CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 17

Communicating During the PenTesting Process

Objectives

- Explain the importance of communication during the penetration testing process.

Lesson 17

Topic 17A

Define the Communication Path

Define the Communication Path

- Good communication with all stakeholders during the PenTest is essential for the success of the PenTest.
- Having an escalation path for communications protects the team from having to make risky or potentially damaging decisions.
- Agree upon thresholds and protocols include:
  - When and how the client will notify the PenTest team that a test is unacceptably interfering with operations/system performance.
  - When and how the PenTest team will involve the client IT department if an accident occurs, or a system becomes destabilized or unresponsive.

Outlining the Communication Path

- In a PenTest, it is important to ensure that the right people are informed and what information should be shared.
  - The client IT manager and CIO/CISO should be aware of the engagement.
  - Key department managers should be aware, in case unforeseen incidents affect their departments.
- However, the organization might not want all staff to know when a PenTest is occurring
  - Particularly if they want to check on the effectiveness of using social engineering to launch an attack

Communicating with Client Counterparts

- The designated lead of the PenTesting team should have close communication with their client counterpart (IT manager).
- To reduce confusion, all communication between the PenTesting team and the client should go through these points of contact.
- The two lead roles must both be hands-on.
  - This allows for immediate response in case of incidents, unexpected discoveries, and additional client requests.

Defining Contacts

- **Primary contact -** responsible for handling the project on the client's end.
  - This can usually be a CISO or other party responsible for the major decisions surrounding the penetration test.
- **Technical contact** - responsible for handling the technology elements
  - They have a more in-depth knowledge of the technical aspects of the system, the impact of the activities in the client's network, and constraints of the PenTest might.
- **Emergency Contact –** available in case of urgent matters.
  - Ideally, the emergency contact should be available 24/7 or at least during the hours that the activity is being performed if done during business hours.

Review Activity: Define the Communication Path

- Explain why it’s essential to have good communication with all stakeholders during the PenTest.
- Describe reasons the team should take steps to ensure that the right people are informed and what information should be shared.
- Discuss the importance of maintaining communicating with the team's client counterparts
- List a few key contacts involved in the PenTest process.

Lesson 17

Topic 17B

Communication Triggers

Triggering Communication Events

- All facets of communication need to be evaluated and define what should trigger official communications.
- Here are a few examples of reasons to initiate communication:
    - Status reports are regular progress briefings with the client
    - Emergencies should be handled separately, although ongoing issues such as delays, or other problems should be raised at status meetings.
    - Critical findings are identified issues that imply a very high risk to the client's organization.

Prioritize Findings

- The nature of a PenTest is that it is a fluid process
- The team must be able to prioritize findings as they occur.
    - Information that is discovered during the reconnaissance phase drives the decisions on what exploits to try and, ultimately, what solutions to propose.
- Awareness of the need for contingency planning for the PenTest engagement itself, enables you to incorporate it into your plans
    - Might require the team to reprioritize the goals of one activity or large sections of the PenTest.

Providing Situational Awareness

- During the PenTest, a situation might need to be addressed if the PenTest attempt is detected.
- In this cases, it will be necessary for the team to communicate these situations to the appropriate contacts from the client.
- Providing situational awareness to key client personnel can help deconflict the breach
  - This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

Recognizing Criminal Activity

- It is incumbent upon a company to fully disclose vulnerabilities and breaches to anyone who may be harmed by the breach.
- During the PenTest, if the team discovers vulnerabilities and breaches, any findings should be kept strictly confidential
- An exception to this is if the team were to uncover criminal conduct
    - In this case, you might be obligated to notify law enforcement. You should consult with your team's legal counsel for further details.

Triggering False Positives

- Automated scans have the potential to produce large numbers of false positives. Some reasons that may trigger a false positive:
  - The scanner is using a vulnerability database with outdated definitions.
  - The scanner incorrectly scores a vulnerability as more severe, or more easily exploited, than it is.
  - Customizations in the target environment are inadvertently triggering the scanner to identify a vulnerability.
  - The scanner is not properly configured

Investigating False Positives

- As a PenTester, you must be able to identify when results indicate a false lead on a vulnerability.
- There are several tactics you can employ to identify false positives; one of the most effective is results validation.
- There may be gaps in your knowledge, especially if you're conducting an unknown environment test.
    - In this case, you'll need to try your best with what you have and concede that you won't necessarily be able to avoid false positives entirely.
    - You may choose to conduct more reconnaissance on the target environment if you are intent on avoiding as many false positives as possible.

Review Activity: Communication Triggers

- List some reasons to initiate communication during the PenTest
- Discuss why the team must be able to prioritize findings as they occur.
- Describe why it’s essential to provide situational awareness
- Review best practice if the team observes evidence of criminal activity
- List reasons that can trigger a false positive
- Explain reasons you might need to identify when results indicate a false lead on a vulnerability.

Lesson 17

Topic 17C

Use Built-In Tools for Reporting

Presenting the Findings

- One way to share your findings is by using an established standard, such as Penetration Testing Execution Standard (PTES).
    - Provides guidance on how to present results in a way that is easily readable and is meaningful.
- Here is an example on how to assess and classify vulnerabilities:
    - Vulnerability Classification Levels
    - Technical Vulnerabilities
    - Logical Vulnerabilities
    - Summary of Results

Sharing Findings with Dradis

- The Dradis framework can help to greatly reduce repetition
  - This will help provide consistency of the report when different pieces have been worked by members from the beginning.
- The framework focuses on sharing details about the information gathering phase, useful exploits, and report findings.
  - This ensures that your team is not missing important areas to scan or that two team members are working on the same exploit at the same time.

Building Reports with Nessus

- Nessus is a well-established vulnerability scanner with a module dedicated to reporting
- The module can be expanded with the use of templates that define the structure of the report.
- The objective is to provide consistency, even across different clients
- Can help identifying common vulnerabilities and issues found on different infrastructures.

Review Activity: Use Built-In Tools for Reporting

- Discuss some best practice on how best to present the findings of the PenTest
- Discuss why the team might choose to use Dradis to provide details of the PenTest
- Explain the benefit of creating reports with Nessus

Lesson 17

Summary