CompTIA PenTest+

Analyzing and Reporting the Pen Test Results

Introduction

Planning
Penetration Testing
PenTest+
Sanitization
Normalization
Encryption

Welcome to the **Analyzing and Reporting the Pen Test Results** Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Guidance on Analyzing the Pen Test Data
- Exercise 2 - Develop Recommendations for Mitigation Strategies
- Exercise 3 - Write and Handle Reports
- Exercise 4 - Conduct Post-Report-Delivery Activities

After completing this lab, you will have covered the following topics:

- Perform Pen Test Data Collection
- Perform Pen Test Data Categorization
- Prioritize the Results
- Suggest Solutions regarding People, Processes, and Technology
- Create Categories of Findings
- Conduct End-user Training
- Password Encryption and Hashing
- Multi-factor Authentication
- Input Sanitization
- System Hardening
- Data Normalization
- Report Structure
- Report Storage, Handling, and Disposition
- Post-Engagement Cleanup Tasks
- Removal of Credentials
- Removal of Various Tools
- Client Acceptance
- Attestation of Findings
- Lesson Learned
- Follow-up Actions

Exam Objectives

The following exam objectives are covered in this lab:

- **PT0-001:** 5.1 Given a scenario, use report writing and handling best practices
- **PT0-001:** 5.2 Explain post-report delivery activities
- **PT0-001:** 5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities
- **PT0-001:** 5.4 Explain the importance of communication during the penetration testing process.

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to*

research theoretical topics in more detail.

Lab Duration

It will take approximately **1 hour** to complete this lab.

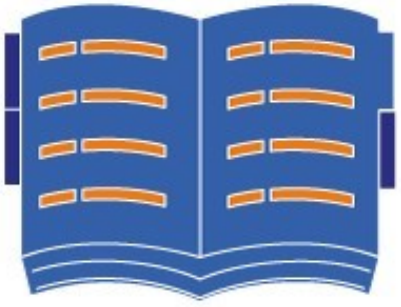
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for PenTest+.



Click **Next** to proceed to the first exercise.

Exercise 1- Guidance on Analyzing the Pen Test Data

Penetration Test, or Pentest, is a simulated cyber-attack to exploit vulnerabilities in a network and systems. A person conducting the pentest can attempt to exploit applications, protocols, Application Programming Interfaces (APIs), servers, firewalls, and anything that can be exploited on a network. The core intent is to discover any vulnerabilities before an attacker from the outside world can and exploit them to simulate the amount of damage that can be caused.

In this exercise, you will learn about analyzing the pen test data.

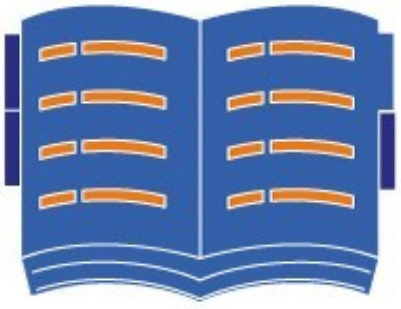
Learning Outcomes

This exercise covers the following:

- Perform Pen Test Data Collection
- Perform Pen Test Data Categorization
- Prioritize the Results

Your Devices

This exercise contains supporting materials for PenTest+.



Learning about Performing Pen Test Data Collection

During penetration testing, you are likely to gather some of the following information:

- IP addresses of the systems and servers
- Network map or the layout
- Number of servers
- Operating systems and their versions

- Applications and their versions
- Security devices and configurations
- Vulnerabilities

As a result, you are likely to perform and document some of the following tasks:

- Social engineering attacks
- Access to secure areas
- System compromise
- Privilege escalation
- Evading detection by a security device, such as firewalls
- Web application attacks

Since you will be documenting this information, you need to ensure the security of any data that you gather. If this data falls into the wrong hands, it is likely to be misused.

Perform Pen Test Data Categorization

Just like asset categorization, the test results should also be categorized, although there are no correct or incorrect ways of categorizing test data. When you categorize the data, you need to be specific about what is being tested and the type of asset it is. For example, you can categorize the test data in the following manner.

Category: Application

Sub-category: Web application

In the given example, you have set the Category as Application. Any application-based pen test data would be classified in the category Application. Then, there could be different types of applications. For example, it could be a cloud-based application, locally hosted application, or a Web application. You should mention the sub-category.

Some more examples of sub-category that you can use are:

- Database
- Front-end

- Code

The categorization does not have any specific rules, but it should be agreed upon between you and the client.

Prioritize the Results

The results of penetration testing can be prioritized depending on the client's needs. The simplest method of prioritizing results is to label them 1 - 10, where higher the number, more critical the issue. Alternatively, you can also label them as:

- Critical
- High
- Medium
- Low

However, you need to understand the client's reason for penetration testing. If the client is opting for compliance (such as PCI DSS), then labeling should be done according to that standard. For example, what you might call a critical vulnerability may not be considered critical as per PCI DSS compliance.

Exercise 2 - Develop Recommendations for Mitigation Strategies

After gathering data and categorizing it, you need to ensure you develop recommendations for your findings. As a pentester, you are not responsible for the implementation, but the client would expect you to provide mitigation strategies that are suitable to best address your findings.

In this exercise, you will learn about developing the recommendations for mitigation strategies.

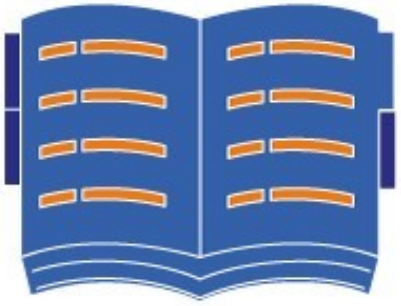
Learning Outcomes

This exercise covers the following:

- Suggest Solutions regarding People, Processes, and Technology
- Create Categories of Findings
- Conduct End-user Training
- Password Encryption and Hashing
- Multi-factor Authentication
- Input Sanitization
- System Hardening

Your Devices

This exercise contains supporting materials for PenTest+.



Suggest Solutions Regarding People, Processes, and Technology

When you are suggesting mitigation strategies, you need to ensure you cover three important aspects of an organization. These aspects are people, processes, and technology. The mitigation strategies that you suggest must cater to all three aspects. If this is not done carefully, then there will be chances that you will end up leaving vulnerabilities, which is not the end goal. It is fine to have mitigation strategies for all three overlap.

People

Remember that people or users are the weakest links in the security chain. Here are some suggested mitigation strategies:

- **Technical Controls**: You can reduce the risk of an incident by implementing multiple technical controls. It is worth noting that while you reduce a risk, it can never be fully avoided.
- **Leadership**: You should get leadership involved. Let them set the tone and lead by example. Most often, the leadership is only involved in sanctioning the budget but does not follow the security-related processes themselves. Therefore, their involvement can be a game-changer.
- **Reminders**: You need to keep reinforcing security-related messages. It is always good to make them interesting by adding examples. Regular change in wallpaper and posters on the wall can help.
- **Rewards and Penalties:** There should be penalties for non-compliance. Depending on the severity of the non-compliance, you can suggest the penalties. In the same manner, you should also set rewards for people who follow the set security practices.
- **Ownership:** You should give responsibilities of ownership to the users. For example, if a user sees an incident, then the user should report it. In return, a reward can be given. Security incidents are less likely to occur in an organization where the users have a sense of ownership over security practices.

Processes

Processes are created by people, but yet, people do not tend to follow them. As and when there is a process change, people tend to avoid the new process. Any avoidance of security practices can lead to attacks. Here are some suggested mitigation strategies:

- **Technical Controls:** As above, technical controls can help you avoid several risks that can be present in the organization due to poorly designed processes. You should implement multiple technical controls to ensure that there are no process loopholes. Processes must be reviewed for their vulnerabilities and changed accordingly.
- **Leadership**: Leadership should be involved in processes, as well. After all, they have to lead by example, and therefore, they need to not only understand the processes but also approve them.
- **Return-on-investment (ROI**): You will need to monitor the ROI on security processes, and it can be done through implementing Key Performance

Indicators (KPI).

Technology

Technology helps in solving a multitude of issues that may arise and pose a risk to the business and its users. Here are some suggested mitigation strategies:

- **Vulnerability Scans**: Must be done on a monthly basis, but it depends on the size of the IT infrastructure that you are managing. It may not be possible to do it monthly on the entire infrastructure, and in such scenarios, you should focus on critical devices and servers for monthly scans and the remaining devices and servers once in two months.
- **Penetration Testing**: This should be done once per year. You need to plan the scope and targets carefully.
- **80/20 Rule**: You must consider the 80/20 rule when dealing with risk. 80 percent of vulnerabilities can be closed or dealt with whilst only using 20 percent effort and cost. This is a globally used rule when dealing with risk reduction.
- **Technology solutions**: You should use the latest technology solutions, such as Transport Layer Security (TLS) instead of SSL. Another example could be to configure the Web servers to use HTTPS instead of HTTP.

Create Categories of Findings

In penetration testing, you are likely to have several findings. You will need to categorize them properly and put the suggested remediation for each one of them. Some of the findings can be:

- **Finding**: Shared logins in use.
- **Remediation**: Each user must use a different user account. With a shared user account, accountability is not possible.
- **Finding:** Weak and simple passwords in use.
- **Remediation**: Use a complex password. In a Windows environment, password policies can be set. For example, a password must be 8 characters long with the combination of letters, numbers, and special characters. It must be changed every 90 days.
- **Finding**: Passwords stored in plain text.

- **Remediation**: If passwords are being stored, they must be encrypted or hashed. Similarly, the passwords in transmission must also be encrypted.
- **Finding**: Multi-factor authentication not implemented.
- **Remediation**: Implement multi-factor authentication with critical servers and services.

These are some of the examples of findings and remediations. Not necessarily that you will find them in all penetration tests that you perform, but some are likely to occur. Each finding can have unique remediation.

Conduct End-user Training

Users are a critical part of IT security. You can implement multiple layers of security and use several technical controls, but a single user can bring the network down by sharing passwords or downloading malware from a suspicious Website. As such, regular training is a must for users. Whenever there are changes in the IT environment, the users must be trained. Users should also know whom to approach if they find or see something suspicious. They should be trained to report the incident to the appropriate authorities. Most users tend to avoid training, which should not be the case.

Password Encryption and Hashing

As a mitigation process, you should suggest that passwords must never be stored in plaintext and must be either encrypted or hashed. Both methods are different; Passwords are encrypted using symmetric encryption, which uses a key. When the password is encrypted, a key is generated. Anyone with the key can decrypt the password to obtain the actual value.

Hashing is not a reversible process, and once a hash is generated, it cannot be reversed. When a user creates a password, the username is appended to the password, and a hash value is generated.

Passwords must never be hardcoded into applications. If an attacker finds the hardcoded password, he can then gain complete control over the application. A hardcoded password is coded within the application itself. This is done by the developers to have a backdoor entry in most cases. When the application is compiled,

the hardcoded password remains within the code and allows the developers to bypass the usual security methods such as login.

Multi-factor Authentication

Most organizations use single-factor authentication with critical systems and services. You should strongly suggest multi-factor authentication in such scenarios. Multi-factor authentication can be used with the following:

- **Something only you know**: a password
- **Something only you have**: a smart card
- **Something you are**: a fingerprint or retina scan

You can suggest the use of any two of them.

Input Sanitization

Web applications, if not programmed properly, are prone to some of the key attacks:

- SQL injection
- Cross-site scripting (XSS)
- Remote file inclusion (RFI)

Input validation and sanitization are two methods that can be used to prevent attacks on Web applications. You should use both methods to ensure that a user inputs the correct value and then validate the values.

You can also validate an input made by the user. For example, the user needs to use a complex password when creating a user account. The validation process must validate that the user has entered the password that meets the validation process. If not, then the application must prompt the user with an error.

System Hardening

Several organizations don't pay attention to system hardening and use systems with the default settings. If you come across a situation like this, then you must recommend system hardening. Some of the recommendations that should reduce the attack surface should include:

- Systems should not have unnecessary services running.
- Systems should not have unnecessary ports open.
- Systems must be updated with the latest patches and updates.
- Systems must have the latest device drivers.
- Systems must be protected with an anti-malware solution.
- Systems must have firewalls running.
- Systems should not have unnecessary applications installed that are not being used.
- Users should not have administrative privileges on the systems.
- Data must not be shared in unencrypted form.
- Data at rest must be encrypted.

These are some of the guidelines or mitigation strategies that you can suggest to the client.

Exercise 3 - Write and Handle Reports

After you are done with categorizing penetration testing data and assigning priorities to the results, you need to write reports for final submission. You will need to write, handle, store, and ensure secure disposition of the report.

In this exercise, you will learn about writing and handling the report.

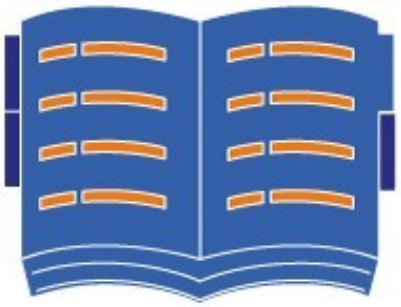
Learning Outcomes

This exercise covers the following:

- Data Normalization
- Report Structure
- Report Storage, Handling, and Disposition

Your Devices

This exercise contains supporting materials for PenTest+.



Data Normalization

Data normalization is a concept that is used in databases. It focuses on eliminating data redundancy and ensuring that data is stored logically. Data normalization also ensures the integrity of data by removing anomalies that can occur from insertion, update, or deletion. When writing a report, which will not be in a database format, you still need the data normalization principles to be applied.

There will be different stakeholders who receive the reports. You need to ensure that the report is prepared in a manner that can cater to the stakeholders. For example, senior management will not have any interest in the technical findings section. They would rather look at something that they can understand. Such information can be included in the Executive Summary.

The technical team at the client end will not have any interest in the Executive Summary, but they will surely look for the technical findings. At the same time, the end-users will have no interest in this section. Therefore, you need to create a report for the right stakeholders with the appropriate information, which can include technical and non-technical data.

Report Structure

Depending on the stakeholders and audience for the penetration testing report, there can include a variety of information. However, there are some key sections that must be included in a penetration testing report. These sections are:

1. **Executive Summary**: This section must be written in simple language. It should talk about the risks and business impact of the vulnerabilities that have been discovered. You need to ensure that there is no technical jargon included in this section. Rather, focus on high-level findings and possible remediation that can

reduce the risk for the business. This section is for senior management, who can use this information to make an informed decision about their business. It is good to add visuals, such as graphs.

2. **Methodology**: This section should focus on methods used in penetration testing. Each step in the methodology should be repeatable to reproduce the results if required.

3. **Technical Risks:** You must include technical risks. It would be good to categorize the risks by labeling them with a risk rating. To be able to do this, you should include the risk rating table.

4. **Vulnerability Measurement:** You should also use a measurement system for vulnerabilities. For example, you can use 1 for low impact and 5 for high impact. Each value in the measurement system must be explained clearly. You must clearly outline the potential impact of each vulnerability with the help of a rating.

5. **Remediation:** For each vulnerability, along with its rating, you need to define the remediation method.

6. **Conclusion:** This is the wrap-up section that should state whether the objective of penetration testing has been met or not. It is good to highlight some of the key points in the report.

7. **Annexure:** The supporting data, such as scan reports, test results, etc. can go in this section.

Report Storage, Handling, and Disposition

For report storage, handling, and disposition, you should ensure the following:

Report Storage

1. The penetration testing report must be stored on a secure and encrypted drive.

2. The penetration testing report must never be transported via a portable drive, such as unencrypted USB. It should be transported via encrypted portable media.

3. At any given point in time, the report should not be shared with unauthorized personnel.

4. You need to define the time for which you need to store the report.

5. The report must be available only to the required stakeholders.

Report Handling

1. The integrity, confidentiality, and authenticity of the penetration test must be maintained.

2. The report must be transferred securely over the network.

3. You need to protect the report from accidental disclosure.

4. You should also maintain a record of who is accessing the report.

5. You must ensure that there is versioning implemented in the report.

6. You must also ensure that the chain of custody is enforced when transferring the ownership of the report.

Disposition

1. It is a method of transferring the report to an authorized individual.

2. The authorized person in possession of the report is responsible for the report.

3. The transfer should include the following:

- Printed copies of the report
- Electronic copies of the report
- Related documentation
- Acknowledgment
- Sign-off by the recipient

4. After disposition, you must move the report and related artifact to a secure location. The report and related artifact must not be on your working laptop or desktop.

Exercise 4 - Conduct Post-Report Delivery Activities

After the penetration testing, there are certain post-report delivery activities that you must perform. Some of these tasks include cleanup of credentials and tools used in penetration testing.

In this exercise, you will learn about conducting post-report delivery activities.

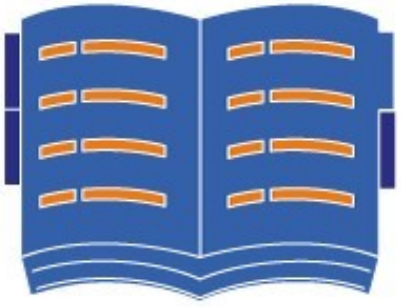
Learning Outcomes

This exercise covers the following:

- Post-Engagement Cleanup Tasks
- Removal of Credentials
- Removal of Various Tools
- Client Acceptance
- Attestation of Findings
- Lesson Learned
- Follow-up Actions

Your Devices

This exercise contains supporting materials for PenTest+.



Post-Engagement Clean-up Tasks

During penetration testing, you would have installed various tools and created various files and user accounts. In the post engagement clean-up, you need to ensure that you remove all of these without fail. Leaving them could compromise the security of the system. For example, during system exploitation, you had created a user account with administrative privileges. If you fail to remove this, you are compromising the security of the system as the user account might just come in handy for an attacker.

The clean-up tasks can be split into two parts:

- Removal of certain tools and credentials
- Restoration of original settings and data

For example, to cover your tracks, you had previously deleted the log files from a server. As part of the clean-up tasks, you should restore its logs back in the original state. Another example can be installing a backdoor in a server for easy entry. You must remove the backdoor. Leaving it can compromise the server security if discovered by an attacker.

Removal of Credentials

Removing the user credentials in the clean-up task is necessary. Depending on how the user account was created, you will use different methods of removal. Consider the following:

- Removal of the user accounts created on a domain controller - if these accounts are used in various systems, then removing them from there will not help. These user accounts must be deleted from the domain controller.
- Removal of user accounts created locally - even though these user accounts are restricted to a local system but depending on their privileges, they can be used for compromising the system. Therefore, you must remove them.
- Removal of user accounts in a database - There can be a chance that an application allows you to create a user account but does not offer a deletion feature. In that case, you must remove the user account from the backend database. Similarly, any user account created within a database directly must also be deleted.

Removal of Various Tools

During the penetration testing, you might have installed various tools or added certain features or tasks that must be removed in the clean-up. For example, you might have created a few registry keys to exploit a Windows system. You need to ensure that these registry keys are removed to save the Windows system from being compromised later.

Some of the key tools that you must remove if they are installed during the penetration testing:

- Metasploit payloads and exploits
- Keyloggers
- Netcat binaries
- Vulnerability scanners and agents
- Any other tool that may have aided in penetration testing
- Any output or associated files with these tools

If you had created any automated tasks on Windows or Linux systems, then you must remove them. Some tools may be loaded in the memory, and therefore, it is better to reboot the server to clean the memory.

Client Acceptance

Penetration testing was performed on an agreed-upon scope. After you have completed the scope of penetration testing, you need to obtain client acceptance; you can do this in two different ways:

- Submit a formal report and get the client to agree with your findings
- Hold a face-to-face meeting with the technical and business teams and share your findings. You are likely to be asked several questions, which should be answered.

With the client acceptance of your report or discussion, the formal engagement of penetration testing comes to an end.

Attestation of Findings

Most organizations, who hire external consultants to do the penetration testing, require attestation of the final penetration testing report. Attestation is the process of signing off the final report stating that the data in the report is correct, and those tasks have been performed. Attestation of the final report is typically in the form of a letter that confirms that penetration testing has been performed by you, and findings are correct.

In some cases, the organizations may also require you to submit proof of your work. For example, you could submit some of the following as proof of your work:

- Captured sensitive plaintext data in transit
- Live demonstration of SQL injection,
- Screenshot of your access to sensitive and confidential data
- Copy of confidential data that you obtained during penetration testing
- Breaking of simple passwords, which could be through brute-force or dictionary attacks

You may or may not use all these methods. However, some proof of your work maybe required.

Lessons Learned

As and when projects, be it of any kind, are completed, they offer new learnings for each individual in the team. In the context of penetration testing, when a project is completed, the entire team should get together for the lessons learned meeting. Each task in the penetration testing project should be documented in the lessons learned document.

The core intent of the lessons learned meeting is to increase the efficiency and effectiveness of each individual and processes in the penetration testing, along with using the knowledge to improve the output in the upcoming penetration testing projects. In the lessons learned meeting, everyone should speak about their experiences in the project and the learnings they have done. Every experience and learning should be documented. For example, an experienced pentester has found a workaround to exploit a specific vulnerability. When this is documented and shared with the other team members, it is a learning for them. Next time, another pentester

can use the same workaround and exploit the vulnerability. This will help the pentester in saving time and effort.

The document should include not only what went well but also what did not go well. For example, a specific exploit did not work under a specific condition. Therefore, the expected task of exploiting a system took more than the anticipated time. This type of learning must be documented in detail, and if possible, a workable solution must also be mentioned so that the next time, another pentester does not face the same challenge.

In the lessons learned document, you should include some of the following:

- What new penetration tasks did the team perform and learn from them?
- What did go well, and what did not in the current penetration testing project?
- Was there any new technology explored during the penetration testing project?
- Did the team come across a new exploit, vulnerability, or risk that the team should document and learn more about?
- Was the scoping of the penetration project correct? If not, what is learned from it?
- Was there enough time to complete the tasks in the penetration testing project?

These are some of the questions that should be answered in the lessons learned document and shared with each team member.

Follow-up Actions

Depending on the scope of the engagement of penetration testing, follow-up actions may or may not be included. If they are not included as part of the engagement, then the client is likely to approach you to perform some of the follow-up activities, which could include:

- Prepare and schedule for another round of penetration testing
- Verify the suggested mitigation activities from the first round of penetration testing
- Re-test the vulnerabilities discovered in the first penetration test
- Attempt to discover any new vulnerability that may have occurred because of mitigation activities

Depending on clients requirements, the second round of penetration testing can be limited to test only some of the critical vulnerabilities. It is also possible that the client may want the entire exercise to be repeated as a follow-up project.

Review

Well done, you have completed the **Analyzing and Reporting the Pen Test Results** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Guidance on Analyzing the Pen Test Data
- Exercise 2 - Develop Recommendations for Mitigation Strategies
- Exercise 3 - Write and Handle Reports
- Exercise 4 - Conduct Post-Report-Delivery Activities

You have covered the following topics:

- Perform Pen Test Data Collection
- Perform Pen Test Data Categorization
- Prioritize the Results
- Suggest Solutions regarding People, Processes, and Technology
- Create Categories of Findings
- Conduct End-user Training
- Password Encryption and Hashing
- Multi-factor Authentication
- Input Sanitization
- System Hardening
- Data Normalization
- Report Structure
- Report Storage, Handling, and Disposition
- Post-Engagement Cleanup Tasks

- Removal of Credentials
- Removal of Various Tools
- Client Acceptance
- Attestation of Findings
- Lesson Learned
- Follow-up Actions

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.