PLEXTRAC EBOOK

Hack Your Pentesting Routine

10 phases for creating a seamless pentesting experience for pentesters *and* stakeholders

PlexTrac®

Table of Contents

Introduction

Penetration testing has finally hit its groove. More businesses and organizations than ever recognize the need for cybersecurity in general and pentesting in particular. As cybercrime climbs and insurance costs have risen in reaction, cybersecurity has rapidly evolved from an indulgence to a necessity.

In response to increased demand, the cybersecurity industry has grown in scope and efficiency, creating routines and standards that providers and internal teams use to deliver a high level of service to their clients and stakeholders. When it comes to pentesting, most security firms (independent and in-house) use a standard set of work phases to guide the process of a pentest engagement. Oftentimes, these phases can be labeled as

- **Discovery**
- **Enumeration**
- **Analysis**
- **Exploitation**
- **Post-Exploitation**

When clearly defined and followed, these phases provide all members of the engagement — leadership, operators, pentesters, sales team, and stakeholder/ client — with a roadmap of how the pentest will progress, set the stakeholder's expectations, and establish an understanding of how and when the pentest will be successfully completed.

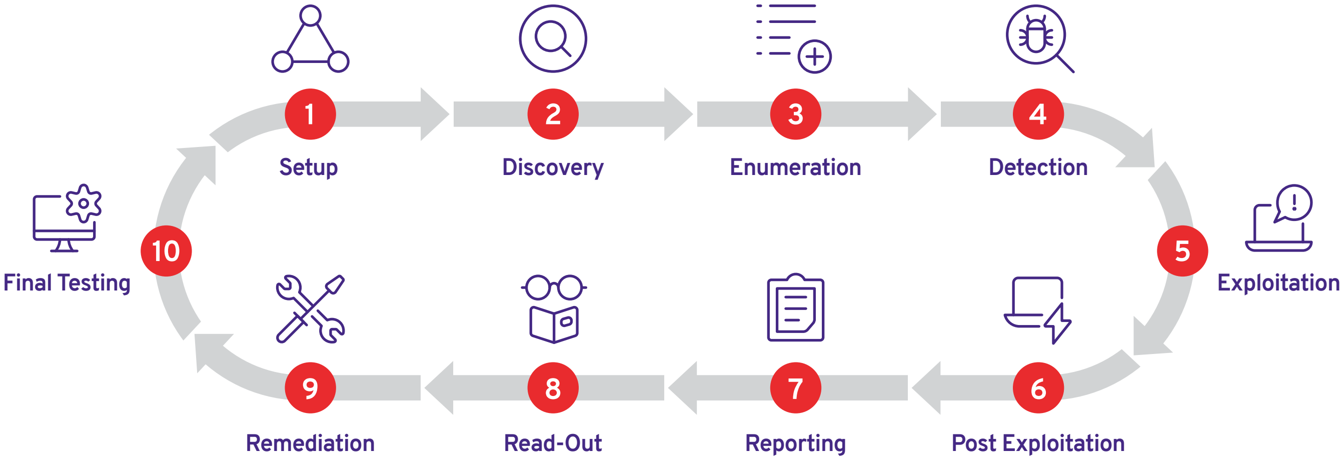
But do these phases really cover every critical activity involved in testing or do these overly simplify the process causing missed steps in managing both the pentest and the deliverables?

Mapping Out a Better Pentest Experience

While this system of pentesting covers most of the major steps of a standard pentest, it neglects a crucial aspect of the engagement: relations with the primary stakeholder or recipient of the testing results.

The stakeholder is the customer organization or internal personnel who will receive the information uncovered by the testing and need to use it to improve their organization's security posture. While not directly involved in the execution of the pentest, the stakeholder still plays a crucial role in the overall engagement. The stakeholder determines the extent of the pentest, the overall goals of the engagement, the time frame, the budget, and what actions should be taken after the pentesters submit their report.

With this and other possible shortcomings in mind, we suggest that there might be a better way to plan out a pentest engagement: **The 10-Phase Approach.**



1. **Setup:** The start of project management for the pentest, this is where all involved parties decide how the pentest should be conducted, who is in charge of what, and when the pentest should be considered complete.

2. **Discovery:** Standard information gathering and scanning, identifying the targeted network's ports and services.

3. **Enumeration:** Identifying active IP addresses, user accounts, and vulnerable connections, ports, and other points of access that provide an all-encompassing picture of the testing target.

4. **Detection:** Verifying the services and applications associated with the ports during the Enumeration phase.

5. **Exploitation:** Using the information from phases 2, 3, and 4 to gain access and/or control of the target's systems, networks, and/or devices.

6. **Post-Exploitation:** Determining the value of the exploited asset, and using that asset to uncover ways to elevate access.

7. **Reporting:** Compiling the pentest findings and results into a report that is easy for the stakeholder to understand and take action on.

8. **Readout:** Reviewing the pentest report with the stakeholder, which encourages dialogue and questions between all parties.

9. **Remediation:** Fixing — or letting the stakeholder's internal team fix — the flaws and vulnerabilities identified during the pentest.

10. **Final Testing (or Retesting):** Determining if the remediation was successful by retesting on reported issues.

The 10-Phase Approach provides a seamless, logical, and appropriately detailed method for the entire pentesting process. Although some of these steps might be implied in the standard, pentest-centered approach, making them independent phases ensures that no critical element of the process is neglected and that the communication necessary to make sure the stakeholder's security posture actually improves is prioritized. And while different types of pentesting might not use every phase in this approach explicitly, the principles behind each phase are worth noting and implementing.

Let's dive deeper into these 10 phases, and see how they can help your next pentesting engagement improve.

Phase 1: Setup

The Setup Phase enables the pentesting team to lay the foundation of the engagement. And just like the foundation of a building, if there are weaknesses or if corners are cut at this stage, then the risk of the entire engagement being a failure increases dramatically. Without a proper setup, without clear guidelines and expectations, the entire pentesting process can be easily misdirected, not given the necessary support, or it may fail to provide any valuable information.

Without a proper setup, without clear guidelines and expectations, the entire pentesting process can be easily misdirected, not given the necessary support, or it may fail to provide any valuable information.

This phase includes everyone involved in the engagement — sales, operations, pentesters, and stakeholder — and provides some foundational expectation setting, answering such questions as

- What is the purpose of this pentest?
- Who are all of the team members, and what will their function be?
- What actions will be taken during the pentest?
- What criteria will be used to judge the success of the engagement?
- What is the required deliverable, and what will it look like?

Every member of the team must focus on clear and timely communication at this stage in order to get all of the crucial details established and thoroughly documented. And at this stage, there will be a large amount of documentation, such as the non-disclosure agreement, master service agreement or statement of work, client information, scope of work, rules of engagement, policies, procedures, and other critical items.

At this phase, operations will also determine the reporting standards and template for the stakeholder. With some practices and MSSPs having a dozen or more templates available, it best serves all parties to determine the template at this early stage; this way, the pentester won't have to scramble for details later on in the engagement and will know exactly what information should be recorded and how it should be formatted. Internal pentesting teams might not have a formal reporting standard but should still communicate clearly on what evidence will be tracked and how it will be documented to ensure testing results are valuable and actionable.

Due to the nature of the Setup Phase, it will require a large number of meetings and emails: internal, external, pre-kickoff, kickoff, updates, and meetings with and without the stakeholder. The large amount of information exchanged at this stage requires each member to have an established method of documenting and storing this information. In order to ensure that no information is lost, every party member should ideally have access to a shared platform where this information can be stored, accessed, and organized.

Phase 2: Discovery

The Discovery Phase involves information gathering and scanning, identifying network ports and services, and the rest of the preliminary research and testing that enables the pentesting team to get the best perspective for the upcoming attack. In this phase, the pentest team begins to throw packets at their targets, and it constitutes the start of the actual engagement.

The initial findings of the Discovery Phase reveal another reason why the Setup Phase is so crucial. The Discovery Phase provides the information needed to fully define the scope of the engagement, determining how much time, resources, personnel, and tools are necessary to meet the expectations established in the Setup Phase. If data uncovered during the Discovery Phase leads to a need to change the scope of work or the rules of engagement, then the documents and lines of communication and collaboration defined in the Setup Phase should make implementing these changes quick and easy.

The operations side of the engagement should use the Discovery Phase to secure all of the resources they need as soon as possible. By referring to the expectations of the Setup Phase, and adjusting these during the Discovery Phase, the team can ensure that they get all of the resources they need for the entire engagement as soon as possible, which will avert any last-minute scrambles for resources and administrative headaches.

The Discovery Phase provides the information needed to fully define the scope of the engagement.

Phase 3: Enumeration

The Enumeration Phase involves the pentesting team identifying active IP addresses, user accounts, vulnerable connections, ports, and other points of access that provide an all-encompassing picture of the testing target.

This phase may feel very straightforward, but that doesn't mean that it is simple or easy. Pentesting teams can and should rely on automated tools to work through a target with a wide scope or a large number of assets. However, these automated tools cannot be relied upon to be completely accurate. The Enumeration Phase requires a very human touch — the experienced eye of a pentester who knows the difference between what vulnerabilities, assets, and hurdles that their tool may see and what is really there.

The Enumeration Phase requires a very human touch — the experienced eye of a pentester.

The Enumeration Phase also requires a delicate touch when applying these tools. Unleashing NMAP or Nessus and flooding targets with packets will not yield the number or quality of results that a pentesting team needs and could cause the source IP to shut down just as the team begins its work. This phase requires experienced and subtle handling if the team hopes to move into the Detection Phase with a solid foundation of reliable and thorough information.

Phase 4: Detection

In the Detection Phase, the pentesting team verifies the services and applications associated with the ports identified during the Enumeration Phase, identifies protocols and applications, and discovers vulnerabilities and other information that can move the team along the attack chain.

This phase, on the surface, can be confusing due to the way that firewalls can affect the responses, latency can alter results, and services running on non-traditional ports can trip up the detection process.

Also, this phase can be hampered if the pentesting team is working remotely; residential internet services are frequently filtered by ISPs, so if team members are working from home, their efforts may be impeded. During the Detection Phase, pentesters must be able to approach the target from multiple directions, using tools hosted in different environments, and even changing geographical locations, in order to get a complete and accurate picture of the target environment.

The rules of engagement established in the Setup Phase will be crucial during the Detection Phase. Many an ambitious or inexperienced pentester have dived into detection, unwittingly unleashed an automated tool on off-limit assets and brought the whole thing crashing down. Make sure that the entire team has reviewed the rules of engagement and scope of work before starting the Detection Phase to increase the chances of avoiding major gaffes.

The rules of engagement established in the Setup Phase will be crucial during the Detection Phase.

Phase 5: Exploitation

The Exploitation Phase provides the initial vector into the targeted networks or applications. As with the Detection Phase, a review of the rules of engagement before diving in will help the operations team stay clear of any off-limits assets and ensure the uptime of the production assets under examination. Any exploitation is invasive and can potentially impact the system or application, so this review is crucial.

Throughout the engagement, proper documentation is critical, but it is especially so during the Exploitation Phase.

This phase is the first where the pentesting team is on the network or inside the application or where they have completed the first successful social engineering step. The pentesting team will identify weaknesses in the applications or protocols, which will hopefully provide further access or additional useful information.

Throughout the engagement, proper documentation is critical, but it is especially so during the Exploitation Phase. If the pentesting team comes to the stakeholder during the Reporting Phase with a simple list of items that were "exploitable," the report will be unconvincing and unhelpful. Instead, the team should include documentation of the process, the specific weaknesses uncovered, the results of the exploitation, and (if possible) evidence that the exploit occurred. With this level of detail, the pentesting team will be able to justify the actions they took and the stakeholder will have a well-written guide to addressing the most significant weaknesses in the targeted asset.

Phase 6: Post-Exploitation

The Post-Exploitation Phase is all about escalation, where attacks move from one persona and perspective to another, probing further into the targeted asset, looking for better credentials, different views of the network and different ways to move deeper within the system.

Circling back to the Setup Phase, it is ideal to include as many post-exploitation activities as possible in the engagement's statement of work. Without sufficient post-exploitation, an engagement can end up being little more than a validated vulnerability scan, which will only give the stakeholder surface-level information. The Post-Exploitation Phase is (hopefully) the closest that the stakeholder will come to being completely hacked, and the information gleaned in this phase can be extremely valuable.

Because of the invasive nature of the Post-Exploitation Phase, stakeholders may feel uneasy about including many of these activities in the statement of work. Stakeholders who have had penetration tests performed on their systems or applications may have been burned in the past by pentesters being too ambitious and damaging the tested targets. This situation can easily occur if the testers are inattentive or reckless or if the targets are particularly fragile. In this case, well-written rules of engagement can benefit both stakeholder and pentester — they keep the pentester in line, while reassuring the stakeholder that the target will not be significantly damaged. The rules of engagement can include limits such as untouchable systems, no denial of service attacks, no system reboots, no brute forcing of web email submission forms, and others.

The Post-Exploitation Phase is (hopefully) the closest that the stakeholder will come to being completely hacked, and the information gleaned in this phase can be extremely valuable.

A well-written statement of work also helps by providing the criteria to determine when the Post-Exploitation Phase is over. A pentest can, in theory, keep going for as long as the participants have the time, money, and endurance to spare. A clearly stated goal, whether that is a set of assets or a collection of information, will let the pentester know exactly when to stop.

Another hassle faced by pentesters in this phase is the huge amount of information to collect. Due to the invasive nature of this phase, a complete log must be kept of all changes made to the systems as pentesters exploit them, capture credentials, and plunder file shares and databases. Since some exploits leave remnants behind them, a thorough log (including files, screenshots, and file samples) can be invaluable to the stakeholder when these remnants are uncovered long after the initial engagement.

Phase 7: Reporting

The Reporting Phase involves the pentesting team creating and presenting the stakeholder with the results of the multi-stage pentest. It is up to the pentesting team to take the mountain of information gleaned during the pentest, and present it in a cohesive, actionable format.

At this stage, access and communication are critical — the stakeholder must be able to view all of the vital findings (and the supporting evidence), and understand what is being presented to them. The stakeholder may or may not be able to fully understand the findings within the report; the responsibility rests with the pentesters and other people involved in writing the report to make the findings, and the recommended remediations, as clear as possible.

Your reporting methodology demands just as much attention as your technical execution — they are equally crucial.

Your reporting methodology demands just as much attention as your technical execution — they are equally crucial. A pentester is really only as good as their last report. After spending significant time performing technical wizardry and discovering valuable information that will benefit their stakeholders, many pentesting organizations still fail to provide reports that offer any beneficial insights. Relying on manually pulling in disparate data sets, copy and pasting, and working with the sheer volume that can be relevant to reporting means that your reporting strategy needs to be as professionally polished, and as well-aligned with stakeholder goals, as your hacking abilities. Implementing a system of record — one that enables collaboration, curation, and reporting — can elevate a pentesting team's work and the stakeholder's overall satisfaction.

PlexTrac enables pentesters and stakeholders to be able to work with findings, track remediation status, make notes, add evidence, gather metrics, combine outputs, and rapidly generate report documentation. PlexTrac was built so that reporting, one of the most important phases of the pentest, actually leads to a better security posture and gives stakeholders a better understanding of the risks revealed.

Phase 8: Readout

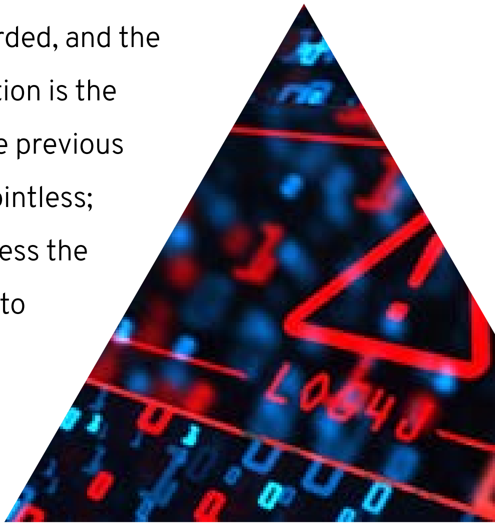
During the Readout Phase, the assessors will present the report and work through it, and the stakeholder will have an opportunity to discuss and ask questions.

The Readout Phase provides the stakeholder with an opportunity to give feedback. If the pentest is not a regulatory pentest (where the stakeholder has to take action on the findings of the report), the stakeholder has the option to come back after reviewing the report with issues about the severity levels assigned to weaknesses, or even about the validity of the findings. In this case, the pentesters can return to the report, modify the report as necessary, and submit it for another readout. The ultimate goal of this phase is to refine a report that will satisfy and sufficiently engage the stakeholder so that they will be ready to move on to the Remediation Phase.

When pentesting teams give stakeholders the chance to interact with the report after the initial assessment is complete, the Readout Phase becomes a collaborative process that ultimately benefits all parties .

When pentesting teams give stakeholders the chance to interact with the report after the initial assessment is complete, the Readout Phase becomes a collaborative process that ultimately benefits all parties – the pentesting and operations teams are able to refine their testing and reporting methods for future use, and the stakeholder is given a more thorough understanding of their own systems and the magnitude of the assessment.

Phase 9: Remediation



The Remediation Phase, when the stakeholder addresses the vulnerabilities revealed in the Reporting and Readout Phases, is where all of the hard work of the pentest is rewarded, and the stakeholder implements the action plan to elevate their security posture. Remediation is the primary purpose of any pentest, red team operation, or vulnerability scan. While the previous phases all have their use, without the Remediation Phase, they are all ultimately pointless; identifying vulnerabilities is important, of course, but unless action is taken to address the vulnerabilities or mitigate the risks, then all of the previous steps taken do nothing to help the stakeholder.

The handling of the Remediation Phase depends partially on the pentester's organizational structure. Internal teams and service providers have an advantage over consultancies as they are typically able to collaborate more closely with the remediation team. But however the pentesting team is placed, they must do all they can to ensure that the stakeholder is staged to act on the results of the Reporting and Readout Phases.

One of the most effective ways of ensuring stakeholder engagement in the Remediation Phase is to take particular care with the phrasing and presentation in the Reporting Phase. A good pentesting report will ensure that

- **The report is credible**, with plenty of proofs to back up vulnerability findings
- **The report articulates** and ranks vulnerability risks clearly
- **The report motivates** the stakeholder to take action by clearly stating what will happen if these vulnerabilities are exploited

If the report is sufficiently clear and persuasive, the stakeholder is far more likely to take action quickly and address the risks, which leads us to…

But however the pentesting team is placed, they must do all they can to ensure that the stakeholder is staged to act on the results of the Reporting and Readout Phases.

Phase 10: Final Testing

The Final Testing (or Retesting) Phase is where the pentesting team determines if the actions taken in the Remediation Phase were successful.

In a successfully run Final Testing Phase, retesting will determine that the highest priority weaknesses are fixed, the system is decommissioned, or the flaws are otherwise rendered unassailable or invisible to hackers. The targeted system or application will often need multiple rounds of reviewing to ensure that all weaknesses have been addressed and that any last-minute remediations do not create other weaknesses.

The Final Testing Phase usually ends up being slightly larger in scope than the original test, as the actions taken in the Remediation Phase might disturb the environment and create new vulnerabilities. Clear communication and expectations about this in the Setup Phase will help the stakeholder be prepared for a more invasive scan.

After successful Remediation and Final Testing Phases have been completed, the stakeholder's security posture should be significantly improved and all parties involved in the engagement will have a clear understanding of the stakeholder's future security needs. While it is impossible for any organization with online access to be entirely free of cybersecurity risk, a successful and complete pentesting engagement should give the stakeholder a better chance at keeping their systems safe and give them the tools to recognize weaknesses that may appear in the future.

The 10-Phase Path to Success

While going from a rough pentest-centric routine to the more refined 10-Phase routine might at first seem like adding more work for everyone, the 10-Phase plan ends up saving work and time for everyone involved. If it is implemented well and incorporated as a routine, every group involved in the engagement will save the time usually lost in chasing down resources, negotiating changes to the scope or rules of engagement in the middle of testing, performing unnecessary tests, and pursuing off-limit assets. Apart from time saved during the initial engagement, clear communication and set goals during the engagement lead to compounding efficiencies in the future: Uncovered flaws are successfully repaired in the Remediation and Retesting Phases, which leads to more efficient future pentest engagements and, hopefully, far fewer breach attempts as time goes on.

Committing to the 10-Phase routine will result in

- a better product for your client,
- generate a better reputation for the pentesting team (both for general effectiveness and for high-quality stakeholder service and communication),
- and provide proof that the operations team gives high-quality findings and an action plan that gives the stakeholder all of the tools they need to make their systems and applications more secure.

PlexTrac Every Step of the Way

In order to successfully execute the 10-Phase routine, all parties involved must focus on communication — laying out expectations, assignments, limits, routines, strategies, information, reports, suggestions, reactions, and more in a way that is clear and easy to access.

Fortunately, PlexTrac provides an ideal platform for all stages of the pentesting engagement, seamlessly bringing all involved parties together, streamlining communication, and compiling scattered testing results from a variety of sources into easy-to-read reporting templates. Pentesting teams can use PlexTrac to keep stakeholders informed of progress, track the progress of the various stages of pentesting, and keep their finger on the pulse of the entire engagement.

Interested in taking your team to an elevated level of efficiency and effectiveness with PlexTrac?

Click here to book your free demo today

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com

PlexTrac®