Chapter 01: Introduction to Ethical Hacking

Introduction

Attackers infiltrate systems for a variety of motives and objectives. It is crucial to understand how malicious hackers exploit systems and the underlying reasons for their attacks. As Sun Tzu aptly states in *The Art of War*, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." To effectively protect their infrastructure, system administrators and security professionals must understand the tactics and intentions of malicious hackers who aim to misuse the same systems for unlawful purposes.

By the end of this chapter, you will be able to:

- Identify the key components of information security
- Explain information security attacks and the concept of information warfare
- Define hacking concepts and categorize hacker types
- Discuss ethical hacking concepts, including AI-driven ethical hacking
- Outline various hacking methodologies and frameworks
- Explore information security controls such as information assurance, defense-in-depth, risk management, cyber threat intelligence, threat modeling, the incident management process, and the role of AI/ML
- Understand key information security acts and laws

Information Security Overview

System security consists of methods and processes used for protecting information and information systems from unauthorized access, disclosure, usage, or modification. Information security ensures the confidentiality, integrity, and availability of information. If an organization lacks security policies and appropriate security rules, its confidential information and data will not be secure, putting the organization at great risk. Well-defined security policies and procedures help protect an organization's assets from unauthorized access and disclosures.

Millions of users interact with each other every minute in the modern world with the help of the latest technologies and platforms. These sixty seconds can be very vulnerable and costly to private and public organizations due to the presence of various types of old and modern threats present worldwide. The public internet is the most common and rapid option for spreading threats worldwide. Malicious Codes and Scripts, Viruses, Spam, and Malware are constantly waiting to be accessed. This is why security risks to a network or a system can never be eliminated. Implementing a security policy that is effective and efficient, rather than consisting of unnecessary security implementations that can result in a waste of resources and create loopholes for threats, is a continual challenge.

It is necessary to understand some essential cyber security terminology. These terminologies will help in understanding information security concepts.

- **Hack Value** refers to the attractiveness, interest, or thing of worth to the hacker. The value describes the target's level of attractiveness to the hacker.

- **Zero-Day Attack** refers to threats and vulnerabilities that can be used to exploit the victim before the developer identifies or addresses them and releases a patch for them.
- **Vulnerability** refers to a weak point or loophole in any system or network that can be helpful and utilized by attackers to hack into the system. Any vulnerability can be an entry point from which they can reach their target.
- **Daisy Chaining** is a sequence of hacking or attacking attempts to gain access to a network or system, one after another, using the same information and the information obtained from the previous attempt.
- **Exploit** is a system security breach through vulnerabilities, Zero-Day Attacks, or any other hacking technique.
- **Doxing** means publishing information, or a set of information, associated with an individual. This information is collected from publicly available databases, mostly social media and similar sources.
- **Payload** refers to the actual section of information or data in a frame as opposed to automatically generated metadata. In information security, a payload is a section or part of a malicious and exploited code that causes potentially harmful activities and actions such as exploiting, opening backdoors, and hijacking.

A **Bot** is software that controls the target remotely and executes predefined tasks. It is capable of running automated scripts over the internet. Bots are also known as Internet Bots or Web Robots. These Bots can be used for social purposes, for example, chatterbots and live chats. Furthermore, they can also be used for malicious purposes in the form of malware. Hackers use Malware bots to gain complete authority over a computer.

Data Breaches

eBay Data Breach

One famous example demonstrating the need for corporate information and network security is the data breach that occurred at eBay. eBay is a well-known online auction platform that is widely used all over the world.

In 2014, eBay reported a massive data breach. According to eBay, the sensitive data of 145 million customers was compromised in this attack. The data included the following:

- Customers' names
- Encrypted passwords
- Email addresses
- Postal addresses
- Contact numbers
- Dates of birth

Information such as that listed above must always be stored in an encrypted form rather than in plain text, and it must use strong encryption. eBay claims that no information related to security numbers such as credit cards was compromised because its database containing financial information is kept in a separate and encrypted format. However, identity and password thefts can also result in severe risks.

Hackers carried out the eBay data breach by compromising a small number of employees' credentials through phishing between February and March 2014. Specific employees may have been targeted to gain access to eBay's network, or it is possible that eBay's entire network was being monitored prior to the attack. eBay claims to have detected this cyber-attack within two weeks.

Google Play Hack

A Turkish hacker, Ibrahim Balic, hacked Google Play twice. He admitted responsibility for the Google Play attack and claimed that he had been behind Apple's Developer site attack. He tested vulnerabilities in Google's Developer Console and found a flaw in the Android Operating System. He tested the flaw twice to ensure a vulnerability existed and used the results of his vulnerability testing to develop an Android application to exploit the flaw. When the developer's console crashed, users could not download applications, and developers could not upload their applications.

The Home Depot Data Breach

The theft of information from payment cards, for example, credit cards, is very common nowadays. On the 8th of September 2014, Home Depot released a statement claiming hackers had breached their Point-of-Sale system.

The attacker accessed the POS network and gained access to third-party vendors' login credentials. The Zero-Day vulnerability exploited Windows, which created a loophole to enter Home Depot's corporate network via a path from the third-party environment. After accessing the corporate network, Memory Scrapping Malware was released, and then the Point-of-Sale terminals were attacked. Memory Scraping Malware was highly effective and successfully grabbed the information on millions of payment cards.

Home Depot took remedial action against the attack. They started using EMV Chip and Pin payment cards. These Chip and Pin payment cards have a security chip embedded into them to avoid duplicity of the magnetic stripe. EMV cards prevent fraudulent transactions. Several countries today use EMV cards as standard payment cards because of the chip card technology. It is capable of declining certain types of credit card fraud.

Elements of Information Security

Confidentiality

The National Institute of Standards and Technology (NIST) defines confidentiality as "Preserving authorized restrictions on information access and disclosure while including means for protecting personal privacy and proprietary information". We always want to make sure that our secret and sensitive data is secure. Confidentiality means that only authorized personnel can work with and see our infrastructure's digital resources. It also implies that unauthorized persons should not have any access to the data. There are two types of data in general. First is data in motion, as it moves across the network and data at rest when the data is in any media storage (such as servers, local hard drives, the cloud). For data in motion, we need to ensure data encryption before sending it over the network. Another option, which we can use along with encryption, is to use a separate

network for sensitive data. For data at rest, we can apply encryption on storage media drives so that it cannot be read in the event of theft.

Integrity

The NIST defines integrity as “Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity”. We never want our sensitive and personal data to be modified or manipulated by unauthorized persons. Data integrity ensures that only authorized parties can modify data. NIST SP 800-56B defines data integrity as a property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. This recommendation states that a cryptographic algorithm "provides data integrity" means that the algorithm is used to detect unauthorized alterations.

Availability

Ensuring timely and reliable access to and using information applied to systems and data is termed as Availability. Suppose authorized personnel cannot access data due to general network failure or a Denial-of-Service (DoS) attack. In that case, it is considered a critical problem from the point of view of business, as it may result in loss of revenue or of records of some important results.

We can use the term “CIA” to remember these basic yet most important security concepts.

CIA	Risk	Control
Confidentiality	Loss of privacy, Unauthorized access to information & Identity theft	Encryption, Authentication, Access Control
Integrity	Information is no longer reliable or accurate, Fraud	Maker/Checker, Quality Assurance, Audit Logs
Availability	Business disruption, Loss of customer confidence, Loss of revenue	Business continuity, Plans and tests Backup storage, Sufficient capacity

Table 1-01: Cyber Risk and Protection with respect to CIA

Authenticity

Authentication is the process of identifying the credentials of authorized users or devices before granting privileges or access to a system or network and enforcing certain rules and policies. Similarly, authenticity ensures the appropriateness of certain information and whether it has been initiated by a valid user who claims to be the source of that information. Authenticity can be verified through the process of authentication.

Figure 1-01: Elements of Information Security

Non-Repudiation

Non-repudiation is one of the Information Assurance (IA) pillars. It guarantees transmitting and receiving information between the sender and receiver via different techniques, such as digital signatures and encryption. Non-repudiation is the assurance of communication and its authenticity so that the sender is unable to deny the sent message. Similarly, the receiver cannot deny what she/he has received. Signatures, digital contracts, and email messages use non-repudiation techniques.

The Security, Functionality, and Usability Triangle

In a system, the level of security is a measure of the strength of a system's Security, Functionality, and Usability. These three components form the Security, Functionality, and Usability triangle. Consider a ball in this triangle—if the ball is sitting in the center, it means all three components are stronger. On the other hand, if the ball is closer to Security, it means the system is consuming more resources for Security, and the system's Function and Usability require attention. A secure system must provide strong protection and offer the user complete services, features, and usability.

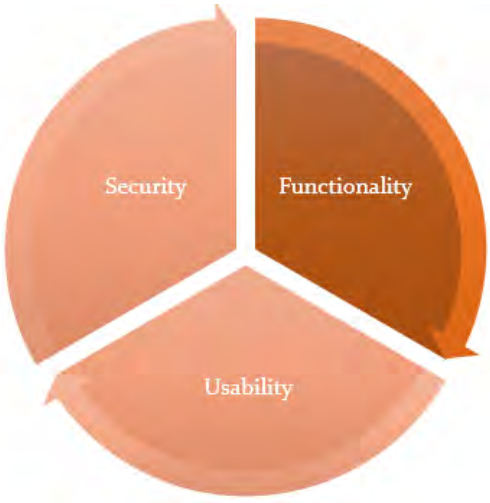


Figure 1-02: Security, Functionality, and Usability Triangle

Implementation of high-level security typically impacts the level of functionality and ease of usability. High-level security will quite often make the system nonuser-friendly and cause a decrease in performance. While deploying security in a system, security experts must ensure a reliable level of functionality and ease of usability. These three components of the triangle must always be balanced.

Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) describe the patterns and methods used by threat actors. Understanding TTPs is crucial for analyzing threats, profiling attackers, and improving an organization's security.

- **Tactics**: The overall strategy an attacker uses to execute an attack.
- **Techniques**: The specific methods used to achieve intermediate goals during the attack.
- **Procedures**: The systematic steps followed to carry out the attack.

Threats and Attack Vectors

Motives, Methods, and Vulnerabilities

An attacker attacks the target system to penetrate information security with three attack vectors in mind: motive or objective, method, and vulnerability. These three components are the major blocks on which an attack depends.

- **Motive or Objective:** The reason an attacker focuses on a particular system
- **Method:** The technique or process used by an attacker to gain access to a target system
- **Vulnerability:** These help the attacker in fulfilling his intentions

An attacker's motive or objective for attacking a system may be a thing of value stored in that specific system. It may be ethical, or it may be non-ethical. However, there is always a goal for the hacker to achieve that leads to a threat to the system. Some typical motives behind attacks are information theft, manipulation of data, disruption, propagation of political or religious beliefs, attacks on the target's reputation, or revenge. The method of attack and vulnerability run side by side. To achieve their motives, hackers use various tools and techniques to exploit a system once a vulnerability has been detected.

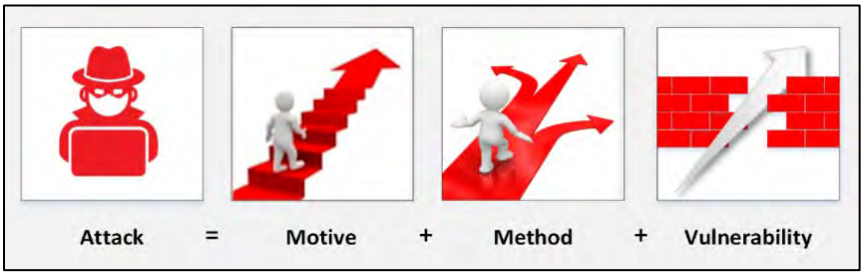


Figure 1-02: Attack Methodology

Top Information Security Attack Vectors

Cloud Computing Threats

Cloud computing has become a popular trend today. Its widespread implementation has exposed it to several security threats. Most of the threats are similar to those faced by traditionally hosted

environments. It is essential to secure cloud computing for the purpose of protecting important and confidential data.

Following are some threats that exist in cloud security:

- In the environment of cloud computing, a major threat to cloud security is a single data breach that results in a significant loss. It allows the hacker to have access to records; hence, a single breach may compromise all the information available on the cloud. It is an extremely serious situation, as the compromise of a single record can lead to multiple records being compromised
- Data loss is one of the most common potential threats to cloud security. Data loss may be due to intended or accidental means. It may be large-scale or small-scale; though massive data loss is catastrophic and costly
- Another major threat to cloud computing is hijacking an account or a service over the cloud. Applications running on a cloud with flaws, weak encryption, loopholes, and vulnerabilities allow the intruder to gain control, manipulate data, and alter the functionality of the service

Figure 1-03: Cloud Computing Threats

Furthermore, there are several other threats faced by cloud computing, which are as follows:

- Insecure APIs
- Denial-of-Services
- Malicious Insiders
- Misconfigurations
- Poorly Secured Multi-Tenancy

Advanced Persistent Threats

An Advanced Persistent Threat (APT) is the process of stealing information through a continuous procedure. An advanced persistent threat usually focuses on private organizations or political

motives. The APT process relies upon advanced and sophisticated techniques to exploit vulnerabilities within a system. The term "persistent" defines the process of an external command and controlling system that continuously monitors and fetches data from a target. The term "threat" indicates the involvement of an attacker with potentially harmful intentions.

The characteristics of APT criteria are:

Characteristics	Description
Objectives	Motive or goal of threat
Timeliness	Time spent in probing & accessing the target
Resources	Level of knowledge & tools
Risk Tolerance	Tolerance to remain undetected
Skills & Methods	Tools & techniques used throughout the event
Actions	Precise action of threat

Table 1-02: APT Criteria Characteristics

Viruses and Worms

The term virus in network and information security describes malicious software. This malicious software is designed to spread by attaching itself to other files. Attaching itself to other files helps it to transfer onto other systems. These viruses require user interaction to trigger, infect, and initiate malicious activities on the resident system.

Unlike viruses, worms are capable of replicating themselves. This ability of worms enables them to spread on a resident system very quickly. Worms have been propagated in different forms since the 1980s. A few types of worms have emerged that are very destructive and are responsible for devastating DoS attacks.

Mobile Threats

Emerging mobile phone technology, especially smartphones, has raised the focus of attacks on mobile devices. As smartphones became popularly used all over the world, attackers' focus shifted to stealing business and personal information through mobile devices. The most common threats to mobile devices are:

- Data Leakage
- Unsecure Wi-Fi
- Network Spoofing
- Phishing Attacks
- Spyware
- Broken Cryptography
- Improper Session Handling

Insider Threat

An insider can also misuse a system within a corporate network. Users are termed "Insider" and have different privileges and authorization power to access and grant the network resources.

Figure 1-04: Insider Threat

Botnets

Botnets are the group of bots connected through the internet to perform a distributed task continuously. They are known as the workhorses of the internet. These botnets perform repetitive tasks (Robot) over the internet (Network). Botnets are mostly used in Internet Relay Chats. These types of botnets are legal and useful.

A bot may be used for positive intentions, but there are also illegal bots intended for malicious activities. These malicious bots can gain access to a system by using malicious scripts and codes, either directly exploiting the vulnerability of the system or through a "Spider". A Spider program crawls over the internet and searches for holes in security. Bots introduce the system to the hacker's web by contacting the master computer. It alerts the master computer when the system is under control. Attackers remotely control all bots from the master computer.

Threat Categories

Information Security Threats can be categorized as follows:

Network Level Threats

The primary components of network infrastructure are routers, switches, and firewalls. These devices perform routing and other network operations and control and protect the running applications, servers, and devices from attacks and intrusions. A poorly configured device allows an intruder to exploit targets. Common vulnerabilities that are present on a network include using default installation settings, open access controls, weak encryption, and passwords, and devices lacking the latest security patches. Top network-level threats include:

- Scanning

- Sniffing and Eavesdropping
- Spoofing
- Session Hijacking
- Man-in-the-Middle Attack
- DNS and ARP Poisoning
- Password-based Attacks
- Denial-of-Services Attacks
- Compromised Key Attacks
- Firewall and IDS Attacks

Host Level Threats

Host threats are focused on system software. Applications such as Windows 2000, .NET Framework, and SQL Server are built or run over this software. Host-level Threats include:

- Malware
- Dictionary Attacks
- Arbitrary Code Execution
- Logon bypass
- Privilege Escalation
- Backdoors

Application Level Threats

The best practice to analyze application threats is by organizing them into application vulnerability categories. The main threats to the application are:

- Improper Data / Input Validation
- Authentication and Authorization Attack
- Security Misconfiguration
- Information Disclosure
- Broken Session Management
- Buffer Overflow Issues
- Cryptography Attacks
- SQL Injection
- Improper Error Handling and Exception Management

Classification of Attacks

Passive Attacks

Passive attacks involve intercepting and monitoring network traffic without altering the data. These attacks are primarily used for reconnaissance, allowing attackers to gather sensitive information such as unencrypted data, clear-text credentials, or other exploitable details. Since there is no direct interaction with the target system, these attacks are difficult to detect. Attackers use tools like sniffers to capture data being transmitted in the network. Examples of passive attacks include footprinting, sniffing, eavesdropping, network traffic analysis, and decrypting weakly encrypted

traffic. Information gathered in passive attacks can often be used to launch more intrusive active attacks.

Active Attacks

Active attacks involve tampering with data in transit, disrupting communication, or directly compromising secured systems. Unlike passive attacks, these involve active interaction with the target system, which makes them more detectable. Attackers may send malicious traffic, modify data, or disrupt services to exploit vulnerabilities within the target network. These attacks aim to gain unauthorized access, compromise internal systems, or manipulate the data flow. Examples of active attacks include denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and traffic injection.

Distribution Attacks

Distribution attacks occur when attackers tamper with hardware or software during production or distribution. This can involve implanting backdoors or malicious code, which are then delivered to the end user without detection. By exploiting these backdoors, attackers gain unauthorized access to sensitive information, systems, or networks. Such attacks can compromise an organization's security from the moment a system is deployed. Examples of distribution attacks include modifying software or hardware at the manufacturing stage or altering components during transit.

Operating System Attacks

In operating system attacks, vulnerable OS versions are mostly targeted. Sometimes, a newer update of an OS also brings a zero day. This is a continuous cycle of finding bugs and vulnerabilities in the source code and patching it.

Bugs in the source code of an operating system are another way for attackers to intrude. This vulnerability might be a mistake by the developer while developing the program code. Attackers can discover these mistakes and use them to gain access to the system.

Unpatched operating systems keep the system at risk and invite attackers to exploit the vulnerability. Successful intrusions can impact severely in the form of compromising sensitive information, causing data loss, and disrupting regular operations.

Some of the most common vulnerabilities of an operating system are:

Buffer Overflow

Buffer Overflow is one of the major types of operating system attacks. It is related to software exploitation attacks. When a program or application does not have well-defined boundaries, such as restrictions or pre-defined functional areas regarding the capacity of data it can handle, or the type of data that can be inputted, buffer overflow causes problems such as Denial-of-Service (DoS), rebooting, attaining unrestricted access, and freezing.

How does it occur?

- Due to an excess of data in the buffer memory
- When a program or process attempts to write more data to a fixed-length block of memory (a buffer)

- Coding errors

How to prevent it?

Open Web Application Security Project (OWASP) defines a number of general techniques to prevent buffer overflows. These include:

- Code auditing (automated or manual)
- Developer training – Bounds checking, use of unsafe functions, and group standards
- Non-executable stacks – Many operating systems have at least some support for this
- Compiler tools – StackShield, StackGuard, and Libsafe, among others
- Safe functions – Use strncat instead of strcat, strncpy instead of strcpy, etc.
- Patches – Be sure to keep your web and application servers fully patched and be aware of bug reports relating to applications upon which your code is dependent
- Periodically scan your application with one or more of the commonly available scanners that look for buffer overflow flaws in your server products and your custom web applications

Misconfiguration attacks are common in a corporate network. While installing new systems, the administrator must change the default configurations. If systems are left on default configuration, any user who does not have the privilege to access but has connectivity can access it using default credentials. It is not a big deal for an intruder to access such systems because the default configuration has common and weak passwords, and no security policies are enabled on systems by default.

Similarly, permitting an unauthorized person or giving resources and permission to a person beyond the privileges might also lead to an attack. Additionally, using the organization's name as a username or password makes it easier for hackers to guess the credentials.

Shrink Wrap Code is another technique for gaining access to a system. This type of attack targets unpatched operating systems and poorly designed software and applications. To understand shrink wrap vulnerabilities, consider an operating system that has a bug in its original software version. The vendor may have released the update, but the time between the release of a patch by the vendor and the client's system updates is very critical. During this critical time, unpatched systems are vulnerable to the Shrink wrap attack. Shrink wrap attacks also exploit vulnerable software in an operating system, bundled with insecure test pages and debugging scripts. The developer must remove these scripts before releasing the software.

Information Warfare

Information warfare is a concept of warfare over control of information. The term "Information Warfare" or "Info War" describes the use of Information and Communication Technology (ICT) to get a competitive advantage over an opponent or rival. Information warfare is classified into two types:

Defensive Information Warfare

The term "Defensive Information Warfare" refers to all defensive actions taken to protect oneself from attacks executed to steal information and information-based processes. Defensive Information warfare areas are:

- Prevention
- Deterrence
- Indication and Warning
- Detection
- Emergency Preparedness
- Response

Offensive Information Warfare

Offensive warfare is an aggressive operation that proactively takes against a rival rather than waiting for the attackers to launch an attack. The fundamental concept of offensive warfare is accessing their territory to occupy it rather than lose it. During offensive warfare, the opponent and his strategies are identified, and the attacker makes the decision to attack based on the available information. Offensive Information warfare prevents the information from being used by considering integrity, availability, and confidentiality.

Hacking Concept

What is Hacking?

Hacking in computer security refers to exploiting system vulnerabilities and bypassing security controls to gain unauthorized access to system resources. It involves altering system or application features to achieve objectives beyond their intended purpose. Hacking can result in stolen intellectual property, causing significant business losses. Common network hacking techniques include creating viruses and worms, denial-of-service (DoS) attacks, unauthorized remote access via trojans or backdoors, botnets, packet sniffing, phishing, and password cracking. The motives behind hacking vary, including stealing information, financial gain, curiosity, experimentation, power, or vengeance.

Who is a Hacker?

A hacker is an individual who breaks into systems or networks without authorization to destroy, steal data, or conduct malicious attacks. Hackers possess advanced computer skills and a deep understanding of software and hardware, enabling them to identify system vulnerabilities. Many hackers are engineers or programmers with expertise in programming languages and computer systems. Some hackers pursue hacking as a hobby, aiming to compromise as many systems as possible. While some seek knowledge, others engage in illegal activities, such as stealing business data, credit card information, or social security numbers.

Hackers and Their Motivations

Script Kiddies: Unskilled individuals who use pre-written scripts and tools to compromise systems. They focus on quantity over quality, aiming to gain attention or demonstrate technical skills without specific targets or goals.

- **White Hat Hackers:** Ethical hackers who use their skills defensively. They work with organizations, often as security analysts, to identify vulnerabilities and strengthen system security with the owner's consent.

- **Black Hat Hackers:** Malicious hackers who exploit their skills for illegal purposes, often engaging in criminal activities such as data theft and system sabotage.
- **Gray Hat Hackers:** Hackers who operate both offensively and defensively. They may identify vulnerabilities for vendors while also assisting other hackers at times.
- **Hacktivists:** Activists who hack government or corporate systems to promote political or social agendas. They often deface websites, disrupt services, or leak confidential information. Despite their motives, unauthorized access remains a crime.
- **Blue Hat Hackers**: Contract-based cybersecurity professionals hired to evaluate systems for vulnerabilities, conducting assessments and penetration testing.
- **Red Hat Hackers**: Aggressive hackers who neutralize black hat activities by actively destroying threats, going beyond defense to prevent breaches.
- **Green Hat Hackers**: Aspiring cybersecurity professionals focused on learning ethical hacking to contribute positively to security efforts.
- **Suicide Hackers**: Individuals willing to sacrifice their lives to disrupt critical infrastructure for a cause, unconcerned with consequences.
- **State-Sponsored Hackers**: Government-employed hackers who penetrate systems to gather intelligence or damage foreign infrastructures.
- **Cyber Terrorists**: Hackers motivated by political or religious beliefs, seeking to create fear by disrupting networks.
- **Corporate Spies**: Individuals engaged in corporate espionage, stealing trade secrets or sensitive data from competitors using APTs and social engineering.
- **Hacker Teams**: Groups of skilled hackers collaborating to research, identify vulnerabilities, and execute coordinated cyber-attacks.
- **Insiders**: Trusted employees who use privileged access to intentionally harm or exploit an organization's resources or information systems.
- **Criminal Syndicates**: Organized groups performing planned criminal activities, including cyber-attacks and money laundering, across jurisdictions.
- **Organized Hackers**: Structured groups of criminals using rented devices and botnets to conduct cyber-attacks for financial gain or intellectual property theft.

Ethical Hacking Concept

What is Ethical Hacking?

Ethical hacking involves using computer and network skills to help organizations test and secure their systems against vulnerabilities. Ethical hackers, also known as White Hats or security analysts, have permission from system owners to identify and fix security flaws. Unlike malicious hackers, they work with transparency and intent to improve security. Ethical hacking employs the same tools and techniques used by attackers but is always legal as it's performed with consent. The goal is to think like a hacker, uncover vulnerabilities, and recommend solutions to enhance security.

Why Ethical Hacking is Necessary

As technology advances, so do the risks. Ethical hacking is essential to counter attacks by thinking like a hacker. It helps predict vulnerabilities and fix them proactively, preventing external breaches. Since hacking requires creativity, relying solely on vulnerability testing and security audits is not enough. Organizations must use a "defense-in-depth" approach by simulating attacks to identify weaknesses.

Reasons organizations hire ethical hackers:

- To prevent unauthorized access to information systems
- To identify vulnerabilities and assess risks
- To strengthen security policies, infrastructure, and practices
- To implement preventive measures against breaches
- To protect customer data
- To raise security awareness across the organization

Scope and Limitations of Ethical Hacking

Ethical hacking is a structured security assessment, typically as part of penetration testing or security audits, aimed at identifying risks and suggesting corrective actions. It is vital in risk assessment, auditing, counter fraud, and improving information system security. Ethical hackers define the scope of the assessment based on the client's concerns and may work as part of a "Tiger Team" for comprehensive testing.

However, ethical hackers must always obtain legal permission before performing any hacking activities and adhere to strict ethical guidelines. They must follow these principles:

- Obtain client authorization and a signed contract for testing
- Maintain confidentiality, following a Non-Disclosure Agreement (NDA)
- Perform tests only within agreed-upon limits, avoiding potential harm like denial-of-service (DoS) attacks that could disrupt services

Skills of an Ethical Hacker

Technical Skills

Ethical hackers need in-depth knowledge of major operating systems like Windows, Unix, Linux, and macOS. They must understand networking concepts, technologies, and hardware/software intricacies. Proficiency in launching sophisticated attacks and expertise in security domains are also crucial for identifying vulnerabilities effectively.

Non-Technical Skills

Adaptability to new technologies, a strong work ethic, and problem-solving and communication skills are key. Ethical hackers must uphold an organization’s security policies while being aware of local standards and laws to ensure lawful practices.

AI-Driven Ethical Hacking

As cyberthreats grow more sophisticated, hackers are leveraging AI to automate and enhance attacks. Ethical hackers use AI-driven tools, machine learning models, and automation frameworks

to improve the scalability, efficiency, and effectiveness of their penetration tests. This modern approach helps them anticipate threats, strengthen defenses, and create a safer digital ecosystem. AI-driven ethical hacking empowers professionals to proactively mitigate risks and stay ahead of malicious actors.

How AI-Driven Ethical Hacking Helps

- **Enhanced Efficiency:** AI automates repetitive tasks like vulnerability scanning and network monitoring, freeing ethical hackers to focus on complex challenges.
- **Predictive Analysis:** Machine learning models predict potential breaches by identifying patterns and learning from past attacks, enabling proactive vulnerability management.
- **Advanced Threat Detection:** AI detects zero-day vulnerabilities and subtle indicators of compromise using deep learning and anomaly-detection techniques.
- **Informed Decision-Making:** AI provides data-driven insights and recommendations, helping ethical hackers allocate resources effectively and respond to threats strategically.
- **Adaptive Learning:** AI evolves with new cyber threats, continuously improving detection and response strategies without manual updates.
- **Detailed Reporting:** AI generates accurate reports on vulnerabilities and their impact, helping organizations prioritize security measures.
- **Simulation and Testing:** AI tools simulate real-world attacks to test system resilience and identify areas needing improvement.
- **Scalability:** AI efficiently manages large-scale and complex IT environments, crucial for organizations with diverse infrastructures.
- **Continuous Monitoring:** AI ensures real-time vulnerability identification and mitigation through continuous security posture assessments.
- **Adaptive Defense:** AI updates its defense mechanisms to counter evolving hacking techniques, maintaining robust cybersecurity.

Myth: AI Will Replace Ethical Hackers

- AI-driven ethical hacking enhances the efficiency of cybersecurity efforts but cannot replace human expertise.
- While AI automates tasks, it lacks the creativity, critical thinking, and deep contextual understanding that human ethical hackers provide.
- Ethical hacking involves problem-solving, understanding complex systems, and adapting to new challenges—tasks requiring human judgment and flexibility.
- AI tools need human oversight to ensure accuracy, interpret results, and make decisions where rigid rules do not apply.
- Human hackers leverage their unique insights to craft tailored security solutions and anticipate attack strategies in ways AI alone cannot.

ChatGPT-Powered AI Tools for Ethical Hackers

ChatGPT-powered tools revolutionize ethical hacking by integrating natural language processing

(NLP) and machine learning to enhance efficiency, accuracy, and threat mitigation.

Key Features:

- **Data Collection & Configuration:** Gather data from diverse sources like social media, forums, and public databases to identify vulnerabilities.
- **Task Automation:** Automate tasks like vulnerability scanning, threat analysis, and reporting using advanced NLP and machine learning.
- **Threat Intelligence Integration:** Provide contextual insights by linking with threat intelligence databases, improving accuracy and response to security breaches.

Examples:

1. **ShellGPT:** Automates shell commands, writes secure code, and generates documentation.
2. **AutoGPT:** Automates task execution and data processing for actionable insights.
3. **WormGPT:** Generates malware scripts for testing defenses.
4. **ChatGPT with DAN Prompt:** Expands hacking capabilities using custom prompts.
5. **FreedomGPT:** Provides unrestricted access to AI for deeper exploration.
6. **FraudGPT:** Detects and prevents fraud through pattern analysis.
7. **ChaosGPT:** Simulates chaotic system behaviors for better defense planning.
8. **PoisonGPT:** Studies AI model poisoning to develop robust countermeasures.

Applications & Benefits:

- **Enhanced Security:** Strengthen cybersecurity by efficiently identifying and mitigating threats.
- **Operational Efficiency:** Automate routine tasks, enabling faster and more comprehensive assessments.
- **Better Decision-Making:** Use threat intelligence and data analysis to prioritize vulnerabilities and craft effective mitigation strategies.

Additional ChatGPT-Powered Hacking Tools

The emergence of AI-driven hacking tools has revolutionized cybersecurity, enabling ethical hackers to address sophisticated threats. Below are notable ChatGPT-powered tools that enhance security operations:

HackerGPT

Source: www.chat.hackerai.co

Assists ethical hackers by automating complex tasks, providing real-time insights, and simplifying vulnerability assessments.

BurpGPT

Source: www.burpgpt.app

Enhances Burp Suite by leveraging AI for accurate vulnerability detection, reducing false positives, and automating security report generation.

BugBountyGPT

Source: www.chatgpt.com/g/g-Rsk7ADgbD-bugbountygpt

Tailored for bug bounty hunters, it automates vulnerability detection and integrates seamlessly with bug bounty platforms.

PentestGPT

Source: www.github.com/GreyDGL/PentestGPT

Streamlines penetration testing by automating assessments and generating detailed reports using AI.

GPT White Hack

Source: www.chatgpt.com/g/g-3ngv8eP6R-gpt-white-hack

Offers real-time threat detection and mitigation recommendations with AI-driven risk assessments.

CybGPT

Source: www.github.com/Coinnect-SA/CybGPT

A versatile tool that integrates threat intelligence and automates security assessments and incident responses.

BugHunterGPT

Source: www.chatgpt.com/g/g-y2KnReow4-bug-hunter-gpt

Assists in bug identification and reporting with AI-driven insights and automated vulnerability detection.

Hacking APIs GPT

Source: www.chatgpt.com/g/g-UZxOCmqLH-hacking-apis-gpt

Focuses on API security, automating vulnerability scanning, and delivering detailed analysis reports.

h4ckGPT

Source: www.chatgpt.com/g/g-1ehIOoAPO-h4ckgpt

Provides real-time support for ethical hackers, automating tasks and offering actionable insights.

HackerNewsGPT

Source: www.chatgpt.com/g/g-BIfVX3cVX-hackernews-gpt

Aggregates cybersecurity news and trends with AI-driven analysis and customizable alerts.

Ethical Hacker GPT

Source: www.chatgpt.com/g/g-j4PQ2hyqn-ethical-hacker-gpt

Delivers tools for vulnerability assessments, real-time support, and comprehensive reporting.

GP(en)T(ester)

Source: www.chatgpt.com/g/g-zQfyABDUJ-gp-en-t-ester

Automates red teaming workflows, identifies vulnerabilities, and generates detailed AI-powered reports.

CEH Ethical Hacking Framework

The EC-Council's CEH framework outlines a systematic approach to ethical hacking, mirroring the process followed by malicious attackers but with distinct goals and strategies. This methodology provides ethical hackers and security professionals with a comprehensive understanding of the phases used by real hackers to achieve their objectives.

By studying the CEH framework, ethical hackers gain insights into various tactics, techniques, and tools employed during different hacking phases. This knowledge equips them to effectively identify and mitigate vulnerabilities, ensuring a successful ethical hacking process.

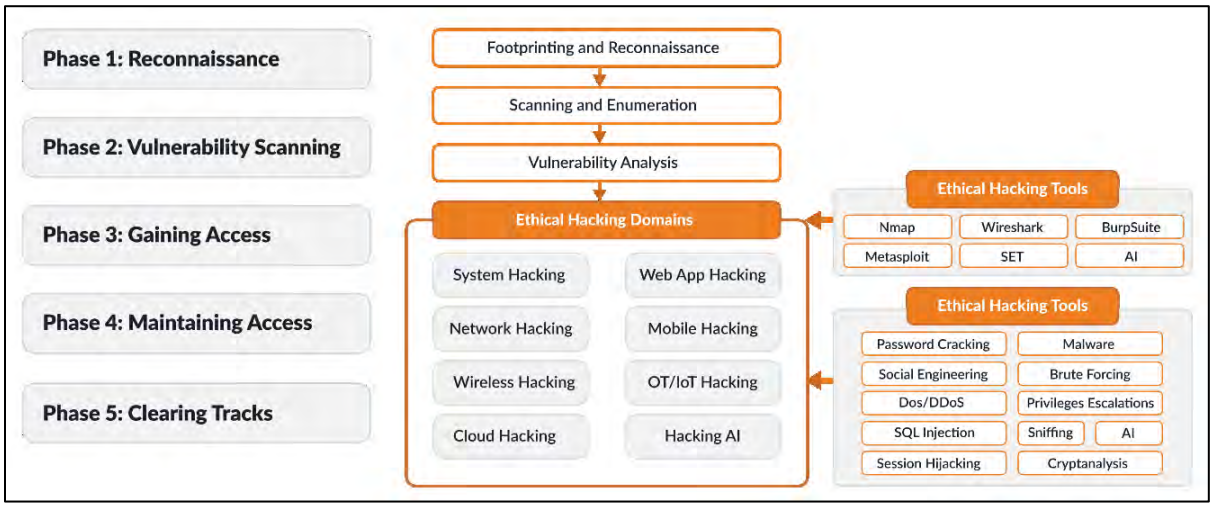


Figure 1-06: CEH Ethical Hacking Framework

Phases of the CEH Ethical Hacking Framework

1. Reconnaissance

This preparatory phase involves gathering information about the target to create a detailed profile. Techniques include:

- **Footprinting:** Identifying IP addresses, domain names, and employee details.
- **Scanning:** Identifying active hosts, open ports, and unnecessary services.
- **Enumeration:** Probing systems to extract network user lists, security flaws, and more.

2. Vulnerability Scanning

Attackers analyze the target's systems and networks to identify security loopholes. The goal is to classify vulnerabilities for further exploitation.

3. Gaining Access

The actual hacking begins here. Attackers exploit vulnerabilities using techniques like password cracking and buffer overflows to gain entry. They often escalate privileges to gain full control of the system.

4. Maintaining Access

Once inside, attackers establish long-term control by installing backdoors and other malicious tools. They use the compromised system for further attacks or data manipulation while remaining undetected.

5. Clearing Tracks

Attackers erase logs and evidence of their activity to avoid detection, ensuring no trace of the compromise remains.

Cyber Kill Chain Concepts

Lockheed Martin developed the Cyber Kill Chain framework. It is an intelligence-driven defense model for identifying, detecting, and preventing cyber intrusion activity by understanding the adversary tactics and techniques during the complete intrusion cycle. This framework helps to identify and enhance the visibility into a cyber-attack. It also helps blue teams understand the tactics of APTs. There are seven steps of the Cyber Kill Chain.

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

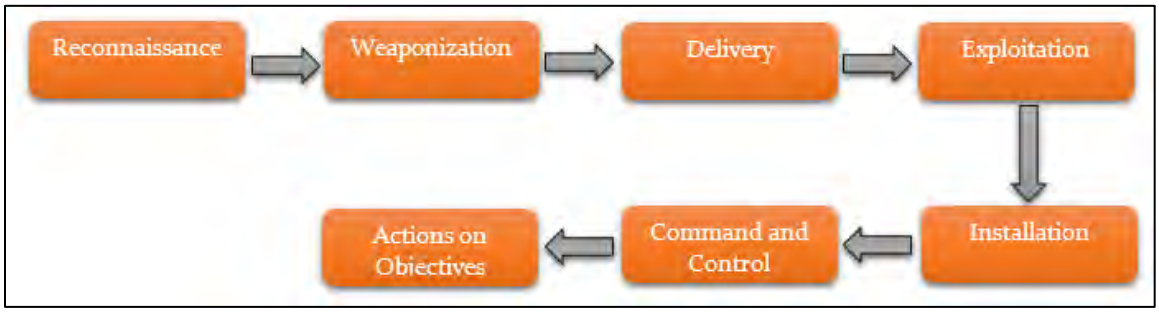


Figure 1-07: Cyber-Kill Chain

Reconnaissance

Reconnaissance is the beginning stage of the cyber kill chain. In this planning phase, adversaries collect information about the target using different techniques. This information gathering helps

the adversaries profile the target and helps them understand which vulnerability will lead them to meet their objectives. Following are some reconnaissance techniques:

- Information gathering via social networking platforms
- Social engineering
- Information gathering via search engines
- Email address harvesting
- Network scanning
- WHOIS searches / DNS queries

For security teams, it is very difficult to identify and detect reconnaissance. Adversaries can collect enough information about the target without any active connection. However, adversaries need to build an active connection with the target to discover internet-facing servers, open ports, running services, and other required information. If security teams identify reconnaissance activity, it can help them reveal the intent and subsequent actions. Organizations should have a strict policy regarding information disclosure on public and social forums. Security teams should monitor and respond promptly if any confidential or even relevant information that adversaries can misuse is posted publicly. Following are some behaviors the security team should monitor to identify reconnaissance activities:

- Website visitors log
- Internal scanning activities
- Port scanning on public-facing servers
- Vulnerability scanning on public-facing servers

Weaponization

After the collection of sufficient information about the target, adversaries prepare the operation in the Weaponization phase. Weaponization may include preparing an exploit for an identified target's vulnerability or the development of a malicious payload. Following are some preparation techniques used by adversaries to weaponize themselves:

- Preparing a weaponizer or obtaining one from private channels
- Preparing decoy documents (file-based exploits) for victims
- Command and Control (C2) implantation
- Compilation of backdoor

Security defenders cannot detect weaponization as the payload is not yet delivered. However, it is an essential phase for defenders; they can keep their security controls hardened against advanced tactics and techniques of malware. Security teams mostly conduct malware analysis and reverse engineering, which helps them identify different malware development and dropping techniques. In this way, security teams prepare the most durable and resilient defense. Following are some blue team techniques to counter:

- Conducting malware analysis for trending malware
- Building detection rules for weaponizers
- Intelligence collection about new campaigns, IoCs

- Correlation of artifacts with APT campaigns

Delivery

After all the preparation and weaponization, in the delivery phase, adversaries launch the attack by conveying the malware or weaponized payload prepared specially for the target. Following are some common methodologies of launching an attack:

- Phishing emails
- Malware on a USB stick
- Direct exploitation of web servers
- Via compromised websites

This is a very important phase for security defenders to identify, detect, and block the delivery operation. Security teams monitor incoming and outgoing traffic, analyze delivery mediums, and monitor public-facing servers to detect and block delivery. Following are some actions for security teams to detect the delivery of malware:

- Monitoring Emails Campaigns
- Leverage weaponizer artifacts to detect new malicious payloads at the point of entry
- Monitoring suspicious networks communications
- Monitoring alerts, detections on security controls
- Building signature-based detection rules

Exploitation

Exploitation is the phase in which an adversary gains access to the victim. In order to gain access, the adversary needs to exploit a vulnerability. As the adversary already has probably collected information about the vulnerabilities in the reconnaissance phase and has already been prepared for the weaponization, the adversary can exploit the victim by using any of the following techniques:

- Exploiting any software, hardware, or human vulnerability
- Using exploit code
- Exploiting operating system vulnerability
- Exploiting application vulnerability
- Victim triggered exploitation via phishing email
- Click Jacking

To counter the exploitation phase, security teams should follow traditional security measures, understand new tactics and techniques, and harden assets to prevent exploitation. Following are some key measures for security defenders to counter exploitation:

- User awareness training
- Phishing drill exercises for employees
- Periodic Vulnerability assessment
- Penetration testing
- Endpoint Hardening
- Secure coding

- Network Hardening

Installation

After successful exploitation, the adversary moves next to the installation phase. It establishes persistence at the victim either by installing a backdoor or opening a connection from the victim toward C2. This way, the adversary can maintain access to lateral movements. Following are some ways of maintaining the access activities:

- Installation of web shell
- Installation of backdoor
- Adding auto run keys

Security defenders use different security controls such as HIPS, EDR, AV engines to detect block installation of backdoors. Security teams should monitor the following to detect installations:

- Suspicious application using administrator privileges
- Endpoint process auditing
- Suspicious file creations
- Registry changes
- Auto run keys
- Security Control alerts

Command and Control

In Command and Control (C2) phase, the adversary opens a two-way communication or command channel with its C2 server. This C2 server is owned and managed by the adversary to send commands to the infected hosts. Adversaries can alter queries and commands to manipulate the victim remotely. The following are some characteristics of C2 channels:

- Victim opens two-way communication channel towards C2
- Mostly, the C2 channel is on the web, DNS, or email
- Encoded commands are queried by C2

For security defenders, this is the last chance in this kill chain to detect and block the attack by blocking the C2 channel. If the C2 channel is blocked immediately, an adversary cannot issue commands to the victim. Following are some techniques for security teams to defend against C2 communication:

- Collect and block C2 IoC via Threat Intelligence or Malware analysis
- Require proxies for all types of traffic (HTTP, DNS)
- DNS Sink Holing and Name Server Poisoning
- Monitoring network sessions

Actions on Objectives

At this stage, the adversary has a victim with persistent access connected to the C2 server. Now adversary can accomplish the objectives. What will the adversary do? That depends on his intent. At this stage, the adversary has CKC7 access. Following are some different intents or possible next actions of adversaries in this phase:

- Collection of credentials from infected machines
- Privilege Escalation
- Lateral movement in the network
- Data exfiltration
- Data corruption
- Data modification
- Destruction

At this stage, Security defenders must detect the adversary as earliest as possible. Any delay in detection at this stage can cause a severe impact. Security teams should be well-prepared and ready to respond in this stage to lower the impact. Following are some preparations for security defenders:

- Immediate incident response playbooks
- Incident readiness
- Incident response team with SMEs
- Communication and incident escalation point of contacts

Adversary Behavioral Identification

Adversary behavioral identification focuses on detecting techniques used by attackers to penetrate networks, enabling security professionals to plan defenses against cyberattacks. Key adversarial behaviors include:

1. Internal Reconnaissance

Adversaries enumerate systems, hosts, and processes using commands to gather data such as user context, system configuration, and active connections. Monitoring unusual Batch scripts, PowerShell activity, and packet captures can help detect this behavior.

2. Use of PowerShell

PowerShell is exploited for data exfiltration and attack automation. Security professionals can track misuse by analyzing PowerShell transcript logs, Windows Event logs, and user agent strings.

3. Unspecified Proxy Activities

Adversaries create multiple domains pointing to the same host to evade detection. Security teams can detect these by monitoring domain data feeds and unsolicited communication.

4. Command-Line Interface

Attackers use the command line to manipulate files, create accounts, and download malicious code. Detection involves reviewing logs for suspicious process IDs and arbitrary file names.

5. HTTP User Agent

Adversaries modify the HTTP user agent field to establish communication with compromised systems. Monitoring user agent fields can reveal these attacks early.

6. Command and Control Server

Adversaries use command and control (C2) servers for remote communication. Detection includes tracking outbound traffic, open ports, and other anomalies.

7. DNS Tunneling

DNS tunneling hides malicious traffic within legitimate DNS requests, enabling data exfiltration and C2 communication. Identifying DNS tunneling involves analyzing DNS payloads and unspecified domains.

8. Use of Web Shells

Web shells allow attackers to manipulate servers remotely. Detection methods include reviewing server access logs, error logs, and identifying suspicious strings or user agent anomalies.

9. Data Staging

Adversaries collect sensitive information for exfiltration or destruction. Monitoring for unusual file transfers, file integrity changes, and event logs can reveal data staging activities.

Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are critical clues that indicate potential intrusions or malicious activities within an organization's IT infrastructure. These indicators, which can include forensic data, artifacts, and anomalies, serve as early warning signs for security professionals, enabling them to detect and respond to cyber threats effectively. While IoCs are not inherently actionable intelligence, they are foundational data points that contribute to threat intelligence. Organizations can enhance their incident-handling strategies by continuously monitoring IoCs, which helps detect and mitigate security breaches more efficiently.

Types of IoCs

IoCs are categorized into three main types based on their complexity and role in identifying threats:

- Atomic Indicators are simple and indivisible data points that do not change in meaning. Examples include IP addresses, email addresses, and domain names, which provide direct insights into potentially malicious activity.
- Computed Indicators are derived from incident data and involve calculations or algorithms. For instance, hash values and regular expressions are used to detect malware or compromised files in a system.
- Behavioral Indicators combine atomic and computed indicators to identify patterns of malicious behavior. These include abnormal activities like code injection, remote command execution, or unauthorized privilege escalation, which reveal an adversary's tactics.

Categories of IoCs

IoCs can be further grouped into four categories based on the nature of the threat they detect:

- Email Indicators involve identifying threats through email-related clues such as the sender's address, suspicious links, or attachments. Attackers often use phishing or socially engineered emails to breach security.
- Network Indicators focus on anomalies in network traffic that could signal malicious activities, such as suspicious URLs, domain names, or IP addresses. These indicators are essential for detecting malware delivery and command-and-control (C2) communication.
- Host-Based Indicators emerge from analyzing infected systems. They include file hashes, registry changes, suspicious DLLs, and unusual mutex activity, which help in pinpointing the compromised system.

- Behavioral Indicators reveal specific actions linked to malicious intent, such as scripts executed from documents or unexpected usage of legitimate system services. These indicators are crucial for identifying evolving threats.

Key Indicators of Compromise

Some commonly monitored IoCs include unusual outbound network traffic, multiple failed login attempts, geographical login anomalies, and changes to system files or registry keys. Other indicators include suspicious activity on privileged user accounts, increased database read volumes, mismatched port-application traffic, and repeated file access requests. Detecting these signs early can prevent further exploitation of vulnerabilities.

Benefits of Monitoring IoCs

By continuously monitoring IoCs, security teams can enhance their detection capabilities and stay ahead of evolving threats. This proactive approach strengthens an organization's ability to thwart cyberattacks, enabling faster incident response and mitigation. Additionally, frameworks like STIX and TAXII facilitate the sharing of standardized threat intelligence, allowing organizations to collaborate in preventing similar attacks. Through IoC monitoring, organizations can not only improve their cybersecurity posture but also safeguard critical assets from advanced threats.

MITRE ATT&CK Framework

The MITRE ATT&CK® framework is a knowledge base with information on the different strategies that a cyberattacker can use to accomplish specific objectives. It provides techniques for obtaining various goals that serve an attacker's interests and is arranged in accordance with the life cycle of a cyberattack.

MITRE developed and kept up the ATT&CK framework. Cybersecurity is one of MITRE's research areas as a federally supported research and development center (FFRDC) of the US government. The MITRE ATT&CK framework was developed to standardize cybersecurity terminology and raise awareness of attack methods and risks.

Who Uses MITRE ATT&CK Framework

In the cybersecurity sector, the MITRE ATT&CK framework is commonly utilized. The following are a few possible applications:

- Standardized terminology and threat perception for cybersecurity
- Measuring the reach of cybersecurity defenses
- Organizing penetration test engagements
- Showing how to cover cybersecurity solutions

Consequently, a rising number of scenarios are using the MITRE ATT&CK paradigm. Nowadays, it is typical for cybersecurity companies to offer clear mappings of the functionalities of their tools to the MITRE ATT&CK paradigm. Planning defenses and engagements often involve using it, as do internal security teams and penetration testing service providers.

MITRE ATT&CK Matrices

Information regarding cybersecurity attack vectors and threat actors is organized hierarchically using the MITRE ATT&CK methodology. Four distinct ATT&CK Matrices outline strategies, techniques, sub-techniques and processes, mitigations, and other pertinent data.

The "matrices" that make up the MITRE ATT&CK framework are arranged in groups. The four MITRE ATT&CK matrices in use right now are:

PRE-ATT&CK: The stages of the cyberattack life cycle known as PRE-ATT&CK are reconnaissance and weaponization. It is intended to assist an organization in identifying warning indicators that they might be the target of an attack and the data that an attacker might use to do so.

Enterprise: The enterprise matrix covers the remainder of the cyberattack life cycle. It describes how an attacker could penetrate a business network and use it to conduct operations.

Mobile: The same phases of the cyberattack life cycle are covered by the mobile matrix as they are by the enterprise matrix. The emphasis is on potential dangers and attack methods for mobile devices, though.

Industrial control system (ICS): The ICS matrix describes the ways an attacker could access and use a network, including ICS devices.

Tactics

The highest level of organizational structure employed in a MITRE ATT&CK matrix is called a tactic. These strategies describe the overarching "objective" of a certain stage of a cyberattack.

Each matrix has a different collection of specialized tactics that it contains. There are identical sets of techniques in the corporate and mobile matrices, and the ICS matrix is basically equivalent (dropping some tactics and adding some ICS-specific ones). Because it concentrates on a new phase of the cyberattack life cycle, the PRE-ATT&CK matrix approaches are distinctive.

Levels of Tactics

The MITRE ATT&CK structure divides information into various layers below the level of tactics:

Technique: A technique is a way to carry out the objective stated in a specific tactic. For instance, the Brute Force technique in the tactic Credential Access.

Sub-procedures: There are several possible ways to carry out some techniques, which MITRE ATT&CK classifies into sub-techniques. The Brute Force technique has several sub-techniques, including Credential Stuffing, Credential Cracking, Password Guessing, and Password Spraying.

Procedures: A process is a particular way to carry out the objectives of a technique or sub-technique. There is typically a list of tools, malware, and threat actors in this section of a MITRE ATT&CK matrix known to use that specific technique.

Along with this hierarchy, MITRE ATT&CK provides a tonne of other details about a specific approach. This includes information on the technique's description, the platforms it affects, information sources to help identify it, and more.

Mitigations

MITRE ATT&CK aims to educate users about cybersecurity attacks and related defenses. Each MITRE ATT&CK approach includes a section on mitigations in addition to a description of an attack vector.

These mitigations include a selection of laws, instruments, and other techniques designed to lessen or do away with the usefulness of a specific tactic. Along with the detection information in the remaining sections of the approach description, this offers support for prevention.

MITRE ATT&CK Matrix

The MITRE ATT&CK matrix contains a collection of methods that adversaries employ to achieve a particular goal. In the ATT&CK Matrix, those goals are grouped as tactics. From the initial point of reconnaissance through the ultimate target of exfiltration or "impact," the objectives are outlined linearly. The following adversary methods are characterized when using the most inclusive version of ATT&CK for Enterprise, which includes Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, and Containers:

- Gathering knowledge about the target organization (i.e., reconnaissance) to organize future hostile actions
- Resource Development: building up tools to assist operations, such as infrastructure for command and control
- Attempting to enter your network using spear phishing as the initial access
- Execution: attempting to run malicious code involves launching a remote access tool.
- Consistency: attempting to stay in their position by switching up arrangements
- Attempting to obtain higher-level permissions or using a vulnerability to acquire access is known as privilege escalation.
- Defense Evasion: attempting to avoid detection, i.e., concealing malware via trustworthy processes
- Keylogging, also known as credential access, involves obtaining account names and passwords.
- Investigating what they can control means discovering your surroundings.
- Lateral Movement: navigating your surroundings by switching between many platforms while utilizing valid credentials.
- Collection: accumulating information useful to the adversary's objective, such as using cloud storage for information
- Controlling compromised systems through communication, such as by simulating legitimate web traffic to reach a victim network, is known as command and control.
- Exfiltration is data theft or moving data to a cloud account.
- Impact: tamper with, disrupt, or destroy systems and data, such as by using ransomware to encrypt data.

MITRE ATT&CK vs. The Cyber Kill Chain

There are two key differences when comparing MITRE ATT&CK to Cyber Kill Chain.

First, using ATT&CK techniques and sub-techniques, the MITRE ATT&CK architecture provides a lot more detail on how each stage is carried out. In order to stay abreast of the most recent

approaches, MITRE ATT&CK is frequently updated with feedback from the industry. Defenders should similarly periodically update their own procedures and attack modeling.

In addition, the Cyber Kill Chain does not take into account the various strategies and methods used in a cloud-native attack. The Cyber Kill Chain concept assumes that an enemy will introduce a payload, like malware, to the target environment; however, this approach is considerably less applicable in the cloud.

The Diamond Model of Intrusion Analysis

The useful framework that is typically used when an intrusion occurs is called the Diamond Model. The federal US government intelligence community designed the Diamond Model of intrusion analysis.

For further details, you can visit the given URL:

https://apps.dtic.mil/docs/citation/ADA586960 ***(Guide)***

The above-mentioned guide is focused on helping you understand the intrusion that has occurred in the environment.

The Diamond Model of intrusion analysis applies scientific principles to intrusion analysis. These may include measurement, repeatability, and testability. These are the focus of this Diamond Model.

Consider a scenario in which an attacker has deployed a capability against a victim via infrastructure. The diamond model can assist in determining the relationship between all those domains and gathering the necessary information and documents to resolve this intrusion.

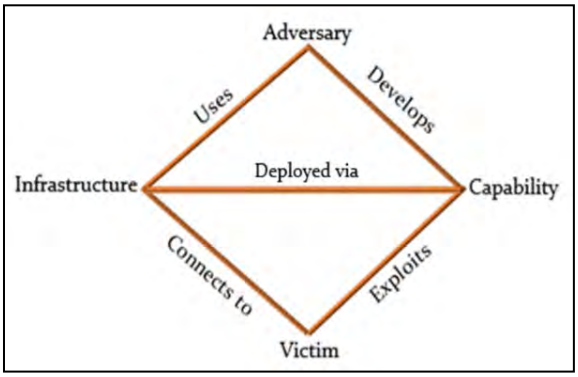


Figure 1-08: The Diamond Model of Intrusion Analysis

Adversary

An enemy is somebody who attempts to compromise your systems or networks in order to advance their own goals. A hostile insider, an outside danger actor, a threat group, or even an organization could all be considered an adversary. Hence the definition is intentionally broad to reflect this. It's rare that you will be aware of the identity of the opponent when you first detect an intrusion incident.

Capability

A tool or tactic used by an adversary in a situation is called a capacity. Although the potential tools that different adversaries could employ are practically limitless, some examples include brute-force password guessing, installing backdoors to establish command and control, etc.

Infrastructure

Infrastructure does not refer to your IT environment's infrastructure. Instead, the phrase refers to hackers' channels to distribute their tools. Among the examples are domain names, USB drives, hacked accounts, malware staging servers, etc.

Victim

They have an enemy they want to use their resources against, and the victim is their objective. According to the model, the victim need not always be a person or business; it might just be an email address or a domain. Given the variety of potential outcomes, you can be more specific when defining victims by dividing them into victim persona (individuals and businesses), and victim assets (the attack surface that includes all of the IT assets that an adversary can deploy capabilities against).

Note: An important aspect of how an event connects to these four key characteristics is that most of the information about the key characteristics is unknown until fresh information is added by input from further data gathered about the event. The diamond model asks analysts to assign a confidence rating that gauges their level of subjective assurance in the accuracy of their evaluation of a particular event feature. This requirement reflects that information about features depends on future investigation and high-quality data sources.

How Useful is the Diamond Model for Threat Intelligence

Any security analyst concentrating on threat intelligence should use the diamond model of intrusion analysis. With the aid of this model, personnel in charge of producing cyber threat intelligence may quickly analyze massive amounts of incoming data and create unmistakable connections between different types of dangerous information. The result for your security teams is a greater understanding of the intentions and tactics of your adversaries, which helps your company create proactive defenses against fresh and developing cyber threats.

The diamond model lays the foundation for knowledge management, cyber taxonomies, ontologies, threat intelligence exchange protocols, and identifying intelligence gaps. While it is an extremely useful tool for threat intelligence analysts trying to stay ahead of developing cyber threats, keep in mind that it has limitations, just like any model or tool.

Information Security Controls

Information Security Controls are the safeguards or measures implemented to minimize cyber risk, and detect and counteract information security threats to an organization. These risks may include data exfiltration, information breaches, and unauthorized access. These information security controls help protect the CIA triad of information security.

Information Assurance (IA)

Information Assurance, in short, IA, depends upon Integrity, Availability, Confidentiality, and Authenticity. Combining these components guarantees the assurance of information and

information systems and their protection during usage, storage, and communication. These components have already been defined earlier in this chapter.

Key Processes for Achieving Information Assurance

Information assurance is the practice of ensuring the confidentiality, integrity, and availability of information systems. Achieving a robust information assurance framework requires implementing a series of processes that safeguard data and mitigate potential risks. Below are some of the essential processes:

- **Developing Local Policy, Process, and Guidance:** Establishing clear policies, processes, and guidelines is a foundational step in maintaining the security of information systems. These documents provide a framework for ensuring that systems operate at an optimum security level. By setting specific rules and protocols, organizations can guide employees and stakeholders in their roles and responsibilities regarding information security.
- **Designing Network and User Authentication Strategy:** A secure network design protects sensitive user data and records from unauthorized access. Implementing a strong user authentication strategy, such as multi-factor authentication (MFA), ensures that only authorized individuals can access the information system. This dual approach significantly reduces the risk of unauthorized access and data breaches.
- **Identifying Network Vulnerabilities and Threats:** Conducting regular vulnerability assessments is crucial for identifying potential weaknesses in a network's security. These assessments provide a clear picture of the organization's security posture, helping to identify vulnerabilities and potential threats. Once these are identified, appropriate measures can be taken to remediate the risks.
- **Identifying Problems and Resource Requirements:** A thorough analysis of the information system can help identify existing issues and resource gaps. This step allows organizations to allocate resources effectively, ensuring that critical areas of the network are well-protected and operational.
- **Creating a Plan for Identified Resource Requirements:** Once resource requirements are identified, creating a detailed plan ensures that those resources are acquired and deployed effectively. This plan should align with the organization's overall security strategy, focusing on improving weak points and strengthening overall system resilience.
- **Applying Appropriate Information Assurance Controls**: Implementing security controls such as firewalls, intrusion detection systems (IDS), and encryption is essential to safeguard data. These controls help prevent unauthorized access, ensure data integrity, and protect sensitive information from cyber threats.
- **Performing the Certification and Accreditation (C&A) Process:** The Certification and Accreditation process involves a thorough evaluation of the information system's security posture. By identifying vulnerabilities during this process, organizations can take appropriate measures to address and mitigate these risks. C&A ensures that the system complies with security standards and is safe for operational use.
- **Providing Information Assurance Training**: Educating personnel about information assurance is critical in both federal and private organizations. Awareness training ensures

that employees understand their role in protecting information systems and the importance of following security protocols. This proactive approach fosters a culture of cybersecurity awareness and minimizes human-related vulnerabilities.

Continual/Adaptive Security Strategy

The **adaptive security strategy** focuses on maintaining a proactive and dynamic approach to network defense by continuously predicting, preventing, detecting, and responding to potential threats. This approach ensures that organizations stay ahead of evolving cyber threats and mitigate risks effectively. The strategy is composed of the following key elements:

- **Protection**: Protection involves implementing preventative measures to eliminate potential vulnerabilities before they can be exploited. This includes establishing robust **security policies,** ensuring **physical security,** securing **hosts,** deploying **firewalls**, and utilizing **intrusion detection systems (IDS).** By taking these actions, organizations create multiple layers of defense to protect critical assets from unauthorized access and cyberattacks.
- **Detection:** Detection focuses on identifying anomalies in the network, such as potential attacks, unauthorized access attempts, or system modifications. Regular monitoring is essential to detect and locate security breaches promptly. Tools such as **network monitoring software** and **packet sniffers** play a critical role in continuously analyzing network traffic for suspicious activities, enabling quick identification of threats.
- **Responding:** Incident response is a crucial aspect of an adaptive security strategy. It involves promptly identifying incidents, determining their root causes, and developing an appropriate response plan. Response actions include **investigating the incident, containing its impact, mitigating damages**, and **eradicating threats.** Additionally, security professionals evaluate whether the incident is a genuine security breach or a false positive, which helps avoid unnecessary disruptions and refine future response strategies.
- **Prediction:** Prediction aims to anticipate potential threats, identify vulnerable targets, and recognize possible attack methods before they materialize. This proactive approach involves conducting **risk and vulnerability assessments,** performing **attack surface analyses,** and leveraging **threat intelligence data** to forecast and prepare for future threats. By predicting risks, organizations can adopt preemptive measures to minimize their exposure to cyberattacks.

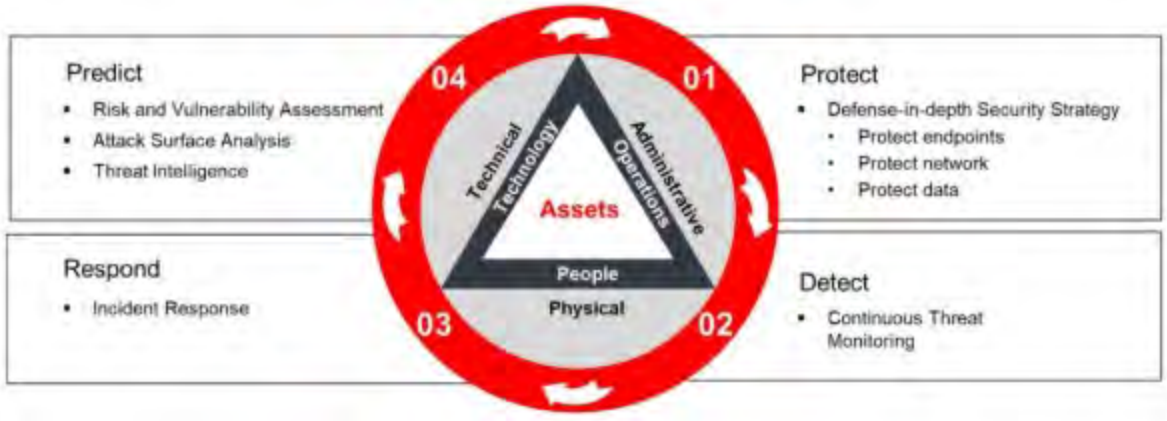


Figure 1-09: Continual/Adaptive Security Strategy

Information Security Policies

Information Security Policies are the fundamental and most dependent component of any information security infrastructure. Fundamental security requirements, conditions, and rules are configured to be enforced in an information security policy to secure the organization's resources. These policies cover the outlines of management, administration, and security requirements within an information security architecture.

Note: Information Security Policy (ISP) is a set of rules and policies for users or employees to comply with issued by an organization.

Figure 1-10: Steps to Enforce Security Policies

The basic goals and objectives of Information Security Policies are:

- Cover security requirements and conditions of the organization
- Protect the organization's resources
- Eliminate legal liabilities
- Minimize the wastage of resources
- Prevent unauthorized access/modification etc.
- Minimize risks
- Information Assurance

Categories of Security Policies

The different categories of security policies are as follows:

1. Promiscuous Policy
2. Permissive Policy
3. Prudent Policy
4. Paranoid Policy

Promiscuous Policy: The Promiscuous Policy provides for no restriction on the usage of system resources.

Permissive Policy: The Permissive Policy restricts only widely known dangerous attacks or behaviors.

Prudent Policy: The Prudent Policy ensures all the policies' maximum and the strongest security. However, it allows known and necessary risks while blocking all other services except the individually enabled ones. Every event is logged in a prudent policy.

Paranoid Policy: Paranoid Policy denies everything and limits internet usage.

Information Security Management Program

Information Security Management programs are designed to reduce the risks and vulnerabilities concerning the information security environment. This is done in order to train organizations and users to work in less vulnerable states. Information Security Management is a combined management solution to achieve the required level of information security using well-defined security policies as well as processes of classification, reporting, and management standards. Figure 1-11 shows the Information Security Management Framework:

Figure 1-11: Information Security Management Framework

Enterprise Information Security Architecture (EISA)

Enterprise Information Security Architecture is the combination of requirements and processes that helps in determining, investigating, and monitoring the structure of the behavior of an information system. The following are the goals of EISA:

- Identifying Assets

- Monitoring and Detection of Network Behavior
- Paying attention to various threats
- Detection and Recovery of security breaches
- Risk Assessment
- Cost-effectiveness

Threat Modeling

Threat Modeling is the process or approach to identifying, diagnosing, and assessing the threats and vulnerabilities of a system or application. It is a threat assessment approach dedicated to analyzing the systems and applications while considering the security objectives. This identification of threats and risks helps to validate security and enables an organization to take remedial action to achieve the specified objectives of the application. The threat modeling process includes capturing data and implementing the controls to identify and assess the captured packets to analyze the impact in case of compromise. The application overview consists of the identification process of an application to determine the trust boundaries and data flow. The decomposition of an application and identification of threats helps create a detailed review of threats breaching security control. This identification and detailed review of every aspect exposes the vulnerabilities and weaknesses of the information security environment.

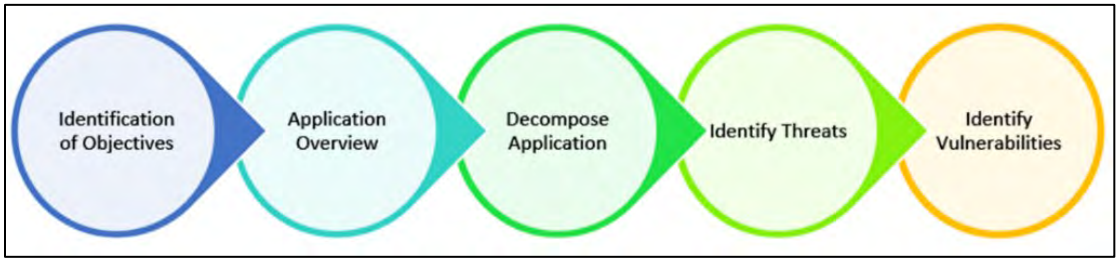


Figure 1-12: Threat Modeling

Network Security Zoning

Network Security Zoning manages and deploys an organization's architecture in different security zones. These security zones are a set of network devices with a specific security level. Different security zones may have a similar or different security level. Defining different security zones with their security levels helps monitor and control inbound and outbound traffic across the network.

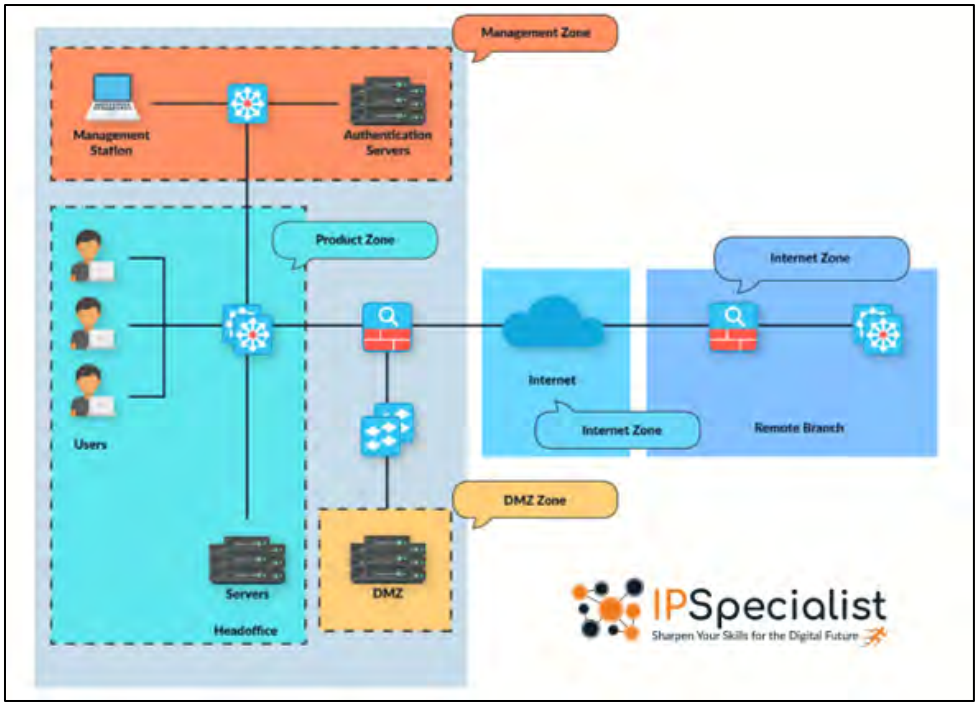


Figure 1-13: Network Security Zoning

Physical Security

Physical Security is always the top priority in securing anything. Information Security is also considered important and regarded as the first layer of protection. Physical security includes protection against human-made attacks such as theft, damage, and unauthorized physical access, as well as environmental impacts such as rain, dust, power failure, and fire.

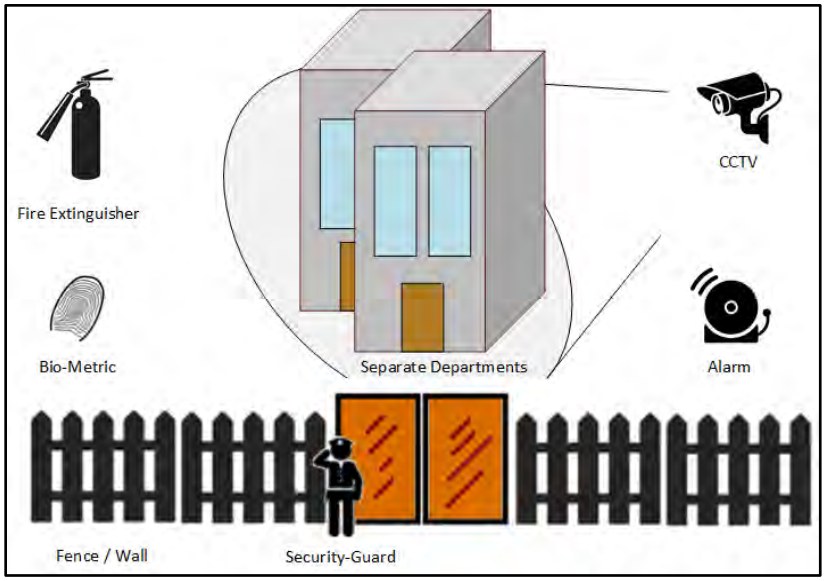


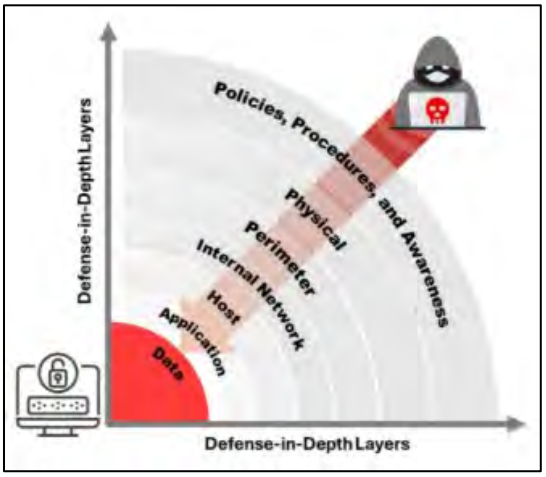
Figure 1-14: Physical Security Measures

Physical security is required to prevent theft, tampering, damage, and many more physical attacks. To secure the premises and assets, fences, guards, CCTV cameras, intruder monitoring systems,

burglar alarms, and deadlocks are set up. Only authorized persons should be allowed to access important files and documents. These files should not be left at any unsecured location, even within an organization. Functional areas must be separated and biometrically protected. Continuous or frequent monitoring, such as monitoring wiretapping, computer equipment, HVAC, and firefighting systems, should also be done.

Defense-in-Depth

Defense-in-depth is a comprehensive security approach where multiple protective layers are implemented throughout an information system. Based on the military concept that a complex, multi-layered defense is harder to breach than a single barrier, this strategy aims to deter direct attacks on the system and its data. If one layer is compromised, the attacker is confronted with additional defenses in subsequent layers. In the event of a breach, defense-in-depth reduces the overall impact and provides administrators and engineers with time to deploy new or updated countermeasures, helping to prevent future intrusions.



Figur 1-09: Defense-in Depth

What is Risk?

Risk is the potential for damage or loss due to an adverse event affecting a system or its resources. It can be defined as:

- The likelihood of a threat causing harm to an organization.
- The possibility of a threat exploiting a vulnerability.
- The product of the likelihood and the impact of an event on an asset.

In equation form:

$$\text{RISK} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$

Risk also considers the asset's value and vulnerability:

$$\text{RISK} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$$

Ultimately, risk is the combination of the probability and consequence of an adverse event.

Risk Level

Risk level evaluates the potential impact on a network by analyzing the frequency and severity of risks. A common approach involves a two-dimensional matrix based on:

- Likelihood: Probability of the incident.
- Consequence: Potential impact.

The formula for risk calculation is:

$$\text{Level of Risk} = \text{Consequence} \times \text{Likelihood}$$

Risks are classified into four levels: extreme, high, medium, and low. While control measures may reduce risk levels, they rarely eliminate risks entirely.

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent Danger	• Immediate action is necessary to address the risk. • Identify and implement controls to lower the risk to an acceptable level.
Medium	Moderate Danger	• Urgent action is not mandatory, but measures should be implemented promptly. • Apply controls swiftly to bring the risk to a reasonably low level.
Low	Negligible Danger	• Take preventive measures to minimize the impact of the risk.

Risk Matrix

A risk matrix visually represents the likelihood and impact of risks, showing their severity and potential for mitigation. It simplifies risk assessment and aids management decision-making by categorizing risks as a product of probability and severity. While standard matrices exist, organizations should customize their own.

Probability		Consequences					
	Likelihood		Insignificant	Minor	Moderate	Major	Severe
81 - 100%		Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%		High Probability	Low	Medium	High	High	Extreme
41 - 60%		Equal Probability	Low	Medium	Medium	High	High
21 - 40%		Low Probability	Low	Low	Medium	Medium	High
1 - 20%		Very Low Probability	Low	Low	Medium	Medium	High

Figure 1-15: Risk Matrix

Risk Management

Risk management involves identifying, assessing, and addressing risks to control their impact. It is a continuous, complex process integral to the security lifecycle and tailored to each organization. A risk management plan is essential for all.

Risk Management Processes and Concepts

Risk management can also be called the "*Decision Making Process*." All the components like threat assessment, risk assessment, and security implementation approach arranged within the process of business management describe the risk management

Threat Assessment

An organized interpretation of the threat that encounters a firm is known as Threat assessment. Threats cannot be changed; however, the way it affects them can be changed. Therefore, threats are necessary to figure out.

Environment

The Environment is one of the biggest sources of threat to the system. There is a variety of sources that cause environmental change, like weather, storm, flood, lightning, etc. These environmental changes disrupt the normal operation of the system and increase risk. To overcome this situation, make the system resilient to mitigate the risk sources and reduce impacts on the enterprise.

Manmade

As the name implies, manmade threats are those threats caused by the action of a person. These threats result from both the attacker's adverse action and the users' accidents. Therefore, appropriate control against intended and unintended actions is necessary to deal with the risk of the system.

Risk Types

The risk can define the identifiable assets that could be affected by an attack. Several types of risk can define, identify the threats and expose the disruption of service.

External Threat

The risk can occur from the external side of an organization where a hacker group tries to access the data or might be a former employee of an organization.

Internal Threat

The risk could also be presented inside the organization. It might be the employees coming to work daily or any partner. Some disgruntled employees have access to the internals of the network. They can easily use this access to create a security event.

Legacy Systems

If you do not pay attention to the assets of your network, then those assets could be used against you. The legacy system normally runs outdated operating systems, and the manufacturer no longer supports older software that you might find in your network.

There may be significant security concerns with the software that is running on those systems. As these devices become older, it becomes more difficult and complex to find security patches.

Multi-party

Sometimes, security breaches may involve more than one entity. It could be that your organization and many others are involved because all your networks are connected in the same way.

In May of this year, the American Medical Collection Agency was a prime illustration of this. This company handled debt collection for a variety of companies, and they suffered a data breach that affected 24 million people. This collection agency was in charge of 23 different healthcare groups. As a result, one data breach impacted 23 additional companies, forcing them to notify their consumers that their information had been exposed.

Intellectual Property (IP) Theft

IP theft can be significant if an organization has a lot of IPs, such as an idea, inventions, and creative expressions. Third parties could gain access to the intellectual property through no fault. People could make a mistake in setting up permissions in the cloud, and all that information is available to the world.

It is also possible that someone is actively hacking your system to find this Intellectual Property (IP) or someone inside the company who has access.

Software Compliance/Licensing

Another risky area of concern is software compliance in the organization and how you handle application licensing. You should purchase a proper license according to your organization's requirements. The unneeded license in the organization creates some hurdles, such as:

- The operational risk with too few licenses
- The financial risk with budgeting and over-allocated licenses
- Legal risk if proper licensing is not followed

Risk Management Strategies

Acceptance

Risk can be accepted. Risk acceptance is the practice of accepting a specific risk, typically based on an organizational decision that may also weigh the cost versus the benefits of dealing with the risk in another way.

Avoidance

It is possible to escape danger. Risk avoidance is the process of devising a plan to avoid the occurrence of the risk in the issue.

Transference

It is possible to transfer risk. The activity of passing on risk to another entity, such as an insurance company, is known as risk transfer.

- **Cybersecurity Insurance** - Cybersecurity insurance is intended to mitigate losses from the spread of cyber incidents, as well as knowledge breaches, business interruption, and network damage.

Mitigation

Most of the development approaches covered in the preceding section include a way to perform a risk analysis of the current development cycle. When a risk has been recognized, a strategy for mitigating that risk should be devised. Furthermore, it can document causes of risk that might be ignored or not addressed during a certain phase of the development process.

Risk Management Phases

The risk management process consists of four key steps:

Risk Identification

The first step in risk management aims to identify potential risks, including their sources, causes, and possible consequences. This helps address internal and external risks before they impact the organization. The effectiveness of this step depends on the skills and expertise of the individuals involved, varying across organizations.

Risk Assessment

This phase evaluates risks by estimating their likelihood and impact. It is an ongoing process that prioritizes risk mitigation and implementation plans, providing both quantitative and qualitative risk values. Risk assessment identifies, prioritizes, and addresses risks when immediate control is not possible. Regular updates to information facilities follow this process to ensure effectiveness.

Risk Treatment

Risk treatment involves selecting and applying controls to modify identified risks based on their severity. Guided by the risk assessment results, this step prioritizes risks and determines appropriate actions to reduce them to acceptable levels. It ensures risks are treated, monitored, and reviewed systematically to align with the organization's risk tolerance.

Risk Tracking and Review

An effective risk management plan requires continuous tracking and review to ensure proper risk identification, assessment, and control implementation. This phase evaluates the adequacy of measures, procedures, and information used in risk assessments. Regular policy and standard reviews help identify improvement opportunities. Monitoring ensures appropriate controls are in place, and all procedures are clearly understood and consistently followed.

Risk Monitoring

Risk monitoring is a continuous process that tracks and evaluates an organization's risk levels. Along with monitoring, the discipline tracks and evaluates the effectiveness of risk management strategies. The findings produced by risk monitoring processes can be used to assist in creating new strategies and updating previous strategies that may have proved ineffective.

The objective of risk monitoring is to constantly track the risks that occur and the effectiveness of the responses that an organization implements. Monitoring can help to ascertain whether suitable policies were adopted, whether new risks can now be identified, or whether the old strategies to do with these risks are still valid. Monitoring is most important because the risk is not static.

NIST Risk Management Framework

Managing and controlling risk is one of the major goals of businesses, particularly in the information security program. Risk management gives the vehicle for maintaining the balance between resources, compliance, and security. Organizations should be able to protect their information assets by establishing and creating an efficient risk management program, considering the organization's environment, threats, resources, and sensitivity of its data.

The NIST Risk Management Framework (RMF) process is defined in NIST 800-37 r2 (Risk Management Framework for Information Systems and Organizations). It provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems, as well as links to a suite of NIST standards and guidelines to aid in the implementation of risk management programs to meet the Federal Information Security Modernization Act's (FISMA) requirements

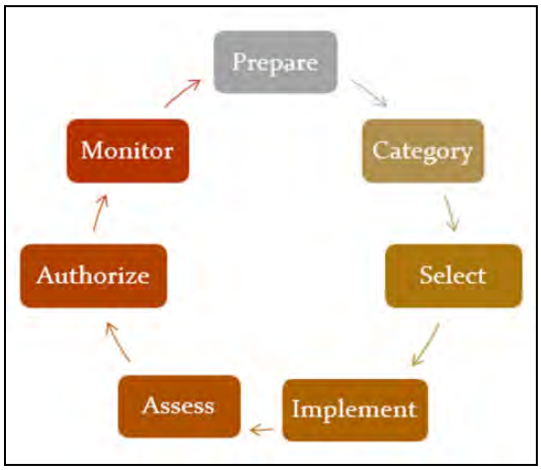


Figure 1-16: The 7-Step Process of NIST RMF

The main purpose of each step required in the Risk Management Framework is summarized in table 1-03.

Step #	Step name	Purpose
1.	Prepare	It holds all the essential activities to help prepare all the levels that an organization requires to measure its security and privacy risk
2.	Category	The steps find all the disastrous effects in terms of loss of confidentiality, integrity, availability of the system, information processes, etc. It is also responsible for informing the organizational risk management processes and tasking about these effects
3.	Select	It selects, documents, and piles up all the necessary controls to safeguard the corresponding risk faced by the system and organization
4.	Implement	This step implements all the necessary controls for security and privacy
5.	Assess	This step is responsible for ensuring that all the controls are implemented correctly, operating as planned, and creating the desired

		results required to meet the security and privacy requirements for the system and the organization
6.	Authorize	It provides the responsibility features if the security and privacy risk based on the operation of a system is allowed
7.	Monitor	It maintains the current situational information regarding the security and privacy posture of the system and organization to accept the risk management-based findings

Table 1-03: Purpose of Steps in RMF

EXAM TIP: The Risk Management Framework process can also be useful to the new provisioning systems and technologies (e.g., IoT, control systems), etc.

NIST Cybersecurity Framework

Today, data is the most valuable asset, which is the reason why security has become the highest priority-based agenda. Data breaches and security failures introduce risk and require national and economic security. Therefore, the US issued an executive to develop a Cybersecurity Framework to help reduce the cyber risk

Also, the NIST Cybersecurity Framework combines industry standards with best practices to help the systems and organizations manage and monitor their cybersecurity risk (threats, vulnerabilities, and impacts). The designed framework also helps to reduce the risks by utilizing customized measures.

Note: The NIST Cybersecurity Framework, which was launched in early 2014, was created by the private sector and the US government. In the "Cybersecurity Enhancement Act of 2014," Congress confirmed this initiative as a NIST obligation.

Figure 1-17: NIST Cybersecurity Framework

Reason for Adoption:

- 2015: Initial recognition and guidance for cybersecurity practices
- 2016: Increased awareness and early adoption by critical sectors
- 2017: Wider adoption due to rising cyber threats
- 2018: Regulatory encouragement and industry mandates
- 2019: Greater adoption by critical infrastructure industries
- 2020: Broad recognition as a best practice framework
- 2021: Support from government initiatives for adoption
- 2022: Enhanced regulatory compliance requirements
- 2023: Growing trust in NIST CSF's effectiveness
- 2024: Standardization and industry-wide integration

Cyber Threat Intelligence (CTI)

A threat is the potential for malicious activity to disrupt or damage an organization's systems, impacting its integrity and availability. Cyber Threat Intelligence (CTI) involves collecting and analyzing information about threats and adversaries to enable informed decision-making for defense against cyberattacks. CTI focuses on identifying "unknown threats" and implementing proactive measures to enhance an organization's cybersecurity posture. By anticipating attacks, CTI helps secure systems, facilitate safe data sharing, and strengthen defenses against cybercrime, hacktivism, and espionage.

Types of Threat Intelligence

Threat intelligence provides contextual insights to guide organizations in managing risks. It is categorized into four types based on its purpose and consumers:

- Strategic Intelligence: High-level insights for executive decision-making.
- Tactical Intelligence: Focused on immediate threat patterns and behaviors.
- Operational Intelligence: Real-time information about specific attacks or campaigns.
- Technical Intelligence: Detailed data on threat tactics, tools, and techniques.

Threat Intelligence Lifecycle

The threat intelligence lifecycle transforms raw data into actionable insights to counter risks, with continuous feedback from executives. It includes five phases: **Planning and Direction,** where intelligence requirements are defined, data collection methods are established, and an intelligence team is formed. This phase sets the foundation for gathering relevant intelligence from internal and external sources, ensuring efficient operations in subsequent stages.

Collection

In this phase, the focus is on gathering the intelligence defined in the planning phase using various methods like HUMINT, OSINT, SIGINT, and more. Data is collected through technical means or human sources, either openly or covertly, from critical applications, networks, and security infrastructures. Once collected, the data is transferred to the next phase for processing.

Processing and Exploitation

The collected raw data is processed and transformed into meaningful information for analysis. Using advanced tools and techniques, trained professionals structure, decrypt, filter, and aggregate the data, ensuring it is in a usable format for the analysis phase. Automated tools assist in functions like language translation and data correlation to make the data actionable.

Analysis and Production

In this phase, the processed intelligence is analyzed to refine information, allowing for the anticipation of potential threats and attacks. The analysis is objective, timely, accurate, and actionable, using reasoning techniques like deduction, induction, and the scientific method. Analysts combine data from various sources, applying qualitative, quantitative, machine-based, and statistical methods to convert raw data into actionable intelligence. The refined information is then elevated to intelligence to identify potential threats and support the development of countermeasures.

Dissemination and Integration

The analyzed intelligence is integrated and distributed to the relevant consumers through automated or manual methods. Threat information, such as indicators, adversary tactics, techniques, and procedures (TTPs), and security alerts, are shared through reports tailored to meet strategic, operational, tactical, and technical needs. These reports assist in informing decision-making at various organizational levels.

Threat Modeling

Threat modeling is a risk assessment approach to analyze an application's security by understanding the adversary's perspective, system security, and potential threats. It helps identify relevant threats, vulnerabilities in design, and improve security. Administrators should focus on the approach, not rigid steps, and adapt if obstacles arise. They should use scenarios, existing design documents, and begin with a whiteboard to brainstorm before documenting details. A digital camera can be useful for capturing and sharing the information.

Steps in Threat Modeling

1. Identify Security Objectives

Security objectives define the goals and constraints around an application's confidentiality, integrity, and availability. These objectives guide the threat modeling process and influence how much effort should be applied to each phase. To identify security objectives, administrators should consider questions like:

- What data needs protection?
- Are there compliance requirements?
- Are there specific quality-of-service needs?
- Are there intangible assets that need safeguarding?

2. Application Overview

Identify key components, data flows, and trust boundaries. Draw a rough deployment diagram to outline the application's structure, subsystems, deployment, and key elements, including logical layers, services, ports, and external dependencies.

Identify Roles

Determine the users, roles, and permissions within the application, including who can read, update, or delete data.

Identify Key Usage Scenarios

Use application use cases to understand both proper usage and potential misuse.

Identify Technologies

List technologies in use, such as operating systems, servers, development languages, and features, to focus on technology-specific threats.

Identify Application Security Mechanisms

Recognize key security mechanisms such as input validation, authentication, session management, cryptography, and auditing.

3. Decompose the Application

Break down the application to find trust boundaries, data flows, entry and exit points. Identify areas needing extra access control or privilege.

Identify Entry Points

Focus on the application's entry points for both user interaction and potential attack vectors, particularly those leading to critical functions.

Identify Exit Points

Administrators should identify and prioritize exit points where the application transfers data to external systems, especially where data from untrusted sources (e.g., shared databases) is written.

4. Identify Threats

Administrators, with input from development and test teams, should identify relevant threats using the application overview and decomposition. A question-driven approach helps pinpoint potential risks.

5. Identify Vulnerabilities

Vulnerabilities are weaknesses that attackers can exploit. Administrators should identify these weaknesses based on the threats found, using vulnerability categories, and address them to prevent security breaches.

Incident Management

Incident Response Management is the procedure and method of handling any incident that occurs. This incident may be a violation of any condition, policy, etc. Similarly, in information security, incident responses are the remediation actions or steps taken to respond to an incident to make the system stable, secure, and functional again. Incident response management defines the roles

and responsibilities of an organization's penetration testers, users, or employees. Additionally, incident response management defines the action required to be taken when a system faces a threat to its confidentiality, integrity, authenticity, and availability depending upon the threat level. Initially, the important thing to remember is when a system is dealing with an attack, it requires sophisticated and dedicated troubleshooting by an expert. While responding to an incident, the expert collects evidence, information, and clues that are helpful for prevention in the future, tracing the attacker and finding loopholes and vulnerabilities in the system.

Incident Management Process

Incident Response Management processes include:

1. Preparation for Incident Response
2. Detection and Analysis of Incident Response
3. Classification of an incident and its prioritization
4. Notification and Announcements
5. Containment
6. Forensic Investigation of an Incident
7. Eradication and Recovery
8. Post-Incident Activities

Incident Response Team

An Incident Response team consists of members who are well-aware of how to deal with incidents. This response team has a team of trained officials who are experts in gathering information and securing all evidence of an attack collected from the incident system. An Incident Response team is made up of IT personnel, HR, Public Relations officers, local law enforcement, and a chief security officer.

Responsibilities of an Incident Response Team

- The major responsibility of this team is to act according to the Incident Response Plan (IRP). If an IRP is not defined or not applicable to that case, the team has to follow the leading examiner to perform a coordinated operation
- Examine and evaluate an event, determine the damage or scope of an attack
- Document the event and processes
- If required, get the support of an external security professional or consultant
- If required, get the support of local law enforcement
- Collection of facts
- Report

Incident Handling and Response (IH&R)

IH&R is the process of managing and responding to security incidents or cyberattacks through a set of organized steps. It involves logging, recording, and resolving incidents, aiming to restore normal operations quickly and with minimal impact. The process includes preparation, detection, containment, eradication, and recovery. Key steps include defining policies, building response teams, auditing assets, and training employees.

Step 1: Preparation

The preparation phase involves auditing resources, defining security rules and procedures, building and training response teams, and equipping employees with the necessary tools and training to secure systems.

Step 2: Incident Recording and Assignment

The incident is reported and recorded, with proper communication plans defined for employees, IT support, or ticket submissions.

Step 3: Incident Triage

Incidents are analyzed, validated, categorized, and prioritized. The compromised device is examined to identify attack details, severity, target, impact, and vulnerabilities.

Step 4: Notification

The IH&R team informs stakeholders, including management, vendors, and clients, about the incident.

Step 5: Containment

This phase prevents the spread of infection and minimizes further damage to organizational assets.

Step 6: Evidence Gathering and Forensic Analysis

Evidence related to the incident is collected and analyzed by the forensic team to identify attack methods, exploited vulnerabilities, and compromised systems.

Step 7: Eradication

The root cause of the incident is removed, and attack vectors are closed to prevent future incidents.

Step 8: Recovery

Affected systems, services, and data are restored, ensuring minimal disruption to business operations.

Step 9: Post-Incident Activities

The incident undergoes a final review and analysis to assess the response and improve future handling processes.

Role of AI and ML in Cybersecurity

AI and ML are crucial in cybersecurity to detect and mitigate emerging threats like ransomware, botnets, and malware. AI processes large datasets to identify trends and anomalies, while ML enables systems to learn from data and identify deviations in real-time. ML techniques include:

- **Supervised Learning:** Uses labeled data to learn distinctions between classes, including classification (identifying class types) and regression (for continuous data).
- **Unsupervised Learning:** Analyzes unlabeled data to identify patterns, with subcategories like clustering (grouping similar data) and dimensionality reduction (simplifying data attributes).

AI and ML reduce the burden on security teams by automating threat detection and alerting when necessary.

How Do AI and ML Prevent Cyber Attacks

AI and ML are increasingly used across industries like IT, finance, and manufacturing to defend against cyber threats. Here are key applications:

- **Password Protection and Authentication:** AI enhances biometric systems, like face recognition, to prevent unauthorized access.
- **Phishing Detection:** AI scans emails and websites to identify phishing attacks faster than humans.
- **Threat Detection:** Machine learning helps detect cyberattacks by analyzing data and alerting admins to threats.
- **Vulnerability Management:** AI and ML identify and alert admins about vulnerabilities before they can be exploited.
- **Behavioral Analytics:** AI detects unusual behavior to flag potential account compromise.
- **Network Security:** AI analyzes network traffic and suggests security policies to protect systems.
- **AI-based Antivirus**: AI-based antiviruses detect abnormal program behavior to identify new malware.
- **Fraud Detection:** AI and ML spot anomalies in transactions to block fraudulent activity.
- **Botnet Detection:** AI detects suspicious network behavior and identifies botnets that bypass traditional systems.
- **AI to Combat AI Threats:** AI detects and counters attacks that use AI to exploit vulnerabilities.

Vulnerability Assessment

Vulnerability assessment is the procedure of examining, identifying, and analyzing the ability of a system or application, including security processes running on a system, to withstand any threat. Through vulnerability assessment, you can identify weaknesses in a system, prioritize vulnerabilities, and estimate the requirement and effectiveness of any additional security layer.

Types of Vulnerability Assessment

The following are the types of vulnerability assessment:

1. Active Assessment
2. Passive Assessment
3. Host-based Assessment
4. Internal Assessment
5. External Assessment
6. Network Assessment
7. Wireless Network Assessment
8. Application Assessment Network

Vulnerability Assessment Methodology

Network Vulnerability Assessment is an examination of the possibilities of an attack and vulnerabilities in a network. The following are the phases of a Network Vulnerability Assessment:

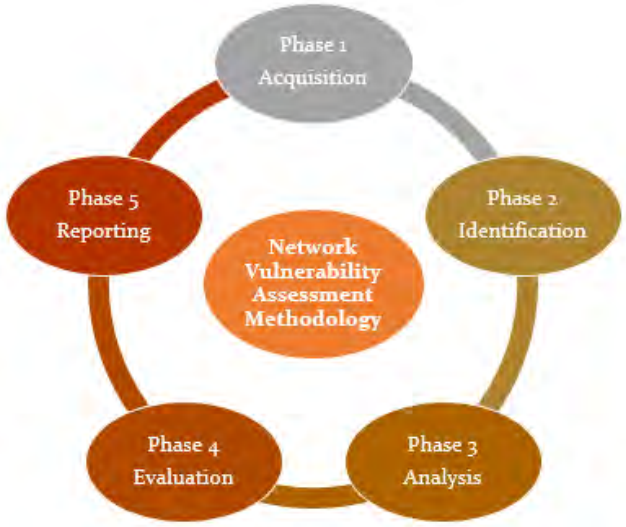


Figure 1-18: Network Vulnerability Assessment Methodology

Acquisition

The Acquisition phase compares and reviews previously identified vulnerabilities, laws, and procedures that are related to network vulnerability assessment.

Identification

In the Identification phase, interaction with customers, employees, administration, or other people involved in designing the network architecture to gather the technical information.

Analysis

The Analysis phase reviews the gathered information. It basically consists of:

- Reviewing information
- Analyzing the results of previously identified vulnerabilities
- Risk assessment
- Vulnerability and risk analysis
- Evaluating the effectiveness of existing security policies

Evaluation

The Evaluation phase includes:

- Inspection of identified vulnerabilities
- Identification of flaws, gaps in an existing network, and required security considerations in a network design
- Determination of security controls required to resolve issues and vulnerabilities
- Identification of the required modifications and upgrades

Generating Reports

In the Reporting phase, reports are drafted to document the security event and present them to higher authorities such as a security manager, board of directors, or others. This documentation is also helpful for future inspection. The report helps to identify vulnerabilities in the acquisition phase. Audit and Penetration also require these previously collected reports. When any modification in the security mechanism is required, these reports help to design the security infrastructure. Central databases usually hold these reports. Reports contain:

- Tasks completed by each member of the team
- Methods and tools used
- Findings
- Recommendations
- Gathered information

Penetration Testing

Penetration Testing is the process of hacking a system, with permission from the owner of that system, to evaluate security, Hack Value, Target of Evaluation (TOE), attacks, exploits, zero-day vulnerability, and other components such as threats vulnerabilities, and daisy-chaining. In the environment of Ethical Hacking, a pentester is an individual authorized by an owner to hack into a system to perform penetration testing.

The Importance of Penetration testing

In today's dynamic technological environment, denial-of-service, identity theft, theft of services, and information theft have become the most common cybercrimes. System penetration is used to protect the system from such malicious threats by identifying vulnerabilities in it. Some other major advantages of penetration testing are:

Identifying vulnerabilities in systems and security controls in the same way an attacker searches for and exploits vulnerabilities to bypass security.

- Identifying the threats and vulnerabilities of an organization's assets
- Providing a comprehensive assessment of policies, procedures, design, and architecture
- Setting remedial actions before a hacker identify and breaches security
- Identifying what an attacker can access to steal
- Identifying the value of information
- Testing and validating the security controls and identifying the need for any additional protection layer
- Modifying and upgrading currently deployed security architecture
- Reducing the expense of IT Security by enhancing Return on Security Investment (ROSI)

Vulnerability Assessment and Penetration Testing (VAPT) is needed because it protects us from harm, secures us from intrusion, keeps our confidential data confidential, and conceals our information from prying eyes. Every corporate manager or network administrator needs to know their weak points so they can address them. We all know that networks are vulnerable, but we do not all know where and how; this is where vulnerable assessment comes in.

It is a comprehensive check of physical weaknesses in computers and networks. It identifies potential risks and threats at any exposure and develops strategies for dealing with them.

“Prevention is better than cure.”

Another reason for VAPT is to prevent hacking incidents. We are very much aware of hacks such as the loss of:

- Sensitive data
- Account numbers
- Email addresses
- Personal information

These security incidents happen every day in the world of computer networking. This is why you need to look at your network from the outside and see it as an attacker would see it. Learn its strengths, its weaknesses and then plug the gaps. Your infrastructure may be secure; your servers may lock down the firewall on strong policies, but what about the default configuration of peripheral devices, such as printers, scanners, fax machines, etc. Your network is adorned with them, and their vulnerability is often neglected. A vulnerability assessment and penetration testing would highlight any problems in seconds. Any network with users is not as secure as you might think. Protecting your network should be your priority. In summary, the reasons for performing VAPT are:

- To protect the network from attacks
- To learn its strengths and weaknesses
- To safeguard information from theft
- To comply with data security standards
- To add reliability and value to services

Security Audits	Vulnerability Assessments	Pnetration Testing
Security audits are the evaluation of security controls. It makes sure that controls are being enforced and followed properly throughout th organization, without any cncern about the threats and vulnerabilities	Vulnerability Assessment process is to identify vulnrabilities and threats, which may exploit and impact an organization financially or reputationally	Pnetration is the process of scurity assessment, which includes security audits and vulnerability assessment. Futhermore, it demonstrates the attach, its solution and required remedial actions

Table 1-01: Comparison Chart

Types of Penetration Testing

It is important to understand the difference between the three types of Penetration Testing because a penetration tester might be asked to perform any one of them.

Black Box is a type of penetration testing in which the pentester is blind testing or double-blind testing. This means that the pentester has no prior knowledge of the system or any information about the target.

Gray Box is a type of penetration testing in which the pentester has very limited prior knowledge of the organization's network. For example, the operating system or network information might be very limited.

White Box is a type of penetration testing in which the pentester has complete information about the system and the target. This type of penetration testing is performed by internal security teams or security audit teams in order to carry out an audit.

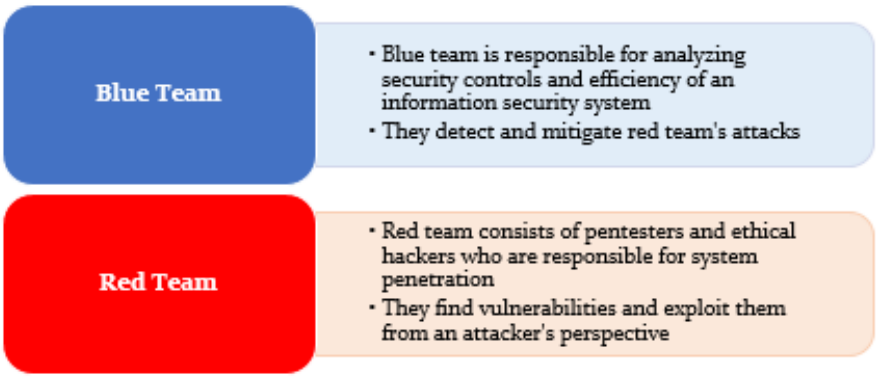


Figure 1-19: Red vs. Blue Team

Phases of Penetration Testing

Penetration Testing is a three-phase process:

1. Pre-Attack Phase
2. Attack Phase
3. Post-Attack Phase

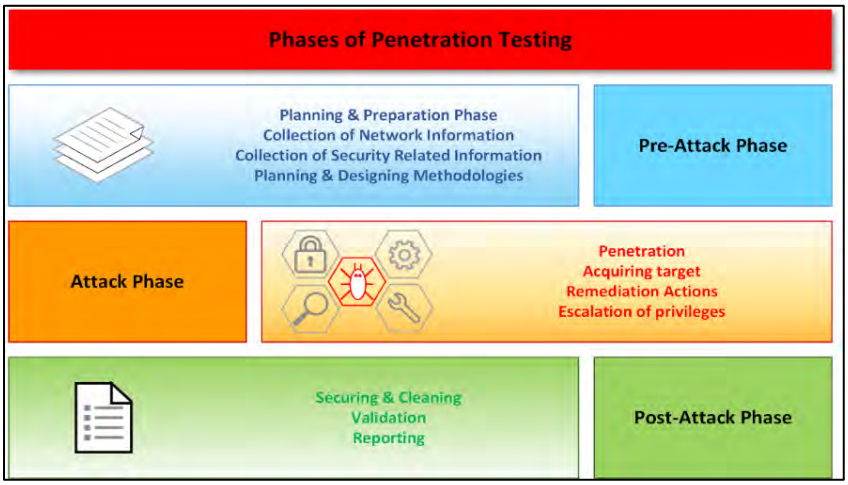


Figure 1-20: Penetration Testing Phases

Security Testing Methodology

There are some methodological approaches to be adopted for security or penetration testing. Industry-leading Penetration Testing Methodologies are:

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)

- Information Systems Security Assessment Framework (ISAF)
- Licensed Penetration Tester (LPT) Methodology

Python is popularly used but limited to penetration testing, information gathering, scripting tools, automating, and forensics.

Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed security testing and analysis manual whose results are verified facts. These facts provide actionable information that can measurably improve your operational security.

Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products to ensure that they meet an agreed-upon security standard for governmental deployment.

Information Security Laws and Standards

Law is a rule created and enacted by the judicial system of a country. Similarly, International laws are created by mutual understanding and are applicable across the globe. Any violation of these laws can be prosecuted in the national or international court. Cyber laws are focused on information and cybersecurity. These laws specify adoptions, restrictions, mandatory compliance, and other legal aspects. Regulations and standards ensure the entire process complies with the law operationally and legally. Standards also baseline the security parameters to be adopted at different layers of organizational hierarchy.

Payment Card Industry Data Security Standard (PCI-DSS)

Payment Card Industry Data Security Standard (PCI-DSS) is a global information security standard created by the "PCI Security Standards Council". It was created for organizations to develop, enhance and assess security standards required for handling cardholder information and payment account security. The PCI Security Standards Council develops security standards for the payment card industry and provides the tools required to enforce these standards, such as training, certification, assessment, and scanning.

The founding members of this council are:

- American Express
- Discover Financial Services
- JCB International
- MasterCard
- Visa Inc.

PCI data security standard deals basically with cardholder data security for debit, credit, prepaid, e-purse, POS, and ATM cards. A high-level overview of PCI-DSS provides:

- Secure Network
- Strong Access Control
- Cardholder Data Security
- Regular Monitoring and Evaluation of the Network
- Maintaining Vulnerability Program
- Information Security Policy

ISO/IEC 27001:2013

The International Organization for Standardization (ISO) and International Electro-Technical Commission (IEC) are organizations that globally develop and maintain their standards. ISO/IEC 2700 1:20 13 standard ensures the requirement for implementation, maintenance, and improvement of an information security management system. This standard is a revised edition (second) of the first edition of ISO/ISE 27001:2005. ISO/IEC 27001:2013 covers the following key points of information security:

- Implementing and maintaining security requirements
- Information security management processes
- Assurance of cost-effective risk management
- Status of information security management activities
- Compliance with laws

Other Relevant ISO/IEC Standards

- **ISO/IEC 27701:2019:** Extends ISO/IEC 27001 to privacy management, focusing on protecting personally identifiable information (PII) and helping organizations manage privacy risks.
- **ISO/IEC 27002:2022**: Provides best practices for cybersecurity areas like access control and cryptography to enhance security and ensure compliance.
- **ISO/IEC 27005:2022:** Offers guidelines for information security risk management, aiding organizations in effective risk assessment and mitigation.
- **ISO/IEC 27018:2019:** Focuses on protecting PII in cloud environments by providing cloud-specific controls for data privacy.
- **ISO/IEC 27032:2023:** Covers Internet, Web, network security, and cybersecurity, helping organizations improve their resilience against cyber threats.
- **ISO/IEC 27033-7:2023**: Provides guidelines for securing virtual networks, addressing specific risks in virtualization environments.
- **ISO/IEC 27036-3:2023:** Focuses on securing the supply chain by ensuring the secure acquisition and integration of products and services.
- **ISO/IEC 27040:2024:** Provides guidelines for data storage security, ensuring the integrity, confidentiality, and availability of stored data.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 by Congress. The HIPAA works with the Department of Health and Human Services (HHS) to develop and maintain a regulation associated with health information privacy and security. It establishes the national standards and safeguards that must be implemented to secure electronically protected health information. The HIPAA also defines general rules for risk analysis and management of E-PHI. These rules include a series of administrative, physical, and technical security procedures to ensure the confidentiality, integrity, and availability of electronically protected health information (E-PHI).

The major domains in information security where the HIPAA is developing and maintaining standards and regulations are:

- Electronic Transaction and Code Sets Standards
- Privacy Rules
- Security Rules
- National Identifier Requirements
- Enforcement Rules

Sarbanes Oxley Act (SOX)

The U.S. Congress passed the Sarbanes-Oxley Act of 2002 on July 30 of that year in an effort to safeguard investors against misleading financial reporting by businesses. Also referred to as the SOX Act of 2002, it required stringent updates to current securities laws and placed severe new penalties on offenders.

The Sarbanes-Oxley Act of 2002 was passed in reaction to the early 2000s financial crises involving publicly traded firms like WorldCom, Tyco International plc, and Enron Corporation. The high-profile thefts undermined investor faith in the reliability of corporate financial statements and prompted many to call for an update to long-standing regulatory norms.

The key requirements or provisions of the Sarbanes Oxley Act (SOX) are organized in the form of 11 titles, and they are as follows:

Title	Major
Title I	Public company accounting oversight board
Title II	Auditor independence
Title III	Corporate responsibility
Title IV	Enhanced financial disclosures
Title V	Analyst conflicts of interest
Title VI	Commission resources and authority
Title VII	Studies and reports
Title VIII	Corporate and criminal fraud accountability
Title IX	White-collar crime penalty enhancements
Title X	Corporate tax returns
Title XI	Corporate fraud and accountability

Table 1-04: SOX Titles

Some other regulatory bodies offer standards that are being deployed worldwide, including the Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA). The DMCA is the United States copyright law—whereas The FISMA is a framework for ensuring the effectiveness of information security control. According to Homeland Security, FISMA 2014 codifies the Department of Homeland Security's role in administering the implementation of information security policies for Federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. The legislation provides the Department with the authority to develop and oversee the implementation of binding

operational directives to other agencies in coordination and consistency with OMB policies and practices. The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA).

DMCA (Digital Millennium Copyright Act)

The DMCA (Digital Millennium Copyright Act) is U.S. copyright law that enforces two 1996 WIPO treaties, prohibiting circumvention of technological protections and alteration of copyright management info. It contains five titles:

- **Title I: WIPO Treaty Implementation** – Implements WIPO treaties, prohibiting circumvention and tampering with copyright protections, with civil and criminal penalties.
- **Title II: Online Copyright Infringement Liability Limitation** – Limits liability for online providers under specific conditions (e.g., transitory communications, caching, user storage).
- **Title III: Computer Maintenance or Repair** – Allows making copies of software for computer maintenance or repair.
- **Title IV: Miscellaneous Provisions** – Covers issues like copyright office authority, nonprofit exemptions, and webcasting amendments.
- **Title V: Protection of Certain Original Designs** – The Vessel Hull Design Protection Act protects vessel hull designs under specific conditions.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) of 2002 establishes a framework to ensure the security of information resources supporting federal operations. It mandates federal agencies to create, document, and implement information security programs for their operations and assets, including those managed by contractors. Key components of FISMA include:

- Categorizing information and systems by mission impact.
- Defining minimum security requirements.
- Providing guidance for selecting and assessing security controls.
- Offering guidance for security authorization of information systems.

GDPR

The General Data Protection Regulation (GDPR) is the biggest European Union legislation giving ordinary people and precedented control over how their data is collected and used and forces companies to justify everything they do with it. It hugely affects businesses outside the EU, including the US.

As everything is moving their future toward the digital domain, the massive collection of sensitive data requires strict and protected regulations from holding them.

Any type of data that can identify you with your name, contact details, username, IP address, and location is required by the GDPR. The organizations will have to prove that they have a lawful reason for holding the particular kind of data.

Why is it needed?

Before smartphones, a massive amount of sensitive information was collected from sources like Google and Facebook. GDPR gives organizations guidelines on what they can and cannot do with personal data. It also makes them gives users more clarity over the kind of data being used and how companies will use it.

Principles

The following principles for the acquisition, storage, and use of personal data are defined by GDPR: There must be the following personal information:

a. Processed in a manner that is fair, legal, and transparent

b. Collected for specific, clear, and legal purposes and not used for further processing in a way that is not related to those purposes

c. In respect to the purposes for which they are processed, appropriate, relevant, and limited to what is necessary

d. Accurate and kept up to date as needed

e. Retained in a manner that makes it possible to identify data subjects for no longer than is required to fulfill the objectives for which the personal data are processed.

f. Using the required technical or organizational measures to guarantee that personal data is handled securely, including protection against unauthorized or unlawful processing and against unintentional loss, destruction, or damage.

Controllers and Processors

Controllers - The organization that holds the data and manages how, where, and when personal data is processed is referred to as the controller; they are primarily responsible under the law.

Processors - The entity performing operations on the data on behalf of the controller is known as the processor, and they are legally obligated to maintain the security of the data.

GDPR and The Ethical Hacker

There are several ways that GDPR affects what we perform in penetration tests.

Personal data must only be used for the purposes for which it was obtained, according to principle (b). This means that we are unable to use customer personal information for the penetration test since it is doubtful that the users were made aware that it might be used for security testing.

Unless the organization has a specific provision in its security policy that indicates otherwise, the same limitations apply to the employees' personal data. We must maintain a record of what, when, and how personal information was used if it was used during the penetration test.

We must consider principle (f) when we have extracted personal information for the penetration test. It is legally required of the ethical hacker to guarantee data security. The pentesting scope should include this specification as a requirement.

Industry-Standard Framework and Reference Architecture

Industry-standard framework and reference architecture can be referred to as a conceptual model that describes the operation and structure of the IT system in any organization.

Regulatory

The business processes and procedures that are compliance-related are known as Regulatory bodies. Some rules and regulations are required to be followed for performing specific functions. For example, public companies deal with a lot of Sarbanes Oxley (SOX) regulations.

Non-Regulatory

Some processes in an organization are not compliance concerned, meaning that no rule of law is required to perform a particular function. For example, NIOSH (National Institute for Occupational Safety and Health) is a non-regulatory body.

National vs. International

There are a lot of national and international frameworks that provide proper instructions and practices for information security. FISMA (Federal Information Security Management Act) is a United States' law developed for the protection of government data and resources against dreadful threats.

Industry-Specific Framework

Bodies within a specific industry have formed the Industry-Specific Framework for addressing regulatory requirements or because of industry-specific risks or concerns. Examples of Industry-Specific Frameworks are HITRUST Common Security Framework (CSF) and COBIT (Control Objectives for Information and Related Technologies).

Benchmarks/Secure Configuration Guides

When Operating Systems, database servers, web servers, or other technologies are installed, they are far away from the secured configuration. Systems with a default configuration are not secure. Some guidelines are needed to keep everything safe and secure.

Platform-Specific Guide

The Platform-Specific Guide is the finest guide to come from the manufacturer of each device. This guide includes all the essential principles regarding installation, configuration, and sometimes operations as well.

Payment Card Industry Data Security Standards (PCI DSS): The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.

Sarbanes-Oxley Act: The Sarbanes-Oxley Act is designed to oversee the financial reporting landscape for finance professionals. Its purpose is to review legislative audit requirements and to protect investors by improving the accuracy and reliability of corporate disclosures.

Data Protection Act 2018 (DPA)

The Data Protection Act 2018 (DPA) governs data protection law in the UK, replacing the Data Protection Act 1998. Effective from May 25, 2018, and amended in January 2021 to reflect the UK's departure from the EU, the DPA regulates the processing of personal data. Key provisions include:

- Ensuring personal data is processed lawfully, fairly, and with the data subject's consent or other legal grounds.
- Granting individuals rights to access, correct, and control their data.
- Outlining the responsibilities of the Information Commissioner to monitor and enforce data protection laws, with a focus on securing personal data while considering the interests of data subjects and public interest.

Summary

This chapter covered key topics in information security, including types of attacks, information warfare, and hacking. It explored ethical hacking, its scope, limitations, and skills required, alongside AI-driven ethical hacking. The chapter examined various hacking frameworks such as CEH, the cyber kill chain, MITRE ATT&CK, and the diamond model for intrusion analysis. It discussed security controls like defense-in-depth, risk management, cyber threat intelligence, and incident management. Finally, it reviewed various information security laws and acts, providing a comprehensive overview of the field.

Mind Map

Figure 1-21: Mind Map

Practice Questions

1. Which of the following does an Ethical Hacker require to penetrate a system?
   A. Training
   B. Permission
   C. Planning
   D. Nothing

2. What is Gray Box Pentesting?
   A. Pentesting with no knowledge

B. Pentesting with partial knowledge
C. Pentesting with complete knowledge
D. Pentesting with permission

3. If you have been hired to perform an attack against a target system to find and exploit vulnerabilities, what type of hacker are you?
   A. Gray Hat
   B. Black Hat
   C. White Hat
   D. Red Hat

4. Which of the following describes an attacker who goes after a target to draw attention to a cause?
   A. Terrorist
   B. Criminal
   C. Hacktivist
   D. Script Kiddie

5. What is the level of knowledge of a Script Kiddie?
   A. Low
   B. Average
   C. High
   D. Advanced

6. A White Box test requires _____.
   A. No knowledge
   B. Some knowledge
   C. Complete knowledge
   D. Permission

7. Which of the following describes a hacker who attacks without regard for being caught or punished?
   A. Hacktivist
   B. Terrorist
   C. Criminal
   D. Suicide Hacker

8. A penetration test is required for which of the following reasons? (Choose 2)
   A. Troubleshooting network issues
   B. Finding vulnerabilities
   C. To perform an audit

D. To monitor performance

9. Hacker using their skills for both benign and malicious goals at different times are _____.
   A. White Hat
   B. Gray Hat
   C. Black Hat
   D. Suicide Hacker

10. Vulnerability assessment is basically _____.
   A. Monitoring for threats
   B. Disclosure, scope & prioritization of vulnerabilities
   C. Defending techniques from vulnerabilities
   D. Security application

11. What is Black Box testing?
   A. Pentesting with no knowledge
   B. Pentesting with complete knowledge
   C. Pentesting with partial knowledge
   D. Pentesting performed by Black Hat

12. What does TOE stand for?
   A. Type of Evaluation
   B. Time of Evaluation
   C. Term of Evaluation
   D. Target of Evaluation

13. The term "Vulnerability" refers to _____.
   A. A virus
   B. A malware
   C. An attack
   D. A weakness

14. "Adversary implanting a backdoor on a victim system to create persistency" is an action that belongs to which step of Cyber Kill Chain?
   A. Weaponization
   B. Exploitation
   C. Installation
   D. Command and Control

15. Which step of the Cyber Kill Chain establishes two-way communication between the victim's system and the adversary-controlled server?
    A. Exploitation
    B. Installation
    C. Command and Control
    D. Action on Objective

16. How many MITR ATT&CK matrices are there?
    A. Two
    B. Four
    C. Five
    D. Seven

17. Which of the following is a regulation in EU law on data protection?
    A. GDPR
    B. SOX
    C. HIPAA
    D. PCI-DSS

18. Depending on the positions offered in IT industries and companies, what is the legal form of hacking?
    A. Non-Ethical Hacking
    B. Cracking
    C. Hacktivism
    D. Ethical Hacking

19. Any company or organization's IT security is handled and maintained by _____.
    A. Software Security Specialist
    B. Cyber Security Intern
    C. IT Security Engineer
    D. Security Auditor

20. A _____ is an attempt to steal, spy on, harm, or destroy computer networks, systems, or the data they contain.
    A. Cyber attack
    B. Digital hacking
    C. Cyber security
    D. Computer Security

Answers

1. Answer: B

Explanation: Ethical Hackers always require legal permission.

2. Answer: B

Explanation: Gray Box is a type of penetration testing in which the pentester is provided with very limited prior knowledge of the system or any information on targets.

3. Answer: C

Explanation: White Hat Hackers always have legal permission to perform penetration testing against a target system.

4. Answer: C

Explanation: Hacktivists draw attention to the target to deliver a message or promote an agenda.

5. Answer: A

Explanation: Script Kiddies have no or very low knowledge about hacking.

6. Answer: C

Explanation: White Box testing requires complete knowledge of a target.

7. Answer: D

Explanation: Suicide Hackers are those who aim for destruction without worrying about punishment.

8. **Answer:** B and C

Explanation: Penetration testing is required in an environment to perform an audit, find vulnerabilities, and exploit them to address them before an attacker reaches them.

9. Answer: B

Explanation: Gray Hats are those who work for both offensively and defensively.

10. Answer: B

Explanation: A vulnerability assessment is a process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

11. Answer: A

Explanation: The Black Box is a type of penetration testing in which the pentester is blind testing, or double-blind testing, i.e., the pentester is provided with no prior knowledge of the system or any information about the target.

12. Answer: D

Explanation: TOE stands for Target of Evaluation. It is a term that is frequently used in the context of security and evaluations, particularly when assessing the security attributes and characteristics of a particular technology, system, or product. The TOE is the object of the assessment, which compares it to predetermined security standards or criteria to ascertain its security posture and if it complies with predetermined security requirements.

13. Answer: D

Explanation: Vulnerability is a weak point or loophole in any system or network which an attacker can exploit.

14. Answer: C

Explanation: Adversaries implant backdoors or create auto-run keys to maintain access. Such activities to maintain access to the victim are part of the installation step in the Cyber Kill Chain.

15. Answer: C

Explanation: In order to communicate and transfer data back and forth, command and control sets up two-way communication between the victim's system and the server under the control of the enemy.

16. Answer: B

Explanation: The four MITRE ATT&CK matrices in use right now are:

- **PRE-ATT&CK:** The stages of cyberattack life cycle known as PRE-ATT&CK are reconnaissance and weaponization. It is intended to assist an organization in identifying warning indicators that they might be the target of an attack as well as the data that an attacker might use to do so.
- **Enterprise:** The remainder of the cyberattack life cycle is covered by the enterprise matrix. It describes how an attacker could penetrate a business network and use it to conduct operations.
- **Mobile:** The same phases of the cyberattack life cycle are covered by the mobile matrix as they are by the enterprise matrix. The emphasis is on potential dangers and attack methods for mobile devices, though.
- **Industrial control system (ICS):** The ICS matrix describes the ways an attacker could access and use a network, including ICS devices.

17. Answer: A

Explanation: The General Data Protection Regulation (GDPR) is the biggest European Union legislation giving ordinary people and precedented control over how your data is collected, used, and forces companies to justify everything they do with it. It hugely affects businesses outside the EU, including the US.

As everything is moving their future toward the digital domain, the massive collection of sensitive data requires strict and protected regulations from holding them.

Any type of data that can identify you with your name, contact details, username, IP address, and location is required by the GDPR. The organizations will have to prove that they have a lawful reason for holding the particular kind of data.

18. Answer: D

Explanation: White-hat hackers use ethical hacking to conduct penetration tests and find possible threats inside of any organizations and businesses.

19. Answer: C

Explanation: This is a position at an intermediate level held by a person in an organization or firm who develops and maintains various systems and the related security tools of the firm or organization to which he or she belongs.

20. Answer: A

Explanation: A cyber-attack is an effort to steal, snoop on, harm, or destroy various cyberspace components, such as computer systems, related peripherals, network systems, and information.