PENETRATION TESTING

Chapter 9

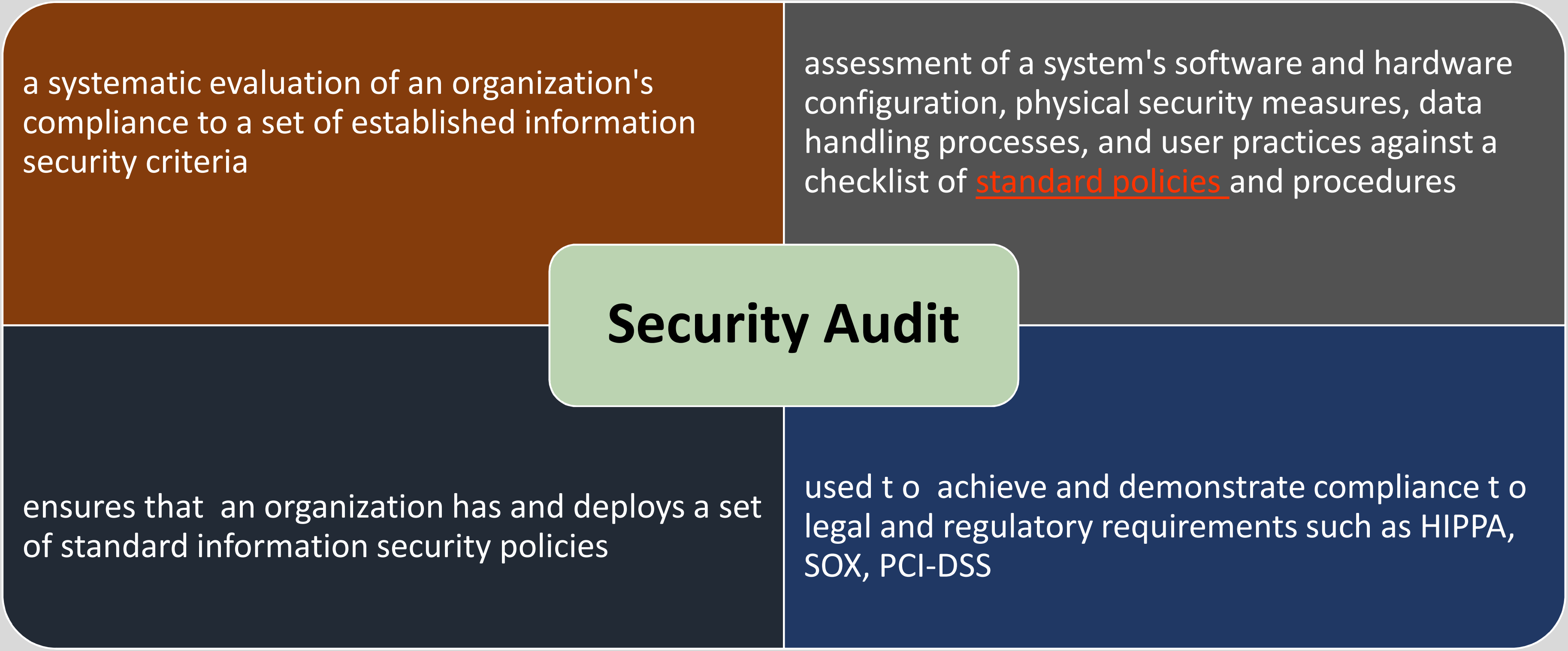
Topic

- Security Assessment
- Penetration Testing
- PT Methodology
- PT Tool
- Limitation of PT
- Summary

Security Assesement

What is Security Assesment

- Security Audits
  - Focus on the people and processes
  - To design, implement, and manage security on a network.
  - There is a baseline involved for processes and policies within an organization.
  - use the specific baseline to audit the organization
- Vulnerability Assessment
  - identifying security vulnerabilities.
- Penetration Testing
  - act of testing an organization' s security by simulating the actions of an attacker



Security Audit

a systematic evaluation of an organization's compliance to a set of established information security criteria

assessment of a system's software and hardware configuration, physical security measures, data handling processes, and user practices against a checklist of standard policies and procedures

ensures that an organization has and deploys a set of standard information security policies

used to achieve and demonstrate compliance to legal and regulatory requirements such as HIPPA, SOX, PCI-DSS

Vulnerability Assesments

Network Scanning

- Scan Network for known security weaknesses
- Based on CVE

Test/System Network

- Finding exposure to common attacks
- search for computers exposed t o known or publicly reported vulnerabilities

Security Mistake

- Identify common security configuration mistakes

Scanning Tools

- Host Based (weak file access permission, poor password, logging faults)
- Network Based(open ports, app sec. exploit and buffer overflow)

VA limitation

Security

- The methodology used as well as the diverse vulnerability scanning software packages assess security differently

Detection

- Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

Update

- It must be updated when new vulnerabilities are discovered or modifications are made to the software being used

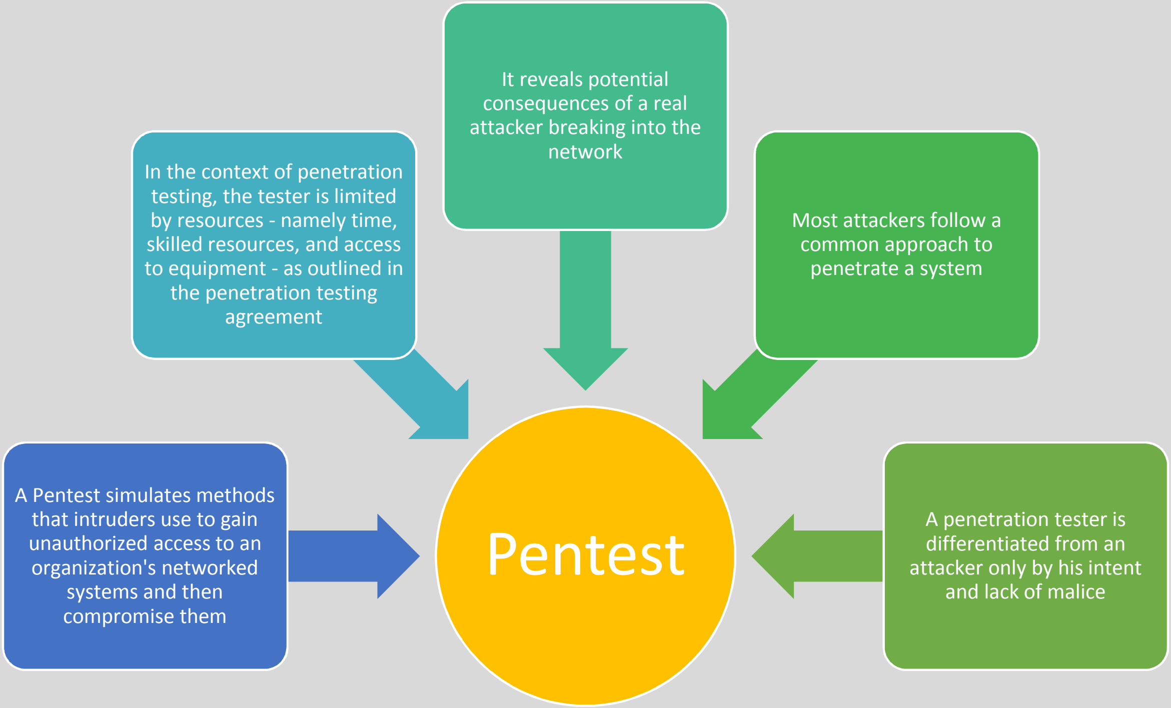
Influence

- It does not measure the strength of security controls

Penetration Testing (PT)

PT

- find flaws in the system in order to take appropriate security measures to protect the data and maintain functionality



Pentest

It reveals potential consequences of a real attacker breaking into the network

In the context of penetration testing, the tester is limited by resources - namely time, skilled resources, and access to equipment - as outlined in the penetration testing agreement

Most attackers follow a common approach to penetrate a system

A Pentest simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them

A penetration tester is differentiated from an attacker only by his intent and lack of malice

Why PT ? 1

- Computer related crime is on the rise.
- Find holes now before somebody else does.
- Report problems to management.
- Verify secure configurations.
- Security training for network staff.
- Discover gaps in compliance.
- Testing new technology.

Why PT ? 2

- You can identify the threats facing an organization's information assets.
- You can reduce an organization's IT security costs and provide a better Return On IT Security Investment (ROSI) by identifying and resolving vulnerabilities and weaknesses.
- You can provide an organization with assurance: a thorough and comprehensive assessment of organizational security covering policy, procedure, design, and implementation.
- You can gain and maintain certification to an industry regulation (BS7799, HIPAA, etc.).
- You can adopt best practices by conforming to legal and industry regulations.
- You can test and validate the efficiency of security protections and controls.
- It focuses on high-severity vulnerabilities and emphasizes application-level security issues to development teams and management.
- It provides a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation.
- You can evaluate the efficiency of network security devices such as firewalls, routers, and web servers.
- You can use it for changing or upgrading existing infrastructure of software, hardware, or network design.

Why PT is different from SA and VA

SA	VA	PT
• A security audit just checks whether the organization is following a set of standard security policies and procedures	• A vulnerability assessment focuses on discovering the vulnerabilities in the information system but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability	• Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attacker

Role of a Penetration Tester

- A penetration tester has the following roles −
  - Identify inefficient allocation of tools and technology.
  - Testing across internal security systems.
  - Pinpoint exposures to protect the most critical data.
  - Discover invaluable knowledge of vulnerabilities and risks throughout the infrastructure.
  - Reporting and prioritizing remediation recommendations to ensure that the security team is utilizing their time in the most effective way, while protecting the biggest security gaps.

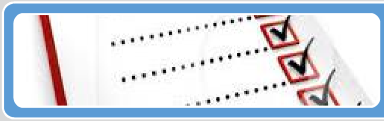
Certification

- A certified person can perform penetration testing.
- Certification held by the tester is the indication of his skill sets and competence of capable penetration tester.
- Following are the important examples of penetration testing certification
  - Certified Ethical Hacker (CEH).
  - Offensive Security Certified Professional (OSCP).
  - CREST Penetration Testing Certifications.
  - Communication Electronic Security Group (CESG) IT Health Check Service certification.
  - Global Information Assurance Certification (GIAC) Certifications for example, GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Advance Penetration Tester (GXPN), and GIAC Exploit Researcher.

When to Perform Penetration Testing ?

- Security system discovers new threats by attackers.
- add a new network infrastructure.
- update system or install new software.
- Relocation of office.
- set up a new end-user program/policy.

What is good PT



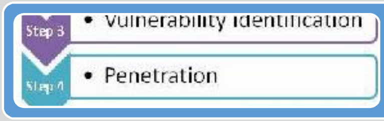
Establish the parameters for the penetration test such as objectives, limitations, and the justification of procedures.

The establishment of these parameters helps you in know the purpose of conducting penetration test.

Hire skilled and experienced professionals to perform the test.

If the penetration testing is not done by the skilled and experienced professionals there are chances of damaging the live data and more harm can happen than the benefits.

Choose a suitable set of tests that balance cost and benefits.



Follow a methodology with proper planning and documentation.

It is very important to document the test at each phase for the further references.

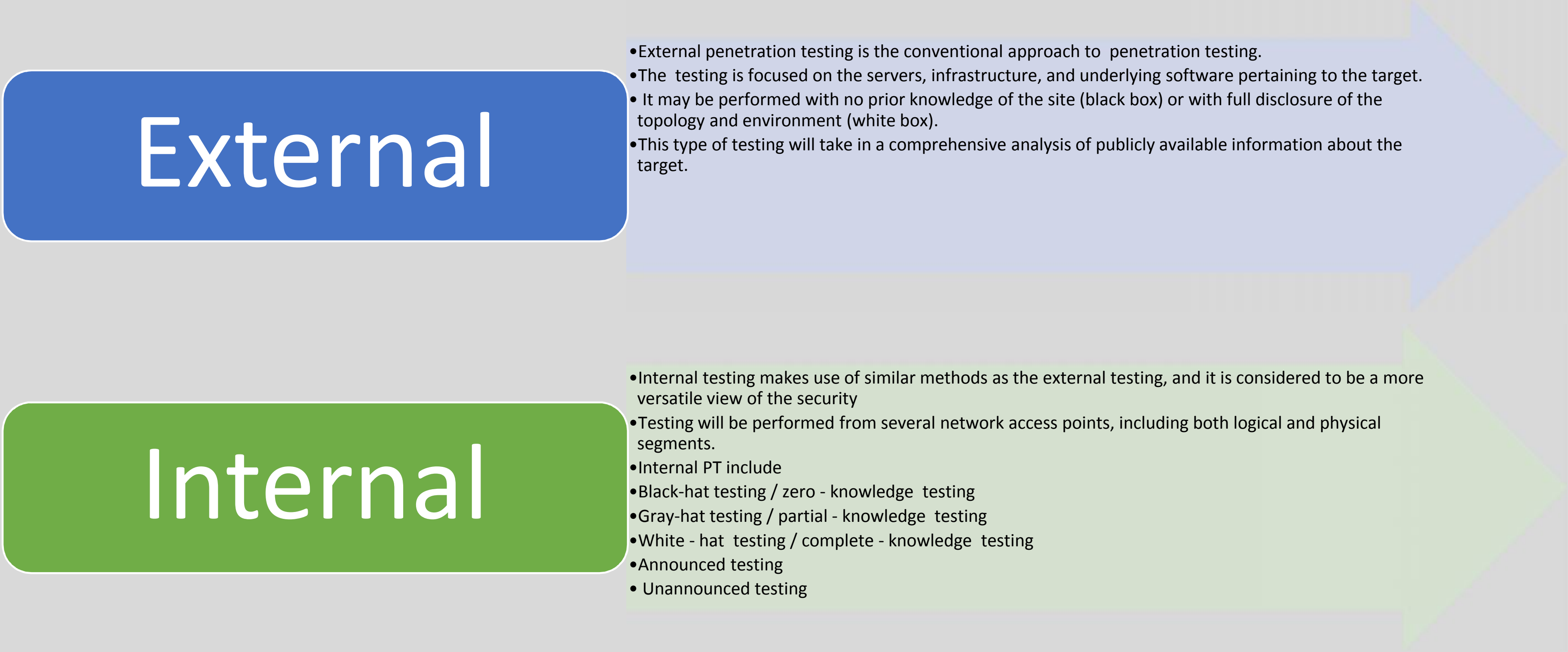
Document the result carefully and making it comprehensible for the client.

State the potential risks and findings clearly in the final report.

Testing Location

- The pentest team may have a choice of doing the test either remotely or on-site
- A remote assessment may simulate an external hacker attack. However, it may missassessing internal guards
- An on-site assessment may be expensive and may not simulate an external threat exactly

Types of PT



External

- External penetration testing is the conventional approach to penetration testing.
- The testing is focused on the servers, infrastructure, and underlying software pertaining to the target.
- It may be performed with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (white box).
- This type of testing will take in a comprehensive analysis of publicly available information about the target.

Internal

- Internal testing makes use of similar methods as the external testing, and it is considered to be a more versatile view of the security
- Testing will be performed from several network access points, including both logical and physical segments.
- Internal PT include
- Black-hat testing / zero - knowledge testing
- Gray-hat testing / partial - knowledge testing
- White - hat testing / complete - knowledge testing
- Announced testing
- Unannounced testing

Wireless Security Penetration Testing

- Wireless technology of your laptop and other devices provides an easy and flexible access to various networks.
- The easily accessible technology is vulnerable to unique risks; as physical security cannot be used to limit network access.
- An attacker can hack from the remote location.
- Hence, wireless security penetration testing is necessary for your company/organization.
- The following are the reasons for having wireless technology −
  - To find the potential risk caused by your wireless devices.
  - To provide guidelines and an action plan on how to protect from the external threats.
  - To improve the overall security system.
  - For preparing a comprehensive security system report of the wireless networking, to outline the security flaw, causes, and possible solutions.

Black Box Testing

- Pen tester carries out the test without having any prior knowledge the target.
- Simulate real-world attacks and minimize false positives,
- A zero-knowledge attack, with no information or assistance from the client
- Map the network while enumerating services, shared file systems and operating systems discreetly
- Drawback: Time consuming and expensive type of test

Gray Box Testing

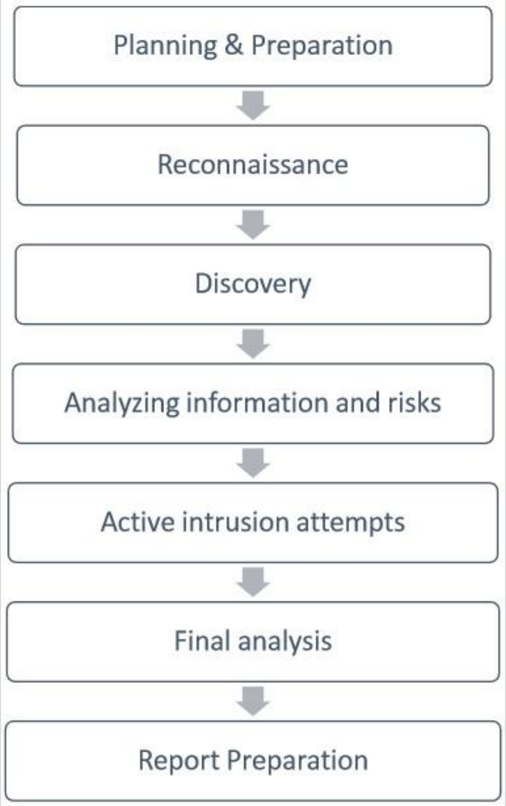
- In gray-box penetration testing, the test is conducted with limited knowledge about infrastructure, defense mechanism, and communication channels of the target on which test is to be conducted.
- It is simulation of those attacks that is performed by the insider or outsiderwith limited accesses privileges
- organizations would prefer to provide the pen testers with partial knowledge or information that hackers could find

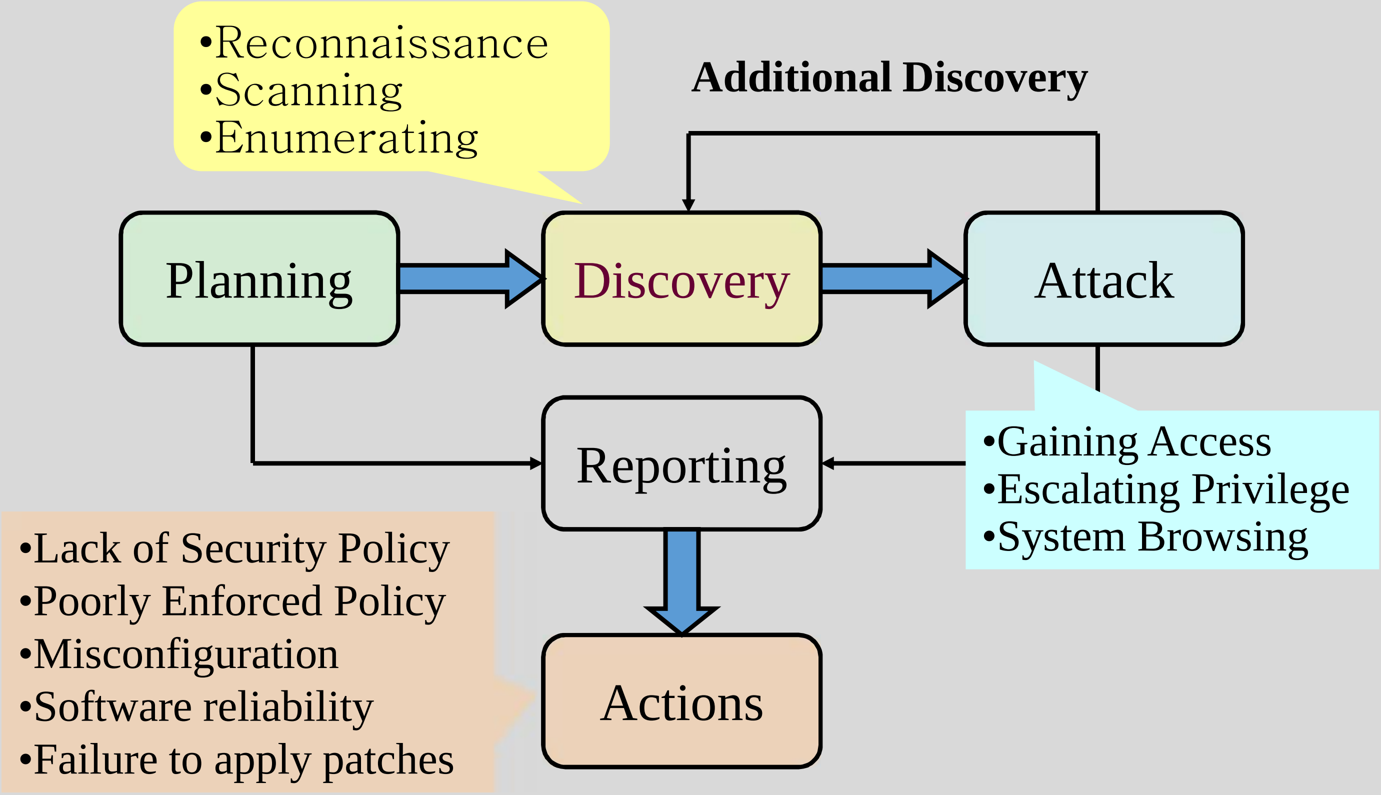
White Box Testing

- conducted with full knowledge of infrastructure, defense mechanism, and communication channels of the target on which test is being conducted
- In this case, the complete information about the target is given t o the pen testers.
- The information provided can include network topology documents, asset inventory, and valuation information.

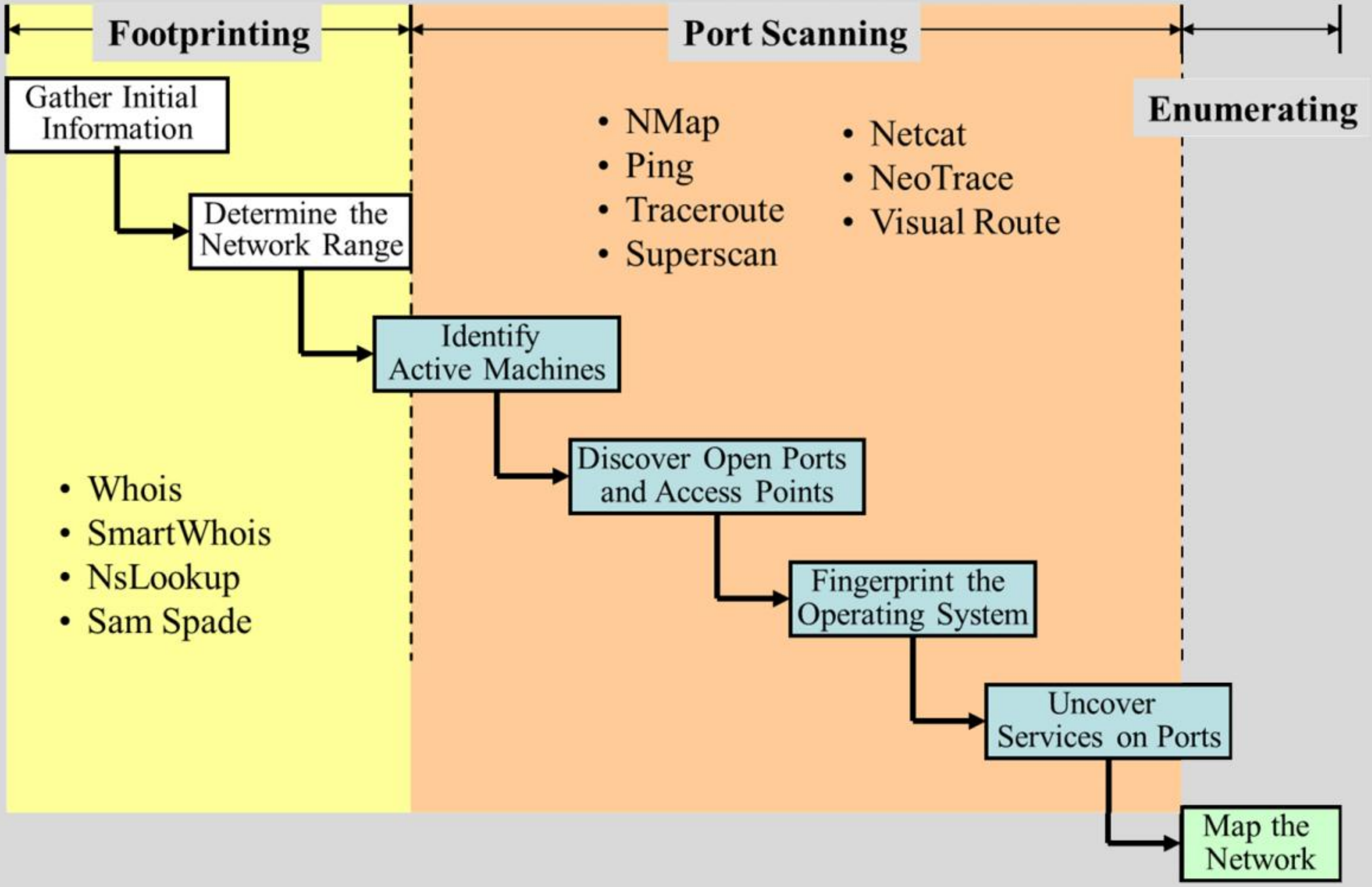
PT Methodology

Steps of Penetration Testing Method




•Reconnaissance
•Scanning
•Enumerating
Additional Discovery
Planning
Discovery
Attack
Reporting
•Gaining Access
•Escalating Privilege
•System Browsing
•Lack of Security Policy
•Poorly Enforced Policy
•Misconfiguration
•Software reliability
•Failure to apply patches
Actions

Discovery Phase of PT



Footprinting

Port Scanning

Enumerating

Gather Initial Information

Determine the Network Range

Identify Active Machines

Discover Open Ports and Access Points

Fingerprint the Operating System

Uncover Services on Ports

Map the Network

- Whois
- SmartWhois
- NsLookup
- Sam Spade

- NMap
- Ping
- Traceroute
- Superscan

- Netcat
- NeoTrace
- Visual Route

Planning & Preparation

- Planning and preparation starts with defining the goals and objectives of the penetration testing.
- The client and the tester jointly define the goals so that both the parties have the same objectives and understanding. The common objectives of penetration testing are −
  - To identify the vulnerability and improve the security of the technical systems.
  - Have IT security confirmed by an external third party.
  - Increase the security of the organizational/personnel infrastructure.

What are the Legal Issues?

- Following are some of the issues which may arise between a tester and his client −
  - The tester is unknown to his client – so, on what ground, he should be given access of sensitive data
  - Who will take the guarantee of security of the lost data?
  - The client may blame for the loss of data or confidentiality to tester
- Penetration testing may affect system performance, and can raise confidentiality and integrity issues; therefore, this is very important, even in an internal penetration testing, which is performed by an internal staff to get permission in writing.
- There should be a written agreement between a tester and the company/organization/individual to clarify all the points regarding the data security, disclosure, etc. before commencing testing.

- A **statement of intent** should be drawn up and duly signed by both the parties prior to any testing work. It should be clearly outlined that the scope of the job and that, you may and may not be doing while performing vulnerability tests.
- For the tester, it is important to know who owns the business or systems which are being requested to work on, and the infrastructure between testing systems and their targets that may be potentially affected by pen testing.
- The idea is to make sure;
  - **the tester** has the permission in writing, with clearly defined parameters.
  - **the company** has the details of its pen tester and an assurance that he would not leak any confidential data.
- A legal agreement is beneficial for both the parties.
- Remember, regulations change from country to country, so keep yourself abreast with the laws of the country.
- Sign an agreement only after considering the respective laws.

Define the PT Scope

- Network Security
- System Soft ware Security
- Client-side Application Security
- Server-side Application Security
- Social Engineering
- Application Communication Security
- Physical Security
- Dumpster Diving
- Inside Accomplices
- Sabotage Intruder Confusion
- Intrusion Detection
- Intrusion Response

Reconnaissance

- Reconnaissance includes an analysis of the preliminary information. Many times, a tester doesn’t have much information other than the preliminary information, i.e., an IP address or IP address block.
- The tester starts by analyzing the available information and, if required, requests for more information such as system descriptions, network plans, etc. from the client.
- This step is the passive penetration test, a sort of.
- The sole objective is to obtain a complete and detailed information of the systems.

Discovery

- In this step, a penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities.
- These tools normally have their own databases giving the details of the latest vulnerabilities.
- However, tester discover
  - **Network Discovery** − Such as discovery of additional systems, servers, and other devices.
  - **Host Discovery** − It determines open ports on these devices.
  - **Service Interrogation** − It interrogates ports to discover actual services which are running on them.

Technique of PT

Techniques	Description
Passive Research	Is used to gather all the information about an organization's system configurations
Open Source Monitoring	Facilitates an organization to take necessary steps to ensure its confidentiality and integrity
Net. Mapping and OS Fingerprinting	Is used to get an idea of the network's configuration being tested
Spoofing	Is the act of using one machine to pretend to be another Is used here for both internal and external penetration tests
Network Sniffing	Is used to capture the data as it travels across a network
Trojan Attacks	Are malicious code or programs usually sent into a network as email attachments or transferred via " Instant Message" into chat rooms
Bruteforce Attacks	Is the most commonly known password cracking method. Can overload a system and possibly stop it from responding to the legal requests
Vulnerability Scanning	Is a comprehensive examination of the targeted areas of an organization's network infrastructure
Scenario Analysis	Is the final phase of testing, making a risk assessment of vulnerabilities much more accurate

Analyzing Information and Risks

- In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system.
- Because of larger number of systems and size of infrastructure, it is extremely time consuming.
- While analyzing, the tester considers the following elements −
  - The defined goals of the penetration test.
  - The potential risks to the system.
  - The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.
- However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.

Active Intrusion Attempts

- This is the most important step that has to be performed with due care.
- This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks.
- This step must be performed when a verification of potential vulnerabilities is needed.
- For those systems having very high integrity requirements, the potential vulnerability and risk needs to be carefully considered before conducting critical clean up procedures.

Report Preparation

- Report preparation must start with overall testing procedures, followed by an analysis of vulnerabilities and risks.
- The high risks and critical vulnerabilities must have priorities and then followed by the lower order.
- However, while documenting the final report, the following points needs to be considered −
  - Overall summary of penetration testing.
  - Details of each step and the information gathered during the pen testing.
  - Details of all the vulnerabilities and risks discovered.
  - Details of cleaning and fixing the systems.
  - Suggestions for future security.

Content of Penetration Testing Report

- Executive Summary
  - Scope of work
  - Project objectives
  - Assumption
  - Timeline
  - Summary of findings
  - Summary of recommendation
- Methodology
  - Planning
  - Exploitation
  - Reporting
- Detail Findings
  - Detailed systems information
  - Windows server information
- References
  - Appendix

Manual Vs Automatic PT

Manual Penetration Testing	Automated Penetration Testing
It requires expert engineer to perform the test.	It is automated so even a learner can run the test.
It requires different tools for the testing.	It has integrated tools does required anything from outside.
In this type of testing, results can vary from test to test.	It has fixed result.
This test requires to remember cleaning up memory by the tester.	It does not.
It is exhaustive and time taking.	It is more efficient and fast.
It has additional advantages i.e. if an expert does pen test, then he can analyze better, he can think what a hacker can think and where he can attack. Hence, he can put security accordingly.	It cannot analyze the situation.
As per the requirement, an expert can run multiple testing.	It cannot.
For critical condition, it is more reliable.	It is not.

PT Tools

What are Penetration Testing Tools

Tool Name	Purpose	Portability	Expected Cost
Hping	Port Scanning Remote OC fingerprinting	Linux, NetBSD, FreeBSD, OpenBSD,	Free
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Free
SuperScan	Runs queries including ping, whois, hostname lookups, etc. Detects open UDP/TCP ports and determines which services are running on those ports.	Windows 2000/XP/Vista/7	Free

p0f	Os fingerprinting Firewall detection	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows, and AIX	Free
Xprobe	Remote active OS fingerprinting Port Scanning TCP fingerprinting	Linux	Free
Httprint	Web server fingerprinting SSL detection Detect web enabled devices (e.g., wireless access points, switches, modems, routers)	Linux, Mac OS X, FreeBSD, Win32 (command line & GUI	Free
Nessus	Detect vulnerabilities that allow remote cracker to control/access sensitive data	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Free to limited edition

GFI LANguard	Detect network vulnerabilities	Windows Server 2003/2008, Windows 7 Ultimate/ Vista, Windows 2000 Professional, Business/XP, Sever 2000/2003/2008	Only Trial Version Free
Iss Scanner	Detect network vulnerabilities	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SO1, Windows XP Professional with SP1a	Only Trial Version Free
Shadow Security Scanner	Detect network vulnerabilities, audit proxy and LDAP servers	Windows but scan servers built on any platform	Only Trial Version Free
Metasploit Framework	Develop and execute exploit code against a remote target Test vulnerability of computer systems	All versions of Unix and Windows	Free
Brutus	Telnet, ftp, and http password cracker	Windows 9x/NT/2000	Free

PT Limitation

Limitation of PT

- **Limitation of Time** − As all of us know, penetration testing is not at all time bound exercise; nevertheless, experts of penetration testing have allotted a fixed amount of time for each test. On the other hand, attackers have no time constrains, they plan it in a week, month, or even years.
- **Limitation of Scope** − Many of the organizations do not test everything, because of their own limitations, including resource constraints, security constraints, budget constraints, etc. Likewise, a tester has limited scope and he has to leave many parts of the systems that might be much more vulnerable and can be a perfect niche for the attacker.
- **Limitation on Access** − More often testers have restricted access to the target environment. For example, if a company has carried out the penetration test against its DMZ systems from all across its internet networks, but what if the attackers attack through the normal internet gateway.
- **Limitation of Methods** − There are chances that the target system can crash during a penetration test, so some of the particular attack methods would likely be turned off the table for a professional penetration tester. For example, producing a denial of service flood to divert a system or network administrator from another attack method, usually an ideal tactic for a really bad guy, but it is likely to fall outside of the rules of engagement for most of the professional penetration testers.
- **Limitation of Skill-sets of a Penetration Tester** − Usually, professional penetration testers are limited as they have limited skills irrespective of their expertise and past experience. Most of them are focused on a particular technology and having rare knowledge of other fields.
- **Limitation of Known Exploits** − Many of the testers are aware with only those exploits, which are public. In fact, their imaginative power is not as developed as attackers. Attackers normally think much beyond a tester's thinking and discover the flaw to attack.
- **Limitation to Experiment** − Most of the testers are time bound and follow the instructions already given to them by their organization or seniors. They do not try something new. They do not think beyond the given instructions. On the other hand, attackers are free to think, to experiment, and to create some new path to attack.

Summary

Summary

- What is SA
- What is PT
- Type of PT
- How PT is conducted
- Tool use in PT
- What is PT Limitation

END …….