tcdi

CYBERSECURITY RISK MANAGEMENT

Not All Pen Tests Are Created Equal

WHAT YOU NEED TO KNOW ABOUT PENETRATION TESTING

A pen test is arguably one of the most important security assessments an organization will undertake. This simulated cyber-attack can identify critical issues that, if left unresolved, could result in a major security incident such as data exfiltration or ransomware. Not all pen tests, however, are created equal. Penetration testing service providers can take very different approaches to the same engagement. They may use the same terminology to describe vastly different services, both in terms of quality and scope, which can make it challenging when choosing between providers.

The goal of a pen test is to identify and verify the systems that can be exploited by an attacker and effectively communicate the findings and recommendations in a way that makes the remediation process as efficient as possible. In the end, the company's data is better protected, and the job of the IT team was made that much easier. The likelihood of achieving this goal relies on the testing methodology, tools, people, communication, and reporting.

Given the importance of uncovering systems that can be exploited, and the possibility of the pen tester missing them, selecting the right service provider is an important part of the due diligence process. Before selecting a provider based purely on price, it is important to understand how different providers may approach an engagement.

DIFFERENT TYPES OF PENETRATION TESTS

There are several different types of penetration tests that can be conducted by a trusted advisor. Depending on the reason an organization is conducting a penetration test, they may only need one type of test or a combination of multiple tests to satisfy the necessary requirements.

External

An external network penetration test identifies and validates vulnerabilities in internet-facing hosts and addresses the ability of a hacker to gain access to an internal network from outside the firewall.

During the test, cybersecurity engineers will use a combination of automated and manual processes to identify and exploit vulnerabilities in an organization's external-facing hosts, including active IP addresses and applications.

Firewall

A firewall penetration test involves a configuration review of an organization's perimeter devices. This often includes an analysis of a firewall's rules and settings against industry best-practices in order to identify potential security gaps.

Web Application

A web application penetration test identifies and validates vulnerabilities from a credentialed and non-credentialed perspective. Cybersecurity engineers will attempt to gain unauthorized access or privileges to the web app with and without a valid username and password.

This will identify flaws that are open to exploitation by analyzing system configurations, authentication mechanisms, session management, authorization, and data validation, among other factors.

Internal

An internal penetration test analyzes an attack from inside the firewall by an employee, trusted vendor, and / or unauthorized user who has gained access to the network.

Attempts are made to uncover and identify vulnerabilities in internal devices, including workstations, servers, and other devices, as well as internal applications.

Further attempts are made to manually exploit targeted systems to achieve privilege escalation, pivot to other systems, and gain access to sensitive organizational resources.

Wireless

A wireless penetration test evaluates an organization’s wireless network and infrastructure, including routers and Voice-over-IP (VoIP) systems, to identify and validate vulnerabilities that could lead to access to an organization’s internal network or other wirelessly connected systems.

Physical

Physical security incorporates the review of tangible security controls that protect access to information systems and valuable equipment. Elements include cameras, lighting, security personnel coverage, locks, and other security mechanisms.

Cybersecurity engineers will evaluate physical security controls to protect against unauthorized access, theft, or damage of equipment, and often includes an attempt to gain access to an organization’s facilities via tailgating and other social engineering tactics.

Social Engineering

Social engineering phishing tests determine how likely personnel are to fall victim to a phishing, spear-phishing, or vishing (voice phishing) attack.

Conducting regular social engineering campaigns and providing access to on-demand training, organizations can turn their number one liability into their first line of defense.

VULNERABILITY SCANS VS. PENETRATION TESTS

Unfortunately, some “penetration tests” are nothing more than a thinly veiled vulnerability scan. A vulnerability scan is not a true penetration test, and it does not accomplish the aforementioned goals.

A vulnerability scan is an automated process whereby systems are scanned for known vulnerabilities, and a report is automatically generated detailing the low, medium, high and critical vulnerabilities. Relying solely on a vulnerability scan can result in many false positives, which wastes time during remediation. In addition, there is no threat modeling nor any attempts at actual exploitation. During a penetration test, the vulnerability scan is only one step in a much more in-depth process that brings the human element into the equation.

PEOPLE

Although a highly technical test, some could argue that a penetration test is also very much about people. It brings the human element to a simulated cyber-attack. Although the test involves scanners, software, CVEs (Common Vulnerabilities and Exposures), and a lot of computing power, it also relies heavily on the person behind the tools and technology. More specifically, the test depends on how the person performing the test analyzes and interprets the data, researches possible exploits, and develops and executes their attack plan. This is why every pen test is unique. It relies on the background, training, sophistication, diligence, creativity, and communication skills of the penetration tester.

An experienced penetration tester will create custom attacks rather than simply relying on automation. They will examine systems and know when and where to dig deeper and use combined vulnerabilities in their attempts at exploitation. When service enumeration is not possible, for example, a human attacker may use manual methods such as source code analysis to find vulnerabilities a scanner would

Our team of pen testers hold over 40 cybersecurity certifications, including:

- CISSP – Certified Information Systems Security Professional
- HISP – Holistic Information Security Practitioner
- MPCS – Metasploit Pro Certified Specialist
- CompTIA Security+
- CompTIA CySa+
- MCSA – Microsoft Certified Solutions Associate
- CEH (Master) – Certified Ethical Hacker (Master)

miss. They may also utilize “chaining” to combine two or more vulnerabilities to craft a much more serious attack than the severity of the individual vulnerabilities would indicate.

For example, a cross-site scripting vulnerability on a website that sets session cookies without the http only flag can be reported as two separate findings. Or, they can be combined to send these cookies to a malicious server in order to demonstrate the potential for user session compromise. It is this curiosity and experience that can uncover exploitable systems and critical vulnerabilities that may otherwise be overlooked by a less experienced pen tester. Failing to identify exploits that a real-world attacker would uncover defeats the purpose of the engagement. That is why the experience of the pen tester matters.

The trustworthiness of the person performing the pen test is also another important consideration. You are giving them access to your systems and permission to break into them. If successful, they will have the knowledge of how to hack into your organization and may find themselves with access to a variety of sensitive data. As such, it is imperative to engage a trusted and reputable provider. Is the pen testing provider willing to sign a non-disclosure or business associate agreement? Are they using outside contractors or consultants for any part of the engagement? Do they perform background checks? Are any of the pen testers located outside of the country? What experience and certifications do they have?

THE TCDI DIFFERENCE

Our pen testing team has years of real-world experience with incident response, security design, and proactive defense. This adds a unique perspective to ethical hacking projects that better simulates a skilled, patient, and motivated attacker.

DON’T TAKE OUR WORD FOR IT....

“When seeking a partner to assist us with assessing our cybersecurity vulnerabilities, audit our existing IT provider, and reduce our overall security risk, we looked for a firm with the same level of dedication to client service and level of industry expertise as our own.

With TCDI, we have a committed partner providing not only security expertise, but an above-and-beyond level of client service. TCDI provided a final, in-person meeting after our testing and met with both our Audit Committee and Board of Directors. In addition, we invited them to speak at our biennial meeting of clients. TCDI’s team is always available to answer questions and help grow our overall cybersecurity program. This type of relationship is invaluable.”

Tracy Mikuta
Managing Director,
Compliance and Technology
Piedmont Trust Company

TOOLS

Tools are a pen tester's best, friend because they give them the ability to perform important tasks. In the same way that a mechanic may use very specialized tools to work on various parts of an engine, the same applies to penetration testing. Unfortunately, over-reliance on open source software, a single tool, and/or automation can present major issues. For example, a free vulnerability scanner like OpenVas may not have as many CVEs in its database compared to a commercial scanner like Nessus®.

It may also be missing robust detection capabilities resulting in more false-positives and may miss things by labeling a service as a false-negative. As a result, an open-source scanner may miss vulnerabilities that a commercial scanner will find. Relying on just a single tool may also result in missed vulnerabilities. It is not uncommon for one scanner to find a vulnerability that another scanner missed. Combining many tools, including commercial, opensource, and proprietary, will result in a more thorough pen test and with better results.

Furthermore, automated pen testing and vulnerability scanning tools are not necessarily equal to a pen test, because they do not evaluate the vulnerabilities as a whole but rather on an individual basis. While these tools can be used to automate some basic tasks, they should not be relied on for the entirety of the testing. Maintaining the human element in a penetration testing engagement provides a more holistic view of the exploitable vulnerabilities in your environment and how a skilled and patient attacker would attempt to exploit them.

It may be tempting to cut costs by relying solely on open source software or taking the human element out of the process through automation. This approach, however, could easily miss the one exploit that an attacker uncovers using human logic to compromise an environment.

THE TCDI DIFFERENCE

The recipe for an effect pen test is to combine talented cybersecurity experts with sophisticated technology. Our penetration testing toolkit is comprised of 40+ applications and tools to ensure thorough analysis and testing is performed.

METHODOLOGY

The methodology used by the pen tester, particularly during the information gathering stage, will play a key factor in the likelihood of uncovering hard to find vulnerabilities. Are they simply "scratching the surface" or are they taking a deep dive when searching for vulnerabilities and exploits? For example, are only the most common ports being scanned during the enumeration stage, or are all the ports being scanned? Are multiple scanners and methodologies being used or just one? The pen tester should rely on several different scanning methodologies to deliver the most comprehensive results in terms of port enumeration and service enumeration. If not, they may very well miss critical vulnerabilities that would otherwise have been discovered.

To conduct a more in-depth analysis, pen testers will often identify vulnerability chaining opportunities, research enumerated versions using several sources to uncover non-public zero-day exploits (as well as public exploits), evaluate the systems' responses to their efforts in order to expand their exploitation attempts, and filter out false positives through manual validation. All of these items largely rely on the background and experience of the "human behind the keyboard" rather than an automated scan or process. Without an experienced tester and thorough methodology, the likelihood that things will get missed and your environment will still be vulnerable increases drastically.

THE TCDI DIFFERENCE

We perform true pen testing with experts who will filter out false positives, develop custom attack plans, and manually exploit vulnerabilities. In addition, we view ourselves as an extension of our clients' team and pride ourselves in being responsive to their needs.

DON'T TAKE OUR WORD FOR IT....

"TCDI's cybersecurity team is reliable, professional and accessible. Regarding cybersecurity services, what is at stake is so vital in terms of the health and well being of the organization - TCDI's team was sensitive to the confidentiality of the matter, highly qualified and quickly addressed our needs. In fact, we were initially going to engage two providers, but the TCDI team was able to get the job done before the other firm was even able to contribute. We have utilized TCDI's cybersecurity services several times and will continue to work with them - we consider them a true partner."

Lovell Custard
President & CEO
Murtis Taylor Human
Services System

COMMUNICATION AND REPORTING

Regular communication throughout the project is essential and the client should be alerted immediately of any major findings so they can be addressed upon discovery. For example, critical vulnerabilities like Eternal Blue are commonly uncovered during internal pen tests. These vulnerabilities could be disastrous if malware were to appear on the network prior to remediation. That is why notifying the client upon discovery of critical issues, rather than waiting until the end of the engagement, is important when the vulnerabilities pose a very serious risk to the environment.

The pen test is of little value if the issues identified are not corrected. That is why the job of the pen tester isn't done until they have effectively communicated their findings and recommendations in the written report so that the client can efficiently remediate their systems. Put simply, the pen tester's job is to make the client's job easier by reducing the time and cost associated with remediation.

The written report should include, at a minimum, the vulnerabilities that were discovered, the exploits that were executed and demonstrated impact, prioritized recommendations based on the findings, risk scores and metrics, and an executive summary of the overall results of the pen test. The report is the roadmap that will be used to remediate systems. It should be organized accordingly with links to resources and additional details on how to address the various issues that were identified.

Metrics and scoring are invaluable for evaluating the overall level of risk based on the findings. Furthermore, they are useful for tracking remediation progress and how risk has changed over time. For example, the metrics and scoring from the first pen test can be used as the baseline and then compared to the results for subsequent tests. These data points and trends can provide valuable insight to various stakeholders and those responsible for securing the environment.

Finally, a project debrief meeting is critical to the communication process. They provide an opportune time for the pen tester to verbally explain his or her findings recommendations. They also provide the client with the opportunity to ask questions about the written report. The conclusion of the project

DON'T TAKE OUR WORD FOR IT....

"We've done pen testing with other vendors in the past, but one of the reasons we picked TCDI was you could tell how thorough their reporting process was just by looking at their sample pen testing report. When we received the completed pen testing report, it shed light on vulnerabilities that our previous vendors didn't even consider or test for. It was very thorough and well done, and their team took the time to explain and answer any questions we had about how to remediate."

Brian Schreiner
Director of IT
Sentinel Risk Advisors

debrief meeting, however, should not mark the end of the engagement. Rather, the pen tester should make themselves available for any follow-up questions from the client during the remediation process to help ensure the recommendations are properly implemented. In some instances, a retest to confirm the exploited vulnerabilities have been patched will be performed as well.

THE TCDI DIFFERENCE

At TCDI, the job isn't over until it's over. Once the penetration test is complete, our cybersecurity team will conduct a post-engagement client meeting to go over the results of the test and answer any questions about the vulnerabilities identified and / or recommendations. We also provide a letter of attestation after every engagement for our clients to use in the event it is requested by a third-party.

CONCLUSION

Not all pen tests are created equal. There are numerous variables that play a role in the quality and sophistication of the pen test, including the:

- Skills, experience and determination of the person performing the test;
- Process and methodology utilized;
- Tools used to test, analyze and exploit the target systems;
- Communication throughout the project; and
- Quality and utility of the final report.

These variables may be difficult to compare when evaluating potential pen testing service providers. As a result, price too often becomes the primary decision-making factor. Selecting the lowest priced provider, however, often means sacrifices in one or more of the areas listed above. Given the importance of uncovering systems that can be exploited, and the possibility of the pen tester missing them, identifying service providers who can provide high quality service is paramount. Understanding how different providers may take very different approaches to the same engagement, both in terms of quality and scope, and asking the right questions during the vetting process is crucial.

APPLES TO APPLES COMPARISON

Even when you know what to look for, getting an apples to apples comparison from multiple vendors can be difficult. At TCDI, we are dedicated to providing transparent and predictable pricing. We also pride ourselves in being a true partner and can help you evaluate and compare different proposals. We will provide recommendations based on what is best for your organization, not what is best for us. Contact us today to get started.