TY Btech CSE (CSF) Semester VI (AY 2023-2024)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

CET4010B: Vulnerability Identification and Penetration Testing

Examination Scheme:

Continuous Assessment: 60 Marks End Semester Examination: 40 Credit: 3+1 =4

Course Objectives:

1. Knowledge: (i) Study the importance and benefits of Vulnerability Identification and Penetration Testing

(ii) Learn ethical guidelines and industry best practices for performing Penetration Testing assessments

2. Skills: (i) Demonstrate the knowledge to perform Vulnerability Identification and Penetration Testing

3. Attitude: (i) Identify breaches/ Vulnerability found in a network using Penetration Testing

Course Outcomes:

After completion of the course the students will be able to :-

1. Understand how to exploit a program and different types of software exploitation techniques
2. Understand the exploit development process
3. Search for vulnerabilities in closed-source applications
4. Analyze and apply different VAPT tools and generate report

Pre-requisites

- Network Security

Syllabus

Unit: I	**Penetration Testing-Principles and Practices** Importance and benefits of Penetration Testing assessments. Penetration testing-Principles and concepts, PT work flows and examples, blind tests, Function of malware and destructive viruses. Ethical hacking techniques, Ethical guidelines and industry best practices for performing Penetration Testing assessments.	**9 Hrs**
Unit: II	**Vulnerability Identification** Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads Using Nmap to sweep IP ranges for live hosts, Performance tuning Nmap scans. Discovering hosts using commonly known ports. Understanding security posture, cyber security issues. Gathering Information about target computer systems – Foot printing and Investigation. Scanning computers in the Networks. Network infrastructure vulnerabilities. Enumeration- Listing the systems/users and connecting them. Identifying Vulnerabilities associated with systems. Ethical hacking- penetrate into the security to locate vulnerabilities	**9 Hrs**
Unit: III	**Penetration Testing** Exploring Ethical Hacking, Malware Threats and their Counter measures. Monitoring and Capturing Data Packets using Sniffing. Restricting the System Access – DoS Attack, Gather Confidential Information – Social Engineering. Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Vulnerability assessment for natural disaster, technological hazards and terrorist threats; implications for emergency response, vulnerability of critical infrastructures.	**9 Hrs**

Syllabus (Continue)

Unit: IV	**VIPT Audit and Uses cases** Discovering patching vulnerabilities, Discovering web server vulnerabilities. Synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates. Perform Penetration Testing assessments, detect and respond to network breaches found in a Penetration Testing assessments. Preparation of a Penetration Test report. Auditing the Systems. Analysis and Reporting. Case Studies of recent vulnerabilities and attacks**.**	**9 Hrs**
Unit: V	**Attacks** Exploitation-exploiting default credentials, exploiting buffer overflow in third party software, Password attacks-online password attacks, offline password attacks, Client side exploitation- bypassing filters with metasploit payload, Client side attacks, bypassing antivirus applications, Social Engineering- spear phishing attacks	**9 Hrs**
Books:- (Text)	1. The Art of Network Penetration Testing by Royce Devis, copyright Manning Publications-2020. 2. Penetration Testing: A Hands-On Introduction to Hacking 1st Edition by Georgia Weidman, No-starch Press, ISBN-13: 978-1593275648.	
Books:- (Reference)	1. Advanced Infrastructure Penetration Testing by Chiheb Chebbi, Packt Publishing Bermingham – Mumbai, 2018. 2. The basic of Hacking and Penetration testing, second edition on ethical hacking and penetration by Patrick Engebretson. 3. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8. 4. Metasploit: The Penetration Tester&#39;s Guide, David Kennedy, Jim O&#39;Gorman, Devon Kearns, Mati Aharoni. 5. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm.	

Guidelines for CCA and LCA

Examination Scheme

Sr. No.	Examination Scheme	Marks
1. 2.	Class Continuous Assessment (CCA) Laboratory Continuous Assessment (LCA)	30 30
3.	End Term Theory Examination	40

CCA Marks Distribution

Examination	Marks
Mid-Term Theory Exam	15
Theory Assignment 1	5
Active Learning	10
	30

LCA Marks Distribution

Examination	Marks
Practical Performance	10
AL/MP	10
Endterm Exam	10
	30

Unit 1: Penetration Testing-Principles and Practices

Importance and benefits of Penetration Testing assessments. Penetration testing-Principles and concepts, PT work flows and examples, blind tests, Function of malware and destructive viruses. Ethical hacking techniques, Ethical guidelines and industry best practices for performing Penetration Testing assessments.

Vulnerability Identification and Penetration Testing

The vulnerability identification process enables you to identify and understand weaknesses in your system, underlying infrastructure, support systems, and major applications.

A vulnerability assessment is a systematic review of security weaknesses in an information system

A vulnerability assessment is the process of reviewing services and systems for potential security issues, whereas a penetration test actually performs exploitation and Proof of Concept (PoC) attacks to prove that a security issue exists.

Penetration tests go a step beyond vulnerability assessments by simulating hacker activity and delivering live payloads.

Penetration testing is also known as

- Pen testing
- PT
- Hacking
- Ethical hacking
- White hat hacking
- Offensive security
- Red teaming.

- Penetration testing can be defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure. The process includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real.
- It is a digital simulated cyber attack on a computer system or network that evaluates the security posture of the target systems or applications. The goal of a penetration test is to identify vulnerabilities that could be exploited by an attacker.
- Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test.

Q. Differentiate between an ethical hacker and a malicious hacker.

History

- Cybersecurity penetration testing traces back to the 1960s when the US Air Force conducted ‘tiger team’ security tests. Security experts would conduct tests using adversarial techniques to identify computer vulnerabilities and strengthen defenses.
- James P. Anderson was the first to develop the outline of what we now know as the penetration testing process. This model of testing became more popular during the 1980s and 1990s as computers increased in popularity.

Importance of Penetration Testing

Penetration tests are a crucial part of any security program as they help identify a wide range of vulnerabilities, including:

- Unpatched software
- Misconfigured security controls
- Weak passwords
- Social engineering vulnerabilities

Regular penetration testing is vital to comply with security regulations, enhance security posture, and minimize the risk of cyber attacks.

Benefits of Penetration Testing

Penetration testing is essential because it helps you highlight a target's hidden vulnerabilities and predict how low-risk liabilities can transform into larger threats. As the **need for robust security** grows, consistent and exhaustive penetration testing can offer your business many more benefits:

- **Reduce chances of future damage:** Retracting applications post-launch to address security issues wastes time, money, and **resources**, and it can negatively affect your reputation. When you successfully time the pen test of a product, you can worry less about fixing it after it's been released. Penetration tests also prepare you for potential problems, so you can address them quickly and with confidence should they occur in a real scenario.
- **Assess potential impacts:** Pen testing allows you to predict future challenges and judges how well your platform's security defenses perform against specific attacks. Understanding this information helps you adopt a proactive security approach, which in turn allows you to stay on top of your software's safety and performance.
- **Create with confidence:** As you perform pen tests, you can stay updated on whether or not your software meets regulatory requirements. Once you're sure that your platform is safe, you can focus on **innovation** and developing features or experiences that will entice **customers**. Any **Creator** who uses your platform will know that your organization takes security seriously, and they'll trust you to keep their sensitive data secure, giving your reputation a big boost.

Benefits of Penetration Testing

- **Identifying vulnerabilities:** helps identify security weaknesses in an organization’s systems, networks, and applications before attackers can exploit them.
- **Mitigating risk**: by identifying vulnerabilities, organizations can fix them in a structured way (e.g. low/medium/high risk) before they are exploited by attackers.
- **Meeting regulatory requirements**: many industry regulations and compliance standards require regular security reviews or penetration testing as part of their protocols.
- **Improving security posture:** helps improve security posture by providing an unbiased review and giving recommendations for improvement.
- **Providing assurance**: assures stakeholders, customers, and partners that an organization is taking cybersecurity seriously and is actively working to protect its systems and data.
- **Cost savings**: identifying and fixing vulnerabilities early is less expensive than dealing with the aftermath of a data breach or a successful cyber attack.
- **Increase business continuity:** pen tests help minimize the risk of a disruption that could impact operations**.**
- **Safeguards reputation:** reputations can take years to build and minutes to knock down. By reducing the likelihood of attacks, penetration testing helps safeguard your reputation. **Enhancement of the Management System** − It provides detailed information about the security threats.
- **Avoid Fines** − Penetration testing keeps your organization’s major activities updated and complies with the auditing system. So, penetration testing protects you from giving fines.

When does a company really need a penetration test?

If a company is wondering whether it should do a penetration test, I advise answering the following questions honestly. Start with simple yes/no answers. Then, for every yes answer, the company should see if it can back up that answer with, “Yes, *because* of internal process/procedure/application XYZ, which is maintained by employee ABC”:

- Is there an up-to-date record of every IP address and DNS name on the network?
- Is there a routine patching program for all operating systems and third-party applications running on the network?
- Do we use a commercial vulnerability scan engine/vendor to perform routine scans of the network?
- Have we removed local administrator privileges on employee laptops?
- Do we require and enforce strong passwords on all accounts on all systems?
- Are we utilizing multi-factor authentication everywhere?

If your company can’t answer a solid yes to all of these questions, then a decent penetration tester would probably have little to no trouble breaking in and finding your organization’s crown jewels.

Challenges and limitations of penetration testing

While penetration testing can provide significant benefits, there are also some challenges and limitations to be aware of:

- **False sense of security**: penetration testing provides a point-in-time snapshot of an organization’s security posture but can’t account for vulnerabilities discovered after the test or over-reliance on it.
- **Limited scope:** penetration testing is designed for specific areas and may not identify all vulnerabilities.
- **Impact on system performance**: can be resource-intensive and negatively impact system performance during the testing period.
- **Complexity**: security penetration testing requires expertise and resources, posing challenges for smaller organizations.
- **Cost:** professional penetration testing can be expensive, especially for larger organizations or those with complex computing environments.
- **Limited human factor testing**: network penetration tests do not account for human errors or behavior, such as phishing attacks or social engineering.
- **Ethical considerations:** responsible and ethical conduct is crucial in simulating cyber attacks during penetration testing.

Penetration testing phases

Typical penetration testing steps are as follows:

- **Planning and reconnaissance**: define scope, identify targets, gather information.
- **Scanning:** use tools to scan for vulnerabilities and weaknesses.
- **Gaining access:** exploit vulnerabilities to gain system access.
- **Maintaining access:** establish backdoors, install malware, maintain access.
- **Analysis:** evaluate data, assess testing effectiveness, identify improvements.
- **Reporting and remediation:** provide detailed results, vulnerability analysis, and recommendations for improvement.

What happens after a pen test?

After conducting a vulnerability assessment and penetration testing exercise, organizations will:

- **Review and analyze the results:** Review and analyze the results to understand the vulnerabilities and risks identified.
- **Prioritize remediation efforts:** Prioritize the remediation efforts needed based on test results and address the most critical vulnerabilities.
- **Plan and implement fixes:** Develop a plan to address identified vulnerabilities and implement the necessary fixes or patches.
- **Retest:** Conduct a retest to verify that the identified vulnerabilities have been successfully addressed.
- **Report findings:** Report findings to relevant stakeholders, including executives, IT teams, and other appropriate personnel.
- **Improve security posture:** Take additional steps to improve its security posture and remain proactive.

Penetration testing tools

- **Metasploit:** widely used open-source framework for developing and executing exploit code against target systems.
- **Nmap**: network mapping and port scanning tool used to identify hosts and services on a network.
- **Burp Suite**: web application testing tool used to identify vulnerabilities in web applications.
- **John the Ripper:** password cracking tool used to test the strength of passwords.
- **Wireshark:** network protocol analysis tool used to capture and analyze network traffic.
- **Nessus:** vulnerability scanning tool used to scan for known vulnerabilities in systems and applications.
- **Acunetix**: web vulnerability scanner used to identify vulnerabilities in web applications.
- **Aircrack-ng:** wireless network auditing tool used to test the security of wireless networks.
- **Hydra**: password cracking tool used to test the security of password-protected systems.
- **Sqlmap**: open-source tool for detecting and exploiting SQL injection vulnerabilities in web applications.

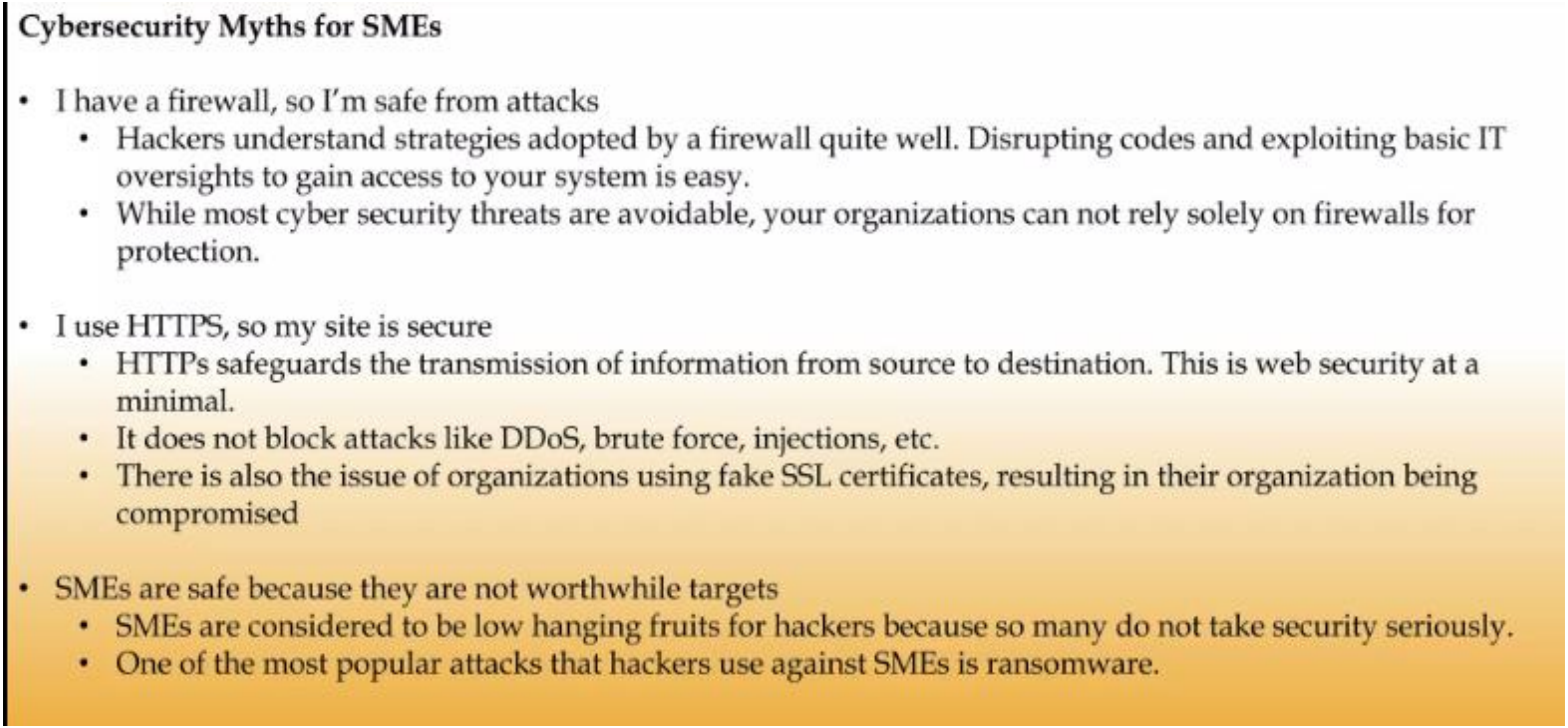
Penetration Testing Principles

- Uses a targeted approach to attempt to break through IT security and defences.
- Tries to simulate a real-life attack by hackers and other bad actors.
- Attempts to gain access to critical systems and sensitive information.
- Adapts according to resistance and tries to find new attack vectors.
- Is not as concerned with previously-identified, specific vulnerabilities
- Can use a variety of software, hacks, scripts, and other methods to penetrate defences

Penetration Testing Checklist

These are the typical items to be in place before the testing

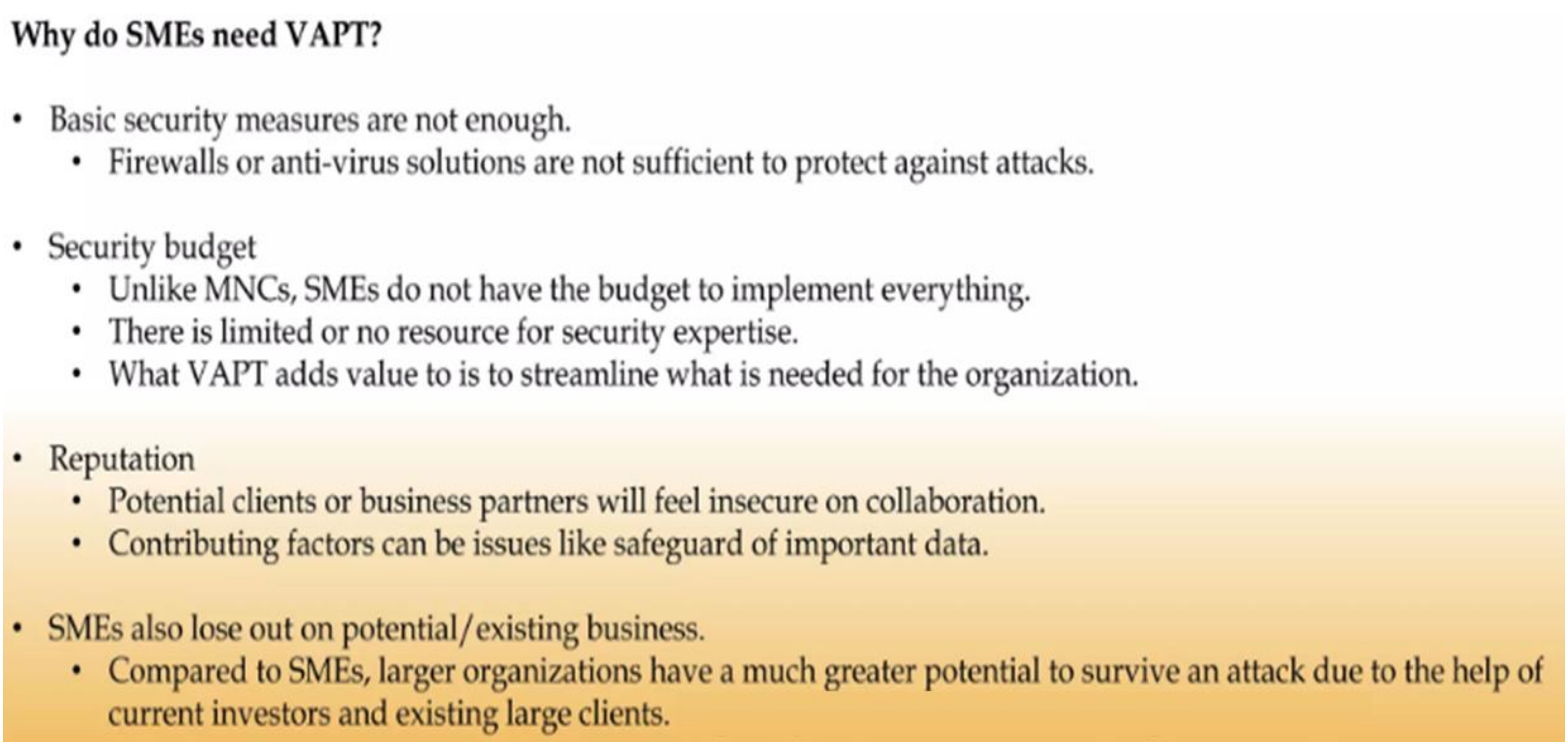
- ✓ A formally documented and approved scope
- ✓ A signed contract with legal elements and NDA
- ✓ Adequate and complete insurance coverage
- ✓ Ensure reporting channles are agreed along with reporting times
- ✓ Is access to the building arranged, user credentials established?
- ✓ Is IT Support in place and available when testing commences?
- ✓ A process for following up on penetration test findings
- ✓ An agreement on how findings will be rated and ranked
- ✓ Agreement on the process and timeframes for follow up testing



Cybersecurity Myths for SMEs

- I have a firewall, so I'm safe from attacks
  - Hackers understand strategies adopted by a firewall quite well. Disrupting codes and exploiting basic IT oversights to gain access to your system is easy.
  - While most cyber security threats are avoidable, your organizations can not rely solely on firewalls for protection.
- I use HTTPS, so my site is secure
  - HTTPs safeguards the transmission of information from source to destination. This is web security at a minimal.
  - It does not block attacks like DDoS, brute force, injections, etc.
  - There is also the issue of organizations using fake SSL certificates, resulting in their organization being compromised
- SMEs are safe because they are not worthwhile targets
  - SMEs are considered to be low hanging fruits for hackers because so many do not take security seriously.
  - One of the most popular attacks that hackers use against SMEs is ransomware.

Q. Exploitable and Non-Exploitable Vulnerabilities



Why do SMEs need VAPT?

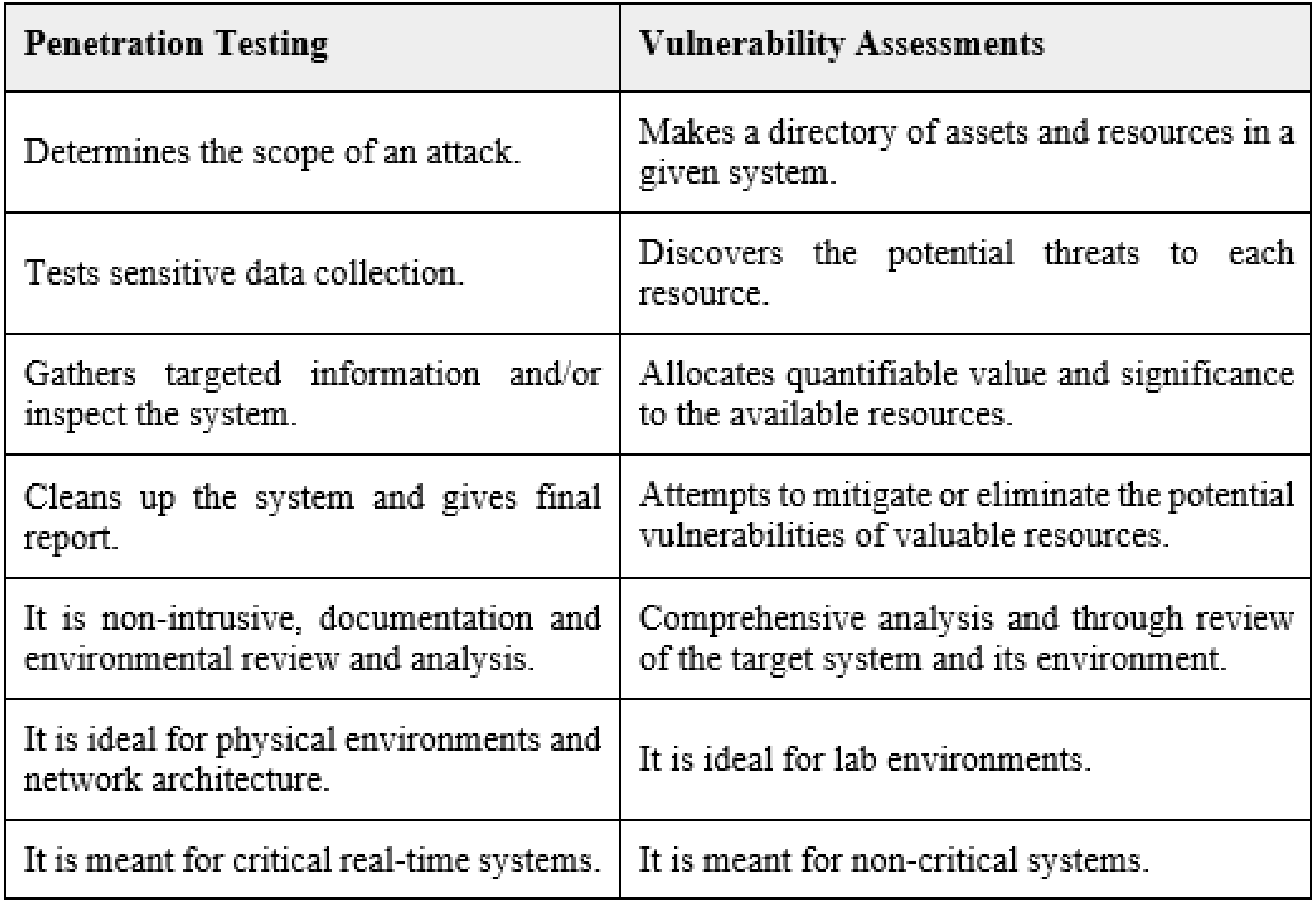
- Basic security measures are not enough.
  - Firewalls or anti-virus solutions are not sufficient to protect against attacks.

- Security budget
  - Unlike MNCs, SMEs do not have the budget to implement everything.
  - There is limited or no resource for security expertise.
  - What VAPT adds value to is to streamline what is needed for the organization.

- Reputation
  - Potential clients or business partners will feel insecure on collaboration.
  - Contributing factors can be issues like safeguard of important data.

- SMEs also lose out on potential/existing business.
  - Compared to SMEs, larger organizations have a much greater potential to survive an attack due to the help of current investors and existing large clients.

Differences between penetration testing and vulnerability assessments



Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

Which Option is Ideal to Practice?

- Both the methods have different functionality and approach, so it depends upon the security position of the respective system. However, because of the basic difference between penetration testing and vulnerability assessment, the second technique is more beneficial over the first one.
- Vulnerability assessment identifies the weaknesses and gives solution to fix them. On the other hand, penetration testing only answers the question that "can anyone break-in the system security and if so, then what harm he can do?"
- Further, a vulnerability assessment attempts to improve security system and develops a more mature, integrated security program. On the other hand, a penetration testing only gives a picture of your security program’s effectiveness.
- As we have seen here, the vulnerability assessment is more beneficial and gives better result in comparison to penetration testing. But, experts suggest that, as a part of security management system, both techniques should be performed routinely to ensure a perfect secured environment.

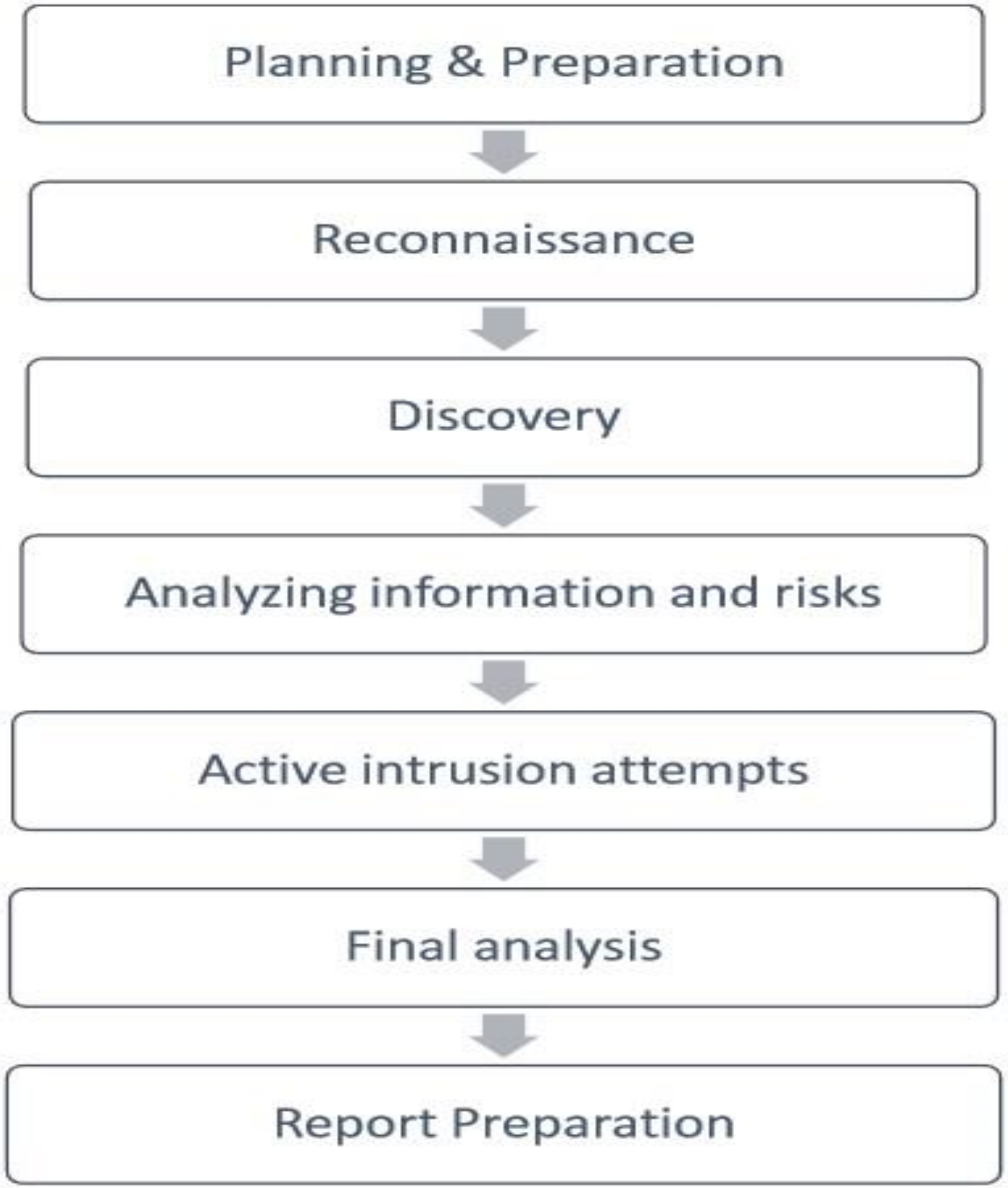
Following are the major limitations of Penetration Testing

- **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.

Penetration Testing Concepts

- Penetration testing, normally consists of information gathering, vulnerability and risk analysis, vulnerability exploits, and final report preparation.
- It is also essential to learn the features of various tools which are available with penetration testing.

Penetration Testing – Method (work flows)



Planning & Preparation

Reconnaissance

Discovery

Analyzing information and risks

Active intrusion attempts

Final analysis

Report Preparation

Penetration Testing - Method

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.

Penetration Testing - Method

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 analysing 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.

Penetration Testing - Method

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.

Penetration Testing - Method

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 owns 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.

- **Final Analysis**

  This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks. Further, the tester recommends to eliminate the vulnerabilities and risks. Above all, the tester must assure the transparency of the tests and the vulnerabilities that it disclosed.

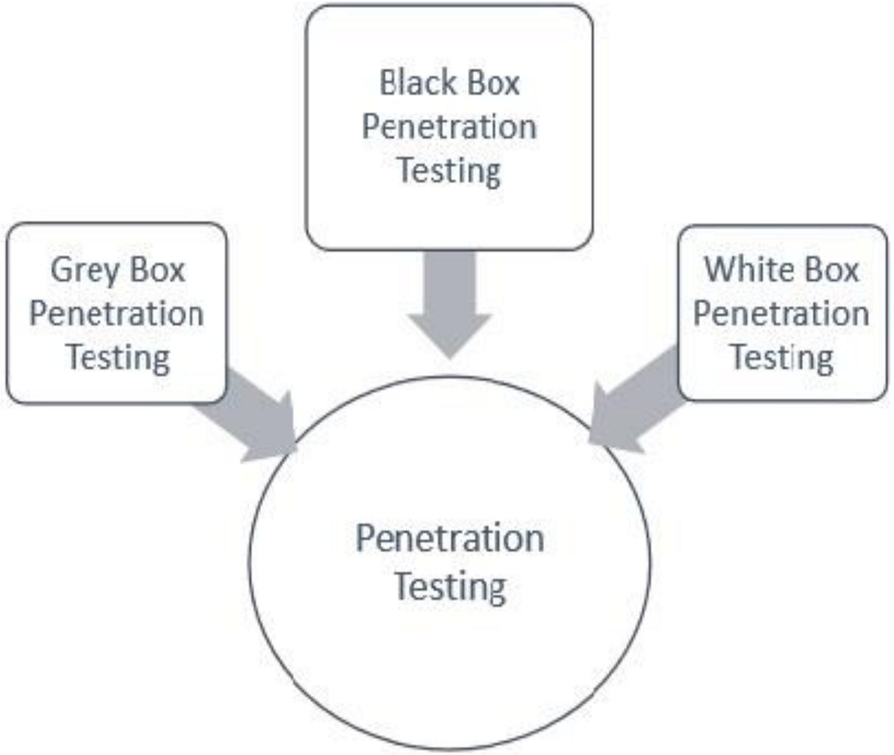
•A vulnerability is **a flaw or weakness** in an asset’s design, implementation, or operation and management that could be exploited by a threat.
•A threat is a **potential** for a threat agent **to exploit a vulnerability**.
•A risk is the **potential for loss** when the threat happens.

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.

Types of Pen Testing

- Following are the important types of pen testing –
  - Black Box Penetration Testing
  - White Box Penetration Testing
  - Grey Box Penetration Testing


Black Box Penetration Testing
Grey Box Penetration Testing
White Box Penetration Testing
Penetration Testing

Black Box Penetration Testing

- In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.
- Advantages of Black Box Penetration Testing
  - Tester need not necessarily be an expert, as it does not demand specific language knowledge
  - Tester verifies contradictions in the actual system and the specifications
  - Test is generally conducted with the perspective of a user, not the designer

White Box Penetration Testing

- This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.
- White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.
- Advantages of White Box Penetration Testing
  - It ensures that all independent paths of a module have been exercised.
  - It ensures that all logical decisions have been verified along with their true and false value.
  - It discovers the typographical errors and does syntax checking.
  - It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

Grey Box Penetration Testing

- In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.
- Advantages of Grey Box Penetration Testing
  - As the tester does not require the access of source code, it is non-intrusive and unbiased
  - As there is clear difference between a developer and a tester, so there is least risk of personal conflict
  - You don’t need to provide the internal information about the program functions and other operations

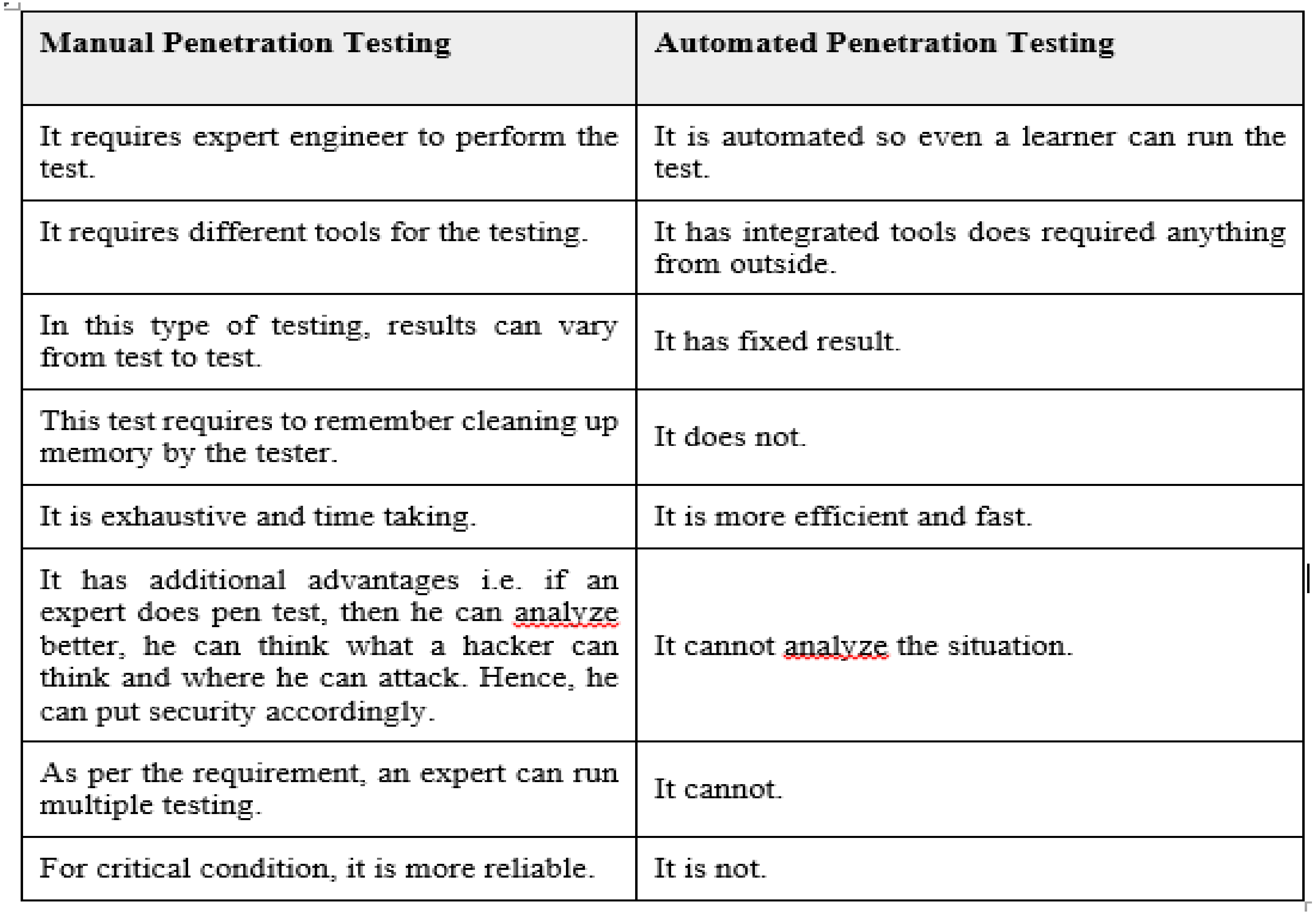
Penetration testing is normally done in the following three areas

- **Network Penetration Testing** − In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identities security flaws in design, implementation, or operation of the respective company/organization’s network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc

- **Application Penetration Testing** − In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application’s security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometime, it needs focused testing especially when traffic is allowed to pass through the firewall.

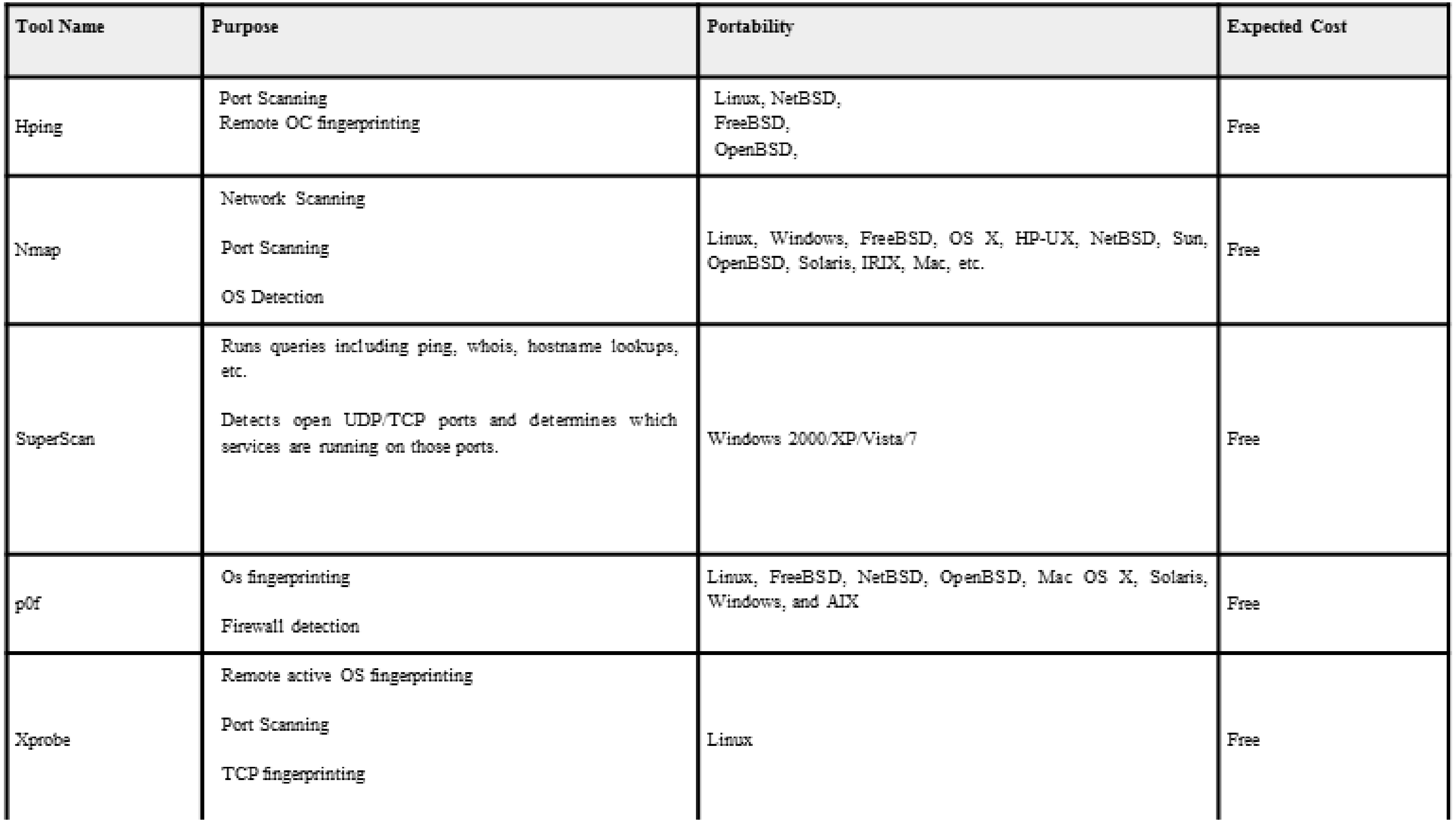
- **The response or workflow of the system** − This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

Difference between the manual and automated penetration testing



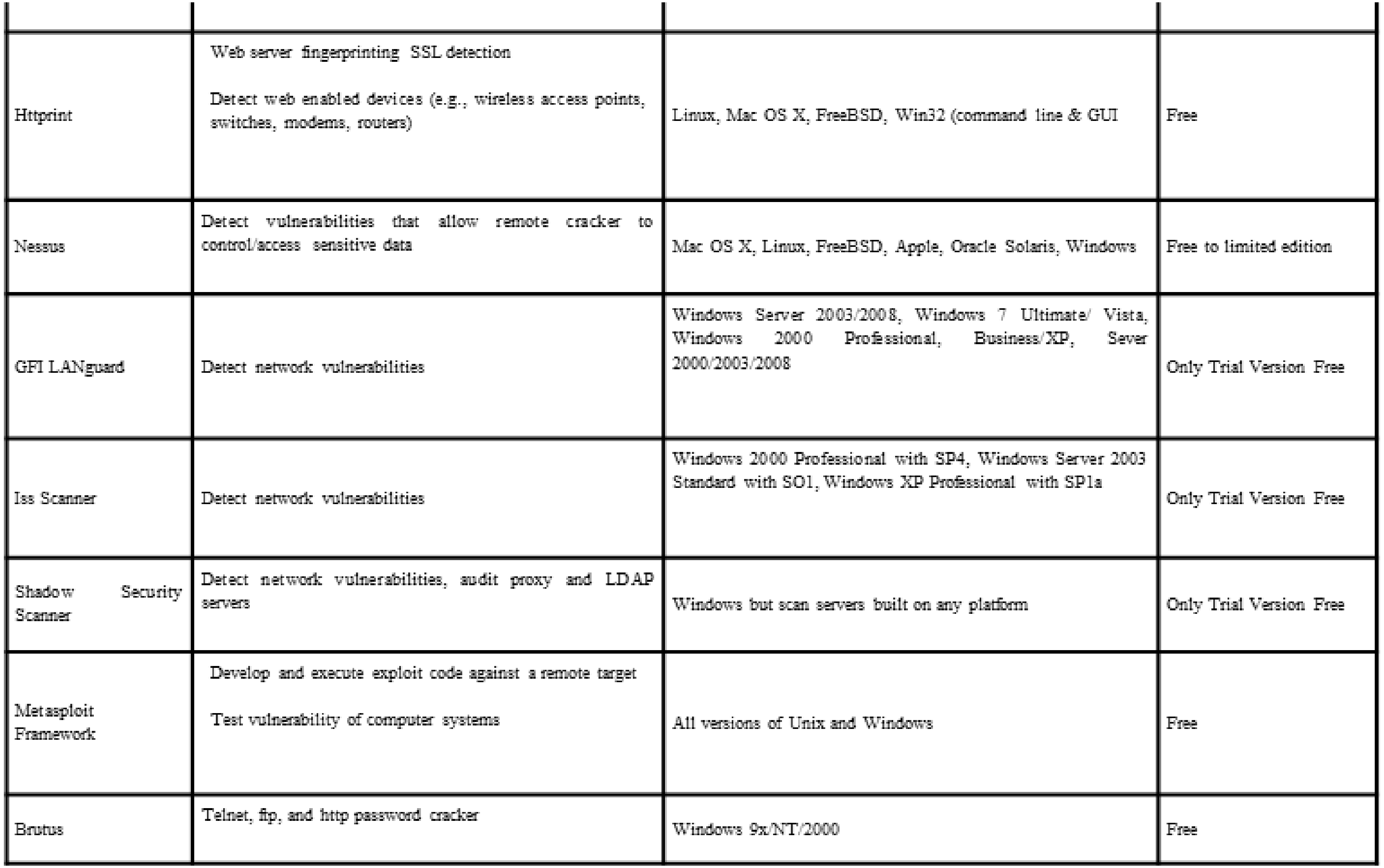
Manual Penetration Testing	Automated Penetration Testing
It requires expert engineer to perform the test.	It is automated so even a learner can run the test.
It requires different tools for the testing.	It has integrated tools does required anything from outside.
In this type of testing, results can 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.

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

Penetration Testing Tools



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

Blind tests

- Internal testing

  Internal penetration testing mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of penetration testing is useful for estimating how much damage an annoyed employee could cause.

- External Testing

  External penetration testing targets an organization's externally-visible servers or devices including domain name servers (DNS), email servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

- Blind Testing

  A blind penetration testing strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the organization.

- Double Blind Testing

  Double blind penetration testing takes the blind test and carries it a step further. In this type of penetration test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

Function of malware and destructive viruses

- **Malware**

  "Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand-alone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan.

- **Virus**

  Virus is a program written to enter to your computer and damage/alter your files/data. A virus might corrupt or delete data on your computer. Viruses can also replicate themselves. A computer Virus is more dangerous than a computer worm as it makes changes or deletes your files while worms only replicates itself with out making changes to your files/data.

  The purpose of malware is to intrude on a machine for a variety of reasons. From theft of financial details, to sensitive corporate or personal information, malware is best avoided, for even if it has no malicious purpose at present, it could well have so at some point in the future.

  Malware is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed. A virus is a specific type of malware that self-replicates by inserting its code into other programs.

Ethical hacking

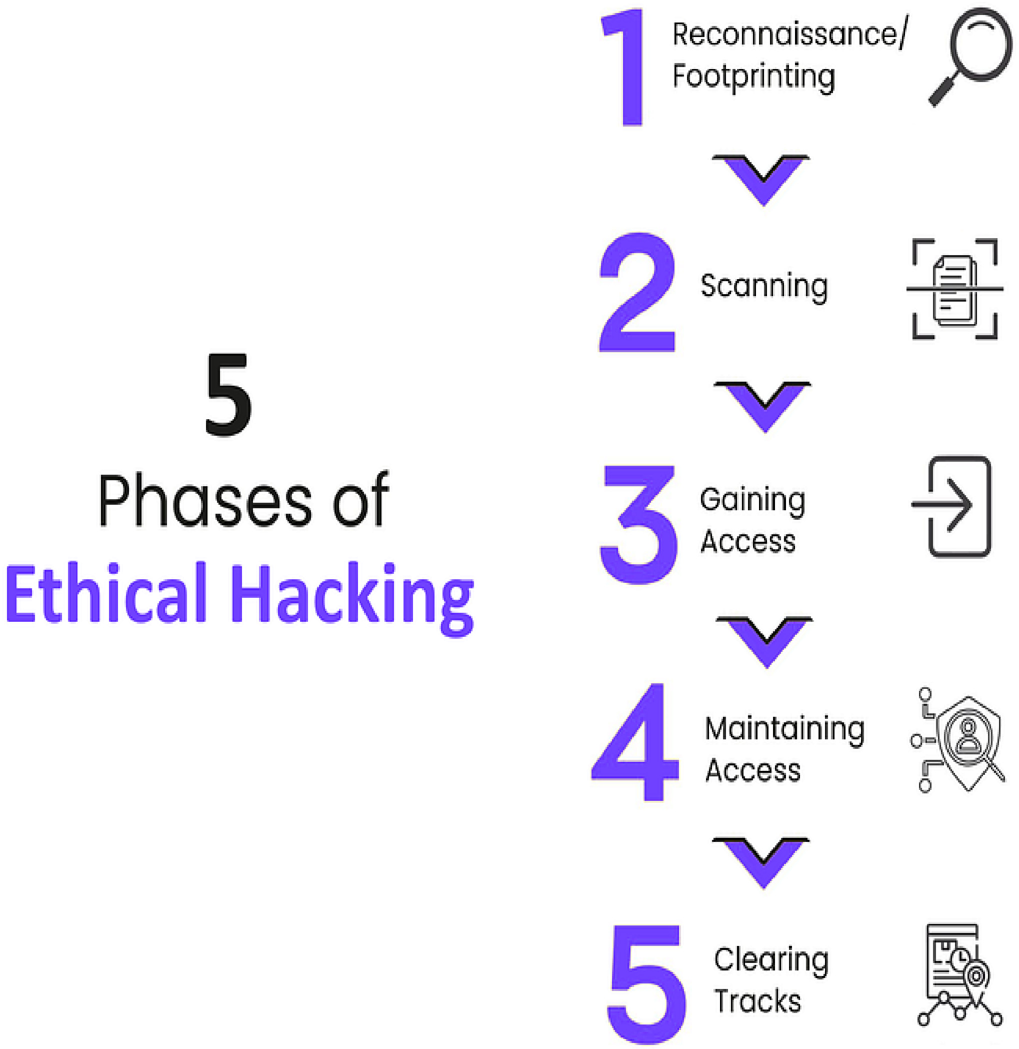
- What is ethical hacking?

  Ethical hackers are the computer experts who are legally allowed to hack a computer system with the objective to protect from the criminal hackers. An ethical hacker identifies the vulnerabilities and risks of a system and suggests how to eliminate them.

  Ethical hacking involves a collection of processes where organizations authorize individuals to exploit a system’s vulnerabilities for a deeper understanding of their existing security posture. When performing an ethical hack, a security professional or researcher replicates the actions and strategies of a malicious hacker. This helps development and security teams to detect and identify security risks before hackers can exploit them.

Ethical Hacking: 5 Phases

Ethical hacking involves simulating attacks to evaluate and assess the security of a system or network. The primary goal is to discover any vulnerabilities or weaknesses and offer suggestions for enhancing security. Ethical hacking plays a crucial role in contemporary cybersecurity by enabling organizations to detect and mitigate security risks proactively, preventing potential exploits by malicious actors.



5 Phases of Ethical Hacking

1 Reconnaissance/ Footprinting

2 Scanning

3 Gaining Access

4 Maintaining Access

5 Clearing Tracks

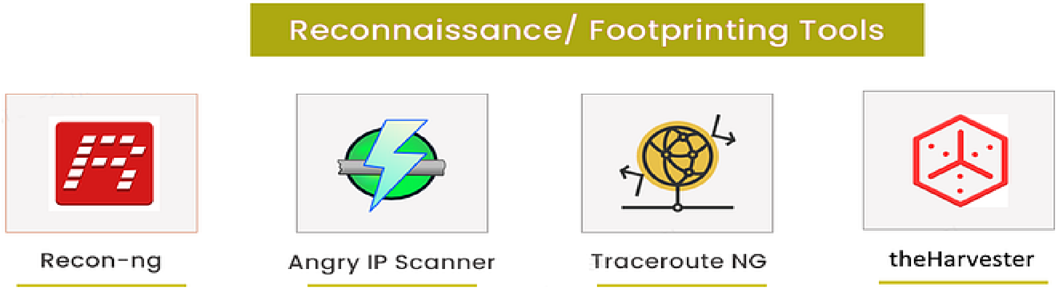
Phase 1: Reconnaissance/Footprinting/ Data Gathering

- In this phase, security professionals meticulously acquire information and intelligence pertaining to a target system, network, or entity. This process involves the methodical collection of publicly accessible data, facilitating an in-depth comprehension of the target’s technological infrastructure, system architecture, and potential security vulnerabilities.

Methods Employed in Phase 1:

- **Passive Information Gathering:** This involves collecting data about the target without directly interacting with it. It includes activities such as searching for publicly available information on websites, social media, forums, and search engines.
- **Active Information Gathering:** Security professionals actively interact with the target to gather information. This can include techniques like port scanning to identify open ports, network mapping to understand the network's topology, and banner grabbing to retrieve information about services running on the target.
- **OSINT (Open Source Intelligence):** Leveraging publicly available sources of information, such as public records, domain registration details, and social media profiles, to build a comprehensive profile of the target.
- **WHOIS Lookups:** Querying WHOIS databases to obtain information about domain ownership and registration details.

Software applications utilized in Phase 1



- **Recon-ng:** Recon-ng is a reconnaissance framework that assists in collecting information from various sources, including online databases and APIs.
- **Angry IP Scanner**: Angry IP Scanner is an open-source network scanning tool used to identify live hosts and open ports on a network. It offers customizable scans and is widely utilized by network administrators and security professionals for network reconnaissance and troubleshooting.
- **Traceroute NG**: Traceroute NG, short for “traceroute-next generation,” is an advanced version of the traditional traceroute tool used in network troubleshooting. It offers enhancements like support for IPv6, extended information about network hops, multiple queries, and geographical data, providing more comprehensive insights into network routing and performance issues.
- **theHarvester:** This tool automates the process of collecting email addresses, subdomains, and virtual hosts from public sources.

Phase 2: Scanning

- Scanning typically involves the systematic exploration of a target network or system to identify open ports, services, and potential vulnerabilities. This phase is crucial in the ethical hacking process as it provides valuable information for subsequent penetration testing or security assessment activities.

Approaches applied in Phase 2

- **Port Scanning**: Port scanning is a fundamental technique that involves probing a target system to identify open ports and the services running on them. This information helps ethical hackers understand the attack surface and potential entry points into the target.
- **Vulnerability Scanning:** Vulnerability scanning tools, such as Nessus or OpenVAS, are used to systematically scan the target for known vulnerabilities in software and services. This technique aids in identifying weaknesses that could be exploited by attackers.
- **Banner Grabbing:** Banner grabbing is the practice of extracting information from service banners or headers, revealing details about the versions and configurations of services running on open ports. This information assists ethical hackers in identifying potential vulnerabilities and misconfigurations.

Software applications utilized in Phase 2

- **Metasploit:** Metasploit is a penetration testing framework that includes various modules for scanning, exploiting, and post-exploitation activities. It’s used to identify and exploit vulnerabilities.
- **Nmap (Network Mapper)**: Nmap is a versatile and widely-used open-source tool for network discovery and security auditing. It excels in port scanning, service detection, and OS fingerprinting.
- **Nessus**: Nessus is a powerful vulnerability scanning tool that helps identify known vulnerabilities in target systems and provides detailed reports on potential security issues.
- **Nikto:** Nikto is an open-source web server and web application scanner that aids cybersecurity professionals in identifying vulnerabilities and security issues. It assesses web servers, checks for known vulnerabilities, inspects web applications for common security flaws, and generates detailed reports to assist in securing online assets.

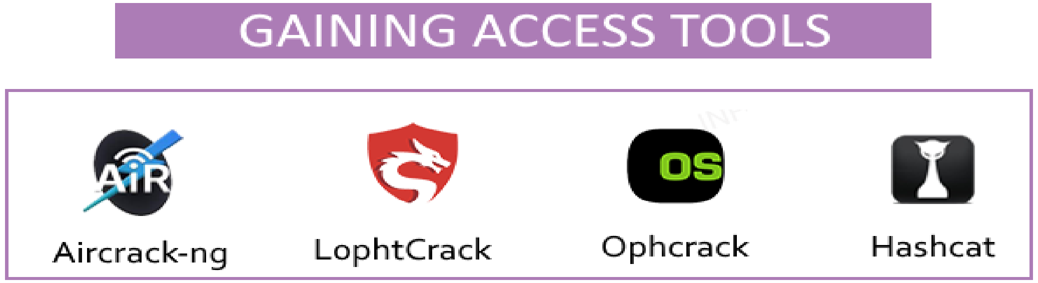
Phase 3: Gaining Access

‘Gaining Access,’ ethical hackers engage in a systematic process of exploiting previously identified vulnerabilities. This phase involves executing precise technical actions to gain entry into the target system or network. The goal is to assess the security posture comprehensively by simulating potential attacker techniques. The insights gained guide organizations in strengthening their defenses against real-world cyber threats.

Methods employed in Phase 3

- **Exploiting Software Vulnerabilities**: Ethical hackers may attempt to exploit known software vulnerabilities in operating systems, applications, or services running on the target system. This can involve techniques like buffer overflows, SQL injection, or remote code execution.
- **Brute Force Attacks:** Brute force attacks involve systematically trying all possible combinations of usernames and passwords to gain unauthorized access to user accounts or systems.
- **Credential Theft:** Ethical hackers may attempt to steal credentials through techniques such as phishing, keylogging, or password cracking. Once obtained, these credentials can be used to access the target system.
- **Pharming and DNS Spoofing:** These techniques involve redirecting network traffic to malicious servers, tricking users or systems into connecting to unauthorized resources.

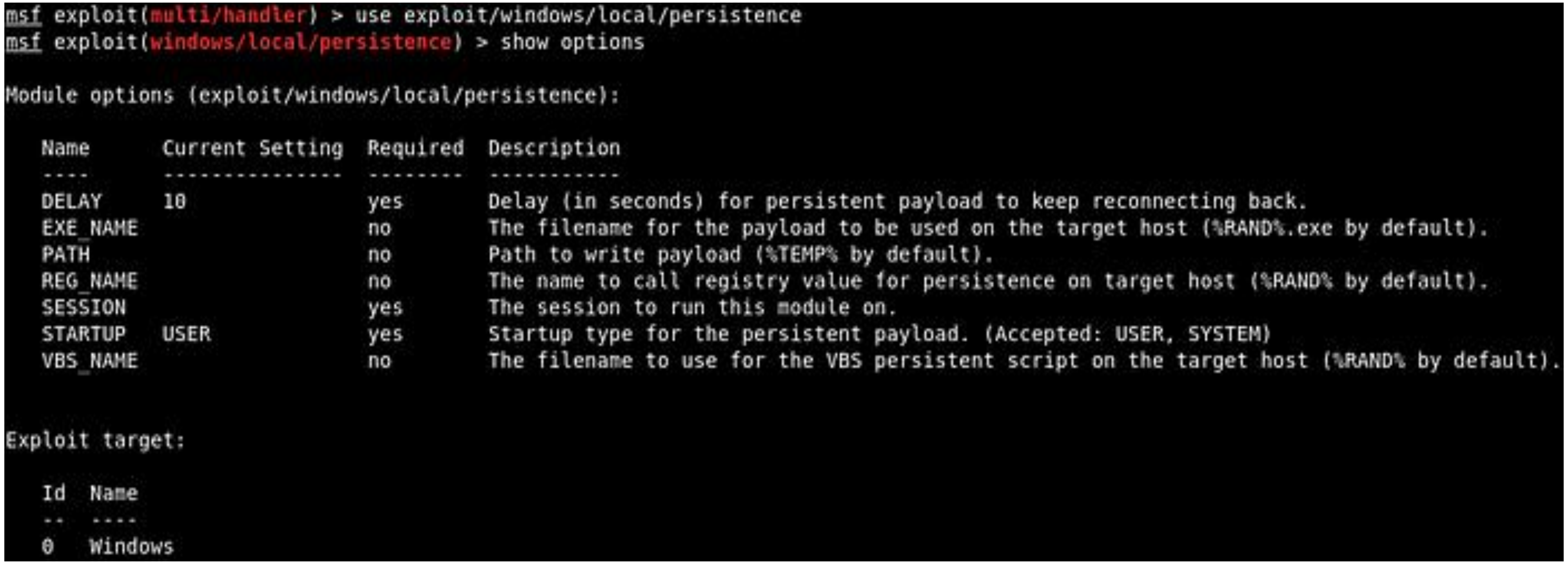
Software applications utilized in Phase 3



- **Aircrack-ng**: Aircrack-ng is a widely-used suite of tools for assessing the security of Wi-Fi networks. It enables security professionals to capture and analyze network traffic, crack encryption keys, and perform various tests to identify vulnerabilities and enhance the security of wireless networks.
- **L0phtCrack**: L0phtCrack, or LC5, is a tool used to evaluate the security of Windows passwords. It aids in password recovery and auditing by testing password strength and helping users manage their passwords effectively.
- **Ophcrack:** Ophcrack is an open-source password recovery tool that utilizes rainbow tables and advanced algorithms to crack Windows login passwords. It’s frequently employed for technical password recovery and security auditing tasks on Windows operating systems.
- **Hashcat:** Hashcat is a versatile open-source tool known for efficiently cracking password hashes. Security professionals rely on it to assess password security and recover lost or forgotten passwords due to its broad support for cryptographic hash algorithms. Its flexibility and high-performance capabilities make it a valuable asset in cybersecurity assessments.

Phase 4: Maintaining Access

“Maintaining Access,” is a critical stage in ethical hacking where security professionals or penetration testers, having gained initial access to a target system, work to maintain their foothold and establish persistent access. This phase involves various tactics and techniques to ensure continued control over the compromised system or network, replicating real-world attacker persistence to assess the potential risks and impact on the target.



```
msf exploit(multi/handler) > use exploit/windows/local/persistence
msf exploit(windows/local/persistence) > show options

Module options (exploit/windows/local/persistence):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
   EXE_NAME                   no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   PATH                       no        Path to write payload (%TEMP% by default).
   REG_NAME                   no        The name to call registry value for persistence on target host (%RAND% by default).
   SESSION                    yes       The session to run this module on.
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
   VBS_NAME                   no        The filename to use for the VBS persistent script on the target host (%RAND% by default).


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

Strategies employed in Phase 4

- **Backdoors:** Backdoors are hidden entry points or software mechanisms that allow ethical hackers to regain access to a compromised system after initial access has been established. They provide a secret pathway to maintain control.
- **Privilege Escalation:** Privilege escalation involves elevating user privileges on the compromised system. Ethical hackers seek to gain higher-level access, such as administrative privileges, to control critical resources and systems.
- **Persistence Scripts:** These are scripts or scheduled tasks created by hackers to run at specific intervals on the compromised system. They ensure that unauthorized access remains intact over an extended period, even if the initial entry point is discovered.
- **Trojans (Remote Access Tools — RATs):** Trojans or RATs are malicious software programs used to create covert communication channels between the attacker and the compromised system. They enable remote control and data exfiltration.

Software applications utilized in Phase 4:

1. Poshc2: POSHC2, or "Posh Command and Control," is an open-source post-exploitation framework used in cybersecurity. It leverages PowerShell to maintain control over compromised Windows systems, enabling ethical hackers to perform advanced post-exploitation tasks, such as lateral movement and privilege escalation, during security assessments.

2. Rootkits: Rootkits are stealthy malicious software that masks their existence on compromised systems by altering core operating system components. They are commonly utilized by cybercriminals to maintain covert, unauthorized access and execute malicious activities. Detecting and removing rootkits demands specialized tools and expertise. Examples of well-known rootkits include:

- **TDSS/TDL Rootkit:** Also known as Alureon, this rootkit infects the Master Boot Record (MBR) and is notorious for its ability to hide from antivirus software.
- **Zeus:** Zeus, or Zbot, is a Trojan that often includes a rootkit component. It specializes in stealing sensitive information, such as banking credentials.
- **Rustock:** The Rustock rootkit was associated with one of the largest spam botnets in the world. It aimed to hide its malicious activity on infected systems.

3. PowerSploit: PowerSploit is an open-source framework primarily used in ethical hacking and penetration testing. It employs Microsoft PowerShell to perform various post-exploitation tasks like privilege escalation, data exfiltration, and maintaining access on compromised systems, aiding security professionals in assessing the security of Windows environments

Phase 5: Clearing Tracks

“Clearing Tracks,” is a crucial step in ethical hacking where security professionals, having completed their assessment, take measures to conceal any traces or evidence of their presence and activities on the target system or network. This phase ensures that the ethical hacking engagement remains covert and does not leave any lingering signs of intrusion, protecting the integrity and confidentiality of the assessment.

Approaches implemented in Phase 5

- **Log Deletion:** Ethical hackers remove or manipulate log files that may contain records of their activities, ensuring that their actions go unnoticed.
- **Registry Cleanup:** Entries related to the hacker’s activities in the Windows Registry are removed or altered to erase any signs of intrusion.
- **Anti-Forensic Techniques:** Techniques to hinder forensic analysis, such as anti-forensic tools or encryption, are employed to make it harder for investigators to reconstruct events.

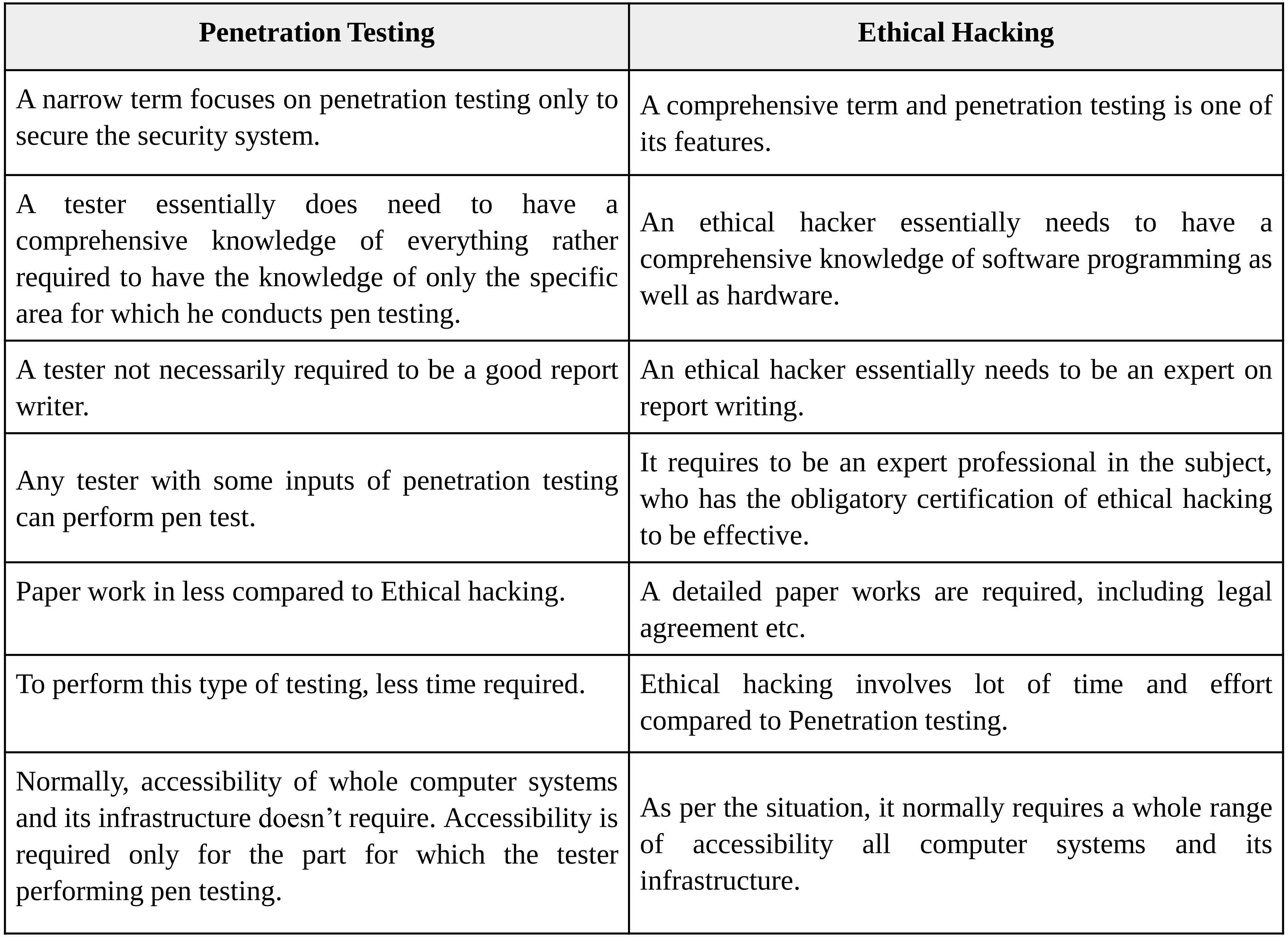
Techniques used in phase 5

- **LogCleaner:** Tools and scripts erase or manipulate log files on a system, removing evidence of the hacker's actions. For example, they can delete or modify Windows Event Logs like "Security," eliminating records of login attempts.
- **Network Traffic Cleaning Tools** (e.g., Scapy): Specialized tools like "Scapy" enable hackers to manipulate network traffic. For instance, Scapy can forge or modify packet headers to obscure communication origins, making it hard for investigators to trace during assessments.
- **Registry Cleaning Tools:** These Windows-specific applications are used to sanitize and modify the Windows Registry, eliminating or altering entries related to an ethical hacker's actions to prevent detection.
- **Anti-Forensic Suites:** Comprehensive toolkits with various utilities designed to erase digital traces, modify metadata, and obstruct forensic investigations, preserving the hacker's anonymity and activities.

EH four principle values

- Keeping the exploits legal by obtaining client approval before conducting the vulnerability assessment
- Predefining the scope of the attack so that the security assessments stay within the approved legal boundaries
- Reporting all discovered vulnerabilities and providing remediation recommendations to the organization administering the system
- Agreeing to the set terms and conditions regarding respect for data privacy and confidentiality

The aim of ethical hacking is to mimic the actions of hackers and identify both existing and potential vulnerabilities that may arise in the future. To accomplish this, an ethical hacker undertakes multiple stages of assessment to gain as much in-depth knowledge of the system as possible.



Penetration Testing	Ethical Hacking
A narrow term focuses on penetration testing only to secure the security system.	A comprehensive term and penetration testing is one of its features.
A tester essentially does need to have a comprehensive knowledge of everything rather required to have the knowledge of only the specific area for which he conducts pen testing.	An ethical hacker essentially needs to have a comprehensive knowledge of software programming as well as hardware.
A tester not necessarily required to be a good report writer.	An ethical hacker essentially needs to be an expert on report writing.
Any tester with some inputs of penetration testing can perform pen test.	It requires to be an expert professional in the subject, who has the obligatory certification of ethical hacking to be effective.
Paper work in less compared to Ethical hacking.	A detailed paper works are required, including legal agreement etc.
To perform this type of testing, less time required.	Ethical hacking involves lot of time and effort compared to Penetration testing.
Normally, accessibility of whole computer systems and its infrastructure doesn’t require. Accessibility is required only for the part for which the tester performing pen testing.	As per the situation, it normally requires a whole range of accessibility all computer systems and its infrastructure.

Q. Penetration Testing vs ethical hacking vs vulnerability assessment

Ethical Hacking Techniques

Ethical hacking has the potential to test, scan, and secure systems and data. Ethical hacking techniques can be learnt using an ethical hacking PDF and some of the techniques are listed below.

1. Phishing

Phishing is a cyber-security attack where a hacker sends messages pretending to be a trusted person. These types of messages manipulate a user causing them to perform actions like installing a malicious file and clicking a malicious link.

A phisher uses public resources to collect information about the personal and work experience of the victim. They then use this information to create a reliable fake message.

2. Sniffing

Sniffing is the process of keeping track and capturing all the packets passing through a given network. This is done using some sniffing tools. It is also known as wiretapping as it is in the form of tapping phone wires and can get to know about the conversation.

A sniffer turns the NIC of the system to promiscuous mode.

3. Social Engineering

Social engineering is used to convince people to reveal their confidential information. The attacker deceives the people by taking advantage of their trust and lack of knowledge. There are three types of social engineering - human-based, mobile-based, and computer-based.

Due to loose security policies and the absence of hardware or software tools to prevent it, it is difficult to detect a social engineering attack.

4. Footprinting

In this **ethical hacking** technique, the hacker gathers as much data as possible about a specific targeted system and infrastructure to recognize opportunities to penetrate them.

The hacker might use various tools and technologies to get information to crack a whole system.

5. SQL injection

SQL injection is an attack in which the attacker sends a SQL query, a statement, to a database server that modifies it as required. An SQL injection happens when the user input is improperly sanitized before using it in an SQL query.

SQL allows securing a response from the database. It will help the hacker understand the construction of the database, as the table names.

6. Enumeration

Enumeration also means information gathering. In this process, the attacker creates a connection with the victim to find as many attack vectors which are used to exploit the system in the future.

A hacker needs to establish an active connection with the target host. First, the vulnerabilities are counted and assessed. Then, it is done to search for attacks and threats to target the system. This is used to collect the username, hostnames, passwords, and IP addresses.

Ethical guidelines and industry best practices for performing Penetration Testing assessments.

- What are the ethical and legal considerations of penetration testing?

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.

Before allowing someone to test sensitive data, companies normally take measures regarding the availability, confidentiality, and integrity of data. For this agreement to be in place, legal compliance is a necessary activity for an organization.

The most important legal regulations which have to be observed when establishing and maintaining security and authorization systems are presented below in context for using in implementing penetration tests.

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
- 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 your respective country. Sign an agreement only after considering the respective laws.

Penetration testing best practices

- Pen testing basics. Software penetration testing is all about discovery. First, collect information from the available sources to enable penetration tests, then perform a range of tests to find flaws in target software.
- It's a best practice to document this work carefully, including the means pen testers use to obtain information, the actual steps and processes they use to test, and the observed results. This way, developers can reproduce flaws later to study and remediate them. Organizations typically conduct penetration testing over a defined time period.
- Ultimately, penetration testing requires a team's security professionals to think and act like real hackers, while behaving in a manner that supports business interests -- i.e., to be ethical hackers. Confidentiality is crucial.
- Penetration testing use cases. Penetration testing is valuable for all types of security evaluations, but a full-scale effort might not always be worth the work and expense. A simple software module with limited access to data storage, for instance, won't require a multi-team security assessment. Low- or no-code applications enterprises use for internal business tasks are also low priority.

- Some software development projects, however, require thorough penetration testing. A retail or financial services company should demand comprehensive, full-scale penetration testing for software involved with monetary transactions, customer data and financial holdings. Similarly, software in certain data- and security-sensitive sectors, including military and healthcare, typically receives detailed penetration testing to find and remediate flaws that might cost lives. Penetration testing can also validate software components external programmers develop.
- Finally, an organization can use penetration testing after a security breach. Forensic pen testing provides insight into the flaw that led to the exploit. Developers can then search for additional flaws in the code and its supporting infrastructure hackers have yet to exploit.
- Identifiable application security risks. Countless flaws can put an application at risk and threaten information security. Pen testers commonly find flaws in:
  - the OS
  - application code
  - configuration files

Penetration testing drawbacks

- While a valuable approach for the business and IT, penetration testing isn't perfect.
  - First, penetration testing guarantees nothing. The test approach only succeeds when a flaw is found and fixed. You can miss flaws, only to have them discovered later.
  - Second, penetration testing consumes considerable time and staff resources. Weigh the benefits against the project budget. Budget can restrict how much penetration testing a team performs on a build. Sensitive projects with significant penetration testing requirements can get pricey.
- Penetration testing can result in unexpected downtime and data loss or corruption -- side effects of exploited flaws in software. Mitigate these problems through A/B testing, in which an older build continues to run while the new build undergoes software testing and validation. Data protection methods, such as backups and snapshots, also help guard against unexpected data loss.