Introduction to Penetration Testing

1

Table of Contents

Introduction to Penetration Testing 2

- **Penetration Testing 2**

Common Penetration Testing Approaches and Techniques 3

Types of Penetration Testing 4

- **Black Box Penetration Testing 4**
- **White Box Penetration Testing 5**
- **Gray Box Penetration Testing 5**

Coverage, Speed, and Efficiency Between Pentesting Approaches 5

Penetration Testing Teams 6

Penetration Testing Types 6

- **Network Services Penetration Testing 6**
- **Web Application Penetration Testing 7**
- **Physical Penetration Testing 7**
- **Social Engineering Penetration Testing 8**
- **Client-Side Penetration Testing 8**
- **Mobile Application Penetration Testing 8**
- **Wireless Pentesting 8**

Penetration Testing Methodologies 9

- **Scope Establishment 9**
- **Pentest Execution 9**
- **Results Reporting and Delivery 9**

Required Skill Sets for a Penetration Tester 10

Penetration Testing Methodology 10

Pen Testing from Contract to Report, First Edition. Alfred Basta, Nadine Basta, and Waqar Anwar.

Companion website: www.wiley.com/go/basta

Penetration Testing Methodologies List 10
Open-Source Security Testing Methodology Manual (OSSTMM) 10
Open Web Application Security Project (OWASP) 10
Penetration Testing Execution Standard 10
NIST 800-115 10
Penetration Testing Framework 11
Information Systems Security Assessment Framework (ISSAF) 11
Frequency of Penetration Testing 11
Certifications that Pentesters may Acquire 11
Offensive Security Certified Professional (OSCP) 11
Offensive Security Certified Expert (OSCE) 12
GIAC Penetration Tester (GPEN) 12
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) 12
LPT – Licensed Penetration Tester 12
Why Companies Should do Penetration Testing 12
Penetration Testing's Advantages 13
Phases of Pentesting 13
Attack Phase 13
Actions Taken After an Attack 13
Points to Consider Before Signing a Contract 14
Most Commonly Used Penetration Testing Tools 14
Pentesting Use Cases 15
Opportunities and Challenges 16
Trends and Emerging Technologies 16
References and Resources 17

Introduction to Penetration Testing

Penetration Testing

Penetration testing, commonly known as pentesting, is a method of evaluating the security of computer systems, networks, and applications by simulating an attack from a malicious actor. The goal of a penetration test is to identify vulnerabilities and weaknesses in the target system that could be exploited by attackers. Penetration testing is a vital aspect of cybersecurity, as it helps organizations identify and address security weaknesses before they can be exploited by malicious actors. The process of penetration testing involves identifying potential entry points, attempting to exploit vulnerabilities, and reporting on the effectiveness of the security measures in place.

Penetration testing can be performed manually or with the help of automated tools. It is frequently directed at the following endpoints:

- **Servers**: This can include various types of servers, such as web servers, file transfer servers, Dynamic Host Configuration Protocol (DHCP) servers, and domain name system (DNS) servers.

- **Network services and devices**: This includes all types of network services and devices, such as routers, switches, and firewalls. Penetration testers may try to find flaws in how these devices are set up or check if they allow unauthorized access to sensitive data or the ability to manipulate or shut down the network.
- **Wireless devices and networks**: This includes all types of wireless devices and networks, such as WiFi, NFC, and Bluetooth. Penetration testers may attempt to identify vulnerabilities in the wireless protocols or encryption mechanisms used by these devices and networks.
- **Network security devices**: This includes all types of network security devices, such as firewalls, intrusion detection and prevention systems, and virtual private network (VPN) gateways. Penetration testers may try to find flaws in the way these devices are set up or put together that could let attackers get around or avoid them.
- **Web applications and software**: This includes all types of web applications and software used by the organization.
- **Mobile devices**: This includes all types of mobile devices, such as smartphones and tablets. Penetration testers may attempt to identify vulnerabilities in the operating system or applications installed on these devices that could allow attackers to compromise them or steal sensitive data.

It should be noted, though, that the real pentest simply does not end here. The main objective is to penetrate the IT infrastructure to reach a company's electronic assets.

Common Penetration Testing Approaches and Techniques

1. **Clients**: Organizations that engage penetration testers to test their systems and networks are referred to as clients. Client-focused topics could include:
    - **Testing methods and styles**: Each customer has a varied choice for how they want the penetration test to be done. Some may prefer a "black box" approach in which the penetration tester has no previous knowledge of the system, while others may prefer a "white box" approach in which the penetration tester has access to certain system information. This enables the penetration tester to personalize the test to the unique demands of the customer, resulting in a more complete and effective test. It also helps the client confirm that the test is being carried out in a safe and secure manner because the penetration tester has a better grasp of the system.
    - **Frequency**: How often should a penetration test be carried out? Some businesses may require annual penetration tests, while others may prefer more regular testing. Tests can be performed quarterly, biannually, or as needed to maintain the security of their systems and networks, depending on the demands of the company.
    - Why should a company do a penetration test? Compliance requirements, risk management, or just detecting vulnerabilities before an attacker does can all fall under this category.
    - **Phases**: The penetration testing process has different parts, such as planning, reconnaissance, scanning, exploitation, and post-exploitation.
    - **Use cases**: Clients may want to know how penetration testing can be used for specific business use cases, such as securing a cloud-based infrastructure or protecting sensitive customer data.

    Example: A healthcare institution may choose to conduct a penetration test to ensure compliance with HIPAA regulations. To guarantee that all systems and networks are adequately

tested, the business may require a "white box" approach. They may also wish to repeat the test on a yearly basis to assure continuous compliance.

2. **Penetration testers**: Professionals who conduct penetrating tests are known as penetration testers.
   - What skills are required for a penetration tester? These can involve technical skills like programming language expertise and network protocol understanding, as well as soft skills like communication and problem-solving.
   - **Certifications**: What credentials should a penetration tester possess? This can include certifications like Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Offensive Security Certified Professional (OSCP) (CISSP).
   - **Common tools**: What tools do penetration testers usually use? This could include network scanners, vulnerability scanners, and exploitation frameworks.

   Example: A penetration tester working for a financial institution, for example, may need to be well-versed in banking protocols and transactional systems, as well as hold a certification such as the Certified Information Systems Auditor (CISA) or CISSP.
3. **Both**: Topics that can focus on both clients and penetration testers can include:
   - **Penetration testing services**: What do penetration testers provide? This can involve web application testing, network testing, and wireless testing.
   - **Points to consider**: What should clients consider before hiring a penetration tester? This can include things like the scope of the penetration test, the cost, and the amount of time necessary.
   - **Considerations before signing a contract**: What should penetration testers take into account before establishing a contract with a client? This includes things like the scope of the penetration test, payment conditions, and legal liabilities.

   Example: A major e-commerce firm, for example, may choose to engage a penetration tester to evaluate its website and mobile app. When signing a contract, the firm should think about the scope of the test, such as which parts of the website and app will be tested, as well as the cost and time involved. The scope of the test, as well as any legal responsibilities that may develop during the test, should be considered by the penetration tester.

Types of Penetration Testing

- Black box
- White box
- Gray box

Black Box Penetration Testing

In this type of test, the tester receives absolutely no information during the test. The pentester imitates the tactics of an attacker, starting from initial access, execution, and exploitation. Black box penetration testing is more realistic since it shows how an adversary without inside information would target and infiltrate an organization. The pentester is in charge of the attack's reconnaissance phase, during which they collect any sensitive information they will need to successfully breach the network. Black box penetration testers gather information about their

target system and use it to create a blueprint of its inner workings. Like an unprivileged attacker, a pentester creates the map based on their own observations, investigation, and analysis of the target system. The pentester then employs these results in an attack on the target. They may use whatever methods are required, including brute-force attacks and password cracking. Following the breach, the pentester mimics the actions of an attacker by attempting privilege escalation and establishing a persistent presence, but without really causing any harm. After completing the test, the pentester will create a report and clean up the workspace.

White Box Penetration Testing

This method entails giving the tester access to all network and system data, including network maps, login passwords, and IP addresses. In this type of testing, time is saved, and the total cost of the engagement is reduced. White box penetration testing is done to mimic a particular attack on a system by using as many attack pathways as feasible.

Gray Box Penetration Testing

Gray box penetration testing is a type of testing that combines elements of both black box and white box testing. During a gray box penetration test, the testers are provided with a limited amount of information about the target system, typically authentication credentials or partial access to the system. The purpose of this is to simulate an attacker with some prior knowledge of the system, such as an insider or a compromised user account.

One of the primary benefits of gray box testing is its ability to reveal the extent of access that a privileged user might have on a system. By limiting the information given to the testers, it forces them to use their knowledge and experience to identify potential vulnerabilities and exploit them to gain access to sensitive data. This information can be extremely useful to organizations since it can help them understand the potential impact of a successful attack from an insider or an external attacker with some knowledge of their systems.

Gray box testing is also useful for businesses that want to avoid the time-consuming reconnaissance and information gathering that typically come with black box testing. By providing testers with a limited amount of information, it can help them focus their efforts and identify vulnerabilities more quickly. This can be particularly beneficial for businesses with limited resources, as it allows them to maximize their testing efforts and get a good outcome without spending excessive time and money on reconnaissance.

Coverage, Speed, and Efficiency Between Pentesting Approaches

Each pentesting approach involves tradeoffs between coverage, speed, and efficiency. Here are some important differences:

Black box penetration testing is regarded as the quickest kind of pentest. However, pentesters may overlook flaws in the system they are testing since they have no prior knowledge of the infrastructure. Since there is a lack of details, the pentest may not be as effective. In comparison to black box testing, gray box testing might take more time to complete. Nonetheless, a gray box test offers more speed and coverage than a black-box test since pentesters have access to certain information before an attack begins. Testers may be more efficient, for instance, when they have access to the design documentation they need.

White box testing is regarded as the slowest but most thorough kind of penetration testing. It takes time for white box penetration testers to analyze the massive volumes of data they get. Yet, the breadth of data and access may greatly increase the likelihood of detecting and fixing external and internal flaws.

Penetration Testing Teams

Penetration testing is a critical process for ensuring the security of an organization's digital assets. As such, it is important to have a skilled and experienced penetration testing team carry out the testing. A typical penetration testing team is composed of the following roles:

1. **Penetration tester**: This is the person who performs the actual testing. They are responsible for identifying and exploiting vulnerabilities in the organization's systems and applications. Penetration testers must have strong technical skills, including knowledge of programming languages, network protocols, and operating systems.
2. **Team leader**: The team leader is responsible for managing the team and ensuring that the testing is conducted according to the plan. They should have experience managing penetration testing projects and have a good understanding of the organization's IT infrastructure.
3. **Project manager**: The project manager oversees the entire penetration testing project. They are responsible for ensuring that the project is completed on time and within budget. The project manager should have experience managing cybersecurity projects and be familiar with industry standards and best practices.
4. **Subject matter expert**: The subject matter expert provides technical expertise in specific areas, such as web applications, databases, or mobile devices. They work closely with the penetration tester to identify vulnerabilities and develop testing strategies.
5. **Quality assurance**: The quality assurance specialist is responsible for ensuring that the testing is conducted in accordance with industry standards and best practices. They review the testing results and provide feedback to the team to improve the testing process.

A well-rounded penetration testing team with diverse skills and experience is crucial for a successful penetration testing project. The team should work together to identify and remediate vulnerabilities and provide actionable recommendations to improve the organization's security posture.

Penetration Testing Types

Network Services Penetration Testing

In the realm of pentesting, this is the most common and requested test to do for a client. This kind of test involves discovering network infrastructure security flaws and weaknesses. This test can be conducted onsite at the company's location or remotely. To collect as much information as possible, it is highly recommended to use both strategies. A network services pentest aims to discover security flaws and vulnerabilities in the system prior to their exploitation by malicious actors. The following are examples of some of the services and devices that are scanned for vulnerabilities in this type of test:

Firewall

- DMZ
- IPS/IDS
- VPN
- Routers and switches
- DNS

- Remote Access Protocols
- Workstations
- Printers

Web Application Penetration Testing

This kind of test is significantly more comprehensive. This test detects security flaws or vulnerabilities in web-based applications. Web application penetration testing *is* considered much more complicated. Thus, a significant amount of time is required to accurately and fully test the web application vulnerabilities. The Open Web Application Security Project (OWASP) is a free and open community of experts working to make the web a safer place for users and other entities. The findings of a web application penetration test should include the vulnerabilities discovered and any successful exploits. This information may assist the company in determining how to prioritize vulnerabilities and implement remedies. The OWASP "Top 10" is a set of guidelines for common vulnerabilities and how to avoid them. Security professionals must refer to OWASP TOP in order to design a secure application.

OWASP's Top 10 web application vulnerabilities:

- Broken access control
- Injection
- Cryptographic failures
- Insecure design
- Vulnerable and outdated components
- Security misconfiguration
- Identification and authentication failures
- Security logging and monitoring failures
- Software and data integrity failures
- Server-side request forgery (SSRF)

Physical Penetration Testing

As technology continues to advance, so do the threats it poses. Unfortunately, some businesses are still ignorant of this and continue to disregard the hazards posed by physical security vulnerabilities, leaving them open to external threats such as burglaries, corporate espionage, and natural catastrophes such as fires and floods. Even in a "flawless" building, an obscure technique may remain to get entry. A physical penetration test becomes very important in this situation. During a physical pentest, security measures, including locks, cameras, sensors, and obstacles, are examined for any flaws that might allow an attacker to break through. A server room, for instance, may be subjected to a physical pentest in order to determine the likelihood of an intruder gaining access to sensitive data. This entryway provides potential access to the internal company network. Social engineering, badge cloning, tailgating, and other forms of physical attack may all be evaluated via physical penetration testing. By the time this pentest is complete, the company will have been informed of any physical security loopholes found and recommendations for closing them. The following processes can also be put in place to protect the organization against physical attacks (OWASP, 2021)

- Testing access controls
- Perimeter assessment
- Testing for alarm responses
- Location review
- Environmental analysis

Social Engineering Penetration Testing

A social engineering pentest is an exercise designed to test a company's preparedness for, and response to, a social engineering attack. This kind of penetration test attempts to determine how an organization will respond in the event of a social engineering attack. The company is presented with a report that may assist, build, or strengthen an awareness program and related security policies. A social engineering attack aims to induce a company's workers or other parties with access to the company's resources to reveal sensitive information or credentials by using deception, threats, or extortion.

Client-Side Penetration Testing

A client-side pentest aims to identify readily exploitable software flaws on a client device, such as a workstation or web browser. It is common for a client-side pentest to reveal previously unknown threats. Examples include clickjacking, malware infections, HTML injections, and cross-site scripting (XSS) attacks.

Mobile Application Penetration Testing

A mobile penetration test attempts to attack how a mobile application receives user input, how securely it is kept on the phone, how securely it is transported over the internet, and any web service vulnerabilities that may exist in the API. (Core Sentinel, 2018)

Wireless Pentesting

As the name indicates, this test comprises inspecting all wireless devices utilized in a company. Tablets, laptop computers, cellphones, and other similar devices fall under this category. A cybercriminal may find it simple to infiltrate your system via wireless networks. No locks need to be picked, no one has to be deceived, and the whole operation can be done, for example, from a parking lot. In certain cases, it may provide attackers access to a network within a company without needing to go through a firewall. In fact, hackers use a technique called "war driving" to find targets. This method involves utilizing computers, cellphones, and other mobile devices while driving to look for a WiFi network. Due to the prevalence of wireless networks as a target for hackers, wireless penetration testing is a requirement of several security standards (including PCI DSS, SOC2, and HIPAA). This in-depth analysis of wireless network's risks enables businesses to recognize exposure, calculate the consequences of failure, and allocate resources effectively. The following are also examined for security flaws:

- Wireless protocols
- Administrative credentials
- Wireless access points

- WiFi networks
- Mobile networks
- Wireless devices like mice and keyboards
- Bluetooth-enabled printers and scanners
- RFID and other RF technologies
- Bluetooth devices

Penetration Testing Methodologies

Before assessing networking devices and system vulnerabilities, the process for conducting penetration tests inside a company must be established. The following processes are part of the penetration testing process:

- Scope establishment
- Pentest execution
- Results reporting and delivery

Scope Establishment

Prior to conducting a penetration test, it is required to determine the testing scope. The whole infrastructure and individual components, such as routers, web servers, DNS servers, firewalls, FTP servers, and mail servers, can be tested using the same criteria. That is why it is very important to define the scope with the client before conducting any kind of test.

Pentest Execution

Every organization must ensure that the pentest they are employing are adequate. This includes acquiring all relevant information about security vulnerabilities. It is the tester's obligation to ensure that the networks, systems, and applications are not subject to security risks that might allow unauthorized access.

Results Reporting and Delivery

Upon the completion of the penetration testing, the pentesters review all information produced from the testing procedure. The following information is included in the delivery report:

- A prioritized list of vulnerabilities and threats
- Details on the current security system's strengths and weaknesses
- Risk levels classified as high, medium, or low
- Details on the vulnerabilities of each device

Pentesters also give recommendations for addressing discovered vulnerabilities as well as provide technical knowledge on how to remedy system flaws. They can also supply the business with beneficial resources that may be useful for seeking further information or fixes to remedy discovered vulnerabilities.

Required Skill Sets for a Penetration Tester

Penetration testers get training in a variety of technical and nontechnical skills that enable them to test client networks in a professional and ethical manner. Many testers are skilled programmers who are familiar with many languages that may be used to create vulnerabilities and payloads. In addition to being proficient coders, ethical hackers need to be well-versed in networking and network protocols. They must comprehend how actual attackers get unauthorized access by using protocols like DNS, TCP/IP, and DHCP.

Soft skills are essential for success in the field of penetration testing. Part of a penetration tester's duty is to solve complex challenges quickly and creatively. Ethical hackers must be able to think critically and solve problems creatively, since many attacks fail or do not go as planned.

Penetration Testing Methodology

Penetration testing methodologies provide uniform execution with outcomes that can be verified and repeated and are tailored to a certain level of security. As a result, pentesters are able to organize their testing/attack strategy depending on the data they have collected.

Penetration Testing Methodologies List

The following methodology assists a penetration tester by systematically applying the testing pattern.

Open-Source Security Testing Methodology Manual (OSSTMM)

It is a set of typical penetration tests that are used to generate security metrics. It is generally accepted as the de facto standard for the highest level of testing, assuring exceptional consistency and accuracy.

Source: https://www.isecom.org/OSSTMM.3.pdf

Open Web Application Security Project (OWASP)

Offers a collection of tools as well as a knowledge base to aid with the protection of web applications. It is useful for developers, system architects, customers, vendors, and cybersecurity experts who might be involved in developing, deploying, and testing web application and web service security.

Source: https://www.owasp.org/images/1/19/OTGv4.pdf

Penetration Testing Execution Standard

A set of guidelines was developed by InfoSec experts with the intention of establishing a uniform procedure for doing penetration testing. By adhering to the Penetration Testing Execution Standard (PTES), businesses of all sizes are able to conduct a successful pentest that reveals any cybersecurity flaws.

NIST 800-115

An in-depth technical manual for doing audits and reviews of information security. It gives a reasonably high-level overview of planning, executing, and maintaining inspection and testing methods and procedures for technical information security. It is designed to assist organizations in organizing and performing tests to discover flaws in a network or system and confirm compliance with a policy or other standards.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Penetration Testing Framework

Is an open-source, step-by-step manual for conducting penetration tests, including a framework that covers each stage of the process in depth. In addition, examples of how the security testing tools were put to use across various types of testing are provided. The PTF is an all-inclusive, practical manual for doing penetration tests.

Source: http://www.pen-tests.com/penetration-testing-framework.html

Information Systems Security Assessment Framework (ISSAF)

A comprehensive resource for pentesting that includes project management and testing sections. Even though it is no longer maintained and hence a bit out of date, its strength is that it links particular pentest techniques with pentesting mechanisms. Its goal is to provide an all-inclusive manual for running a pentest, and it may serve as a template for creating your own unique approach.

Source: https://sourceforge.net/projects/isstf/, https://untrustednetwork.net/files/issaf0.2.1.pdf

Frequency of Penetration Testing

The frequency of penetration testing depends on several factors, such as the size of the organization, the complexity of the IT infrastructure, the nature of the business, and the regulatory requirements. In general, penetration testing should be conducted on a regular basis to ensure the security of the organization's systems and data. For instance, organizations required to comply with the PCI DSS must conduct external penetration tests at least once a year and after any significant infrastructure or application upgrade or modification. The frequency of penetration testing should be determined by a risk-based approach that takes into account the level of risk associated with the organization's assets and the potential impact of a security breach. For example, a financial institution that handles sensitive customer data and processes transactions online may require more frequent and thorough penetration testing compared to a small retail store that only has a basic website.

In addition to risk, variables including new system or application rollouts, large software upgrades, and shifts in network design can affect how often penetration testing is performed. These changes may create new vulnerabilities and necessitate further testing to verify that the organization's security posture remains robust. Penetration testing is often performed once a year or twice a year, with more regular testing for mission-critical systems or applications. Nevertheless, this approach may not be appropriate for all businesses and may need to be modified based on the organization's particular risk profile and IT infrastructure.

Due to the dynamic nature of the threat landscape and the ever-changing nature of the IT landscape, penetration testing is not a one-and-done task but rather one that must be performed continuously. Testing on a regular basis can assist in uncovering any security flaws that have been left unpatched over time and strengthen the company's defenses against cyberattacks.

Certifications that Pentesters may Acquire

A qualified penetration tester needs to possess at least one of the following credentials; however it is not required.

Offensive Security Certified Professional (OSCP)

This is the minimum proficiency requirement for an entry-level penetration tester. It is a highly regarded, rigorous certification for anyone working in information security. Achieving and maintaining this certification demonstrates that you have the skills necessary to do penetration

testing using the tools provided by the Kali Linux distribution. Kali is a free and open-source Linux distribution based on Debian that can be used to conduct penetration tests and other security-related tasks.

Offensive Security Certified Expert (OSCE)

In terms of penetration testing expertise, OSCEs are at the highest level. OSCEs show an exceptional level of perseverance, drive, and capacity to execute under pressure throughout the rigorous 48-hour test, and they are also able to think creatively and outside the box to devise novel techniques to penetrate internal networks. They've already established that they can develop their own exploits, launch attacks, and compromise systems in order to get root privileges. An OSCE is also acquainted with sophisticated security measures such as ASLR.

GIAC Penetration Tester (GPEN)

GIAC, a subsidiary of SANS, is regarded as a prominent authority for a range of certifications. The GIAC Penetration Tester (GPEN) certificate is one of GIAC's pentesting credentials. GPEN focuses on pentesting methodology, best practices, and pentesting legal problems. The certification is valid for four years. (Tollefson, 2022)

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

GXPN is an expert certification that is significantly difficult to pass. The essential skills include exploitation of Windows and Linux, penetration testing, network attacks, cryptography, and familiarity with technologies and terms such as Python, Scapy, and Fuzzing. After rigorous training, candidates can also conduct customized fuzzing test sequences. Individuals who get this certification may professionally simulate and report on security threats. The GXPN credential is issued after completing a three-hour, 60-question exam. However, the activities need more than just knowledge. A novice penetration tester cannot pass this examination. GIAC certifications typically cost around $2,500.

LPT – Licensed Penetration Tester

The LPT certification is the most sophisticated one granted by the EC Security Council. Those who possess this certification are often regarded as specialists in their profession. The LPT practical examination lasts a staggering 18 hours.

Above are just some examples of penetration testing certifications. The list is not exhaustive.

Why Companies Should do Penetration Testing

- To verify the effectiveness of existing security measure controls and how they are implemented and placed.
- In order to design defenses against the infrastructure, programs, or process flaws that have been uncovered in software, people, and hardware.
- To investigate the consequences of numerous vulnerabilities and how they could be linked together.

- To assess how well input validation rules in an application are working. Wherever user input is submitted, fuzz is undertaken to ensure that only sanitized input is allowed.
- To make it faster for security to respond. An internal penetration test may be used to evaluate and enhance incident response processes and procedures by revealing how various groups manage intrusions.

Penetration Testing's Advantages

Penetration testing reveals flaws that conventional methods would not have detected, such as vulnerability scanning. False positives are taken away due to the manual, human assessment. Furthermore, it displays what access and data may be acquired by trying to exploit weaknesses uncovered in the same manner that a real-world attacker would. This clearly displays the true risk of successful exploitation, given each flaw exploited. Penetration testing will also put an organization's cyber defenses to the test. It is also used to evaluate the performance of intrusion detection systems (IDS), intrusion prevention systems (IPS), web application firewalls (WAF). These systems should trigger alarms and internal procedures during a penetration test, prompting a response from security operations staff. Companies conduct penetration testing to ensure they are in compliance with standards like PCI-DSS and ISO 27001's control objective A12.6.

Phases of Pentesting

Pre-attack phase: This phase focuses on collection about the target as much as possible. It can be intrusive, such as scanning for information, or non-intrusive, such as checking public records.

The majority of leaked information is about network structure and the types of services available on the network infrastructure. The penetration tester uses this data to map out the target network infrastructure in order to organize a more coordinated attack method later. The pre-attack phase includes active and passive reconnaissance, which will be discussed in detail in the "Foot printing and Reconnaissance chapter."

Attack Phase

In this phase, the penetration tester compromises the actual target. An attacker might gain entry to the system by exploiting a weakness discovered in the pre-attack phase or using security vulnerabilities such as a poor security policy. Companies need to defend many entry points, even when an attacker only requires one. Once inside, the attacker might elevate privileges and implant a shell to maintain access to the system and exploit it. We will discuss this phase in detail in the "System Hacking" chapter 8.

Actions Taken After an Attack

This stage is essential to every penetration test since it is the tester's responsibility to restore the systems to their pre-test condition. The purpose of the test is to identify security flaws, and this phase must be completed unless the penetration test agreement is modified to assign the tester the responsibility of improving the security posture of the systems. The following procedures are included in this phase's activities:

- Deleting all files that have been uploaded to the system
- Removing any vulnerabilities produced during the test and cleaning up any registry entries

- Undoing all file and setting modifications performed during the test
- Undoing any modifications in privileges and user settings
- Eliminating all tools and exploits from the systems that have been tested
- Bringing the network back to the pre-testing stage by eliminating shares and connections
- Network state mapping
- Documenting and recording all logs generated throughout the test
- Analyzing and reporting all findings to the organization.

Points to Consider Before Signing a Contract

During the penetration test, some of the activities may pose certain risks and cause unwanted organization situations, such as a denial-of-service condition that locks out critical accounts or crashes critical servers and applications.

Some of the risks arising from penetration testing are:

- Testers can gain access to the protected or sensitive data after a successful penetration test attempt.
- Testers can obtain information about the vulnerabilities existing in the organizational infrastructure.
- DoS penetration testing can bring the organization's services down.

Organizations can avoid such risks by signing a non-disclosure agreement (NDA) and other legal documents, including details about what is and is not allowed to the penetration testing team. A social engineering attack attempts to convince or manipulate personnel or others with access to company assets into giving information and credentials.

Most Commonly Used Penetration Testing Tools

Depending on what you are testing, you may choose from a broad range of penetration testing tools in your toolbox. As the most popular Linux distribution among penetration testers, Kali contains the vast majority of these tools. The scope of this discussion is just too wide to include every possible testing method. Nevertheless, the below are tools you must become well acquainted with:

1. Nmap's primary function was to "map" networks by discovering hosts and scanning their ports. But now it can be used for host ID, service ID, and vulnerability detection, which together efficiently enumerate all services running on a host (s) and any vulnerabilities discovered on them.

   Source: https://nmap.org/

2. Netcat is a versatile network utility that facilitates communication between computers, chat sessions, file transfers, port redirection, and the execution of both forward and reverse shells on connect, earning it the nickname "Swiss Army knife" of the network world. Here is a great reference sheet from SANS: source: https://www.sans.org/security-resources/sec560/netcat – cheat sheet v1.pdf.

3. Burp (or Burp Suite) is a toolkit for doing penetration tests on websites created by Portswigger. This is the tool of choice for serious web application security researchers

and bug bounty hunters. Its user-friendliness is a better option than similar free tools like OWASP ZAP. It is a graphical tool used to perform security testing of web applications, from basic mapping and analysis of a web app's threat landscape to discovering and exploiting security flaws.

Source: https://portswigger.net/burp/

4. **SQLMap**: SQLMap is a free and open-source tool for discovering and exploiting SQL injection vulnerabilities and gaining control of database servers. From database identification and data retrieval to file system access and OS command execution through out-of-band connections, this tool has it everything. It also has a robust detection engine and numerous specialized capabilities for the most advanced penetration tester.

   Source: http://sqlmap.org/

5. **Nessus**: As a penetration tester, if you need to check for security flaws, Nessus is a good choice. When doing a penetration test, it is common practice to employ a vulnerability scanner to look for uninstalled updates and easy targets. The scan finds vulnerabilities that can be detected by a scan and exploited as a jumping-off point for an exploit to acquire rapid access.

   Source: https://www.tenable.com/products/nessus-vulnerability-scanner

6. The Metasploit Framework is a modular penetration testing platform based on Ruby that allows you to build, test, and run exploit code. The Metasploit Framework includes a set of tools for testing security flaws, enumerating networks, executing attacks, and evading detection. The Metasploit Framework is, at its root, a set of widely used tools that offer a full platform for pentesting and exploit creation. Source: https://www.metasploit.com/

7. Python is the most widely used language for penetration testing and cybersecurity. Python is an excellent language to learn if you are an expert penetration tester interested in modifying or designing your own tools. It contains simple code and a modular architecture, and there are several libraries that you may use to develop your own security tools, ranging from modules that do basic I/O operations to libraries that produce API calls for particular platforms.

   Source: https://www.python.org/

8. **Bash**: When doing a penetration test, familiarity with the bash shell and scripting using the various Linux command line tools is crucial. To prepare data for display or import into another program, you should be able to build together individualized scripts easily.

9. **Google**: During a penetration test, Google is a great place to obtain open-source information that might be useful, such as the location of potentially sensitive documents that should not be publicly accessible. The Google Hacking Database (GHDB) is another great resource for finding public exploits and sensitive information. We will cover this topic in detail in the subsequent chapters.

   Source: https://www.exploit-db.com/google-hacking-database/

Pentesting Use Cases

Penetration testing is an essential method for finding security flaws and securing an organization's defenses. Some common use cases for penetration testing include:

1. **Compliance requirements**: Many firms must adhere to industry rules and standards, including HIPAA, PCI-DSS, and ISO 27001. In order to prevent hefty penalties and legal

concerns, these businesses can use penetration testing to ensure they are in compliance with regulations. For instance, HIPAA mandates frequent testing and evaluation of IT security, making penetration testing a crucial part of the compliance process.

2. **Risk management**: Regular penetration testing can assist firms in locating possible security problems and addressing them before they are taken advantage of by criminal actors. In the long run, this can assist in lessening the likelihood of security incidents and data breaches. Penetration testing, for instance, can be used to determine the effectiveness of anti-malware solutions and to locate and fix vulnerabilities in the network security architecture.
3. **Incident response planning**: As part of an organization's incident response planning, penetration testing can be performed to detect possible security vulnerabilities and build plans for responding to security incidents. Penetration testing, for instance, can mimic a malicious attack to expose security flaws such as insecure configurations, a lack of patching, and inadequate access control.
4. **Application security**: Penetration testing can be used to find weaknesses in software utilized by a company, including web applications, mobile applications, and other software. This can assist in improving application security and avoiding threats like SQL injection and XSS.
5. **Network security**: Penetration testing can be utilized to uncover flaws in a company's network infrastructure, such as firewalls, routers, and switches. As a result, the network's overall security can be improved, and unwanted intrusions and data breaches can be avoided.
6. **Third-party security**: Many businesses rely on third-party suppliers and partners for a variety of services, such as IT infrastructure and software. In order to determine whether or not these outside providers are upholding adequate security measures, penetration testing can be performed.

Opportunities and Challenges

Penetration testing presents a number of challenges, such as ensuring that the testing process is morally and legally acceptable, accurately identifying vulnerabilities, and developing efficient remedial processes. Also, it may be challenging to find a balance between the need for rigorous testing and the expenses and effort that go along with it. Nonetheless, these difficulties also provide opportunities for development and improvement.

Establishing a continuous testing plan that permits ongoing monitoring of a company's security posture is one opportunity. If vulnerabilities are found and fixed using this approach, the probability of data breaches and other security issues can be decreased. Penetration testing can serve as a component of a larger cybersecurity strategy that often includes things like risk assessments, incident response plans, and regular employee security training. Businesses can assess the efficiency of their security measures and the extent to which their staff is aware of and follows corporate security policies and procedures.

Trends and Emerging Technologies

The field of penetration testing is always changing as new technologies come out and threat actors come up with new tactics and techniques. Some of the most recent developments and trends in the industry include:

- **Cloud Security Testing**: As more businesses move their operations to the cloud, a greater need is being felt for penetration testing services that are especially made to evaluate the security of cloud-based systems and apps. The cloud environment is quite distinct from traditional IT infrastructure; thus, security testing must be done differently. Services for cloud security testing assist businesses in securing their data, identifying possible vulnerabilities, and assuring compliance with security laws.
- **IoT Security Testing**: With more connected devices in use today, IoT security testing is receiving more attention. This entails evaluating the security of gadgets, including wearables, industrial IoT devices, and smart home assistants. This is especially important given the potential impact these devices can have on people's lives and the potential for malicious actors to use them to gain access to sensitive data or disrupt services. IoT security testing can be performed to find flaws and make sure that devices are safe before they are made available to the public.
- **Artificial Intelligence and Machine Learning**: As threat actors become more sophisticated, the need for penetration testing tools and procedures that combine artificial intelligence and machine learning increases. These technologies can assist in identifying trends and anomalies that can point to a security risk. Machine learning techniques, for instance, can be utilized to find suspicious behavior in system log data, such as login attempts from odd places or odd times. Moreover, AI can be utilized to detect malicious code injected into networks or web applications, assisting in the early detection of possible risks.

References and Resources

There are many resources available for those interested in learning more about penetration testing, including books, online courses, and certification programs. These include:

- **The Penetration Testing Execution Standard (PTES)**: This is a framework for conducting penetration tests that includes precise instructions for the different testing phases. The PTES provides a comprehensive foundation for carrying out penetration tests in an ethical and consistent manner. In addition to outlining the essential procedures and stages for completing the tests correctly, it specifies the test's scope. It also includes instructions on risk assessment and ways to present the findings.
- **The Metasploit project**: This is an open-source framework for penetration testing that has a number of techniques and tools for evaluating security. It allows users to create custom exploit code, test security systems, and do vulnerability analyses. It also has a database of known flaws and exploits, which makes it simpler for users to identify and minimize security risks.
- **The OWASP Top 10**: This is a list of the top 10 web application security risks, as identified by the Open Web Application Security Project (OWASP). It is a valuable resource for anyone involved in web application security testing. This list contains the most common and most critical security risks to web applications, and provides guidance on how to identify, mitigate and prevent these issues. It is regularly updated to keep up with the latest security threats, making it an invaluable resource for any web application security professional.

In addition to these resources, there are also many online communities and forums where penetration testers can connect with one another, share ideas and best practices, and stay up to date on the latest trends and emerging technologies in the field. These communities provide a great opportunity for penetration testers to network, learn from each other, and stay on top of industry developments. They also serve as a support system for professionals in the field, allowing them to ask questions and get feedback from other experienced professionals.

REFERENCES

Core Sentinel (2018). *Definitive guide to penetration testing*. https://www.coresentinel.com/definitive-guide-penetration-testing/.

OWASP Top 10:2021 (2021). *OWASP Top 10 – 2021*. https://owasp.org/Top10/.

Tollefson, R. (2022). *Top 10 penetration testing certifications for security professionals*. Infosec Resources. https://resources.infosecinstitute.com/topic/top-5-penetration-testing-certifications-security-professionals/.