GUIDE

BISHOPFOX

20 TIPS

TO MAKE THE MOST OF YOUR PENETRATION TESTING

Introduction

Not All Pen Test are Created Equal.

Spending money on penetration tests is an investment in your product. And as a sizable investment in your product, you'll want to ensure you are getting your money's worth. However, there are a number of common pitfalls that can cost you in terms of quality, project delays, or unnecessary expense.

So whether you have conducted many pen tests or are about to contract your first, this list contains helpful guidance for companies at every stage of security program maturity.

01 CONDUCT YOUR OWN PRE-ASSESSMENT

02 KNOW YOUR ASSESSMENT GOALS

03 AIM FOR ACCURATE SCOPING SURVEYS

04 CONSIDER A MULTI-TIERED ASSESSMENT

05 DISABLE YOUR WAF

06 DISABLE RISK-BASED SESSION EXPIRATION

07 ENSURE A STABLE, RESPONSIBLE TEST ENVIRONMENT

08 FILL THE TEST ENVIRONMENT WITH DATA

09 ENSURE DEV TEAM AVAILABILITY DURING TESTING

10 CONFIRM ON-TIME PRE-ENGAGEMENTS

11 PROVIDE SOURCE CODE IF POSSIBLE

12 PROVIDE TEST SUITES AND DEV TOOLS

13 PROVIDE DEV AND CONSUMER DOCUMENTATION

14 TEST THE SECUIRTY, NOT THE OBSCURITY

15 ASSIGN A RESOURCE TO RESOLVE BLOCKERS

16 MAINTAIN OPEN COMMUNICATION WITH TESTERS

17 ESTABLISH AN ESCALATION PLAN FOR HIGH-RISK FINDINGS

18 SCHEDULE TESTS DURING THE SUMMER

19 USE PENETRATION TESTERS FOR PENETRATION TESTING

20 ASK QUESTIONS DURING THE REPORT WALK-THROUGH

20 Tips to Make the Most of Your Pen Test

01 CONDUCT YOUR OWN PRE-ASSESSMENT

If you have the staff, consider performing your own in-house assessment prior to contracting a penetration test or opening a bug bounty program. This will help eliminate the low-hanging fruit (i.e., bugs that are easily detected with automation and scanning).

This can be especially important with bug bounty programs because having to pay out for many easy-to-find bugs could cost more money in bounties than the allocation of a fulltime resource.

Eradicating these vulnerabilities in advance will allow you to rely on the professionals for the harder to find bugs.

02 KNOW YOUR ASSESSMENT GOALS

Determine specific goals and trophy targets. As with any project, clearly stating goals for the assessment ahead of time helps keep everyone on track and allows the team to prioritize vulnerabilities surrounding your greatest concerns.

Put Yourself in Their Shoes

If you are a product company, unauthorized access to schematics/design documents, unreleased marketing material, or any other information that could be at risk for corporate espionage might be the primary goal for the assessment team. While the team will still test other functionality and produce any other findings encountered, a primary goal will provide a clear focus for the penetration test.

03 AIM FOR ACCURATE SCOPING SURVEYS

It is important to describe the size and scope of the application as accurately as possible. Scoping teams will often provide a survey for your team to fill out to describe various aspects of the target(s) being assessed. It may take a little more time upfront, but it will also ensure that the project's assigned hours are accurate as well, thereby setting the project up for success from the start.

Overestimating (or over-scoping) poses fewer risks because your penetration test team can always dig deeper into any application or reallocate the hours for a different testing activity. Reporting an accurate (or even slightly overestimated scope) is the first step to ensuring project success.

OVER-SCOPING

When determining the line of code (LoC) count for a source code review, be sure to remove test cases from repositories before running automated tooling. Let's say you're running a tool like cloc **(https://github.com/AlDanial/cloc)** to provide a source code estimate. Although it will automatically subtract comments and blank lines, which is helpful, it cannot distinguish between test cases and product source code cases. This could mean that a result of 400k LoC could include 100k LoC of test cases, overestimating the source code count by 25%.

UNDER-SCOPING

If you have a web application and you guess that it had 50 endpoints when it in fact has 100, then the test will be under-scoped. Under-scoping may require a last-minute change order which could mean more hours, causing budget issues, project delays, or interference with other deadlines. Going ahead without a change order means you will end up with a more limited test than you planned.

04 CONSIDER A MULTI-TIERED ASSESSMENT

While it's common to test the outward-facing portion of your application, a multi-tiered assessment can help ensure strong detection and defense mechanisms after various levels of compromise and will lead to more robust application security. This form of assessment provides the assessment team with authenticated access to various levels of the underlying architecture directly, as opposed to requiring a code execution to be discovered.

WEB APPLICATION ASSESSMENTS

In a multi-tiered web application assessment, the team might assess the application as various user roles (as you would find in a standard assessment), but then they would also simulate the compromise of customer service users, an application server, or a back-end server.

These roles could be set up as the following:

- No access/public sign-in
- Application user roles (e.g., users, organization users, and administrators)
- Customer support user
- Command-line access to a primary web service
- Command-line access to a secondary back-end service

Attempting attacks from these privileged spaces allows the network monitoring team to become familiar with what malicious behavior looks like, and it allows security at the server level to be evaluated. For most organizations, security at this level is not formally evaluated until a break-in occurs or until privileged access is obtained during a penetration test.

05 DISABLE YOUR WAF DURING TESTING

Why should you disable your web application firewall (WAF) during a security test after spending all that money on it? It's the same reason a patient helps a doctor by pulling up their sleeve when looking for chicken pox. Disabling the WAF is the fastest and most time-effective way to diagnose issues in the underlying application. If you disable the WAF, it allows the team to focus on identifying flaws in your application, instead of flaws in third-party appliances. Don't give the WAF a free penetration test.

That said, if you're concerned about the efficacy of a WAF in relation to your application, coordinate with the team to re-enable the WAF toward the end of the assessment. That way, they can look for specific bypasses to determine when the WAF may be effective in stopping an attack.

Alternatively, consider having two test environments: one with defense-in-depth controls (e.g., a WAF) and one without. This allows the team to discover application vulnerabilities without spending excess time bypassing filters. In our experience, WAFs slow down attacks more than they prevent them.

06 DISABLE RISK- BASED SESSION EXPIRATION

Disable application features that may interfere with testing, such as session expiration associated with malicious payloads. While this feature may slow down attackers in production, it will also slow down your penetration testers and limit the number of tests performed per billable hour.

07 ENSURE A STABLE, RESPONSIVE TEST ENVIRONMENT

For the most effective penetration test, ensure that the test environment is just as responsive, complete, and stable as the production environment. To ensure stability, don't alter the test environment during a penetration test. If the environment is altered, it can result in missed findings due to downtime or false positives from in-progress bug fixes.

Downfalls of an Unstable Testing Environment

In worst-case scenarios at Bishop Fox, we've seen test environments with five to ten seconds of latency request. We've also had penetration tests conducted through screen control on WebEx. If a product has egress to WebEx servers, there are better solutions for a testing environment.

08 FILL THE TEST ENVIRONMENT WITH DATA

Do not provide an empty test environment. Fill it with test data to allow consultants to demonstrate authorization bypasses, such as gaining access to another user's files. Without this data, it will be more challenging to validate findings, and the final report may lack strong examples of business impact.

Some customers mirror production data to the test environment, while others fill it with QA data. If you like, you can add specific trophy files or data to the environment for us to focus on obtaining

09 ENSURE DEV TEAM AVAILABILITY DURING THE TEST

Lack of product team availability is a commonly overlooked risk to successful projects. Penetration tests often involve discussions with development or security team members to strategize solutions. When these team members aren't available, project delays can occur, and the assessment team can be limited in providing tailored remediation recommendations.

As a result, before scheduling a penetration test, confirm that your development, security, and any other essential team members have availability on their calendars and are not out of office.

10 CONFIRM ON-TIME PRE-ENGAGEMENTS

Most testing firms will provide a list of access requirements in advance that are necessary to test your application. To avoid wasting time, deliver pre-engagement requirements on time. Feel free to reach out to your consulting team and ask them to confirm access before testing is scheduled to begin to ensure an on-time start.

For instance, access requirements might entail provisioning multiple user roles for an application. However, there are multiple ways access might be incomplete. Perhaps the accounts were provisioned, but they were linked to an employee email account instead of a tester's email account. Or maybe the accounts were added, but the team can't test the application because the test environment gateway needs to whitelist the team's IP addresses. All of these issues can lead to delays or slow down a test, taking away valuable testing hours from a project. Bottom line: it's always good to confirm access prior to the start of testing.

11 IF POSSIBLE, PROVIDE SOURCE CODE

Source code is always better than no source code. Even if you are purchasing a black-box penetration test, providing source code allows the team to track down issues faster and identify more vulnerabilities. No penetration tester will reject source code.

12 PROVIDE TEST SUITES & DEV TOOLS

The more information you can share, the better. In addition to source code, provide any QA/dev tools (e.g., Postman collections, custom dev tools, and test data) that might allow the assessment team to more effectively interact with, compile, or test your application. This will also reduce the amount of time the consultants need to construct preliminary test cases.

13 PROVIDE DEV & CUSTOMER DOCUMENTATION

Provide any developer and customer-facing documentation or diagrams. Like onboarding a new developer, it reduces the time the consulting team requires to gain a baseline understanding of the application's architecture.

14 TEST THE SECURITY, NOT THE OBSCURITY

If your application relies on any obfuscation or anti-debugging, disable that obfuscation during the test, unless you want to focus on assessing the efficacy of the obfuscation instead.

These tactics are typically used to slow down an attacker, which, while valuable in an attack scenario, may incur an unnecessary cost when assessing your application's security.

15 ASSIGN A RESOURCE TO RESOLVE BLOCKERS

Remember, like lawyers, consulting firms track billable hours. Make the best use of the time you're paying for by assigning a resource from your team to resolve any blockers that might emerge, which will allow the assessment team to solve problems faster.

While some clients choose to provide consulting teams with an email distribution list to resolve issues, an assigned project manager can ensure a quick turnaround and use internal escalation paths to expedite resolutions, which is much more effective.

For example, if the assessment team is missing credentials, a delayed response could significantly affect the team's ability to test. For this reason, consider assigning a specific resource to unblock your consulting team and ensure information or access requests are fulfilled in a timely manner.

16 MAINTAIN OPEN COMMUNICATION WITH TESTERS

Consider creating a Slack channel (or any other instant messaging platform) with your development team where the assessment team can ask questions or request information. You might also have the resource assigned to blockers serve as a conduit to ensure your team is responding within a few hours.

17 ESTABLISH AN ESCALATION PLAN FOR HIGH-RISK FINDINGS

Have a plan in place for handling critical- and high-risk vulnerabilities. Ensure the relevant development teams are aware of this possibility so they can be prepared to triage any high-risk issues as they are reported. Keeping everyone in the loop and having your various teams prepared to push a new release will eliminate unforeseen chaos.

18 SCHEDULE TESTS DURING THE SUMMER

Many security teams find themselves rushing to spend unused budget dollars at the end of the year. As a result, consulting firms are busiest in November and December, so you might not get your penetration test on the calendar. Instead, test in the summer, which will afford you more testing flexibility, more diverse availability of resources, and more opportunities to extend timelines or schedule follow-up assessments.

19 USE PENETRATION TESTERS FOR PENETRATION TESTING

Consultants that specialize in penetration testing may be great at finding vulnerabilities in your application, but may not be skilled at delivering training on how to do secure development.

To ensure a successful assessment, scope the project correctly from the start so that you have the right resources to successfully complete each of the items described in the statement of work. Education may be something a consulting firm can offer, but it will need to be considered during the initial scope and may require different consultants; this also reduces project risk (e.g., causing delays due to staffing changes or additional costs).

20 ASK QUESTIONS DURING THE REPORT WALK-THROUGH

Here are Some Questions that May be Helpful to Ask:

1. After we remediate these findings, how will you feel about the security of this application?

2. Did you feel like you got a thorough view of the application? If not, what would you have wanted to test further?

3. What should we focus on for our next penetration test? What functionality or feature concerns you the most?

4. Are there any strategic design changes that you would recommend?

5. How can we have our QA team test for issues like ____________________________ to avoid them in the future?

6. Are there any automated tools that we should consider adding to our CI/CD pipeline?

7. We are considering migrating to the ____________________________ service/platform/framework. What things should we consider during this migration?

8. I noticed there weren't many (or any) findings on the ____________________________ feature. What were your observations during testing?

9. Did you have any blockers or delays during testing? If so, what can we do to reduce those in the future?

10. How can I stay up to date on security risks for ____________________________? Are there any projects, newsletters, or news sources that my team should consider monitoring?

About Bishop Fox

Bishop Fox is recognized as the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

Over the past 16 years, we've worked with more than 25% of the Fortune 100, 8 of the top 10 global tech companies, and hundreds of other organizations to improve their security. Our award-winning Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards and our offerings are consistently ranked as "world class" in customer experience surveys.

Security isn't just a job to us. We do this because we love it — and because we're committed to the common good. In fact, we have authored 15 open-source tools, shared groundbreaking research, and published more than 50 security advisories in the last 5 years.

Cosmos

Cosmos proactively defends dynamic attack surfaces by combining advanced technology, automation, and expert-driven testing to continuously identify and remediate high-risk exposures before attackers even know they exist.

Leveraging a proprietary asset discovery and exposure reconnaissance engine, Cosmos continuously discovers and maps your ever-changing attack surface and identifies dangerous vulnerabilities targeted by attackers.

Acting as an extension of your security team, our operators provide deep insights into findings, deliver real-time answers to pressing questions, and conduct on-demand retesting to validate remediation procedures and accelerate the closure of attack windows.

Consulting Services

Application Penetration Testing

Our award-winning, in-depth application penetration testing goes well beyond discovering vulnerabilities to analyze the inner workings of your applications and identify critical issues, exposure points, and business logic flaws.

External Penetration Testing

By nature, your internet facing services and systems are the most exposed and often attacked. Our external penetration testing services proactively identify security holes replicating the same methods and exploits that a real-world adversary would use to gain an initial foothold within your network.

Internal Penetration Testing

By simulating an attacker who has gained access to the internal network, we locate the most likely vulnerabilities, attack paths, and exploit chains an internal threat actor would leverage to gain access to sensitive data and critical systems.

CONNECT WITH US

Get started today.

Are you ready to start "defending forward"? Get in touch with our offensive security experts today to explore solutions that meet your unique business needs.

Request a Meeting

Explore Cosmos

8240 S. Kyrene Rd. • Tempe, AZ 85284
480.621.8967
hello@bishopfox.com • bishopfox.com

22030706 © Bishop Fox. All rights reserved worldwide.