ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-03 INFORMATION SECURITY

BLOCK

2 SECURITY THREATS AND VULNERABILITIES

Unit-1: Overview of Security Threats and Vulnerabilities

Unit-2: Malwares

Unit-3: Security Counter Measures

Unit-1 Overview of Security Threats and Vulnerabilities

Unit Structure

1.0 INTRODUCTION

In our everyday lives, many of us work with computers for our employers, play on computers at home, go to school online, buy goods from merchants on the Internet, take our laptops to the coffee shop and check our e-mail carry our smart phones on our hips and use them to check our bank balances etc. Although this technology enables us to be more productive and allows us to access a host of information with only a click of the mouse, it also carries with it a host of security issues. If the information on the systems used by our employers or our banks becomes exposed to an attacker, the consequences can be dire indeed.

Although technology changes at an increasingly rapid rate, and specific implementations arise on a seemingly daily basis, much of the theory that discusses how we go about keeping ourselves secure changes at a much slower pace and does not always keep up with the changes to our technology. If we can gain a good understanding of the basics of information security, we are on a strong footing to cope with changes as they come along.

In this unit we will discuss different types of security threats and vulnerabilities in the cyber world. We will also discuss different types of attacks on our security goals; Confidentiality, Integrity and Availability.

1.1 LEARNING OBJECTIVES

After going through this unit you will be able to:

- Overview the concept of Information Security
- Understand the Information Security Model
- Understand possible kind of attacks on security goals
- Differentiate between Threats, Vulnerabilities and Risks

1.2 OVERVIEW OF INFORMATION SECURITY

Information Technology sometimes referred to as computer security is a security mechanisms applied to Information Technology (most often some form of computer system). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

1.2.1 What is information security?

Information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure,*

disruption, modification, or destruction. In essence, it means we want to protect our data and our systems from those who would seek to misuse it. In a general sense, security means protecting our assets. This may mean protecting them from attackers invading our networks, natural disasters, adverse environmental conditions, power failures, theft or vandalism, or other undesirable states. Ultimately, we will attempt to secure ourselves against the most likely forms of attack, to the best extent we reasonably can, given our environment.

1.2.2 What is Information assurance?

It is the act of ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

1.2.3 When are we secure?

Defining the exact point at which we can be considered secure presents a bit of a challenge.

- Are we secure if our systems are properly patched?
- Are we secure if we use strong passwords?
- Are we secure if we are disconnected from the Internet entirely?

Even from common-sense, all of these questions can be answered with a "no." Even if our systems are properly patched, there will always be new attacks to which we are vulnerable. When strong passwords are in use, there will be other avenues that an attacker can exploit. When we are disconnected from the Internet, our systems can be physically accessed or stolen. In short, it is very difficult to define when we are truly secure. We can, however, turn the question around. Defining when we are **insecure** is a much easier task, and we can quickly list a number of items that would put us in this state:

- Not patching our systems
- Using weak passwords such as "password" or "1234"
- Downloading programs from the Internet
- Opening e-mail attachments from unknown senders
- Using wireless networks without encryption

We could go on for some time creating such a list. The good thing is that once we are able to point out the areas in an environment that can cause it to be insecure; we can take steps to mitigate these issues. This problem is akin to cutting something in half over and over; there will always be some small portion left to cut again. Although we may

never get to a state that we can definitively call "100 percent secure, we can take steps in the right direction.

1.3 MODELS FOR DISCUSSING SECURITY ISSUES

When we discuss security issues, it is often helpful to have a model that we can use as a foundation or a baseline. This gives us a consistent set of terminology and concepts that we, as security professionals, can refer to when security issues arise.

1.3.1 The Confidentiality, Integrity and Availability Triad

Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad. The CIA triad gives us a model by which we can think about and discuss security concepts, and tends to be very focused on security, as it pertains to data. The common notation for confidentiality, integrity, and availability is CIA. In certain materials, largely those developed by ISC2 we may see this rearranged slightly as CAI. No change to the concepts is implied in this rearrangement, but it can be confusing for those who do not know about it in advance. We may also see the CIA concepts expressed in their negative forms: i.e disclosure, alteration, and denial (DAD).

1.3.1.1 Confidentiality

In information security, confidentiality *"is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes"* (Excerpt ISO27000). Confidentiality is a concept similar to, but not the same as, privacy. Confidentiality is a necessary component of privacy and refers to our ability to protect our data from those who are not authorized to view it. Confidentiality is a concept that may be implemented at many levels of a process. As an example, if we consider the case of a person withdrawing money from an ATM, the person in question will likely seek to maintain the confidentiality of the personal identification number (PIN) that allows him, in combination with his ATM card, to draw funds from the ATM. Additionally, the owner of the ATM will hopefully maintain the confidentiality of the account number, balance, and any other information needed to communicate to the bank from which the funds are being drawn. The bank will maintain the confidentiality of the transaction with the ATM and the balance change in the account after the funds have been withdrawn. If at any point in the transaction confidentiality is compromised, the results could be bad for the individual the owner of the ATM, and the bank, potentially resulting in what is known in the information security field as a breach.

Confidentiality can be compromised by the loss of a laptop containing data, a person looking over our shoulder while we type a password, an e-mail attachment being sent to the wrong person, an attacker penetrating our systems, or similar issues.

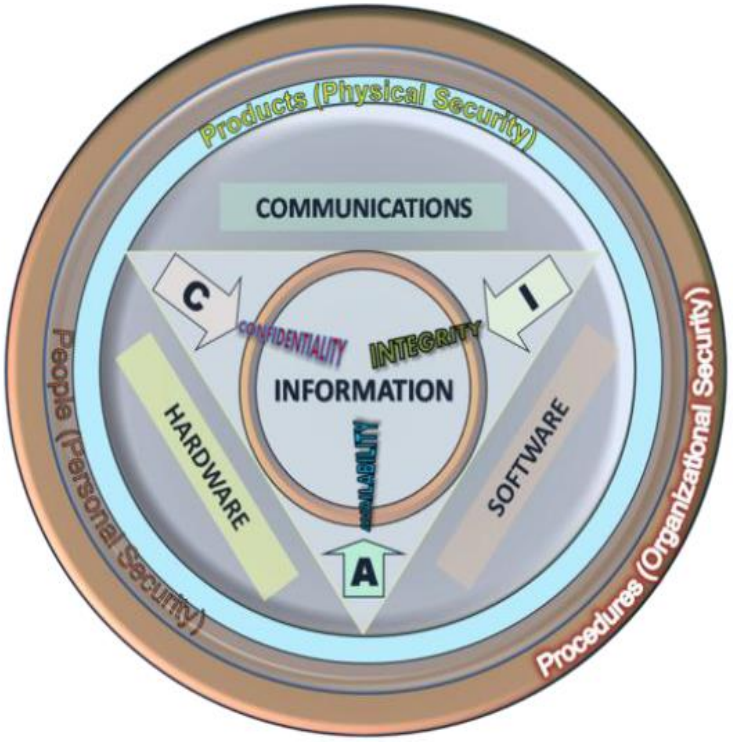


Fig: The CIA Triad

1.3.1.2 Integrity

Integrity refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner. This could mean the unauthorized change or deletion of our data or portions of our data, or it could mean an authorized, but undesirable, change or deletion of our data. To maintain integrity, we not only need to have the means to prevent unauthorized changes to our data but also need the ability to reverse authorized changes that need to be undone. We can see a good example of mechanisms that allow us to control integrity in the file systems of many modern operating systems such as Windows and Linux. For purposes of preventing unauthorized changes, such systems often implement permissions that restrict what actions an unauthorized user can perform on a given file. Additionally, some such systems, and many applications, such as databases, can allow us to undo or roll back changes that are undesirable. Integrity is particularly important when we are discussing the data that provides the foundation for other decisions. If an attacker were to alter the data

that contained the results of medical tests, we might see the wrong treatment prescribed, potentially resulting in the death of the patient.

1.3.1.3 Availability

The final leg of the CIA triad is availability. Availability refers to the ability to access our data when we need it. Loss of availability can refer to a wide variety of breaks anywhere in the chain that allows us access to our data. Such issues can result from power loss, operating system or application problems, network attacks, compromise of a system, or other problems. When such issues are caused by an outside party, such as an attacker, they are commonly referred to as a denial of service (DoS) attack.

1.3.2 Relating the CIA triad to security

Given the elements of the CIA triad, we can begin to discuss security issues in a very specific fashion. As an example, we can look at a shipment of backup tapes on which we have the only existing, but unencrypted, copy of some of our sensitive data stored. If we were to lose the shipment in transit we will have a security issue. From a confidentiality standpoint, we are likely to have a problem since our files were not encrypted. From an integrity standpoint, presuming that we were able to recover the tapes, we again have an issue due to the lack of encryption used on our files. If we recover the tapes and the unencrypted files were altered, this would not be immediately apparent to us. As for availability, we have an issue unless the tapes are recovered since we do not have a backup copy of the files. Although we can describe the situation in this example with relative accuracy using the CIA triad, we might find that the model is more restrictive than what we need in order to describe the entire situation. An alternative model does exist that is somewhat more extensive.

1.3.3 The Parkerian Hexad

The Parkerian hexad, named for Donn Parker and introduced in his book Fighting Computer Crime, provides us with a somewhat more complex variation of the classic CIA triad. Where the CIA triad consists of confidentiality, integrity, and availability, the Parkerian hexad consists of these three principles, as well as possession or control, authenticity, and utility for a total of six principles, as shown in figure below. Although it is considered by some to be a more complete model, the Parkerian hexad is not as widely known as the CIA triad. If we decide to use this model in discussion of a security situation, we should be prepared to explain the difference to the uninitiated.

1.3.3.1 Confidentiality, Integrity and Availability

As we mentioned, the Parkerian hexad encompasses the three principles of the CIA triad with the same definitions we just discussed. There is some variance in how Parker describes integrity, as he does not account for authorized, but incorrect, modification of data, and instead focuses on the state of the data itself in the sense of completeness.

Figure: The Parkerian hexad

1.3.3.2 Possession or Control

Possession or control refers to the physical disposition of the media on which the data is stored. This enables us, without involving other factors such as availability, to discuss our loss of the data in its physical medium. In our lost shipment of backup tapes, let us say that some of them were encrypted and some of them were not. The principle of possession would enable us to more accurately describe the scope of the incident; the encrypted tapes in the lot are a possession problem but not a confidentiality problem, and the unencrypted tapes are a problem on both counts.

1.3.3.3 Authenticity

Authenticity allows us to talk about the proper attribution as to the owner or creator of the data in question. For example, if we send an e-mail message that is altered so as to appear to have come from a different e-mail address than the one from which it was actually sent, we would be violating the authenticity of the e-mail. Authenticity can be enforced through the use of digital signatures. A very similar, but

reversed, concept to this is non-repudiation. Non-repudiation prevents someone from taking an action, such as sending an e-mail, and then later denying that he or she has done so.

1.3.3.4 Utility

Utility refers to how useful the data is to us. Utility is also the only principle of the Parkerian hexad that is not necessarily binary in nature; we can have a variety of degrees of utility, depending on the data and its format. This is a somewhat abstract concept, but it does prove useful in discussing certain situations in the security world. For instance, in one of our earlier examples we had a shipment of backup tapes, some of which were encrypted and some of which were not. For an attacker, or other unauthorized person, the encrypted tapes would likely be of very little utility, as the data would not be readable. The unencrypted tapes would be of much greater utility, as the attacker or unauthorized person would be able to access the data.

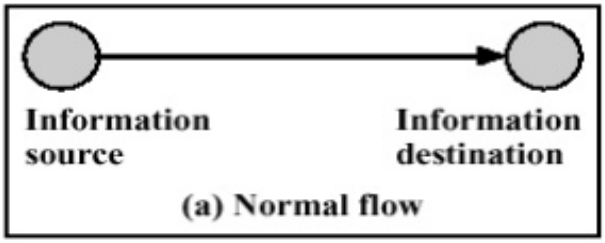
1.4 TYPES OF ATTACKS ON SECURITY GOALS

In computer and computer networks an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. We may face attacks from a wide variety of approaches and angles. When we look at what exactly makes up an attack, we can break it down according to the type of attack that it represents, the risk the attack represents, and the controls we might use to mitigate it.

When we look at the types of attacks we might face, we can generally place them into one of four categories: interception, interruption, modification, and fabrication. Each category can affect one or more of the principles of the CIA triad, as shown in figure below.

Normal Flow of Information (No attack)

In a normal flow of data in any communication data is originated from the source and received at the destination without any modification and leakage.



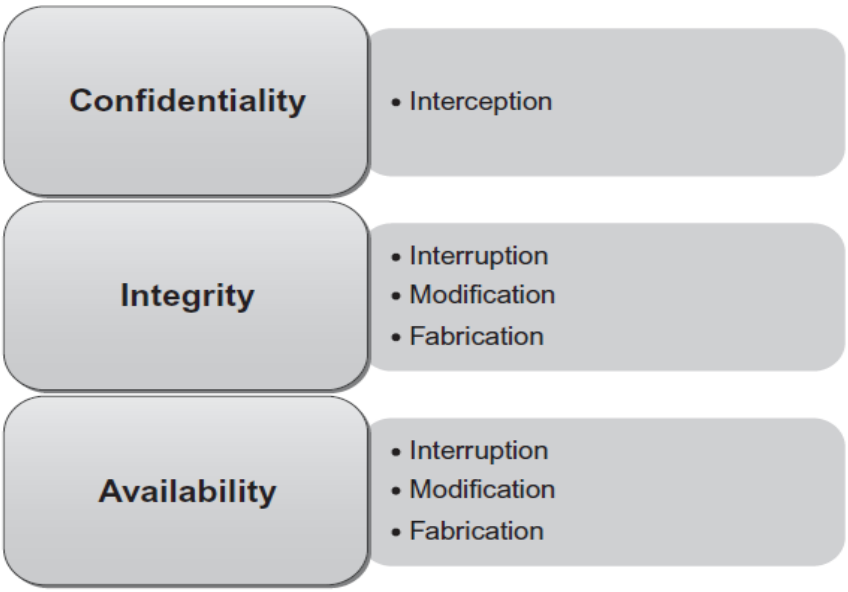
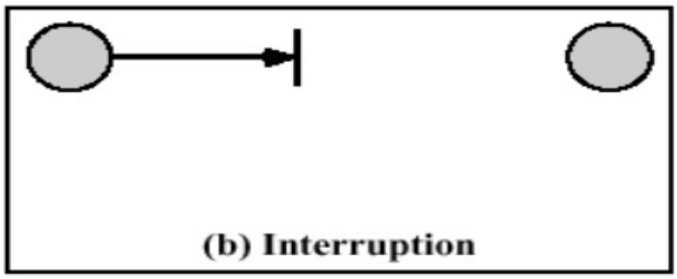


Fig: Category of CIA triad

1.4.1 Interruption

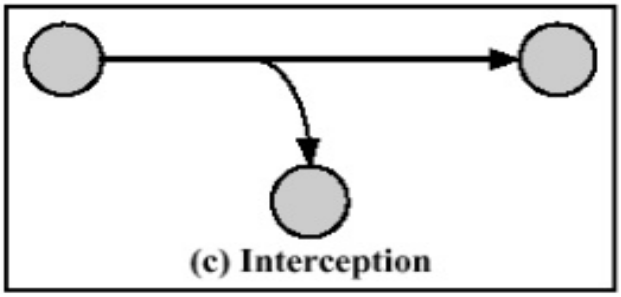
Interruption attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. In the case of a DoS attack on a mail server, we would classify this as an availability attack. In the case of an attacker manipulating the processes on which a database runs in order to prevent access to the data it contains, we might consider this an integrity attack, due to the possible loss or corruption of data, or we might consider it a combination of the two.



We might also consider such a database attack to be a modification attack rather than an interruption attack.

1.4.2 Interception

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.

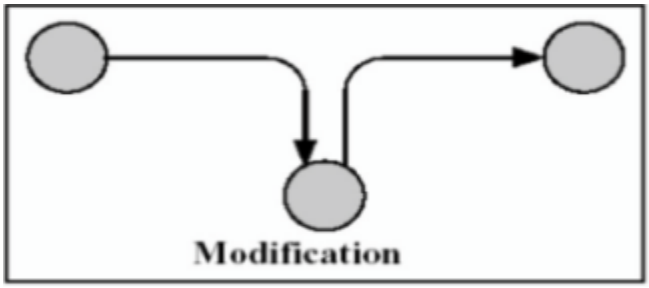


Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be conducted against data at rest or in motion. Properly executed, interception attacks can be very difficult to detect.

1.4.3 Modification

Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.

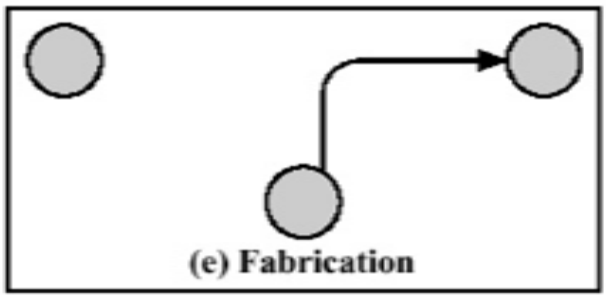
However, if we consider the case where the file in question is a configuration file that manages how a particular service behaves, perhaps one that is acting as a Web server, we might affect the availability of that service by changing the contents of the file.



If we continue with this concept and say the configuration we altered in the file for our Web server is one that alters how the server deals with encrypted connections, we could even make this a confidentiality attack.

1.4.4 Fabrication

Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well. If we generate spurious information in a database, this would be considered to be a fabrication attack.



We could also generate e-mail, which is commonly used as a method for propagating malware, such as we might find being used to spread a worm. In the sense of an availability attack, if we generate enough additional processes, network traffic, e-mail, Web traffic, or nearly anything else that consumes resources, we can potentially render the service that handles such traffic unavailable to legitimate users of the system.

1.5 THREATS VULNERABILITIES AND RISK

In order to be able to speak more specifically on attacks, we need to introduce a few new items of terminology. When we look at the potential for a particular attack to affect us, we can speak of it in terms of threats, vulnerabilities, and the associated risk that might accompany them.

Information security vulnerabilities are weaknesses that expose an organization to risk. Vulnerability is a weakness in a system that could allow an attacker to compromise the security of the organization.

It may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

1.5.1 Threats

Threats can exploit the vulnerabilities to impact the performance of the systems. A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system. Threats can include everything from viruses, Trojans, and back doors to outright attacks from hackers. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

Ultimately, this is what a threat is-something that has the potential to cause us harm. Threats tend to be specific to certain environments, particularly in the world of information security. For example, although a virus might be problematic on a Windows operating system, the same virus will be unlikely to have any effect on a Linux operating system.

Ten web threats

1. DDoS Attacks-Distributed Denial of Service Attacks.
2. **Old Browsers, Vulnerable Plug-Ins-**e.g., browser vulnerabilities and, more frequently, the browser plug-ins that handle Oracle's Java and Adobe's Flash and Reader.
3. **Good Sites Hosting Bad Content**- attackers infected legitimate financial and tech industry websites.
4. **Mobile Apps and the Unsecured Web-** bring-your-own-device movement has led to a surge in consumer-owned devices inside corporate firewalls
5. **Failing to Clean up Bad Input-** SQL injection has held the top spot on the Open Web Application Security Project's list of top 10 security vulnerabilities
6. **The Hazards of Digital Certificates-** a series of hacks against certificate authorities gave attackers the tools they needed to issue fraudulent SSL certificates that could disguise a malicious website as a legitimate
7. **The Cross-Site Scripting Problem-** An attacker going after a banking site with a cross-site scripting vulnerability could run a script for a login box on the bank's page and steal users' credentials.
8. **The Insecure 'Internet Of Things**‘--- Routers and printers, videoconferencing systems, door locks and other devices are now networked via Internet protocols and even have embedded Web servers. In many cases, the software on these devices is an older version of an open source library that's difficult
9. **Getting in the Front Door---** Automated Web bots scrape from Web pages information that can give a competitor better intelligence on your business.
10. **New Technology, Same Problems---** People click links all day long -- people are pretty trained to think that clicking a link on the Web is safe.

Major Security Threats on Information Systems

1. **Intrusion or Hacking** means gaining access to a computer system without the knowledge of its owner---Tools: . Poor Implementation of Shopping Carts, Hidden fields in the html forms, Client-side validation scripts, Direct SQL attack, Session Hijacking, Buffer Overflow Forms, Port Scan
2. **Viruses and Worms**--- programs that make computer systems not to work properly--- Polymorphic Virus, Stealth Virus, Tunneling Virus, Virus Droppers, and Cavity Virus.

3. **Trojan Horse**--- These programs are having two components; one runs as a server and another one runs as a client; data integrity attack, steal private information on the target system, store key strokes and make it viewable for hackers, sending private local as an email attachment.
4. **Spoofing:** It is the act of fooling other computer users to think that the source of their information is coming from a legitimate user- Examples include: IP Spoofing, DNS Spoofing, ARP Spoofing.
5. **Sniffing** is used by hackers for scanning login_ids and passwords over the wires. TCP dump and Snoop are better examples for sniffing tools.
6. **Denial of Service**: The main aim of this attack is to bring down the targeted network and make it to deny the service for legitimate users. In order to do DoS attacks, people do not need to be an expert. They can do this attack with simple ping command.

1.5.2 Vulnerabilities

Vulnerabilities are weaknesses that can be used to harm us. In essence, they are holes that can be exploited by threats in order to cause us harm.
Vulnerability might be a specific operating system or application that we are running, a physical location where we have chosen to place our office building, a data centre that is populated over the capacity of its air-conditioning system, a lack of backup generators, or other factors.

Types of vulnerabilities

"Some weaknesses of a system or vulnerabilities are."

- Physical vulnerabilities
- Natural vulnerabilities
- Hardware/software vulnerabilities
- Media vulnerabilities (e.g., stolen/damaged disk/tapes)
- Emanation vulnerabilities---due to radiation
- Communication vulnerabilities
- Human vulnerabilities

Examples of Information Security Vulnerabilities

Information security vulnerabilities are weaknesses that expose an organization to risk.

- **Through employees**: Social interaction, Customer interaction, Discussing work in public locations, Taking data out of the office (paper, mobile phones, laptops), Emailing documents and data, Mailing and faxing documents, Installing unauthorized software and apps, Removing or disabling security tools, Letting unauthorized

persons into the office (tailgating) , Opening spam emails, Connecting personal devices to company networks, Writing down passwords and sensitive data, Losing security devices such as id cards, Lack of information security awareness, Keying data

- **Through former employees**: Former employees working for competitors, Former employees retaining company data, Former employees discussing company matters
- **Though Technology**: Social networking, File sharing, Rapid technological changes, Legacy systems, Storing data on mobile devices such as mobile phones, Internet browsers
- **Through hardware**: Susceptibility to dust, heat and humidity, Hardware design flaws, Out of date hardware, Misconfiguration of hardware.
- **Through software**: Insufficient testing, Lack of audit trail, Software bugs and design faults, Unchecked user input, Software that fails to consider human factors, Software complexity (bloatware), Software as a service (relinquishing control of data), Software vendors that go out of business or change ownership
- **Through Network**: Unprotected network communications, Open physical connections, IPs and ports, Insecure network architecture, Unused user ids, Excessive privileges, Unnecessary jobs and scripts executing , Wifi networks
- **Through IT Management**: Insufficient IT capacity , Missed security patches, Insufficient incident and problem management, Configuration errors and missed security notices , System operation errors, Lack of regular audits, Improper waste disposal, Insufficient change management, Business process flaws, Inadequate business rules, Inadequate business controls, Processes that fail to consider human factors, Overconfidence in security audits, Lack of risk analysis, Rapid business change, Inadequate continuity planning Lax recruiting processes
- **Partners and suppliers**: Disruption of telecom services, Disruption of utility services such as electric, gas, water, Hardware failure, Software failure, Lost mail and courier packages, Supply disruptions, Sharing confidential data with partners and suppliers

1.5.3 Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Risk is the likelihood that something bad will happen. In order for us to have a risk in a particular environment, we need to have both a threat and a vulnerability that the specific threat can exploit. For example, if we have a structure that is made from wood and we set it on fire, we have

both a threat (the fire) and a vulnerability that matches it (the wood structure). In this case, we most definitely have a risk .Likewise, if we have the same threat of fire, but our structure is made of concrete, we no longer have a credible risk, because our threat does not have a vulnerability to exploit. We can argue that a sufficiently hot flame could damage the concrete, but this is a much less likely event. We will often have similar discussions regarding potential risk in computing environments, and potential, but unlikely, attacks that could happen. In such cases, the best strategy is to spend our time mitigating the most likely attacks. If we sink our resources into trying to plan for every possible attack, however unlikely, we will spread ourselves thin and will be lacking in protection where we actually need it the most.

Risk management

- Risk management is the "Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost." --- assessment of risk and the implementation of procedures and practices designed to control the level of risk

- Risk assessment is the "assessment of threats to, impact on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence."- Identification of the risk, analysis of the risk in terms of performance, cost, and other quality factors; risk prioritization in terms of exposure and leverage. Risk can be assessed as per the following matrix representation.

Information Security Risks, Threats and Vulnerabilities
© simplicable.com

1.6 KEY TERMS AND CONCEPTS

Information security aims at "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information assurance is the act of ensuring that data is not lost when critical issues arise.

CIA Triad: Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad.

Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner.

Availability refers to the ability to access our data when we need it.

An **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Interruption attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. **Interception** attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.

Modification attacks involve tampering with our asset. Such attacks are considered attacks on integrity but could also represent an availability attack.

Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. **Vulnerability** is a cyber-security term that refers to a flaw in a system that can leave it open to attack.

A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system. It may refer to an object or people who pose a potential danger to an asset (via attacks).

1.7 SELF ASSESMENT QUESTIONS

1. What do you mean by information assurance?
   .....
   .....
   .....
   .....
   .....
2. List different types of attacks on confidentiality?
   .....
   .....
   .....
   .....
   .....

3. Name and explain possible attacks on Integrity and availability.

   .....
   .....
   .....
   .....
   .....

4. Differentiate between threat and attack.

   .....
   .....
   .....
   .....
   .....

5. Differentiate between Threat, vulnerabilities and risks with an example.

   .....
   .....
   .....
   .....
   .....

1.8 REFERENCES AND SUGGESTED READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e e-Governance and Cyber Security.
3. Big List of Information Security Vulnerabilities, John Spacey, 2011 http://simplicable.com/new/the-big-list-of-information-security-vulnerabilities
4. Top Ten Database Security Threats, Amichai Shulman, *www.schell.com/**Top_Ten_Database_Threats**.pdf*
5. 10 Web Threats that could harm your business, Robert Lemos,2013, http://www.darkreading.com/vulnerability/10-web-threats-that-could-harm-your-busi/240150315
6. Information Security, John Peter Jesan, 2006. http://ubiquity.acm.org/article.cfm?id=1117695

UNIT-2:
MALWARES:VIRUS WORMS AND OTHER MALWARE

Unit Structure

2.0 INTRODUCTION

Malware stands for —*Malicious Software* and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers.

In this unit will discuss about different types of virus, worms and other malware.

2.1 LEARNING OBJECTIVES

After studying this unit, you should be able to understand:

- A Malware and its types?
- A Virus and its types?
- A Worm and its types?
- A Trojan horse?

2.2 TYPES OF MALWARE

There are various types of malwares present in the Internet. Some of the popular ones are:

2.2.1 Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

Fig: Adware

2.2.2 Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without theknowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programmes from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

Fig: Spyware

2.2.3 Browser hijacking software

There are some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

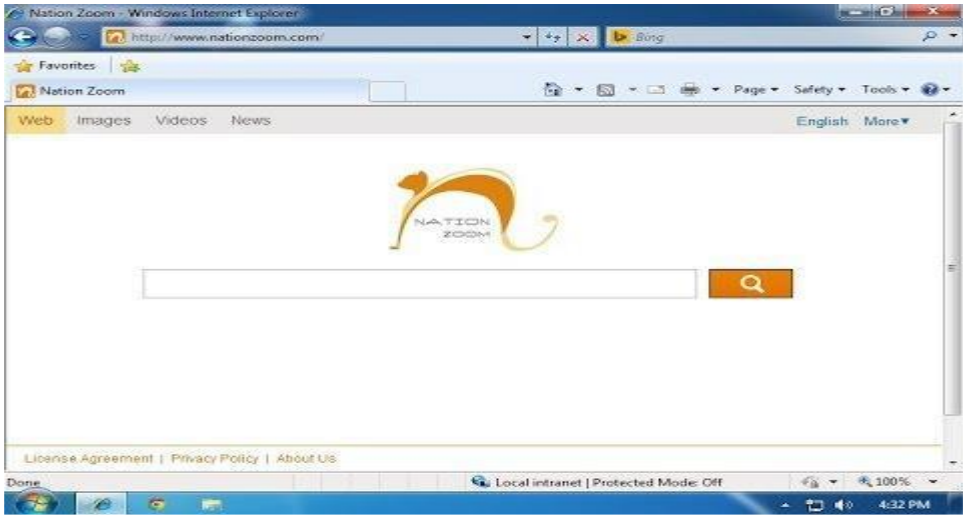


Fig: Browser hijacking

2.2.4 Virus

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention. Until and unless the executable file (.exe) is executed, a virus cannot be activated in the host machine.

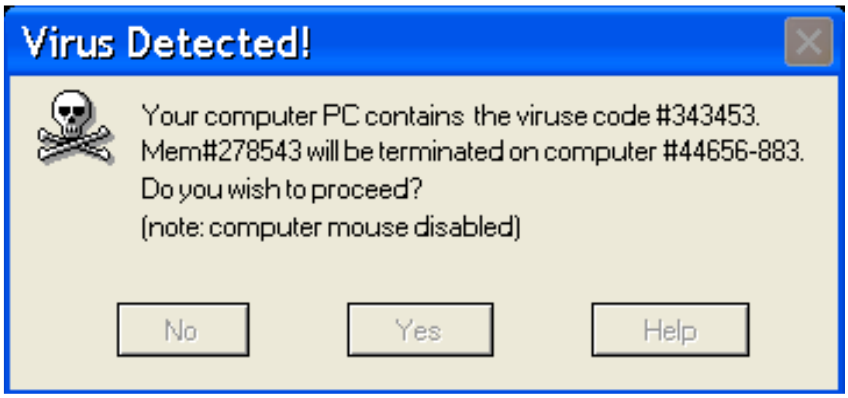


Fig: Computer virus

2.2.5 Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke. It is a program that views the infection point as another computer rather than as other executable files on an already infected computer.

In simplistic terms this normally means when infected you will only have a single infected program on your computer rather than thousands of the programs you have installed being infected. A worm is much sneakier at infecting a computer, but thankfully they are also much easier to identify once infected. The reason they are considered to be sneakier is because a worm has many more tools at its disposal that it can use to infect you than a virus has. They not only use infected files to lure you, but they take advantage of the fact that programs have bugs that allow them to wiggle into your computer. This means that a worm can infect your computer without you ever

having to execute a program infected with a worm; instead they can gain entrance through an open communications port on your computer (which is a virtual port that has no physical self).

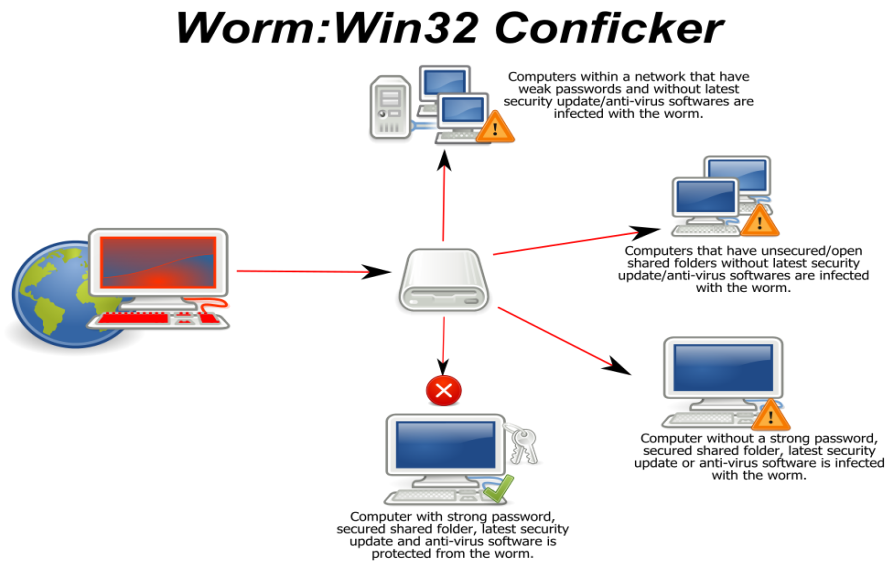


Fig: An example of a Computer worm- Conficker

2.2.6 Trojan Horse

A Trojan virus is a piece of software designed to look like a useful file or software program but performs a possibly nefarious function once installed on a client computer. The virus takes its name from the ―Trojan Horse‖ from Greek mythology setup outside of the city of Troy. Trojan horse viruses differ from other computer viruses in that they are not designed to spread themselves. Instead Trojan horse malware is either delivered as the payload of another virus or piece of malware or through manual end-user action by downloading infected files or inserting infected drives into a computer. Once a computer is infected with a Trojan virus, the malware can be designed to steal end-user information, perform destructive harm on the target computer, or even download additional computer malware. A Trojan virus will normally consist of a server and client component. The client component is the portion of the malware that infects the end-user‘s computer. Once established or executed, the virus can be designed to establish a certain level of control over the infected computer.

It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer.

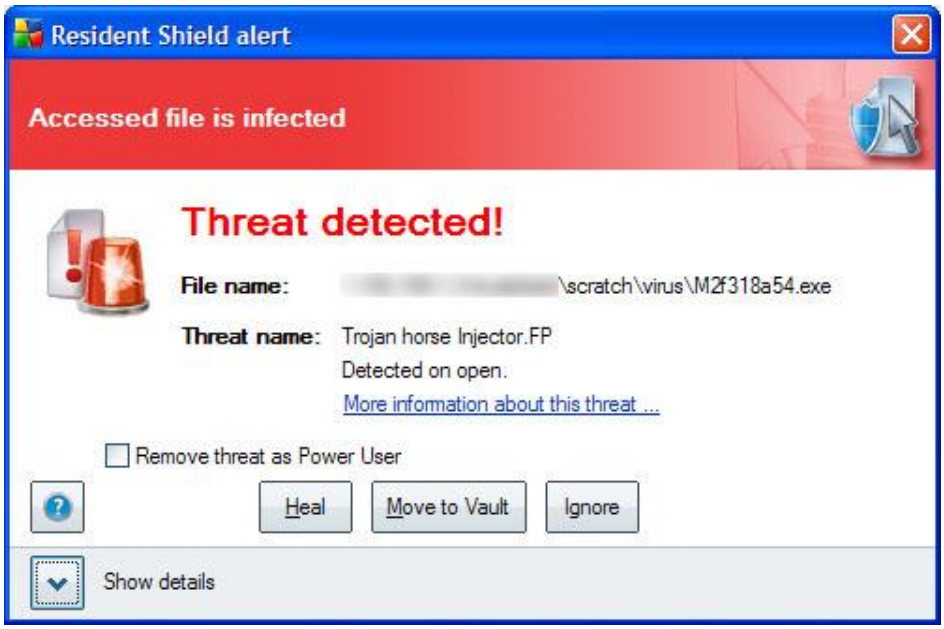


Fig: Trojan horse

It can become a part of *botnet (*ro*bot-net*work*)*, a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojans neither infect the other computers in the network nor do they replicate.

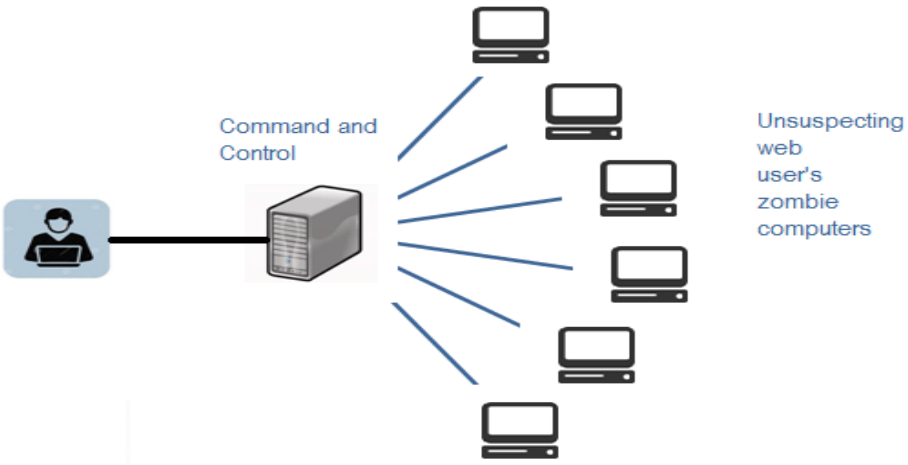


Fig: A typical botnet

The categories currently used to define the different variants of Trojan viruses include:

- **Remote access:** virus will give the hacker/attacker full control over the targeted computer equivalent to the user‘s permissions.
- **Password sending:** the malware will search for all cached passwords and copy those that are entered by the end-user.
- **Destructive:** A destructive Trojan virus‘s primary purpose is to delete or remove files on the targeted computer.

- **Key loggers:** are a variant of Trojan virus that is designed to record the keystrokes on an infected computer and then send the log files to a remote server or email account.
- **Denial of service:** A denial of service (DoS) attack Trojan virus will be designed to use the infected computer as a bot to attack another web server or computer. Combined with other computers that are infected, the Internet connection for the attacked computer can become too busy to allow regular users to make use of the site.
- **Proxy:** A proxy or Wingate Trojan virus is designed to make the infected computer act as a Wingate or proxy server. As a result of the infection, the targeted computer can then be used by other to surf the Internet in an anonymous fashion.
- **FTP:** A FTP Trojan virus is one of the most basic Trojan viruses in the wild and is one of the most outdated. The primary purpose of the malware is to open port 21 on the infected computer. Once opened, anyone can then connect to the computer using the FTP protocol.
- **Software detection killers:** The purpose of this variant of Trojan virus is to disable known antivirus and computer firewall programs.
- **Trojan down loaders:** The sole job that a Trojan downloader does on the infected computer is to download additional computer malware onto the infected computer.

2.2.7 Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user‘s computer.

Fig: Scare ware

As a remedial measure, the message suggests the used download the full paid version of the software. As the user proceeds to

download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid.

2.3 COMPUTER VIRUS AND ITS TYPES

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". Whenever the host programs are executed, the virus instructions get activated along with the program.

2.3.1 How Computer Virus Works

As said earlier, computer virus operates by attaching themselves to an already existing file or program and replicates itself to spread from one computer to another. In most cases, they tend to infect executable files that are parts of legitimate programs. So, whenever the infected file is executed on a new computer, the virus gets activated and begins to operate by further replication or causing the intended damage to the system.

A virus cannot perform its task of harming and replication unless it is allowed to execute. This is the reason why viruses often choose an executable file as its host and get attached to them. Viruses are mainly classified into two types:

a. Non-Resident Viruses: This kind of virus will execute along with its host, perform the needful action of finding and infecting the other possible files and eventually transfers the control back to the main program (host). The operation of the virus will terminate along with that of its host.

b. Resident Viruses: In case of resident viruses, whenever the infected program is run by the user, the virus get activated, loads its replication module into the memory and then transfer the control back to the main program. In this case, the virus still remains active in the memory waiting for an opportunity to find and infect other files even after the main program (host) has been terminated.

2.3.2 Type of Computer Viruses

There are many kinds of virus created from many sources. Some of them are explained as follows.

2.3.2.1 File Virus

File Virus uses the file system of a given OS (or more than one) to propagate. File viruses include viruses that infect executable

files, companion viruses that create duplicates of files, viruses that copy themselves into various directories, and link viruses that exploit file system features. A subset of file viruses, known as *script virus*, written in one of a variety of script languages like Visual Basic Script, JavaScript, Windows Batch, PHP, etc. either infects other scripts, e.g., Windows or Linux command and service files, or forms a part of a multi-component virus. Script viruses are able to infect other file formats, such as HyperText Markup Language (HTML), if that file format allows the execution of scripts.

2.3.2.2 Boot sector virus

This type of virus infects the boot sector or the master boot record or displaces the active boot sector of a hard drive. Once the hard drive is booted up, boot sector viruses load themselves into the computer‘s memory. Many boot sector viruses, once executed, prevent the OS from booting. Boot sector viruses were widespread in the 1990s, but have almost disappeared since the introduction of 32-bit processors and the near-disappearance of floppy disks as a storage medium for executables.

2.3.2.3 Macro virus

Written in the macro scripting languages of word processing, accounting, editing, or project applications, it propagates by exploiting the macro language‘s properties in order to transfer itself from the infected file containing the macro script to another file. The most widespread macro viruses are for Microsoft Office applications (Word, Excel, Power Point, Access). Because they are written in the code of application software, macro viruses are platform independent and can spread between Mac, Windows, Linux, and any other system running the targeted application.

2.3.2.4 Electronic mail (email) virus

Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim‘s email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim‘s email address book and repeats its propagation process. Email virus refers to the delivery mechanism rather than the infection target or behaviour.

2.3.2.5 Multi-variant virus

The same core virus but implemented with slight variations, so that an anti-virus scanner that can detect one variant will not be able to detect the other variants.

Polymorphic Virus is the virus which changes their characteristic after each infection. There are various techniques which are employed to achieve polymorphism by self-modification of code and hence infected files are infected with different variants. And in other cases, the virus encrypts itself with different key for different file.

Metamorphic Virus is the virus that is rewritten such that, with each iteration so that each succeeding version of the code is different from the preceding one.

2.3.3 Creating and distributing viruses over internet

A Computer virus is a parasitic program written intentionally to enter a computer without the users' permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some viruses do little but replicate others can cause serious damage or effect program and system performance.

A virus should never be assumed harmless and left on a system– Symantec. Five most common types of virus distributed over the internet are as follows:

1. **Macro virus -** this type of virus usually comes as part of a document or spreadsheet, often in email.
2. **Boot sector viruses** - this type of virus overwrites the boot sector on your hard drive or floppy drive.
3. **File infector viruses** - this type of virus attaches itself to executables, for example .com and .exe files.
4. **Stealth viruses** - this type of virus tries to fool antivirus software by catching its requests to the operating system (asking to open a file, for example).
5. **Self-modifying virus** - this type of virus was designed to avoid detection by antivirus software by changing itself internally.

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

2.4 COMPUTER WORM S

A computer worm is a standalone *malware* computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security weakness on the target computer to access it. Unlike a computer virus, it does not

need to attach itself to an existing program (or clicking on the Web link for a malware Web site) for replication, dissemination, or execution. They can run independently and can propagate a complete working version of itself onto other hosts on a network. Each subsequent copy of the worm can also self-replicate, therefore infection can spread very rapidly. Computer worms can exploit network configuration errors (for example, to copy themselves onto a fully accessible disk) or exploit loopholes in operating system and application security. Many worms will use more than one method in order to spread copies via networks. One of the many mechanisms used by the worm to propagate is:

Files sent as email attachments

- Via a link to a web or FTP resource
- Via a link sent in an ICQ or IRC message
- Via P2P (peer-to-peer) file sharing networks.

Some worms are spread as network packets. They directly penetrate the computer memory, and the worm code is then activated. There are many different types of computer worms and many can cause high levels of destruction. Worms can be broadly categorized as:

2.4.1 Types of Worm

1. **Email worms:** They spread via infected email attachments. Embedded in an email attachment, which must be opened by the intended victim to enable the worm to install itself on the victim‘s host, from which it can copy and disseminate itself to other hosts.
2. **Instant messaging worms:** They spread via infected attachments to IM messages or reader access to Uniform Resource Locators (URL) in IM messages that point to malicious Web sites from which the worm is downloaded.
3. **Instant Relay Chat (IRC) worm:** Comparable to IM worms, but exploit IRC rather than IM channels.
4. **Web or Internet worm:** They spread via user access to a Web page, File Transfer Protocol (FTP) site, or other Internet resource. File-sharing or peer-to-peer (P2P) worm
5. Copies itself into a shared folder, and then uses P2P mechanisms to announce its existence in hopes that other P2P users will download and execute it.
6. **Warhol worm:** It is a worm conceived by a researcher at University of California at Berkeley. This worm has a property to spread across the Internet to infect all vulnerable servers within 15 minutes of activation. (Warhol‖ refers to Andy Warhol‘s claim that every person has 15 minutes of fame).

7. **Flash worm:** It is a theoretical worm that spreads within seconds of activation to all of the vulnerable hosts on the Internet.

2.5 KEY TERMS AND CONCEPTS

- **Malware** stands for *Malicious Software* and it is designed to gain access or installed into the computer without the consent of the user.
- **Spyware** is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine.
- **Malware**, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.
- A **botnet** is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.
- **Viruses** are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.
- **Worms** are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.
- **Ransom ware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.
- **Scareware** is scam software with malicious payloads, usually of limited or no benefit that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.
- A **Trojan horse**, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

2.6 SELF-ASSESMENT QUESTIONS

1. What is a malware? Name different types of malwares?

   ……
   ……
   ……
   ……
   …….

2. What is Virus? How does it harm a computer?

   ……
   ……
   ……
   ……
   ……

3. What is the difference between a worm and a virus?

   ……
   ……
   ……
   ……
   ……

4. What is a scareware?

   ……
   ……
   ……
   ……
   …….

5. What is a Trojan horse?

   ……
   ……
   ……
   ……
   ……

   …….

2.7 REFERENCES AND SUGGESTED READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.
3. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.

UNIT-3 SECURITY COUNTER MEASURES

3.0 INTRODUCTION

Protecting one's own computer from external and internal attacks is said to be a security countermeasure. Physical security countermeasures mainly include computer virus countermeasures such as antivirus software, elimination of vulnerabilities, encryption of information/data, making backup copies of information/data, plus for intra-company networks, installation of firewall and Intrusion Detection Systems (IDS) /Intrusion Prevention Systems (IPS), and network monitoring and control on proxy servers. Also maintenance and security countermeasures are of great importance.

In this unit we will mainly discuss about the counter measures like Intrusion Detection System (IDS) and Antivirus software.

3.1 LEARNING OBJECTIVE

After going through this unit you should be able to understand

- What are different security countermeasures?
- What is Insider and Outsider attacks?
- What is an Intrusion Detection Systems (IDS)?
- What are different types of IDS?
- What is an antivirus?

3.2 TYPES OF ATTACKS

The security attacks can be classified according to their origin. Based on whether the attacker is from inside or outside the organization, an attack can further be classified as:

a. An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. It can be any disgruntled employee who wants to attack on the system.

b. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

3.2.1 Insider Attack

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access such as employees, former employees, contractors or business associates, who

have inside information concerning the organization's security practices, data and computer systems.

Insiders that perform attacks have a trenchant advantage over external attackers because they have authorized system access and also familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

3.2.1.1 Types of Insider Attack

a. Compromised actors: Insiders with access credentials or computing devices that have been compromised by an outside threat actor. These insiders are more challenging to address since the real attack is coming from outside, posing a much lower risk of being identified.

b. **Unintentional actors**: Insiders who expose data accidentally, such as an employee who accesses company data through public Wi-Fi without the knowledge that its unsecured.

A large number of data breach incidents result from employee negligence towards security measures, policies, and practices.

c. Emotional Attackers: Insiders who steal data or destroy company networks intentionally, such as a former employee who injects malware or logic bomb in corporate computers on his last day at work.

d. Tech savvy actors: Insiders who react to challenges. They use their knowledge of weaknesses and vulnerabilities to breach clearance and access sensitive information. Tech savvy actors can pose some of the most dangerous insider threats, and are likely to sell confidential information to external parties or black market bidders.

3.2.1.2 How to prevent Insider Attack

If you consider the full attack path of an external hacker, the first step is to gain internal access. Usually organizations expend an extra ordinary amount of resources on protecting their edge specifically to counter insider threats. Every organization need to create an effective security policy is understand your attack surface. Below are the steps for preventing insider attack:

Step 1: The first step in protecting a company‘s assets from internal attacks is to identify and classify what those assets are and what controls are currently in place to protect those assets. If a company‘s most important asset is money, then it will be important to note its physical location, how it is accessed, how it is guarded, who currently protects it, how much of it exists, and how the amount is recorded and maintained safe from alteration.

If the most important asset is data, it will be important to note what form is it stored in (electronic or physical), where it is stored (on a server, in a file cabinet), how it is accessed (over the network, physically opening a file cabinet), who has access to it (employees, managers), how changes are logged, and what controls are in place to secure it (usernames & passwords, lock & key). After identifying the assets and all the means of accessing them, the company should determine who, within the company, has access to these assets. This list should be reviewed and re-evaluated against job roles to ensure that only those employees that actually need access to conduct their daily responsibilities continue to have access. For all other employees, regardless of rank or managerial influence, their access should be removed.

Step 2- Assigning Owners: Classify your information so you can design and implement the proper controls for different types of data. The owner should be typically a senior ranking official, who have a solid understanding of the high level business processes but he/she should not be involved in the daily routine of operations or maintenance.

Step 3- Recognize Suspicious behaviour: It is difficult to prevent a malicious attack from a motivated insider, there are ways to spot bad behaviour before it becomes a big problem. Each employee has logical patterns of information usage, and the organization should look for abnormal usage and investigate when this occurs.

Step 4- File sharing on internal network: Most common vulnerabilities of companies are caused by their inherent desire to share everything internally. When members of a team want to communicate or share files with each other, they will create a folder on an internal file server, give it their team‘s name, and begin sharing files. Although we like to believe our employees are inherently good, it is not good practice to leave the bank vault completely unlocked. As with network file shares, if the Finance and Accounting team creates a folder that has employee or customer banking information in it, does this really need to be visible to everyone?

Step 5: Permission Allotment: A small company may have one employee tasked with multiple jobs. As the company grows this employee will begin to delegate his responsibilities to new employees, thereby reducing his access requirements to specific assets. The trouble is, many companies focus their efforts on providing access to their employees and do not focus on removing access or ensuring alignment with actual job responsibilities. If an employee started out as a database developer and was promoted after three years to manager and then three years later to director of operations, it is likely that their access requirements would be significantly different today

versus when they started. But there are many directors and vice presidents that still possess their same permissions that they had when they started with the company. This can pose a significant risk to a company if that VP or director becomes disgruntled or didn‘t get that raise they were expecting.

Step 6: Data Portability: The Internet provides a backbone of communication for legitimate business use but also facilitates employees sending internal information outside the company. This can be accomplished by email, file transfer protocol, instant messaging, or even over the web via hypertext transfer protocol (HTTP). Along with relying on networks to send and receive data, employees can also take advantage of local data portability from their desktop or laptop via CD/DVD burners or even USB thumb drives. While the devices may simplify the transfer of data between machines, their use also increases the risk of data theft. Employees with access to the company‘s intellectual property may rationalize the transfer from their work machines to their home systems to work at home. The problem is that once the data leaves a company computer, the company can no longer ensure the security or legitimate use of the data.

Step 7: Manage Incident Response: Incident response is a very tricky and precise job. Even a small mistake can lead to major pieces of evidence being lost or some other evidence being tainted in a way that makes it inadmissible in court. If your security team is not trained and certified in incident response, you should have a relationship with an organization that is and call them as soon as you identify a problem. They will likely want to get on the ground immediately.

3.2.2 Outsider Attack

Outsider threat occurs when an individual or a group seeks to gain protected information by infiltrating and taking over profile of a trusted user from outside the organization. Attacks perpetrated by adversaries that do not have access to direct access to any of the authorized nodes in the network. However, the adversary may have access to the physical medium, particularly if we are dealing with wireless networks. Therefore, attacks such as replay messages and eavesdropping fall into this classification. However, coping with this attack is fairly easy by using traditional security techniques such as encryption and digital signatures. Malicious attackers use various method, tools, and techniques to enter, disrupt, and steal information from a system.

3.2.2.1 Types of Outsider Attack

a. E-mail Hacking: The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing e-mail messages to be easily forged. Although extensions to these basic protocols do exist, the decision whether to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that both ends support.

b. Social Engineering: It can be used both by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information. A common example of social engineering would be where a hacker sends e-mail to an employee, claiming to be an administrator who needs the employee's password to do some administrative work. The normal user who has not been taught about security might not know the difference between the actual administrator and the imposter administrator, especially in a large organization.

c. Intrusion Attacks: This often happens when attackers use known vulnerabilities in the network. In updateable systems, administrators may not have or take the time to install all the necessary patches in a large number of hosts.

Users may also demand network services and protocols that are known to be flawed and subject to attack. For example, a user might ask, "Why can't I just FTP the files down?" It is very important that security policies deal not only with end-user demands but also with the threats and vulnerabilities associated with those demands. Realistically, however, it is seldom possible to remove all vulnerabilities.

d**. Denial-of-Service Attacks:** DoS attacks are designed to prevent legitimate use of a service. Attackers achieve this by flooding a network with more traffic than it can handle. Examples of this include:

- Saturating network resources, thereby preventing users from using network resources.
- Disrupting connections between two computers, preventing communications between services.
- Preventing a particular individual from accessing a service.
- Disrupting services to a specific system or client.

DoS attacks flood a remote network with an enormous amount of protocol packets. Routers and servers eventually become overloaded by attempting to route or handle each packet. Within minutes, network activity exponentially rises and the network stops responding to normal traffic and service requests from clients. This is also known as a network saturation attack or bandwidth consumption attack. Attackers strike with various tools, including Trin00 and Tribe Flood Network (TFN, TFN2K)

3.2.2.2 How to prevent Outsider Attack

For many a system is a hub of significant documents, files, and applications, but there is always a risk of losing the important files because of outside threat8. Outside threats have become a big concern for all users, especially those who use the internet regularly. Starting from damage to your system to cyber crime like identity theft, outside threats pose many dangers to your system. However, the silver lining to this concern is the presence of ways to protect and guard your system from these threats. You do not need to be a computer wizard to do this, as you just have to follow some simple steps. When it comes to computer security, you have to look after many aspects such as risk analysis, kinds of threats, security policy, and then come protection techniques. Viruses, key logging, worms and phishing attacks are all around your system to damage it, but there are ways through which you can assure the security of your system. The main ways of computer security includes:
Antivirus programs, which can scan and keeps you alert about viruses

- Firewall of your system, which can be configured for enabling you to transfer selected information between your system and internet.
- Backup is another way of protecting your important files and documents, as this helps to restore lost files because of virus attack.

Points to Note:

Apart from the main security options for your data, there are some more points that you should keep in mind. These are as follows:

- Indentify the symptoms of threats, so that you can take proper measures to tackle them
- Keep the virus database of your antivirus program updated
- Scan your system once in a week, to look out for new bugs
- Be alert of emails that ask for personal information
- Scan USB devices that you use for transferring data
- Keep your web browser and OS up to date

3.3 INTRUSION DETECTION SYSTEMS (IDS)

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An Intrusion Prevention System (IPS) is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.

Intrusion detection system usually performs the following activities.

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

3.3.1 Components of IDS

There are three main components to the Intrusion detection system.

a. Network Intrusion Detection system (NIDS)–It performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behaviour is sensed, the alert can be send to the administrator. Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into your firewall.

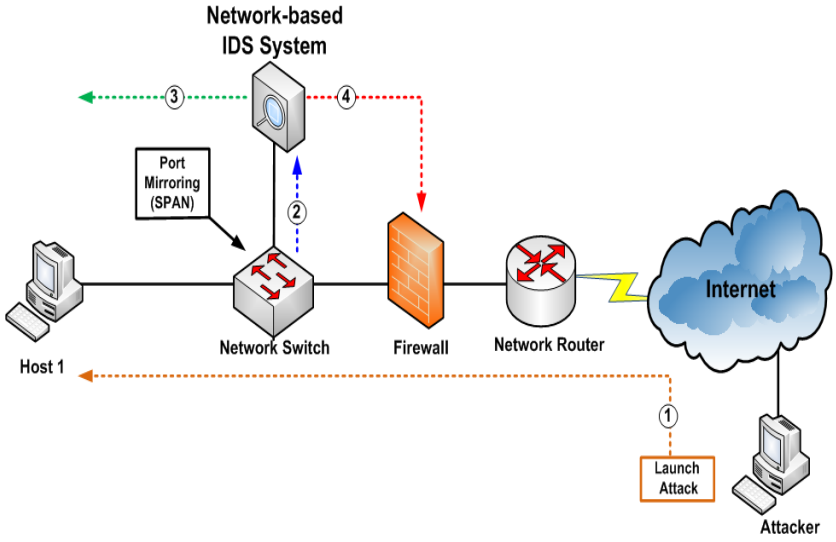


Fig: Network Intrusion Detection system (NIDS)

b. Host Intrusion Detection System (HIDS) – It takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines that are not expected to change their configuration.

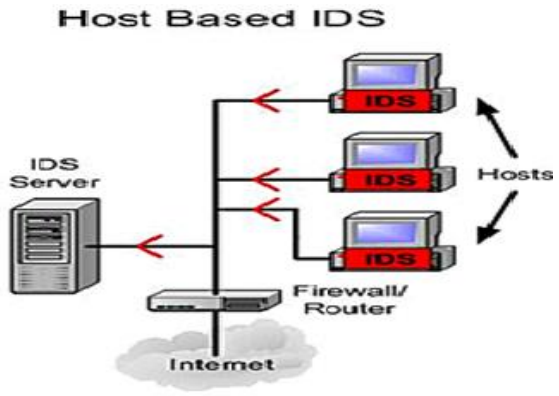


Fig: Host Intrusion Detection System (HIDS)

c. Network Node Intrusion detection system (NNIDS) – It performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device.

3.3.2 Functions of IDS

Irrespective of the type, all the IDS typically have the same functionalities as follows:

a) **Observing and monitoring**: An IDS observes the system and the network for any suspicious events. The criteria for observation depend on the type of IDS.

b) **Logging of Events**: On encountering a suspicious activity, the IDS records the information related to the observed activity. This is either performed locally by the concerned system (if the IDS has been installed on a single system) or by a centralized logging server (if the IDS has been set up for monitoring an entire network).

c) **Alerting System Administrators**: Once the events have been logged onto a database, the IDS can be set up to send alerts to the System Administrator. An IDS can send alerts through web pages, emails, messages, etc.

Reports on Intrusions:

A detailed report is prepared listing the details on the events, which had been captured and logged. These reports can be used by System Administrators to analyze the security setup for the organization and for determining vulnerabilities.

3.3.3 Intrusion Detection Methods

Broadly there are two types of detection methods namely signature-based and anomaly-based detections.

Signature-based Intrusion Detection

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

Anomaly-based Intrusion Detection

Anomaly-based IDS were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behaviour against this model. Although this approach enables the detection of previously unknown attacks, it suffers from false positives: previously unknown legitimate activity may also be classified as malicious.

3.3.4 Applications of IDS

An Intrusion Detection System can be implemented by an organization for the following reasons.

- An IDS tends to act as an extra layer of protection along with the other security mechanisms in an organization.
- It aids in the process of detecting intrusions and other malicious events when other security measures in the organization fail.
- It can detect an attack in its preliminary stages when the attacker initiates a port scan to determine vulnerable ports.
- It can log events and present reports that can be used by the system administrator to determine the existing threats to an organization.
- It acts as quality control tool and aids in strengthening the vulnerabilities in an organization.
- It provides an easy technique for analyzing the security measures of an organization.

3.3.5 Intrusion Prevention System (IPS)

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**) are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are considered as extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.

3.4 ANTIVIRUS SOFTWARE

Antivirus or anti-virus software, sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Antivirus software was originally developed to detect and remove computer viruses, hence the name.
However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious Browser Helper Objects (BHOs), browser hijackers, ransomware, key loggers, backdoors, root kits, Trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, Advanced Persistent Threat (APT), botnets and DDoS attacks.

3.4.1 Identification methods for viruses

One of the few solid theoretical results in the study of computer viruses is Frederick B. Cohen's 1987 demonstration that there is no algorithm that can perfectly detect all possible viruses. However, using different layer of defense, a good detection rate may be achieved. There are several methods which antivirus engine can use to identify malware:

- **Signature-based detection:** is the most common method. To identify viruses and other malware, the antivirus engine compares the contents of a file to its database of known malware signatures.

- **Heuristic-based detection:** is generally used together with signature-based detection. It detects malware based on characteristics typically used in known malware code.
- **Behavioural-based detection:** is similar to heuristic-based detection and used also in Intrusion Detection System. The main difference is that, instead of characteristics hardcoded in the malware code itself, it is based on the behavioural fingerprint of the malware at run-time. Clearly, this technique is able to detect (known or unknown) malware only after they have starting doing their malicious actions.
- **Sandbox detection:** is a particular behavioural-based detection technique that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment; logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not. If not, then, the program is executed in the real environment. Albeit this technique has shown to be quite effective, given its heaviness and slowness, it is rarely used in end-user antivirus solutions.
- **Data mining techniques:** are one of the latest approach applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file (as either malicious or benign) given a series of file features that are extracted from the file itself.

3.4.2 Signature-based detection

Traditional antivirus software relies heavily upon signatures to identify malware. Substantially, when a malware arrives in the hands of an antivirus firm, it is analyzed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software. When a particular file has to be scanned, the antivirus engine compares the contents of the file with all the malware signatures in the signatures database. If the file matches one signature, then the engine knows which malware it is and which procedure has to be performed in order to clean the infection.

Signature-based detection technique can be very effective but, clearly, cannot defend against malware unless some of its samples have already been obtained, a proper signature generated and the antivirus product updated. Signature-based detection systems rely on the premise that, generally speaking, the more infective a malware is the faster arrives in the hands of security researchers. Thus, even if it does not guarantee perfection, it protects from the most widespread threats.

However, this approach is not really effective against zero-day or next-generation malware, i.e. malware that has not been yet encountered / analysed.
As new malware are being created each day, the signature-based detection approach requires frequent updates of the signatures database. To assist the antivirus firms, the software may automatically upload new malware to the company or allow the user to manually do it, allowing the antivirus firms to dramatically shorten the life of those threats. Some antivirus products includes also advanced software to spot zero-day or next-generation malware.[citation needed]
Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of them or otherwise modify them as a method of disguise, so as to not match virus signatures in the dictionary.

3.4.3 Heuristics

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware. Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition. For example, the Vundo trojan has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, Trojan. Vundo and Trojan. Vundo. B. While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code. A detection that uses this method is said to be "heuristic detection."

3.4.4 Rootkit detection

Anti-virus software can attempt to scan for rootkits. A rootkit is a type of malware designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult

to remove, in some cases requiring a complete re-installation of the operating system.

3.4.5 Real-time protection

Real-time protection, on-access scanning, background guard, resident shield, auto protect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data loaded into the computer's active memory: when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.

3.5 KEY TERMS AND CONCEPTS

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations.

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**) are network security appliances that monitor network or system activities for malicious activity.

Antivirus or anti-virus software, also known as anti-malware software, is computer software used to prevent, detect and remove malicious software from a computer.

3.6 SELF-ASSESMENT QUESTIONS

1. What is an Intrusion Detection System? What are the different ways to classify an Intrusion Detection System?

   ……
   ……
   ……
   ……
   ……

2. What are drawbacks of signature based IDS?

   ……
   ……
   ……
   ……
   ……

3. What are characteristics of Host based IDS?

……
……
……
……
……
……

4. What are strengths of the host based IDS?

……
……
……
……
……

5. What is an antivirus? Why it is necessary?

……
……
……
……
……
……

3.7 REFERENCES AND SUGGESTED READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.
3. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.
4. https://en.wikipedia.org/wiki/Intrusion_detection_system
5. https://en.wikipedia.org/wiki/Antivirus_software

3.8 ANSWER TO SELF ASSESMENT QUESTIONS (UNIT1)

1. What do you mean by information assurance?

Information assurance (IA) is the practice of assuring **information** and managing risks related to the use, processing, storage, and transmission of **information** or data and the systems and processes used for those purposes. It is the act of ensuring that data is not lost when critical issues arise. These issues include natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

2. List different types of attacks on confidentiality?

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.

Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be conducted against data at rest or in motion. Properly executed, interception attacks can be very difficult to detect.

3. Name and explain possible attacks on Integrity and availability.

a) **Interruption** attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. In the case of a DoS attack on a mail server, we would classify this as an availability attack. In the case of an attacker manipulating the processes on which a database runs in order to prevent access to the data it contains, we might consider this an integrity attack, due to the possible loss or corruption of data, or we might consider it a combination of the two.

b) **Modification** attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.

c) **Fabrication** attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well. If we generate spurious information in a database, this would be considered to be a fabrication attack.

4. Differentiate between threat and attacks.

The differences between Threat and attacks are given below.

Threat	Attack
A threat is a category of objects, persons, or other entities that represents a constant danger to an asset.	An attack is an act or event that exploits vulnerability.
Threat can be either intentional or unintentional	Attack is always intentional
Threat is a circumstance that has potential to cause loss or damage.	Attack is attempted to cause damage
Threat to the information system doesn't mean information was altered or damaged	Attack on the information system means there might be chance to alter, damage, or obtain information when attack was successful.

5. Differentiate between threat, vulnerabilities and risks with an example.

Threat is a potential cause of an incident that may result in harm to an Information system or organization

Vulnerability is a **weakness of an asset** (resource) or a group of assets that can be exploited by one or more threats

Risk is a potential for loss, damage, or destruction of an asset as a result of a threat exploiting vulnerability

Example: In a system that allows weak passwords, here

a. Vulnerability means the password is vulnerable for dictionary or exhaustive key attacks
b. Threat means "An intruder can exploit the password weakness to break into the system"
c. Risk means "the resources within the system are prone for illegal access/modify/damage by the intruder".

3.9 ANSWER TO SELF ASSESMENT QUESTIONS (UNIT-2)

1. What is a malware? Name different types of malwares?

Malware stands for *—Malicious Software* and it is designed to gain access or installed into the computer without the consent of the user.

The most common types of malware; adware, bots, bugs, root kits, spyware, Trojan horses, viruses, and worms.

2. What is Virus? How does it harm a computer?

A **computer virus** is a malware that, replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". Whenever the host programs are executed, the virus instructions get activated along with the program.

A virus should never be assumed harmless. It can harm your computer in many ways. Viruses affect your computer by corrupting files, interrupting Internet traffic and taking over basic functions of your operating system. These behaviours can knock a system offline and cause crashes. Viruses can record keystrokes and screen data, and they may steal personal information and passwords to transmit back to the malware author.

3. What is the difference between a worm and a virus?

Viruses and worms: Viruses and worms are very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software's or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples. Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained.

4. What is a scareware?

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user‘s computer.

As a remedial measure, the message suggests the used download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid.

5. What is a Trojan horse?

A Trojan virus is a piece of software designed to look like a useful file or software program but performs a possibly nefarious function once installed on a client computer. The virus takes its name from the ―Trojan Horse, from Greek mythology setup outside of the city of Troy. Trojan horse viruses differ from other computer viruses in that they are not designed to spread themselves. Instead Trojan horse malware is either delivered as the payload of another virus or piece of malware or through manual end-user action by downloading infected files or inserting infected drives into a computer. Once a computer is infected with a Trojan virus, the malware can be designed to steal end-user information, perform destructive harm on the target computer, or even download additional computer malware. A Trojan virus will normally consist of a server and client component. The client component is the portion of the malware that infects the end-user‘s computer. Once established or executed, the virus can be designed to establish a certain level of control over the infected computer.

It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer.

3.10 ANSWER TO SELF ASSESMENT QUESTIONS (UNIT-3)

1. **What is an Intrusion Detection System? What are the different ways to classify an Intrusion Detection System?**

   An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

   The two main categories of Intrusion Detection Systems are:

   - Signature-based Intrusion Detection
   - Anomaly-based Intrusion Detection

2. **What are drawbacks of signature based IDS?**

   The main drawbacks include the following.

   - They suffer from false alarms.
   - They have to be programmed again for every new pattern to be detected
   - They are unable to detect novel attacks

3. **What are characteristics of Host based IDS**?

   The main characteristics of Host Based IDS are as follows.

   - The host operating system logs in the audit information
   - Logs includes logins, file opens and program executions
   - Logs are analyzed to detect tails of intrusion

4. **What are strengths of the host based IDS?**

   Some of the advantages of host based IDS include the following.

   - They can do attack verification
   - They perform system specific activity
   - No additional hardware is required

5. **What is an antivirus? Why it is necessary?**

   Antivirus or anti-virus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, Trojan horses, spyware and adware.

   However, it is possible that a computer may be infected with new malware for which no signature is yet known.

   An antivirus is necessary because it protects our computer from malicious attacks and prevents data loss by malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers.