Syllabus

Elements of Information Security, Authenticity and Non-Repudiation, Security Challenges, Effects of Hacking, Hacker – Types of Hacker, Ethical Hacker ,Role of Security and Penetration Tester, Penetration Testing Methodologies :– OSSTMM, NIST, OWASP, Categories of Penetration Test, Types of Penetration Tests, Vulnerability Assessment.

Elements of Information Security

- Elements of an Information Security and its critical elements, including systems and hardware that use, store, and transmit that information.
- Information security system is the process of protecting and securing the data from unauthorized access, disclosure, destruction or disruption.
- Information security is the application of measures to ensure the safety and privacy of data by managing its storage and distribution.
- Information security is defined as "a state of well information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable".
- It relies on five major elements: ***confidentiality, integrity, availability, authenticity, and non-repudiation.***
- **Confidentiality:**
  - Data and information assets should be confine to individuals license to access and not be disclose to others; Confidentiality assurances that the information is accessible those who are authorize to have access.
  - Confidentiality breaches may occur due to improper data handling or a hacking attempt. It controls include data classification, data encryption, and proper equipment disposal (i.e., of DVDs, CDs, etc.), Confidentiality is roughly adoring privacy.
  - Measures undertaken to confirm confidentiality are design to prevent sensitive data from reaching the incorrect people. Whereas ensuring the correct people will really get it: Access should be restricted those licensed look at information in question.
  - It's common for information to be categorize consistent with quantity and kind of injury might be done. It makes up unintended hands.
  - A lot of or less rigorous measures will then be implemented according to those classes.

- ***Integrity:***
  - Keeping the information intact, complete and correct, and IT systems operational; Integrity is the trustworthiness of data or resources in the prevention of improper and unauthoriz changes the assurance that information is sufficiently accurate for its purpose.
  - Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only the authorized people can update, add, and delete data to protect its integrity).
  - Integrity involves maintaining the consistency, accuracy, and trustworthiness of information over its entire life cycle.
- ***Availability***
  - An objective indicating that data or system is at disposal of license users once require.
  - Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users.
  - Availability means data is accessible by licensed users.
  - If an attacker isn't able to compromise the primary components of data security (see above) they'll try and execute attacks like denial of service that will bring down the server, creating the web site unavailable to legitimate users because of lack of availability.
  - Measures to maintain data availability can include redundant systems' disk arrays and clustered Machines, anti-virus software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.
- ***Authenticity***
  - A security policy includes a hierarchical pattern. It means inferior workers is typically certain to not share the small quantity of data they need unless explicitly approved.
  - Conversely, a senior manager might have enough authority to create a choice what information is shared and with whom, which implies that they're not tied down by an equivalent data security policy term. That the logic demands that ISP ought to address each basic position within the organization with specifications which will clarify their authoritative standing.

- Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or corrupted.
- The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as bio metrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.
- The user should prove access rights and identity. Commonly, usernames and passwords are used for this method. However, this kind of authentication may be circumvented by hackers.
- A much better form of authentication is bio metrics, as a result of it depends on the user's presence and biological features (retina or fingerprints).
- The PKI (Public Key Infrastructure) authentication methodology uses digital certificates to prove a user's identity. Different authentication tools will be key cards or USB tokens.
- The best authentication threat occurs with unsecured emails that seem legitimate.

 Non-Repudiation

- It is the assurance that somebody cannot deny the validity of one thing. It may be a legal thought that's widely used in data security and refers to a service that provides proof of the origin of information and also the integrity of the information.
- In different words, non-repudiation makes it very difficult to successfully deny who/where a message came from also as the authenticity of that message.
- Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

Security challenges

 Capability Challenges: Many challenges are related to the lack of experience and skills gained over time. In fact, there's a threshold difference between different ethical hacking teams. Moreover, there's no standardised threshold that unifies the skills and experience of ethical hackers into a single capability and capacity. Therefore, some ethical hacking teams may have more skills, experience, and knowledge, compared to other groups when

performing their pen testing, along with the availability of a much more sophisticated tools and kits.

- ***Capacity Challenges:*** Another challenge is performing the necessary pen testing in order to evaluate the level of security and immunity of a given organisation against cyber-attacks, especially in terms of risk management. The capacity is based on the limited experienced manpower, and the available resources, used to perform the pen testing technique(s) and attack(s). Therefore, this is another challenge that requires a deeper focus and attention.
- ***Cost Challenges***: The cost of performing a pen testing attack is not cheap. However, it is necessary to avoid any exploitation of any vulnerability or security gap. In fact, pen testing is divided into two main steps.
  - ✔ The first one requires the identification of already existing exploitable vulnerabilities which requires a defined cost.
  - ✔ The next step is based on the ability to offer security measures to further protect the system, which also requires an additional cost.
- ***Legal Challenges***: Many legal challenges also surround the ethical hackers, along with the ethical hacking as well. In other terms, ethical hackers do not perform their pen testing without signing a legal document called the Non-Disclosure Agreement (NDA). This also requires notifying the required authorities so their testing is not classified as a cyber-crime. Therefore, without the signing of legal processes, ethical hackers' risk being legally prosecuted and arrested.
- ***Heterogeneous Challenges***: Such heterogeneous challenges are based on different ethical hacking groups performing different pen testing attacks and types from their perspectives and skills. Though it is important and necessary, an exploitable vulnerability identified by one ethical hacking team, may not be identified by another ethical hacking team, and vice versa. Therefore, the choice of the right ethical hacking team to perform the right and necessary pen testing is somewhat of hard task and challenge.
- ***Knowledge Challenges***: Knowledge challenges are based on the ability of ethical hackers to perform their pen testing against exploitable vulnerabilities and security gaps. This includes software bug, misconfiguration or other bugs (i.e hardware, configuration, or coding). However, their pen testing and knowledge are based on the ability to identify and

overcome the only already existing attacks. In other terms, pen testing is unable to detect new attacks such a zero-day attacks. This is due to these attacks being based on exploiting a vulnerability that was not detected by ethical hackers who were conducting their pen testing. This also includes the birthday attack in a way, which is quite similar to zero-day. This is done, in addition to the presence polymorphic malware and crypting services that keep on changing their signature and behaviour patterns. Thus, their identification and mitigation process are becoming seriously challenging. This is all due to their ability to avoid and evade being detected by intrusion detection systems, firewalls and anti-viruses.

Effects of hacking

- Communication has significantly changed over the years. Historically, the only way to communicate was to write a letter. Then, technology started to advance with the invention of the telephone in 1876. (Hochfelder, 2018, para.1).
- Technology continued to rise with the computer being invented around 1936 ("First programmable computer", 2018, para. 4) which then brought us emailing in the 1970's. (Peter, 2004, para. 6).
- With this rise of computer technology and finding faster ways for people to communicate, remain connected, share photos online and exchange thoughts or ideas.
- Social media has more recently become a forum whereby like-minded people are able to meet each other and if they so desire, begin meaningful relationships. This form of modern communication has several effects on family relationships and the health and well-being of individuals and community.
- More prominently, these include issues such as cyber bullying which has targeted the very young individual, some as young as eight years old to the older.
- Computer hacking is the act of modifying computer hardware or software, in order to cause damage to sensitive data or to simply steal confidential information. (Buzzle.com, 2018).
- The Internet is a chance for a computer to connect to the world, which also makes it susceptible to attacks from hackers.
- Computer hacking can be an indictable crime. Computer hacking is a fall foul of computer security. It can leak sensitive user data and risk user privacy.

- Hacking exposes confidential information of the user. Identity theft online is another important hacking effect.
- Hacking may also danger your national security and fraud also is another major effect of computer hacking.

Hackers

- A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more.
- Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.
- Hackers breach defenses to gain unauthorized access into computers, phones, tablets, IoT devices, networks, or entire computing systems.
- Hackers also take advantage of weaknesses in network security to gain access.
- The weaknesses can be technical or social in nature:
  - *Technical weaknesses: Hackers can exploit software vulnerabilities or weak security practices to gain unauthorized access or inject malware, for example.*
  - *Social weaknesses: Hackers can also use social engineering to convince those with privileged access to targeted systems to click on malicious links, open infected files, or reveal personal information, thereby gaining access to otherwise hardened infrastructures.*
- Hackers usually have an advanced level knowledge regarding computer security and possess all the technical knowledge required as well but are not necessarily skilful as hackers. Few of them are skilled enough to develop their own software and tools.
- Hackers aim to counter attack threats posed by crackers to the computer systems as well as internet security across networks.

Types of Hackers

- Computers and the Internet have changed the work environment of the world beyond imagination.
- Computers on taking over a major part of our lives, all our data has got transferred from records and ledgers to computers. Though this kind of shift in working has reduced the physical burden on workers it has also increased the chances of data theft.

- People involved in stealing data or harming the systems are knowledgeable people with wrong intentions known as Hackers.
- There are different types of hackers:

1) ***White Hat Hackers***
   - *White hat hackers are types of hackers who're professionals with expertise in cybersecurity.*
   - *They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system.*
   - *They hack the system from the loopholes in the cybersecurity of the organization.*
   - *This hacking is done to test the level of cybersecurity in the organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources.*
   - *White hat hackers work per the rules and regulations the government sets. White hat hackers are also known as ethical hackers.*
   - *The goals of these types of hackers are helping businesses and an appetite for detecting gaps in networks' security. They aim to protect and assist companies in the ongoing battle against cyber threats.*
   - *A White Hat hacker is any individual who will help protect the company from raising cybercrimes. They help enterprises create defences, detect vulnerabilities, and solve them before other cybercriminals can find them.*

2) ***Black Hat Hackers***
   - *Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry.*
   - *On gaining entry they might steal the data or destroy the system.*
   - *The hacking practices these types of hackers use depend on the individual's hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal.*
   - *The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.*

- *To hack into organizations' networks and steal bank data, funds or sensitive information.*
- *Normally, they use the stolen resources to profit themselves, sell them on the black market or harass their target company.*

3) ***Gray Hat Hackers***

- *The intention behind the hacking is considered while categorizing the hacker.*
- *The Gray hat hacker falls between the black and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain.*
- *The intention behind hacking decides the type of hacker. If the intention is for personal gain, the hacker is considered a gray hat hacker.*
- *The difference is, they don't want to rob people nor want to help people in particular. Rather, they enjoy experimenting with systems to find loopholes, crack defenses, and generally find a fun hacking experience.*

4) ***Script Kiddies***

- *It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateur's types of hackers in the field of hacking.*
- *They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites.*
- *The intention behind the hacking is just to get the attention of their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.*
- *One standard Kiddie Script attack is a DoS (Denial of Service) or DDoS attack (Distributed Denial of Service). This simply means that an IP address is flooded with too much excessive traffic that it collapses.*

5) ***Green Hat Hackers***

- *Green hat hackers are types of hackers who learn the ropes of hacking. They are slightly different from the Script Kiddies due to their intention.*
- *The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.*

6) ***Blue Hat Hackers***

- *Blue Hat Hackers are types of hackers who're similar to Script Kiddies. The intent to learn is missing.*
- *They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries.*
- *Blue Hat Hackers is dangerous due to the intent behind the hacking rather than their knowledge.*

7) ***Red Hat Hackers***

- *Red Hat Hackers is synonymous with Eagle-Eyed Hackers. They are the types of hackers who're similar to white hackers.*
- *The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is that the process of hacking through intention remains the same.*
- *Red hat hackers are quite ruthless when dealing with black hat hackers or counteracting malware. The red hat hackers continue to attack and may end up having to replace the entire system setup.*

8) ***State/Nation Sponsored Hackers***

- *Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers.*
- *They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country.*
- *The sensitive information aids in being on top of every situation but also in avoiding upcoming danger. They report only to their governments.*

9) ***Hacktivist***

- *These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist.*
- *Hacktivists can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks.*
- *The data gained from government files accessed are used for personal political or social gain.*

10) ***Malicious insider or Whistleblower***

- *These types of hackers include individuals working in an organization who can expose confidential information.*
- *The intent behind the exposure might be a personal grudge against the organization, or the individual might have come across illegal activities within the organization.*
- *The reason for exposure defines the intent behind the exposure. These individuals are known as whistleblowers.*

Ethical Hackers

- An ethical hacker, also referred to as a white hat hacker, is an information security (infosec) expert who penetrates a computer system, network, application or other computing resource on behalf of its owners -- and with their authorization.
- Organizations call on ethical hackers to uncover potential security vulnerabilities that malicious hackers could exploit.
- The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in target systems, networks or system infrastructure.
- The process entails finding and then attempting to exploit vulnerabilities to determine whether unauthorized access or other malicious activities are possible.
- An ethical hacker needs deep technical expertise in infosec to recognize potential attack vectors that threaten business and operational data.
- People employed as ethical hackers typically demonstrate applied knowledge gained through recognized industry certifications or university computer science degree programs and through practical experience working with security systems.
- Ethical hackers generally find security exposures in insecure system configurations, known and unknown hardware or software vulnerabilities, and operational weaknesses in process or technical countermeasures.
- Potential security threats of malicious hacking include distributed denial-of-service attacks in which multiple computer systems are compromised and redirected to attack a specific target, which can include any resource on the computing network.
- An ethical hacker is given wide latitude by an organization to legitimately and repeatedly attempt to breach its computing infrastructure. This involves exploiting known attack vectors to test the resiliency of an organization's infosec posture.

- Ethical hackers can help organizations in a number of ways, including the following:
  - ***Finding vulnerabilities****: Ethical hackers help companies determine which of their IT security measures are effective, which need updating and which contain vulnerabilities that can be exploited. When ethical hackers finish evaluating an organization's systems, they report back to company leaders about those vulnerable areas, which may include a lack of sufficient password encryption, insecure applications or exposed systems running unpatched software. Organizations can use the data from these tests to make informed decisions about where and how to improve their security posture to prevent cyberattacks.*
  - ***Demonstrating methods used by cybercriminals****: These demonstrations show executives the hacking techniques that malicious actors could use to attack their systems and wreak havoc on their businesses. Companies that have in-depth knowledge of the methods the attackers use to break into their systems are better able to prevent those incursions.*
  - ***Helping to prepare for a cyber attack****: Cyber attacks can cripple or destroy a business -- especially a smaller business -- but most companies are still unprepared for cyber attacks. Ethical hackers understand how threat actors operate, and they know how these bad actors will use new information and techniques to attack systems. Security professionals who work with ethical hackers are better able to prepare for future attacks because they can better react to the constantly changing nature of online threats.*
- Ethical hackers also rely on social engineering techniques to manipulate end users and obtain information about an organization's computing environment.
- Like black hat hackers, ethical hackers rummage through postings on social media or GitHub, engage employees in phishing attacks through email or texting, or roam through premises with a clipboard to exploit vulnerabilities in physical security.
- However, there are social engineering techniques that ethical hackers should not use, such as making physical threats to employees or other types of attempts to extort access or information.

Role of Security and Penetration Tester

Hacking and Legal Implications

- A hacker is someone who gains access to a computer system or network without authorization.
- Such access is illegal, even if no harm is done. The U.S. Department of Justice classifies all such acts as hacking.
- Cracker vs Hacker:
  - Crackers: Break in with malicious intent (e.g., data theft, damage).
  - Hackers: May explore or test systems just to prove they can — not always with harmful intent.
- In this course/book, no distinction is made — all unauthorized access is termed hacking.

Who is an Ethical Hacker?

- An ethical hacker performs activities similar to a hacker, but with legal permission from the owner.
- The purpose is to find security weaknesses before someone with malicious intent does.
- Ethical hacking helps organizations:
  - Protect sensitive data.
  - Understand vulnerabilities in their systems.
- **Difference**: Consent makes the act legal and constructive — no criminal charges involved.

Why Organizations Hire Ethical Hackers

- Companies understand that **cyber attacks** are a constant threat.
- Rather than **waiting to be attacked**, they:
  - Hire professionals to **test** their systems.
  - Discover issues in **network configuration, firewalls, applications**, etc.
- This proactive approach saves:
  - **Money**, **reputation**, and **operational downtime**.

Types of Hackers

- **Script Kiddies / Packet Monkeys**:
  - Use pre-made tools or scripts created by others.
  - Lack deep technical understanding.
  - Often young or amateur users.
- **Professional Hackers / Penetration Testers**:
  - Write their own scripts and programs to test or exploit systems.
  - Use languages like:
    - Python, Ruby, Perl, C
  - Perform more sophisticated, targeted testing.

- A **script** is a set of instructions used to automate tasks such as scanning, attacking, or logging into systems.

Hacktivism and Hacktivists

- A **hacktivist** is someone who uses hacking for **political or social causes**.
- Motivated by **activism**, not personal gain.
- Example: The group **Anonymous**
  - In 2015, hacked the **KKK's Twitter** account and threatened to release names.
- This act of digital protest is called **hacktivism**.
- Often controversial — some see it as activism, others as cybercrime.

What is Penetration Testing?

- **Penetration testing**, also known as **ethical hacking** or **white hat hacking**, is the practice of legally testing computer systems, networks, and applications for security weaknesses.
- It helps organizations **find and fix vulnerabilities before malicious hackers exploit them**.

Purpose of Security Testing

- To simulate real-world cyber attacks and assess the **strength of security defenses**.
- It protects **critical digital assets** like customer data, financial records, and confidential information.
- Especially crucial for sectors like:
  - **Banking/Finance**
  - **Healthcare**
  - **Government and IT Infrastructure**

Tools and Setup for Penetration Testers

- Penetration testers usually carry a **customized laptop** with:
  - Multiple Operating Systems (e.g., Linux, Windows, macOS).
  - Specialized tools (for scanning, exploiting, reporting).
- Most use **Kali Linux**, a security-focused Linux distro.
  - Pre-loaded with tools for:
    - Network testing
    - Web application testing
    - Wireless auditing
- Kali Linux is freely available at: https://www.kali.org

Real-World Penetration Tester Job Description

Typical responsibilities include:

1. **Vulnerability and Penetration Assessments**:
   - Simulate attacks on Internet, Intranet, and wireless networks.
2. **Port and Service Scanning**:
   - Discover what services are open and potentially exploitable.
3. **Exploit Usage**:
   - Gain and escalate access using known vulnerabilities.
4. **Application Testing**:
   - Review source code for flaws (e.g., SQL injection, XSS).
5. **Client Interaction**:
   - Communicate before, during, and after testing.
6. **Reporting and Documentation**:
   - Log findings clearly and suggest remediation.
7. **Post-engagement Debriefing**:
   - Explain vulnerabilities and risk levels to the client.
8. **Continuous Learning & Research**:
   - Stay updated with new threats and techniques.
9. **Understanding Legal Boundaries**:
   - Must be aware of **local/national cyber laws**.

Many of these jobs are advertised on platforms looking for certified professionals with real-world experience.

Security test engineer

- The ***security test engineer*** will be part of the audit team that shall conduct security audits for the clients in order to identify the gaps in terms of web security, application security, web-application security, mobile app security, Network security and IT infrastructure security.He is responsible to
  - **Conduct Security Audits**-Test websites, apps, networks, and IT systems to find security weaknesses.
  - **Assess Risk**-Understand how serious each issue is based on the system being tested.
  - **Know the Threats**-Stay aware of current cyber threats and explain key risks clearly.
  - **Communicate to All Levels**-Share findings in a way that both tech teams and managers can understand.
  - **Hands-On Security Testing**-Perform deep and practical testing using tools and new techniques to find real issues.
- The ***Security Tester*** will be responsible for leading teams on client engagements as well as working on their own.

- ***Penetration testers*** need a solid understanding of information technology (IT) and security systems in order to test them for vulnerabilities.
- Skills you might find on a pen tester job description include:
  - Network and application security
  - Programming languages, especially for scripting (Python, BASH, Java, Ruby, Perl)
  - Threat modeling
  - Linux, Windows, and MacOS environments
  - Security assessment tools
  - Pentest management platforms
  - Technical writing and documentation
  - Cryptography
  - Cloud architecture
  - Remote access technologies
- Penetration testing is the official name for "good" hacking—in other words, identifying security gaps that could lead to cybersecurity attacks before malicious hackers find them. It also goes by the names "white hat hacking" or "ethical hacking."
- ***Penetration testers*** help organizations identify security gaps and vulnerabilities in their IT infrastructures.
- Penetration testing is valuable for any company with digital data to protect—which is just about all companies in the digital age.
- Financial and medical institutions, which both stores highly sensitive data, are often the keenest to use penetration testing to protect themselves from breaches, but organizations in any industry can benefit from this tech service.
- There are a few qualities that many penetration testers share.
  - ***Sense of curiosity, and an eagerness to learn***. Technology doesn't stay the same for long. Hackers are continuously updating their bags of tricks to find new ways to accomplish data breaches, which means penetration testers need to stay on their toes. A good penetration tester is a person who's curious about how things work and constantly learns new things in order to hack the system and be one step ahead of hackers.
  - ***Strong communication skills***. Penetration testers will have an easier time accomplishing their goals if they're skilled at making sure everyone on their team is

on the same page. They also need to clearly communicate with clients, which can be tricky. They need to be able to explain what's wrong to people who are not in the industry and don't understand their technical language.

- ***Detail-oriented problem-solvers***. Some systems might have glaring vulnerabilities that are easy to find. But to think like a hacker, penetration testers need a keen eye for detail so they can spot problems that aren't easy to see. Once they've identified a gap in security, they need the problem-solving skills to fix it.

- Most penetration testing begins with a team meeting to agree on a strategy and work assignments for the current project.
- Next, they'll move onto the actual assessments. Some responsibilities include planning and designing penetration tests to pinpoint the weaknesses in the best way, conducting tests, creating reports and advising on security improvements.

Penetration Testing Methodologies

Penetration Testing Models

Ethical hackers choose a testing model based on how much information they are given before the test begins. The three primary models are:

1.White Box Testing

- **Also called** Clear Box or Glass Box Testing

- **Here** tester is given **full knowledge** of the system, to simulate an **insider attack** or **developer-level audit,** including:
  - Network architecture
  - Source code
  - Admin credentials
  - System configurations

- **Advantage**: Deep and comprehensive testing; helps in identifying flaws in design, logic, and internal security.

Use When:

- Testing for secure coding practices
- Auditing internal systems
- Time is limited and full coverage is desired

2. Black Box Testing

- The tester has **no prior knowledge** of the target system.
- Simulates a **real-world attack by an external hacker**.
- Testers rely on:
    - Reconnaissance (e.g., DNS lookups, scanning)
    - Publicly available information
    - Trial and error techniques
- **Advantage**: Realistic simulation of how a real attacker would operate.

⚠️ **Limitation**:

- Time-consuming and may not uncover deep or internal flaws
- Coverage is limited compared to white box

Use When:

- Simulating an attack from outside the organization
- Assessing perimeter/network defenses

3. Grey Box Testing

- The tester has **partial knowledge** of the internal system, such as:
    - User credentials (non-admin)
    - Network diagrams
    - Limited API documentation or internal info
- Simulates a **semi-informed attacker**, like a rogue employee or contractor.
- Combines both **internal insight** and **external attack methods**.

  Advantage: Balanced approach offering realistic attack simulation with focused, efficient testing.
- ⚠️ **Limitations:**
    - May miss low-level logic flaws due to lack of complete system access
- 🔍 **Use When:**
    - Testing role-based access or privilege escalation
    - Simulating attacks from trusted insiders
    - Assessing security of internal applications or APIs

Penetration testing is a systematic process used to identify and exploit security vulnerabilities in a network, application, or system, with the goal of strengthening its defenses before malicious attackers can exploit them. It involves simulating real-world attacks using various tools and techniques to uncover gaps in security, such as misconfigurations, weak access controls, or software flaws. A well-executed penetration test not only reveals vulnerabilities but also provides detailed insights into their potential impact on the organization. This helps businesses prioritize risks, improve their security posture, and safeguard sensitive information from unauthorized access.

The steps involved in Penetration Testing are:

- Determining the feasibility of a particular set of attack vendors
- Identifying risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
- Figuring out vulnerabilities that maybe difficult to detect with automated network applications
- Assessing the magnitude of potential business and operational impacts of successful attacks
- Providing evidence to support increased investment in security personnel and technology

Penetration Testing is an evolving function of the IT infrastructure of many enterprises today. Its wings are forever expanding to encompass many inter-departmental concerns like social engineering, web application security and physical penetration testing.There are multiple penetration testing methodologies that can be put to use depending on the category of the target business, the goal of the pentest, and its scope.

Phases of Penetration Testing Methodology:

1. ***Data collection***: *There are a plenty of methods used to get target system data, including Google Search. While Web page source code analysis is another technique to get more information about the system, software and plugin versions, there are an array of free tools and services available in the market too that provides information like database, table names, software versions and hardware used by various third-party plugins.*

2. ***Vulnerability Assessment:*** *Based on the data collected via first step, security weakness in the target system can be identified with ease. This helps penetration testers to launch attacks using identified entry points in the system.*
3. ***Actual Exploit:*** *This being the crucial step, it requires special skills and techniques to launch attack on target system. Experienced penetration testers can use their skills to launch attack on the system*
4. ***Result analysis and report preparation****: After completion of penetration tests detailed reports are prepared for taking corrective actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. You can customize vulnerability report format (HTML, XML, MS Word or PDF) as per your organization needs.*

Penetration Testing Methodologies

Penetration testing methodologies provide a structured approach to ethically hack systems and identify vulnerabilities in a controlled and repeatable manner. These methods ensure thoroughness, consistency, and alignment with industry best practices.

Here are the most widely adopted penetration testing methodologies:

OSSTMM (Open-Source Security Testing Methodology Manual)

- *It is a methodology to test the operational security of physical locations, workflow, human security testing, physical security testing, wireless security testing, telecommunication security testing, data networks security testing and compliance. OSSTMM can be supporting reference of IOS 27001 instead of a hands-on penetration testing guide.*
- *OSSTMM includes the following key sections:*
  - *Operational Security Metrics*
  - *Trust Analysis*
  - *Work Flow.*
  - *Human Security Testing*
  - *Physical Security Testing*
  - *Wireless Security Testing*
  - *Telecommunications Security Testing*
  - *Data Networks Security Testing*
  - *Compliance Regulations*

- *Reporting with the STAR (Security Test Audit Report)*

- *The Open-Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed pen testing methodology (Institute for Security and Open Methodologies, 2010).*
- *It provides a scientific framework for network pentesting and vulnerability assessment and offers a comprehensive guide that can be properly utilized by a certified pen tester.*
- *The OSSTMM covers five categories:*
  - *Data and information controls*
  - *Cyber Security awareness among personnel*
  - *Fraud and social engineering controls*
  - *Controls for networked devices, including computers and wireless devices*
  - *Physical security controls*
- *One of the main benefits of the OSSTMM is its high level of flexibility. If pen testers apply the OSSTMM properly, they can use it to resolve vulnerabilities found on multiple devices, including computers, servers, wireless devices, and more.*
- *The four modules defined by OSSTMM are:*

Phase I: Regulatory

- *Posture review – review relevant regulatory and legislative frameworks and standards*
- *Logistics – identify any physical and technical constraints to the processes in the channel*
- *Active detection verification – evaluate interaction detection and response*

Phase II: Definitions

- *Visibility audit – assess the visibility of information, systems and processes relevant to the target*
- *Access verification – assess access points to the target*
- *Trust verification – assess trust relationship between the systems (or between people)*
- *Control verification – assess controls to maintain confidentiality, integrity, privacy and non-repudiation within the systems*

Phase III: Information Phase

- *Process verification – review the security processes of the organisation*
- *Configuration verification – evaluate the processes under various security level conditions*

- *Property validation – examine the physical or intellectual property available at the organisation*
- *Segregation review – determine the levels of personal information leaks*
- *Exposure review – evaluate sensitive information exposure*
- *Competitive intelligence – determine information leaks which could aid competitors*

Phase IV: Interactive Controls Test Phase

- *Quarantive verification – evaluate the effectiveness of quarantine functions on the target*
- *Privileges audit – review effectiveness of authorisation and potential impact of unauthorised privilege escalation*
- *Survivability validation – assess systems resilience and recovery*
- *Alerts and logs review – review audit activities in ensuring reliable events trail*

- *OSSTMM focuses on which items need to be tested, what to do before, during and after a security test, and how to measure the results.*
- *One particularly useful part of OSSTMM is that it has a section covering international best practices, laws, regulations and ethical standards.*

NIST (National Institute of Standards and Technology)

- *NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST) based on existing standards, guidelines, and practices.*
- *The framework "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes",in addition to guidance on the protection of privacy and civil liberties in a cybersecurity context.*
- *It has been translated to many languages, and is used by several governments and a wide range of businesses and organizations.*
- *The NIST Cybersecurity Framework organizes its "core" material into five "functions" which are subdivided into a total of 23 "categories".*
- *For each category, it defines a number of subcategories of cybersecurity outcomes and security controls, with 108 subcategories in all.*
- *For each subcategory, it also provides "Informative Resources" referencing specific sections of a variety of other information security standards, including ISO 27001,*

COBIT, NIST SP 800-53, ANSI/ISA-62443, and the Council on CyberSecurity Critical Security Controls (CCS CSC, now managed by the Center for Internet Security).

- *Here are the functions and categories, along with their unique identifiers and definitions, as stated in the framework document:*

1. Identify

- *"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."*
- *Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.*
- *Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.*
- *Governance (ID.GV):- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.*
- *Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*
- *Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.*
- *Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.*

2. Protect

- *"Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."*
- *Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.*

- *Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.*
- *Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*
- *Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*
- *Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.*
- *Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*

3. Detect

- *"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."*
- *Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.*
- *Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.*
- *Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.*

4. Respond

- *"Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident."*
- *Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.*

- *Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.*
- *Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.*
- *Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.*
- *Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.*

5. Recover

- *"Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."*
- *Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.*
- *Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.*
- *Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.*

Open Web Application Security Project (OWASP)

- *The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security.*
- *One of OWASP's core principles is that all of their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security.*
- *The materials they offer include documentation, tools, videos, and forums. Perhaps their best-known project is the OWASP Top 10.*
- *The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks.*

- *The report is put together by a team of security experts from all over the world.*
- *OWASP refers to the Top 10 as an 'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.*
- *The security risks reported in the OWASP Top 10 2017 report:*

1. Injection

- ✔ *Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack.*
- ✔ *Injection attacks can be prevented by validating and/or sanitizing user-submitted data. (Validation means rejecting suspicious-looking data, while sanitization refers to cleaning up the suspicious-looking parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.*

2. Broken Authentication

- ✔ *Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use a script to try all those combinations on a login system to see if there are any that work.*
- ✔ *Some strategies to mitigate authentication vulnerabilities are requiring two-factor authentication (2FA) as well as limiting or delaying repeated login attempts using rate limiting.*

3. Sensitive Data Exposure

- ✔ *If web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and sellor utilize it for nefarious purposes. One popular method for stealing sensitive information is using an on-path attack.*
- ✔ *Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching* of any sensitive information. Additionally, web application*

developers should take care to ensure that they are not unnecessarily storing any sensitive data.

- ✔ *Caching is the practice of temporarily storing data for re-use. For example, web browsers will often cache webpages so that if a user revisits those pages within a fixed time span, the browser does not have to fetch the pages from the web.*

4. XML External Entities (XEE)

- ✔ *This is an attack against a web application that parses XML input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.*
- ✔ *The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON, or at the very least to patch XML parsers and disable the use of external entities in an XML application.*
- ✔ *XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications.*
- ✔ *JavaScript Object Notation (JSON) is a type of simple, human-readable notation often used to transmit data over the internet. Although it was originally created for JavaScript, JSON is language-agnostic and can be interpreted by many different programming languages.*

5. Broken Access Control

- ✔ *Access control refers a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators. For example, a web application could allow a user to change which account they are logged in as simply by changing part of a url, without any other verification.*
- ✔ *Access controls can be secured by ensuring that a web application uses authorization tokens and sets tight controls on them.*
- ✔ *Many services issue authorization tokens when users log in. Every privileged request that a user makes will require that the authorization token be present. This is a secure*

way to ensure that the user is who they say they are, without having to constantly enter their login credentials.

6. Security Misconfiguration

- ✔ *Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly-descriptive errors which may reveal vulnerabilities in the application.*
- ✔ *This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.*

7. Cross-Site Scripting

- ✔ *Cross-site scripting vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users. This vulnerability can be exploited to run malicious JavaScript code on a victim's browser. For example, an attacker could send an email to a victim that appears to be from a trusted bank, with a link to that bank's website. This link could have some malicious JavaScript code tagged onto the end of the url. If the bank's site is not properly protected against cross-site scripting, then that malicious code will be run in the victim's web browser when they click on the link.*
- ✔ *Mitigation strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and/or sanitizing user-generated content. Using modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.*

8. Insecure Deserialization

- ✔ *This threat targets the many web applications which frequently serialize and deserialize data.*
- ✔ *Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it.*
- ✔ *Deserialization is just the opposite: converting serialized data back into objects the application can use.*

- ✔ *Serialization is sort of like packing furniture away into boxes before a move, and deserialization is like unpacking the boxes and assembling the furniture after the move.*
- ✔ *An insecure deserialization attack is like having the movers tamper with the contents of the boxes before they are unpacked.*
- ✔ *An insecure deserialization exploit is the result of deserializing data from untrusted sources, and can result in serious consequences like DDoS attacks and remote code execution attacks. While steps can be taken to try and catch attackers, such as monitoring deserialization and implementing type checks, the only sure way to protect against insecure deserialization attacks is to prohibit the deserialization of data from untrusted sources.*

9. Using Components With Known Vulnerabilities

- ✔ *Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks.*
- ✔ *Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.*
- ✔ *Component developers often offer security patches and updates to plug up known vulnerabilities, but web application developers don't always have the patched or most-recent versions of components running on their applications.*
- ✔ *To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.*

10. Insufficient Logging And Monitoring

- ✔ *Many web applications are not taking enough steps to detect data breaches. The average discovery time for a breach is around 200 days after it has happened. This gives attackers a lot of time to cause damage before there is any response.*

✔ *OWASP recommends that web developers should implement logging and monitoring as well as incident response plans to ensure that they are made aware of attacks on their applications.*

Categories of Penetration Test

✔ ***White box penetration testing***

White box penetration testing, sometimes referred to as crystal or oblique box pen testing, involves sharing full network and system information with the tester, including network maps and credentials. This helps to save time and reduce the overall cost of an engagement. A white box penetration test is useful for simulating a targeted attack on a specific system utilising as many attack vectors as possible.

✔ ***Black box penetration testing***

In a black box penetration test, no information is provided to the tester at all. The pen tester in this instance follows the approach of an unprivileged attacker, from initial access and execution through to exploitation. This scenario can be seen as the most authentic, demonstrating how an adversary with no inside knowledge would target and compromise an organisation. However, this typically makes it the costliest option too.

✔ ***Grey box penetration testing***

In a grey box penetration test, also known as a translucent box test, only limited information is shared with the tester. Usually this takes the form of login credentials. Grey box testing is useful to help understand the level of access a privileged user could gain and the potential damage they could cause. Grey box tests strike a balance between depth and efficiency and can be used to simulate either an insider threat or an attack that has breached the network perimeter.

Types of Penetration Tests

1. Internal/External Infrastructure Penetration Testing

An assessment of on-premise and cloud network infrastructure, including firewalls, system hosts and devices such as routers and switches. Can be framed as either an internal penetration test, focusing on assets inside the corporate network, or an external penetration test, targeting internet-facing infrastructure. To scope a test, you will need to know the number of internal and external IPs to be tested, network subnet size and number of sites.

2. Wireless Penetration Testing

A test that specifically targets an organisation's WLAN (wireless local area network), as well as wireless protocols including Bluetooth, ZigBee and Z-Wave. Helps to identify rogue access points, weaknesses in encryption and WPA vulnerabilities. To scope an engagement, testers will need to know the number of wireless and guest networks, locations and unique SSIDs to be assessed.

3. Web Application Testing

An assessment of websites and custom applications delivered over the web, looking to uncover coding, design and development flaws that could be maliciously exploited. Before approaching a testing provider, it's important to ascertain the number of apps that need testing, as well as the number of static pages, dynamic pages and input fields to be assessed.

4. Mobile Application Testing

The testing of mobile applications on operating systems including Android and iOS to identify authentication, authorisation, data leakage and session handling issues. To scope a test, providers will need to know the operating system types and versions they'd like an app to be tested on, number of API calls and requirements for jailbreaking and root detection.

5. Build and Configuration Review

Review of network builds and configurations to identify misconfigurations across web and app servers, routers and firewalls. The number of builds, operating systems and

application servers to be reviewed during testing is crucial information to help scope this type of engagement.

6. Social Engineering

An assessment of the ability of your systems and personnel to detect and respond to email phishing attacks. Gain precise insight into the potential risks through customised phishing, spear phishing and Business Email Compromise (BEC) attacks.

7. Cloud Penetration Testing

Custom cloud security assessments to help your organisation overcome shared responsibility challenges by uncovering and addressing vulnerabilities across cloud and hybrid environments that could leave critical assets exposed.

8. Agile Penetration Testing

Continuous, developer-centric security assessments designed to identify and remediate security vulnerabilities throughout the entire development cycle. This agile approach helps to ensure that every product release, whether it is a minor bug fix or a major feature, has been vetted from a security perspective.

Vulnerability Assessment

- A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.
- Using a risk-based approach, vulnerability assessments may target different layers of technology, the most common being host-, network-, and application-layer assessments.
- Vulnerability testing helps organizations identify vulnerabilities in their software and supporting infrastructure before a compromise can take place.
- A vulnerability can be defined in two ways:
  - A bug in code or a flaw in software design that can be exploited to cause harm. Exploitation may occur via an authenticated or unauthenticated attacker.
  - A gap in security procedures or a weakness in internal controls that when exploited results in a security breach.

- There are three primary objectives of a vulnerability assessment.
  - Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
  - Document the vulnerabilities so that developers can easily identify and reproduce the findings.
  - Create guidance to assist developers with remediating the identified vulnerabilities.
- The three dimensions of vulnerability we will explore are exposure, sensitivity, and adaptive capacity.
  - *Exposure* is the degree to which people and the things they value could be affected or "touched" by coastal hazards.
  - *Sensitivity* is the degree to which they could be harmed by that exposure.
  - *Adaptive Capacity* is the degree to which the community could mitigate the potential for harm by taking action to reduce exposure or sensitivity. This can also be thought of as a measure of resilience.
- Several types of vulnerability assessments can be conducted, including:

1. Network-Based Vulnerability Assessment

  - A network-based vulnerability assessment identifies vulnerabilities in network devices such as routers, switches, firewalls, and other network infrastructure components.
  - The primary goal of a network-based vulnerability assessment is to identify weaknesses in the network that attackers could exploit to gain unauthorized access, steal data, or launch attacks.
  - Network-based vulnerability assessments typically involve specialized software tools and techniques that scan the network for vulnerabilities. These tools may use various methods to identify vulnerabilities, such as port scanning, vulnerability scanning, password cracking, and network mapping.

2. Application-Based Vulnerability Assessment

  - An application vulnerability assessment identifies vulnerabilities in software applications, including web applications, mobile applications, and desktop applications.
  - These assessments typically involve testing the application for common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

- Application vulnerability assessments can be performed using both automated and manual methods.

3. API-Based Vulnerability Assessment

- API vulnerability assessment is conducted to identify and mitigate potential security risks in APIs.
- This process identifies vulnerabilities and weaknesses in the API's design, implementation, and deployment.
- The goal is to ensure that the API is secure, reliable, and resilient to attacks.

4. Host-Based Vulnerability Assessment

- A host-based vulnerability assessment identifies vulnerabilities in individual host systems, including servers, workstations, and laptops.
- These assessments typically involve scanning the host system for known vulnerabilities, such as missing security patches or outdated software.
- Host-based vulnerability assessments can be performed using both automated and manual methods.

5. Wireless Network Vulnerability Assessment

- A wireless network vulnerability assessment focuses on identifying vulnerabilities in wireless networks, including Wi-Fi networks. These assessments typically involve testing the wireless network for common vulnerabilities, such as weak encryption, default passwords, and rogue access points.
- Wireless network vulnerability assessments can be performed using specialized software tools and techniques.

6. Physical Vulnerability Assessment

- A physical vulnerability assessment identifies vulnerabilities in physical security measures, such as locks, surveillance cameras, and access control systems.
- These assessments typically involve physical inspections of the facility and its security measures and testing the effectiveness of those measures.

7. Social Engineering Vulnerability Assessment

- A social engineering vulnerability assessment identifies vulnerabilities in human behavior, such as phishing attacks and other social engineering techniques.
- This vulnerability assessment type typically involves simulated attacks against employees to test their awareness of security threats and their ability to identify and respond to them.

8. Cloud-Based Vulnerability Assessment

- A cloud-based vulnerability assessment identifies vulnerabilities in cloud infrastructure and services, such as Amazon Web Services (AWS) and Microsoft Azure.