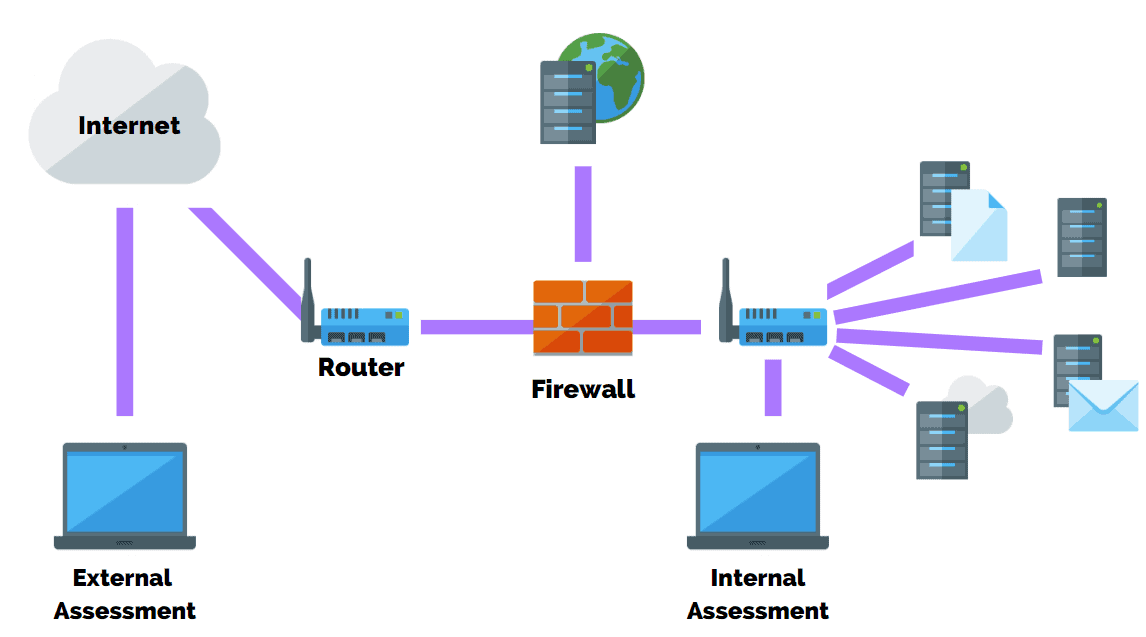
## INTRODUCTION

A penetration test, or pen test, is an effort to assess the security of an IT infrastructure by exploiting vulnerabilities in a controlled manner. These vulnerabilities may be caused by flaws in operating systems, services, and applications, improper settings, or risky end-user conduct. Such evaluations are also helpful for validating the effectiveness of defensive mechanisms and end-user compliance with security policies.

Typically, penetration testing employs manual or automated techniques to compromise servers, endpoints, web apps, wireless networks, network devices, mobile devices, and other possible entry points. Once vulnerabilities have been successfully exploited on a particular system, testers may attempt to use the compromised system to launch subsequent exploits against other internal resources, specifically by attempting to achieve incrementally higher levels of security clearance and deeper access to electronic assets and information via privilege escalation.



<https://purplesec.us/wp-content/uploads/2020/10/what-is-a-penetration-test.png>

Information about any security vulnerabilities effectively exploited during penetration testing is typically compiled and presented to IT and network system managers in order to assist these pros in drawing strategic conclusions and establishing remediation priorities. The primary objective of penetration testing is to evaluate the likelihood of system or end-user compromise and the potential impact of such incidents on the affected resources and activities.

It may be useful to think of penetration testing as attempting to break into your own home to determine if someone else can. Penetration testers, also known as ethical hackers, assess the security of IT infrastructures by attacking, identifying, and exploiting vulnerabilities in a controlled environment. Instead of examining the windows and doors for weaknesses, they evaluate servers, networks, web applications, mobile devices, and other possible entry points.

Pen testing is a proactive cybersecurity measure because it entails consistent, self-initiated changes based on the test's reports. This contrasts with reactive methods, which do not address emerging weaknesses. An example of a nonproactive approach to cybersecurity would be a business updating its firewall after a data breach has occurred. Proactive measures, such as pen testing, aim to minimise the number of retroactive upgrades and optimise the security of a company.

## DIFFERENCE BETWEEN VULNERABILITY AND PENETRATION TEST

# Penetrating Evaluations

## Penetration testing mimics the actions of an external or internal cyber attacker/s whose objective is to breach information security, steal sensitive data, or disrupt the normal operations of the organisation. Therefore, a penetration tester (also known as an ethical hacker) employs sophisticated tools and techniques to attempt to control vital systems and obtain access to sensitive data.

# Risk Assessment

## A vulnerability assessment, on the other hand, is the process of discovering and quantifying security vulnerabilities in a particular environment. It is a comprehensive assessment of the computer security situation (result analysis). In addition, it identifies possible vulnerabilities and provides the appropriate mitigation measures (remediation) to remove or reduce these vulnerabilities below the risk threshold.

## NECESSITY OF PENETRATION TESTING

## Before discussing why a Penetration Test is essential, it is necessary to understand when to conduct one. Vulnerability Testing is not a one-time event and should be conducted regularly. In addition, it is recommended to conduct a Penetration Test whenever the following occurs:

## When your business physically relocates or adds a new network location.

## When installing security patches.

## When required by IT Governance and regulatory compliance requirements.

## The following are the necessities of penetration testing:

# 1. To Recognize and Fix Vulnerabilities

## It is typical for bugs and security flaws to manifest during the creation and implementation of an enterprise-wide system or network. Hackers who stay on the cutting edge of technology and rely on their experience to exploit known flaws in these systems can exploit these vulnerabilities.

## You can hire us (VISTA InfoSec) to perform a thorough Pen Test on your system and identify vulnerabilities. The test would consist of finding vulnerable systems that could allow for a full takeover of your network or bypassing security mechanisms to gain access to administrative features in your application.

## These skilled pros will provide your team with a hacker's perspective and aid in the identification of vulnerabilities that could be exploited by hackers. Moreover, they implement an optimised method for addressing the vulnerabilities while keeping normal operations.

# 2. To comply with multiple Regulatory Rules

## Organizations are needed, for legal and business purposes, to comply with an assortment of industry-specific regulatory requirements. For instance, if you desire to accept payments from customers using a credit or debit card system, you must be PCI compliant, which requires an annual Penetration Test.

## If you are a SaaS provider, your clients or partners may require a Penetration Test of your SaaS application. This helps identify potential vulnerabilities, safeguards your clients and assets, and allows you to maintain compliance. Compliance enables you to continue conducting business and establishing new partnerships to grow your company without incurring fines or encountering legal issues.

# 3. To minimise Network downtime and Remediation Expenses

## The process of recovering from a security breach can be time-consuming and costly, as your business may become inoperable and accrue ongoing expenses. According to a study by IBM, the average cost of a data breach in 2020 will be $3.86 million, and the average time to discover a breach will be 207 days.

## In contrast, a Penetration Test is proactive and identifies high-risk exploitable weaknesses in your system. To ensure business continuity, it is recommended that organisations perform regular Penetration Tests at least once or twice per year.

# 4. To Implement Efficient Security Devices

## A Penetration Test provides valuable information to your business regarding identified security gaps and their present and potential impact on the system's functionality and performance. An experienced Penetration Tester will provide you with a list of suggestions outlining the issue's severity and the deadline for its resolution. In addition, they will help you create a reliable information security system to objectively prioritise future cybersecurity investments.

## Choose a reputable and experienced company for your Penetration Tests because, despite the use of automated tools, the focus is still on manual skills, making the expert knowledge and experience of Penetration Testers the most valuable asset.

# 5. Assist in the acquisition of new companies and create a plan for enhancements.

## The Penetration Test aids in the purchase of new businesses. The acquisition of a new business necessitates the purchase of a new IT network, which introduces a number of potential security flaws. Any vulnerabilities in the other company's security are now vulnerabilities in your system.

## Prior to the merging of systems and the transfer of data, it is advisable to conduct a Penetration Test to identify and monitor any issues that need to be resolved. Some vulnerabilities may be instantly reparable, whereas others may take time. With the information gleaned from the Pen Test, you can make an informed choice and build a road map with clear dates for when the vulnerability will be patched and the technicians responsible for the fix. This makes the difficult process of merging two organisations a little less cumbersome.

# 6. Protect your organisation from cyberattacks and tell management

## In 2019, 88% of global organisations encountered spear-phishing attempts, according to Proofpoint research. This research by RiskBased Security indicates that data breaches exposed 36 billion records in the first half of 2020.

## With countless new methods for attackers to target and breach organisations being discovered on a daily basis, even large organisations with well-established cybersecurity teams and hygiene practices are becoming increasingly cautious. Penetration Testing finds the vulnerabilities that hackers are most likely to exploit, along with the potential consequences of those exploits.

## Even if your IT team understands these vulnerabilities, they may lack the experience or expertise to effectively convey this information to higher management, or management may choose to ignore this information. Consequently, they may not allocate the necessary resources to execute corrective measures or make the required modifications to safeguard your vulnerable systems and applications.

## A Pen Test, on the other hand, involves collaborating with experts whose job it is to grasp the impact of cybersecurity risks on your organisation. At the end of the test, management receives a detailed report describing each vulnerability and its potential consequences if exploited.

## It also contains an executive summary that describes the risks and vulnerabilities in language that non-technical stakeholders can understand. Therefore, management will be better equipped to understand and execute effective cybersecurity measures.

## THE STAGES OF PENETRATION TESTING

 These six stages are essential for the planning and execution of a successful penetration test. Discover more about each step of penetration testing in the sections that follow.

Diagram

Description automatically generated

<https://cdn2.hubspot.net/hubfs/3402809/Stages%20of%20Penetration%20Testing.png>

# Interactions Prior to Involvement

Pre-engagement encounters or scoping are an often-overlooked phase of penetration testing. In this preliminary stage, a penetration testing firm will detail the test's setup, what to anticipate from it, any potential legal ramifications, and the customer's stated goals and expectations.

During the Pre-Engagement phase, penetration testers should collaborate with your organisation to completely comprehend any risks, your organisational culture, and the most effective pentesting strategy. A white box, black box, or grey box intrusion test may be necessary. This phase involves planning and aligning your objectives with particular penetesting outcomes.

# OSINT or Open Source Intelligence (OSINT) Collection

Open Source Intelligence (OSINT) or reconnaissance is a crucial first stage in penetration testing. A penetration tester gathers as much information as possible about your company and potential exploit targets.

Depending on the sort of pentest you choose, your penetration tester may have varying degrees of knowledge about your company or may be required to independently identify key information in order to find vulnerabilities and entry points in your environment.

Common intelligence collection methods include: • Search engine inquiries • Domain name/WHOIS lookups

• Social Planning • Fiscal Documents

• Internet Footprinting — including email addresses, passwords, and social networks

• Internal Footprinting — Ping scans, port scanning, reverse DNS, and packet sniffing

A pentester employs a comprehensive checklist to locate open entry points and vulnerabilities within a company. The OSINT Framework offers an abundance of knowledge regarding open information sources.

# Simulation of threats and vulnerability identification

During the phase of threat modelling and identifying vulnerabilities, the tester finds targets and maps attack vectors. Information gathered during the reconnaissance part is used to inform the penetration test's attack strategy.

• Business assets – recognise and categorise high-value assets • Employee data • Customer data • Technical data • These are the most frequent areas that a pentester will map and find.

• Dangers - Identify and classify internal and exterior dangers

• Internal threats – Administration, personnel, suppliers, etc.

• External dangers, including ports, network protocols, web applications, network traffic, etc.

Frequently, a penetration tester will use a vulnerability scanner to find and inventory the security risks posed by identified vulnerabilities. The penetration tester will then determine whether the vulnerability is accessible. At the conclusion of the pentest, the list of vulnerabilities is shared during the reporting process.

# Fraud

The pentester starts testing the exploits discovered within your network, applications, and data after creating a map of all potential vulnerabilities and entry points. The objective of the ethical hacker is to determine how deeply they can penetrate your network, find high-value targets, and remain undetected.

If you created a scope at the outset, the pentester will only go as far as the agreed-upon parameters established during the initial scoping. You may specify in your scope, for instance, that you will not pentest cloud services or conduct a zero-day assault simulation.

Web Application Attacks, Network Attacks, Memory-based Attacks, and Wi-Fi Attacks are a few of the most common hacking techniques.

• Zero-day vulnerability • Bodily assaults • Social engineering

In addition to reviewing and documenting how vulnerabilities are exploited, the ethical hacker will describe the techniques and strategies used to gain access to high-value targets. Lastly, during the exploitation process, the ethical hacker must provide a detailed explanation of the exploit's impact on high-value targets.

# Risk Analysis and Suggestions Following Exploitation

After the exploitation phase is complete, the objective is to record the methods used to gain access to the valuable information of your organisation. The penetration tester must be able to determine the worth of compromised systems and the value of any sensitive data captured.

Some penetration testers are unable to quantify the impact of data access or provide remediation suggestions for the environment's vulnerabilities. Request a sanitised penetration testing report that includes clear suggestions for fixing security holes and vulnerabilities.

After the final suggestions from the penetration test have been made, the tester should clean up the environment, reconfigure any access he or she obtained to penetrate the environment, and take any other necessary measures to prevent future unauthorised access to the system.

Some common ways to clean up are:

* Deleting all executables, scripts, and temporary files from compromised systems
* Reconfiguring settings to their original values prior to the pentest
* Deleting any rootkits installed in the environment
* Deleting any user accounts created to connect to the compromised system.

# Retest

Penetration testing can and should be employed frequently, particularly when deploying new applications or infrastructure. Even if your organisation thinks it has remedied every vulnerability identified in a previous report, retesting is the best way to ensure that your remediations are effective. In addition, IT environments and attack methods are continuously evolving, so it is reasonable to anticipate the emergence of new vulnerabilities.

With so many data breaches dominating the news, it is more important than ever to reduce the likelihood that an incident could jeopardise the image and credibility of your company. Organizations should make every effort to recognise and avoid behaviors that place them at risk. Pen testing is an integral component of a risk assessment strategy and ensures that your organisation reduces the likelihood of a damaging security breach happening within its environment.

# Reporting

Reporting is frequently considered to be the most important element of a pentest. It is where you will receive written recommendations from the penetration testing firm and have the chance to review the report's findings with the ethical hacker (s).

The report's findings and explanations will provide you with insights and opportunities to greatly enhance your security posture. The report should detail precisely how entry points were discovered during the OSINT and Threat Modeling phases, as well as how security issues revealed during the Exploitation phase can be remedied.

## HOW OFTEN DO YOU PEN TEST?

As we have established, pen testing is not a one-and-done job, nor is it a method where a cookie-cutter strategy is appropriate. Due to the nature of their job or the scope of their internet presence, some organisations are exposed to greater risks than others.

For these groups, a regular Pen Test, perhaps annually or biannually, is preferable. The frequency with which a Penetration Test should be performed is influenced by business size, industry, budget, and regulatory requirements. Ethical hacking performed via a Pen Test enables you to gain a comprehensive understanding of how an attacker could abuse your organization's vulnerabilities, where your weaknesses lie, and what you must do to strengthen security.

For these reasons, we suggest regular and timely Penetration Tests for the safety and security of any modern organisation.

## TYPES OF PENETRATION TESTING

# 1. Checking for Network Penetration

The most vulnerable network infrastructure components, such as servers, firewalls, and switches, are discovered and exploited during network penetration testing. This sort of testing can safeguard your organisation against common network-based attacks, such as:

• Incorrect firewall setup and firewall breach • Database-based attacks • MitM-based attacks • FTP/SMTP-based attacks

# 2. Vulnerability Assessment of Online Application

The testing of web application vulnerability detects vulnerabilities in web-based apps It is a three-stage process that involves:

* An online application's web servers, operating systems, services, and other tools are investigated during reconnaissance.
* Identification of web application flaws and preparation of attack vectors for penetration testing.
* An attack is the exploitation of a security vulnerability to obtain unauthorised access to a computer programme or its data.

The security testing of Web applications can detect vulnerabilities in databases, source code, and backend networks. Not only can it find vulnerabilities, but it can also help prioritise them and offer mitigation options.

# 3. Investigating Wireless Intrusion

The wireless communications services that enable data to enter and exit networks must be protected against unauthorised access and data exfiltration. The purpose of wireless penetration testing is to identify wireless network risks and evaluate their vulnerabilities, such as:

* Deauthentication attacks
* Wireless router configuration errors
* Session reuse
* Unauthorized wifi devices

# 4. Validation of Effective Entry

If a threat actor gains physical entry to a server room or other sensitive facility, they may be able to compromise the entire network, which can have catastrophic repercussions for the organisation, its customers, and its partnerships. Physical penetration testing can safeguard a company's tangible assets from threats like social engineering, tailgating, and badge cloning.

Physical penetration testing identifies vulnerabilities in tangible controls, such as locks, doors, cameras, and sensors, and enables a company to patch them swiftly.

# 5. Social Networking Admissions Test

Attackers frequently view users as the security system's weakest component and frequently target them. When assessing a company's security, social engineering penetration testers pay special attention to the people and processes within it. Common social engineering attacks in the workplace, such as phishing, USB dropping, and spoofing, are tried by ethical hackers.

The objective is to identify vulnerable people, groups, or processes and to devise ways to increase security awareness.

# 6. Client-Side Penetration Testing

Client-side penetration testing can identify security flaws in client-side software such as web browsers, media players, and content production applications (such as MadCap Flare, Adobe Framemaker, or Adobe RoboHelp). Frequently, attackers compromise client-side software to obtain access to enterprise infrastructure.

Cross-site scripting (XSS) assaults. Clickjacking assaults CORS (Cross-origin resource sharing) attacks Form theft HTML insertion Wide diversion Virus spread

# 7. IoT Risk Assessment

IoT penetration testing searches for security flaws in connected ecosystems, such as hardware, embedded software, communication protocols, servers, and web and mobile apps associated with IoT devices.

Various hardware, firmware, and communication protocol tests are performed based on the connected device. Some devices may necessitate the gathering and analysis of data via electrical components, firmware analysis, or signal capture.

# 8. Checking Mobile Applications for Vulnerabilities

Mobile application penetration testing comprises both static and dynamic analysis on mobile apps (excluding mobile APIs and servers): • Static analysis extracts source code and metadata and uses reverse engineering to identify vulnerabilities in application code.

• Dynamic analysis finds application vulnerabilities while the application is executing on a computer or device.

## DIVERSE TECHNIQUES OF PEN AND VULNERABILITY TESTING

# Black Box Testing

During a black box penetration test (also known as external penetration testing), the pen tester is provided with minimal information about the IT system of a company.

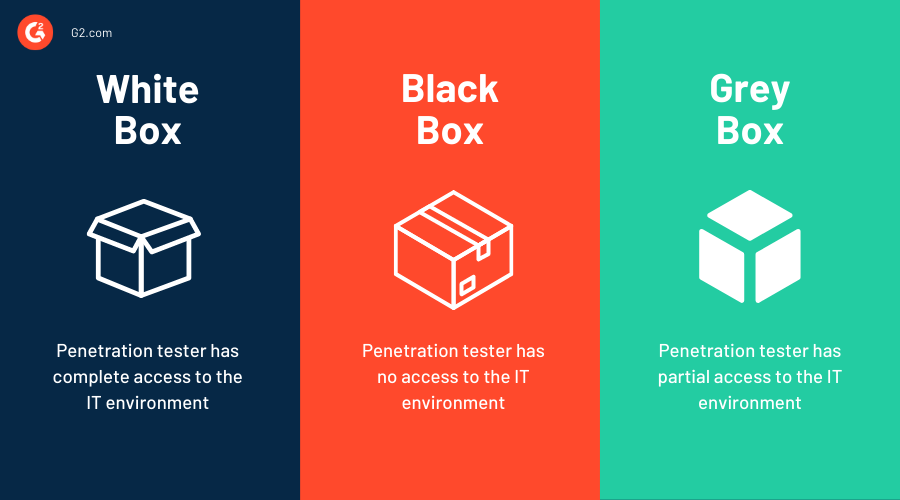
This testing method's primary advantage is that it mimics a real-world cyber attack, with the tester acting as an uninformed attacker.

It can take up to six weeks to finish a black box penetration test, making it one of the longest types of penetration tests.

This relies on the scope of the project.

Starting a sequence of known exploits, such as Kerberoasting, is one of the simplest methods for pen testers to break into a system during a black box test.

This testing strategy is also known as "trial and error," but it requires a high degree of technical skill.



<https://learn.g2.com/hubfs/approach%20to%20penetration%20testing.png>

# White Box Testing

White box penetration testing (also known as clear box testing, glass box testing, or internal penetration testing) is done when the pen tester has complete access to both the source code and the environment, as well as complete knowledge of both.

The objective of a white box penetration test is to perform a comprehensive security audit of an organization's systems and provide as much information as possible to the pen tester.

White box inquiries are not without drawbacks. Given the level of access, a penetration tester has, determining which areas to focus on may require more time. Moreover, this technique of testing frequently necessitates the use of complex and costly instruments, such as code analyzers and debuggers.

In the end, it makes no difference whether a black box or white box penetration test is performed, so long as the main objective of the test is achieved.

# Gray-Box Testing

The penetration tester has limited information or access to an internal network or web application during a grey box test.

The rights of a penetration tester may be elevated from user to domain administrator on a host. Software code and system architecture diagrams may also be required.

A grey box penetration test report provides a more targeted and effective evaluation of the security of your network.

Instead of wasting time with the "trial and error" method, pen testers performing a grey box penetration test can examine network diagrams to identify high-risk areas.

Then, appropriate solutions can be suggested to fill the voids.

## CONTRIBUTION OF VULNERABILITY TESTING TO COMPLIANCE

Cybersecurity teams are typically responsible for assuring compliance with the following regulations:

* HIPAA
* PCI DSS
* SOX
* NERC
* HEOA
* GDPR
* CMMC

Pen testing shows precisely how an attacker could exploit a company's infrastructure to gain access to sensitive information. Periodic required testing ensures that organisations can stay one step ahead of attackers by finding and fixing security vulnerabilities prior to their exploitation. In addition, auditors can use these tests to confirm that other required security measures are in place and functioning correctly.

Many incorrectly assume that third-party testing is necessary to satisfy compliance standards. However, this is not typically the situation. In actuality, PCI DSS, which contains some of the most stringent standards for penetration testing, does not mandate a third-party audit.

Numerous organisations view numerous compliance testing components as simple and even repetitive. A tool for penetration testing, such as Core Impact, offers a straightforward and well-established automated framework that can support these types of tests without needing extensive penetration testing experience.

One of the external tests stipulated by PCI DSS Requirement 11.4 is the web application layer pen test, which must identify weaknesses such as SQL injection and cross-site scripting (XSS). In addition to discovering these vulnerabilities, Core Impact's automated One-Step WebApps Vulnerability Test also finds others, such as broken authentication, broken access control, and security misconfigurations. In addition, Core Impact's intuitive wizards and automation features assist testers with tasks such as collecting information, executing attacks, and increasing their power.

Then, penetration testing tools are used to ensure compliance. For example, PCI DSS mandates that any vulnerabilities found during testing must be remedied, and a subsequent test must be conducted to confirm that they have been resolved. Initial testing may be performed by a third party, followed by the implementation of an automated test by a member of the security team to verify the remediation efforts.

## WIDELY USED PENETRATION TESTING TOOLS

Here are a few examples of penetration testing tools:

# Kali Linux

Kali, formerly known as BackTrack Linux, is completely optimised for offensive penetration testing and is managed by Offensive Security (OffSec), the same organisation that administers the OSCP certification.

Although it is possible to run Kali on its hardware, penetration testers usually use OS X or Windows virtual machines running Kali.

Kali includes the majority of these tools and is the standard operating system for penetration testing in the majority of use cases. Caution is recommended, however, as Kali is designed for offense, not defense, and is easily exploitable in return. Don't keep your super-duper extra secret files in your Kali VM.

# nmap

nmap (short for network mapper) is the grandfather of port scanners and an essential penetration testing tool.

Despite occasional hysteria from non-technical C-level executives that an unknown party is port scanning the company, nmap is completely legal and is analogous to knocking on everyone's front door to see if they are home.

Insurance companies, internet cartographers like Shodan and Censys, and risk scorers like BitSight use specialised port-scanning software (typically nmap competitors masscan or zmap) to map the public security posture of businesses of all kinds. However, malicious intruders perform port scans as well, so this is something to keep in mind for the future.

# Metasploit

This appropriately named meta-software resembles a crossbow: Aim at the target, choose an exploit, pick a payload, and fire. Metasploit is, as its website asserts, "the world's most widely used penetration testing framework" because it automates a vast amount of previously tedious work, making it essential for the vast majority of penetration testers. Metasploit, an open-source initiative backed by Rapid7, is indispensable for securing networks against attackers.

# Wireshark

Wireshark is the usual application for analysing network traffic. Wireshark facilitates the study of hundreds of protocols, including real-time analysis and decryption support for a significant number of these protocols. Wireshark is commonly employed to investigate typical TCP/IP connection problems. If you are unfamiliar with vulnerability testing, you must be familiar with Wireshark.

# John the Ripper

Unlike its namesake, does not conduct serial murders in Victorian London; rather, it decrypts data as rapidly as your computer can process it. This open-source password cracker is intended to be used offline. John can use a word list of likely passwords and modify them by replacing "a" with "@" and "s" with "5" and so on, or brute-force hardware can run indefinitely until a password is found. Given that the overwhelming majority of people use simple, short passwords, John is often successful at breaking encryption.

# Hashcat

The self-proclaimed "fastest and most advanced password recovery utility in the world" is certainly not modest, but the hashcat team recognises its worth. John the Ripper is competing with Hashcat. It is the standard penetration testing tool for cracking hashes and supports multiple brute force password guessing attacks, including dictionary and mask attacks.

Typically, penetration testing includes the exfiltration of hashed passwords, and leveraging these credentials requires running a programme like hashcat offline against them in an attempt to guess or brute-force at least some of the passwords.

Hashcat performs efficiently on a modern GPU (sorry, Kali VM users). Legacy hashcat still allows CPU-based hash cracking but warns users that it is significantly slower than using your graphics card's processing power.

# Hydra

John the Ripper's companion Hydra is activated when you need to decrypt an online password, such as an SSH or FTP login, IMAP, IRC, or RDP, among others. Point Hydra in the direction of the target service, if preferred, and pull the trigger. Hydra is an indicator that rate-limiting password tries and disconnecting users after a small number of unsuccessful login attempts are effective defensive countermeasures against attackers.

# Burp Suite

Web vulnerability scanners are indispensable when discussing penetration testing instruments. Burp Suite, unlike the previously mentioned tools, is neither open source nor free; it is an expert tool that costs money. However, there is a reason why they can charge such outrageous prices. Burp Suite is a powerful website security scanner. When you are ready, point it to the website you desire to test and activate it. Nessus, a rival to Burp, offers a product with comparable effectiveness and pricing.

# Zed Attack Illustration

Those without the financial means to buy Burp Suite will find OWASP's Zed Attack Proxy (ZAP) to be nearly as effective, and it is both open source and free. ZAP, as its name suggests, stands between your browser and the website you're testing and allows you to intercept (also known as "man in the middle") the data in order to inspect and modify it. It lacks many of Burp's features, but its open-source license makes it easier and less expensive to implement on a big scale, and it is an excellent tool for teaching beginners how vulnerable web traffic really is. Nikto, a rival to ZAP, offers a similar open-source application.

# sqlmap

This highly effective SQL injection tool, according to its website, is open-source and "automates the process of identifying and exploiting SQL injection vulnerabilities and seizing control of database servers." Among the supported databases are MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB, and H2. In the past, SQL injections were produced by putting a hot needle into a hard disc. Today, sqlmap will remove the need for penetration testing-related squinting.

# aircrack-ng

This wifi security monitoring application is free/libre, but you must buy your own Pringles can. (According to what we've heard, the darknet market at 7-11 can provide a product on the covert.) Due to bad configuration, weak passwords, and outdated encryption protocols, it is frequently possible to crack Wi-Fi networks today. Aircrack-ng is a popular choice regardless of the presence of a Pringles cantenna.

## TEAMING

The number of attacks is growing, and the amount of study and experience needed to stay ahead of these attacks is increasing the time lag between attack and discovery. Thus the collaboratory exercises in teamwork simulate real-world attack situations, with one squad attacking and the other defending.

# Red Team

The red squad has the offensive position. A red squad is established with the purpose of identifying and assessing vulnerabilities, testing assumptions, examining alternate attack options, and revealing the organization's limitations and security risks.

# Blue Team

The blue team is responsible for protecting the company. Blue teams are responsible for developing and implementing an organization's defensive measures.

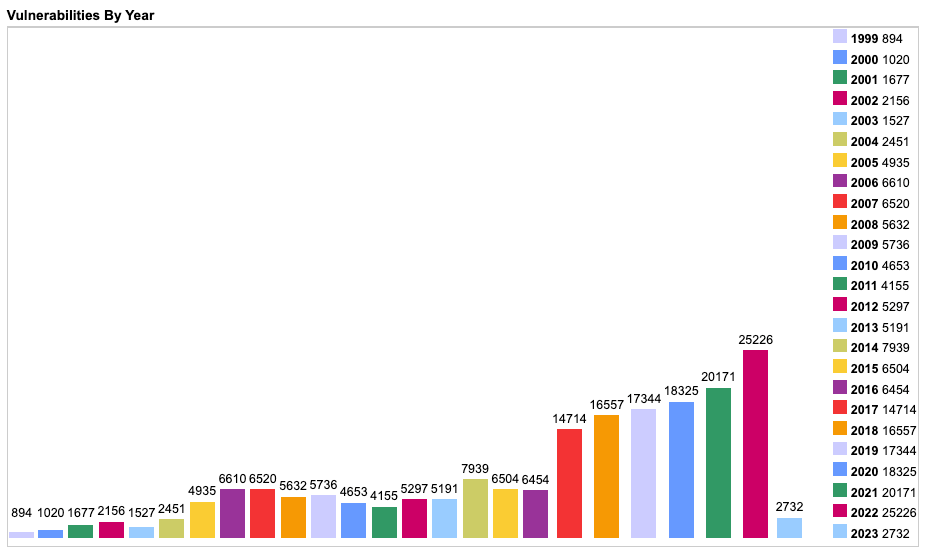
# Purple Team

In teambuilding exercises, the idea of a purple team has recently gained popularity. This is the mentality of viewing and considering the red and blue teams as mutually beneficial. It's not red teams versus blue teams, but rather one big team with a singular focus: enhancing security. The secret to becoming a purple squad is communication between individuals and their respective teams.

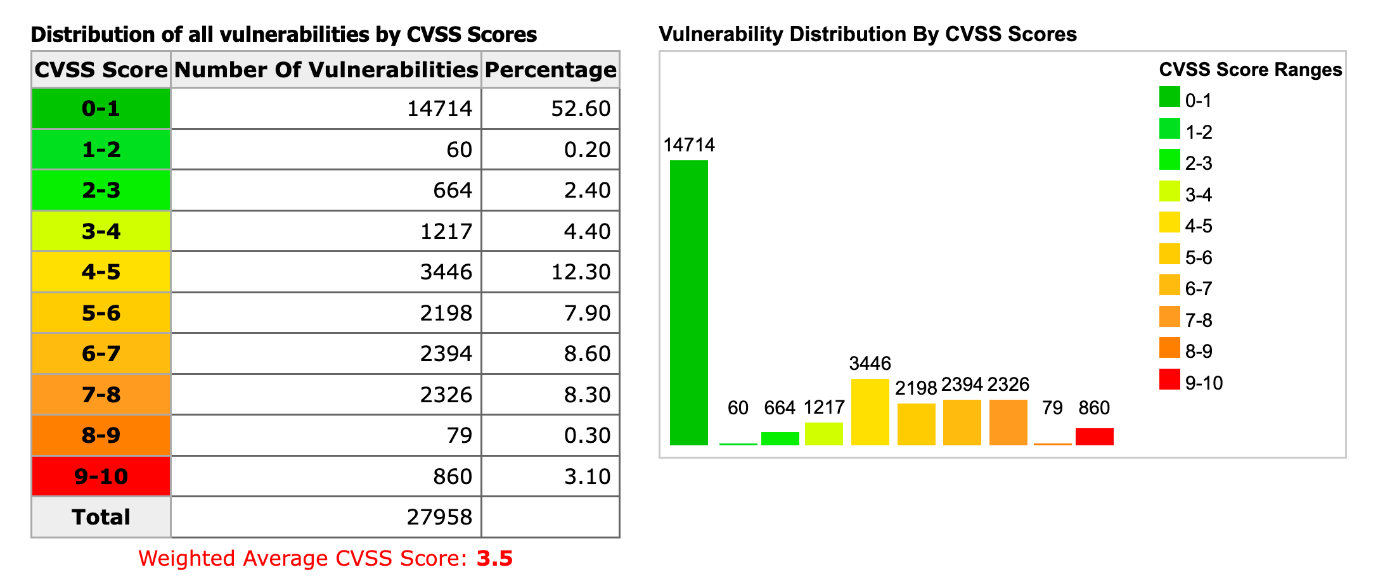
## STATISTICS REGARDING VULNERABILITY AND PEN TESTING

The expanding threat environment continues to have a global impact on companies and their critical infrastructure. For instance, 2022 was a record-breaking year for CVE data publication, with over 250,000 records published. Each day, 68.75 CVEs were published on average.

• More than 13,000 vulnerabilities were reported in 2022, of which 3,238 were assigned CVSSv2 scores (from 7.0 to 10.0). There were roughly 21,000 fewer risks in 2021, a decrease of 40%.



<https://pentest-tools.com/blog/img/asset/YXNzZXRzL2NvbnRlbnQvcGVuZXRyYXRpb24tdGVzdGluZy1zdGF0aXN0aWNzLTIwMjIvdnVsbmVyYWJpbGl0aWVzLWJ5LXllYXItdmlhLW5pc3QucG5n?s=3f41a911a80179179a91145b2c57f239>

* Cobalt's State of Pentesting 2022 names the top five vulnerability categories discovered by the pentesting community: Server Security Misconfigurations (38%), Cross-Site Scripting (13%), Defective Access Control (11%), Exposed Private Information (10%), and Authentication and Sessions (8%).
* According to a study, the number of security vulnerabilities (CVEs) disclosed in 2021 increased to 20,174 from 17,050 in 2020. The top three flaws were cross-site scripting (XSS), memory poisoning (memory poisoning), and SQL.
* On average, security teams required fourteen days to fix vulnerabilities. (The State of Pentesting by Cobalt in 2022)
* ProxyLogon (CVE-2021-26855 and CVE-2021-27065), ProxyOracle (CVE-2021-31196 and CVE-2021-31195), and ProxyShell are the three most notable significant Microsoft vulnerabilities on CISA's list of the most exploited vulnerabilities in 2021. 

https://pentest-tools.com/blog/img/asset/YXNzZXRzL2NvbnRlbnQvcGVuZXRyYXRpb24tdGVzdGluZy1zdGF0aXN0aWNzLTIwMjIvdnVsbmVyYWJpbGl0aWVzLWRpc3RyaWJ1dGVkLWJ5LWN2c3Mtc2NvcmUtaW4tMjAyMi5wbmc=?s=27c4ae42754afdd7ddcbca1403600cb0

These are common and easily preventable security flaws:

* failing to keep configurations,
* software updates
* access management controls

To successfully address and prevent these vulnerabilities, security and development teams need extra resources, particularly personnel, which can be scarce due to talent shortages.

# Actual consequences of labour shortages for security staff

Teams battle to maintain security standards as coworkers leave and positions stay vacant, particularly in terms of supporting compliance and secure development. There is a greater likelihood that weaknesses will go undetected, and teams are concerned that they are unprepared to respond to cyberattacks. Notably, a whopping 90% of respondents who have encountered team member shortages or losses have difficulty managing tasks!

# Even developers sense the pressure.

While security teams seek help from developers, development teams experience the same labour shortage. 7 % of respondents say they have had sufficient staffing for at least six months and expect this to continue for the next six months. The majority of developers (97%) believe that these obstacles make it more difficult to meet crucial deadlines for the launch of new features, while 80% believe that these obstacles compromise the quality and security of developers' code.

# A dearth of talent hinders both security and developer cooperation.

Talent shortages impede the cooperation efforts between the security and development departments. This hinders the capacity of teams to handle critical vulnerabilities and make launch deadlines. In addition, the quality of developers' work deteriorates, which increases the likelihood that new code will bring even more vulnerabilities.

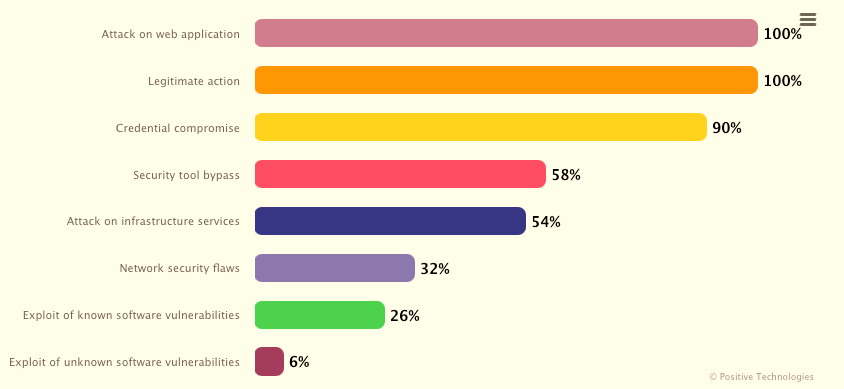
Notable:

* 96% of security teams report a slower response to patching critical vulnerabilities
* 97% of developers battle to meet important launch deadlines
* 80% of developers report that collaboration issues with the security team decrease the quality of their code.

The obstacles outlined by our research are challenging, but not insurmountable. Download The State of Pentesting 2022 to discover what organisations can do to control their vulnerabilities and keep talent during The Great Resignation – and how Pentest as a Service (PtaaS) can help.

# Revenue projections for vulnerability testing for 2021 and 2022

* There are an increasing number of known security flaws, making every business a potential target for cybercriminals.
* Seventy percent of intrusions in 2021 utilized Remote Desktop Protocol (RDP) to acquire unauthorized access.
* As these actors' toolkits and methods become more sophisticated, businesses are under greater pressure to prioritize and implement mitigation solutions. Utilize a professional penetration testing service to alleviate the burden.
* Let's examine the most significant insights that explain why and how businesses use vulnerability testing.
* Seventy-four percent of businesses incorporate penetration testing into their risk management strategies, while another 73 percent use it to assess their security posture and 70 percent use it to assure compliance. (CoreSecurity 2021 Penetration Testing Report)
* In 2021, 39% of businesses reported conducting pentests once or twice annually; by 2022, this percentage increased to 42%. This indicates that retesting, a vital tool for confirming the success of restoration efforts, is underutilized. (CoreSecurity 2021 & 2022 Penetration Testing Report) (CoreSecurity 2021 & 2022 Penetration Testing Report) (CoreSecurity 2022 Penetration Testing Report)
* In 2021, 42% of employees of enterprises formed an internal pentesting squad, rising to 53% the following year. (CoreSecurity 2021 & 2022 Penetration Testing Report)
* According to a report published by Positive Technologies in 2022, the results of external penetration testing of business information systems are intriguing.
* Pentesters were able to violate the network perimeter and gain access to the internal networks of 96% of companies. One hour was all that was needed for the quickest attack. (to break into a local area network).
* All companies have identified vulnerabilities and weak points in their web application configurations as possible entry sites for attackers.



<https://www.ptsecurity.com/ww-en/analytics/results-of-pentests-2022/#id5>

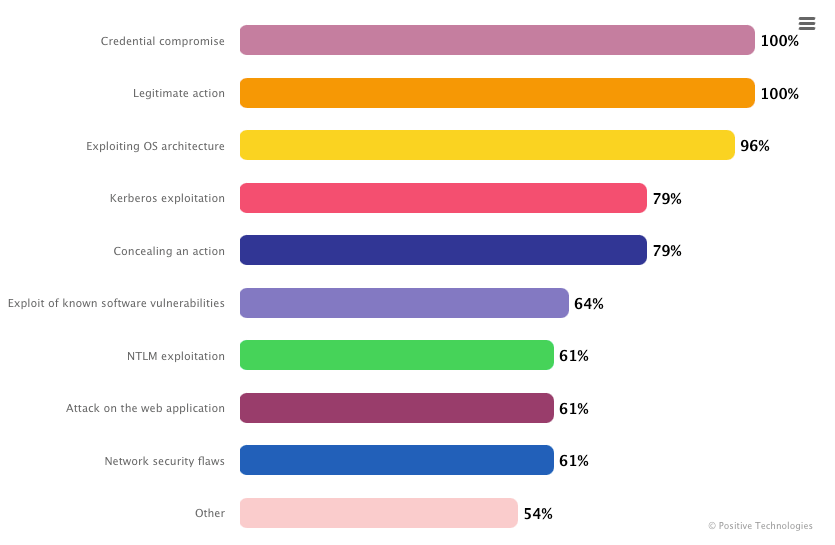
In addition, all one hundred businesses were effectively tested for internal penetration because

• testers were able to assume complete control over the underlying infrastructure. Typically, it took ten days to initiate a mission-critical operation and five days to obtain complete domain access. 57% of businesses discovered at least one simple method for acquiring infrastructure management.

• In 85% of businesses, penetration testers discovered password security defects, and in 60% of these businesses, they discovered high-risk software vulnerabilities.

•All businesses' penetration testers used password sprinkling (49%) and guessing (33% of the time) the most. Occasionally, they employed password-cracking techniques (16%).

The examined group utilized legitimate action and credential brute force predominately.

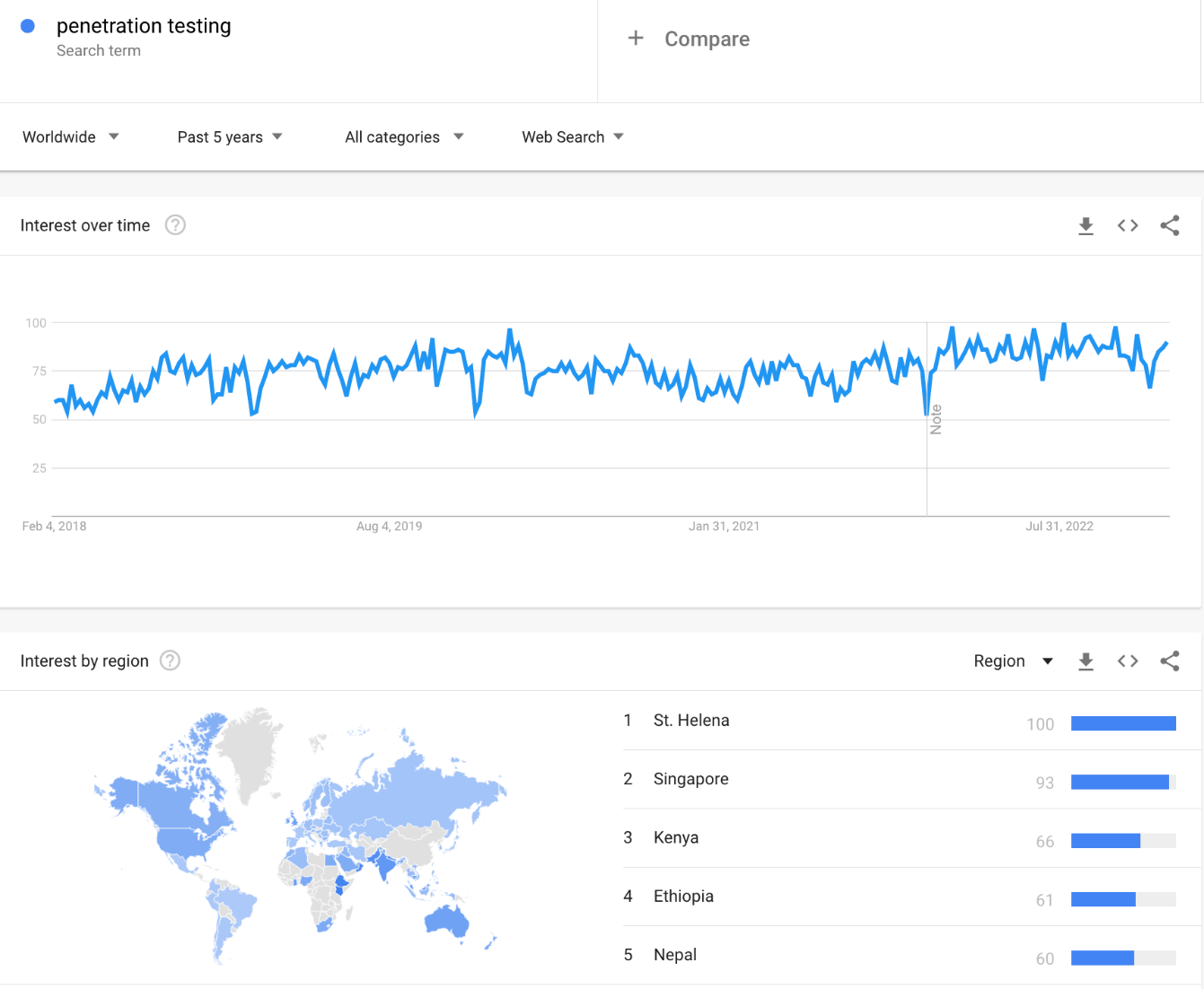


<https://www.ptsecurity.com/ww-en/analytics/results-of-pentests-2022/#id10>

# Information about the industry of penetration testing

Consider the presented data to evaluate the current status of the global penetration testing industry and to identify the primary growth drivers.

By 2026, the global market for penetration testing is projected to reach $3 billion, up from $1.6 billion in 2021. This represents an annual compound growth rate (CAGR) of 13.8%. (GlobeNewswire)



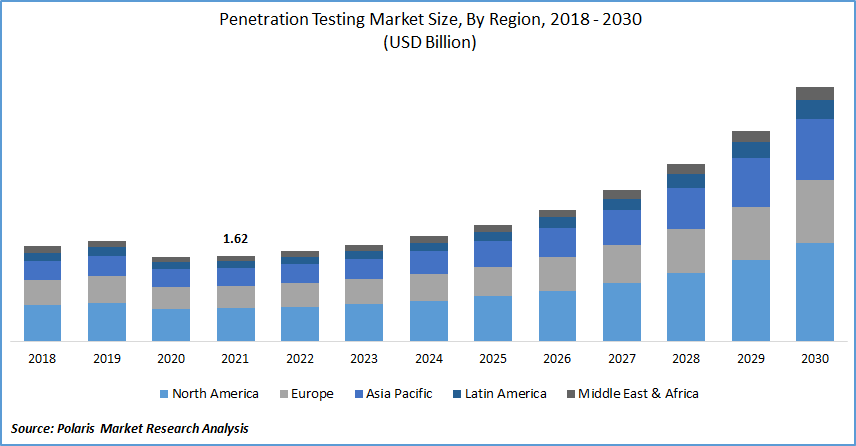
Google Trends for Penetration testing we searches (February 2018- January 2023)

https://pentest-tools.com/blog/img/asset/YXNzZXRzL2NvbnRlbnQvcGVuZXRyYXRpb24tdGVzdGluZy1zdGF0aXN0aWNzLTIwMjIvcGVuZXRyYXRpb24tdGVzdGluZy1zZWFyY2hlcy1pbi1nb29nbGUtdHJlbmRzLS0tdXBkYXRlZC5wbmc=?s=25d7cfb811026f8c9506a934e5dc3163

In 2020, pentesting is anticipated to generate $325.8 million in the United States. In 2027, the Chinese market will be worth $705,9 million, making it the world's second-largest after the United States. (Penetration Testing Global Market 2021 Report)

The United States, Canada, Japan, China, and Europe will contribute the most to the 20.7% CAGR of the mobile application adoption market.

This explosive growth is significantly influenced by the growing demand for software-based product security. It is anticipated that mobile and web-based applications will drive the expansion of the global penetration testing market. The prominence of cloud-based security services will increase penetration testing demand, according to the Mordor Intelligence Penetration testing Market Report.



<https://www.polarismarketresearch.com/wp-content/uploads/2022/05/Penetration-Testing-Market.png>

# Assessment data automation

Understanding how automated penetration testing can reduce the number of time-consuming, manual duties without compromising quality is advantageous. This means that we should never underestimate the significance of human discernment.

Let's examine some of the most revealing statistics regarding automated vulnerability testing.

* Seventy-five percent of businesses use penetration testing to evaluate their security or demonstrate compliance with regulations. 57% of them are specifically contributing to a vulnerability management initiative. (CoreSecurity 2022 Pen test Report)
* 78% of penetration testers use a combination of open-source and commercial security tools, while 11% rely exclusively on free tools.
* Seventy-seven percent of businesses view reporting as a crucial component of commercial pentesting software. 61% are seeking multi-vector testing tools, whereas 67% are purchasing extensive threat libraries.
* Evaluations of vulnerability can uncover more than 50,000 unique categories of external and/or internal vulnerabilities. (SecurityMetrics)
* Automated penetration testing focuses on servers, web applications, and databases primarily. (RidgeSecurity Survey)
* 29% of businesses have entirely automated all security testing. • 44% of organizations have integrated security testing and evaluation into their software development processes. (SANS Survey, 2021). (2021 SANS Survey)

## CONCLUSION

This survey is intended to provide ongoing insight into the penetration testing practices of cybersecurity professionals. There is every indication that penetration testing will continue to be a vital practice for many years to come, as the results revealed a broad variety of pen testing methods used by organisations. The adaptability of its implementation is essential for ensuring that these tests are done on a regular basis; organisations have the option of employing in-house teams, third-party services, and open-source or commercial tools. This demonstrates that any organisation is capable of adapting a programme to its needs and accessible resources. While financing obstacles from the previous year appear to have decreased, the continuing threats of phishing, ransomware, and inattention to specific environments are more worrisome in the long run, particularly given the prevalence of overconfidence in current cybersecurity strategies. Regularly testing your organisation is still the best way to ensure that your cyber risk exposure is constantly reduced. The objective of penetration testing should not be to simply cross it off a list. Penetration testing not only provides short-term value by identifying and prioritizing the security vulnerabilities that currently pose the greatest risk, but it can also provide long-term value as part of a comprehensive security portfolio designed to adapt to both new and persistent cybersecurity challenges.

## REFERENCES

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://static.fortra.com/core-security/pdfs/guides/cs-2022-pen-testing-report.pdf

<https://pentest-tools.com/blog/penetration-testing-statistics>

<https://purplesec.us/resources/cyber-security-statistics/#Start>

<https://www.spiceworks.com/it-security/vulnerability-management/articles/best-penetration-testing-tools/>

<https://www.opensourceforu.com/2022/05/what-is-penetration-testing-and-why-is-it-important/>

<https://www.techtarget.com/searchsecurity/definition/penetration-testing>