of the report.

Key Points to Consider Before Writing a Pentest Report:

A penetration test report provides a detailed overview of the weaknesses of the system being tested. It also outlines how to solve problems.

The goal is to identify problem areas that need attention and to fix the issue.

Here are points to consider before you write a pentest report:

- Identify and specify the aims of penetration testing
- Know the plausible impacts of a breach
- Outline the testing process and other related techniques

What makes a great pen-testing report?

- Penetration testing reports are often overly technical and lack practical steps. Also, they don't explain the business impacts resulting from the listed vulnerabilities' presence.
- A skilled penetration tester does not only find the weaknesses but also specifies the impact they have on the customer. The reports should offer the customer practical solutions to risks.

Types of penetration testing reports

The common report types (based on the main pentesting methodologies) that you should be aware of.

- Black box (or external) penetration testing reports
- White box (or internal) testing reports
- Gray box penetration testing reports

Black box (or external) penetration testing reports

Black box testing reports simulate real-world cyber attacks by providing pentesters with little to no information about the IT infrastructure of a business.

Penetration testers will “go in blind.” This forces them to closely follow the thought process and actions of an unprivileged attacker.

White box (or internal) testing reports

White box penetration testing involves sharing detailed information with pentesters that includes, network, system, and credential information. Testers are granted high-level privileges and are able to view source code. This helps them conduct a more comprehensive internal or behind-the-scenes assessment and report based on one specific aspect of security.

Gray box penetration testing reports

Gray box reports are a step up from black box testing reports. Instead of “going in blind,” attackers are granted some normal user-level privileges and might have some knowledge of a network’s infrastructure.

The test report should include:

- Any security issues discovered
- An assessment by the test team as to the level of risk that each vulnerability exposes the organization or system to
- A method of resolving each issue found
- An opinion on the accuracy of your organization's vulnerability assessment
- Advice on how to improve your internal vulnerability assessment process

Key sections (important for writing any pentest report)

There are many ways to write a penetration testing report. Fortunately, most tests will share several key sections such as an:

- Executive summary,
- Recommendations and remediations,
- Findings and technical details,
- The appendices.

Executive Summary

Objective: Clearly explain the risks that discovered vulnerabilities present and how they'll affect the future of the organization if exploited.

Length: One or two pages. Anything more is not a summary, and will probably be overlooked. Being precise and concise is paramount.

Any report worth reading should include an executive summary to help **non-technical leaders** digest and determine strategic action based on the information in your report.

Keep in mind that your target audience during this part of the report are decision-makers who allocate funds to forward remediations (not technical staff who execute changes).

For this reason, we want to ensure that it is easily understood and should therefore avoid using acronyms, infosec jargon, and including overly technical details.

Recommendations or remediations

Objective: Provide the client with recommendations for short, medium, and long-term implementation that will improve their security posture.

Length: Ideally, you want to report everything to the customers, but this could become cumbersome depending on the severity of your findings. Including the findings that are of critical, high, and maybe even medium importance is a must.

If you have a large number of findings, especially in the low and informational importance, it may be best to include them all in an appendix attached to the report instead of writing a 400-page report filled with extra information

Technical Findings

Objective: Deliver technical details of how clients can remediate the security flaws that you found.

Length: Length doesn't matter here, but want to be clear and concise in demonstrating the path you took and the actions required.

Screenshots are perfect for this purpose.

- **Your methodology**

Write this as you go (which again reinforces the importance of taking notes). It should show your full stream of thought and actions as you progressed through the assessment.

- **Objectives**

What was your mission?

Clearly communicating your mission is key because the technicians who read your report may not have been aware of the assessment.

- **Scope**

Document the agreed scope to include any hosts, IP address blocks, specific domains, and/or any specific applications or hardware that was to be tested.

You want to ensure that technical teams understand what resources were excluded from testing since they could be potential blind spots for them.

- **Details**

This is where we document how we completed our tasks or how we were rebuffed by the customer's defenses.

- **Attack Chains**

Share your successful chains along with those that failed. This lets organizations know where their defenses are working, and what needs attention. These assessments are meant to provide actionable information for the customer, not a highlight reel of our skills.

- **Appendices**
- **Objective:** Deliver technical details of how clients can remediate the security flaws that you found.
- **Length:** The more you can provide to prove your case, the better your report will be.
- The appendices will hold any supporting output, screenshots, and documentation needed to provide proof of your actions and to demonstrate the potential impact your attack path had.

How to make your penetration testing reports stand out

1. **Know your audience:** Tailor the different sections to the audience. For example, *the executive summary is probably the only thing that executives are going to read*. Keep it high level and focus on the things that impact the business and actually pose significant risks to critical systems/clients/data.
2. **Take extensive notes:** Include any tools or tactics that you've tried, especially those that failed. Sometimes you'll want to revisit systems after learning something new and realize that a tactic you tried previously would have worked if you had that information when you tried the first time around.

3. **Simplify complex topics:** Our roles as penetration testers can be highly technical and extremely complex. Nevertheless, if we can't explain something complex in a concise, easy-to-understand manner, we'll limit our ability to help customers and provide value to our employers.
4. **Proofread to protect credibility:** The credibility of an otherwise strong penetration testing report can be derailed by simple errors like spelling and grammar mistakes. Use some form of grammar checking, (Grammarly is my favorite), and ideally, have another team member read it over from a different perspective.

Executive Summary

Overview

Basecamp engaged Doyensec to perform a security assessment of the HEY platform. The project commenced on 06/29/2020 and ended on 07/17/2020 requiring 3 security researchers. The project resulted in twenty one (21) findings of which three (3) were rated as *high* severity.

The project consisted of a manual application security assessment against HEY's web platform and its APIs, mobile (Android, iOS) and desktop (Electron-based) applications.

Testing was conducted remotely from Doyensec EMEA and US offices.

Scope

Through meetings with Basecamp, the scope of the project was clearly defined:

- Identify misconfigurations and vulnerabilities in HEY's web platform and applications
- Review the overall application design in terms of security and privacy
- Evaluate the overall security posture and

- **HEY for iOS**
 - com.hey.app.ios
 - Version 1.0.5 (184)
 - <https://github.com/basecamp/hey-ios>
- **HEY for Android**
 - com.basecamp.hey
 - Version 1.0.8 (73)
 - <https://github.com/basecamp/haystack-android>
- **HEY Web Platform**
 - Cloned on commit #ba365cc40ae523704e1d5aef00d8c43a7ddc1a0f
 - <https://github.com/basecamp/hey-electron>

Scoping Restrictions

During the engagement, Doyensec did not encounter difficulties with testing the application.

The following platform features were not yet available for testing:

- Projects management and invitations
- Mobile OAuth design
- Queenbee controller
- /demo, /development, /post_office endpoints
- Functionality related to custom domains or

Executive Summary

Mandiant was engaged by Accellion, Inc. (Accellion) to perform a security assessment of Accellion's File Transfer Appliance (FTA) software, in the wake of two related but distinct exploits used to attack client Accellion FTA systems—one that was discovered and addressed by Accellion in December 2020 (the "December Exploit"), and another that was discovered and addressed by Accellion in January 2021 (the "January Exploit") (collectively, the "Exploits").

The objectives of Mandiant's security assessment included:

- Independently identifying the security vulnerabilities used in the attack activity, based on review of compromised Accellion FTA instances
- Validating the patches that Accellion issued for the vulnerabilities
- Testing FTA version 9.12.432 (current as of the time of Mandiant testing) for further vulnerabilities in the software

This assessment was performed between February 4, 2021 and February 26, 2021.

Summary of Results

Accellion identified two zero-day vulnerabilities that were part of the December Exploit—CVE-2021-27101 and CVE-2021-27104—and two zero-day vulnerabilities that were part of the January Exploit—CVE-2021-27102 and CVE-2021-27103. Based on Mandiant's own forensic analysis of a sample of compromised Accellion FTA instances—which were provided to Mandiant by Accellion as well as impacted Accellion customers (in investigations Mandiant conducted directly for those customers), Mandiant confirmed that the attacker activity exploited these vulnerabilities (the "Exploited Vulnerabilities"). Mandiant did not identify any additional vulnerabilities that were exploited by the attackers.¹ Mandiant also validated the efficacy of the patches Accellion released to address the Exploited Vulnerabilities, which Accellion made available to FTA customers soon after each Exploit was identified.

The Exploited Vulnerabilities were of critical severity because they were subject to exploitation via unauthenticated remote code execution. Through its source code analysis and penetration testing, Mandiant did not identify any new such unauthenticated remote code-execution vulnerabilities. Mandiant did identify two previously unknown authenticated-user vulnerabilities: (1) Argument Injection (CVE-2021-27730), accessible to authenticated users with administrative privileges; and (2) Stored Cross-Site Scripting (CVE-2021-27731), accessible to regular authenticated users. The Argument Injection finding yielded a Common Vulnerability Scoring System (CVSS v3.0) score of 6.6 (medium severity) and the Stored Cross-Site Scripting finding was rated 8.1 (high severity). Accellion has developed a patch for these two vulnerabilities (FTA 9.12.444), which Mandiant has validated.

Project Scope

Download pentest report

- <https://pentestreports.com>

<https://brightsec.com/blog/penetration-testing-report/>

<https://www.cobalt.io/blog/how-to-write-an-effective-pentest-report-vulnerability-reports>

AI and Penetration test

- The rapid advances in Artificial Intelligence (AI) and Machine Learning (ML) affect many fields in cyber security — among them, penetration testing (pen-testing).
- As cyber threats grow in complexity, traditional manual methods of vulnerability assessment struggle to scale and keep up.
- Integrating AI into pen-testing can enhance detection accuracy, speed, and adaptiveness. However, this transformation also raises new technical, ethical, and operational challenges.

- Input: Target scope, rules of engagement.
- Automated Reconnaissance: NLP-based intelligence gathering.
- Vulnerability Prediction: ML models evaluate potential weaknesses.
- Attack Simulation: RL agent explores and tests exploit chains.
- Analyst Review: Human oversight validates or modifies AI actions.
- Report Generation: Results are compiled into an actionable vulnerability report

What is PentestGPT?

- PentestGPT is an AI-powered penetration testing tool that leverages the OPENAI API to guide users through assessments in an *interactive mode*.
- It automates routine steps, supports local models, and enables *high-quality reasoning* and decision-making during each phase of the testing process.

- Mindgard *does* leverage AI / ML-based techniques but with a specific focus:
 - Mindgard isn't a traditional penetration-testing tool for networks or apps.
 - Instead, it is designed to **test and secure AI/ML systems themselves** (e.g. LLMs, multimodal models, chatbots).

- References :
- **Suman Thapaliya,"AI-Augmented Penetration Testing: A New Frontier in Ethical Hacking" , International Journal of Atharva**
DOI: <https://doi.org/10.3126/ija.v3i2.80099>
- <https://mindgard.ai/>
- <https://abstracta.us/blog/security-testing/pentestgpt-penetration-testing-with-ai>

Thank You