What is Ethical Hacking?

The term 'Hacker' was coined to describe experts who used their skills to re-develop mainframe systems, increasing their efficiency and allowing them to multi-task. Nowadays, the term routinely describes skilled programmers who gain unauthorized access into computer systems by exploiting weaknesses or using bugs, motivated either by malice or mischief. For example, a hacker can create algorithms to crack passwords, penetrate networks, or even disrupt network services.

The primary motive of malicious/unethical hacking involves stealing valuable information or financial gain. However, not all hacking is bad. This brings us to the second type of hacking: Ethical hacking. So what is ethical hacking, and why do we need it? And in this article, you will learn all about what is ethical hacking and more.

What is Ethical Hacking?

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network. Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They can improve the security footprint to withstand attacks better or divert them.

The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying "It takes a thief to catch a thief."

They check for key vulnerabilities include but are not limited to:

- Injection attacks
- Changes in security settings

- Exposure of sensitive data
- Breach in authentication protocols
- Components used in the system or network that may be used as access points

Now, as you have an idea of what is ethical hacking, it's time to learn the type of hackers.

What are the Different Types of Hackers?

The practice of ethical hacking is called "White Hat" hacking, and those who perform it are called White Hat hackers. In contrast to Ethical Hacking, "Black Hat" hacking describes practices involving security violations. The Black Hat hackers use illegal techniques to compromise the system or destroy information.

Unlike White Hat hackers, "Grey Hat" hackers don't ask for permission before getting into your system. But Grey Hats are also different from Black Hats because they don't perform hacking for any personal or third-party benefit. These hackers do not have any malicious intention and hack systems for fun or various other reasons, usually informing the owner about any threats they find. Grey Hat and Black Hat hacking are both illegal as they both constitute an unauthorized system breach, even though the intentions of both types of hackers differ.

White Hat Hacker vs Black Hat Hacker

The best way to differentiate between White Hat and Black Hat hackers is by taking a look at their motives. Black Hat hackers are motivated by malicious intent, manifested by personal gains, profit, or harassment; whereas White Hat hackers seek out and remedy vulnerabilities, so as to prevent Black Hats from taking advantage.

The other ways to draw a distinction between White Hat and Black Hat hackers include:

- **Techniques Used**
  White Hat hackers duplicate the techniques and methods followed by malicious hackers in order to find out the system discrepancies, replicating all the latter's steps to find out how a system attack occurred or may occur. If they find a weak point in the system or network, they report it immediately and fix the flaw.
- **Legality**
  Even though White Hat hacking follows the same techniques and methods as Black Hat hacking, only one is legally acceptable. Black Hat hackers break the law by penetrating systems without consent.

- **Ownership**
  White Hat hackers are employed by organizations to penetrate their systems and detect security issues. Black hat hackers neither own the system nor work for someone who owns it.

After understanding what is ethical hacking, the types of ethical hackers, and knowing the difference between white-hat and black-hat hackers, let's have a look at the ethical hacker roles and responsibilities.

What are the Roles and Responsibilities of an Ethical Hacker?

Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:

- An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network.
- Determine the scope of their assessment and make known their plan to the organization.
- Report any security breaches and vulnerabilities found in the system or network.
- Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.
- Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

Key Benefits of Ethical Hacking

Learning ethical hacking involves studying the mindset and techniques of black hat hackers and testers to learn how to identify and correct vulnerabilities within networks. Studying ethical hacking can be applied by security pros across industries and in a multitude of sectors. This sphere includes network defender, risk management, and quality assurance tester.

However, the most obvious benefit of learning ethical hacking is its potential to inform and improve and defend corporate networks. The primary threat to any organization's security is a hacker: learning, understanding, and implementing how hackers operate can help network defenders prioritize potential risks and learn how to remediate them best. Additionally, getting ethical hacking training or certifications can benefit those who are seeking a new role in the security realm or those wanting to demonstrate skills and quality to their organization.

You understood what is ethical hacking, and the various roles and responsibilities of an ethical hacker, and you must be thinking about what skills you require to become an ethical hacker. So, let's have a look at some of the ethical hacker skills.

Skills Required to Become an Ethical Hacker

An ethical hacker should have in-depth knowledge about all the systems, networks, program codes, security measures, etc. to perform hacking efficiently. Some of these skills include:

- Knowledge of programming - It is required for security professionals working in the field of application security and Software Development Life Cycle (SDLC).
- Scripting knowledge - This is required for professionals dealing with network-based attacks and host-based attacks.
- Networking skills - This skill is important because threats mostly originate from networks. You should know about all of the devices present in the network, how they are connected, and how to identify if they are compromised.
- Understanding of databases - Attacks are mostly targeted at databases. Knowledge of database management systems such as SQL will help you to effectively inspect operations carried out in databases.
- Knowledge of multiple platforms like Windows, Linux, Unix, etc.
- The ability to work with different hacking tools available in the market.
- Knowledge of search engines and servers.

Threats and Attack Vectors

An attack vector is a method of gaining unauthorized access to a network or computer system.

An attack surface is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.

Threat vector can be used interchangeably with attack vector and generally describes the potential ways a hacker can gain access to data or other confidential information.

Why are Attack Vectors Exploited by Attackers?

Cybercriminals can make money from attacking your organization's software systems, such as stealing credit card numbers or online banking credentials. However, there are other more sophisticated ways to monetize their actions that aren't as obvious as stealing money.

Attackers may infect your system with malware that grants remote access to a command and control server. Once they have infected hundreds or even thousands of computers they can establish a botnet, which can be used to send phishing emails, launch other cyber attacks, steal sensitive data, or mine cryptocurrency.

Another common motivation is to gain access to personally identifiable information (PII), healthcare information, and biometrics to commit insurance fraud, credit card fraud or illegally obtain prescription drugs.

Competitors may employ attackers to perform corporate espionage or overload your data centers with a Distributed Denial of Service (DDoS) attack to c`ause downtime, harm sales, and cause customers to leave your business.

Money is not the only motivator. Attackers may want to leak information to the public, embarrass certain organizations, grow political ideologies, or perform cyber warfare on behalf of their government like the United States or China.

How Do Attackers Exploit Attack Vectors?

There are many ways to expose, alter, disable, destroy, steal or gain unauthorized access to computer systems, infrastructure, networks, operating systems, and IoT devices.

In general, attack vectors can be split into passive or active attacks:

Passive Attack Vector Exploits

Passive attack vector exploits are attempts to gain access or make use of information from the system without affecting system resources, such as typosquatting, phishing, and other social engineering-based attacks.

Active Attack Vector Exploits

Active cyber attack vector exploits are attempts to alter a system or affect its operation such as malware, exploiting unpatched vulnerabilities, email spoofing, man-in-the-middle attacks, domain hijacking, and ransomware.

That said, most attack vectors share similarities:

- The attacker identifies a potential target
- The attacker gathers information about the target using social engineering, malware, phishing, OPSEC, and automated vulnerability scanning
- Attackers use the information to identify possible attack vectors and create or use tools to exploit them
- Attackers gain unauthorized access to the system and steal sensitive data or install malicious code
- Attackers monitor the computer or network, steal information, or use computing resources.

One often overlooked attack vector is your third and fourth-party vendors and service providers. It doesn't matter how sophisticated your internal network security and information security policies are — if vendors have access to sensitive data, they are a huge risk to your organization.

This is why it is important to measure and mitigate third-party risks and fourth-party risks. This means it needs to be part of your information security policy and information risk management program.

Consider investing in threat intelligence tools that help automate vendor risk management and automatically monitor your vendor's security posture and notify you if it worsens.

Every organization now needs a third-party risk management framework, vendor management policy, and vendor risk management program.

Before considering a new vendor perform a cybersecurity risk assessment to understand what attack vectors you could be introducing to your organization by using them and ask about their SOC 2 compliance.

What are the Common Types of Attack Vectors?

1. **Compromised Credentials**

Usernames and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams, and malware. When lost, stolen, or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for data exposures and leaked credentials. Password managers, two-factor authentication (2FA), multi-factor authentication (MFA), and biometrics can reduce the risk of leak credentials resulting in a security incident too.

2**. Weak Credentials**

Weak passwords and reused passwords mean one data breach can result in many more. Teach your organization how to create a secure password, invest in a password manager or a single sign-on tool, and educate staff on their benefits.

3. **Insider Threats**

Disgruntled employees or malicious insiders can expose private information or provide information about company-specific vulnerabilities.

4. **Missing or Poor Encryption**

Common data encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks and protect the confidentiality of data being transmitted. Missing or poor encryption for data at rest can mean that sensitive data or credentials are exposed in the event of a data breach or data leak.

5**. Misconfiguration**

Misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure, or AWS, or using default credentials can lead to data breaches and data leaks, check your S3 permissions or someone else will. Automate configuration management where possible to prevent configuration drift.

6**. Ransomware**

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as WannaCry. Minimize the impact of ransomware attacks by maintaining a defense plan, including keeping your systems patched and backing up important data.

7. **Phishing**

Phishing attacks are social engineering attacks where the target is contacted by email, telephone, or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing sensitive data, credentials, or personally identifiable information (PII). Fake messages can send users to malicious websites with viruses or malware payloads.

Learn the different types of phishing attacks here.

8. **Vulnerabilities**

New security vulnerabilities are added to the CVE every day and zero-day vulnerabilities are found just as often. If a developer has not released a patch for a zero-day vulnerability before an attack can exploit it, it can be hard to prevent zero-day attacks.

Learn more about vulnerabilities here.

9. **Brute Force**

Brute force attacks are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works. This could be by attacking weak passwords or encryption, phishing emails, or sending infected email attachments containing a type of malware. Read our full post on brute force attacks.

10. **Distributed Denial of Service (DDoS)**

DDoS attacks are cyber attacks against networked resources like data centers, servers, websites, or web applications and can limit the availability of a computer system. The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.

11. **SQL Injections**

SQL stands for a structured query language, a programming language used to communicate with databases. Many of the servers that store sensitive data use SQL to manage the data in their database. An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't. This is a huge cyber risk if the database stores customer information, credit card numbers, credentials, or other personally identifiable information (PII).

12**. Trojans**

Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread via infected email attachments or fake malicious software.

13**. Cross-Site Scripting** (XSS)

XSS attacks involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors. A common way attackers can deploy cross-site scripting attacks is by injecting malicious code into a comment e.g. embedding a link to malicious JavaScript in a blog post's comment section.

14. **Session Hijacking**

When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.

15. **Man-in-the-Middle Attacks**

Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.

16. **Third and Fourth-Party Vendors**

The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your customer's data and your proprietary data. Some of the biggest data breaches were caused by third parties.

Information Assurance Model in Cyber Security

Information Assurance concerns implementation of methods that focused on protecting and safeguarding critical information and relevant information systems by assuring confidentiality, integrity, availability, and non-repudiation. It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

Information Assurance Model :

The security model is multidimensional model based on four dimensions :

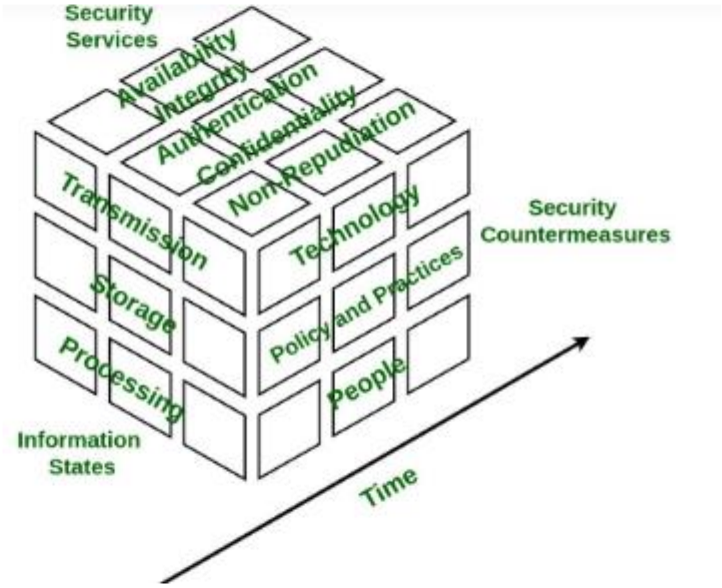
Information States –

Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

1. **Security Services –**
   It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

2. **Security Countermeasures –**
   This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

3. **Time –**
   This dimension can be viewed in many ways. At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized access.



InformationStates :

1. **Transmission –**
   It defines time wherein data is between processing steps.
   Example :
   In transit over networks when user sends email to reader, including memory and storage encountered during delivery.

2. **Storage –**
   It defines time during which data is saved on medium such as hard drive.Example: Saving document on file server's disk by user.

3. **Processing –**
   It defines time during which data is in processing state.
   Example :
   Data is processed in random access memory (RAM) of workstation.

Security Services :

1. **Confidentiality** –
   It assures that information of system is not disclosed to unauthorized access and is read and interpreted only by persons authorized to do so. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as **sensitive information**.
   To ensure confidentiality data is categorized into different categories according to damage severity and then accordingly strict measures are taken.

1. **Example:**

   Protecting email content to read by only desired set of users. This can be insured by data encryption. Two-factor authentication, strong passwords, security tokens, and biometric verification are some popular norms for authentication users to access sensitive data.

   Integrity–

   It ensures that sensitive data is accurate and trustworthy and can not be created, changed, or deleted without proper authorization. Maintaining integrity involves modification or destruction of information by unauthorized access.

   To ensure integrity backups should be planned and implemented in order to restore any affected data in case of security breach. Besides this cryptographic checksum can also be used for verification of data.

   Example:

   Implementation of measures to verify that e-mail content was not modified in transit. This can be achieved by using cryptography which will ensure that intended user receives correct and accurate information.

2. **Availability–**

   It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.

   To ensure availability of corrupted data must be eliminated, recovery time must be speed up and physical infrastructure must be improved.

   Example:

   Accessing and throughput of e-mail service.

3. **Authentication–**

   It is security service that is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.

   To ensure availability of various single factors and multi-factor authentication methods are used. A single factor authentication method uses single parameter to verify users' identity whereas two-factor authentication uses multiple factors to verify user's identity.

   Example:

   Entering username and password when we log in to website is example of authentication. Entering correct login information lets website verify our identity and ensures that only we access sensitive information.

4. **Non-Repudiation–**
   It is mechanism to ensure sender or receiver cannot deny fact that they are part of data transmission. When sender sends data to receiver, it receives delivery confirmation. When receiver receives message it has all information attached within message regarding sender.
   Example:
   A common example is sending SMS from one mobile phone to another. After message is received confirmation message is displayed that receiver has received message. In return, message received by receiver contains all information about sender.

SecurityCountermeasures:

1. **People–**
   People are heart of information system. Administrators and users of information systems must follow policies and practice for designing good system. They must be informed regularly regarding information system and ready to act appropriately to safeguard system.

2. **Policy&Practice–**
   Every organization has some set of rules defined in form of policies that must be followed by every individual working in organization. These policies must be practiced in order to properly handle sensitive information whenever system gets compromised.

3. **Technology–**
   Appropriate technology such as firewalls, routers, and intrusion detection must be used in order to defend system from vulnerabilities, threats. The technology used must facilitate quick response whenever information security gets compromised.

What is threat modeling?

Threat modeling is a proactive strategy for evaluating cybersecurity threats. It involves identifying potential threats, and developing tests or procedures to detect and respond to those threats. This involves understanding how threats may impact systems, classifying threats and applying the appropriate countermeasures.

A typical threat modeling process includes five steps: threat intelligence, asset identification, mitigation capabilities, risk assessment, and threat mapping.

Each of these provides different insights and visibility into your security posture.

There are eight main methodologies you can use while threat modeling: STRIDE, PASTA, VAST, Trike, CVSS, Attack Trees, Security Cards, and hTMM. Each of these methodologies provides a different way to assess the threats facing your IT assets.

Advantages of threat modeling

Threat modeling has the following key advantages:

- **Helps prioritize threats**, ensuring that resources and attention are distributed effectively. This prioritization can be applied during planning, design, and implementation of security to ensure that solutions are as effective as possible.
- **Ensures defenses are in line with evolving threats**. If not, new threats may remain undefended, leaving systems and data vulnerable.
- **Helps teams adopt or develop new tools** or create software. It helps teams understand how tools and applications may be vulnerable in comparison to what protections are offered.
- **Helps development teams prioritize fixes** to existing software, according to the severity and impact of anticipated threats.

What are the five main steps in the threat modeling process?

When performing threat modeling, several processes and aspects should be included. Failing to include one of these components can lead to incomplete models and can prevent threats from being properly addressed.

1. Apply threat intelligence

This area includes information about types of threats, affected systems, detection mechanisms, tools and processes used to exploit vulnerabilities, and motivations of attackers.

Threat intelligence information is often collected by security researchers and made accessible through public databases, proprietary solutions, or security communications outlets. It is used to enrich the understanding of possible threats and to inform responses.

2. Identify assets

Teams need a real-time inventory of components, credentials, and data in use, where those assets are located, and what security measures are in use. This inventory helps security teams track assets with known vulnerabilities.

A real-time inventory enables security teams to gain visibility into asset changes. For example, getting alerts when assets are added with or without authorized permission, which can potentially signal a threat.

3. Identify mitigation capabilities

Mitigation capabilities generally refer to technology to protect, detect, and respond to a certain type of threat, but can also refer to an organization’s security expertise and abilities, and their processes. Assessing your existing capabilities will help you determine whether you need to add additional resources to mitigate a threat.

For example, if you have enterprise-grade antivirus, you have an initial level of protection against traditional malware threats. You can then determine if you should invest further, for example, to correlate your existing AV signals with other detection capabilities.

4. Assess risks

Risk assessments correlate threat intelligence with asset inventories and current vulnerability profiles. These tools are necessary for teams to understand the current status of their systems and to develop a plan for addressing vulnerabilities.

Risk assessments can also involve active testing of systems and solutions. For example, penetration testing to verify security measures and patching levels are effective.

5. Perform threat mapping

Threat mapping is a process that follows the potential path of threats through your systems. It is used to model how attackers might move from resource to resource and helps teams anticipate where defenses can be more effectively layered or applied.

Top threat modeling methodologies and techniques

When performing threat modeling, there are multiple methodologies you can use. The right model for your needs depends on what types of threats you are trying to model and for what purpose.

STRIDE threat modeling

STRIDE is a threat model, created by Microsoft engineers, which is meant to guide the discovery of threats in a system. It is used along with a model of the target system. This makes it most effective for evaluating individual systems.

STRIDE is an acronym for the types of threats it covers, which are:

- **Spoofing** — a user or program pretends to be another
- **Tampering** — attackers modify components or code
- **Repudiation** — threat events are not logged or monitored
- **Information disclosure** — data is leaked or exposed
- **Denial of service (DoS)** — services or components are overloaded with traffic to prevent legitimate use
- **Elevation of Privilege** — attackers grant themselves additional privileges to gain greater control over a system

Process for Attack Simulation and Threat Analysis (PASTA)

PASTA is an attacker-centric methodology with seven steps. It is designed to correlate business objectives with technical requirements. PASTA’s steps guide teams to dynamically identify, count, and prioritize threats.

The steps of a PASTA threat model are:

1. Define business objectives
2. Define the technical scope of assets and components

3. Application decomposition and identify application controls
4. Threat analysis based on threat intelligence
5. Vulnerability detection
6. Attack enumeration and modeling
7. Risk analysis and development of countermeasures

Common Vulnerability Scoring System (CVSS)

CVSS is a standardized threat scoring system used for known vulnerabilities. It was developed by the National Institute of Standards and Technology (NIST) and maintained by the Forum of Incident Response and Security Teams (FIRST).

This system is designed to help security teams assess threats, identify impacts, and identify existing countermeasures. It also helps security professionals assess and apply threat intelligence developed by others in a reliable way.

CVSS accounts for the inherent properties of a threat and the impacts of the risk factor due to time since the vulnerability was first discovered. It also includes measures that allow security teams to specifically modify risk scores based on individual system configurations.

Visual, Agile, and Simple Threat (VAST)

Visual, Agile, and Simple Threat (VAST) is an automated threat modeling method built on the ThreatModeler platform. Large enterprises implement VAST across their entire infrastructure to generate reliable, actionable results and maintain scalability.

VAST can integrate into the DevOps lifecycle and help teams identify various infrastructural and operational concerns. Implementing VAST requires the creation of two types of threat models:

- **Application threat model** — uses a process-flow diagram to represent the architectural aspect of the threat
- **Operational threat model** — uses a data-flow diagram to represent the threat from the attacker’s perspective

Trike

Trike is a security audit framework for managing risk and defense through threat modeling techniques. Trike defines a system, and an analyst enumerates the system's assets, actors, rules, and actions to build a requirement model. Trike generates a step matrix with columns representing the assets and rows representing the actors. Every matrix cell has four parts to match possible actions (create, read, update, and delete) and a rule tree — the analyst specifies whether an action is allowed, disallowed, or allowed with rules.

Trike builds a data-flow diagram mapping each element to the appropriate assets and actors with the requirements defined. The analyst uses the diagram to identify denial of service (DoS) and privilege escalation threats.

Trike assesses attack risks using a five-point probability scale for each CRUD action and actor. It also evaluates actors based on their permission level for each action (always, sometimes, or never).

Attack Trees

Attack trees are charts that display the paths that attacks can take in a system. These charts display attack goals as a root with possible paths as branches. When creating trees for threat modeling, multiple trees are created for a single system, one for each attacker goal.

This is one of the oldest and most widely used threat modeling techniques. While once used alone, it is now frequently combined with other methodologies, including PASTA, CVSS, and STRIDE.

Security Cards

The Security Cards methodology is based on brainstorming and creative thinking rather than structured threat modeling approaches. It is designed to help security teams account for less common or novel attacks. This methodology is also a good way for security teams to increase knowledge about threats and threat modeling practices.

The methodology uses a set of 42 cards, which help analysts answer questions about future attacks, such as who might attack, what their motivation could be, which systems they might attack, and how they would implement an attack. Analysts can deal the cards in a type of table-top game, to simulate possible attacks and consider how the organization might respond.

Hybrid Threat Modeling Method (hTMM)

hTMM is a methodology developed by Security Equipment Inc. (SEI) that combines two other methodologies:

- **Security Quality Requirements Engineering (SQUARE)** — a methodology designed to elicit, categorize and prioritize security requirements
- **Persona non Grata (PnG)** — a methodology that focuses on uncovering ways a system can be abused to meet an attacker's goals

hTMM is designed to enable threat modeling which accounts for all possible threats, produces zero false positives, provides consistent results, and is cost-effective.

It works by applying Security Cards, eliminating unlikely PnGs, summarizing results, and formally assessing risk using SQUARE.

Threat modeling with Exabeam's Next-generation SIEM platform

Threat modeling is a complex process that requires real-time data collection and analysis, as well as a quick (if not real-time) response.

Next-generation SIEM platforms, like Exabeam's Security Management Platform, can help you effectively create, manage, maintain, and automate the threat modeling process of your choice.

Exabeam offers the following modules that you can use to perform threat modeling:

- **Advanced analytics** — using behavioral analytics to identify anomalous behavior that might indicate an attack, and correlating with threat analytics data to identify the type and source of the attack
- **Smart forensic analysis** — collecting all relevant information about a security incident, across multiple users, IP addresses, and IT systems,

combining it with threat intelligence data, and laying it out on an incident timeline

- **Incident response automation** — gathering data from hundreds of tools, automatically identifying incidents, referencing them with threat intelligence data, and even automatically orchestrating containment and mitigation steps
- **Threat hunting** — using threat intelligence data, combined with free exploration of internal security data, to identify new and unknown threats that might be affecting your organization

Exabeam Threat Hunter is especially helpful during the threat modeling process. It helps analysts outsmart attackers by simplifying threat detection. Here's what you can do with Exabeam Threat Hunter:

- **Easy to use interface** — Point-and-click interface makes it simple to query data.
- **Context-aware data** — enables complex searches
- **Automatic incident timelines** — Automation makes gathering evidence simpler and faster than maintaining logs.
- **Provides visual aid** — represents relationships, revealing hidden correlations between data

In addition to these tools, Exabeam also offers a Threat Intelligence Service, which provides a cloud-based solution with proprietary threat intelligence technology. This system collects and analyzes threat indicators from multiple feeds.

The Threat Intelligence Service is free for Exabeam customers as part of the Exabeam Security Management Platform, and can also integrate with TIP vendors for a broader source of IOCs.

Introduction to penetration test

It is commonly known as pen test or pentest in ethical hacking. It is a form of a cyberattack that is basically done to check what is the situation of the security of a system. Often people confuse this penetration test or pen test with the vulnerability assessment test.

Software testing is the process of evaluating a software application or system to ensure it meets specified requirements and to identify any defects. It can be done manually or using automated tools.

Penetration testing, also known as “pen testing,” is a simulated cyber attack on a computer system, network, or web application to evaluate the security of the system. The goal of penetration testing is to identify vulnerabilities that an attacker could exploit and to provide recommendations for mitigating those vulnerabilities.

History of the Penetration test

In 1965 security concerns rose, because many thought that communication lines can be penetrated and the attacker/hacker might be able to get the data that is being exchanged between one person to another person. In an annual joint conference of 1967 various computer experts stated this point that communication lines can be penetrated. The idea of penetration testing came into mind when a corporation found a major threat to internet communications. This is what lead many organizations to assign a team who would try to find the vulnerability in computer networks or systems which will lead to the protection from any unauthorized access.

The concept of penetration testing has its roots in the early days of computer security. In the 1960s and 1970s, the United States government and military began to recognize the need for security testing of their computer systems. Early penetration testing techniques were primarily focused on identifying vulnerabilities in individual systems, rather than entire networks.

In the 1980s, the rise of personal computers and the internet led to an increased need for network security testing. This prompted the development of more sophisticated penetration testing tools and techniques, as well as the creation of the first commercial penetration testing services.

In the 1990s, the field of penetration testing continued to evolve, with a greater focus on automated testing and the use of commercial tools. The growth of e-commerce and the increasing reliance on the internet for business led to a greater need for web application security testing.

Today, penetration testing is an integral part of cybersecurity, with organizations of all sizes and in all industries conducting regular testing to identify and mitigate vulnerabilities in their systems. The penetration testing process is continuously evolving to adapt to new technologies and threat scenarios.

What is a penetration test?

It is a form of cyberattack done to understand the situation of the security of the system. People often confuse this test with the vulnerability assessment test. So penetration test is composed of some methods or instructions whose main aim is to test the organization’s security. This test much proved to be helpful for the organizations because it helps to find the vulnerabilities and check if the attacker /hacker will be able to exploit and be capable of enough of gaining unauthorized access.

A penetration test, also known as a “pen test,” is a simulated cyber attack on a computer system, network, or web application. The purpose of a penetration test is to identify vulnerabilities in the system that an attacker could exploit, and to evaluate the effectiveness of the system’s security controls.

During a penetration test, a team of security professionals, called “white hat” or “ethical hackers,” attempt to gain unauthorized access to the system, just like a real attacker would. They use a variety of techniques, including network scanning, social engineering, and exploit development, to identify vulnerabilities and find ways to bypass security controls.

Once the test is complete, the team will provide a report detailing their findings and recommendations for mitigating the identified vulnerabilities. The goal of a penetration test is not to cause harm to the system, but to identify and help fix security weaknesses before they can be exploited by malicious actors.

It is important to note that there are different types of penetration testing, such as External Penetration testing, Internal Penetration testing, and Web application penetration testing. Each of them has its own scope, methodology, and objectives.

Difference between vulnerability Assessment and penetration test

Vulnerability Assessment:- This test should not be confused with the penetration test. The main aim of the penetration is to find the vulnerability in an asset and document them in an organized manner.

Penetration test:- This test is basically done to see the attacker/hacker can exploit the vulnerabilities or not. If the exploit is possible then those vulnerabilities are documented.

Penetration Testing Process:

The penetration testing process includes five phases:

Reconnaissance:

This phase is also known as the **planning phase.** In this phase, important information about the target system is gathered.
Reconnaissance is the first phase of the penetration testing process. It involves gathering information about the target system or network in order to identify potential vulnerabilities and attack vectors.

During the reconnaissance phase, the penetration tester will gather information from a variety of sources, including:

Publicly available information, such as company websites, social media accounts, and domain name registration records
Network scanning tools, which can be used to identify live hosts, open ports, and running services
Vulnerability scanning tools, which can be used to identify known vulnerabilities in the system
OSINT (Open-Source Intelligence) techniques, which can be used to gather information from various sources such as Google, social media, and other public domains.
The goal of reconnaissance is to gather as much information as possible about the target system or network, in order to identify potential weaknesses that can be exploited during the later phases of the penetration test.

It is a crucial step of the penetration testing process as it allows the testers to understand the target system environment and to define the scope of the test.

Scanning:

In this phase, different scanning tools are used to determine the response of the system towards an attack. Vulnerabilities of the system are also checked. Scanning is the second phase of the penetration testing process, following reconnaissance. It involves using automated tools to actively probe the target system or network in order to identify live hosts, open ports, and running services.

During the scanning phase, the penetration tester will use a variety of tools to perform different types of scans, such as:

Port scans: which identify open ports on live hosts, and the services running on those ports.
Vulnerability scans: which search for known vulnerabilities in the system based on the version and configuration of the software running on the open ports.
Network mapping: which creates a visual representation of the target network, including the hosts, devices and services.
Scanning can be done internally or externally, depending on the scope of the test and the objectives of the organization.

It is an important phase of the penetration testing process as it allows the testers to identify the attack surface of the target system, and to identify potential vulnerabilities that can be exploited during the next phase of the test.

It is important to note that the results of the scan may not necessarily be accurate and should be verified by a human tester in order to avoid false positives.

Gaining Access:

In this phase using the data gathered in the planning and scanning phases, a payload is used to exploit the targeted system.

Gaining access is the third phase of the penetration testing process, following reconnaissance and scanning. In this phase, the penetration tester will attempt to exploit the vulnerabilities identified in the previous phases to gain unauthorized access to the target system or network.

During the gaining access phase, the penetration tester will use a variety of techniques, such as:

Exploiting software vulnerabilities: using known exploits to gain access to a system or network.
Social engineering: tricking employees or users into revealing login credentials or other sensitive information.
Password cracking: using automated tools to guess or crack passwords.
The goal of this phase is to gain access to the system, and to establish a foothold from which the penetration tester can move laterally through the network.

It is an important phase of the penetration testing process as it allows the testers to assess the real impact of the identified vulnerabilities and to evaluate the effectiveness of the security controls in place.

It is important to note that gaining access should be done in a controlled environment, with proper permissions and guidelines, and not to cause any harm to the system or data.

Maintaining Access:

This phase requires taking the steps involved in being able to be continuously within the target environment to collect as much data as possible.
Maintaining access is the fourth phase of the penetration testing process, following reconnaissance, scanning and gaining access. In this phase, the penetration tester will focus

on maintaining their access to the target system or network and expanding their control over it.

During the maintaining access phase, the penetration tester will use a variety of techniques, such as:

Establishing backdoors: creating a way to regain access to the system in case the initial access is closed.
Privilege escalation: increasing their level of access to the system, from a low-privilege user to an administrator or root user.
Persistence: maintaining the access to the system over time by creating a way to bypass security controls.
Lateral movement: moving through the network to gain access to other systems and resources.
The goal of this phase is to maintain access to the system or network for as long as possible and to expand the scope of the attack.

It is an important phase of the penetration testing process as it allows the testers to assess the impact of a successful attack and to evaluate the effectiveness of the security controls in preventing or detecting a prolonged unauthorized access.

It is important to note that maintaining access should be done in a controlled environment, with proper permissions and guidelines, and not to cause any harm to the system or data.

Be hidden from the user

This is the moment where the attacker will have to clear the trace of any activity done in the target system. It is done in order to remain hidden from the user/victim.In the final phase of a penetration test, the tester will focus on being hidden from the user. This phase is also known as “covering tracks.” The goal of this phase is to make it as difficult as possible for the system administrator or security team to detect the tester’s presence and activities on the system.

During the covering tracks phase, the penetration tester will use a variety of techniques to hide their presence, such as:

Clearing logs: deleting or modifying system logs to remove any evidence of the tester’s activities
Hiding files: using techniques such as rootkits or hidden directories to conceal files and tools used during the test
Disabling security controls: disabling or circumventing security controls such as firewalls, intrusion detection systems, and antivirus software to evade detection.
It is an important phase of the penetration testing process as it allows the testers to assess the ability of the system to detect and prevent a prolonged unauthorized access and to evaluate the incident response plan of the organization.

It is important to note that covering tracks should be done in a controlled environment, with proper permissions and guidelines, and not to cause any harm to the system or data. Also, it is important that the tester leaves the system in its initial state after the test.

Rules in penetration testing

There are rules that have to be followed when conducting the penetration test like the methodology that should be used, the start and the end dates, the goals of the penetration test, and more. To make the penetration test possible, there should be a mutual agreement between both the customer and the representative. These are some of the things which are commonly present in rules which are as follows:-

1. There will be a non-disclosure agreement where there will be written permission to hack. This non-disclosure agreement will have to be signed by both parties.
2. There should be a start and end date for penetration testing.
3. What methodology should be used for conducting the penetration test?
4. There should be the goals of the penetration test.

Types of Penetration Testing Methodologies-

1. Black Box penetration testing
2. Grey Box Penetration testing
3. White Box Penetration testing

Black Box Penetration Testing:- In this Method attacker is has no knowledge about the target as it exactly simulates an actual cyber attack where an actual black hat hacker attacks. This testing takes time as the attacker has no knowledge about the system so he gathers them. This method is used to find existing vulnerabilities in the system and used to simulate how far a hacker can go into the system without any info about the system.

Grey Box Penetration Testing:- In this method, the attacker is provided with a bit more information about the target like network configurations, subnets, or a specific IP to test, Attacker has a basic idea of how the machine is to which he/she is going to perform an attack, they may also be provided with low-level login credentials or access to the system which helps them in having a clear approach, This saves time of Reconnaissance the target.

White Box Penetration Testing:- We can say that in this testing method attackers have developer-level knowledge about the system which also includes an assessment of source code, Ethical hackers have full access to the system more in-depth than black box testing. It is used to find out potential threats to the system due to bad programming, misconfigurations, or lack of any defensive measures.

Types of the Penetration test

1. Social Engineering Penetration test:- This test can also be considered as a part of the Network Penetration Test. In this case, an organization might ask the penetration tester to attack its users. This is the moment where the penetration tester eligible to use the speared phishing attack and more to trick the user to do unthinkable.
2. Physical penetration test:- In this case, the penetration tester will be asked to check the physical security controls of the building like locks and RFID mechanisms.
3. Network penetration test:- in this case, the penetration tester will have to test the network environment for potential security vulnerabilities and threats.
4. Web Application penetration test:- This test is nowadays considered to be common as application hosts data’s which can be considered as critical as it can be. The data can be like the username, passwords, or more.
5. Mobile Application penetration test:- This test is done because every organization nowadays used Android or Ios mobile-based applications. So the goal is to make their mobile applications are secured and to make it reliable for the customer to provide personal information when they are using any applications.

Advantages of the Penetration test

- The penetration test can be done to find the vulnerability which may serve as a weakness for the system.
- It is also done to identify the risks from the vulnerabilities.
- It can help determine the impact of an attack and the likelihood of it happening.
- It can help assess the effectiveness of security controls.
- It can help prioritize remediation efforts.

- It can provide assurance that the system is secure.
- It can be used to test the security of any system, no matter how large or small.
- It can be used to find vulnerabilities in systems that have not yet been exploited.
- It can be used to assess the effectiveness of security controls in place.
- It can be used to educate employees about security risks.

Disadvantages of the Penetration test

- The penetration test which is not done properly can expose data that might be sensitive and more.
- The penetration tester has to be trusted, otherwise, the security measures taken can backfire.
- It is difficult to find a qualified penetration tester.
- Penetration testing is expensive.
- It can be disruptive to business operations.
- It may not identify all security vulnerabilities.
- It may give false positives (incorrectly identifying a vulnerability).
- It may give false negatives (failing to identify a vulnerability).
- It may require specialized skills and knowledge.
- The results may be difficult to interpret.
- After the penetration test is completed, the system is vulnerable to attack.

Penetration Testing Tools

1. **Nmap:** It is a network exploration tool and security scanner. It can be used to identify hosts and services on a network, as well as security issues.
2. **Nessus:** It is a vulnerability scanner. It can be used to find vulnerabilities in systems and applications.
3. **Wireshark:** It is a packet analyzer. It can be used to capture and analyze network traffic.
4. **Burp Suite:** It is a web application security testing tool. It can be used to find security issues in web applications.

1. Penetration Testing :

Penetration testing is done for finding vulnerabilities, malicious content, flaws, and risks. It is done to build up the organization's security system to defend the IT infrastructure. Penetration testing is also known as pen testing. It is an official procedure that can be deemed helpful and not a harmful attempts. It is part of an ethical hacking process where it specifically focuses only on penetrating the information system.

2. Vulnerability Assessments :

Vulnerability assessment is the technique of finding and measuring security vulnerabilities (scanning) in a given environment. It is an all-embracing assessment of the information security position (result analysis). It is used to identifies the potential weaknesses and provides the proper mitigation measures to either remove those weaknesses or reduce below the risk level.

Differences between Penetration Testing and Vulnerability Assessments :

S.No.	Penetration Testing	Vulnerability Assessments
1.	This is meant for critical real-time systems.	This is meant for non-critical systems.

2.	This is ideal for physical environments and network architecture.	This is ideal for lab environments.
3.	It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
4.	It cleans up the system and gives final report.	It attempt to mitigate or eliminate the potential vulnerabilities of valuable resources.
5.	It gathers targeted information and/or inspect the system.	It allocates quantifiable value and significance to the available resources.
6.	It tests sensitive data collection.	It discovers the potential threats to each resource.
7.	It determines the scope of an attack.	It makes a directory of assets and resources in a given system.
8.	The main focus is to discovers unknown and exploitable weaknesses in normal business processes.	The main focus is to lists known software vulnerabilities that could be exploited.
9.	It is a simulated cyberattack carried out by experienced ethical hackers in a well-defined and controlled environment.	It is an automated assessment performed with the help of automated tools.
10.	This is a goal-oriented procedure that should be carried out in a controlled manner.	This cost-effective assessment method is often considered safe to perform.
11.	It only identifies the exploitable security vulnerabilities.	It identifies, categorizes, and quantifies security vulnerabilities.