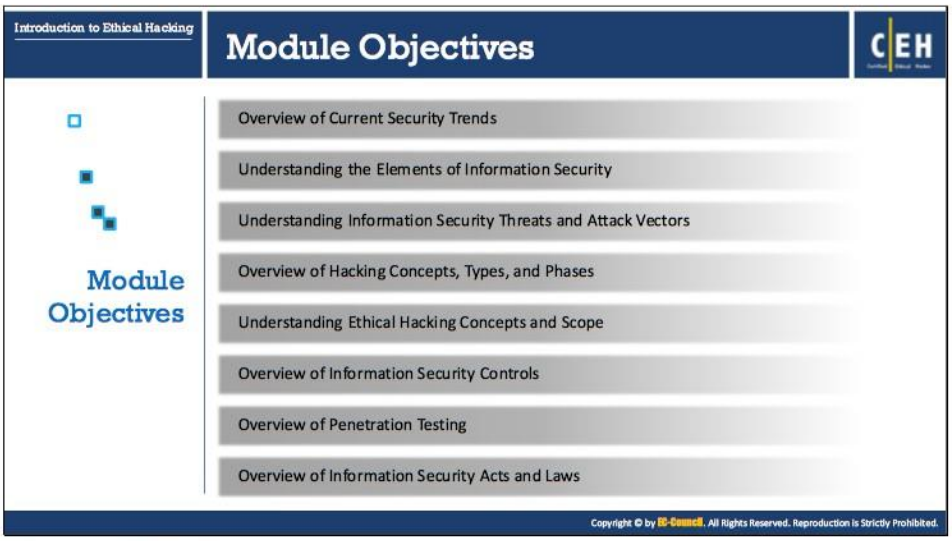


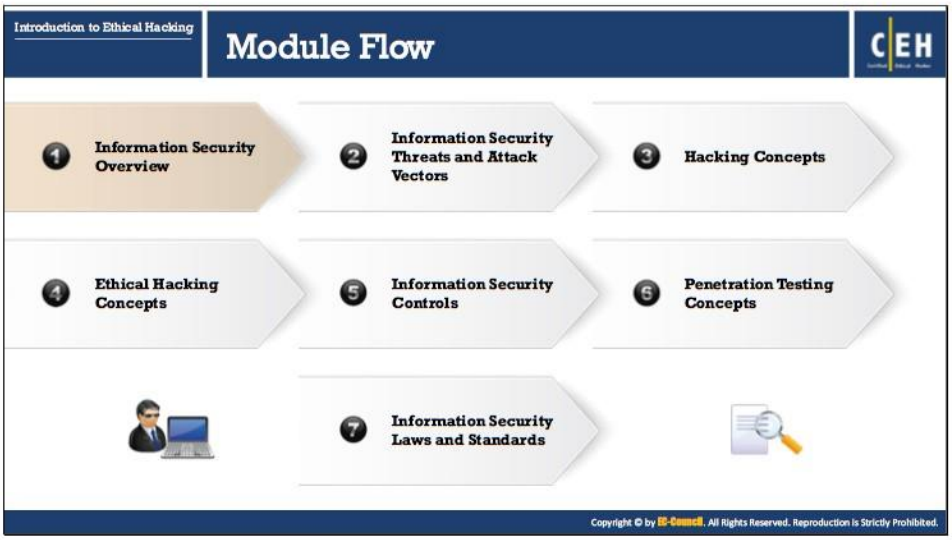
Module Objectives

Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems, and the probable reasons behind those attacks. As Sun Tzu states in the Art of War, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." It is the duty of system administrators and security professionals to guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seeks to use the same infrastructure for illegal activities.

This module starts with an overview of the current security scenario and emerging threat vectors. It provides an insight into the different elements of information security. Later the module discusses hacking and ethical hacking concepts and ends with a brief discussion on information security controls, penetration testing process, and information security laws and Acts.

At the end of this module, you will be able to:

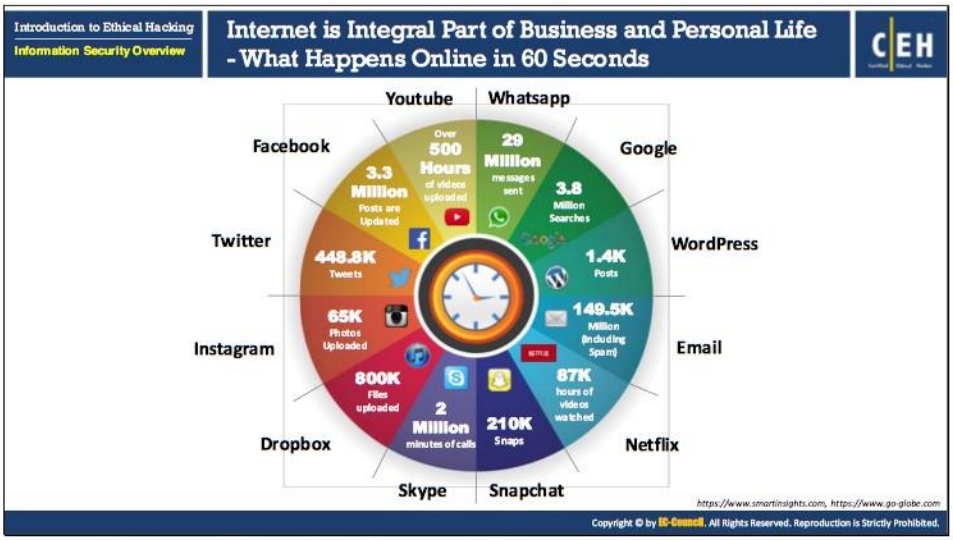
- Understand the current security trends
- Describe the elements of information security
- Explain information security threats and attack vectors
- Describe the hacking concepts, types, and phases
- Explain the ethical hacking concepts and scope
- Understand the information security controls (information security management, defense-in-depth, policies, procedures, awareness, physical security, incident management process, and risk management etc.)
- Understand the penetration testing process
- Know about the information security Acts and Laws



Information Security Overview

Information security refers to the protection or safeguard of information and information systems that use, store, and transmit information from unauthorized accesses, disclosures, alterations, and destructions. Information is the critical asset that organizations need to secure. If sensitive information falls in wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, etc. In an attempt to understand how to secure such critical information resources, let us start with an overview of information security.

This section covers various statistics, threat predictions, and essential terminology pertaining to information security, elements of information security, as well as the security, functionality, and usability triangle.

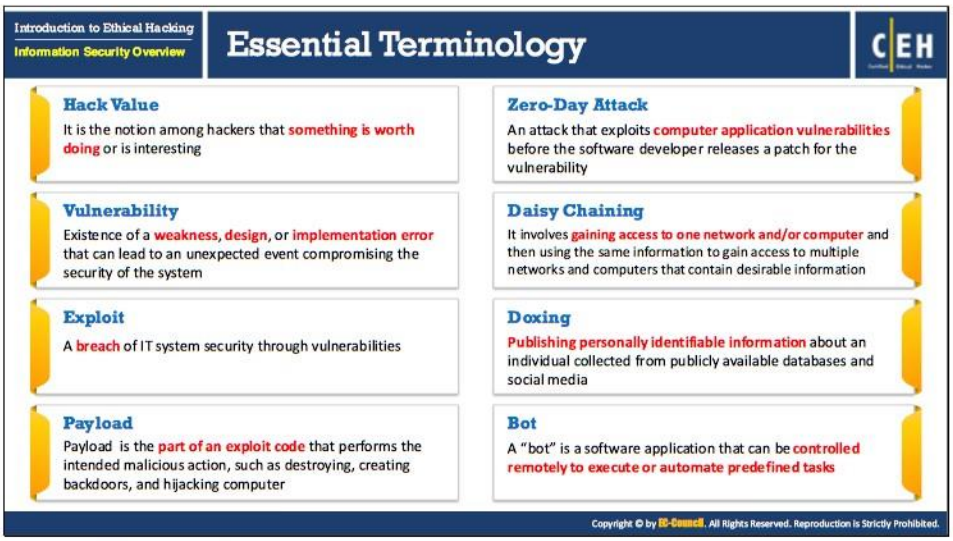


Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds

Source: *https://www.smartinsights.com*, *https://www.go-globe.com*

The Internet has become an integral part of modern business and personal life, as it helps in gaining information easily. Businesses and individuals rely on the Internet for various purposes such as browsing for content, social networking, communicating, shopping, downloading, and chatting, etc.

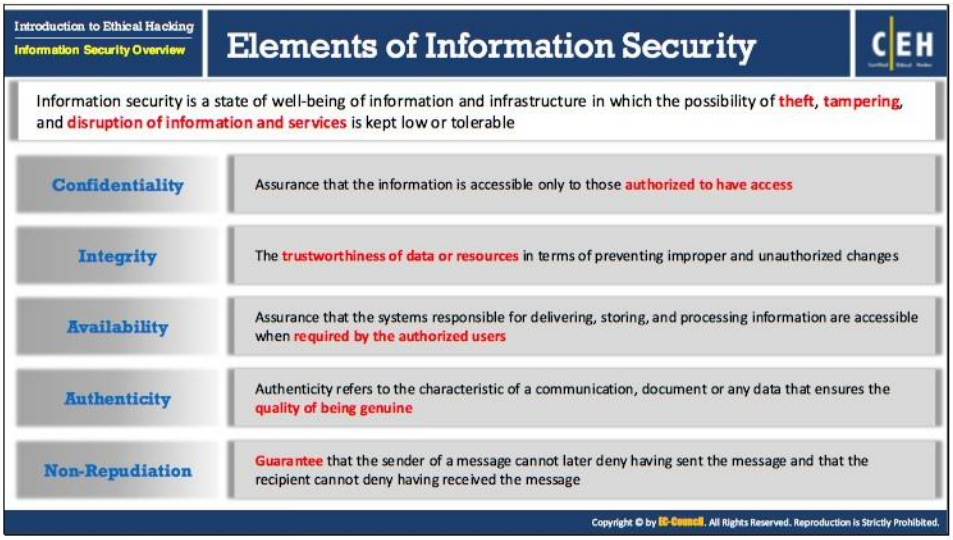
Currently there are approximately 3.81 billion Internet users around the world. It is general practice nowadays for a person to look for a particular solution on the Internet and find satisfaction from an appropriate solution. Along with the facility of finding various Internet services, one of the most important and popular rising topics of general interest nowadays is social networking websites. It is very common for people to use social networking websites for regular contact with friends and relatives. The image in the slide depicts what can happen online in just 60 seconds.



Essential Terminology

- **Hack Value:** Hack value is the notion among hackers to evaluate something that is worth doing or is interesting. Hackers derive great satisfaction from breaking down the toughest network security, and consider it their accomplishment as it is something that not everyone can do.
- **Vulnerability:** Vulnerability is the existence of weakness, design, or an implementation error that, when exploited, leads to an unexpected and undesirable event compromising the security of the system. Simply put, vulnerability is a security loophole that allows an attacker to enter the system by bypassing various user authentications.
- **Exploit:** An exploit is a breach of IT system security through vulnerabilities, in the context of an attack on a system or network. It also refers to malicious software or commands that can cause unanticipated behavior of legitimate software or hardware through attackers taking advantage of the vulnerabilities.
- **Payload:** Payload is the part of a malware or an exploit code that performs the intended malicious actions, which can include creating backdoor access to a victim's machine, damaging or deleting files, committing data theft and hijacking computer. Hackers use various methods to execute the payload. For example, they can activate a logic bomb, execute an infected program, or use an unprotected computer connected to a network.
- **Zero-Day Attack:** In a Zero-Day attack, the attacker exploits vulnerabilities in a computer application before the software developer can release a patch for them.
- **Daisy Chaining:** It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information.

- **Doxing:** Doxing refers to gathering and publishing personally identifiable information such as an individual's name and email address, or other sensitive information pertaining to an entire organization. People with malicious intent collect this information from publicly accessible channels such as the databases, social media and the Internet.
- **Bot:** A "bot" (a contraction of "robot") is a software application or program that can be controlled remotely to execute or automate predefined tasks. Hackers use bots as agents that carry out malicious activity over the Internet. Attackers use infected machines to launch distributed denial-of-service (DDoS) attacks, keylogging, spying, etc.



Elements of Information Security

Information security is defined as "a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable." It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to those who are authorized to have access. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper equipment disposal (i.e. of DVDs, CDs, etc.).

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only the authorized people can update, add, and delete data to protect its integrity).

- **Availability**

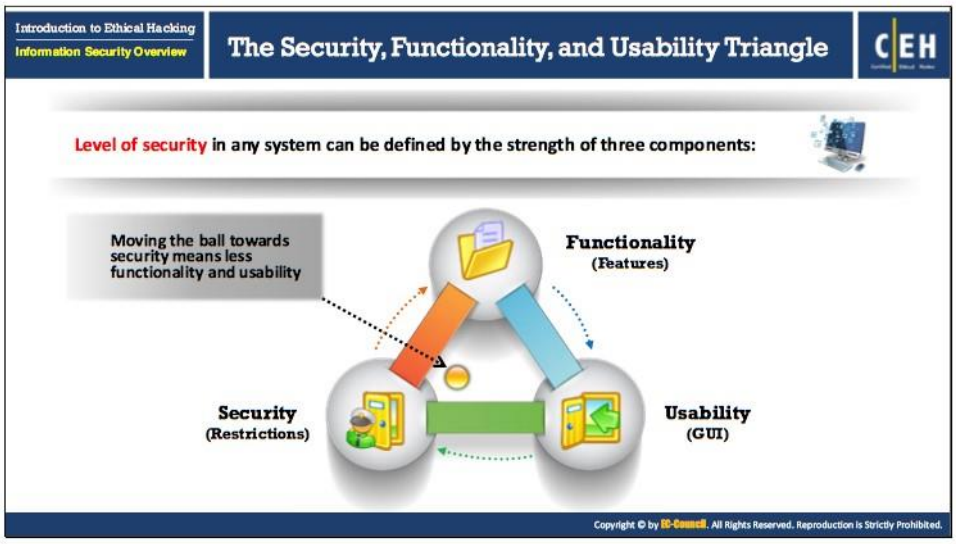
  Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include redundant systems' disk arrays and clustered machines, antivirus software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

  Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.



The Security, Functionality, and Usability Triangle

Technology is evolving at an unprecedented rate. As a result, new products that are reaching the market focus more on ease-of-use than on secure computing. Though technology was originally developed for "honest" research and academic purposes, it has not evolved at the same pace as users' proficiency. Moreover, in this evolution, system designers often overlook vulnerabilities during the intended deployment of the system. However, adding more built-in default security mechanisms allows users more competence. It is becoming difficult for system administrators and system security professionals to allocate resources, exclusively for securing systems, with the augmented use of computers for an increasing number of routine activities. This includes the time needed to check log files, detect vulnerabilities, and apply security update patches.

As routine activities consume system administrators' time, leaving less time for vigilant administration, there is little time to deploy measures and secure computing resources on a regular and innovative basis. This fact has increased the demand for dedicated security professionals to constantly monitor and defend ICT (Information and Communication Technology) resources.

Originally, to "hack" meant to possess extraordinary computer skills to explore hidden features of computer systems. In the context of information security, hacking is defined as the exploitation of vulnerabilities of computer systems and networks and requires great proficiency. However, today there are automated tools and codes available on the Internet that make it possible for anyone, who possesses the will, to succeed at hacking. However, mere compromise of system security does not denote hacking success. There are websites that insist on "taking back the Internet" as well as people who believe that they are doing everyone a

favor by posting details of their exploits. In reality, doing so serves to hamper the skill level required to become a successful attacker.

The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has decreased. The concept of the elite "super attacker" is an illusion. However, the fast-evolving genre of "script kiddies" is largely comprised of lesser-skilled individuals having second-hand knowledge of performing exploits. One of the main impediments contributing to the growth of security infrastructure lies in the unwillingness of exploited or compromised victims to report such incidents for fear of losing the goodwill and faith of their employees, customers, or partners, and/or of losing market share. The trend of information assets influencing the market has seen more companies thinking twice before reporting incidents to law enforcement officials for fear of "bad press" and negative publicity.

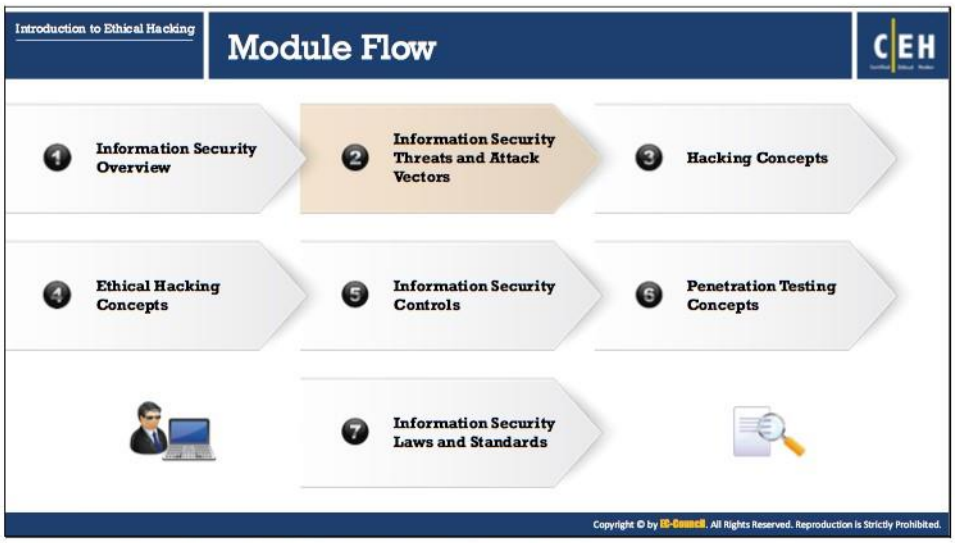
The increasingly networked environment, with companies often using their websites as single points of contact across geographical boundaries, makes it critical for administrators to take countermeasures to prevent exploits that can result in data loss. This is why corporations need to invest in security measures to protect their information assets.

Level of security in any system can be defined by the strength of three components:

- **Functionality**: The set of features provided by the system.
- **Usability**: The GUI components used to design the system for ease of use.
- **Security**: Restrictions imposed on accessing the components of the system.

The relationship between these three components is demonstrated by using a triangle because increase or decrease in any one of the component automatically affects the other two components. Moving the ball towards any of the three components means decreasing the intensity of other two components.

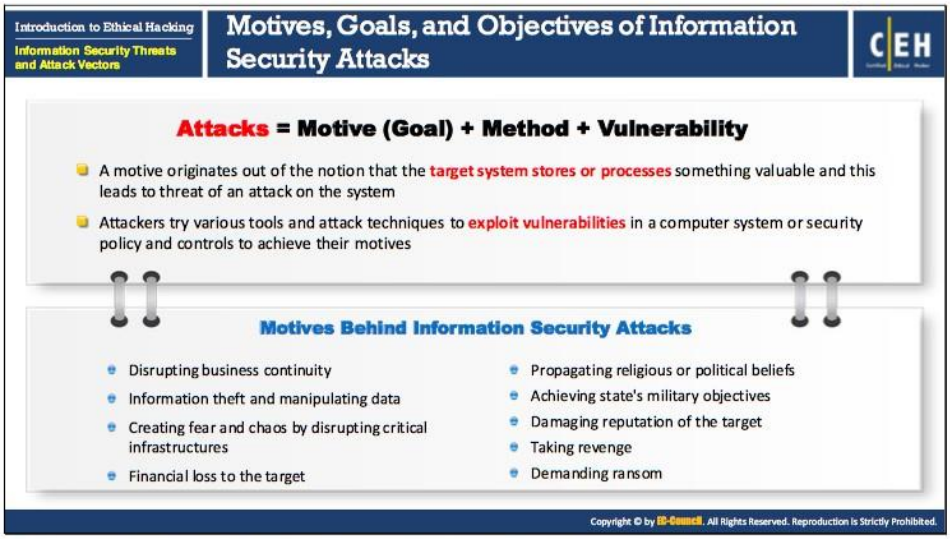
The diagram in the slide represents the relationship between functionality, usability, and security. For example, as shown in the slide above, if the ball moves towards Security it means increased security and decreased Functionality and Usability. If the ball is in the center of the triangle, then all the three components are balanced. If the ball moves towards usability it means an increased Usability and decreased Functionality as well as Security. For any implementation of security controls, all the three components have to be considered carefully and balanced to get acceptable functionality and usability with acceptable security.



Information Security Threats and Attack Vectors

There are various categories of information security threats, such as network threats, host threats, and application threats, and various attack vectors, such as viruses, worms, botnets, that might affect an organization's information security.

This section introduces you to the motives, goals, and objectives of information security attacks, top information security attack vectors, information security threat categories, and the types of attacks on a system.



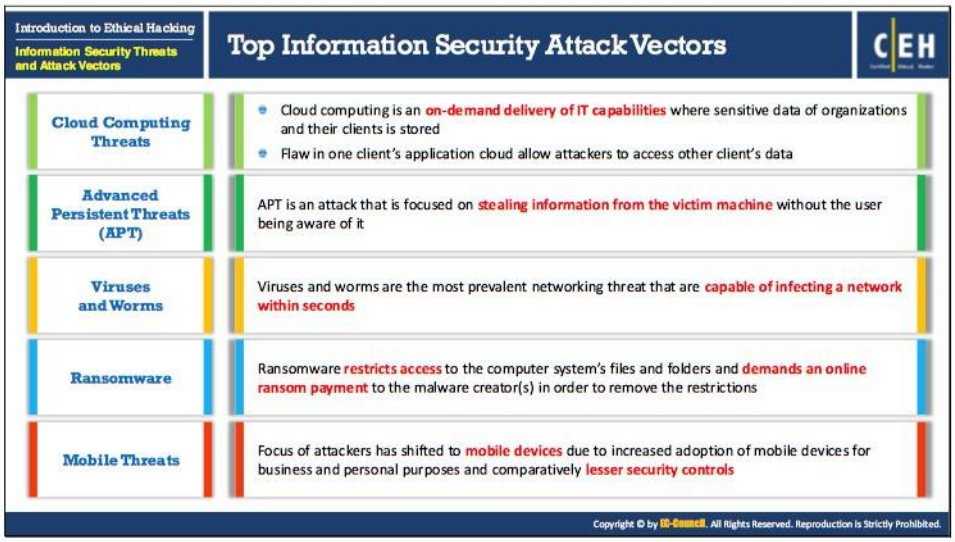
Motives, Goals, and Objectives of Information Security Attacks

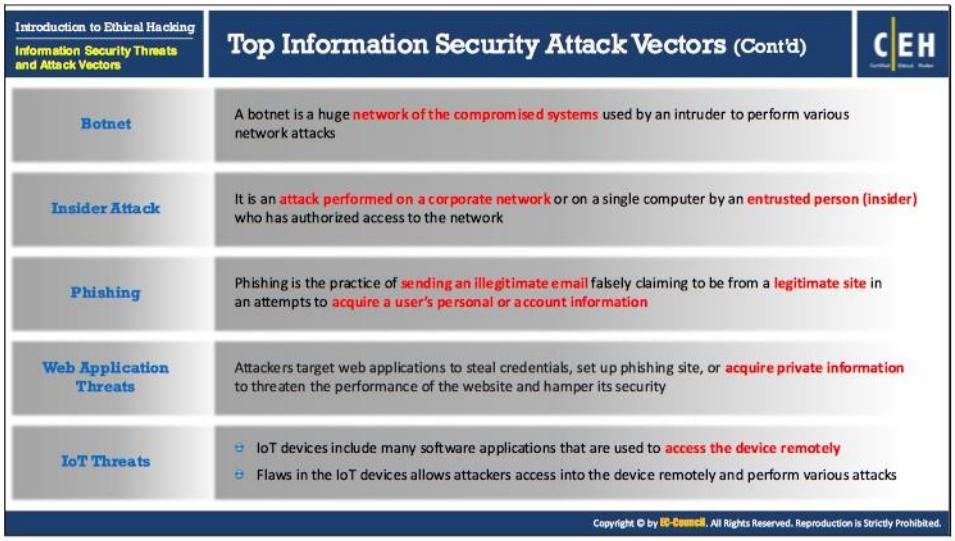
Attackers generally have motives (goals), and objectives behind information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, his/her reason for carrying out such an activity, as well as his/her resources and capabilities. Once the attacker determines his/her goal, he/she can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

- Disrupting business continuity
- Performing information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Bringing financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge
- Demanding ransom





Top Information Security Attack Vectors

Below is a list of information security attack vectors through which an attacker can gain access to a computer or network server to deliver a payload or malicious outcome.

- **Cloud Computing Threats:** Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as a metered service over a network. Clients can store sensitive information on the cloud. Flaw in one

client's application cloud could potentially allow attackers to access another client's data.

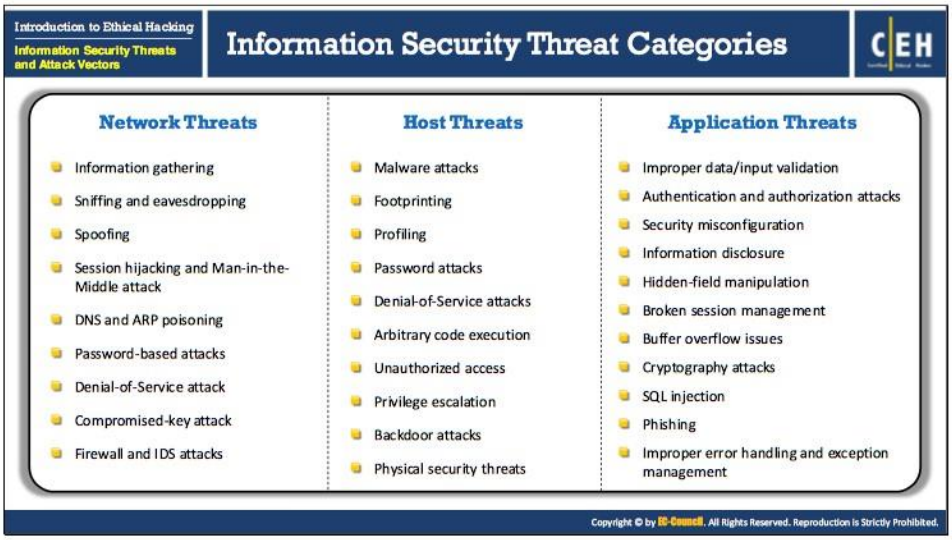
- **Advanced Persistent Threats (APT):** Advanced Persistent Threat (APT) is an attack that focuses on stealing information from the victim machine without its user being aware of it. These attacks are generally targeted at large companies and government networks. APT attacks are slow in nature, so the effect on computer performance and Internet connections is negligible. APTs exploit vulnerabilities in the applications running on a computer, operating system, and embedded systems.
- **Viruses and Worms:** Viruses and worms are the most prevalent networking threats, capable of infecting a network within seconds. A virus is a self-replicating program that produces a copy of itself by attaching to another program, computer boot sector or document. A worm is a malicious program that replicates, executes and spreads across network connections.

  Viruses make their way into the computer when the attacker shares a malicious file containing it with the victim through the Internet, or through any removable media. Worms enter a network when the victim downloads a malicious file, opens a spam mail or browses a malicious website.
- **Ransomware:** Ransomware is a type of a malware, which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions. It is generally spread via malicious attachments to email messages, infected software applications, infected disks or compromised websites.
- **Mobile Threats:** Attackers are increasingly focusing on mobile devices, due to the increased adoption of smart phones for business and personal use and their comparatively fewer security controls.

  Users may download malware applications (APKs) onto their smartphones, which can damage other applications and data and convey sensitive information to attackers. Attackers can remotely access a smartphone's camera and recording app to view user activities and track voice communications, which can aid them in an attack.
- **Botnet:** A botnet is a huge network of compromised systems used by attackers to perform denial-of-service attacks. Bots, in a botnet, perform tasks such as uploading viruses, sending mails with botnets attached to them, stealing data, and so on. Antivirus programs might fail to find—or even scan for—spyware or botnets. Hence, it is essential to deploy programs specifically designed to find and eliminate such threats.
- **Insider Attack:** An insider attack is an attack by someone from within an organization who has authorized access to its network and is aware of the network architecture.
- **Phishing:** Phishing is a practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. Attackers perform phishing attacks by distributing malicious links via some communication channel or mails to obtain private information like account numbers,

credit card numbers, mobile numbers, etc. from the victim. Attackers design emails to lure victims such a way that they appear to be from some legitimate source or at times they send malicious links that resemble a legitimate website.

- **Web Application Threats:** Web application attacks like SQL injection, cross-site scripting has made web applications a favorable target for the attackers to steal credentials, set up phishing site, or acquire private information. Majority of such attacks are the result of flawed coding and improper sanitization of input and output data from the web application. Web application attacks can threaten the performance of the website and hamper its security.
- **IoT Threats:** The IoT devices connected to the Internet have little or no security that makes them vulnerable to various types of attacks. These devices include many software applications that are used to access the device remotely. Due to the hardware constraints such as memory, battery, etc. these IoT applications do not include complex security mechanisms to protect the devices from attacks. These drawbacks make the IoT devices more vulnerable and allow attackers to access the device remotely and perform various attacks.



Information Security Threat Categories

There are three types of information security threats:

- **Network Threats**

  A network is the collection of computers and other hardware connected by communication channels to share resources and information. As the information travels from one system to the other through the communication channel, a malicious person might break into the communication channel and steal the information traveling over the network.

  Listed below are some of the network threats:

  - Information gathering
  - Sniffing and eavesdropping
  - Spoofing
  - Session hijacking
  - Man-in-the-Middle attack
  - DNS and ARP poisoning
  - Password-based attacks
  - Denial-of-Service attack
  - Compromised-key attack
  - Firewall and IDS attack

- **Host Threats**

  Host threats target a particular system on which valuable information resides. Attackers try to breach the security of the information system resource.

  Listed below are some of the host threats:

  - Malware attacks
  - Foot printing
  - Profiling
  - Password attacks

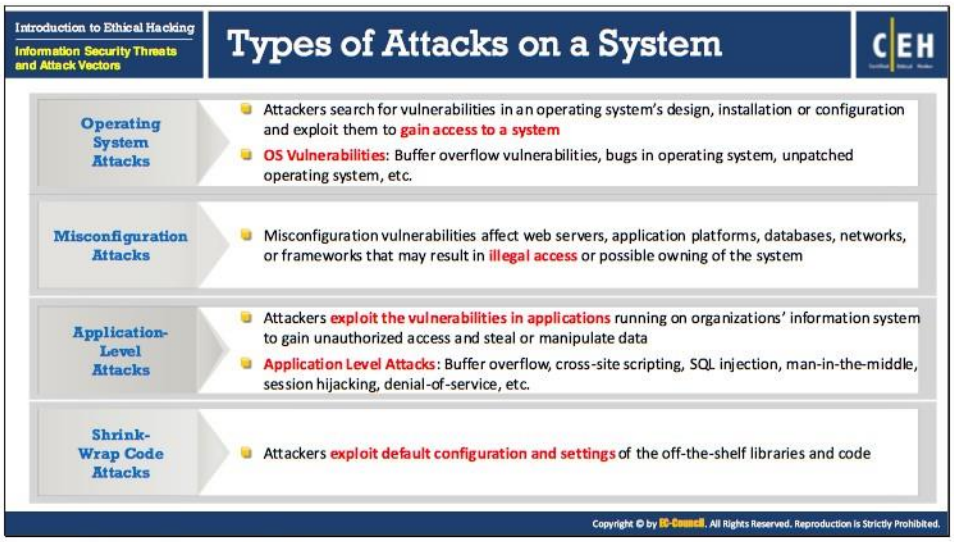
- Denial-of-Service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor attacks
- Physical security threats

- **Application Threats**

  Applications can be vulnerable if proper security measures are not taken while developing, deploying, and maintaining them. Attackers exploit the vulnerabilities present in an application to steal or destroy data.

  Listed below are some of the application threats:

  - Improper data/input validation
  - Authentication and authorization attacks
  - Security misconfiguration
  - Improper error handling and exception management
  - Information disclosure
  - Hidden-field manipulation
  - Broken session management
  - Buffer overflow issues
  - Cryptography attacks
  - SQL injection
  - Phishing



Types of Attacks on a System

Many approaches exist for an attacker to gain access to the system. One common requirement for all such approaches is that the attacker finds and exploits a system's weakness or vulnerability.

- **Operating System Attacks**

  Today's Operating Systems (OS) are loaded with features and are increasingly complex. While users take advantage of these features, they are prone to more vulnerabilities, thus enticing attackers. Operating systems run many services such as graphical user interfaces (GUIs) that support applications and system tools, and enable Internet access. Extensive tweaking is required to lock them down. Attackers constantly look for OS vulnerabilities that allow them to exploit and gain access to a target system or network. To stop attackers from compromising the network, the system or network administrators must keep abreast of various new exploits and methods adopted by attackers, and monitor the networks regularly.

  By default, most operating systems' installation programs install a large number of services and open ports. This situation leads attackers to search for vulnerabilities. Applying patches and hot fixes is not easy with today's complex networks. Most patches and fixes tend to solve an immediate issue. In order to protect the system from operating system attacks in general, it is necessary to remove and/or disable any unneeded ports and services.

  Some OS vulnerabilities include:

  - Buffer overflow vulnerabilities
  - Bugs in the operating system

- An unpatched operating system

Attacks performed at the OS level include:

- Exploiting specific network protocol implementations
- Attacking built-in authentication systems
- Breaking file-system security
- Cracking passwords and encryption mechanisms

- **Misconfiguration Attacks**

Security misconfiguration or poorly configured security controls might allow attackers to gain unauthorized access to the system, compromise files, or perform other unintended actions. Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in illegal access or possible system takeover. Administrators should change the default configuration of the devices before deploying them in the production network. To optimize the configuration of the machine, remove any unneeded services or software. Automated scanners detect missing patches, misconfigurations, use of default accounts, unnecessary services, and so on.

- **Application-Level Attacks**

Software developers are often under intense pressure to meet deadlines, which can mean they do not have sufficient time to completely test their products before shipping them, leaving undiscovered security holes. This is particularly troublesome in newer software applications that come with a large number of features and functionalities, making them more and more complex. An increase in the complexity means more opportunities for vulnerabilities. Attackers find and exploit these vulnerabilities in the applications using different tools and techniques to gain unauthorized access and steal or manipulate data.

Security is not always a high priority to software developers, and they handle it as an "add-on" component after release. This means that not all instances of the software will have the same level of security. Error checking in these applications can be very poor (or even nonexistent), which leads to:

- Buffer overflow attacks
- Sensitive information disclosure
- Cross-site scripting
- Session hijacking
- Man-in-the-middle attacks
- Denial-of-service attacks
- SQL injection attacks
- Phishing
- Parameter/form tampering
- Directory traversal attacks

Examples of Application-Level Attacks

- **Session Hijacking**

  Attackers may exploit session information in the vulnerable applications to perform session hijacking if the code implements a cookie less authentication. When the target tries to browse through a URL, the session or authentication token appears in the request URL instead of the secure cookie, to give access to the URL requested by the target. Here, an attacker using his or her skills and monitoring tools can hijack the targets' session and steal all sensitive information.

  Vulnerable Code

  Given below is the vulnerable code, which allows an attacker to perform session hijacking by exploiting the vulnerability present at the line 4.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseUri">
5:  </system.web>
6: </configuration>
```

  FIGURE 1.1: Session Hijacking Vulnerable Code

  Secure Code

  Use "UseCookies" instead of "UseUri" at line 4 in the above code to secure it from session hijacking attacks.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseCookies">
5:  </system.web>
6: </configuration>
```

  FIGURE 1.2: Session Hijacking Secure Code

- **Denial-of-Service**

  Denial of Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents legitimate use of its resources. In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.

  Vulnerable Code

  Shown below is the vulnerable code that allows an attacker to perform a denial-of-service attack, as it fails to release a connection resource.

```
1:  Statement stmnt = conn.createStatement ();
2:  ResultSet rsltset = stmnt.executeQuery ();
3:  stmnt.close ();
```

FIGURE 1.3: Denial-of-Service Vulnerable Code

Secure Code

You can use a "**`finally`**" block to secure the above code.

```
1:  Statement stmnt;
2:  try {stmnt = conn.createStatement ();
3:  stmnt.executeQuery (); }
4:  finally {
5:  If (stmnt! = null) {
6:  try { stmnt.close ();
7:  } catch (SQLException sqlexp) { }
8:  } catch (SQLException sqlexp) { }
```

FIGURE 1.4: Denial-of-Service Secure Code

- **Shrink-Wrap Code Attacks**

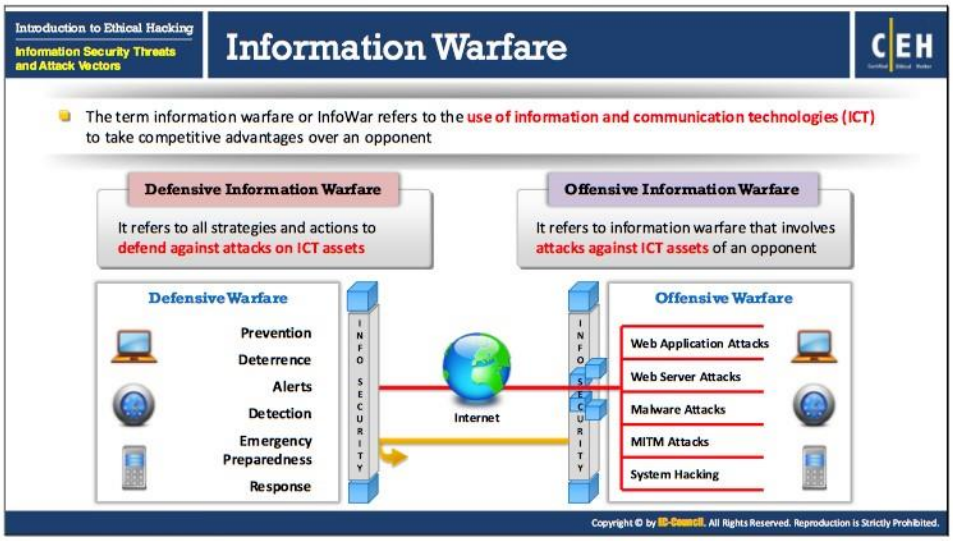
  Software developers often use free libraries and code licensed from other sources in their programs to reduce development time and cost. This means that large portions of many pieces of software will be the same, and if an attacker discovers vulnerabilities in that code, many pieces of software are at risk.

  Attackers exploit default configuration and settings of the off-the-shelf libraries and code. The problem is that software developers leave the libraries and code unchanged. They need to customize and fine-tune every part of their code in order to make it not only more secure, but different enough so that the same exploit will not work.

  Example of shrink-wrap code:

```
go_to = 'http://www3.strongdefenseiz.in/?g2cy6v=16fM3XOrqai1ld7QyKKZi9rmopqq12mJ7arisNmjoqPL1pibnaesiQ%3D%3D';
num_days = 4;
function ged(noDays){
    var today = new Date();
    var expr = new Date(today.getTime() + noDays*24*60*60*1000);
    return  expr.toGMTString();
}

function readCookie(cookieName){

    var start = document.cookie.indexOf(cookieName);
    if (start == -1){
document.cookie = "seenit88=yes; expires=" + ged(num_days);
window.location = go_to;

    } else {
    }
}

var lang = (navigator.language || navigator.systemLanguage || navigator.userLanguage || 'en').substr(0, 2).toLowerCase();
if (window.navigator.userAgent.indexOf ("MSIE") >= 0){
if(lang == 'en' || lang == 'de' || lang == 'fr' || lang == 'it' || lang == 'pl' || lang == 'br'){
window.onFocus=readCookie("seenit88");

}
}
```

FIGURE 1.5: An Example of Shrink-Wrap Code



Information Warfare

Source: *http://www.iwar.org.uk*

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nano machines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki has divided information warfare into the following categories:

- **Command and control warfare (C2 warfare):** In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare:** Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, "intelligence-based warfare" is a warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space.
- **Electronic warfare:** According to Libicki, electronic warfare uses radio electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare:** Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in the battle.

- **Hacker warfare:** According to Libicki, the purpose of this type of warfare can vary from shutdown of systems, data errors, theft of information, theft of services, system monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.
- **Economic warfare:** According to Libicki, economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyber warfare:** Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare and includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes the system over and the system will be perceived as operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of the information warfare, mentioned above, consists of both defensive and offensive strategies.

- **Defensive Information Warfare**: Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare:** Involves attacks against ICT assets of an opponent.

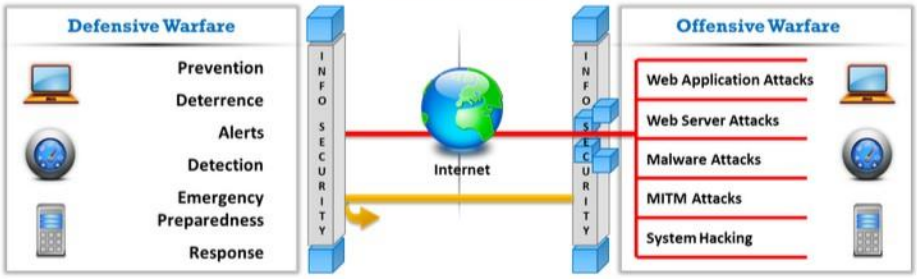
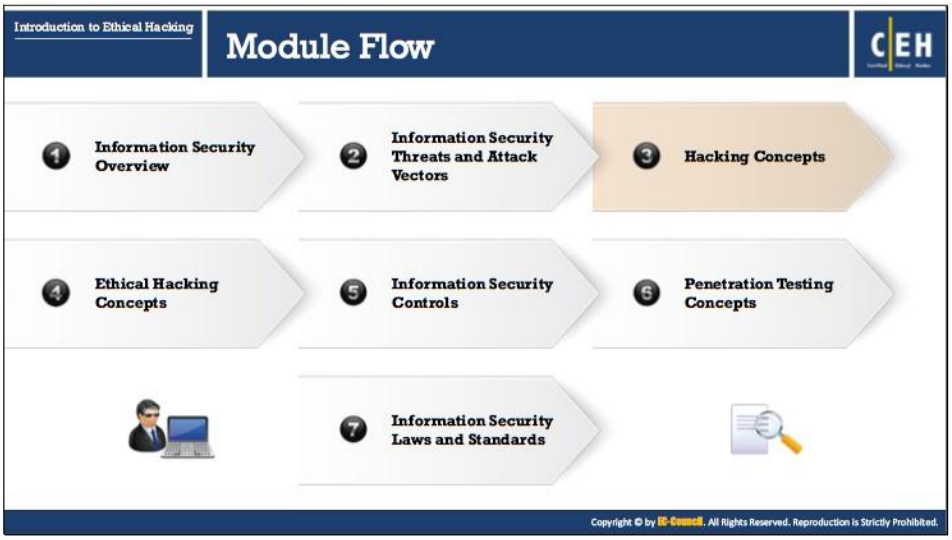
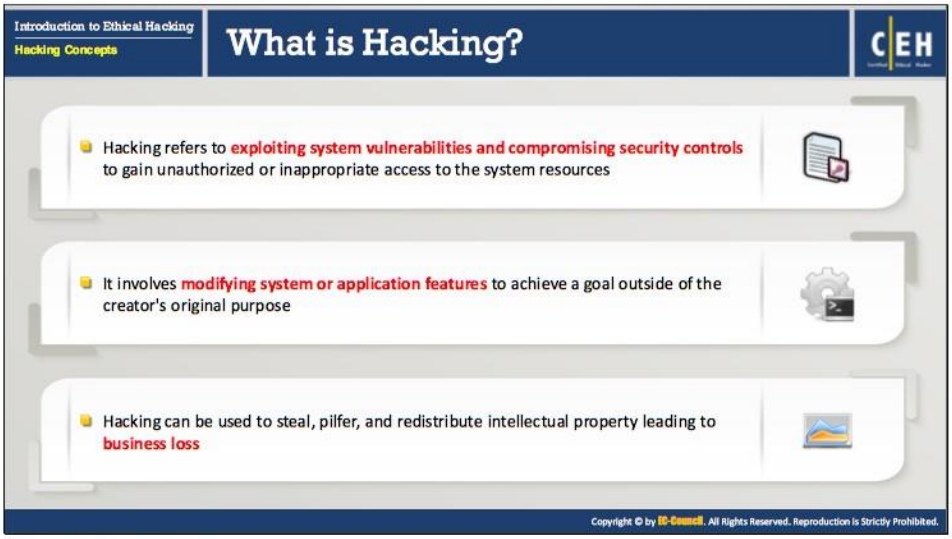


FIGURE 1.6: Block Diagram of Information Warfare



Hacking Concepts

This section deals with basic concepts of hacking: what is hacking, who is a hacker, and hacker classes—the five distinct hacking phases that one should be familiar with before proceeding with ethical hacking methodology.



What is Hacking?

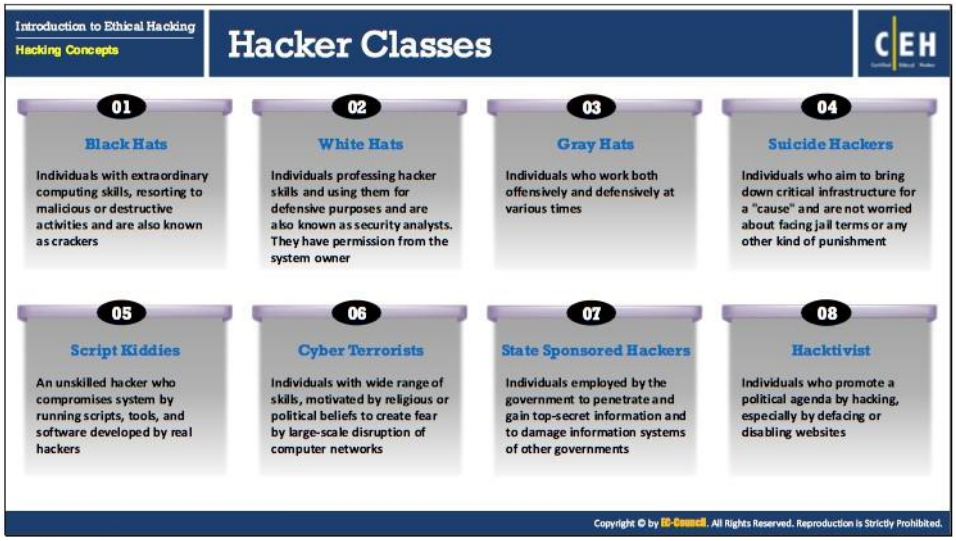
Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, and redistribute intellectual property, thus leading to business loss.

Hacking on computer networks is generally done by means of scripts or other network programming. Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using Trojans/backdoors, creating botnets, packet sniffing, phishing, and password cracking. The motive behind hacking could be to steal critical information and/or services, for thrill, intellectual challenge, curiosity, experiment, knowledge, financial gain, prestige, power, peer recognition, vengeance and vindictiveness, and so on.

Who is a Hacker?

A hacker is a person, who breaks into a system or network without any authorization to destroy, steal sensitive data, or performs malicious attacks. Hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore into the computer's software and hardware. Usually a hacker would be a skilled engineer or programmer with enough knowledge to discover vulnerabilities in a target system. She/he is generally a subject expert and enjoys learning the details of various programming languages and computer systems.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can be either to gain knowledge or to poke around to do illegal things. Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.



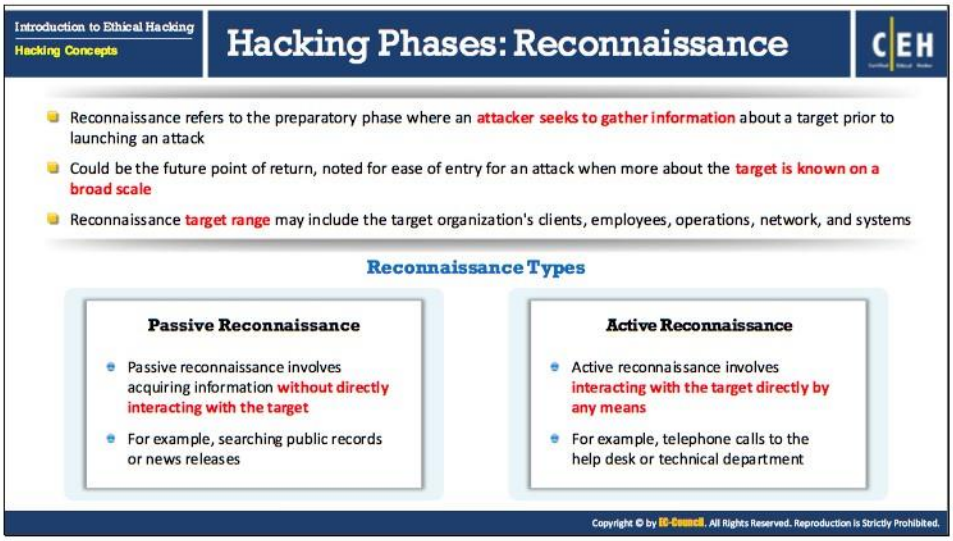
Hacker Classes

Hackers usually fall into one of the following categories, according to their activities:

- **Black Hats:** Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved with criminal activities. They are also known as crackers.
- **White Hats:** White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats:** Gray hats are the individuals who work both offensively and defensively at various times. Gray hats fall between white and black hats. Gray hats might help hackers in finding various vulnerabilities of a system or network and at the same time help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- **Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment. Suicide hackers are similar to suicide bombers, who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.
- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity of attacks rather than the quality of the attacks that they initiate.

- **Cyber Terrorists:** Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs to create fear of large-scale disruption of computer networks.
- **State Sponsored Hackers:** State sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments.
- **Hacktivist:** Hacktivism is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as themselves, in both the online and offline arenas. They are individuals who promote a political agenda by hacking, especially by defacing or disabling websites.

  Common hacktivist targets include government agencies, multinational corporations, or any other entity that they perceive as a threat. It remains a fact, however, that gaining unauthorized access is a crime, irrespective of their intentions.



Hacking Phases

In general, there are five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phase: Reconnaissance

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

This phase allows attackers to plan the attack. This may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using whatever personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target.

Another reconnaissance technique is dumpster diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information. Attackers can use the Internet to obtain information such as employees' contact information, business partners, technologies currently in use, and other critical business knowledge. But dumpster diving may provide them with even more sensitive information, such as user names, passwords, credit card statements, bank statements, ATM receipts, Social Security numbers, private telephone numbers, checking account numbers, and any number of other things.

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

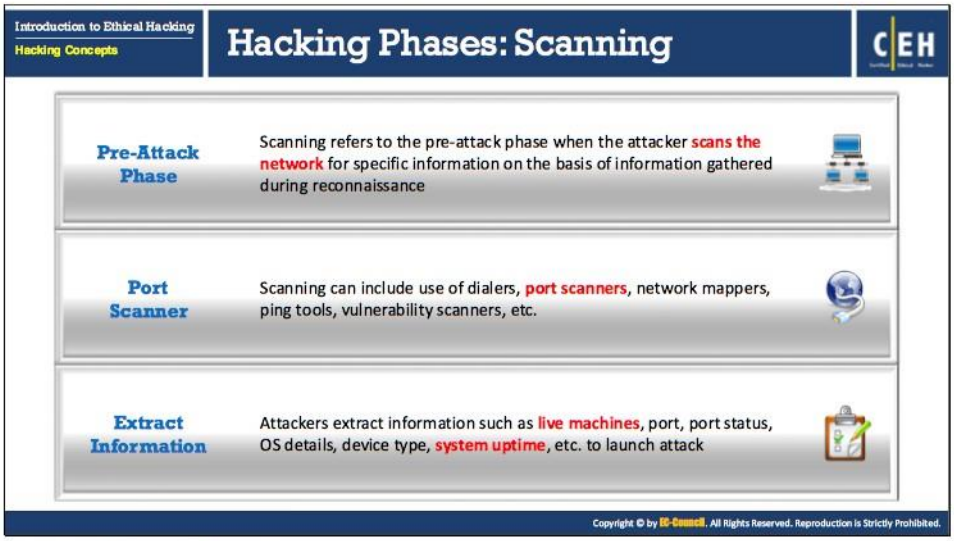
Reconnaissance Types

Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, she/he does not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, etc.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Attackers use active reconnaissance when there is a low probability of detection of these activities. For example, telephone calls to the help desk or technical department.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and/or operational strategy, and be equipped with the proper policies and procedures to check for potential vulnerabilities.



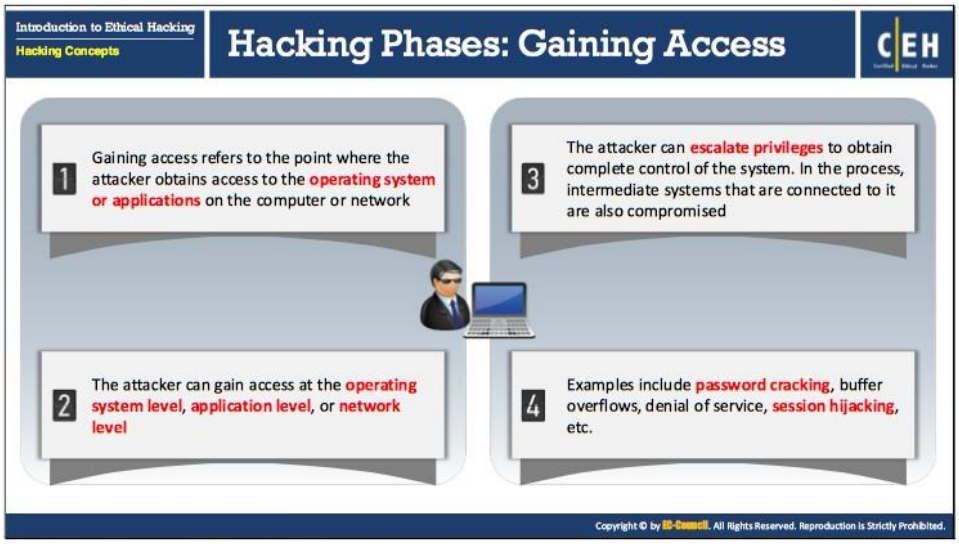
Hacking Phase: Scanning

Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute. Alternatively, they can use tools such as Cheops to add additional information to Traceroute's results.

Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc. Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack.

Port scanners detect listening ports to find information about the nature of services running on the target machine. The primary defense technique against port scanners is to shut down services that are not required, as well as to implement appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant, because attackers can and will use evasion techniques at every step of the way.

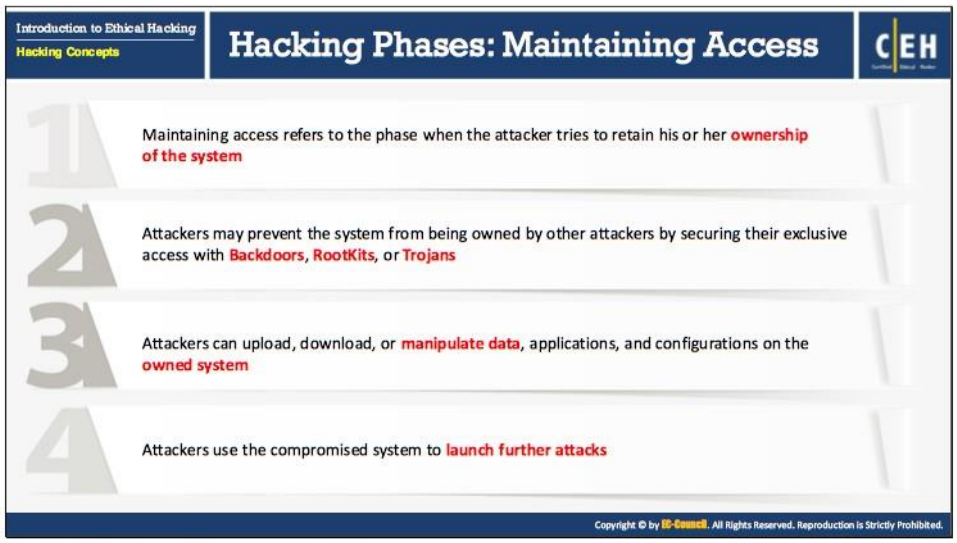


Hacking Phase: Gaining Access

This is the phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phase to gain access to the target system and network. Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network. The attacker can gain access at the operating system level, application level, or network level. Even though attackers can cause plenty of damage without gaining any access to the system, the impact of unauthorized access is catastrophic. For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Ending processes can stop a service, using a logic bomb or time bomb, or even reconfiguring and crashing the system. Thus attackers can exhaust system and network resources by consuming all outgoing communication links.

Attackers gain access to the target system locally (offline), over a LAN, or over the Internet. Examples include password cracking, stack-based buffer overflows, denial-of-service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability. Packet flooding also breaks the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous.

A hacker's chances of gaining access into a target system depend on several factors, such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, he/she then tries to escalate privileges in order to take complete control of the target system. In the process, intermediate systems that are connected to it are also compromised.

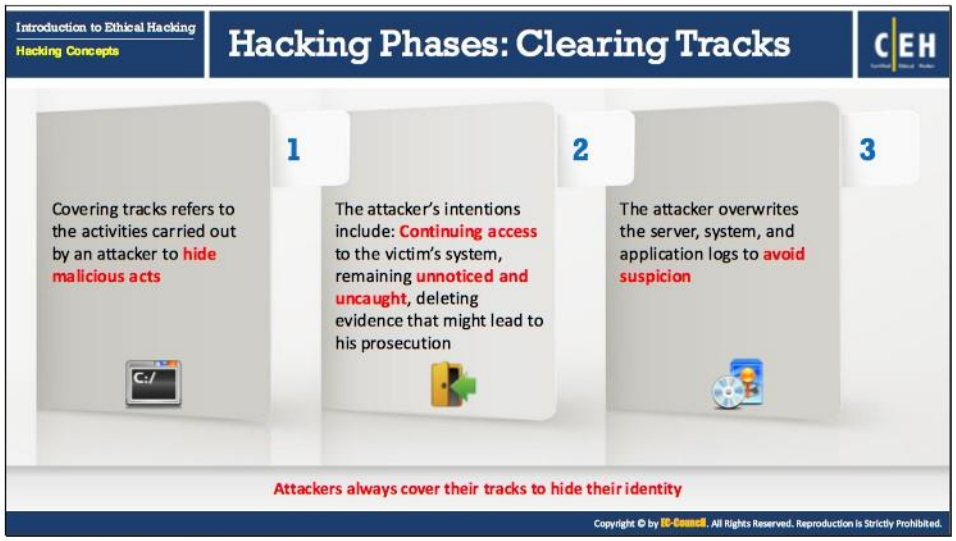


Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system. Once an attacker gains access to the target system with admin/root level privileges (thus owning the system), he or she is able to use both the system and its resources at will, and can either use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can cause a great amount of damage. For instance, the hacker could implement a sniffer to capture all network traffic, including Telnet and FTP (file transfer protocol) sessions with other systems, and then transmit that data wherever he or she pleases.

Attackers who choose to remain undetected remove evidence of their entry and install a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits gain access at the operating system level, while a Trojan horse gains access at the application level. Both rootkits and Trojans require users to install them locally. In Windows systems, most Trojans install themselves as a service and run as local system, with administrative access.

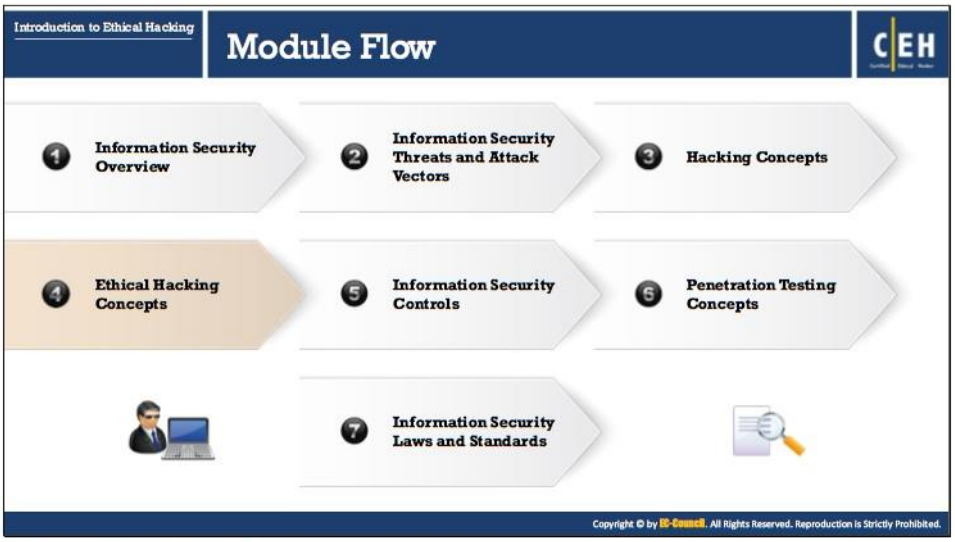
Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and can also use Trojans to transfer user names, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control from them, and sometimes, in the process, render some degree of protection to the system from other attacks. Attackers use the compromised system to launch further attacks.



Hacking Phase: Clearing Tracks

For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker's intentions include continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his/her prosecution. They use utilities such as PsTools (*https://docs.microsoft.com*) tools or Netcat or Trojans to erase their footprints from the system's log files. Once the Trojans are in place, the attacker has most likely gained total control of the system and can execute scripts in the Trojan or rootkit to replace critical system and log files to hide their presence in the system. Attackers always cover their tracks to hide their identity.

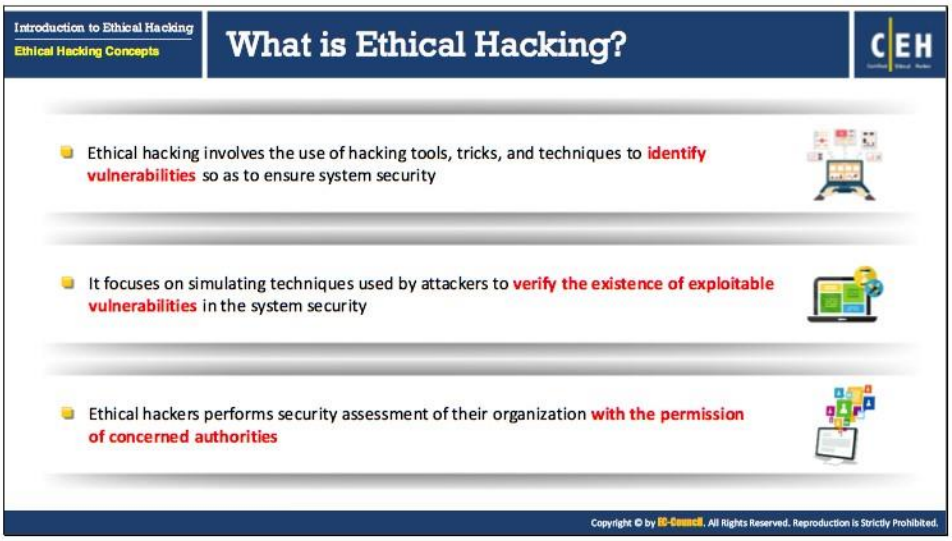
Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the data packet's TCP and IP headers to hide information. An attacker can use the compromised system to launch new attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of the attack can turn into another attack's reconnaissance phase. System administrators can deploy host-based IDS (intrusion detection systems) and antivirus software in order to detect Trojans and other seemingly compromised files and directories. As an ethical hacker, you must be aware of the tools and techniques that attackers deploy, so that you are able to advocate and implement countermeasures, detailed in subsequent modules.



Ethical Hacking Concepts

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain access to a computer system are similar irrespective of the hacker's intensions.

This section provides an overview of ethical hacking, why ethical hacking is necessary, the scope and limitations of ethical hacking, and the skills of an ethical hacker.



What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (private companies, universities, government organizations, etc.) are hiring White Hats to assist them in enhancing their cyber security. They perform hacking in ethical ways, with the permission of the network/system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system. Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker, to verify the existence of exploitable vulnerabilities in the system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

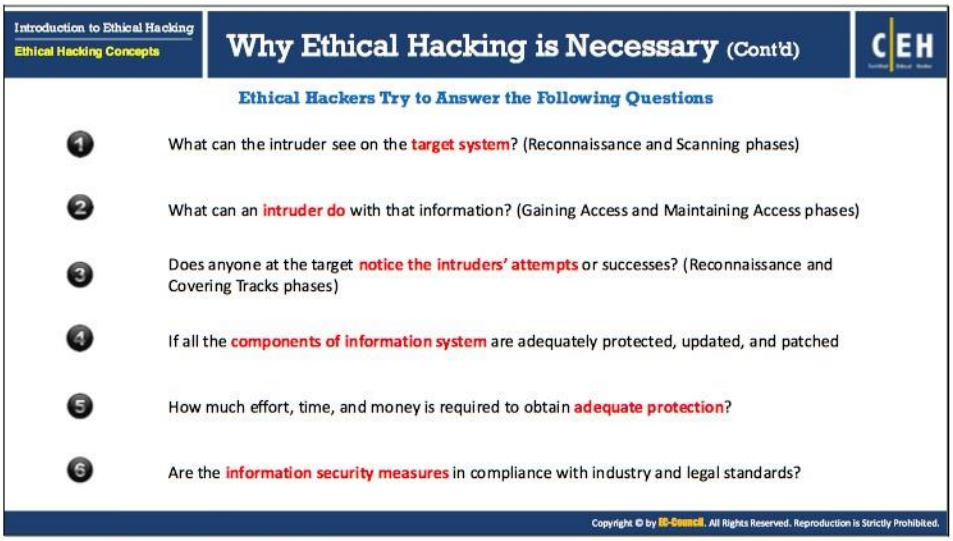
- The noun "hacker" refers to a person who enjoys learning the details of computer systems and stretching his or her capabilities.
- The verb "to hack" describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms "cracker" and "attacker" refer to persons who employ their hacking skills for offensive purposes.

- The term "ethical hacker" refers to security professionals who employ their hacking skills for defensive purposes.

Most companies use IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploits, and can recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers are attempting to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is therefore always legal.



Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. To beat a hacker, you need to think like one!

Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system. Ethical hacking helps to predict the various possible vulnerabilities well in advance and rectify them without incurring any kind of attack from outsiders. As hacking involves creative thinking, vulnerability testing and security

audits cannot ensure that the network is secure. To achieve security, organizations need to implement a "defense-in-depth" strategy by penetrating their networks to estimate vulnerabilities and expose them.

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard customer's data available in business transactions
- To enhance security awareness at all levels in a business

An ethical hacker's evaluation of a client's information system security seeks answers to three basic questions:

1. **What can an attacker see on the target system?**

   Normal security checks by system administrators will often overlook several vulnerabilities. An ethical hacker will have to think about what an attacker would see during the reconnaissance and scanning phases of an attack.

2. **What can an intruder do with that information?**

   The ethical hacker needs to discern the intent and purpose behind the attacks to determine appropriate countermeasures. During the gaining-access and maintaining-access phases of an attack, the ethical hacker needs to be one step ahead of the hacker in order to provide adequate protection.

3. **Are the attackers' attempts being noticed on the target systems?**

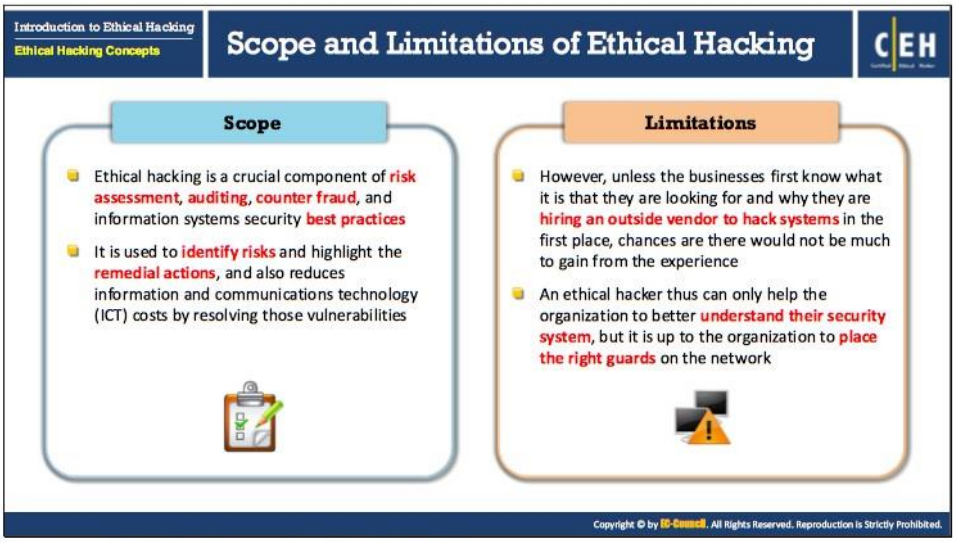
   Sometimes attackers will try for days, weeks, or even months to breach a system. Other times they will gain access, but will wait before doing anything damaging, instead take their time in assessing the potential use of exposed information. During the reconnaissance and covering tracks phases, the ethical hacker should notice and stop the attack.

After carrying out attacks, hackers may clear their tracks by modifying log files and creating backdoors, or by deploying Trojans. Ethical hackers need to investigate whether such activities have been recorded and what preventive measures have been taken. This not only provides them with an assessment of the attacker's proficiency, but also gives them insight into the existing security measures of the system being evaluated. The entire process of ethical hacking and subsequent patching of discovered vulnerabilities depends on questions such as:

- What is the organization trying to protect?
- Against whom or what are they trying to protect it?
- Are all the components of information system adequately protected, updated, and patched?

- How much time, effort, and money is the client willing to invest to gain adequate protection?
- Are the information security measures in compliance to industry and legal standards?

Sometimes, in order to save on resources or prevent further discovery, the client might decide to end the evaluation after the first vulnerability is found; therefore, it is important that the ethical hacker and the client work out a suitable framework for investigation beforehand. The client must be convinced of the importance of these security exercises through concise descriptions of what is happening and what is at stake. The ethical hacker must also remember to convey to the client that it is never possible to guard systems completely, but they can always be improved.



Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target.

Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit and is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices. It is used to identify risks and highlight remedial actions, and also to reduce Information and Communications Technology (ICT) costs by resolving those vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client's security concerns. Many ethical hackers are members of a "Tiger Team." A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization. Ethical hackers need to be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill the ethical and moral obligations. An ethical hacker must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the

test. The information gathered might contain sensitive information and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client, and discuss the needs to be addressed during the testing.
- Prepare and sign NDA documents with the client.
- Organize an ethical hacking team, and prepare a schedule for testing.
- Conduct the test.
- Analyze the results of the testing, and prepare a report.
- Present the report findings to the client.

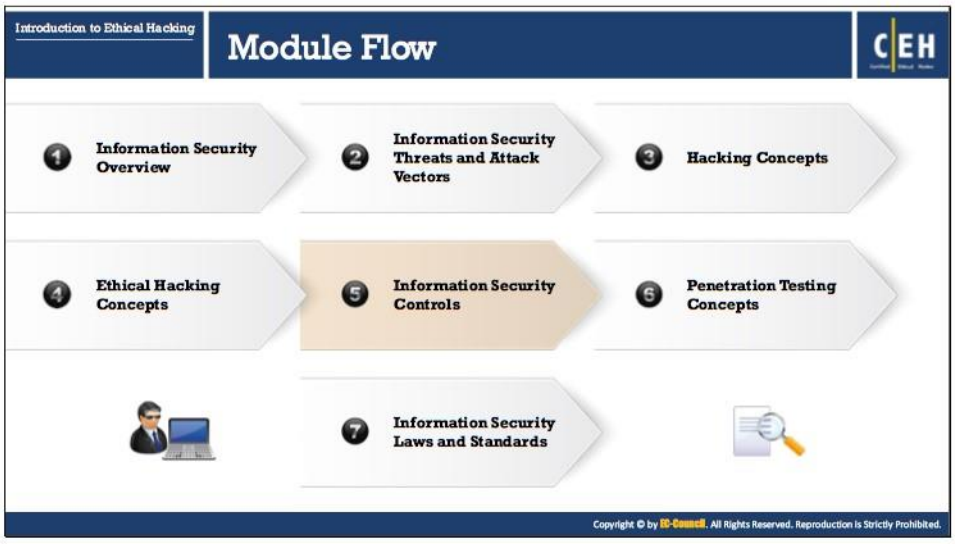
However, there are limitations too. Unless the businesses first know what they are looking for and why they are hiring an outside vendor to hack systems in the first place; chances are there would not be much to gain from the experience. An ethical hacker thus can only help the organization to better understand their security system, but it is up to the organization to place the right guards on the network.

Skills of an Ethical Hacker

It is essential for an ethical hacker to acquire knowledge and skills to become an expert hacker and use this knowledge in a lawful manner. The technical and non-technical skills to be a good ethical hacker are discussed below:

- **Technical Skills**
  - In-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
  - In-depth knowledge of networking concepts, technologies and related hardware and software
  - A computer expert adept at technical domains
  - Knowledge of security areas and related issues
  - High technical knowledge to launch the sophisticated attacks
- **Non-Technical Skills**

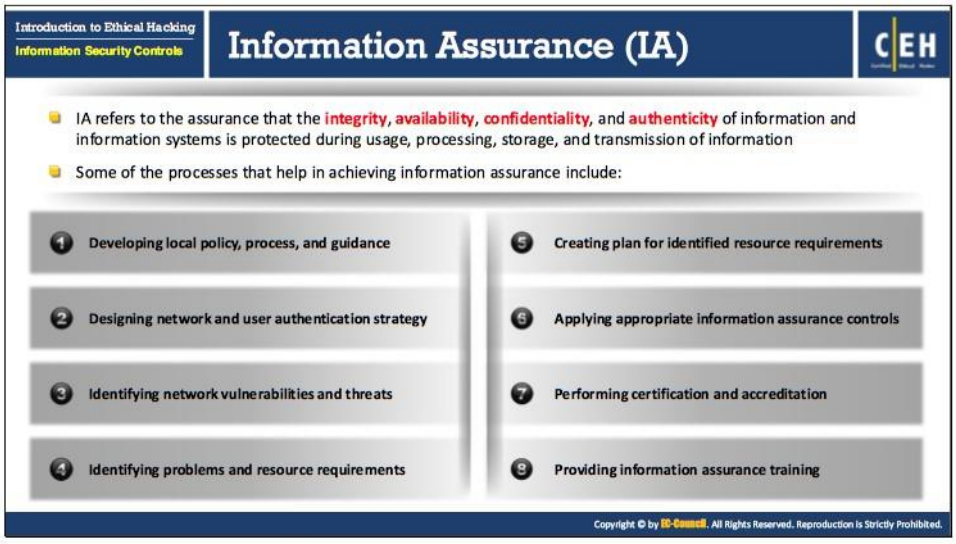
  Some of the non-technical characteristics of an ethical hacker include:
  - Ability to quickly learn and adapt new technologies
  - Strong work ethics and good problem solving and communication skills
  - Commitment to an organization's security policies
  - Awareness of local standards and laws



Information Security Controls

Information security controls prevent the occurrence of unwanted events and reduce risk to the organization's information assets. The basic security concepts critical to information on the Internet are confidentiality, integrity, and availability; those related to the persons accessing information are authentication, authorization, and non-repudiation. Information is the greatest asset to an organization, and it is a must to secure it by means of, for example, various policies, creating awareness, and employing security mechanisms.

This section deals with Information Assurance (IA), defense-in-depth, information security policies, physical security, risk management, threat modeling, incident management, access controls, Identity and Access Management (IAM), data loss prevention, data backup and recovery, and others.

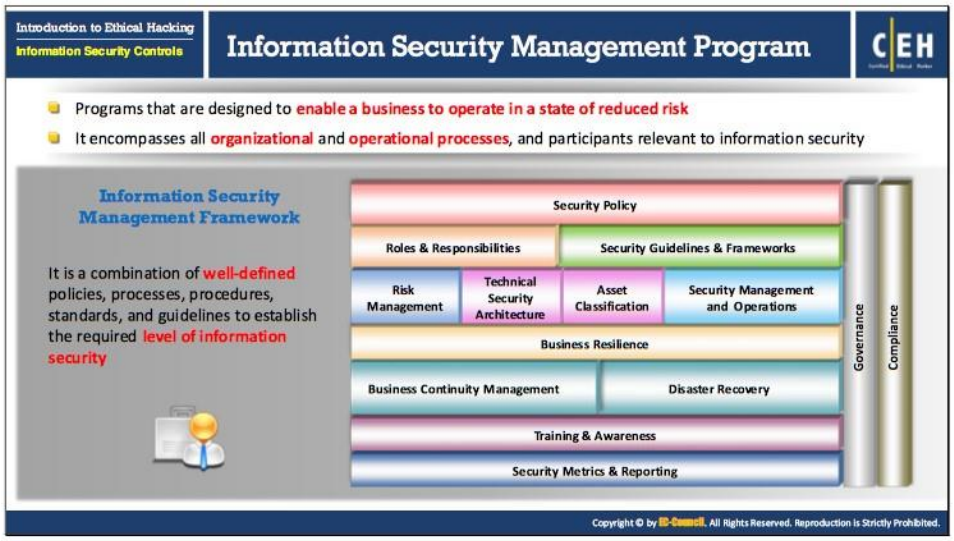


Information Assurance (IA)

IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during usage, processing, storage, and transmission of information. Security experts accomplish the information assurance with the help of physical, technical, and administrative controls. Information Assurance and Information Risk Management (IRM) ensures that only authorized personnel access and use information. This helps in achieving information security and business continuity.

Some of the processes that help in achieving information assurance include:

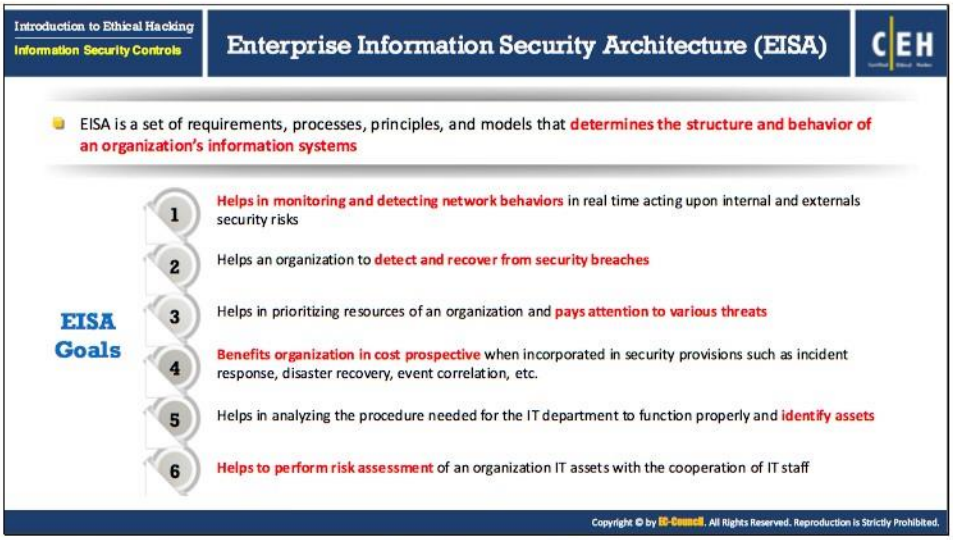
- Developing local policy, process, and guidance in such a way that the information systems are maintained at an optimum security level.
- Designing network and user authentication strategy — A secure network ensures the privacy of user records and other information on the network. Implementing an effective user authentication strategy secures the information systems data.
- Identifying network vulnerabilities and threats — Vulnerability assessments outline the security posture of the network. Performing vulnerability assessments in search of network vulnerabilities and threats help to take proper measures to overcome them.
- Identifying problems and resource requirements.
- Creating plan for identified resource requirements.
- Applying appropriate information assurance controls.
- Performing Certification and Accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them.
- Providing information assurance training to all personnel in federal and private organizations brings among them an awareness of information technology.



Information Security Management Program

Today's information security management programs encompass more than just firewalls and passwords. They are organization-wide programs that enable the business to operate in a state of reduced risk. Information security should be an ongoing process that—when fully developed—will position an organization to address the right security issues, so that the business can fulfill its objectives. The effective management of information security in an organization or enterprise encompasses all organizational and operational processes and participants relevant to information security.

The Information Security Management Framework is a combination of well-defined policies, processes, procedures, standards, and guidelines needed to establish the required level of information security.



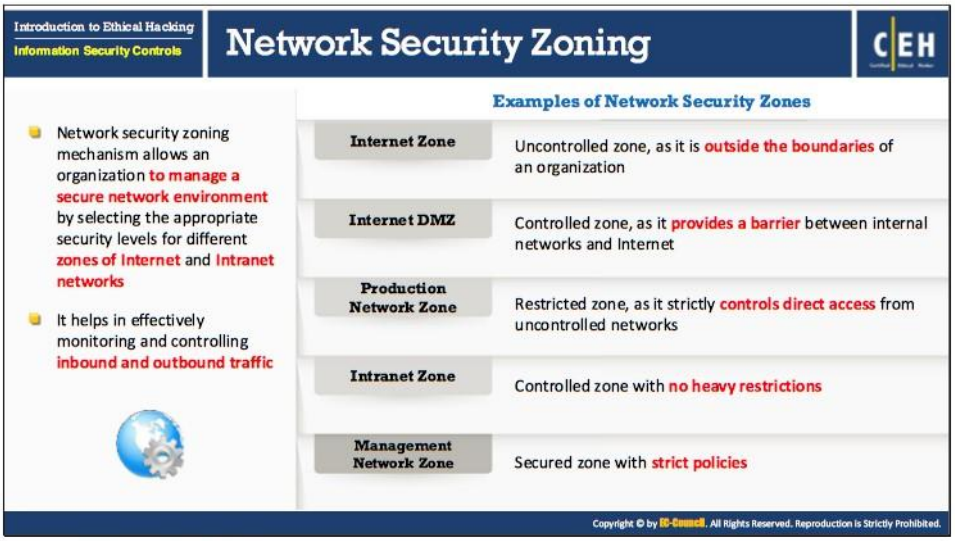
Enterprise Information Security Architecture (EISA)

EISA is a set of requirements, processes, principles, and models that determine the current and/or future structure and behavior of an organization's security processes, information security systems, personnel, and organizational sub-units. It ensures that the security architecture and controls are in alignment with the organization's core goals and strategic direction.

Though EISA deals with information security, it relates more broadly to the security practice of business optimization. Thus, it also addresses business security architecture, performance management and security process architecture. The main objective of implementing EISA is to make sure that IT security is in alignment with business strategy.

The following are the goals of EISA:

- To help in monitoring and detecting network behaviors in real time acting upon internal and externals security risks.
- To help an organization detect and recover from security breaches.
- To aid in prioritizing resources of an organization and pay attention to various threats.
- To benefit the organization in cost prospective when incorporated in security provisions such as incident response, disaster recovery, and event correlation, etc.
- To help in analyzing the procedures needed for the IT department to identify assets and function properly.
- To help perform risk assessment of an organization's IT assets with the cooperation of IT staff.



Network Security Zoning

A security zone is an area within a network that consists of a group of systems and other components with the same characteristics, all of which serve to manage a secure network environment. The network security zoning mechanism allows an organization to efficiently manage a secure network environment by selecting the appropriate level of security for different zones of Internet and intranet networks. It also enforces the organization's Internet security policies, according to the origin of the Web content and helps in effectively monitoring and controlling inbound and outbound traffic.

Properties of security zone:

- Active security policies that enforce rules on the traffic in transit (traffic that can pass through the firewall) and the action to be taken against it
- Pre-defined screening options that detect and block the malicious traffic
- Address book (IP addresses and address sets) to recognize members, so that policies can be applied
- List of interfaces in the zone

Examples of network security zones include:

- **Internet Zone:** The Internet zone, also known as the untrusted zone, is the part of the Internet that is outside the boundaries of an organization. It is highly susceptible to security breaches, as there may be little or no security controls that can block an invasion.
- **Internet DMZ:** The Internet DMZ ("demilitarized zone"; also called a controlled zone) is a controlled, Internet-facing zone that typically contains Internet-facing components of

network web servers and email gateways through which employees of an organization directly communicate. It acts as a barrier between the organization's private network and its public network. The Internet DMZ uses a firewall at each of the two gateway faces, which enable the control of:

- Traffic entering the hosts in a DMZ from the Internet
- Traffic leaving from the hosts in a DMZ to the Internet
- Traffic entering the hosts in a DMZ from internal (private) networks
- Traffic leaving from the hosts in a DMZ to internal networks

Security administrators may install access control software in the DMZ to monitor and control user access to resources stored in the restricted and other controlled zones.

- **Production Network Zone:** The production network zone, also known as a restricted zone, supports functions for which access should be limited. It strictly controls direct access from uncontrolled networks. Typically, a restricted zone employs one or more firewalls to filter inbound and outbound traffic.
- **Intranet Zone:** The intranet zone, also known as a controlled zone, contains a set of hosts in an organization's network located behind a single firewall or set of firewalls, and generally has less restriction. This zone is not heavily restricted in use, but it has an appropriate span of control set up to ensure that network traffic does not compromise the operation of significant business functions.
- **Management Network Zone or Secured Zone:** Access to this zone is limited to authorized users. Access to one area of the zone does not necessarily apply to another area of the zone. It is a secured zone with strict policies.