CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 20

Performing Post-Report Delivery Activities

Objectives

- Explain post-report delivery activities.

Lesson 20

Topic 20A

Post-Engagement Cleanup

Begin the Cleanup Process

- Once the PenTest is complete and the report is handed off, it's time to begin the cleanup tasks.
  - This ensures there are no artifacts left that an attacker could exploit
- Some common cleanup tasks can include, but are not limited to:
  - Delete any new files you created from the affected systems.
  - Restore any log files you deleted.
  - Restore a clean backup copy of any apps that you compromised.

Removing Shells

- During cleanup, the team will need to remove any hidden or dormant shells on the target system
  - **On a Windows system**: Remove any values added to the HKLM and HKCU Run Registry keys that start a shell on a during boot.
  - **On certain Linux distros**: scripts in /etc/init.d/ and /etc/systemd/ are examples of similar run-on-boot functionality.
- Additionally, remove any scheduled tasks in Windows Task Scheduler or the Linux crontab file that call a shell.

Deleting Test Credentials

- Removing tester-created credentials, shells, and tools that were installed on systems is not necessarily a simple task.
  - The exploits might be deeply embedded in the target systems, especially if you applied evasive techniques to escape notice.
- When it comes to removing credentials that you created during the test, keep in mind that not all authentication systems are alike.
  - On to a local system you can delete any local credentials
  - The process is much different for AD domain accounts.

Removing Tester-Created credentials

- Another concern with removing test credentials is that they might be integrated tightly into a particular system
  - Deleting the credentials could lead to system corruption or other issues.
- For example, systems that require an audit trail might not provide a “delete account” feature on the standard interface.
  - In that case, you may need to remove the test accounts from the user database directly

Eliminating Tools

- Besides shells, you'll also need to remove other tools that you added to a system to enable its compromise
  - Metasploit payloads, keyloggers, and vulnerability scanner agents.
- Some of these tools might be loaded into memory and are therefore automatically removed on system reboot
  - Others linger on the target system until manually uninstalled.
- In some cases, you may have to securely destroy the tool’s data and any associated files so that they cannot be recovered by an attacker

Destroying Test Data

- When purging data, follow a technically secure process
  - Adhering to a known procedure such as an automated script, will avoid issues such as forgetting about any exposed sensitive data.
- Shredding data overwrites the storage with new data.
- Save time and effort by automating cleanup using scripts.
  - Revert malicious changes, uninstall malware, restore deleted logs
- NOTE: To properly automate cleanup tasks, you will need to have kept meticulous records on all exploits launched

Review Activity: Post-Engagement Cleanup

- List some of the tasks that take place during cleanup
- Discuss the importance of removing any shells on the target system
- Explain some of the issues that might take place when deleting test credentials
- Describe what's involved when removing tools used during the PenTest.
- Review some best practices when destroying test data

Lesson 20

Topic 20B

Follow-Up Actions

Outlining Post Delivery Activities

- Once the PenTest is complete the team will have a few final remaining tasks to complete.
- The client will have to accept your report and its findings, which must be backed up by evidence of what you found.
- The team should provide recommendations to the client:
  - Scheduling additional tests with the client organization
  - Checking back with the client to see how their mitigation efforts are going
  - Researching and testing new vulnerabilities

Gaining the Clients Acceptance

- After finishing the PenTest and complete the report, you should have a discussion with the client about the findings.
- Obtain confirmation from the client that they agree that the testing is complete and accept the findings as presented in the report.
- Use the meeting to discuss with the client anything that needs to be clarified or changed
- In some cases, they may also voice concerns on how the test was handled, which can help manage future situations.

Confirming the Findings

- Attestation is the process of providing evidence that the findings detailed in the PenTest report are true.
- By signing off on the report, you are attesting that you believe the information and conclusions in the report are authentic.
- The client must believe that what you have said about their people, processes, and technology is accurate.
- You must be prepared to prove what you claim.
  - For example, if you want to prove that you were able to break into a server, you could present exfiltrated data to the client as proof.

Planning the Retest

- A retest is to analyze progress made in applying the mitigations to the attack vectors that were found during the PenTest.
  - Schedule additional tests with the client to assess their progress
  - Provide a window of time for them to fix the issues.
- Focus on researching vulnerabilities that the team could not recommend a mitigation tactic
  - Inform them when/if a tactic is eventually found
  - Research and test new vulnerabilities that were discovered during the test.

Reviewing Lessons Learned

- An important part of any project is to identify lessons learned
- The primary goal of drafting a lessons learned report (LLR), or after-action report (AAR) is to improve your PenTest processes and tools.
  - Failing to learn from the experience can lead to repeating the same mistakes
- When you draft an LLR, include questions about the PenTest:
  - What about the test went well? What didn't go well?
  - What new vulnerabilities, exploits, etc., did the team learn about?

Review Activity: Follow-Up Actions

- Discuss the importance of post delivery activities
- Review the process of confirming that testing is complete
- Explain the significance of attestation of findings
- Outline why the team should schedule a retest
- Describe the significance of creating a learned report (LLR)

Lesson 20

Summary