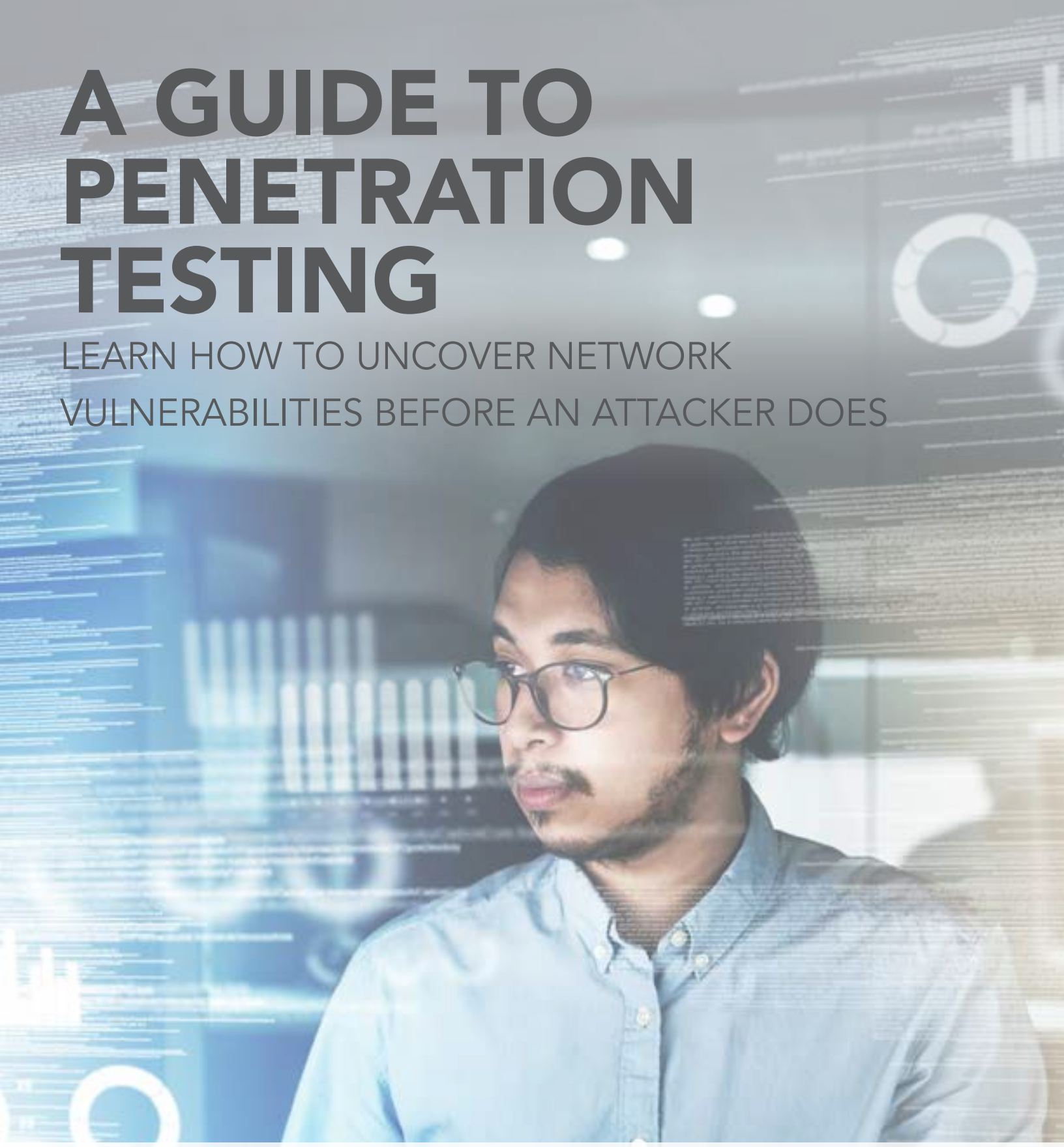
A GUIDE TO PENETRATION TESTING

LEARN HOW TO UNCOVER NETWORK VULNERABILITIES BEFORE AN ATTACKER DOES



tyler technologies

UNCOVER GAPS AND REDUCE RISK

When we ask information security professionals what keeps them up at night, many times they say, "What I don't know."

It's no surprise – with reports of breaches on an almost daily basis, it's impossible to ignore that there are a lot of hackers out there trying to get into networks wherever they can, with tools and techniques that are constantly evolving.

That's why it's important to be diligent about assessing your network security from the perspective of a hacker. And the best way to do this is through a penetration test (pen test).

Our Guide to Penetration Testing will provide you with the fundamental information you need to know in order to effectively incorporate this important practice into your security defense arsenal.

Read this guide to learn:

- The what, why, who, and how of pen testing
- How to choose the right type of pen test for your organization
- Elements of an effective pen test
- 10 tips to reduce common vulnerabilities

"Although there are many ways to secure systems and applications, the only way to truly know how secure you are is to test yourself. By performing penetration tests against your environment, you can actually replicate the types of actions that a malicious attacker would take, giving you a more accurate representation of your security posture at any given time."[1]

[1] Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Sile, R., Mancini, S. (2017). Penetration Testing: Assessing Your Overall Security Before Attackers Do. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/membership/34635 Page I2

Examples of Professional Credentials

- Offensive Security Certified Professional (OSCP)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Offensive Security Advanced Windows Exploitation (AWE)
- Offensive Security Wireless Professional (OSWP)

WHAT IS A PEN TEST?

A pen test is used to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities through an ongoing cycle of research and attack against a system, application, or network.

The basic goals are to:

1. Identify vulnerabilities on systems/applications in scope
2. Penetrate vulnerable systems, services, and/or applications using automated and manual tools and analysis
3. Gain access to systems and/or sensitive data

It's a simulated cyber-attack that can be conducted from an internal or external (internet) perspective.

WHO SHOULD PERFORM A PEN TEST?

When it comes to pen tests, the experience, training, and expertise of the pen tester is directly linked to the value the results will provide you.

Continuous education is a fundamental element of ensuring quality testing and there are several professional credentials for pen testers.

Pen testers also need to stay up-to-date on threats and vulnerabilities by constantly consuming the latest threat intelligence.

WHY PERFORM A PEN TEST?

IDENTIFY VULNERABILITIES AND WEAKNESSES

CHECK EFFECTIVENESS OF EXISTING SECURITY CONTROLS

MEET REGULATIONS AND COMPLIANCE STANDARDS

PRIORITIZE MITIGATION AND REMEDIATION

ASSESS INTRUSION DETECTION AND RESPONSE SYSTEMS

CONFIRM PUBLICLY AVAILABLE NETWORKS/SYSTEMS

tyler technologies

HOW TO PERFORM A PEN TEST

At Tyler, each engagement is customized to meet unique goals and objectives, therefore the specific elements of our methodology that are leveraged is contingent upon the level of testing and defined scope. The following is an accounting of the potential testing phases and their respective individual elements:

FOOTPRINT ANALYSIS/RECONNAISSANCE

Typically the first step, this entails searching various publicly available sources for detailed company-specific information. This allows us to identify target systems and provides information that may prove useful in an attack.

SYSTEM, SERVICE, AND VULNERABILITY IDENTIFICATION

In this phase, a variety of specialized security tools are used to identify the architecture and vulnerabilities. The goal is to identify systems/devices that respond to authorized and unauthorized requests, the services/applications that those systems are providing, and inherent and/or potential vulnerabilities

EXPLOITATION

Here we attempt to gain unauthorized access to systems and/or information utilizing the vulnerabilities identified in the previous phase. Once we gain access to systems/information, we report the finding and move on in an attempt to find additional external vulnerabilities.

REPORTING

In this final phase, we generate an executive summary and a technical report that explains the findings, provides customized remediation recommendations, and, if available, includes details on repeating the attack scenario.

CHOOSING THE RIGHT PEN TEST

Not all penetration tests are created equal. The scale and scope can vary greatly, and it's important that you understand what you are getting. Here are a few common types, and why you choose one over another.

TYPES OF PEN TESTS

External Network Pen Test

What could a hacker access if they breach your network perimeter?

The pen tester will identify vulnerabilities and try to gain control of a system using a combination of automated tools and manual techniques. At Tyler, we customize the level of engagement that will satisfy your unique needs.

Internal Network Pen Test

If an attacker gets inside, how can they expand their reach or access?

In an internal test, the pen tester is already "in" the network, and are sometimes even provided with user level credentials. Then they attempt to escalate those privileges and gain unrestricted access.

Web Application Pen Test

What if a hacker attacks your website or web applications?

This type of testing is performed on websites or other web applications, including customer/employee portals and support sites. It can be conducted from an authenticated or unauthenticated perspective. For the most effective results, web app testing requires a significant manual effort.

Mobile Application Pen Test

What if an attacker attacks your mobile application?

The attack surface for this test can include the mobile application and/or the backend infrastructure that services the application. The goal is to review the app and supporting infrastructure for vulnerabilities that could be the result of insecure configuration settings and data storage on the mobile device itself; or in the web services/infrastructure that supports the mobile application.

tyler technologies

PENETRATION TESTING VERSUS VULNERABILITY ASSESSMENT

"Vulnerability assessments and penetration tests complement each other. In many programs, vulnerability assessments are the first step. From there, one can perform a penetration test to see how exploitable the vulnerability is.

Misunderstanding these important tools can put your company at risk and cost you a lot of money."[1]

There is a misconception that pen tests and vulnerability assessments are synonymous. While both are critical components of a threat and vulnerability management process, they are very different engagements.

OBJECTIVES

Vulnerability Assessment: Identifies known weaknesses in your environment. Findings may include unapplied patches, vulnerable software versions, and gaps in network controls. Primarily an automated assessment.

Pen Test: Simulates a real-world attack and tests your existing defensive controls. Manual testing routinely finds vulnerabilities that automated vulnerability assessment tools are incapable of finding.

TOOLS

Vulnerability Assessment: Primarily performed using automated scanning tools such as Nessus, Qualys, or OpenVas, which are off-the-shelf software packages.

Pen Test: Automated tools are leveraged for efficiency, however, the majority of this effort is manual and relies upon the skill-set and expertise of the pen tester.

DELIVERABLES/FINDINGS

Vulnerability Assessment: Typically a stock report listing all known vulnerabilities found during the scan, prioritized by severity and/or criticality with remediation recommendations.

Pen Test: A more succinct report with vulnerabilities, ranked by severity with remediation recommendations, plus details on how an attacker could breach your defenses.

FREQUENCY

Vulnerability Assessment: Ideal for periodic testing between pen tests and as a quick verification when changes are made to the environment.

Pen Test: Should be performed at least annually and any time significant changes are made to the environment.

[1] Martin-Vegue, T. (2015). Vulnerability scan vs. penetration test vs. risk analysis: What's the difference? Retrieved from https://www.csoonline.com/article/2921148/whats-the-difference-between-a-vulnerability-scan-penetration-test-and-a-risk-analysis.html

ELEMENTS OF AN EFFECTIVE PEN TEST

INDEPENDENT ANALYSIS/SEPARATION OF DUTIES

Information security best practices call for independent testing for several reasons. First, cybersecurity specialists have the latest, most sophisticated technologies and the most current information on exploits. Also, internal teams may see things during tests that should trigger a response, but get ignored because they know the idiosyncrasies of their IT infrastructure — a common but dangerous mistake.

RESEARCH & RECONNAISSANCE

Determining the appropriate scope, defining an effective methodology, and establishing a practical blend of automated vs. manual testing are critical components of an effective pen test. Before any testing begins, the pen tester should have a clear picture of the unique environment. This knowledge is gained through research and reconnaissance.

SECURITY EXPERTISE & TRAINING

A skilled pen tester looks at the vulnerabilities found during a scan, then using research, validates that the vulnerabilities are accurate, and determines how to best take advantage of them to gain access to the system. Having the skill-set to understand the orchestration between what the automated tool reports and how to manually exploit findings is how value is derived from a pen test.

ACTIONABLE INSIGHT

When testing is completed, you need to have actionable findings and effective remediation recommendations. This allows you to prioritize your subsequent remediation process according to your most critical vulnerabilities. After all, what's the point of going through the time and effort unless you're committed to improving your network security posture?

tyler technologies

KEY POINT:

In recent years, 80% of all high vulnerabilities and 46% of all vulnerabilities that Tyler reported in pen tests were found due to the manual techniques that are incorporated into the Comprehensive Level of Pen Testing.

PEN TEST OPTIONS

The scale and scope of a pen test engagement is a function of satisfying business obligations and understanding organizational risk tolerance. Tyler works in a collaborative fashion to customize the level of engagement that will satisfy unique organizational needs. Our options, which are described below, also include a vulnerability assessment, which is primarily automated testing using a commercial network vulnerability scanner.

BASELINE PEN TEST

Tyler attempts to verify/exploit vulnerabilities identified in a penetration scan.

We perform testing for default credentials on any common systems/software found as default passwords are a common and easily exploited attack.

Ideal for budget-conscious organizations with developing cybersecurity programs that would like to get a basic understanding of their external security posture.

COMPREHENSIVE PEN TEST

Building on to what is offered at the baseline level, this test includes manual attack techniques, open source intelligence gathering, and target environment specific research/testing.

A limited amount of unauthenticated web application testing against commonly used applications is also included.

This option is best suited for compliance-driven organizations and high-value targets such as financial institutions and healthcare organizations.

10 TIPS TO REDUCE COMMON VULNERABILITIES

In addition to regular penetration testing, you should stay on a regular schedule of finding issues. Keeping things up-to-date will help you reduce the number of vulnerabilities found on your network during testing as well as shrink the attack surface available to cyber criminals. Here are some tips.

1. Run regular vulnerability scans
2. Patch software regularly
3. Minimize local administrator privileges
4. Configure systems securely, e.g., in accordance with the Center for Internet Security guidelines
5. Practice secure network engineering, e.g., network segmentation to limit access to systems/information
6. Enforce a password policy and use dedicated password managers
7. Change default passwords on all applications and appliances
8. Ensure all devices have unique local administrator passwords
9. Use secure software development practices
10. Have working and tested backups of key systems/data

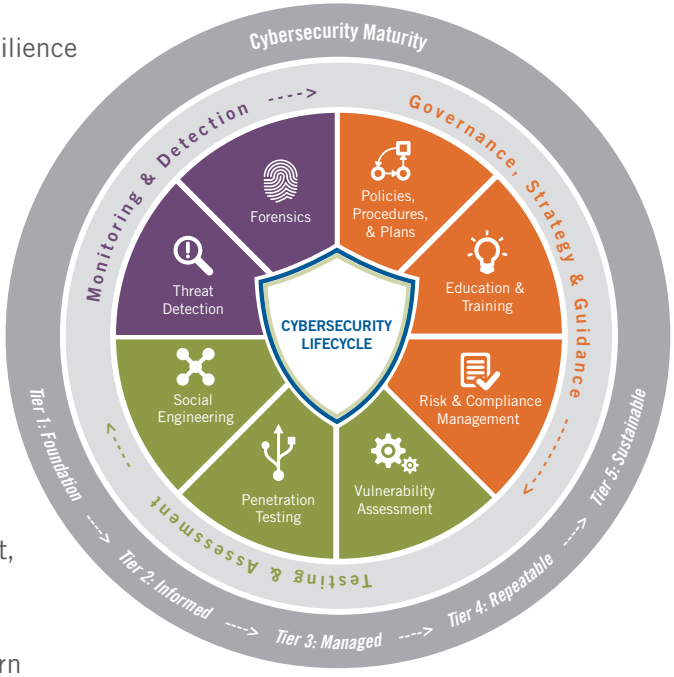
CYBERSECURITY SOLUTIONS FOR THE PUBLIC SECTOR

Cybersecurity is not just about technology. Achieving cyber resilience depends on a cybersecurity lifecycle — an ongoing cycle of interconnected elements that complement and reinforce one another.

As security professionals, Tyler Cybersecurity partners with your organization to help you achieve a robust cybersecurity posture that evolves and adapts with the dynamic threat environment.

We can help you build and mature an effective cybersecurity program over time, without overwhelming your budget or available resources. Our services include program development, risk assessment, training, tech testing, and threat detection.

Contact us today to discuss how you can achieve the best return on your cybersecurity investment.



tyler technologies

About Tyler Cybersecurity

Information security has always been a top priority at Tyler. Tyler has taken that focus to the next level by offering Tyler Cybersecurity, products and services supported by a team of experts dedicated to protecting their clients since 2002. By partnering with Tyler Cybersecurity, our clients realistically and cost-effectively protect their information assets while maintaining a balance of productivity and operational effectiveness.

Tyler Technologies (NYSE: TYL) provides software and services tot ransform communities. Tyler's solutions connect data and processes across disparate systems, allowing clients to gain actionable insights for solving problems. We are proud to deliver effective cybersecurity solutions to help protect our communities.

Tyler was also named to Forbes' "Best Midsize Employers" list in 2018 and recognized twice on its "Most Innovative Growth Companies" list. More information about Tyler Technologies, headquartered in Plano, Texas, can be found at tylertech.com.

CYBERSEC-PENTST-TL-13321-0220

tyler technologies