hackerone

Pre-Pentest Checklist: Essential Questions to Answer Before Your Next Pentest

Diving into pentest readiness, this checklist offers a structured overview to help you answer the what, why, when, who, and how of a successful pentest. This comprehensive preparation guide is adaptable to different types of pentests, regardless of the targets' size or complexity.

What?

- [ ] **What is the scope?** Include the assets you'd want tested, and remember to call out components or features you'd like to be considered as out-of-scope of the test.
- [ ] **What are your success criteria for the pentest?** Consider this question and ponder it internally with the stakeholders. Once you have reached an answer, share it with your pentest vendor so they're aligned to meet your goal.
- [ ] **What key areas would you want the pentester(s) to focus on?** This question may not apply to every customer or pentest. Still, if you recently made changes to the access control model of your web application, you'd want to call those out so the pentesters can prioritize accordingly.
- [ ] **What type of pentest would you like done?** Taking into consideration the asset types being tested, would you prefer to conduct an authenticated (gray-box) or unauthenticated (black-box) test? It is common to see a combination of authenticated and unauthenticated testing, depending on the use case and maturity of the assets in scope for testing.
- [ ] **What type of environment does the pentest need to be conducted on?** You'll want to decide whether to set up a non-production, QA, or test environment identical to production. Will a staging or a production environment be better suited for the type of testing that you'd like conducted?
- [ ] **What restrictions (if any) need to be applied?** Possible restrictions and requirements should be considered, especially the day and time of testing and any specialized skills necessary based on the asset type.
- [ ] **What credentials/certifications should the pentester(s) possess?** Considering compliance or due diligence efforts, specific credentials or certifications will ensure only the most qualified and professional pentesters touch your assets.
- [ ] **What type of deliverables do you need out of this pentest?** Common pentest deliverables include Penetration Test Report, Letter of Attestation, Executive Summary, and CSV format tracker of the number of identified vulnerabilities.
- [ ] **What are your internal timelines to fix Critical and High severity vulnerabilities?** Defining timelines in advance will help set expectations with the internal team and stakeholders, avoid delays, and ensure timely retesting requests are made to the pentesters.

Why?

- [ ] **Why do you need a pentest?** Organizations conduct penetration tests for various reasons. Some common reasons include:
  - Meet and demonstrate compliance with specific regulations, such as PCI DSS.
  - Ensure that any changes made to the product do not introduce new vulnerabilities.
  - Validate results from a vulnerability scanner.
- [ ] **Why is this the right time for a pentest in your security lifecycle?** The response to this question is closely linked with the purpose of the pentest. Some common times to conduct pentests are:
  - Before a major launch or update
  - After significant code changes
  - Following a security incident
  - Continuous improvement
- [ ] **Why have you chosen this particular scope for the pentest?** Scoping a pentest accurately is essential given the time-bound nature of the assessment. Additionally, it sheds a spotlight on the key areas that require the most attention. A few examples include:
  - Risk prioritization
  - Implementation of security controls
  - Phased approach to scoped assets

When?

- [ ] **When do you expect the pentest to kick off and conclude?** Defined timelines are crucial to meeting deadlines, especially when a pentest is part of a broader risk management strategy and impacts subsequent projects.
- [ ] **When do you need the final report?** On a similar note to the previous question, it is critical to inform the vendor as soon as possible of any deadlines to meet for the final report. It is standard to share the final report within a week of the pentest's conclusion.
- [ ] **When is the best time for your team to be involved in a pentest?** Pentests are time-bound; therefore, ensuring that all key and relevant team members are available, have time to dedicate to and promptly respond to any questions before launching and during the pentest.

hackerone

Who?

- [ ] **Who should be informed about the pentest?** It is advisable to inform your organization's defenders about an upcoming pentest to enable them to concentrate on actual threats rather than the traffic generated by an authorized pentest. Pentesting teams will commonly share the testing IP addresses so you can inform the appropriate individuals protecting your organization's infrastructure, such as your SOC teams.

- [ ] **Who will be the primary point of contact for the pentesting team?** Designating a person for this role can significantly improve the efficiency of the process and enhance collaboration throughout the pentest. They will be responsible for addressing pentester questions about the in-scope assets and how the different components interact. Furthermore, they can serve as a point of escalation for the pentesters in case a critical or high-severity vulnerability is discovered.

- [ ] **Who within your organization will be responsible for addressing the findings?** Identifying product owners and teams responsible for the asset being tested is crucial to address reported vulnerabilities during the pentest, especially the critical and high-severity ones requiring immediate attention.

How?

- [ ] **How will the vendor communicate with you before, during, and after the pentest?** Establishing open communication channels and promptly responding to any pentester questions is vital to a successful experience with your chosen pentest vendor. This could be as simple and efficient as creating Slack channels for quick chat among members involved in the pentest. This is the most effective form of communication with a pentesting team and how we connect pentesting teams with customers at HackerOne.

- [ ] **How will the pentesters access the in-scope assets?** It is critical that the pentesters can hit the ground running on day one of the pentest; hence, validating that they can successfully access the in-scope assets is crucial.

  - Are the assets Internet-facing or internal-only?
  - Will the mobile apps be available in their respective stores? Alternatively, will they be available via TestFlight or as a .apk file?
  - Do the pentesters need a VPN to connect and access the assets?
  - Do you need to add their IP address to an allow-list on your perimeter devices?
  - Will they need credentials to test? How will these be provisioned?

- [ ] **How will the final deliverables be shared with you?** It's critical to be very careful about how this occurs. You do not want to receive an unprotected PDF over email as the final report. Ensure that the report is securely shared with you. Vendors are known to share these:

  - Host it on their trusted pentest platform, which you can access and download.
  - Use a mutually agreed upon secure file-share platform.
  - A password-protected PDF is sent over email or other communication channels, where the password is shared out-of-band.

The Efficiency of HackerOne Pentest

HackerOne Pentest revolutionizes traditional pentesting via our Pentest as a service (PTaaS) model. This PTaaS approach provides a comprehensive scoping form guiding you to launch pentests faster than ever, seamless communication between all parties involved, and comprehensive reporting with easy-to-follow remediation steps and demonstrated compliance.

Customers simplify their pentest process with HackerOne, combining operational efficiency with unmatched support by expert Technical Engagement Managers (TEMs) to enhance testing experience in each and every security testing engagement.

Are you ready to take the next step? Share your pentesting requirements with us, and let our experts tailor a strategy that aligns with your security goals.