Post-Engagement

Go to Questions

Table of Contents

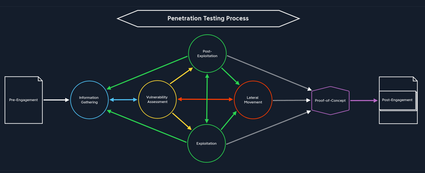
My Workstation

OFFLINE

Start Instance

1 / 1 spawns left

Much like there is considerable legwork before an engagement officially starts (when testing begins), we must perform many activities (many of them contractually binding) after our scans, exploitation, lateral movement, and post-exploitation activities are complete. No two engagements are the same, so these activities may differ slightly but generally must be performed to close out an engagement fully.



Cleanup

Once testing is complete, we should perform any necessary cleanup, such as deleting tools/scripts uploaded to target systems, reverting any (minor) configuration changes we may have made, etc. We should have detailed notes of all of our activities, making any cleanup activities easy and efficient. If we cannot access a system where an artifact needs to be deleted, or another change reverted, we should alert the client and list these issues in the report appendices. Even if we can remove any uploaded files and revert changes (such as adding a local admin account), we should document these changes in our report appendices in case the client receives alerts that they need to follow up on and confirm that the activity in question was part of our sanctioned testing.

Documentation and Reporting

Before completing the assessment and disconnecting from the client's internal network or sending "stop" notification emails to signal the end of testing (meaning no more interaction with the client's hosts), we must make sure to have adequate documentation for all findings that we plan to include in our report. This includes command output, screenshots, a listing of affected hosts, and anything else specific to the client environment or finding. We should also make sure that we have retrieved all scan and log output if the client hosted a VM in their infrastructure for an internal penetration test and any other data that may be included as part of the report or as supplementary documentation. We should not keep any Personal Identifiable Information (PII), potentially incriminating info, or other sensitive data we came across throughout testing.

We should already have a detailed list of the findings we will include in the report and all necessary details to tailor the findings to the client's environment. Our report deliverable (which is covered in detail in the Documentation & Reporting module) should consist of the following:

- An attack chain (in the event of full internal compromise or external to internal access) detailing steps taken to achieve compromise
- A strong executive summary that a non-technical audience can understand
- Detailed findings specific to the client's environment that include a risk rating, finding impact, remediation recommendations, and high-quality external references related to the issue
- Adequate steps to reproduce each finding so the team responsible for remediation can understand and test the issue while putting fixes in place
- Near, medium, and long-term recommendations specific to the environment
- Appendices which include information such as the target scope, OSINT data (if relevant to the engagement), password cracking analysis (if relevant), discovered ports/services, compromised hosts, compromised accounts, files transferred to client-owned systems, any account creation/system modifications, an Active Directory security analysis (if relevant), relevant scan data/supplementary documentation, and any other information necessary to explain a specific finding or recommendation further

At this stage, we will create a draft report that is the first deliverable our client will receive. From here, they will be able to comment on the report and ask for any necessary clarification/modifications.

Report Review Meeting

Once the draft report is delivered, and the client has had a chance to distribute it internally and review it in-depth, it is customary to hold a report review meeting to walk through the assessment results. The report review meeting typically includes the same folks from the client and the firm performing the assessment. Depending on the types of findings, the client may bring in additional technical subject matter experts if the finding is related to a system or application they are responsible for. Typically we will not read the entire report word for word but walk through each finding briefly and give an explanation from our own perspective/experience. The client will have the opportunity to ask questions about anything in the report, ask for clarifications, or point out issues that need to be corrected. Often the client will come with a list of questions about specific findings and will not want to cover every finding in detail (such as low-risk ones).

Deliverable Acceptance

The Scope of Work should clearly define the acceptance of any project deliverables. In penetration test assessments, generally, we deliver a report marked `DRAFT` and give the client a chance to review and comment. Once the client has submitted feedback (i.e., management responses, requests for clarification/changes, additional evidence, etc.) either by email or (ideally) during a report review meeting, we can issue them a new version of the report marked `FINAL`. Some audit firms that clients may be beholden to will not accept a penetration test report with a `DRAFT` designation. Other companies will not care, but keeping a uniform approach across all customers is best.

Post-Remediation Testing

Most engagements include post-remediation testing as part of the project's total cost. In this phase, we will review any documentation provided by the client showing evidence of remediation or just a list of remediated findings. We will need to reaccess the target environment and test each issue to ensure it was appropriately remediated. We will issue a post-remediation report that clearly shows the state of the environment before and after post-remediation testing. For example, we may include a table such as:

#	Finding Severity	Finding Title	Status
1	High	SQL Injection	Remediated
2	High	Broken Authentication	Remediated
3	High	Unrestricted File Upload	Remediated
4	High	Inadequate Web and Egress Filtering	Not Remediated
5	Medium	SMB Signing Not Enabled	Not Remediated
6	Low	Directory Listing Enabled	Not Remediated

For each finding (where possible), we will want to show evidence that the issue is no longer present in the environment through scan output or proof that the original exploitation techniques fail.

Role of the Pentester in Remediation

Since a penetration test is essentially an audit, we must remain impartial third parties and not perform remediation on our findings (such as fixing code, patching systems, or making configuration changes in Active Directory). We must maintain a degree of independence and can serve as trusted advisors by giving general remediation advice on how a specific issue could be fixed or be available to explain further/demonstrate a finding so the team assigned to remediate it has a better understanding. We should not be implementing changes ourselves or even giving precise remediation advice (i.e., for SQL Injection, we may say "sanitize user input" but not give the client a rewritten piece of code). This will help maintain the assessment's integrity and not introduce any potential conflict of interest into the process.

Data Retention

After a penetration test concludes, we will have a considerable amount of client-specific data such as scan results, log output, credentials, screenshots, and more. Data retention and destruction requirements may differ from country to country and firm to firm, and procedures surrounding each should be outlined clearly in the contract language of the Scope of Work and the Rules of Engagement. Per Penetration Testing Guidance from the PCI Data Security Standard (PCI DSS):

> "While there are currently no PCI DSS requirements regarding the retention of evidence collected by the penetration tester, it is a recommended best practice that the tester retain such evidence (whether internal to the organization or a third-party provider) for a period of time while considering any local, regional, or company laws that must be followed for the retention of evidence. This evidence should be available upon request from the target entity or other authorized entities as defined in the rules of engagement."

We should retain evidence for some time after the penetration test in case questions arise about specific findings or to assist with retesting "closed" findings after the client has performed remediation activities. Any data retained after the assessment should be stored in a secure location owned and controlled by the firm and encrypted at rest. All data should be wiped from tester systems at the conclusion of an assessment. A new virtual machine specific to the client in question should be created for any post-remediation testing or investigation of findings related to client inquiries.

Close Out

Once we have delivered the final report, assisted the client with questions regarding remediation, and performed post-remediation testing/issued a new report, we can finally close the project. At this stage, we should ensure that any systems used to connect to the client's systems or process data have been wiped or destroyed and that any artifacts leftover from the engagement are stored securely (encrypted) per our firm's policy and per contractual obligations to our client. The final steps would be invoicing the client and collecting payment for services rendered. Finally, it is always good to follow up with a post-assessment client satisfaction survey so the team and management, in particular, can see what went well during the engagement and what could be improved upon from a company process standpoint and the individual consultant assigned to the project. Discussions for follow-on work may arise in the weeks or months after if the client was pleased with our work and day-to-day interactions.

As we continually grow our technical skillset, we should always look for ways to improve our soft skills and become more well-rounded professional consultants. In the end, the `client will usually remember interactions` during the assessment, communication, and how they were treated/valued by the firm they engage, `not the fancy exploit chain the pentester pulled off to pwn their systems`. Take this time to self-reflect and work on continuous improvement in all aspects of your role as a professional penetration tester.

Questions

Answer the question(s) below to complete this Section and earn cubes!

+2 What designation do we typically give a report when it is first delivered to a client for a chance to review and comment? (One word)

Submit your answer here...

Submit