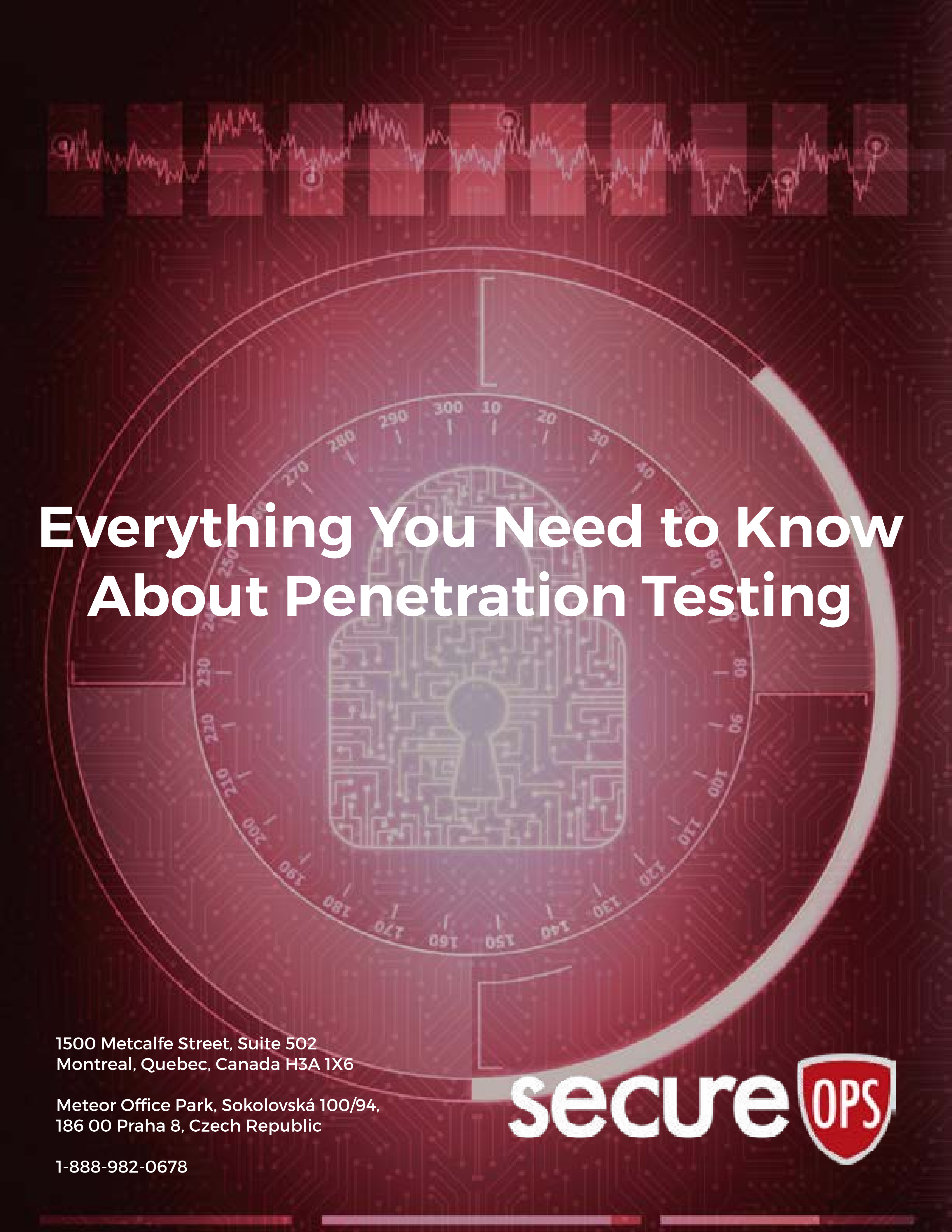


Everything You Need to Know About Penetration Testing

1500 Metcalfe Street, Suite 502
Montreal, Quebec, Canada H3A 1X6

Meteor Office Park, Sokolovská 100/94,
186 00 Praha 8, Czech Republic

1-888-982-0678

secure OPS

Everything You Need to Know About Penetration Testing

Goals and Types of Penetration Testing

Penetration Testing attempts to exploit weaknesses or vulnerabilities in systems, networks, human resources, or physical assets in order to stress test the effectiveness of security controls.

The different types of penetration tests include network services, web application, client side, wireless, social engineering, and physical. A penetration test may be performed externally or internally to simulate different attack vectors. Depending on the goals of each test, a penetration tester may or may not have prior knowledge of the environment and systems they're attempting to breach. Various types of pen tests are known as black box, white box, and gray box penetration testing.

Penetration testing has become an essential tool for IT security teams to understand the strengths and weakness of their security strategy. At SecureOps, we conduct a variety of different penetration tests with a variety of different goals in order to meet the specific objectives of our client. Our goal in this paper is to provide insight into all the different types of penetration tests, how they are performed and why they should be performed; this is so that you can choose the most appropriate type for your organization and business needs.

Before we get started, penetration testing has evolved over the years and different flavors of pen testing have come into vogue including “capture the flag,” “red team assessments,” “war dialing;” they also include terms like ethical hacking, red team, blue team, bug bounty and so many more. We'll start with the basics and touch on the various types of tests and terms associated with pen testing as we go through the detailed explanation of Penetration Testing.

Thank You for Taking Time to Read the Report! Hope You Enjoy It!

The Team @ SecureOps

What is the Main Goal of a Penetration Test?

Penetration testing has become a widely used IT security exercise by all types of organizations in recent years. This is especially true for industries that collect, and store sensitive or private information (PII) such as retail companies, banks and healthcare providers.

While the purpose of a penetration test is to expose vulnerabilities or exploit weaknesses so that the IT security team can prioritize and fix those weaknesses, it's important to note that the main goal can be tied to a business objective that requires a viable cybersecurity strategy. For example, A business may need to meet NIST compliance under certain deadlines if they are to be awarded a $10 million government contract - NIST requires a periodic penetration test. However, the most likely reason an organization conducts a penetration test is to measure the level of maturity of the IT security organization and its practices.

A penetration tester assesses a target environment, seeking to compromise and take control of the targeted systems. The objective of the test is to find vulnerabilities in the environment and deliver a comprehensive report to the organization being tested. In many cases, the scope is not limited to systems or techniques – the penetration tester can direct his attack throughout the target organization's systems and infrastructure.

When the test is complete and the report is delivered, the organization can more effectively measure their level of IT security maturity and assess whether that level is sufficient to meet the business goals of the organization and protect the data of its customers, employees, and stakeholders.

The Different Types and Approaches to Penetration Testing

Penetration tests often differ in the approach and in the part of the infrastructure they attempt to exploit.

The different approaches to penetration testing include:

- External VS Internal
- White Box
- Black Box
- Gray Box

The different types of penetration testing include:

- Network Services
- Web Application
- Client Side
- Wireless
- Social Engineering
- Physical
- Mobile Applications
- IoT Devices

The critical elements that differentiate penetration tests:

- **Penetration tester experience** – Choose organizations that have certified, experienced pen testers. The pen tester is the most critical element concerning what you learn in the test and what steps you will take to manage vulnerabilities.
- **Daily reporting on progress** – The penetration test is a process that needs to be transparent to the client in order to for the client to clearly understand what is being tested and the benefits of the insights from the test.
- **Retest fixed vulnerabilities** – A penetration test will break controls and uncover vulnerabilities; make certain that when the issues are remediated a test is administered to assess the fixes.
- **Integration with other security services for a full turnkey experience** – A penetration test should be part of an overall security program. It should be integrated with vulnerability assessments, vulnerability management tasks and ultimately a risk management and security posture programs.

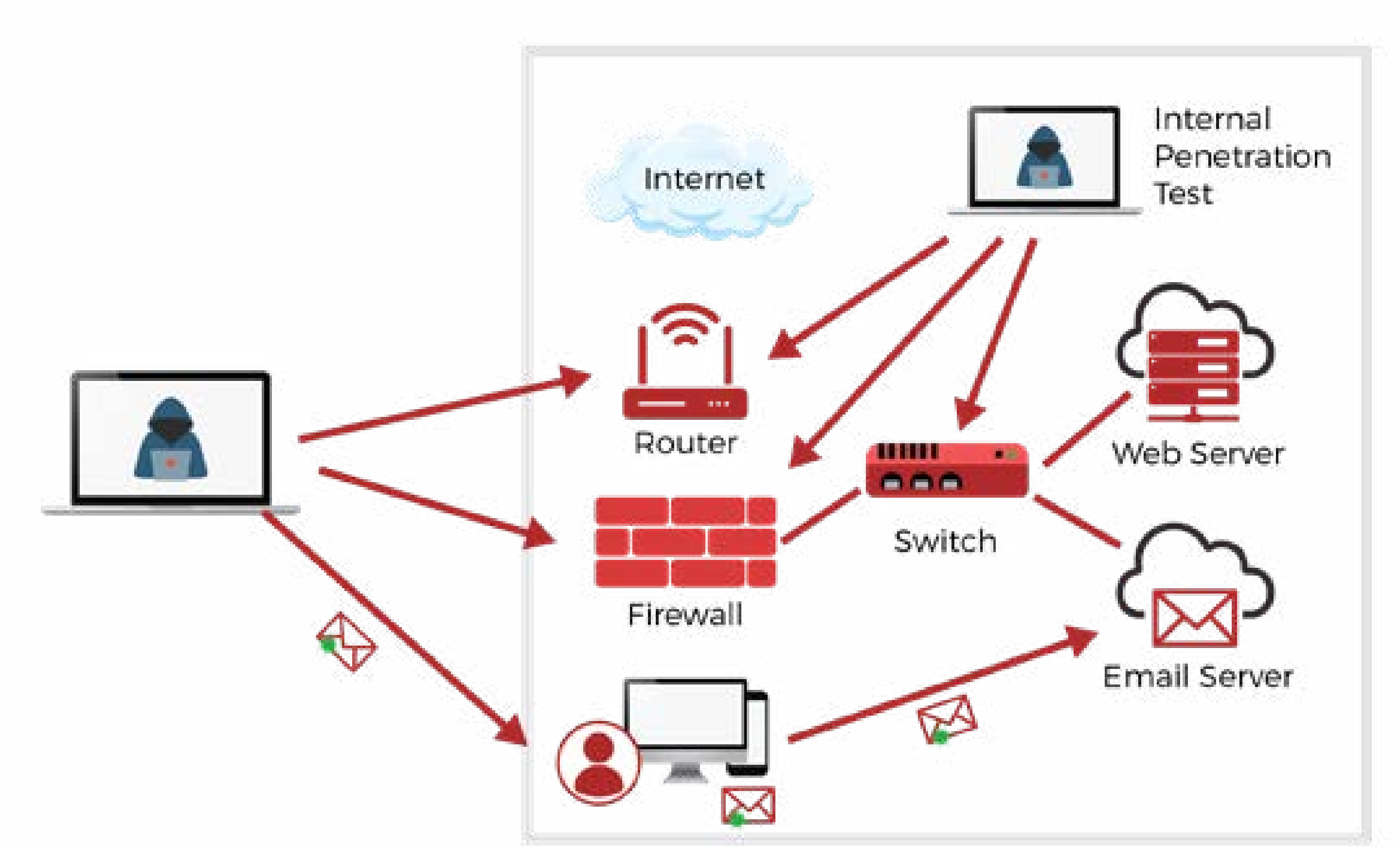
External vs. Internal Penetration Testing

External penetration tests are performed when businesses want to assess their risk of a successful attack on their network from the outside. Over the past 3 or so years businesses are preparing themselves by deploying advanced security technologies such as endpoint protection, advanced anti-virus, next-generation firewalls (NGFW), or by simply conducting security awareness training to prevent successful attacks.

While anti-phishing technology like content filters and URL attachment blocking may help, it doesn't provide the kind of robust protection that would prevent all attacks. This is because malicious actors are aware of the typical security technology and controls that businesses have in place. As a result, new attack vectors and malware are constantly being created to circumvent firewalls and anti-malware software.

Kerberoasting, for example, is a credential access tactic that malicious actors use against systems running Windows. Essentially, weak Active Directory security policies can lead to an unauthorized party being given access to an encrypted hash or identifier of every user profile in your environment. From there, they can brute force the encryption offline to crack it and gain access into your network.

Businesses may also want to know how much damage a malicious actor could cause if they already had access to the internal network. The goal here could be to test if the blue team or defensive team is able to identify the attack, or if the pen tester is able to escalate their privileges to admin rights.



Black Box Penetration Testing

We mentioned Black, White and Gray box penetration tests - in a black box penetration test, the pen tester is given little to no information regarding the IT infrastructure or security practices of a business. As a matter of fact, in many cases they know almost nothing about the business and are asked to compromise systems and data in the same way a hacker with nefarious intent would. The main benefit of this type of test is to simulate a real-world cyber-attack.

A black box penetration test last from a few days to a couple of months based on the complexity of the IT infrastructure and the goals of the pen test. Organizations can expect to pay between $10,000 – $25,000 or more due to the level of effort involved in planning, performing, testing, and completing the exercise and create the report.

One of the easiest ways for pen testers to break into a system during a black block test is by deploying a series of exploits known to work, such as Kerberoasting mentioned above. This type of test is also referred to as the “trial and error” approach, however, there is a high degree of technical skill involved in this process.

To clarify terms, you may hear when discussing pen testing; ethical hacking is similar to penetration testing but has several key differences. The term ethical hacking is a broader term for hacking techniques used by ethical hackers. While a penetration tester might discover flaws and vulnerabilities and deliver a report, an ethical hacker will likely conduct a longer-term assessment, using a greater variety of attack types and more fully exploring the environment.

While a penetration tester is usually focused on identifying vulnerabilities, an ethical hacker will usually pursue a full scope of hacking techniques in an attempt to find as many security flaws as possible. It is less of a point-in-time assessment and more of a holistic security evaluation of a target environment. Ethical hackers also deliver more remediation assistance, commonly working with the organization to ensure the security of the target system with the permission of the system owner.

White Box Penetration Testing

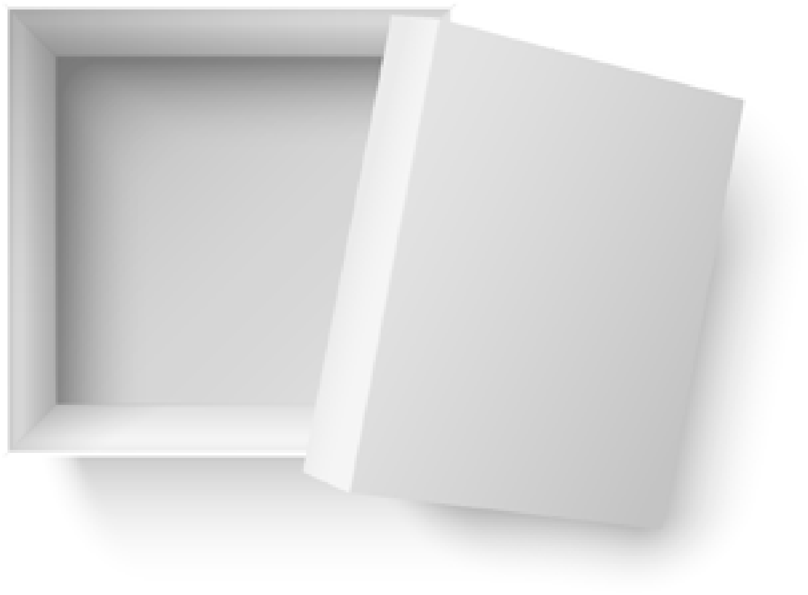
White box penetration testing also called clear box testing or glass box testing. White box pen testers have full knowledge and access to the environment, systems, software, and source code.

The goal of a white box penetration test is to conduct an assessment of the strengths and weaknesses of a business's systems and to provide the pen tester with as much detail as possible. As a result, the tests are more thorough because the pen tester has access to areas where a black box test cannot, such as quality of code and application design.

White box tests do have their disadvantages. For instance, given the level of access the pen tester has it can take longer to decide what areas to focus on. In addition, these types of tests often require sophisticated and expensive tools such as code analyzers and debuggers.

White box tests can take two to four or so weeks to complete and cost between $4,000 – $20,000. To be clear, black box penetration tests are geared to break security controls and compromise a business, white box penetration tests are geared to assess the security controls, maturity, and vulnerabilities of a business.

Sometimes security audits and pen tests are confused; a security audit differs from a penetration test in that it measures cybersecurity performance against a set standard, like the NIST CSF. Usually involving a detailed checklist of security controls, a security audit is more comprehensive, assessing the entirety of a security program – while the penetration test seeks just one vulnerability to access and compromise the environment.

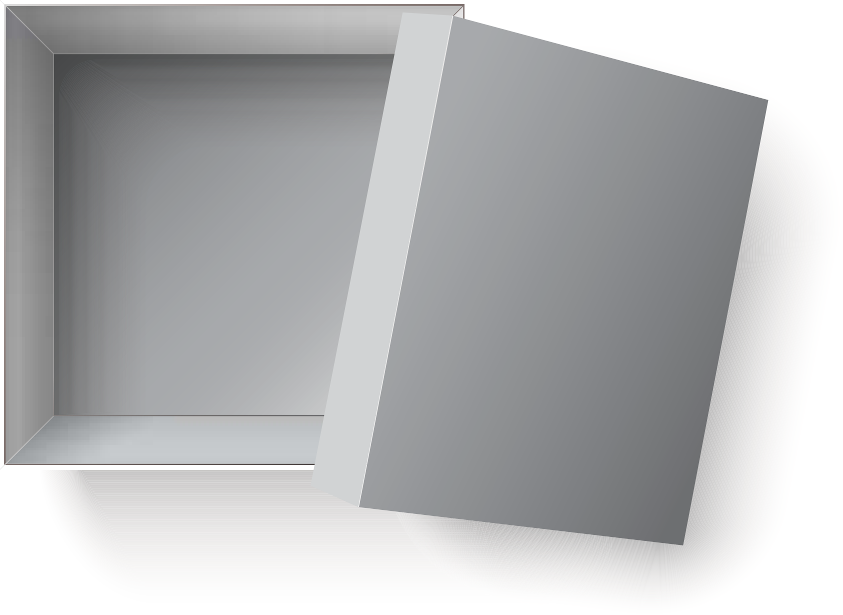


Gray Box Penetration Testing

During a gray box penetration test, the pen tester has partial knowledge or access to an internal network or web application. A pen tester may begin with user privileges on a host and be told to escalate their account to a domain admin. Or, they could be asked to get access to software code and system architecture diagrams.

The purpose of gray-box pen testing is to provide a more focused and efficient assessment of a network's security than a black-box assessment. Using the design documentation for a network, pen testers can focus their assessment efforts on the systems with the greatest risk and value from the start, rather than spending time determining this information on their own. An internal account on the system also allows testing of security inside the hardened perimeter and simulates an attacker with longer-term access to the network.

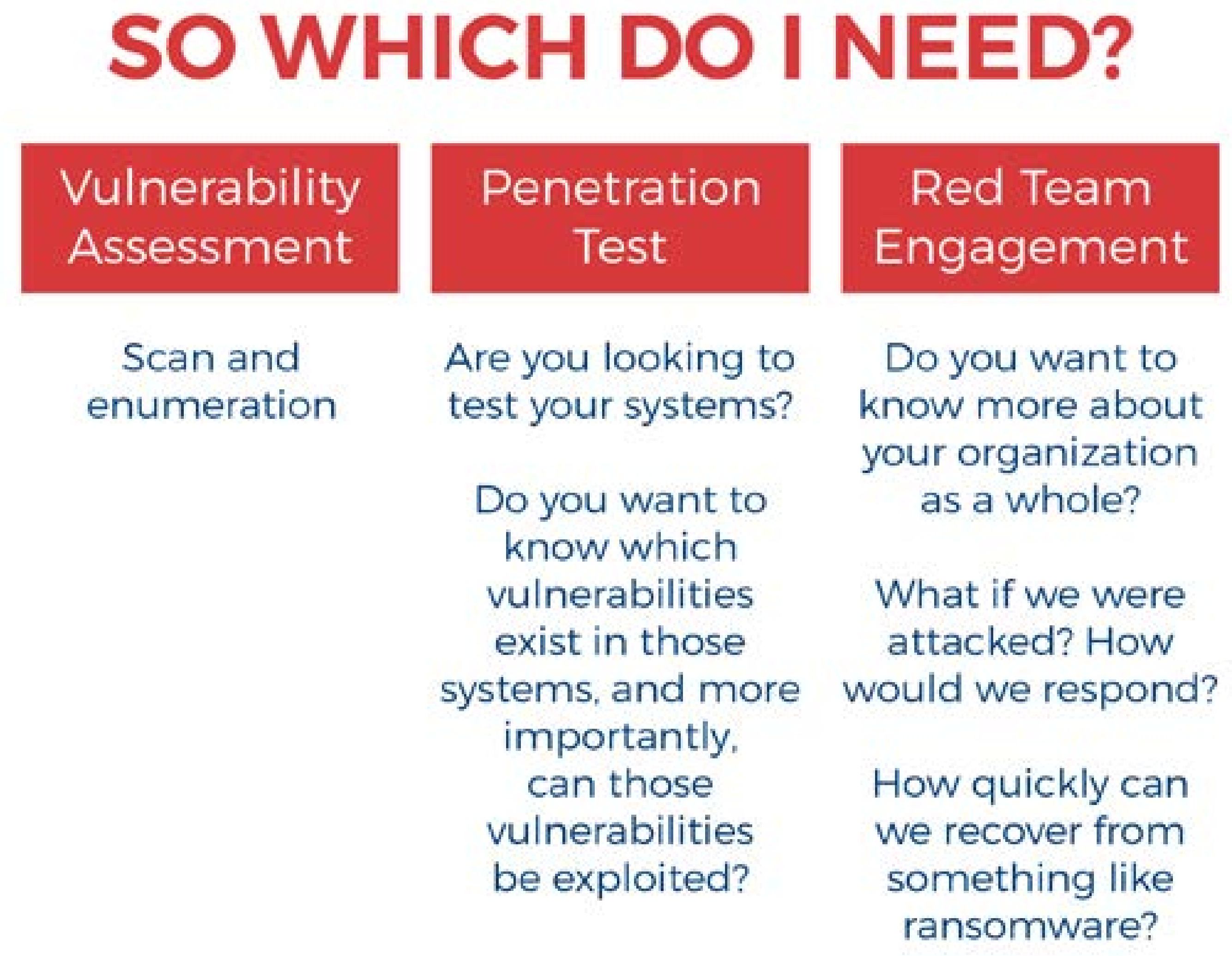
Gray-box testing splits the difference between white-box and black-box testing. Essentially by providing a pen tester with limited information about the target system, gray-box tests simulate the level of knowledge that a hacker with long-term access to a system would achieve through research and system footprinting.



Penetration Testing – Ethical Hacking, Red Teaming, Capture the Flag and Bug Bounty Programs

The variety of penetration tests that have surfaced over the past several years can easily be confused by organizations. The differences between penetration tests, ethical hacking, and red teaming are important to understand for IT security organizations seeking to evaluate their cybersecurity posture and performance.

Penetration testing is a common way for organizations to test their security maturity and identify potential vulnerabilities in their environment. In today's market, however, there are a growing number of options. The terminology surrounding penetration testing can be confusing to even the most educated cybersecurity professionals. With new types of testing available every year, it is important to know the latest and most effective ways of assessing cybersecurity performance. Commonly confused terms include penetration testing, ethical hacking, red teaming and capture the flag exercises.



SO WHICH DO I NEED?

Vulnerability Assessment	Penetration Test	Red Team Engagement
Scan and enumeration	Are you looking to test your systems? Do you want to know which vulnerabilities exist in those systems, and more importantly, can those vulnerabilities be exploited?	Do you want to know more about your organization as a whole? What if we were attacked? How would we respond? How quickly can we recover from something like ransomware?

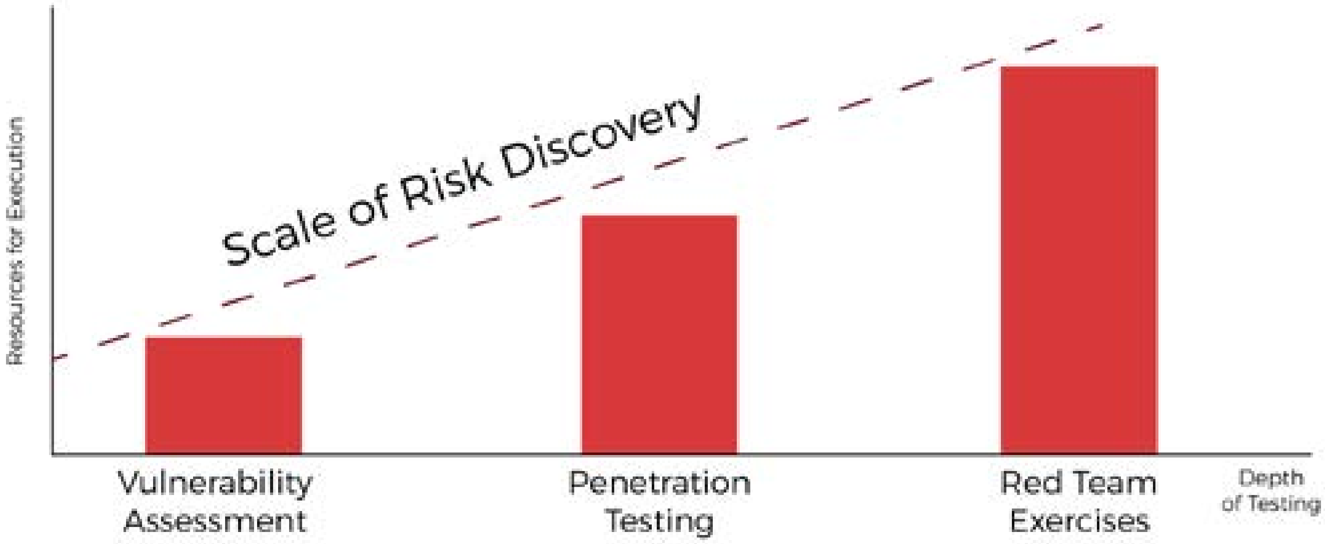
Penetration Testing – Ethical Hacking, Red Teaming, Capture the Flag and Bug Bounty Programs

What Is Red Teaming – A More Advanced Assessment Process
A red team assessment is another type of security testing tactic that is more defined and focused than penetration testing. The goal of a red team assessment is to test the target organizations detection and response capabilities. The main difference is the great lengths taken by the red team to simulate an actual attack.

Organizations are typically not informed of the test, and the red team proceeds to attempt to access critical and sensitive data leveraging a variety of attack methods; essentially simulating the tactics of an actual attacker. The assessments are usually a longer process and a more thorough investigation into security vulnerabilities and their corresponding impact. Methods may also be more extensive, including social engineering, wireless testing, and physical security testing.

Ultimately a Red Team Assessment is similar to a penetration test in many ways but is more targeted. The goal of the Red Team Assessment is NOT to find as many vulnerabilities as possible, rather, the goal is to test the organization's detection and response capabilities. The red team will try to get in and access sensitive information in any way possible, as covertly as possible.

Capture the Flag Penetration Test Exercises
Another penetration test-related exercise is a capture the flag (CTF) exercise. Testers are assigned a specific goal (capturing the flag), which might be exfiltrating a specific data file or accessing a specific system. CTF exercises are often set-up in a competition environment with teams competing to accomplish the goal first. Contests with prizes and open competition are often used to recruit new employees, build security skills, and test systems. CTF exercises are different from a traditional penetration test in that they often use test environments or third-party environments, like the Michigan Cyber Range, as the event is more of an evaluation of the testers' skills than production systems.



What's the Difference Between Penetration Testing and Ethical Hacking?

Penetration testing and ethical hacking are two similar types of cybersecurity testing that are often blurred. Penetration testing is a specific type of security testing assessment focused on identifying vulnerabilities and risks on systems and across an environment. A penetration tester assesses a target environment, seeking to compromise and take control of the targeted systems. The purpose of the test is to find vulnerabilities in the environment and deliver a report to the organization being tested. In many cases, the scope is not limited to systems or techniques – the penetration tester can direct his attack throughout the target organization's systems and infrastructure. Commonly, testers find systems on the targeted network using discovery scans and network traffic to identify potential weak links or systems that may be compromised. Attackers then exploit the systems remotely. The tests can be either internal (within the target's facility) or external (over the Internet).

Ethical hacking is similar to penetration testing but has several key differences. The term ethical hacking is a broader term for hacking techniques used by ethical hackers. While a penetration tester might discover flaws and vulnerabilities and deliver a report, an ethical hacker will likely conduct a longer-term assessment, using a greater variety of attack types and more fully exploring the environment.

What is a Bug Bounty Program?

Bug bounty programs are an emerging vulnerability management tactic to uncover unknown or zero-day vulnerabilities in software. Though not necessarily a type of penetration test, Facebook, and Google started offering hundreds of dollars to researchers able to identify critical vulnerabilities in their applications. Today, bug bounty programs are more popular than ever with the pen testing community and rewards have grown exponentially for individuals willing to put the time and effort into finding unique software flaws and other vulnerabilities.

Larger companies are now regularly offering six figure payouts for substantial findings, like Microsoft's bug bounty offering $100,000 for the discovery of critical vulnerabilities. Another growing trend is the offering of bug-bounty-as-a-service providers. Instead of working directly with the public, companies' partner with a crowd-sourced provider that makes it easy to start and manage a program while delivering the same results.

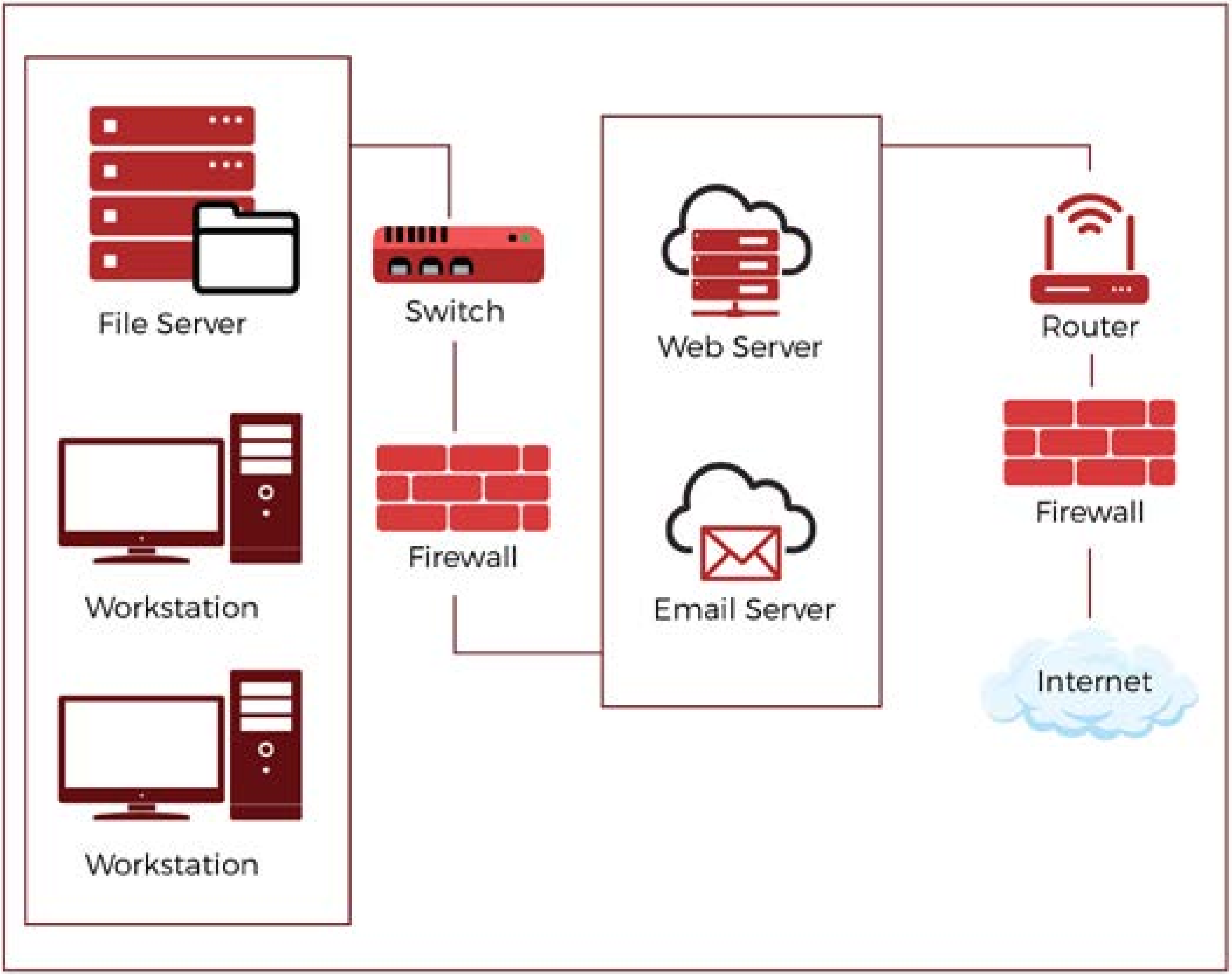
More testers and researchers are participating, and even potential ex-criminal hackers now participate in legitimate testing, drawn by the lucrative payouts for successful vulnerability discoveries. The list of participants is long and varied, and even the Department of Defense is now offering payouts for bug reports.

Network Service Penetration Testing

Network service penetration testing, or infrastructure testing, is one of the most common types of penetration testing performed.

The primary objective for a network penetration test is to identify exploitable vulnerabilities in networks, systems, hosts and network devices (ie: routers, switches) before hackers are able to discover and exploit them. Network penetration testing will reveal real-world opportunities for hackers to be able to compromise systems and networks in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.

The overall time it takes to complete a network penetration test depends on the size and complexity of the in-scope network(s). However, most tests take anywhere from one week to four weeks, start to finish.



How Does a Network Service Penetration Test Work?

There are 6 main steps to performing a network service penetration test including:

1. Planning – In this phase, pen testers review the network user documents, usage, specifications, and meet with teams to discuss goals and the approach. This information is later used to plan a set of test cases for performing the actual test.

2. Information Gathering – Next, the pen tester gathers information on network interfaces, APIs (application programming interfaces), user interfaces, accessible systems, services running on them and other input points. If any of these are not properly configured/designed, it can be a prime target of an attacker to access a network. In addition, the make and model of devices and operating systems in use provide attackers with insight as to how your network operates.

3. Identifying Vulnerabilities – Internal penetration tests often consists of scans, similar to a network vulnerability scan, with the goal of identifying weaknesses on a system.

4. Document Findings – Throughout this process the pen testing team documents this infor- mation in order to further plan their objective. This also makes writing the final report easier as the information is fresh and top of mind.

5. Perform Penetration Test – Only after weeks of planning will the actual test be carried out.

6. Reporting – Finally, a fact-based and objective report is provided to project stakeholders with prioritized findings, rankings, impact and actions for implementing counter-measures.

Essentially this six-step process can be applied to all types of penetration testing.

Why Should You Perform a Network Service Penetration Test?

Network penetration tests should be performed to protect your business from common network-based attacks including:

- Firewall Misconfiguration And Firewall Bypass
- IPS/IDS Evasion Attacks
- Router Attacks
- DNS Level Attacks:
    - Zone Transfer Attacks
    - Switching Or Routing Based Attacks
- SSH Attacks
- Proxy Server Attacks
- Unnecessary Open Ports Attacks
- Database Attacks
- Man In The Middle (MITM) Attacks
- FTP/SMTP Based Attacks

Given that a network provides mission-critical services to a business, it is recommended that both internal and external network penetration tests be performed at least annually. This will provide your business with adequate coverage to protect against these attack vectors.

External Network Assessment
Perimeter networks in almost every organization are attacked every day and even small external vulnerabilities can be damaging. External network penetration testing identifies vulnerabilities on infrastructure devices and servers accessible from the outside internet.

External penetration testing assesses the security posture of the routers, firewalls, Intrusion Detection Systems (IDS) and other security appliances which filter malicious traffic from the internet.

Internal Network Assessment
The benefit of an Internal Network Assessment in ensuring a breach of your external network will not result in a breach of your organizational assets. The local area network should be tested as if you have an insider threat or an attacker on the inside of the organization. Pen testers should look for privileged company information and other sensitive assets. This usually involves incorporating a variety of tools, uncovering user credentials, and attempting to compromise both virtual and physical machines present in the network environment.

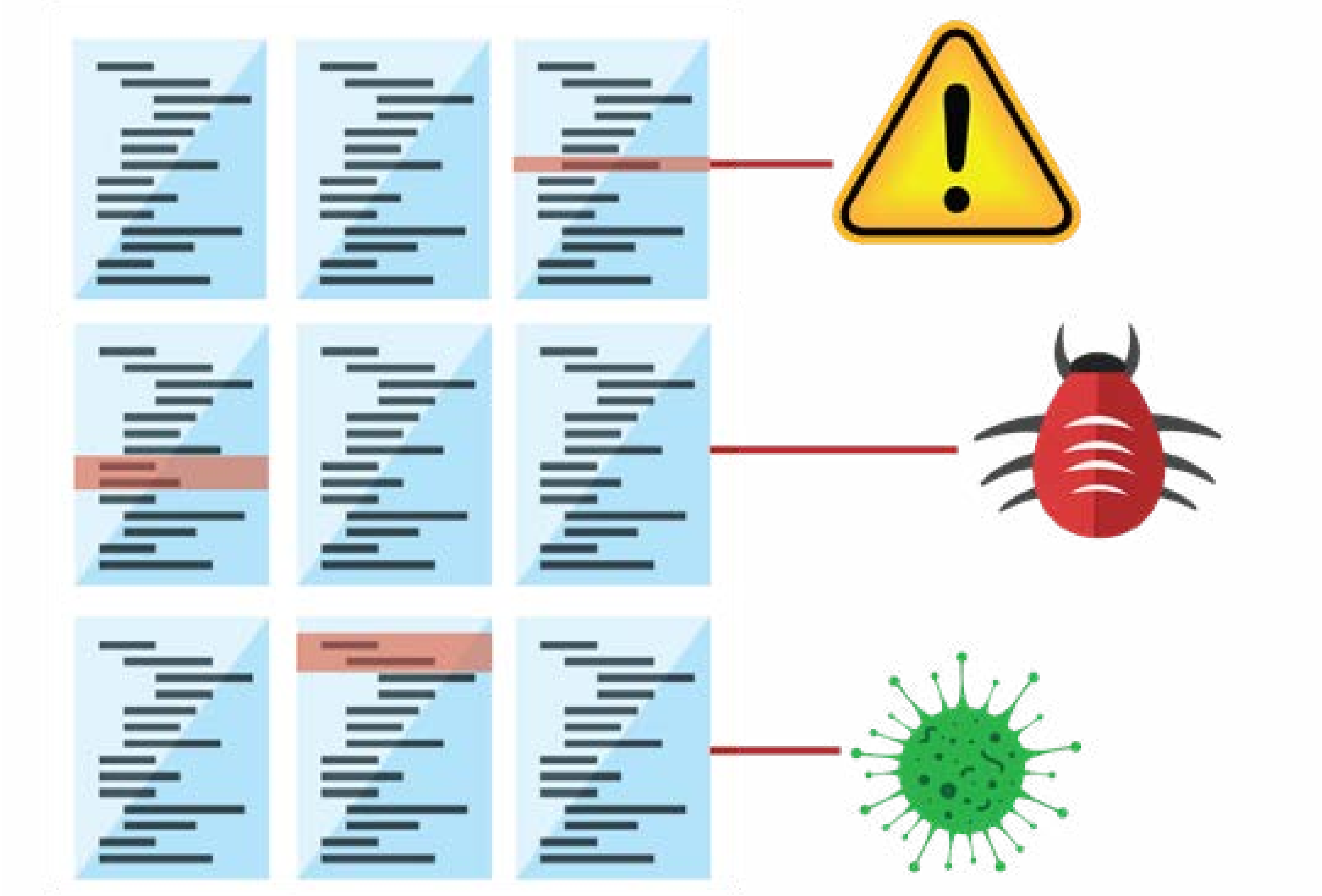
Web Application Penetration Testing

First, A Web application (Web app) is an application program that is stored on a remote server and delivered over the Internet through a browser interface. Web services are Web apps by definition and many, although not all, websites contain Web apps. Users can access a Web application through a web browser such as Google Chrome, Mozilla Firefox or Safari. Web application penetration testing is used to discover vulnerabilities or security weaknesses in web based applications. It uses different penetration techniques and attacks with aims to break into the web application itself.

The typical scope for a web application penetration test includes web based applications, browsers, and their components such as ActiveX, Plugins, Silverlight, Scriptlets, and Applets.

These types of tests are far more detailed and targeted and therefore is considered to be a more complex test. In order to complete a successful test, the endpoints of every web-based application that interacts with the user on a regular basis must be identified. This requires a fair amount of effort and time from planning to executing the test, and finally compiling a useful report.

The techniques of web application penetration testing are continuously evolving with time due to the increase in threats coming from web applications day by day.



How Does a Web Application Penetration Test Work?

As we suggested previously, penetration testers are trained to think with the attacker's perspective in mind. This allows them to attempt exploitations during the test in ways that an actual attacker might. As a result, applications are stress-tested for any known or previously undiscovered point of entry or vulnerability.

Pen testers may use any number of attacks to compromise an application including:

- Cross-Site Scripting Attacks – **40% of all Attacks**
- SQL Injection Attacks – **24% of all Attacks**
- Password Cracking Attacks
- DoS And DDoS Attacks
- Directory Traversal Attack
- Local File Inclusion
- Broken Authentication and Session Management Attacks
- File Upload Flaws
- Cross-Site Request Forgery Attacks
- Security Misconfigurations

Other test scenarios include:

- Deployment Management Testing
- Identity Management Testing
- Input Validation Testing
- Error Handling
- Cryptography
- Business Logic Testing

Why Should You Perform a Web Application Penetration Test?

Web applications are by far the most common method of compromise against e-commerce websites or really any company with an internet presence. A key reason to perform a web application penetration test is to identify security weaknesses or vulnerabilities within the web-based applications and its components like a database, source code, and the back-end network. It also helps by prioritizing the determined weak- nesses or vulnerabilities and provides possible solutions to mitigate them.

In software application development it's considered best practice to continuously improve the codebase although security is rarely considered a primary objective in the application development process. "Deploying a secure and agile code" is the phrase often used to describe this practice.

Agile code deployment is the preferred method over large batch deployments, as the more variables introduced into the code in a single deployment, the more opportunities there are to create bugs or errors leading to security vulnerabilities. As a result, a "technical debt" forms, where developers gradually spend more time implementing fixes to problems than they do improving the functionality of the software by developing new features or updates.

In contrast, agile methodologies use a sandbox environment or copy of the codebase in a clean testing environment to test code functionality and usability prior to launching the software into production. If the initial deployment is unsuccessful, developers can easily single out issues and roll the code back to previous version history. The problem with application development up until now is that that security has not been considered with daily code deployment.

Client Side Penetration Testing

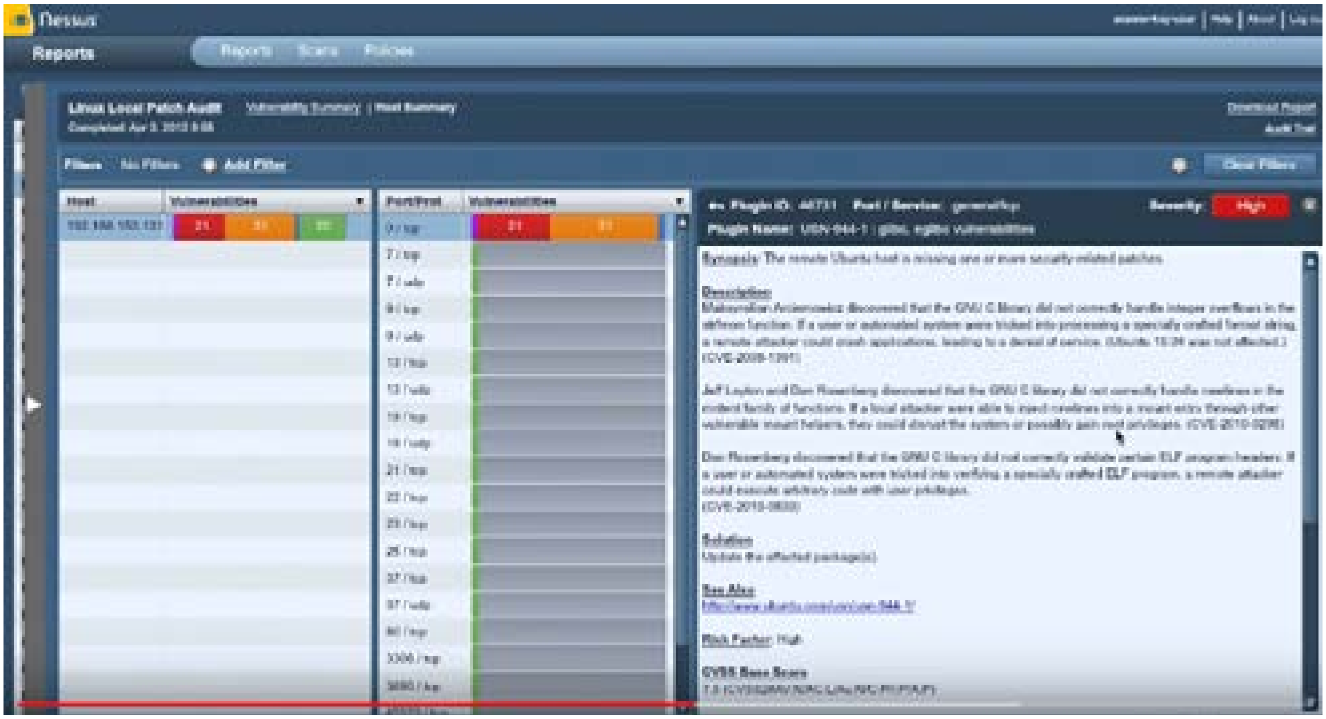
Client-side penetration testing, also known as internal pen testing, is the act of trying to exploit vulnerabilities in client-side application programs such as an email clients like Microsoft Outlook, web browsers (i.e. Chrome, Firefox, Safari, etc.), Macromedia Flash, Adobe Acrobat and others.

Client-side penetration tests are similar in goals to other penetration tests and are performed to answer the following questions:

- How reliable is the security posture of an organization through client-side apps?
- Are there any vulnerabilities in these apps? (Most of these apps do have vulnerabilities)
- What harm can an attacker do by exploiting these vulnerabilities?
- How can a malicious actor exploit a vulnerability?
- Are the access rights and privileges for employees set correctly? (This is critical to understanding how an attack may move through an organization)
- How can the detected weak points be remediated quickly and cost effectively?

How Does a Client Side Penetration Test Work?

Pen testers run a network vulnerability scan as part of a penetration test to identify and categorize applications at risk.



Plugin ID: 46731 Port / Service: general/tcp

Plugin Name: USN-944-1 : glibc, eglibc vulnerabilities

Synopsis: The remote Ubuntu host is missing one or more security-related patches.

Description:
Maksymilian Arciemowicz discovered that the GNU C library did not correctly handle integer overflows in the strfmon function. If a user or automated system were tricked into processing a specially crafted format string, a remote attacker could crash applications, leading to a denial of service. (Ubuntu 10.04 was not affected.) (CVE-2008-1391)

Jeff Layton and Dan Rosenberg discovered that the GNU C library did not correctly handle newlines in the mntent family of functions. If a local attacker were able to inject newlines into a mount entry through other vulnerable mount helpers, they could disrupt the system or possibly gain root privileges. (CVE-2010-0296)

Dan Rosenberg discovered that the GNU C library did not correctly validate certain ELF program headers. If a user or automated system were tricked into verifying a specially crafted ELF program, a remote attacker could execute arbitrary code with user privileges.
(CVE-2010-0830)

Solution:
Update the affected package(s).

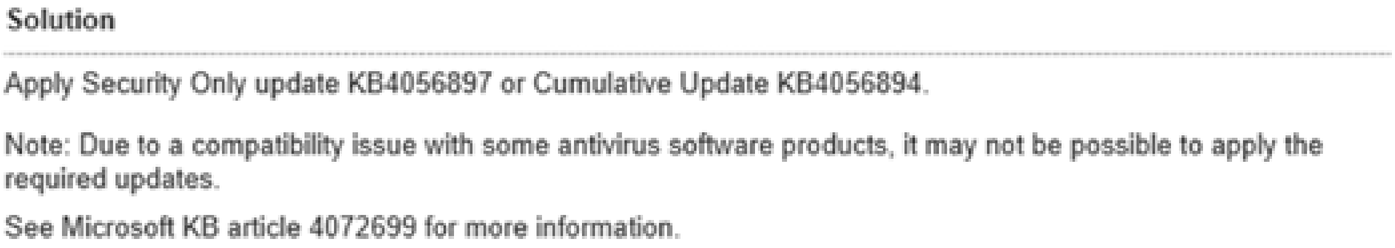
See Also:
http://www.ubuntu.com/usn/usn-944-1/

Risk Factor: High

CVSS Base Score:
7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

The image above shows a Nessus scan of vulnerabilities found on a host. The issue here is that the host is missing a variety of security updates for several application and that without updates through patches the host is vulnerable to an attack.

The scanner also lists the Common Vulnerabilities Exposures (CVE) for each vulnerability.



Solution

Apply Security Only update KB4056897 or Cumulative Update KB4056894.

Note: Due to a compatibility issue with some antivirus software products, it may not be possible to apply the required updates.

See Microsoft KB article 4072699 for more information.

The scan will recommend applying an update or patch as you see above to resolve the vulnerability. The pen tester doesn’t typically apply patches but rather exploits vulnerabilities to gain entry to your network and systems.

Why Should You Perform a Client Side Penetration Test?

As we suggested, a client-side vulnerability often takes the form of unpatched software on a desktop or laptop. Depending on the nature of the vulnerable application, an attacker could exploit it using a malicious email attachment or by convincing the user to visit a malicious Web site; yes, this is a phishing attack.

When assessing your organization's exposure to such threats via client-side penetration testing, you should mimic two common scenarios:

- Attackers targeting specific employees with messages carrying malicious payload or by pointing the victim to a malicious Web site.
- Large-scale client-side infection campaigns that rely on victims to visit compromised Web sites that deliver client-side exploits, possibly through malicious banner ads.

Client-side tests are performed to identify specific cyber-attacks including:

- Cross-Site Scripting Attacks
- Clickjacking Attacks
- Cors-Origin Resource Sharing (CORS)
- Form Hijacking
- HTML Injection
- Open Redirection
- Malware Infection

Wireless Penetration Testing

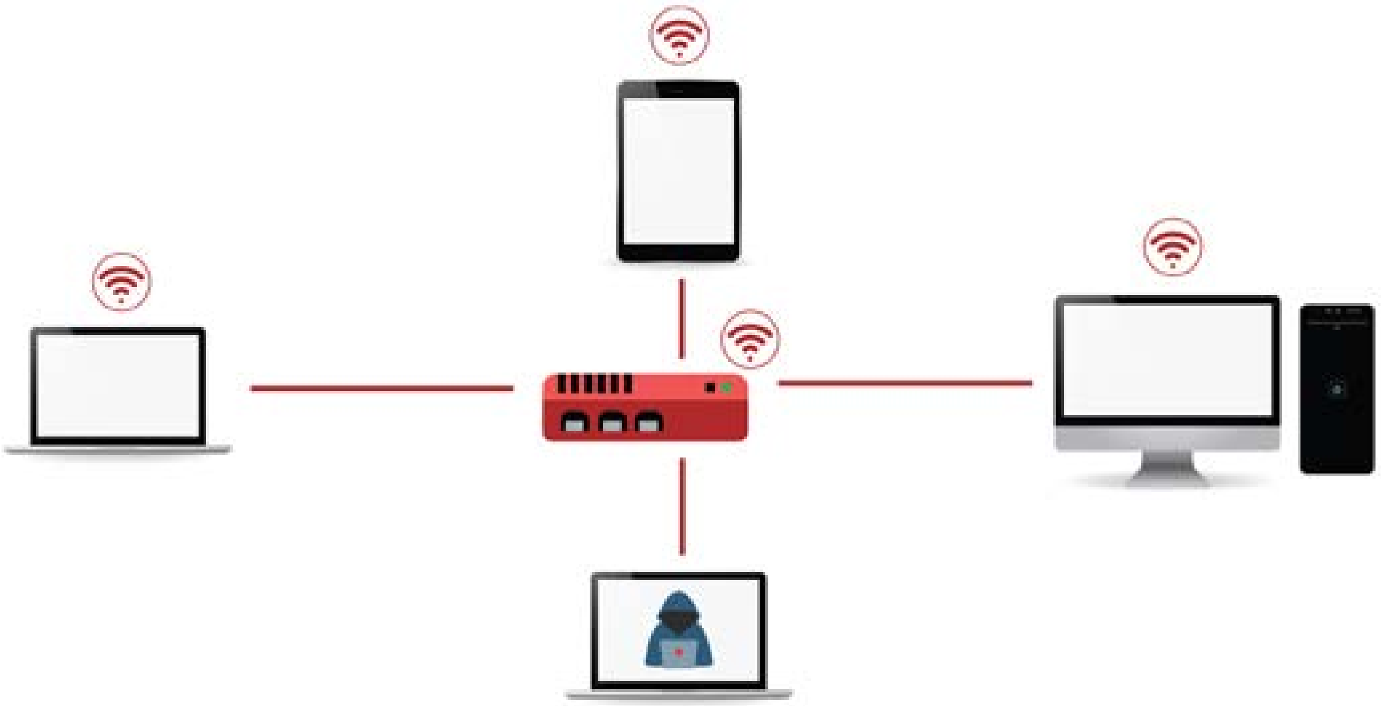
Many organizations continue to overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now ubiquitous in executive suites, financial departments, government offices, retail, and frankly almost everywhere nowadays.

Wireless penetration testing involves identifying and examining the connections between all devices connected to the business's WiFi. These devices include laptops, tablets, smartphones, and any other internet of things (IoT) devices.

For many pen testers, "wireless" was once synonymous with "Wi-Fi," the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning -- not only encompassing the security of Wi-Fi systems, but also the security of Bluetooth, Zigbee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even other proprietary wireless systems.

The testing of wireless networks generally includes:

- Wi-Fi network identification, including wireless fingerprinting, information leakage and signal leakage.
- Determine encryption weaknesses, such as encryption cracking, wireless sniffing and session hijacking.
- Identifying vulnerabilities to penetrate a network by using wireless or evading WLAN access control measures.
- Identify legitimate user identities and credentials to access otherwise private networks and services.



How Does a Wireless Penetration Test Work?

Wireless attacks have become a very common security issue when it comes to networks. This is because such attacks can really get a lot of information that is being sent across a network and use it to commit some crimes in other networks. Every wireless network is vulnerable to such kinds of attacks and it is therefore important that all the necessary security measures are taken to prevent the data leakage that can be caused by such attacks.

One of the most important phases of a wireless penetration test is the information-gathering phase. For example, an access point could still be using default credentials that the device shipped with. If the attacker knows the make and model of the device, then they can deploy a wireless attack to take down or access the network.

Next, the pen tester identifies vulnerabilities in the discovered hardware, checks the Wi-Fi signal strength beyond the organization's physical area, and checks the visible nodes in the Wi-Fi network. As a result, this will map any workstation, server or other devices publicly visible and accessible in the network.

Examples of wireless penetration testing attacks include:

- Bypassing WLAN Authentication – Shared Key, MAC Filtering, Hidden SSIDs
- Cracking WLAN Encryption – WEP, WPA/WPA2 Personal and Enterprise, Understanding encryption based flaws (WEP,TKIP,CCMP)
- Attacking the WLAN Infrastructure – Rogues Devices, Evil Twins, DoS Attacks, MITM, Wi-Fi Protected Setup
- Advanced Enterprise Attacks – 802.1x, EAP, LEAP, PEAP, EAP-TTLS
- Attacking the Wireless Client – Honeypots and Hotspot attacks, Caffe-Latte, Hirte, Ad-Hoc Networks and Viral SSIDs, WiFishing
- Breaking into the Client – Metasploit, SET, Social Engineering
- Enterprise Wi-Fi Worms, Backdoors and Botnets

Why Should You Perform a Wireless Penetration Test?

Poorly secured WiFi networks are targeted by more sophisticated cybercriminals and organized crime groups to gain a foothold in the network. The attacks are among the most lucrative. Access to a business network can allow ransomware to be installed and if malware can be installed on POS systems, the credit/debit card numbers of tens or hundreds of thousands of customers can be stolen.

Also, cybercriminals may use a rogue wireless device, or access point. This is an unauthorized WiFi device added onto the network that isn't under the management of the network admins. They allow potential attackers a gateway into the network.

This sort of device can be maliciously installed if the attacker has direct access to the wired network, but more often than not they are added by staff that are not aware of the implications.

Another wireless hack technique is "Spoofing" a WiFi network, which simply means copying it, which can create an "Evil Twin." This is a network that looks and behaves identically, or at least similarly, to a legitimate network. If the attacker sets up a router with the same name and password as one of your habitual networks, you probably won't give it a second thought when you connect, or your computer connects automatically.

There are dozens of wireless attacks like those described above that could compromise your network, systems and data. Conducing a pen test to uncover common vulnerabilities will eliminate another attack vector and reduce your overall attack surface.

Before performing a wireless penetration test you should consider the following:

- Have all access points been identified and how many use poor encryption methods?
- Is the data flowing in and out of the network encrypted and if so, how?
- Are there monitoring systems in place to identify unauthorized users?
- Is there any possibility the IT team could have misconfigured or duplicated a wireless network?
- What are the current measures in place to protect the wireless network?
- Are all wireless access points using WPA protocol?

Social Engineering Tests

Social engineers are the type of hackers who exploit the one weakness that is found in almost every organization: human behavior and psychology. Using a variety of media, including phone calls, social media, and predominately e-mail these attackers trick people into providing access to sensitive data or other company assets.

The Verizon 2019 Data Breach Investigations Report (DBIR) found e-mail phishing to be the top threat action variety in all breaches analyzed. Phishing, spear phishing, whaling and other forms of e-mail attacks have dominated the cybercrime landscape for the past several years. According to the Verizon report over 70% of all cyber-attacks start with a phishing scam. Unsuspecting employees are sent an e-mail with a malicious attachment or malicious link and because they are not trained at spotting the scams open the attachment or click on the link unleashing the malware into corporate systems.

Social engineering tests are where a malicious actor attempts to persuade or trick users into giving them sensitive information, such as a username and password.

Common types of social engineering tests used by pen testers include:

- Phishing, Spear phishing, and Whaling Attacks
- Tailgating
- Imposters who pose as company employees, 3rd party vendors, or partners
- Name Dropping
- Pre-texting
- Dumpster Diving
- Eavesdropping

How Does a Social Engineering Test Work?

What is phishing exactly? Most phishing scams demonstrate the following characteristics:

- Seek to obtain personal information, such as names, addresses and social security numbers.
- Use link shorteners or embed links that redirect users to suspicious websites in URLs that appear legitimate.
- Use attachments like Microsoft Word or Excel often from e-mail addresses that appear trusted.
- Incorporates threats, fear and a sense of urgency in an attempt to manipulate the user into acting promptly.

Some phishing emails are more poorly crafted than others to the extent that their messages sometimes intentionally have spelling and grammar errors in order to target poorly trained users.

Social engineering penetration testing is the practice of attempting typical phishing or other social engineering scams on an organization's employees to understand the level of vulnerability to this type of attack. Social engineering pen testing is ultimately designed to test employees' compliance to the security policies and practices defined by management.

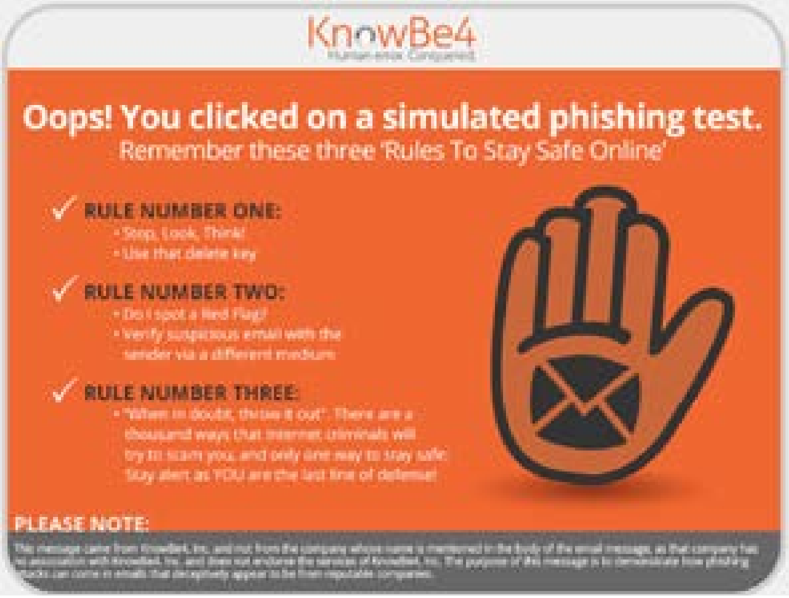
Why Should You Perform Social Engineering Tests?

According to Verizon and other recent report, 98% of all cybercrime rely on some form of social engineering to initiate the scam. As we suggested prior, this is because employee errors including opening malicious attachments and clicking malicious links are the most significant threat to an organization's security. No matter how good the cybersecurity technology is in an organization, human error can help cybercriminals circumvent even the best defenses.

Social engineering tests and awareness programs have proven to be the most effective steps an organization can take to prevent being breached.

An excellent social engineering and email phishing platform, KnowBe4, simulates an email phishing attack. When the user clicks on the malicious link they're taken to a page that informs them that it was a phishing test…and they failed.

Remediation training is then provided to help inform users on the most current phishing attacks and how to avoid them.



Oops! You clicked on a simulated phishing test.

Remember these three 'Rules To Stay Safe Online'

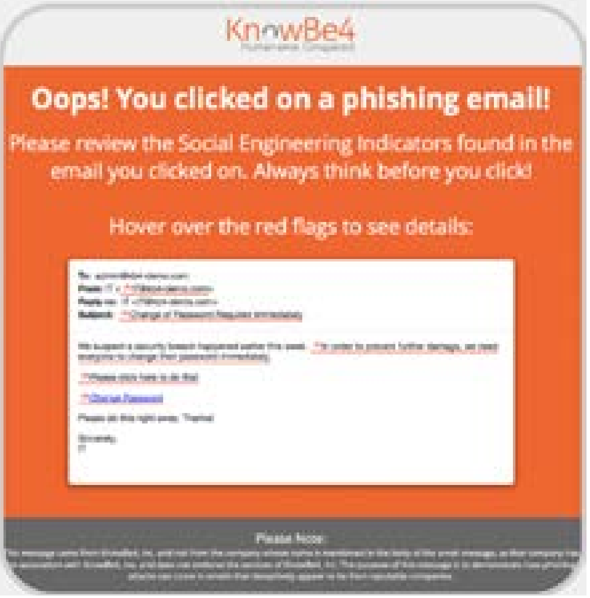
✓ RULE NUMBER ONE:
- Stop, Look, Think!
- Use that delete key

✓ RULE NUMBER TWO:
- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium

✓ RULE NUMBER THREE:
- "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: Stay alert as YOU are the last line of defense!

PLEASE NOTE:

This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.



Oops! You clicked on a phishing email!

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

To: admin@kb4-demo.com
From: IT <IT@kb4-demo.com>
Reply-to: IT <IT@kb4-demo.com>
Subject: Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that:

Change Password

Please do this right away. Thanks!

Sincerely,
IT

Please Note:

This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

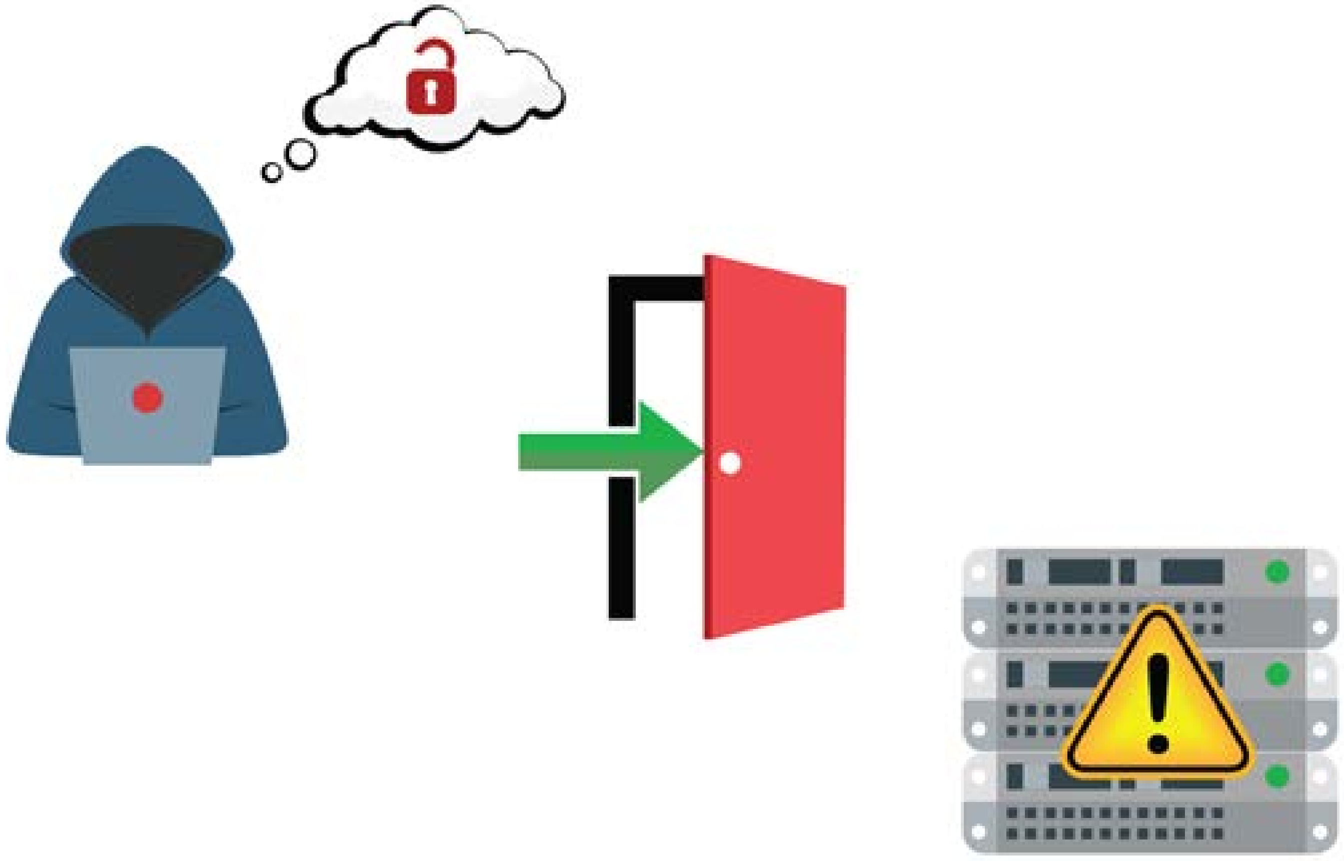
Physical Penetration Testing

Just like a penetration test on IT infrastructures or systems, physical penetration testing, or physical intrusion testing, will uncover real-world opportunities for malicious insiders or cybercriminals to be able to compromise physical barriers (ie: locks, sensors, cameras, keypads, mantraps) in such a way that allows for unauthorized physical access to sensitive areas leading up to data breaches and system/network compromise.

This type of test is an attack simulation carried out by security consultants trained in physical security control to:

- Test perimeter security including alarms, motion detectors, security guards, and other physical and electronic barriers
- Identify physical security control flaws present in the environment
- Understand the level of real-world risk for your organization
- Help remediate physical security vulnerabilities

The overall time to complete a physical pen test depends on the size and complexity of the in-scope facilities. That said, most tests take anywhere from two weeks to six weeks, start to finish. In general, the number of locations, number of physical barriers tested and the objective will ultimately determine the cost.

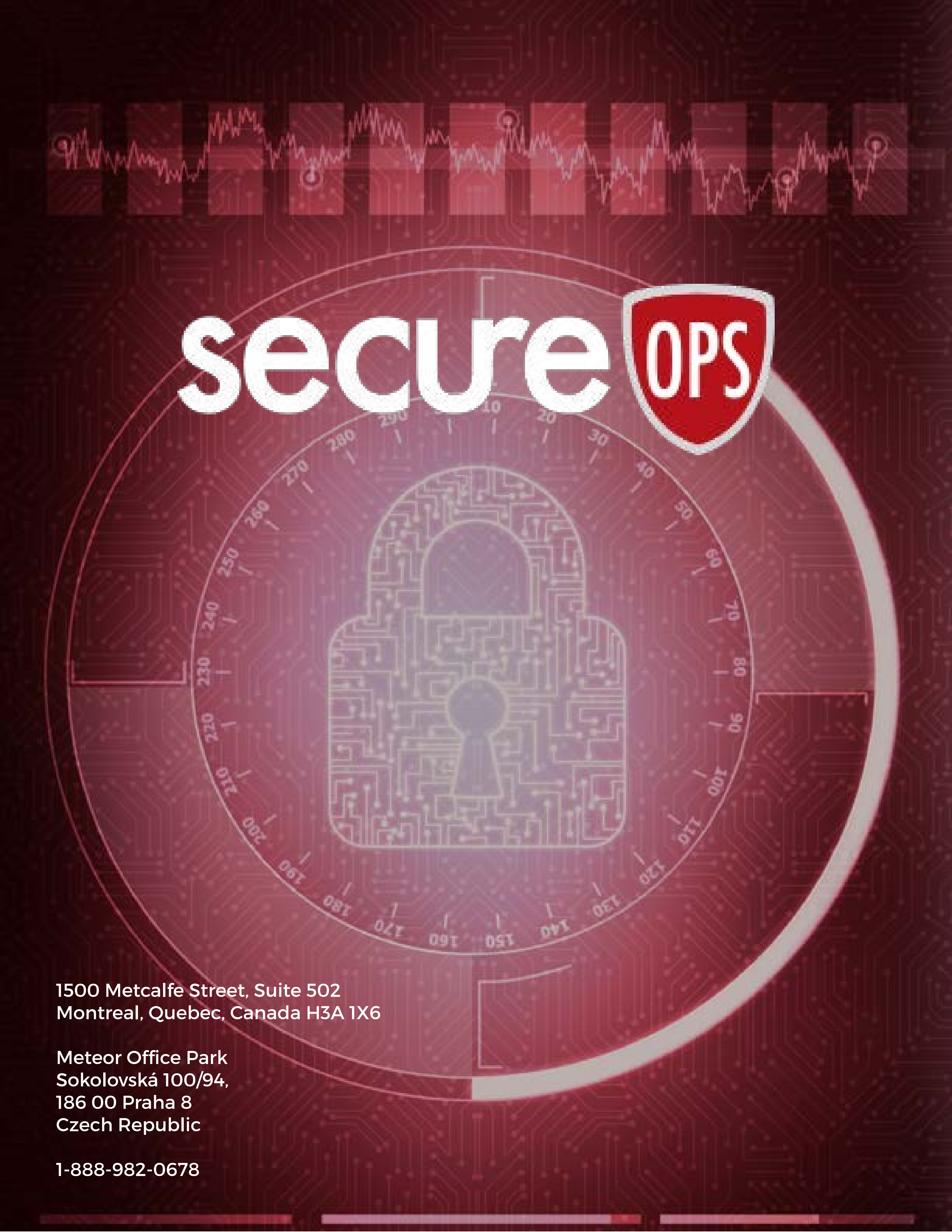


How Does a Physical Penetration Test Work?

Physical security is an often-overlooked component of data and system security. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. Organizations can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

Pen testers use any number of methods during a physical penetration test including:

- Mapping The Entrances An Perimeter
- Lock Picking Entry Points
- Remotely Accessing Sensitive Information
- Targeting Server Rooms, Wires, Or Cables
- Exploiting Fire And Cooling Systems
- Intercepting EM Waves
- Dumpster Diving
- Breaking RFID Tag Encryption
- Tailgating
- Accessing Unprotected Network Jacks
- Checking Rooms For Unattended Devices
- Shoulder Surfing
- Social Engineering



secure OPS

1500 Metcalfe Street, Suite 502
Montreal, Quebec, Canada H3A 1X6

Meteor Office Park
Sokolovská 100/94,
186 00 Praha 8
Czech Republic

1-888-982-0678