Secureworks®

WHITE PAPER

Choosing the Right Penetration Tester

How to Derive the Most Value From the Technical Test

Executive Summary

NIST describes testing as the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors. The key here is identifying the gap between actual outcomes and expectations. The question for most organizations is: who can effectively determine that gap and how will they do it?

Most organizations, needing complete objectivity, turn to external testers. However, what qualifies a third party to identify that gap? It seems there are hundreds of organizations claiming they do penetration testing, so how do you differentiate one from another?

This white paper is intended to guide decision makers on the key considerations to implement in the selection process for security/network testing providers, including:

- How to match the test to your objectives
- What features and selection criteria to look for, including in their people and process
- Questions to ask vendors when going through the selection process

Before the selection process begins, you must determine what the goal is of the test. Defining the goal determines the kind of test you need.

Determine Your Requirements

Before the selection process begins, you must determine what the goal is of the test. Is it meeting compliance, testing a new application, policies, hardware deployments, or has it just been long enough to be considering the next one? This may seem simple, but often, organizations don't clearly define the purpose of their test. Defining the goal determines the kind of test you need.

Below you will find a quick description of some of the most common types of assessments and tests, as well as examples of some of the features typically included.

	Vulnerability Assessment	Penetration Test	Blended Tests	Red Team Test
Description	A largely automated process which checks for known vulnerabilities on a per-host basis. Aimed at meeting compliance and audit requirements, and should be performed at regular intervals, or to supplement existing managed vulnerability services	Tester attempts to bypass security controls (either internal or external) and compromise a group of target systems. By simulating current threat actors, a tester can highlight the paths an actual attacker may take to move through the environment and compromise critical assets. Digs much deeper than a vulnerability assessment (VA) and can identify low-hanging fruit and systemic issues that are hidden to a VA.	To help enhance a penetration test, blended tests that include External, Internal, and Phishing can help mimic real-world attacks because it allows for credentials gathered from the phishing test to be used in the Internal and External portions of the test. When performed prior to an external or internal penetration test, phishing allows further/more complete compromise of the target environment using additional attack vectors and footholds.	A Red Team Test is a multi-faceted, organization-focused, simulated targeted cyberattack of people, processes, systems, and technologies. The objective of a red team is not to test specific systems for vulnerabilities, but rather using blended, cyberattack techniques to test the ability of an organization to respond to a skilled group of attackers (i.e. exercise the Blue Team). Since detection and response is key, to get the most value from these tests, you should have a robust Blue Team in place.

	Vulnerability Assessment	Penetration Test	Blended Tests	Red Team Test
Scoping	Reports on all systems and vulnerabilities found on in-scope systems	Threat Modeling, with client-defined target systems	Threat Modeling, with client-defined target systems	Highly customized engagement goals
Skill level required	Low	High	High	High
Target Users			✓	✓
Objective	Broad Scan	Goal Seeking	Goal Seeking	Goal Seeking
Vulnerability Scanning	✓	Minimal, as needed		
Report	List of vulnerabilities for technical audiences	Detailed, includes narrative with executive summary	Detailed, includes narrative with executive summary	Detailed, includes narrative with executive summary
Post-exploitation		✓	✓	✓
Phishing			✓	✓
OSINT to Gather Additional Targets		✓ (as needed)	✓ (as needed)	✓
Perimeter Breach: Wireless				✓ (as necessary)
Perimeter Breach: Physical Testing and Drop Box Placement				✓ (as necessary)

Forming the Initial List

Once you determine the goal and match it with the relevant testing method, the selection process can begin. When first populating a list of candidates it can be a bit overwhelming because of the number of providers that are out there. Here are a few quick ways to narrow the list down.

Ask your peers. Who did they use? Were they happy with the outcome? What was the process like and how did it compare to other testers they have used? Are your goals similar to what they are trying to accomplish?

Search on community forums. Ask other organizations that are in the same industry and are of similar size. Who do they suggest? Do they have any advice?

Eliminate the generalists. Was a candidate provider's security division a more recent byproduct of their core competency? Did they start out as a security organization or was it something that was developed as a byproduct, e.g. accounting and audit firms, or IT specialists?

Expertise. Do they present at security specific conferences (e.g. BSides, Defcon, Blackhat, Derbycon, Grrcon) and are they active participants in the cybersecurity community through disclosures, education, and large-scale competitions and exercises? Are they on the cutting edge of methodologies and tactics to perform your tests?

How do they rank in the analyst community? Do they have continuous training for their testers and reinvest in them to further their expertise? How many tests do they deliver annually?

Trust. Do they have a good reputation? Do they have fully vetted legal agreements and NDA terms? Do they carry sufficient insurance? Do they carry the required certifications?

Getting into the Selection Details

Once you have determined your initial list of candidates, it's time to analyze the ins and outs of the provider. The big two questions you need to answer are:

- Do they have qualified testers?
- Do they conduct a quality test?

While there is no standard checklist for each of these, the following are things to look for in determining if they conduct a quality test with qualified experts:

The Testers

Remember: organizations don't conduct tests, people do. When working with a technical security consultancy, there is always the risk of being affected by the team lottery: the risk of variance among the assigned tester based on expertise, past experience, timing, and location. Many organizations may claim they have experts; however they may also have interns and recent graduates conducting tests. In addition, they may not have a team entirely dedicated to testing but who instead perform a wide-range of technical engagements.

Penetration testing is a specialized field that requires additional and ongoing training, knowledge of operating systems, networking and network protocols, along with a focus on offensive security.

To ensure you don't fall victim, ask the provider to give you a choice of your tester, ask them for profiles and certifications, or ask to talk to the tester before the test begins to ensure a match between your goals and the tester's capabilities.

The Approach

While a technical test is reliant on the people conducting the test, equally important is the organization's approach to testing. For example, many organizations claim to conduct a penetration test only to conduct a glorified vulnerability assessment. The key is to understand their methodologies and tools being implemented into the process.

While there is no standard process checklist for what a technical test must follow, there are key steps that are important to look for when talking to the provider and examining their methodologies and to ensure you are getting the most value.

On the next page, you will find an example outline of a penetration test. This level of detail should be available to you for any test.

Key considerations that arise from looking at their methodology are:

What tools do they use to conduct the test? Are they proprietary?

Do they have access to the latest research and knowledge on the adversary to allow them to mimic the adversaries, both opportunistic and advanced, state-sponsored?

Do they utilize proprietary threat intelligence?

How much of the process is manual vs. automated?

Does their methodology emulate actual adversary techniques, processes, and procedures?

Many organizations claim to conduct a penetration test only to conduct a glorified vulnerability assessment. The key is to understand their methodologies and tools being implemented into the process.

Secureworks®

Sample Test Outline

Establish Rules of Engagement

Goals and objectives

Scope and validation of targets

Timelines

Reporting requirements

Personnel roles and responsibilities

Execution

Step 1: Recon

- Non-invasive causing little disruption to the client
- Goal is to learn everything about client

Step 2: Enumeration

- Potential vulnerabilities are initially identified
- Involves manual interaction

Step 3: Exploitation

- Attempt to exploit vulnerabilities
- Typically involves manual process and custom tooling

Step 4: Post-Exploitation

- Attempt to leverage exploited vulnerabilities
- Elevates privileges on compromised systems

Step 5: Pilfering

- Obtain access to target systems
- Use recovered passwords and other credentials to gain additional access

Step 6: Clean-Up and Reporting

- Always cleans up afterwards
- A comprehensive report that is actionable

The Report

Lastly, and perhaps the most important part. What is the final deliverable? Don't be afraid to ask for an example. After all, you need this deliverable to provide you with actionable takeaways. Ensure the organization's reporting meets your needs to be thorough and actionable and can be understood or interpreted to a practitioner and higher-level audience. A quality report will typically have the following components:

Executive Summary
Targeted toward a non-technical audience — senior management, auditors, board of directors, and other concerned parties

- **Engagement summary:** Brief description of the results of the engagement
- **Summary of findings and recommendations:** Describes systemic issues and high-risk findings, and recommendations to remedy issues or reduce risk

Detailed Findings
Targeted toward technical staff and provides detailed findings and recommendations:

- **Engagement methodology:** Details of what was performed during the engagement
- **Narrative:** Describes the sequence of events the testers took in their attempts to achieve the goals of the engagement to assist in understanding blended threats and/or dependent phases
- **Detailed findings and recommendations:** Describes any findings, includes website links for further reading, and recommendations for remediation or risk reduction. Evidence of the findings is supplied where applicable and, if possible, sufficient information is supplied to replicate the findings using publicly available tools.

Conclusion

The only way to know how well your network infrastructure will hold up under an attack from real-world cybercriminals is to test it with security experts capable of thinking and acting just like them – this is called adversarial security testing. Choosing the provider and expert essentially boils down to who will conduct the highest quality test with the most qualified personnel. Digging into the details entails a multi-faceted approach and asking the right questions. Secureworks hopes that this white paper provides a basis for those questions as you get into the process of choosing the right provider to meet your specific testing needs. If you take away one thing from this paper, remember that companies don't perform tests — people do — and the success of those testers is based on their training, past experience, and the methodologies and tools with which their organization enables them.

Cheat Sheet / Takeaway Questions

How many tests do you deliver annually? Globally?

Are your penetration testers certified in security and security testing?

Do you offer continuous training for your testers?

Tell me about your training program for testers.

Tell me about your delivery model and capacity.

Are your testing experts active in the cybersecurity community?

What tools do your testers use? Are they proprietary?

How do your testers gain access to the latest research and knowledge on the adversary?

Do they utilize proprietary threat intelligence?

Do your testers emulate actual adversaries? How?

How much of the testing engagement is manual vs. automated?

How much reliance is placed on tools like Nessus and other Vulnerability Scanners?

What is the final deliverable? Do you have a sample report available?

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp