SYNACK GUIDE 2022

PENETRATION TESTING 101

THE BENEFITS, PROCESSES AND DIFFERENCES OF PENTESTING METHODS

Synack.

TABLE OF CONTENTS

Executive Summary **3**

Why Invest in Security Testing? **4**

Benefits of Pentesting **5**

- Knowing your Attack Surface 5
- Fixing Vulnerabilities Before Criminals Find them 5
- Return on Investment 6

Types of Pentests **7**

- Breaking Down Pentesting Categories 7

Pentesting Basics **8**

- Pentesting with Internal or Resource Augmentation 8
- Pentesting Using Internal Resources 9
  - The Architecture of Teams—Red Teams and Pentest Teams 9
- Pentest Teams 9
- Red Teams 9
- Hiring an Outside Testing Service for Pentesting or Red Teaming 10

The Pentesting Process **11**

- What Are the Pentesting Steps? 12
- Different "Flavors" of Asset Access 13
  - Black Box 13
  - Grey Box 13
  - White Box Testing 13

On-Demand Security Testing Platform—Focusing a Diverse Researcher Community to Secure Your Assets **14**

- What is On-Demand Pentesting? 15
- On-Demand Security Testing Platform—Combining the Essential Elements of a Security Test 16

Bringing It All Together **17**

EXECUTIVE SUMMARY

This guide is for anyone wanting to know more about security testing as well as those security veterans who fully understand this discipline, but who need help gaining buy-in from other stakeholders within their organization.

Pentesting in its purest, most basic form involves prodding an organization's network and applications in order to determine how vulnerable the organization is to outside attack and enable the organization to shore up defenses against said attacks so as to be more secure. Testing can be as basic as running through a checklist of typical vulns (such as those dictated by OWASP) or as sophisticated as engaging a community of researchers to systematically attack one's footprint for vulnerabilities.

Pentesting—as provided by Consulting Services Providers, local boutique consulting firms, or dedicated testing companies—is a $10.7 billion business. Yet the market is evolving and there is huge value being brought to the marketplace in more innovative solutions like an on-demand security testing platform, vulnerability disclosure policy, and bug bounty[1].

Pentesting can be done externally through the organizations/vendors referenced above or internally using researchers who are on the payroll and who are tasked with trying to penetrate the organization's defenses to elucidate problems that could be exploited by attackers. As you may imagine, there are pros and cons to both approaches and we'll cover this in the following pages.

[1] Gartner, Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 3Q20 Update, combined with Synack market segment analysis.

WHY INVEST IN SECURITY TESTING?

Security testing is an important part of the security ecosystem, allowing for companies to better understand their environments and where to focus their efforts around building attacker resistance.

Every day we hear news reports about a new cyber attack. The FBI Internet Crime Complaint Center (IC3) cites the total exposed dollar losses at 26.2 Billion over the last few years[2]. One of the most effective methods to secure against cyber attacks is to perform your own penetration testing throughout the year.

While pentesting can be as easy as giving an intern some tools or hiring an accounting firm to run through a checklist, there are other more sophisticated ways to test your environment and minimize your risk. Some of these methods are more effective than others.

> *"The…scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses."*[2]

[2] FBI Internet Crime Complaint Center statistics from 2016 - 2019

BENEFITS OF PENTESTING

Given the considerable effort and resources required to do an adequate job of pentesting, let's talk for a moment about the benefits and the return on that investment. We'll then dive into pentesting in its various incarnations in today's IT environment.

BENEFITS OF PENTESTING INCLUDE:

- Understanding your attack surface
- Finding vulnerabilities before hackers do
- Meeting compliance needs imposed on the organization by its stakeholders
- Measuring the response time of your response team in dealing with a potential attack and mitigating data loss
- Identifying the areas of highest security risk, allowing an organization to focus their budget appropriately
- Getting actionable security intelligence to enable development teams and build stronger products
- Realizing a financial return on investment

KNOWING YOUR ATTACK SURFACE

The first step in shoring up your defenses is understanding what your attack surface (the combined footprint of your network, assets, and even mobile assets if you have them) look like.

FIXING VULNERABILITIES BEFORE CRIMINALS FIND THEM

Needless to say it is far more effective to find and fix vulnerabilities before they are exploited by a cybercriminal. Studies have shown that the cost of a breach far outweighs the cost of shoring up security postures in advance. For example, the average cost to recover from ransomware is currently estimated at $1.85M. Yet a pentest can be purchased for as little as $20K[3].

[3] "Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows", Sophos State of Ransomware Survey, April 2021

RETURN ON INVESTMENT

While the first six bullets are fairly self-explanatory, the ROI concept may seem a little counterintuitive. It is virtually impossible to quantify the ROI of finding a vuln before attackers do—yes, we could use the average dollar loss in fines then try to add in brand devaluation and customer loss. All of these things have been quantified in some manner or another, whether realistically or not. Then we could look at the likelihood of a breach for any given corporation (and yes, these numbers are available). But many organizations are skeptical of this kind of "what if" planning based on breach odds.

Most people don't think in actuary tables and what-ifs. They want to see concretely how one monetary investment leads to a subsequent and real return. And the prospect of reducing the odds of something bad happening can be tough to quantify. (Ironically, quantifying the damage caused by something bad happening—in this case a breach—is in fact easy to quantify and has been done so many times.[4])

What we *can definitively* say is that there is a tangible ROI when moving from standard "gun-for-hire" pentesting (two researchers, two laptops, two weeks) to an on-demand security platform for continuous pentesting.

We'll talk more on this later in the guide.

> *"In the U.S. a data breach costs a company on average $8.19 million, an increase from $7.91 million in 2018, and more than twice the global average. The cost per breached record, $242, is steeper too."[4]*

[4] "What's the Cost of a Data Breach in 2019", Digital Guardian, December 2020

TYPES OF PENTESTS

As you embark on your testing journey, you'll need to consider four key testing methodologies (consider them potential tools to be used) that you can employ to get the breadth (what percentage of your assets) and the depth (how rigorously each asset is tested) that you need to stay safe.

BREAKING DOWN PENTESTING CATEGORIES

Below are depicted the basic four types of security testing methods. Below are depicted the basic four types of security testing methods. You'll see from the diagrams below that they each have their own attributes in terms of *Coverage* and *Signal*.

1 Scanning

2 Traditional Pentesting

3 Bug Bounty

4 On-Demand Security Testing Platform

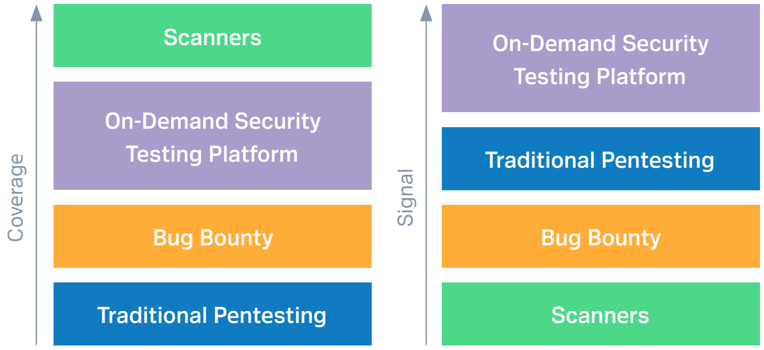

Figure 1: Completeness of Asset *Coverage*[5] and *Signal*[6]

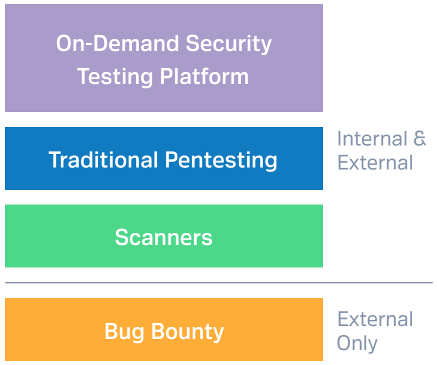

Figure 2: Internal vs External Asset *Coverage*[7]

[5] Asset *Coverage* denotes the ability to cover a wide range of assets (e.g. web, host, mobile) across the organization.

[6] *Signal* denotes effectiveness in finding critical vulnerabilities with significant business impact.

[7] Denotes the ability to test assets that are both externally facing (such as external websites) and internal (such as infrastructure components).

PENTESTING BASICS

So what is pentesting and how does it improve security? Pentesting (also called security testing) entails the act of allowing your infrastructure, mobile apps, and web apps to be tested for security vulnerabilities by a security researcher, before being exposed to attackers in the wild. This greatly reduces the risks organizations face from the digital assets needed to conduct business.

Penetration testing assesses your security posture and highlights your vulnerabilities before an attacker has the chance to exploit them.

PENTESTING WITH INTERNAL OR RESOURCE AUGMENTATION

Now that we've talked about what's involved in and what the benefits are of implementing testing, let's talk through the practical decision of contracting services with an outside vendor in order to shore up your internal resources. While there may be some organizations that have all the security resources they need, this is more the exception than the norm, for a number of reasons:

1. Security resources (i.e. people) are very hard to come by these days and are in high-demand. So they are hard to find and expensive when you do find them
2. Most companies don't have the resources they need already in house. If they do, that's great news but...
3. Most companies don't have the ability to commit these resources to the arduous tasks following-up on all vulns prioritizing/ triaging, and dealing with remediation

These are some things to think about as you read through the following types of testing which may include both internal resources and external vendor-provided resources.

Penetration testing assesses your security posture and highlights your vulnerabilities before an attacker has the chance to exploit them.

PENTESTING USING INTERNAL RESOURCES

Pentesting can be done in house using a dedicated team of ethical hackers (often called researchers) who are on the payroll and can do the testing. These researchers typically fall under the moniker of the Pentest Team but sometimes also reside in groups called Red Teams.

The benefits of using dedicated resources (either in-house or from a traditional consulting firm) are control and visibility. The disadvantages are that the skills of the team members are only as good as the individuals you've hired.

THE ARCHITECTURE OF TEAM—RED TEAMS AND PENTEST TEAMS

There are four distinct groups related to internal teams that are tasked with keeping organizations secure. They are depicted below. In this discussion we will focus on Pentest and Red Teams.

These teams do different things but sometimes the titles can be conflated. Let's first deal with the naming convention.

BLUE TEAM	PENTEST TEAM	RED TEAM	PURPLE TEAM
• Vuln assessment • Prioritization • Impact & likelihood	• Achieve compliance • Bounded and time-boxed	• Block breaches • Covert, longer-range activities for depth • Targeted	• Integrate Blue and Red Teams • Process for data sharing • Making the most out of Red Team discovery

Figure 3. Four different internal groups dealing with vulns.

PENTEST TEAMS

Pentest teams do what you might think they do, based on the description in the previous section. In this case, very simply put, a pentest team is an internal team that tests a corporation's assets and reports out on the results. This reporting is usually done to the Blue Team.

RED TEAMS

Red teams, however, are a different animal altogether. Rather than performing standardized tests or even vulnerability discovery by a process, they are much looser and more adversarial than pentest teams. A Red Team member may engage in an attack that lasts for months, camping out, waiting for the right moment to infiltrate an asset.

HIRING AN OUTSIDE TESTING SERVICE FOR PENTESTING OR RED TEAMING

Both Pentesting and Red Teaming can be done using internal resources or through an outside vendor. In fact most companies, even those with internal pentest teams are resource constrained and draw on outside testing resources to augment and scale their internal teams. The pros and cons of hiring externally, as you'd expect, are somewhat the opposite of those using internal resources. On the positive side, you are putting the testing into the hands of an organization that does this regularly and knows how to do it effectively. The downside is that you lose some control over the process, especially while the testing is being performed; and some models can be particularly prone to loss-of-control (such managed responsibility disclosure programs), depending on their process, tools, and (platform used).

Deciding on whether to build or buy (or both) really comes down to who you are as an organization and what your culture is. If you're in the testing and/or cybersecurity business then building might make sense. Also, if you have access to a number of smart, experienced hacker resources and your needs are very steady from one month to the next, then have at it.

However, if your business is something other than cybersecurity (as is the case for most companies) and you are implementing testing to protect the rest of your business (core assets, people, resources, PII, etc.) then it might be better to leave this business to a third party. Or in the case of highly-regulated industries, you may be required to have a 3rd party pentest even though you already have a large internal security team (e.g. in the financial or healthcare industry). And to be fair, most companies, even very large ones, are not able to hire all of the talent they need in house. Even those that do have internal teams typically need to augment their internal teams. This also enables them to ramp up testing as their needs change (i.e. more assets come on board, the business focus changes, or regulations come on line that require more rigorous testing).

WHAT'S YOUR RESPONSIBILITY IN A VENDOR-PROVIDED PENTEST?

1. Designating a technical point of contact
2. Selecting and defining your test target
3. Providing connectivity to your environment by arranging for adding 2 IPs to your allowlists (for incoming Researcher traffic)

THE PENTESTING PROCESS

Whether you are building from the inside or hiring an outside vendor, the process begins with the client providing direction on asset prioritization based on transaction volume, business impact, compliance requirements, and other criteria.

A researcher then identifies the target assets on which the search for vulnerabilities will occur. This often means, as a starting point, scanning for various assets. There are many tools available; one of those is the Asset Discovery tool provided by Synack. Assets in this case can be infrastructure (servers, databases, storage devices), applications, or in the case of mobile testing, mobile sites and infrastructure. Assets may be on premises or in the cloud.

Only after the asset search is done can the prioritization and targeting of assets occur. In the case of vulnerability disclosure programs or bug bounty, the organization that owns the assets may not determine which assets are targeted, while in the case of a controlled testing process, specific assets are targeted.

Once the specific assets are targeted, researchers can start the process of looking for vulnerabilities. Below is a look at what kinds of vulns they may find.

THESE VULNS MAY INCLUDE:

- Identity issues: problems related to lack of authentication or privilege that are not appropriate given their corporate role
- Routing out misconfigurations: issues that might expose unprotected resources like storage buckets or servers
- Code injection: Lack of safeguards around vulns such as code injection that allow hackers to access database content
- Password weaknesses: discovering weak passwords and other access “holes”
- Sensitive data: finding sensitive data that shouldn’t be exposed but is
- Compliance gaps: ensuring compliance across various frameworks

WHAT ARE THE PENTESTING STEPS?

Typically a pentest comprises five stages that are orchestrated by the researcher[8]:

PLANNING & RECONNAISSANCE

In this first phase the scope and goals of the test are laid out. The specific assets (applications or hosts or other network elements) are determined. There might be search engine queries and domain name searches. Researchers gather intelligence about assets to better understand the best way to approach them and discover potential vulnerabilities.

THREAT MODELING

This stage tries to identify where the assets like websites, customer relationship management tools, etc. are most vulnerable to attack and which threats are the most relevant for this particular test. It also captures what's needed to eventually protect against these threats; after all, the goal is to make the asset safer, ultimately.

EXECUTION

Here the most relevant and (deemed) effective threats are used to infiltrate the network or the application. Scanners may also be used here to perform a broad analysis of the assets and help focus the attack.

EXPLOITATION

In this phase, researchers try to penetrate as far as possible into the asset, all the while, documenting the weaknesses and openings they find along the way. This could be done using publicly-known attack tools or custom exploits built by the researchers themselves. This is a critical phase of the test in that some fragile assets can go down (i.e. an application crash or a server go off-line). Care must be taken to abide by the agreed-upon Rules of Engagement (ROEs) and implement the necessary technical controls.

REPORTING

The findings from the test are compiled into a report which should include all data from all stages of the process. It should cover specific vulnerabilities that were exploited, what data was accessed, and how long the tester was able to reside in the system before being detected. Reports vary widely across different companies and testing processes. And timing of the reports can vary as well, depending on whether the testing is being done by a community of researchers that are all accessing the same platform (in which reports come in as they are reviewed and QA'd) versus a traditional consulting firm which typically provides the report at the end of the testing period.

[8] How Hackers Hack: Attacker Methodology and Exploitation by Jeremiah Roe

DIFFERENT “FLAVORS” OF ASSET ACCESS

There are different levels of access that can be given to the testing organization and this can affect both the content of the test results as well as the effectiveness of the testing process.

BLACK BOX

This is a testing methodology in which testers have no “legitimate” access to assets; in other words, they are not provided with login credentials. Testers have no knowledge about the architecture, flow, or access roles/permissions of the asset. This means they have to find vulns essentially blind, the same way a cybercriminal would. This is, in some sense, more realistic (a positive). However it is often more time consuming (and costly, as a result).

GREY BOX

In grey box pentesting, testers are given a basic amount of information about an asset’s architecture, roles/permissions and they may also have login credentials. This can speed the process of testing and make it more effective. The negative of this is that researchers may be led down a certain path in their testing effort based on how they understand the architecture and roles while an outside attacker might attempt to infiltrate a completely different way and one that the testers might not have thought of, having been, in some sense, led in a specific direction.

WHITE BOX TESTING

White box testing takes an even more open approach by providing source code to the researcher. This allows them to formulate their attacks based on code weaknesses they discover and, as such, they can be much more targeted.

ON-DEMAND PENTESTING—FOCUSING A DIVERSE RESEARCHER COMMUNITY TO SECURE YOUR ASSETS

While pentesting itself, in any incarnation, is a revolutionary approach to finding and fixing vulnerabilities—compared to the old days of internal QA teams bearing the full responsibility; and traditional methods which are still vastly more valuable than previous approaches—an on-demand component adds jet fuel to the whole endeavor.

On-demand security researchers, vetted for talent and skill, can do things that other methods can't, based on access to diverse skills, backgrounds, varied tools, and even different cultures; as well as the ability to ramp resources immediately as needs increase. Think about what Lyft did to the taxi industry. Or, if driving yourself is more your preference, think about what Waze and Google Maps traffic visualizations provide you about what congestion may lie ahead, allowing you to dynamically change your route on the fly. There are things you can get with on-demand pentesting that you can't get with traditional pentesting approaches.

WHAT DO YOU GET WITH AN ON-DEMAND SECURITY TESTING PLATFORM?

✓ Access to skilled, experienced hackers you don't have to train

✓ A diverse set of skills and experience (different approaches to hacking into an asset)

✓ Incentive-driven model in which researchers compete to find vulns and act as if "hackers"

✓ A controlled approach (vs. e.g. bug bounty)

✓ Top researchers from academia, government, and the private sector

✓ A large number of human resources you don't have within your company and whose salaries you don't have to pay; they show up when you need them just like Lyft

WHAT IS ON-DEMAND PENTESTING?

In contrast to the traditional pentesting methods discussed earlier in this document, on-demand pentesting brings in the concept of a pool of independent Researchers (think ethical hackers) who are not employees but whom you can draw on for a specific purpose and time frame. This means you don't carry them on your payroll and you don't have to do screening/interviewing to find the best people.

An on-demand security testing platform offers more than just compliance. Through utilizing a technology platform and on-demand talent, organizations can quickly scale testing from a few to hundreds of assets. Organizations may also integrate testing as part of their product development process. They are enabled by access to a larger pool of testers with greater testing capacity.

WHAT IS INCLUDED IN A PREMIER ON-DEMAND PENTEST?

- ✓ Bounty-driven testing for adversarial perspective
- ✓ End-to-End Program Management and Testing Strategy
- ✓ Offensive Security, Technical Consultation, and Executive Support
- ✓ Platform Access and Real-time Testing Results
- ✓ Quality Assurance and Triage
- ✓ Noise Removal

WHAT IS A RESEARCHER?

- Ethical hacker
- Background in computer science, software, and/or security
- Abides by Rules of Engagement (ROEs) laid out by bounty or test firm
- No criminal record (for highly-vetted communities)
- Loves hacking

ON-DEMAND SECURITY TESTING PLATFORM—COMBINING THE ESSENTIAL ELEMENTS OF A PENETRATION TEST

The most robust testing solution—the Platform-based On-Demand approach—combines the creativity and ingenuity of on-demand vulnerability discovery and the methodology-driven approach of penetration testing, and the control and accuracy of a SaaS platform with clear workflow and ROEs.

The Platform-Based Pentesting approach generates a continuous, always-on, controlled penetration testing process with well-orchestrated coordination between researcher, target assets, and compliance activities. It can also be turned on-off or "paused" as needed to fit operational and business sensitivity needs.

It brings together top security researchers and orchestrated workflows (think about the way the Lyft platform coordinates drivers and passengers to optimize ride services, manage cost, and provide the best possible experience to the customer) to engage the on-demand security researchers for testing. Together, researchers and smart technology work in concert through an integrated platform, which coordinates their interactions; so they augment each other to provide both quality insights and continuous coverage. Because of the precision that comes from the app's smart orchestration, instead of a cap being placed on the bounty, the provider (a.k.a. vendor) assumes responsibility for the full cost of testing, and all important vulnerabilities are brought to your attention.

If done right, the researcher community is comprised of talented and ethical security researchers that are vetted. In the case of Synack, the researcher community (called SRT for Synack Red Team) is composed of a diverse group of highly skilled security experts, which include top researchers from academia, government, and the private sector. It draws representation from over 80 different countries around the world, and hundreds of years of combined testing experience[9].

The primary differentiator from traditional pentesting programs—though not the only one—is that in the Platform-based model, you have an increased level of control, quality and the speed/agility that comes with a platform. On top of this, the software platform allows control over researcher activities and can enable monitoring of researcher activities.

[9] Many Synack researchers are the top producers from notable industry vulnerability disclosure programs, and regularly speak at industry events such as DefCon, AppSec, and Black Hat.

BRINGING IT ALL TOGETHER

Hats off to you for taking some time out to review this material and, more importantly, help educate those around you—who may be in a decision-making capacity—to better understand the problems to be solved and the benefits to be gained through pentesting. Hopefully this will help convince your stakeholders that pentesting in some form or another is a must for securing an organization.

Beyond that, we've also given you food for thought to help you mull over if DIY or outsourced pentesting is your style. And finally, we've made the case that pentesting using the Synack Red Team AND a secure platform to manage that community (because let's face it, getting a call from your security administrator about an outside attack over the weekend, only to find out it's a researcher doing her job but going around ROEs is not most people's idea of a good time) is the way to go.

But there is a lot more to dig into as you become a more security-conscious organization. For tips on what features to expect from an on-demand pentest, schedule a demo with the Synack team. And lastly, check back with us in the near future to learn about how the best and brightest organizations manage their overarching security testing program in our soon-to-be released Enterprise Security Testing Strategy Guide.

Synack.