Group no: - 8

Group Member:- Shrut Shah – 19BCP125

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 1:- Overview of Cyber Security

Introduction

- Viruses, worms, Trojans, and bots are all part of a class of software called malware. Malware or maliciouscode (malcode) is short form of **malicious software**. It is code or software that is specifically designed todamage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.
- There are many different classes of malware that have varying ways of infecting systems and propagatingthemselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability (weak point) in an operating system (OS), network device, or other software.
- Some of the more commonly known types of malware are viruses, worms, Trojans, bots, back doors, spyware, and adware. Damage from malware varies from causing minor irritation (such as browser popupads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks.
- Malware cannot damage the physical hardware of systems and network equipment, but it can damage thedata and software residing on the equipment.

VIRUS

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another,leaving infections as it travels. Like a human virus,
- Almost all viruses are attached to an executable file, which means the virus may exist on your computerbut it actually cannot infect your computer unless you run or open the malicious program.
- It is important to note that a virus cannot be spread without a human action, (such as running an infectedprogram) to keep it going.

Worms

- A worm is similar to a virus by design and is considered to be a sub-class of a virus.
- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.
- The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating ahuge devastating effect.
- Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth)

Trojan Horse

- A Trojan is a harmful piece of software that looks legitimate (legal).
- Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses).
- Trojans are also known to create back doors to give malicious users access to the system.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

Insiders

- A malicious insider threat to an organization is a current or former employee, contractor, or other businesspartner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

- Insider attacks are among the most difficult to detect and prevent.
- Employees already have access and knowledge about the structure and content of corporate databases.

Intruders

- One of the two most publicized threats to security is the intruder (the other is viruses), often referred to asa hacker or cracker
- Intruders can be classified in three Classes:
    - **Masquerader:** An individual who is not authorized to use the computer and who penetrates asystem's access controls to exploit a legitimate user's account
    - **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access isnot authorized, or who is authorized for such access but misuses his or her privileges
    - **Clandestine user:** An individual who seizes supervisory control of the systemand uses thiscontrol to evade auditing and access controls or to suppress audit collection
- The **masquerader** is likely to be an **outsider**; the **misfeasor** generally is an **insider**; and the **clandestine**

  user can be either an **outsider** or an **insider.**

Terrorists

- The terrorists use cyberspace to cause uncertainty. They, for their own reasons, are struggling against stateauthorities and governments and use all available means to achieve their own aim.
- Cyber attacks occur in two forms, one used to attack data, and others focused on control systems.
- The attacks focused on the control systems are used to disable or manipulate the physical infrastructure.
    - A **Trojan** is a program that has hidden instructions enabling it to carry out a malicious act such as thecapture of passwords. These could then be used in other forms of attack.
    - A **worm** is a program that can replicate itself and create a level of demand for services that cannot besatisfied.
    - The term **virus** is also used for a worm that replicates by attaching itself to other programs.

❖ Security Basics – Confidentiality, Integrity, Availability

Data confidentiality

- When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties (wrong Person).
- Information has value, especially in today's world. Bank account statements, personal information, credit card numbers, trade secrets, government documents. Everyone has information they wish to keep a secret. Protecting such information is a very major part of information security.
- A very key component of protecting information confidentiality would be (Authentication methods) encryption. Encryption ensures that only the right people (people who knows the key) can read the information. Encryption is VERY widespread in today's environment and can be found in almost everymajor protocol in use.

Integrity

- Integrity of information refers to protecting information from being modified by unauthorized parties.
- Information only has value if it is correct. Information that has been tampered with could prove costly. For example, if you were sending an online money transfer for $100, but the information was tamperedin such a way that you actually sent $10,000, it could prove to be very costly for you.
- As with data confidentiality, cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparingit with the hash of the original message. However, this means that the hash of the original data must beprovided to you in a secure fashion.

Availability

- Availability of information refers to ensuring that authorized parties are able to access the information when needed.
- Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. Almost every week you can find news abouthigh profile websites being taken down by DDoS attacks.
- The primary aim of DDoS attacks is to deny users of the website access to the resources of the website.Such downtime can be very costly. Other factors that could lead to lack of availability to

important information may include accidents such as power outages or natural disasters such as floods.

- How does one ensure data availability? **Backup is key**. Regularly doing off-site backups can limit the damage caused by damage to hard drives or natural disasters.

Authentication

- Corroboration of the identity of an entity. Two specific authentication services are defined in the standard.
  - ✓ ***Peer Entity Authentication: -***
    - Used in association with a logical connection to provide confidence in the identity of theentities connected.
  - ✓ ***Data Origin Authentication: -***
    - In connection less transfer, provides assurance that the source of received data is as claimed.

Access Control

- In the context of network security, access control is the ability to limit and control the access to host system and application via communication links.
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Non-repudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. There are two types of specific services in Non-repudiation.
  - ✓ ***Non-repudiation, origin:***
    - Proof that the specific parties sent the massage.
  - ✓ ***Non-repudiation, Destination:***
    - Proofs that the massage was receive by the specific parties.

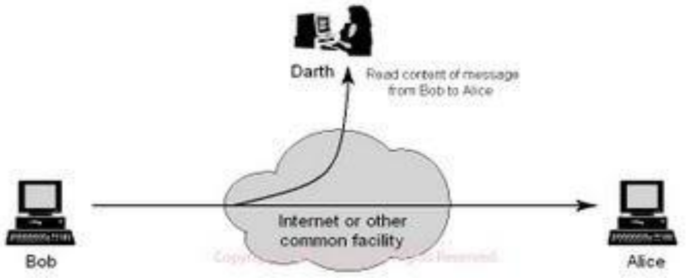
❖ Types of attack:

Passive Attack

- There are two main types of passive attacks and they are release of message contents and trafficanalysis.

1. ***Release of Message contents***

   - In this type of passive attack a mail message, phone call any transferred message pretty muchof sensitive information that would be intercepted or listened to.


Darth
Read content of message from Bob to Alice
Internet or other common facility
Bob
Alice

Release of message contents (Passive Attacks)

Copyright © 2007 kunal. All rights reserved.

2. ***Traffic Analysis***

   - **Traffic Analysis** is a little more complicated. It is very subtle and hard to detect it would be likethis if we had a way to hide the information on a message and the hacker still viewed the information this would be a traffic analysis attack.

   - **Passive attacks** include traffic analysis, monitoring of unprotected communications, decryptingweakly encrypted traffic, and capturing authentication information such as passwords. Active Attack.

- Passive attacks are very hard to detect because they don’t damage or change the information so you can’t tell they have been attacked. There are many different programs out there than can help monitoragainst this type of network attack and against many other attacks. Again these are made for spying and for the attacker not to be noticed.

Active attacks

- An **active attack** is one in which an unauthorised change of the system is attempted. This couldinclude, for example, the modification of transmitted or stored data, or the creation of new data streams.

- There are four sub-categories here: masquerade or fabrication, message replay, message modificationand denial of service or interruption of availability.

  1. **Masquerade attacks**, as the name suggests, relate to an entity (usually a computer or a person)taking on a false identity in order to acquire or modify information, and in effect achieve an unwarranted privilege status. Masquerade attacks can also incorporate other categories.
  2. **Message replay** involves the re-use of captured data at a later time than originally intended in order to repeat some action of benefit to the attacker: for example, the capture and replay of aninstruction to transfer funds from a bank account into one under the control of an attacker. Thiscould be foiled by confirmation of the freshness of a message.
  3. **Message modification** could involve modifying a packet header address for the purpose ofdirecting it to an unintended destination or modifying the user data.
  4. **Denial-of-service attacks** prevent the normal use or management of communication services, and may take the form of either a targeted attack on a particular service or a broad, incapacitating attack. For example, a network may be flooded with messages that cause a degradation of service or possibly a complete collapse if a server shuts down under abnormal loading. Another example israpid and repeated requests to a web server, which bar legitimate access to others. Denial-of- service attacks are frequently reported for internet-connected services.

Distributed Attack

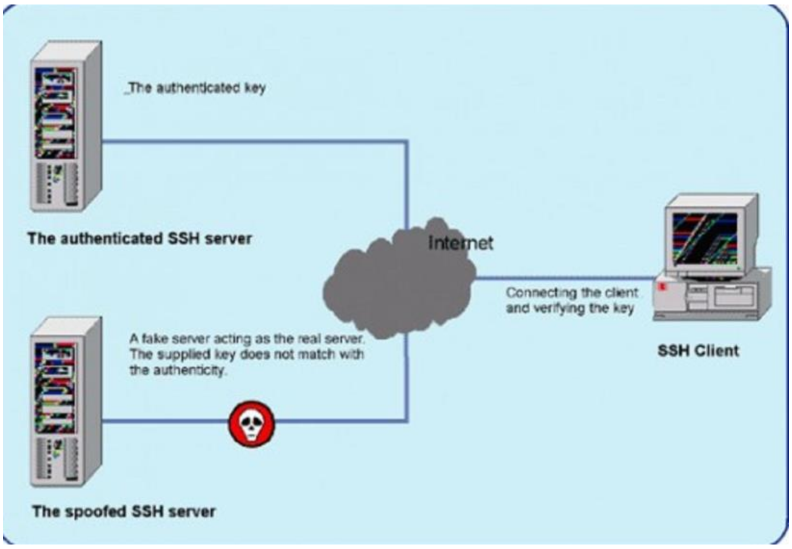
- A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-doorprogram, to a “trusted” component or software that will later be distributed to many other companiesand users.
- Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution.
- These attacks introduce malicious code such as a back door to a product to gain unauthorized access toinformation or to a system function at a later date.

Phishing Attack

- In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as theSBI bank or paypal.
- The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the userinto clicking a link that leads to the fake site.
- When the user attempts to log on with their account information, the hacker records the username andpassword and then tries that information on the real site.

Spoofing attack

- In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.


The authenticated key
The authenticated SSH server
Internet
Connecting the client and verifying the key
SSH Client
A fake server acting as the real server. The supplied key does not match with the authenticity.
The spoofed SSH server

- Any internet connected device necessarily sends IP datagrams into the network. Such internet datapackets carry the sender's IP address as well as data.
- If the attacker obtains control over the software running on a network device, they can then easilymodify the device's protocols to place an arbitrary IP address into the data packet's source addressfield. This is known as IP spoofing.

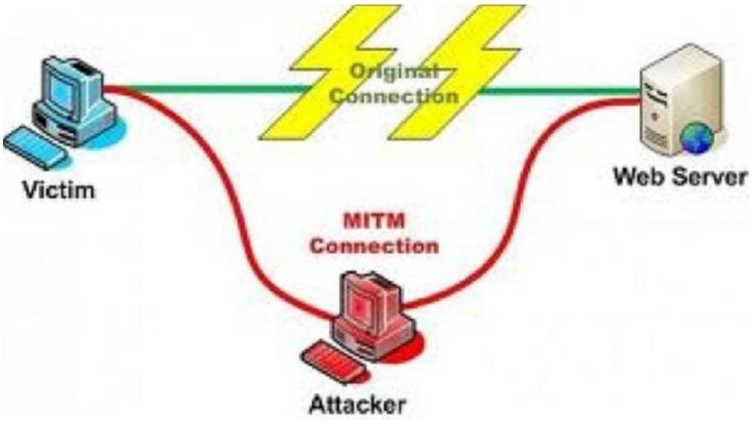
Denial-of-Service Attack

- DoS attack, denial-of-service attack, is an explicit attempt to make a computer resource unavailable byeither injecting a computer virus or flooding the network with useless traffic.
- There are two types of DoS attacks: **Computer attack** and **Network attack**

- ✓ attempts to "flood" a network, thereby preventing legitimate network traffic
- ✓ attempts to disrupt connections between two machines, thereby preventing access to a service
- ✓ attempts to prevent a particular individual from accessing a service
- ✓ attempts to disrupt service to a specific system or person

Man-in-the-Middle Attack

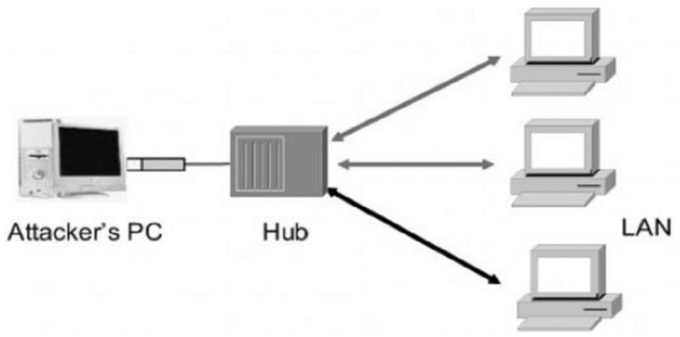
- ➢ As the name indicates, a man-in-the-middle attack occurs when someone between you and the personwith whom you are communicating is actively monitoring, capturing, and controlling your communication transparently.



- ➢ This type of attack is also an access attack, but it can be used as the starting point of a modificationattack.
- ➢ This involves placing a piece of software between a server and the user that neither the server administrators nor the user are aware of.
- ➢ This software intercepts data and then send the information to the server as if nothing is wrong.
- ➢ The server responds back to the software, thinking it's communicating with the legitimate client.
- ➢ Theattacking software continues sending information to the server and so forth.
- ➢ Man-in-the-middle attacks are like someone assuming your identity in order to read your message.
- ➢ The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information.
- ➢ This attack is capable of the same damage as an application-layer attack, described later in this section.

Network sniffing (Packet sniffing)

- A sniffer is an application that can capture network packets.



- Sniffers are also known as network protocol analyzers.
- While protocol analyzers are really network troubleshooting tools, they are also used by hackers forhacking network.
- If the network packets are not encrypted, the data within the network packet can be read using asniffer.
- Sniffing refers to the process used by attackers to capture network traffic using a sniffer.
- Once the packet is captured using a sniffer, the contents of packets can be analyzed.
- Sniffers are used by hackers to capture sensitive network information, such as passwords, accountinformation etc.

Backdoor

- This can have two different meanings.

1) During the development of a complicated operating system or application, programmers add backdoors or maintenance hooks. These back doors allow them to examine operations inside the codewhile the program is running.

2) The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user to log in without a password or gain administrative privileges. A number of tools exist to create a back doorattack such as, Back Orifice, Subseven, NetBus, and NetDevil.

Trapdoors

- A trap door is a secret entry point into a program that allows someone that is aware of the trap door togain access without going through the usual security access procedures.
- Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access. It is difficult to implement operating system controls for trap doors.
- A trap doors in a computer system is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected

Logic Bomb

- Logic bombs are a malicious programming code that is inserted into a network system or a single computer for the purpose of deleting data or creating other malicious acts on a specified date. A logic bomb works similar to a time bomb because it can be set to go off at a specific date. A logic bomb doesnot distribute malicious codes until the specified date is reached.
- The criminal acts include setting a virus to be released into a network system or PC at a specified date or other actions such as deleting or corrupting data and completely reformatting a computer hard drive.
- A logic bomb can be rather difficult to detect, however you can take security measures such as constantly monitoring the network system for any suspicious activity, using antivirus applications and other scanning programs that can detect any new activity in the data on a network system. The scanning systems should also monitor the entire network and the individual computers connected to thenetwork.

Replay Attacks

- These are becoming quite common, This occur when information is captured over a network.
- Replay attacks are used for access or modification attacks.
- In a distributed environment, logon and password information is sent over the network between theclient and the authentication system.
- The attacker can capture this information and replay it later. This can also occur security certificatesfrom systems such as Kerberos.
- The attacker resubmits the certificate, hoping to be validated by the authentication system, andcircumvent any time sensitivity.