TRUSTEDSEC

How to Get the Most Out of Your Pentest

Published by: Luke Bremer

TL;DR

1. Define the goal of an assessment.
2. Take time to choose the right assessment type.
3. The more detail you give about an asset, the better quality your report will be.
4. Select the right environment for the assessment.
5. Consider the timing for performing the assessment.
6. Communicate internally and make sure everyone is up to speed.
7. Do more than remediate findings—use findings to help remediate other areas of an environment.
8. Fix low-severity issues.
9. Ask questions and get feedback.
10. Make sure to change things up once and a while.
11. These are all just suggestions; do as you please.

There are many types of penetration tests and security assessments. Although most of the suggestions below apply to a variety of tests, I am focusing specifically on the following: External and Internal Penetration Tests, and Black-Box, White-Box, Grey-Box, and Hybrid (Source-Assisted Grey-Box) Application Assessments.

Define Goals:

It is important to know why an assessment is being performed. Is it required to pass an audit? Do new features or functionality need to be reviewed? Maybe assessments are part of an overall security posture and are being used to measure improvement. Knowing the goals for an assessment will help you gauge whether a test was successful and help the penetration tester know where to focus efforts.

Choose the right type of assessment:

Once you understand the goals of an assessment, you will be able to select the type of assessment needed to achieve those goals. Sometimes, multiple assessments are needed to cover all sections of a network or application. Based on the budget and type of asset being assessed, you can narrow options down to a few types of assessments.

If you are still unsure which assessment to select, make sure each assessment can achieve the desired goals and base the decision on the differences between each assessment. For each difference, you should be able to perform a cost-benefit analysis to determine the best overall choice. Keep in mind that an assessment that is a good fit for one asset might not be the same for another. Each assessment will be different, and taking time to select the best assessment type can prove beneficial down the road. Of course, if a decision is still not obvious, there is usually an account manager that can make some recommendations.

Give more detail to get the most out of a report:

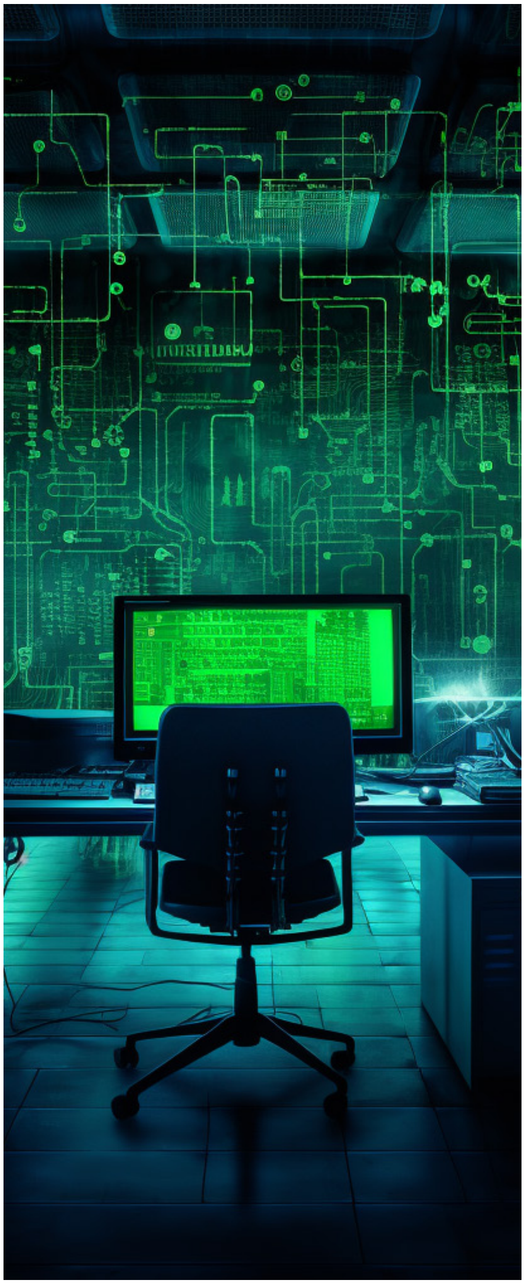
In most cases, each type of assessment comes with its own set of pre-defined rules, including a time constraint. The more information you can provide to a penetration tester about an asset, the more time can be spent finding security issues. This information can include user documents, application demonstrations, network diagrams, source code, keywords used to return data, or lists of technologies in use—all of these can help speed up the reconnaissance phase of an assessment. It could take a large team years to create a network infrastructure or a single application, so any insight you can provide to a tester, who could be reviewing your assets for the first time, can help make the most of the time allotted. This mainly applies to authenticated assessments and would not apply (in most cases) to a Black-Box Application Assessment or External Penetration Test, as these tests intend to find existing issues without inside information.

Select the right environment for testing:

Most mature development programs will have multiple environments set up for use during the life cycle of an application. At a minimum, most development teams will likely have a development environment and a production environment. The environment in which an assessment is performed can have a large impact on the results of the assessment. If an assessment is performed in a development environment that does not contain data or infrastructure close to production, then the results of the assessment might not be a true reflection of the security in the production environment. For this reason, a company may choose to have an assessment performed in a production environment, but this can limit testing some attack vectors that could affect real-world assets. Account lockouts, Denial of Service (DoS), heavy network traffic caused by fuzz lists, or forced browsing can cause issues for users in a production environment and could mean a loss in revenue for some companies.

One of the most effective ways to ensure that most attack paths can be performed during an assessment is to have a testing environment that mirrors the production environment. This can also ensure that assessment results are an accurate representation of the security in the production environment. Having the same production data in a testing environment can cause issues if production data contains sensitive information, such as Personally Identifiable Information (PII), PHI or PCI data. In these cases, masking or anonymizing data can help remove any sensitive data while ensuring the data's structure remains the same.

Added shortcuts to bypass functionality are also common in a testing environment. Functions such as impersonation, Multi-Factor Authentication (MFA) bypass, disabled logging, enabled verbose errors, self-signed certificates, and a checkout process that does not include full functionality can all be in place for convenience or to minimize resource expenditure. Although these shortcuts can greatly increase testing productivity, the production functionality is unlikely to be fully assessed if these shortcuts are in place during an assessment. An assessment environment with all the functionality of a production environment can allow better coverage during an assessment.



Consider the timing for the assessment:

It can be common for an assessment to take place a few weeks before an application goes live to users or during the middle of development. Although it is a good idea to check the security of an application during each stage of the development process, performing an assessment when features of a network or application are incomplete may not provide a true representation of the security of that asset. An assessment is a point-in-time evaluation. This means that only security issues that are present at the time of testing can be identified. If an assessment is performed before all features of that asset are fully developed, then there is a possibility that changes to the environment after the assessment can introduce new security issues that would not be identified. To increase the accuracy of the assessment results, schedule assessments to be performed after all features of an asset are complete and after internal testing has been performed.

If a testing environment is available and all features are complete, do not wait until the last minute to schedule an assessment. Compliance commonly requires a yearly assessment, and companies often wait until the last few months of the year to perform that assessment. Keep in mind that if you have several yearly assessments that need to be performed, so do other organizations. If an assessment is required before the end of the year, take a proactive approach and schedule it as soon as you can. If you wait until the last few months of the year, you may have trouble finding a respected security firm that still has availability. Due to the increased number of requests security companies receive at the end of the year, assessments may increase in cost or need to be scheduled after the end of the year, depending on consultant availability.

It can be difficult to calculate how much time to allow to make security patches after an assessment. Anyone who has worked on a development team or been part of an application release will know that projects rarely finish ahead of deadline. Of course, you may have some amazing project managers that have been around the block, but security is often added after the fact and is less likely to be part of the development process. If an application is being assessed for the first time, it will likely have security issues. For each issue discovered, an internal ticket may need to be created for tracking, and time will need to be allocated to implement and test a security patch. Depending on the issues found, patches can take days or weeks to implement, and a deadline or an application release may be delayed if time is not allocated to patch security issues.

Also, account for remediation times when scheduling a retest or additional assessments. If an assessment is scheduled too close to a previous assessment, internal teams might not have enough time to remediate the identified findings from the previous report. This can lead to extra costs and duplicated reports, which can cause a form of alert fatigue for the remediation team.

Communicate internally:

An assessment can have a lot of moving parts, and preparing can take a decent amount of time and resources. Open communication between management, the development team, third-party contractors, and the security team can help ensure an assessment achieves its goal. Is an environment still in active development? Are patches only applied to a specific environment? Do credentials need to be created? Do firewall rules need to be updated? Do we have the authority to authorize an assessment against this asset? Documenting lessons learned after an assessment can save time and resources internally for the future and can ensure the assessment has all the prerequisite conditions necessary to succeed. If needed, some security firms may even offer a project manager to help with the steps that need to be completed before an assessment; depending on the cost of the service, this can be of great benefit for new security programs.

Get the most out of each finding:

Typically, an assessment will contain a finding for each type of security issue discovered. As an example, a network segment may have many IPs that have the same port open, allowing anonymous access, or an application may have several instances of Cross Site Scripting (XSS). The details of a finding should help remediate that specific security issue—but what if the same issue exists in another application that was not assessed, or an endpoint was missed? Findings can be used not only to fix the specific security issue but also to identify a starting point to investigate the same issues in other sections of the application or network. If you have a security issue on one page of the application, do you also have the same issue on other pages? If you have a misconfiguration in one section of a network, is that same misconfiguration in another section as well? Arguably that is part of the penetration tester's task: to identify all the issues of an asset. There can be situations where a tester does not have access to a section of the application, or an IP range was out of scope during testing. Maybe the assessment was time-based or a sampling of the total assets was used. It may be beneficial to look closely at the assessment findings and perform some internal testing to confirm that the identified issues do not exist in areas of your network or source code that have not been assessed. Identifying the root cause of repeated findings can also help reduce remediation times in the future. Adding a list of allowed third-party libraries or providing developer training for consistency can help reduce common findings that may be shared between reports.

As part of the remediation process, it can also be beneficial to look back at logs related to recent patches. Once a patch has remediated an issue, that issue should be fixed from that point in time forward—but what about the past? How long has that issue been present, and was it found and exploited before it was identified? A detailed assessment report should give context on how to identify a vulnerability and, in some cases, can include indicators of compromise. Information about how a security issue was exploited can be used to search historical records for patterns of similar activity, which could help uncover an insertion point into your network that might not have been apparent.

Consider fixing low-severity issues:

It can be common to have an extended period between identifying and patching a security issue. For lower severity findings, remediation times are often extended further. Often, a yearly assessment will contain some of the same findings as the previous year's assessment, especially for low-severity issues.

Some of these low-severity issues can help an attacker find more severe issues that could be present. An issue could also become more serious in the future as changes are made to an asset. Verbose or default errors can reveal an internal file path or the software versions in use. Response headers can be used to reveal the security protections in place and the software in use. An attacker can find a security issue much faster if the operating system in use is known. Additionally, not knowing what programming languages or software versions are being used can significantly slow down an attacker. The longer it takes an attacker to identify infrastructure and find a vulnerability, the more obvious the suspicious activity becomes.

Often, low-severity findings can be fixed quickly and easily. Adding a line to a configuration file may only take a few minutes. Assessing how long a remediation will take, even for low impact findings, can significantly increase your overall posture.

Get feedback:

The results from an assessment can be used in many ways to improve the security of an application or network. Asking pointed questions about the results can add additional benefit during remediation or future assessments. If the details of a finding are unclear, ask for clarification. Ask what you are doing right so that you can create a baseline and start there. If you are unsure of the best type of assessment for an asset, ask—a good security firm should be able to provide solid recommendations on the most beneficial assessments for your needs. If you have done a specific type of assessment for the past few years, it could be beneficial to reevaluate your goal for the assessment and confirm that the type of assessment you are doing still achieves that goal.

Repetition leads to complacency:

An assessment can be performed by an individual or possibly a small team of consultants who each have a separate knowledge base and set of skills. In teams, consultants often share knowledge between one another and work with one another's skill sets to achieve the best possible results from an assessment. When performing repeated or annual assessments, it can be beneficial to get different perspectives. That can mean changing the type of assessment or requesting changes to the team members performing the assessment.

Comparing results from separate individuals or groups can lead to findings that may have otherwise been missed. Consistency can be an asset in security, but paying extra attention to how an assessment is performed can ensure complete and relevant results. Not all security firms are created equal, and not all penetration testers have the same set of skills. Something that may be missed by one group can be identified by another, and vice versa.

Conclusion:

In the end, many factors can affect implementation of these suggestions. Budget, time, and resources commonly limit the ability to improve a company's security posture. The points listed here are not an exhaustive list—but in our experience, these actions can help develop a more robust security program and can help you get the most out of your next penetration test or security assessment.

TRUSTEDSEC

1.877.550.4728 • INFO@TRUSTEDSEC.COM

TRUSTEDSEC.COM

FORRESTER®
WAVE
LEADER 2024
Cybersecurity
Consulting Services

TrustedSec named
a Leader.