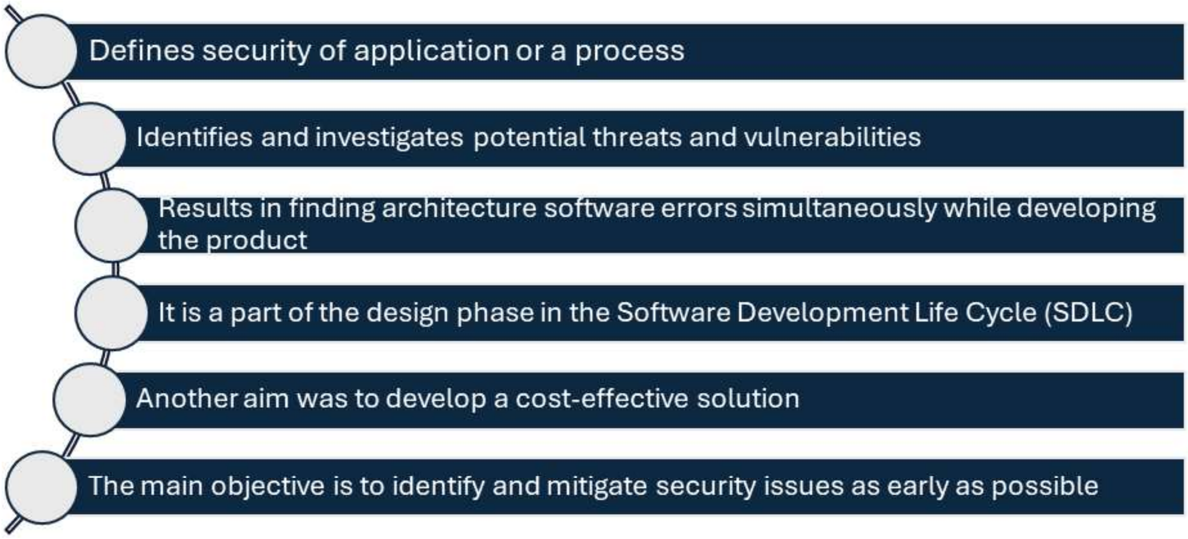
Topic 22: Threat Modeling



Defines security of application or a process

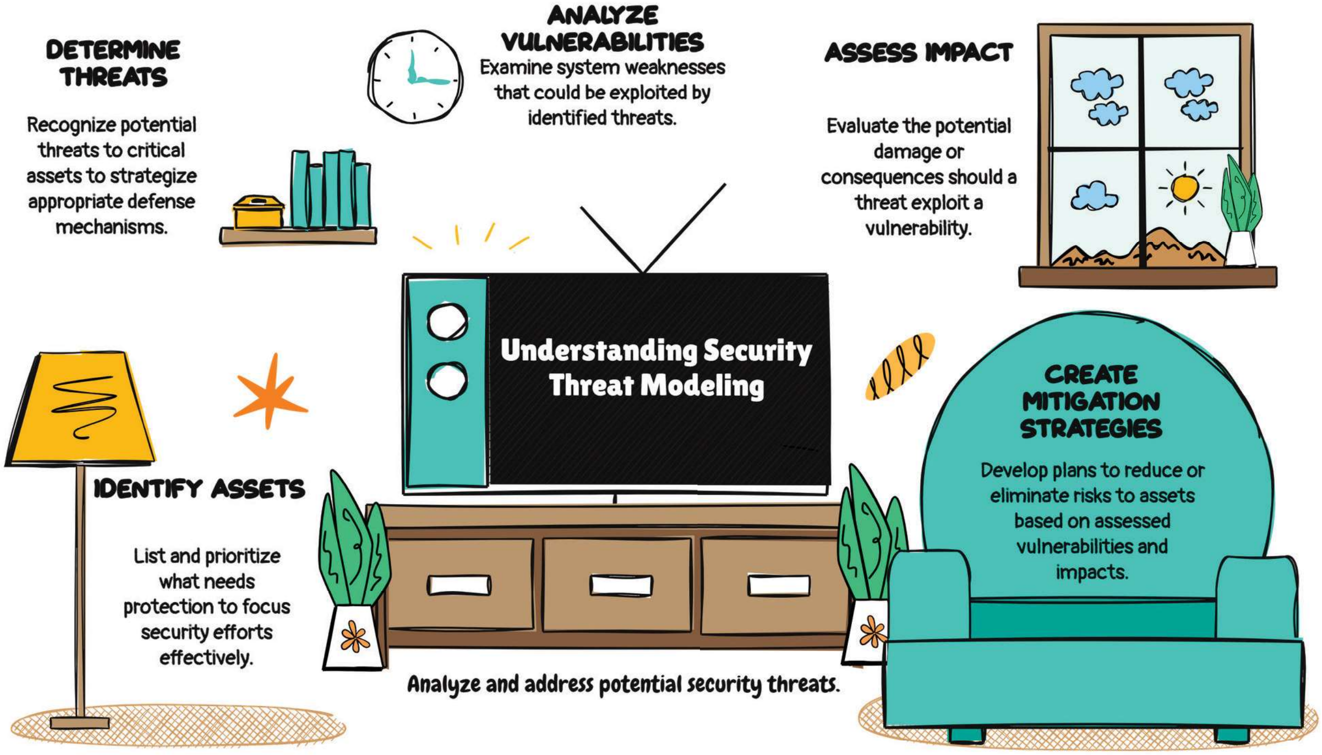
Identifies and investigates potential threats and vulnerabilities

Results in finding architecture software errors simultaneously while developing the product

It is a part of the design phase in the Software Development Life Cycle (SDLC)

Another aim was to develop a cost-effective solution

The main objective is to identify and mitigate security issues as early as possible



Understanding Security Threat Modeling

DETERMINE THREATS

Recognize potential threats to critical assets to strategize appropriate defense mechanisms.

ANALYZE VULNERABILITIES

Examine system weaknesses that could be exploited by identified threats.

ASSESS IMPACT

Evaluate the potential damage or consequences should a threat exploit a vulnerability.

IDENTIFY ASSETS

List and prioritize what needs protection to focus security efforts effectively.

CREATE MITIGATION STRATEGIES

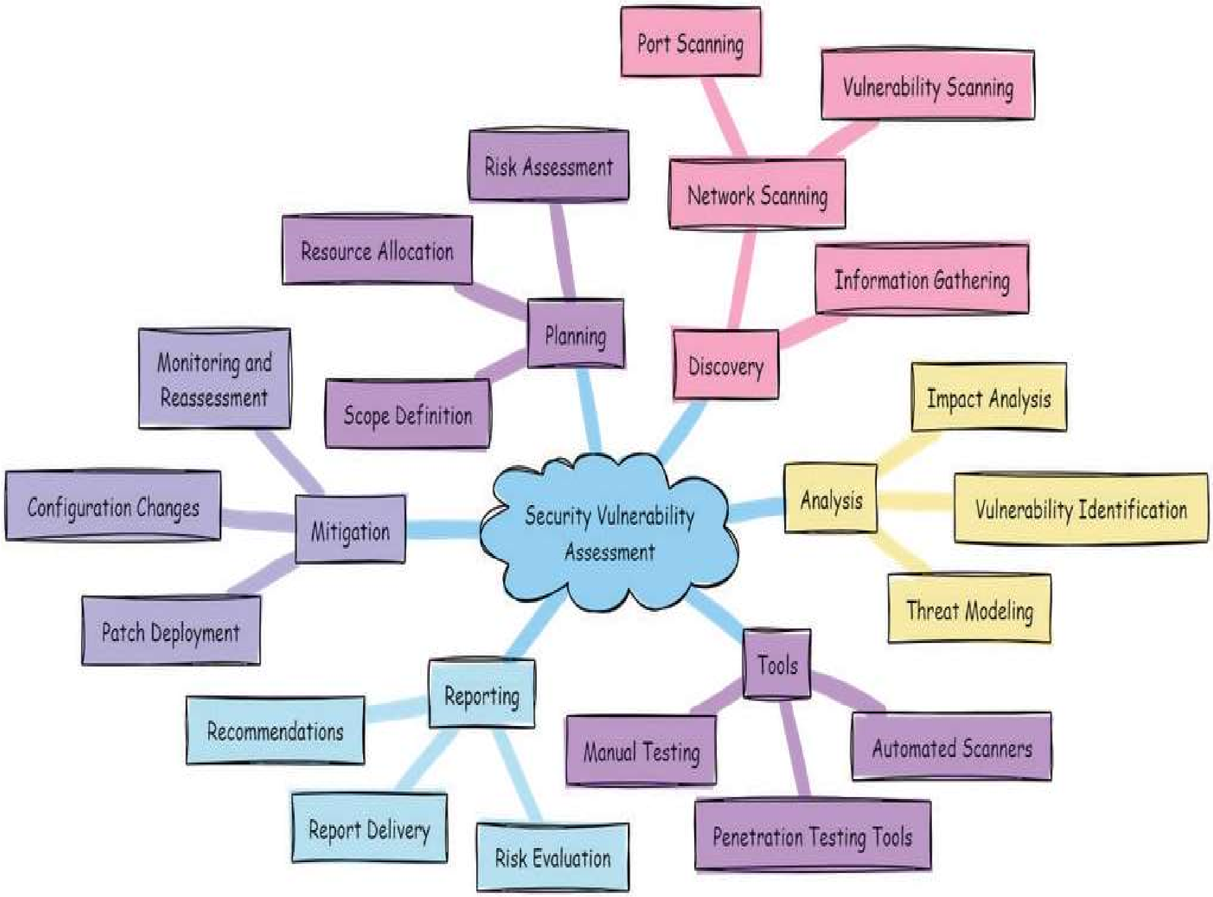
Develop plans to reduce or eliminate risks to assets based on assessed vulnerabilities and impacts.

Analyze and address potential security threats.

Topic 23: Vulnerability Assessment

- Assessment to find the weakness in an information system, security process, internal/ external controls, or implementation.
- It is not impossible to remove every technical vulnerability from a given process or information environment.
- It is based on technical aspects.

- It can be network-based or host-based.
- This can be done with manual or automated scanning tools.
- Typical steps involved are discovery, testing, analysis, and reporting.
- Vulnerability scans can be performed on applications, network environments, hosts, or wireless.
- Scans are primarily performed by matching signatures.
- Zero attacks can be blocked through an automated signature-based vulnerability assessment.
- Network-based scan for a range of listening TCP ports or enumerate running services.
- Host-based scan checks the system's configuration settings, patch details, and ports and services that are also visible to network-based scans.
- Application scans can correct errors in source code as well as specific vulnerabilities.
- Dynamic Application Security Testing (DAST) tools help identify vulnerabilities unique to web software, such as SQL injection, cross-site scripting (XSS), insufficient input validation, and sensitive data exposure.
- Compliance requirements are one of the most critical business cases for vulnerability scanning.
- The results should be documented.
- The distribution of the reports of vulnerability scanning should be restricted.
- Before performing vulnerability scanning in a system or network, prior permission from business owners/stakeholders should be taken.



50. As a security manager, you are very diligent and proactive. A separate vulnerability scanning team performs a regular network and host vulnerability scanning schedule. In addition, your organization uses signature automated vulnerability scanning. Suddenly, you realize from the SOC team the latest malware outbreak in the internal network. What can be the reason for this incident?
    A. Zero-day attacks cannot be flagged during vulnerability scanning
    B. Network firewalls are not configured properly
    C. Periodic pen tests are not performed
    D. The vulnerability scanning team is not competent

Correct Option	Wrong Option	Reason
A		**As previously highlighted, the CISSP candidate needs to understand the scenario presented comprehensively. The key terms within this context are "signature-based" and "latest malware." It's important to note that a signature-based vulnerability scanner relies on a database of known threats to identify vulnerabilities. Consequently, it is inherently unable to detect zero-day attacks—new vulnerabilities that have not yet been documented. This limitation explains why the scanner fails to flag the presence of the newest malware or any emerging zero-day threats in the environment, making option A the most suitable answer.**
	B	Option B is not the BEST option. We are unsure if the network devices are correctly configured in the given scenario. In this type of scenario question, you have to focus on keywords and the solution it's asking for,
	C	Option C is also not the BEST option. In the given scenario, there is no background for whether or not periodic pen tests are conducted. Therefore, there is no scope for the assumption. In this scenario, the reason (A signature-based vulnerability scanner is incapable of zero-day attacks) is already mentioned.
	D	Option D is also not the BEST answer. There is no background for mistakes or errors done by the vulnerability scanning team in the given scenario. In this scenario, the reason (A signature-based vulnerability scanner is incapable of zero-day attacks) is already mentioned.

51. As a security manager, you want to know the vulnerabilities of a network by simulating an external attack. This can be achieved by
    A. Vulnerability scanning
    B. Pentest
    C. Black hat hackers
    D. Business Impact Analysis

Correct Option	Wrong Option	Reason
	A	In this scenario, the keywords are simulating an external attack. Vulnerability scanning is conducted primarily on the inside network, and the attack was not stimulated. Also, for distraction, vulnerabilities are in question.
B		**Option B is the most appropriate choice. A penetration test simulates an external attack, assessing the organization's defenses against real-world threats. To ensure effectiveness and security, it is essential to define a comprehensive scope for the pen test and to secure the necessary approvals from stakeholders before proceeding with the assessment.**
	C	Black Hat hackers are hackers with malicious intent. Black hat hackers will never make an organization aware of its vulnerabilities.
	D	Business Impact analysis is an entirely wrong option in the given scenario.

Stages of Penetration testing

1. **Pre-engagement actions** – This is the MOST critical stage in a pen test. All the approvals and relevant information should be completed before the start of the pen test. Pertinent information such as in-scope network / IP addresses/systems is essential. Everything should be documented and signed by the appropriate authority.

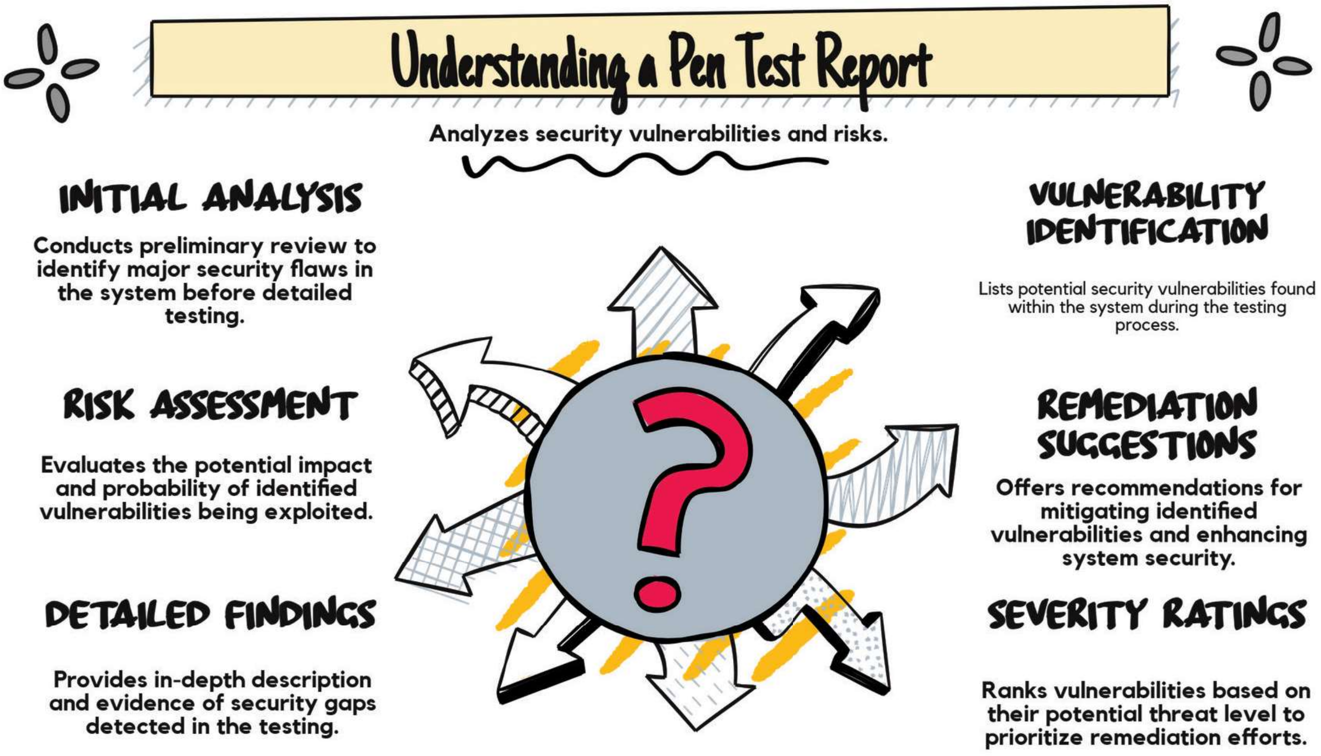
2. **Discovery / Reconnaissance** – The stage where the data are collected and mapped. It depends on the methodology being used. For example, more data must be gathered in the zero-level knowledge pen test, while less information must be collected in the Full knowledge-level pen test. Search engines provide the right level of intelligence. Domain name searches, WHOIS lookups, and reverse DNS to get subdomains are everyday tasks for external pen tests. Social engineering can be used to get information. This is the passive stage of an attack.

3. **Enumeration** – More detailed information is mapped in this stage. This is still a passive stage of an attack. This stage will provide more technical information, such as a system's running ports, an application's network ports, etc.

4. **Vulnerability analysis** – The detailed information is now mapped with known vulnerabilities. There can be many ways by which a network or a system can be hacked. It will define the approach and method by which the hacking must be done.

5. **Execution / Exploitation** – This is an active stage of the attack. Numerous attack scenarios can be activated in this stage. Automated tools or customized tools can be used in the exploitation. All the objectives of this testing should be well documented. Also, the monitoring aspects of various applications and network components are checked. As this is an active phase, hence there should be corresponding logs. The efficiency of the SOC team can also be tested at this stage.

6. **Reporting / Findings –** The final stage is to collate testing reports and results and document them for reference. All the required details are documented, such as security gaps, a list of vulnerabilities, an analysis of log activities, and suggested countermeasures.



Understanding a Pen Test Report

Analyzes security vulnerabilities and risks.

INITIAL ANALYSIS

Conducts preliminary review to identify major security flaws in the system before detailed testing.

RISK ASSESSMENT

Evaluates the potential impact and probability of identified vulnerabilities being exploited.

DETAILED FINDINGS

Provides in-depth description and evidence of security gaps detected in the testing.

VULNERABILITY IDENTIFICATION

Lists potential security vulnerabilities found within the system during the testing process.

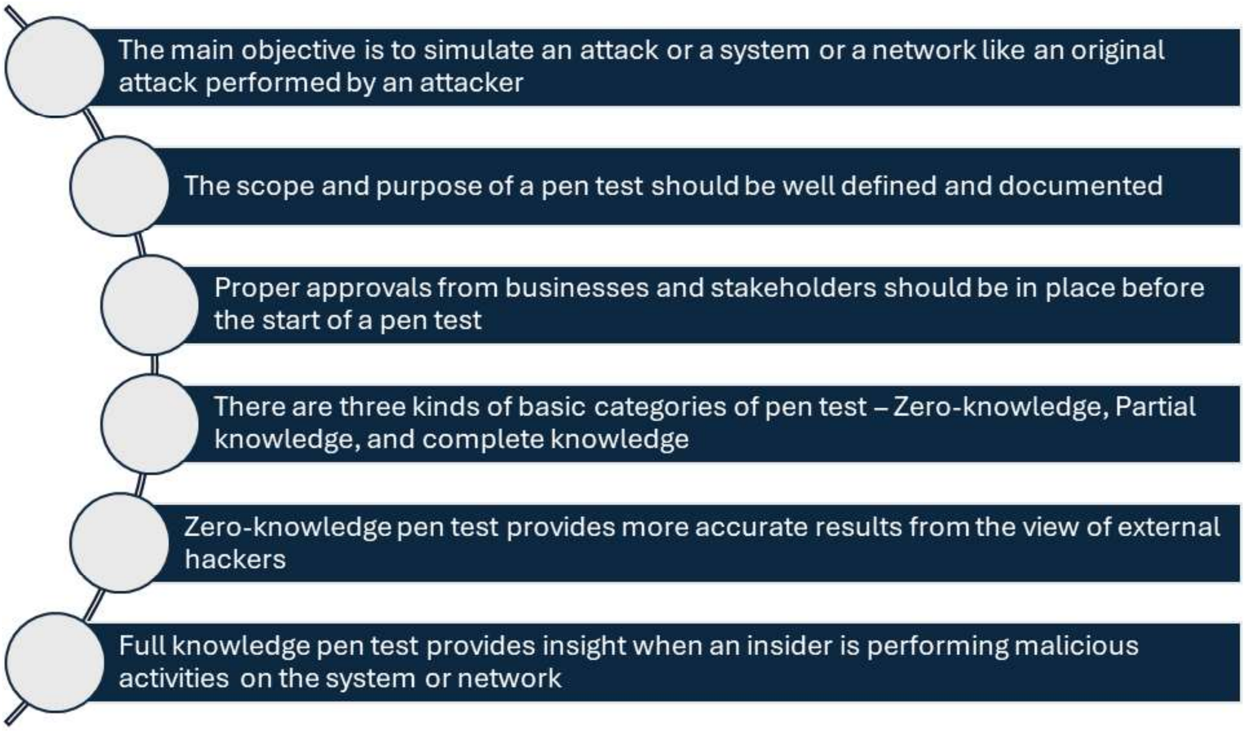
REMEDIATION SUGGESTIONS

Offers recommendations for mitigating identified vulnerabilities and enhancing system security.

SEVERITY RATINGS

Ranks vulnerabilities based on their potential threat level to prioritize remediation efforts.

Topic 24: Penetration Test Strategies and Methodologies



The main objective is to simulate an attack or a system or a network like an original attack performed by an attacker

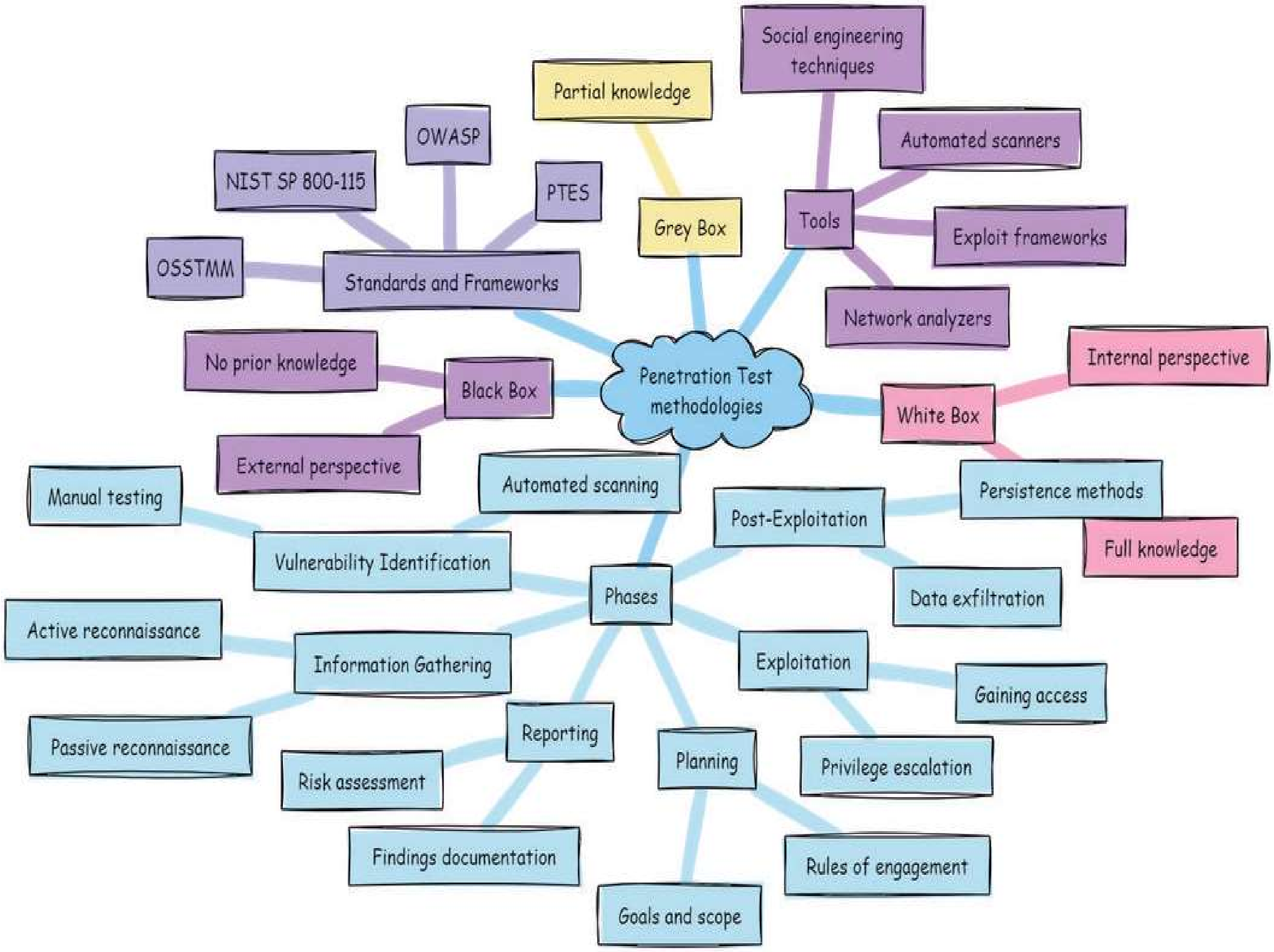
The scope and purpose of a pen test should be well defined and documented

Proper approvals from businesses and stakeholders should be in place before the start of a pen test

There are three kinds of basic categories of pen test – Zero-knowledge, Partial knowledge, and complete knowledge

Zero-knowledge pen test provides more accurate results from the view of external hackers

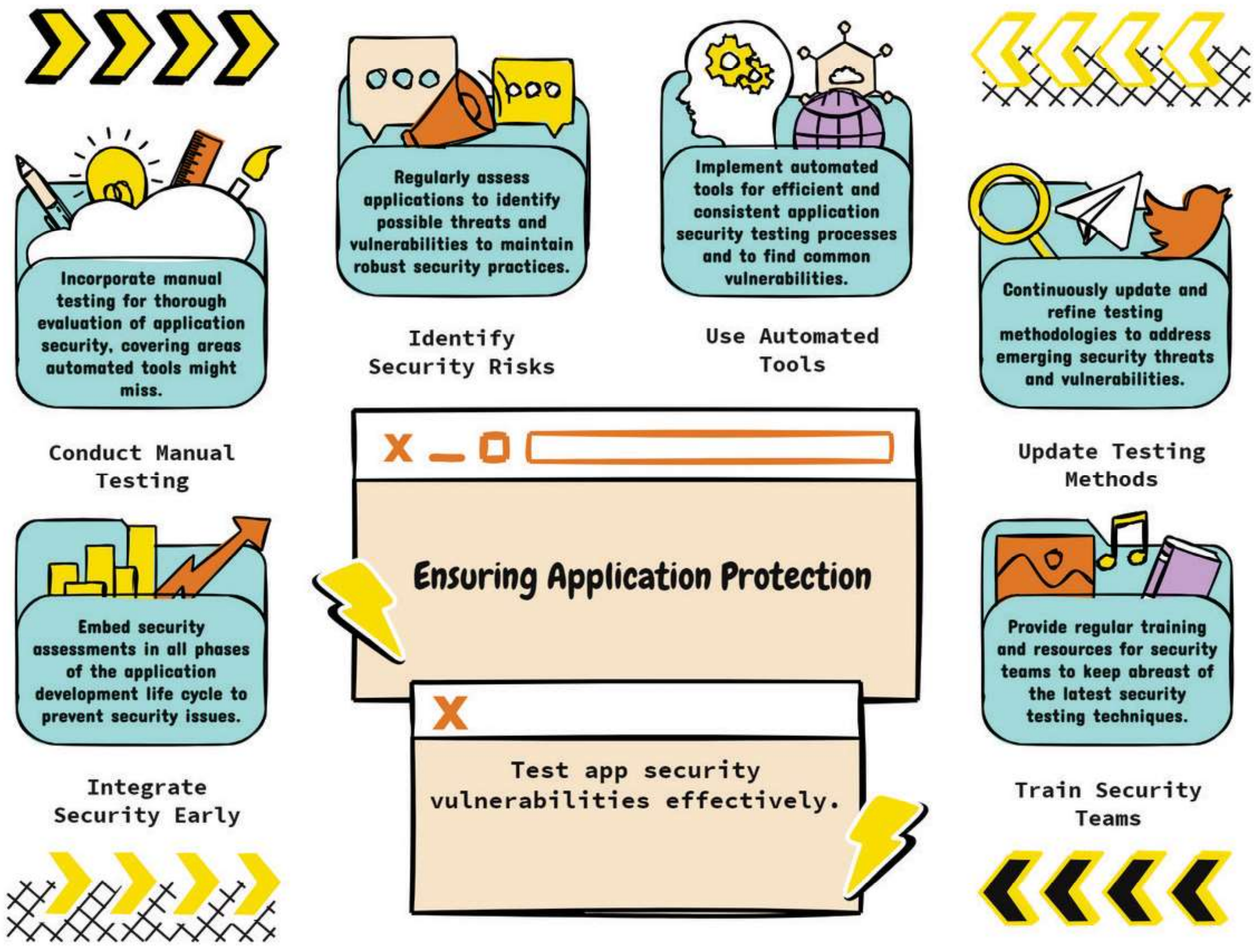
Full knowledge pen test provides insight when an insider is performing malicious activities on the system or network



Application Security testing

- Application Security testing is to validate the internal controls and the information flow within the application. Application Programming Interfaces (APIs)s are also authorized. Many attack scenarios are tested, approved, and documented.

ACE TIPS: Secure session management involves maintaining user state throughout interactions without exposing session IDs. A secure system uses tokens or cookies while implementing best practices like expiration and renewal, preventing unauthorized session hijacking attempts, and maintaining user privacy..


Ensuring Application Protection
Test app security vulnerabilities effectively.
Incorporate manual testing for thorough evaluation of application security, covering areas automated tools might miss.
Conduct Manual Testing
Regularly assess applications to identify possible threats and vulnerabilities to maintain robust security practices.
Identify Security Risks
Implement automated tools for efficient and consistent application security testing processes and to find common vulnerabilities.
Use Automated Tools
Continuously update and refine testing methodologies to address emerging security threats and vulnerabilities.
Update Testing Methods
Embed security assessments in all phases of the application development life cycle to prevent security issues.
Integrate Security Early
Provide regular training and resources for security teams to keep abreast of the latest security testing techniques.
Train Security Teams

ACE TIPS: Pen test should be approved by the stakeholders and should not impact production.

ACE TIPS: Discovery / Reconnaissance is the longest stage in the pen test process.

Topic: 25 Social Engineering attack

- Social Engineering is the most common form of attack. It's a non-technical attack where human interaction and intervention are required. Security awareness training is the MOST critical control for these kinds of attacks.
- List of different social engineering attacks:
  - **Pretexting attack** - Pretexting is a targeted social engineering-based attack in which attackers use continuous conversation to establish a sense of trust with the victim. By creating false

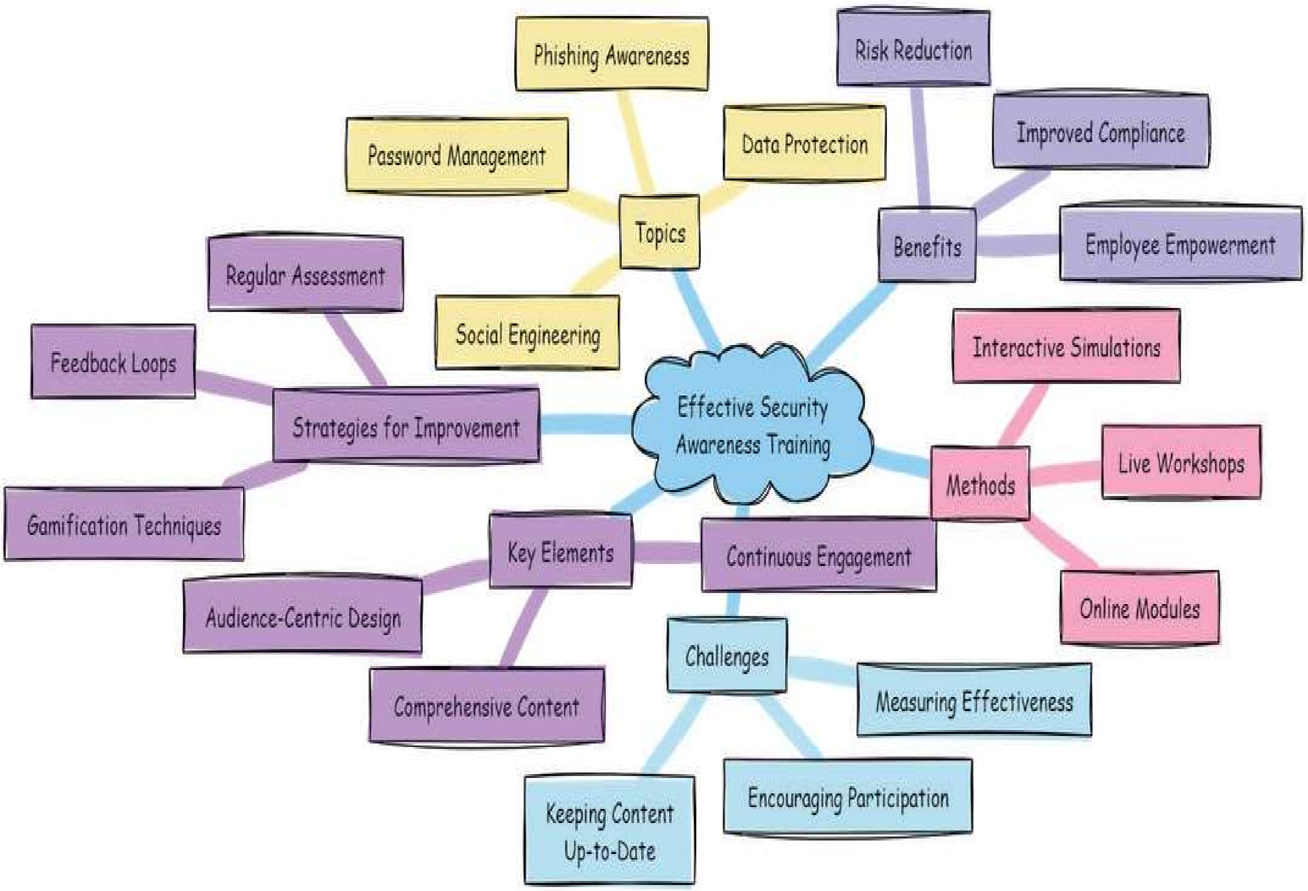
scenarios and acting as a senior employee, a senior member, or a trusted third party, attackers manipulate victims into willingly giving up sensitive information, granting access to systems, or transferring money.

- o **Phishing –** Phishing is the most common form of social engineering. It is generally delivered as an e-mail, chat, web ad, or website designed to impersonate a real system and organization. Phishing messages are designed to deliver a sense of urgency or fear to capture an end user's sensitive data. It may come from a bank, the government, or a significant organization. There are many stages of phishing, such as the user opening a phishing mail, clicking on the hyperlink in the phishing mail, and entering data inside the fake website of the phishing link.
- o Baiting involves offering something to attract an end-user in exchange for login information or confidential data. It can be digital, such as the download of famous games for free.
- o **Piggybacking-** Also known as tailgating. When an unauthorized person physically follows an authorized person into a restricted corporate area or section. One excuse is that they forgot to bring an access or ID card.

52. David saw an unidentified USB drive on his work desktop. The USB was labeled as top-secret documents. Out of curiosity, David plugged that USB drive into his work laptop. This eventually installed a key logger, and his password was compromised. This is an example of

    A. Pretexting attack
    B. Phishing
    C. Baiting
    D. Piggybacking

Correct Option	Wrong Option	Reason
	A	Pretexting is a targeted social engineering-based attack in which attackers use continuous conversation to establish a sense of trust with the victim. By creating a fictitious scenario and posing as a senior employee, member, or a trusted third party, attackers manipulate victims into willingly giving up sensitive information, granting access to systems, or transferring money.
	B	Phishing is the most common form of social engineering. It is generally delivered as an e-mail, chat, web ad, or website designed to impersonate a real system and organization. Phishing messages are crafted to deliver a sense of urgency or fear to capture an end user's sensitive data. A phishing message may come from a bank, the government, or a significant organization.
C		**Option C serves as an illustrative example of Baiting, a tactic where an individual is drawn in by an enticing offer, in this case, a USB drive conspicuously labeled "Top Secret." This type of lure exploits curiosity and the desire for access to classified information, encouraging the unsuspecting victim to connect the device to their computer, potentially leading to malicious software or unauthorized data breaches**
	D	When an unauthorized person physically follows an authorized person into a restricted corporate area or section. One excuse can be that they forgot to bring an ID card.



Key Security Metrics Guide

Track vital security awareness data.

PHISHING SIMULATION RESULTS

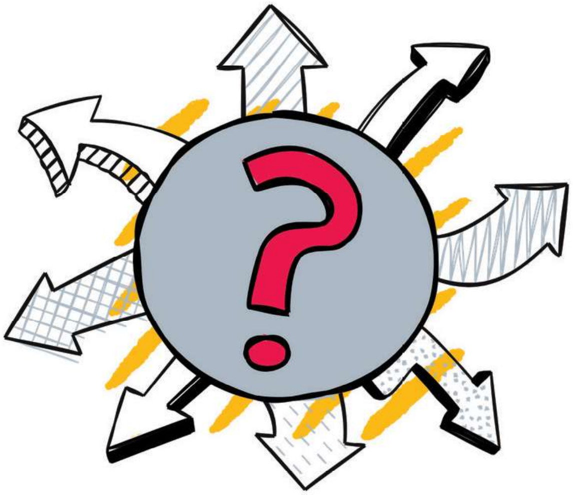
Track employee responses to phishing simulations to gauge awareness and identify areas needing improvement.

POLICY COMPLIANCE

Measure adherence to security policies to assess the effectiveness of training programs.

KNOWLEDGE ASSESSMENT SCORES

Evaluate employees' understanding of security practices through periodic assessments.



INCIDENT REPORTING RATES

High reporting rates indicate awareness. Frequency reveals how often employees recognize and report security issues.

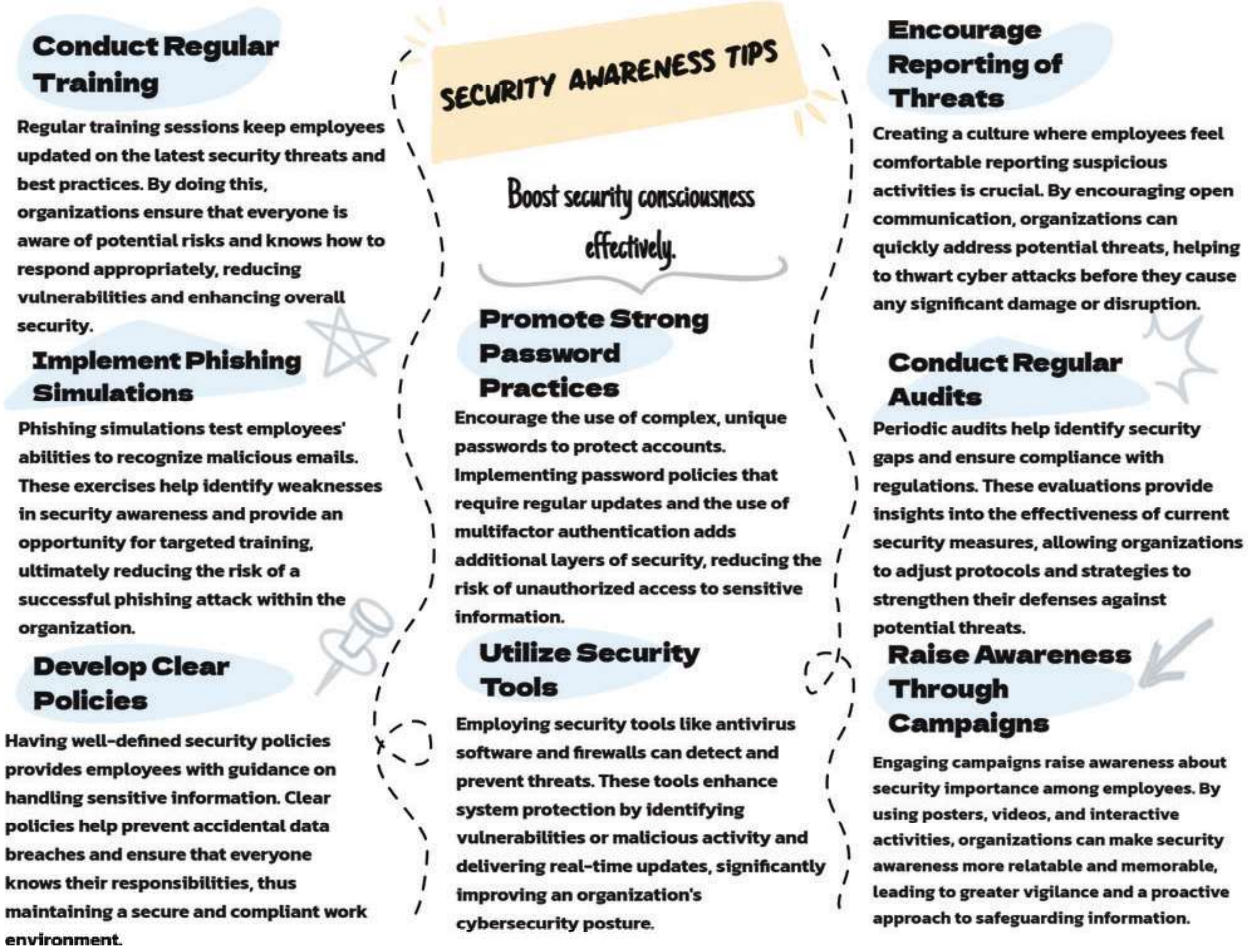
TRAINING COMPLETION RATES

Monitor how many employees complete security training sessions to ensure widespread awareness.

RESPONSE TIME TO THREATS

Track how quickly employees report security threats, indicating the awareness and priority given to security.

ACE TIPS: Metrics allow organizations to track the effectiveness of their security measures over time. By benchmarking performance, they identify improvements or declines in security posture. This continuous monitoring aids in maintaining optimal defense mechanisms and address vulnerabilities promptly, ensuring resilience against evolving threats.



SECURITY AWARENESS TIPS

Boost security consciousness effectively.

Conduct Regular Training

Regular training sessions keep employees updated on the latest security threats and best practices. By doing this, organizations ensure that everyone is aware of potential risks and knows how to respond appropriately, reducing vulnerabilities and enhancing overall security.

Implement Phishing Simulations

Phishing simulations test employees' abilities to recognize malicious emails. These exercises help identify weaknesses in security awareness and provide an opportunity for targeted training, ultimately reducing the risk of a successful phishing attack within the organization.

Develop Clear Policies

Having well-defined security policies provides employees with guidance on handling sensitive information. Clear policies help prevent accidental data breaches and ensure that everyone knows their responsibilities, thus maintaining a secure and compliant work environment.

Promote Strong Password Practices

Encourage the use of complex, unique passwords to protect accounts. Implementing password policies that require regular updates and the use of multifactor authentication adds additional layers of security, reducing the risk of unauthorized access to sensitive information.

Utilize Security Tools

Employing security tools like antivirus software and firewalls can detect and prevent threats. These tools enhance system protection by identifying vulnerabilities or malicious activity and delivering real-time updates, significantly improving an organization's cybersecurity posture.

Encourage Reporting of Threats

Creating a culture where employees feel comfortable reporting suspicious activities is crucial. By encouraging open communication, organizations can quickly address potential threats, helping to thwart cyber attacks before they cause any significant damage or disruption.

Conduct Regular Audits

Periodic audits help identify security gaps and ensure compliance with regulations. These evaluations provide insights into the effectiveness of current security measures, allowing organizations to adjust protocols and strategies to strengthen their defenses against potential threats.

Raise Awareness Through Campaigns

Engaging campaigns raise awareness about security importance among employees. By using posters, videos, and interactive activities, organizations can make security awareness more relatable and memorable, leading to greater vigilance and a proactive approach to safeguarding information.

ACE TIPS: Security metrics communicate risk levels and protection effectiveness to stakeholders. Metrics align stakeholders with security strategies by translating complex security data into understandable insights. This transparency builds trust and ensures everyone is informed and accountable for the organization's security posture.

ACE TIPS: Proper error handling ensures sensitive information isn't leaked to attackers. By customizing error messages and logging errors separately, applications prevent inadvertently sharing application structure details, which could be exploited for further malicious activities or detecting vulnerabilities.