UNIT:1

Introduction and Security threats

CONTENT

- 1.1 Threats to Security
- 1.2 Avenues of Attack
- 1.3 Security Basics
- 1.4 Types of Attacks

Introduction and Security threats

- Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare
- Avenues of Attack, steps in attack
- Basics of Security
- Types of Attack

1.1 Threats to security

- Viruses and Worms
- Intruders, Insiders
- Criminal organizations
- Terrorists
- Information warfare

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 computer but 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 infected program).

Worms

- 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.

INTRUDERS

- One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker.
- Intruders can be classified in three Classes:
- **Masquerader:**

  An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
- **Misfeasor:**

  A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- **Clandestine user:**

  An individual who takeover supervisory control of the system and uses this control to to suppress audit collection

INSIDERS

- A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data.
- He is 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.

TERRORISTS

- The terrorists use cyberspace to cause uncertainty.
- They, for their own reasons, are struggling against state authorities 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.

INFORMATION WARFARE

- **Information warfare** (IW) is a concept involving the battle space use and management of **information** and communication technology in pursuit of a competitive advantage over an opponent.

CRIMINAL ORGANIZATION

- **Organized crime** is a category of transnational, national, or local groupings of highly centralized enterprises run by **criminals** who intend to engage in illegal activity, most commonly for money and profit.
- Some **criminal organizations**, such as terrorist groups, are politically motivated.

1.2 Avenue of Attack/steps in attack

- Two reasons for attack:
- 1)Specifically targeted by the attacker
- 2)Opportunistic target

STEPS IN ATTACK

Step 1: Information gathering: The attacker will gather as much information about organization as possible.

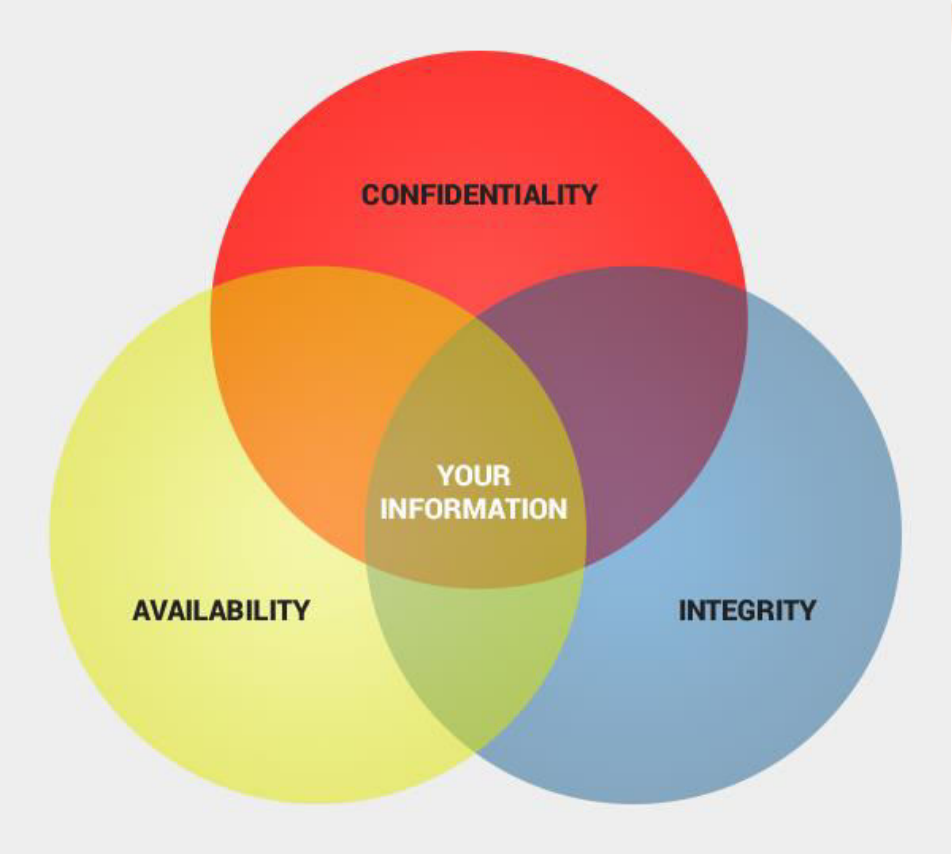
Step 2: Determination of target system: Then determine what target systems are available and active.

Step 3: Find vulnerability & suitable tools: To perform a port scan which gives indication of which services are running on target machine.

Step 4: Attack to the target system: Actualy attacking the target system.

1.3 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.

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 tampered in such a way that you actually sent $10,000, it could prove to be very costly for you.

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.
- 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.

1.4 Types of attack

- Denial of service (DOS),
- backdoors and trapdoors,
- sniffing,
- spoofing,
- man in the middle, replay,
- TCP/IP Hacking,
- Phishing attacks,
- Distributed DOS,
- SQL Injection
- Malware : Viruses, Logic bombs

Denial-of-Service Attack

- DoS attack, denial-of-service attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic.
- It attempts to "flood" a network, thereby preventing legitimate network traffic
- It attempts to disrupt connections between two machines, thereby preventing access to a service
- It attempts to prevent a particular individual from accessing a service
- It attempts to disrupt service to a specific system or person

Preventing Denial of Service (SYN Flood)

- DoS is caused by asymmetric state allocation
  - If server opens new state for each connection attempt, attacker can initiate many connections from bogus or forged IP addresses
- Cookies allow server to remain stateless until client produces:
  - Server state (IP addresses and ports) stored in a cookie and originally sent to client
- When client responds, cookie is verified

DoS and DDoS

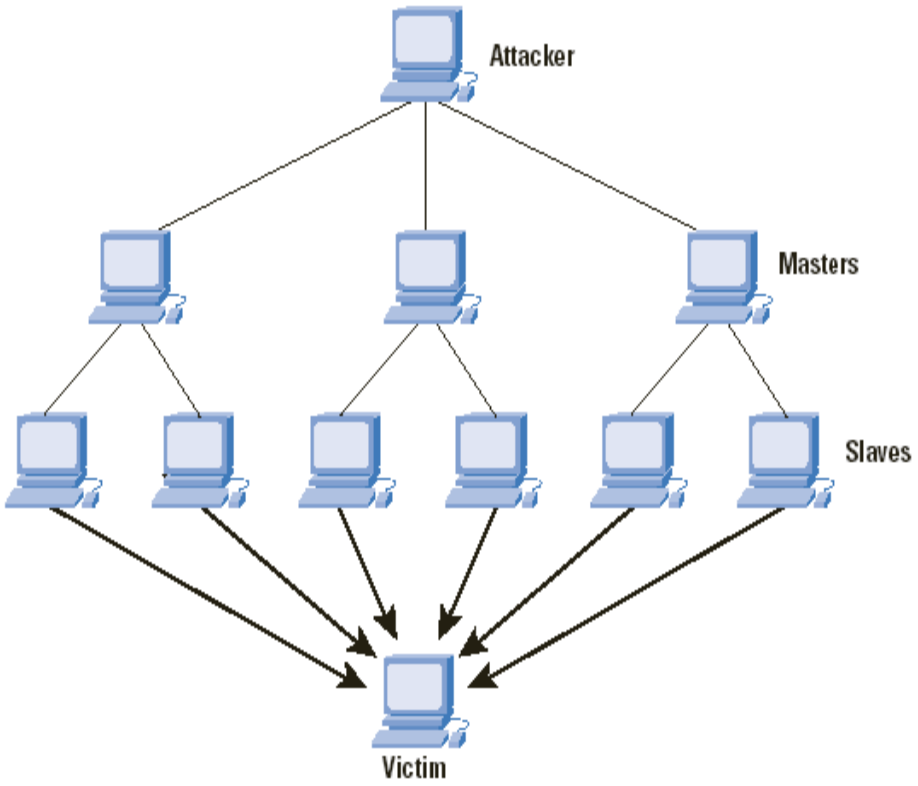
- DoS:
  - source of attack small # of nodes
  - source IP typically spoofed
- DDoS
  - From thousands of nodes
  - IP addresses often not spoofed

DDoS Attacks

- In a typical DDoS attack, the army of the attacker consists of *master zombies* and *slave zombies*.
- The hosts of both categories are compromised machines that have arisen during the scanning process and are infected by malicious code.
- The attacker coordinates and orders master zombies and they, in turn, coordinate and trigger slave zombies.
- The attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking.
- Then, master zombies, through those processes, send attack commands to slave zombies, ordering them to mount a DDoS attack against the victim.
-

CONTINUE…

In that way, the agent machines (slave zombies) begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources.



BACKDOORS

- 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 code while 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 door attack such as, Back Orifice, Subseven, NetBus, and NetDevil

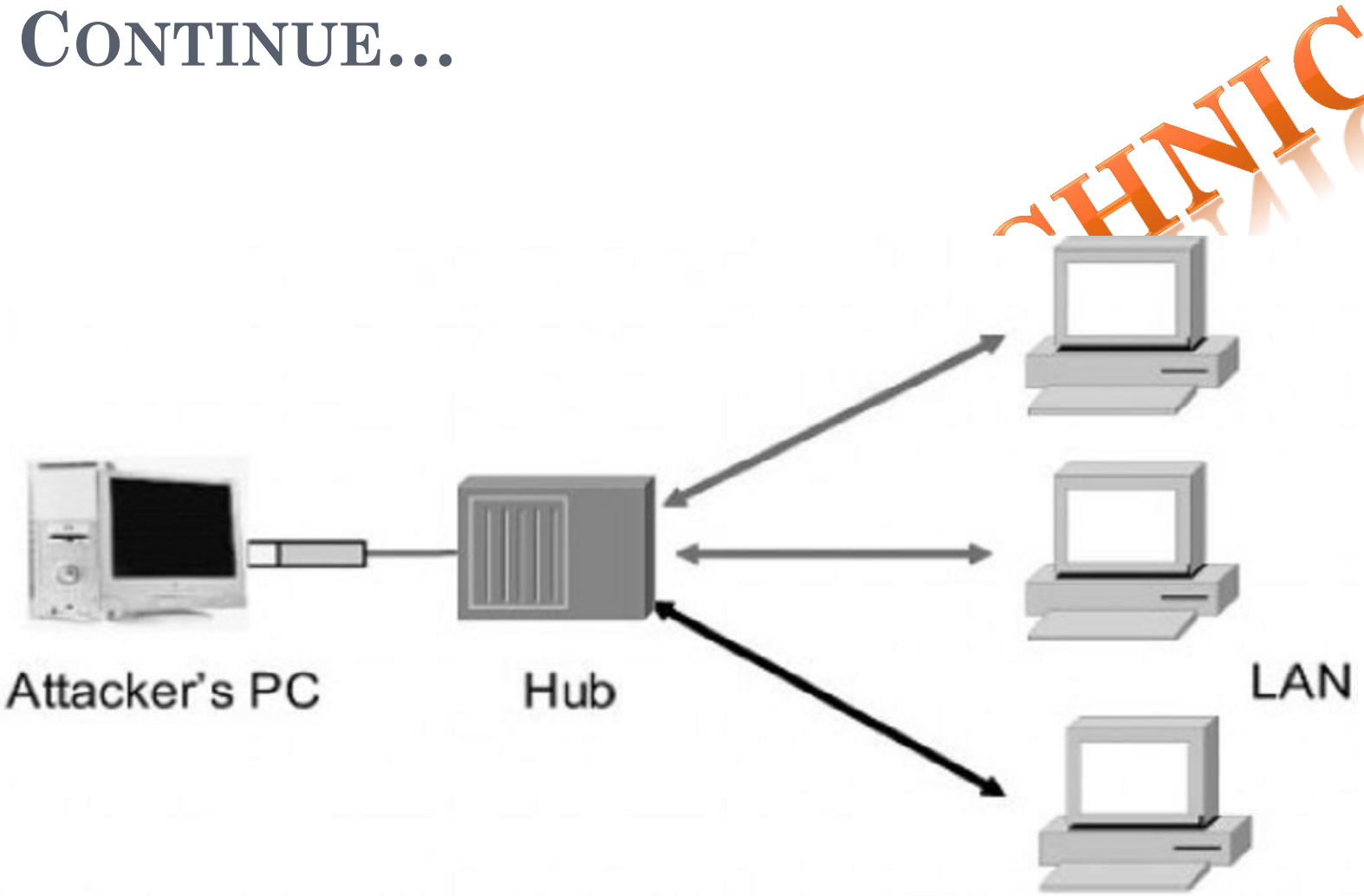
TRAPDOORS

- A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures.
- It is difficult to implement operating system controls for trap doors.

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 for hacking network.

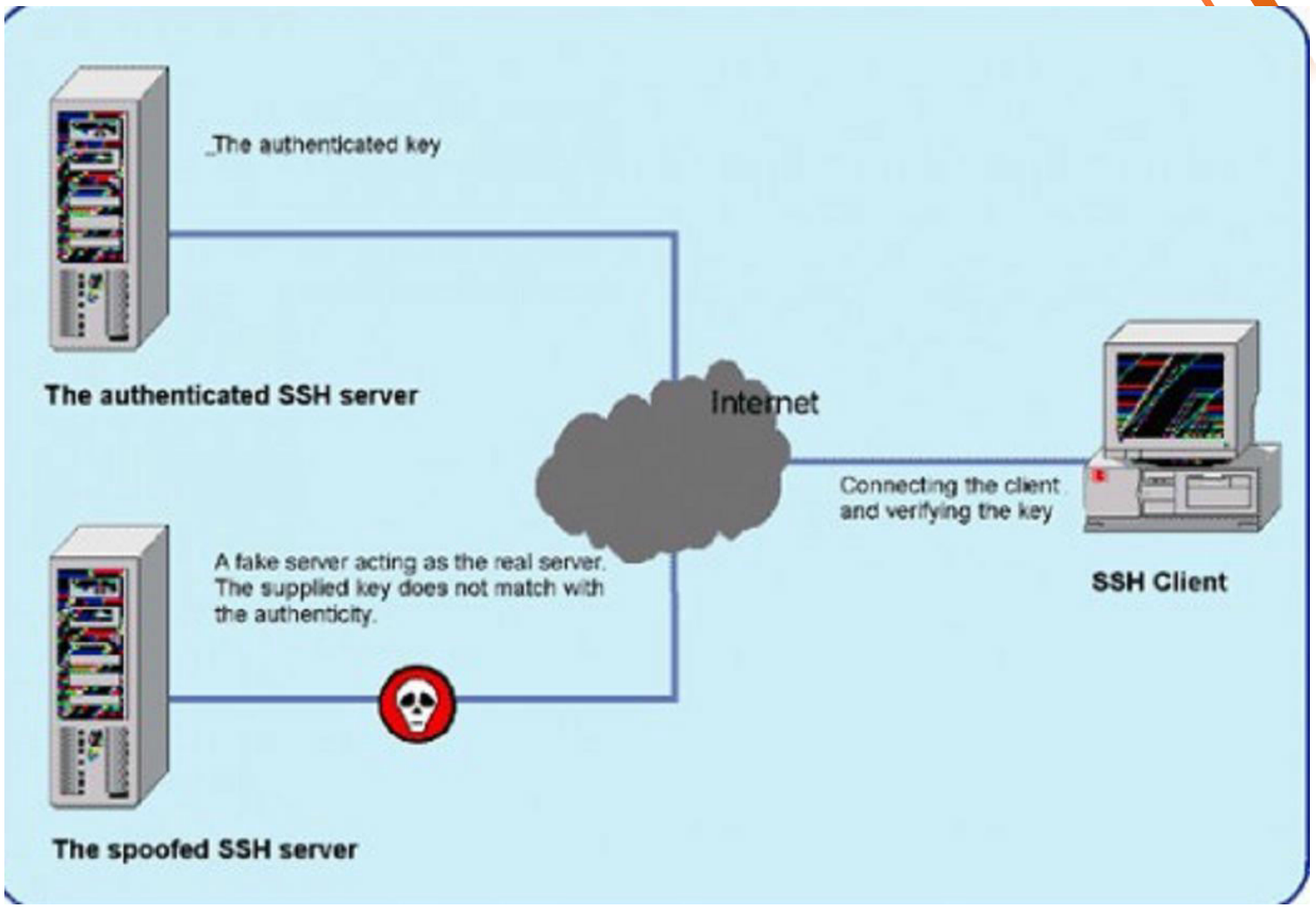
CONTINUE…



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.
- Any internet connected device necessarily sends IP datagram into the network. Such internet data packets 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 easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as **IP spoofing.**

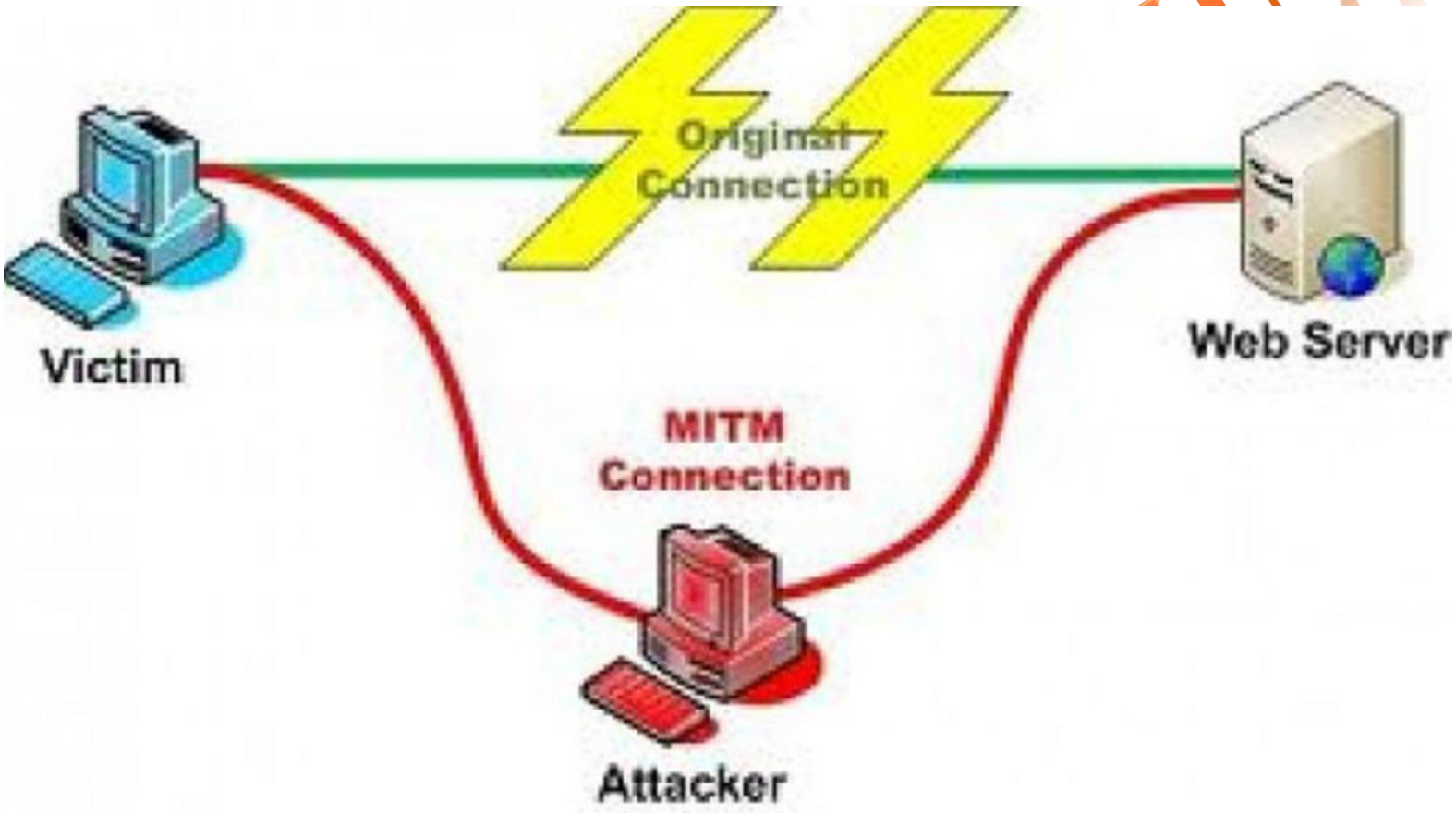
CONTINUE…


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

MAN-IN-THE-MIDDLE ATTACK

- As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with 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 modification attack.
- This involves placing a 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.
- The attacking software continues sending information to the server and so forth.

CONTINUE…

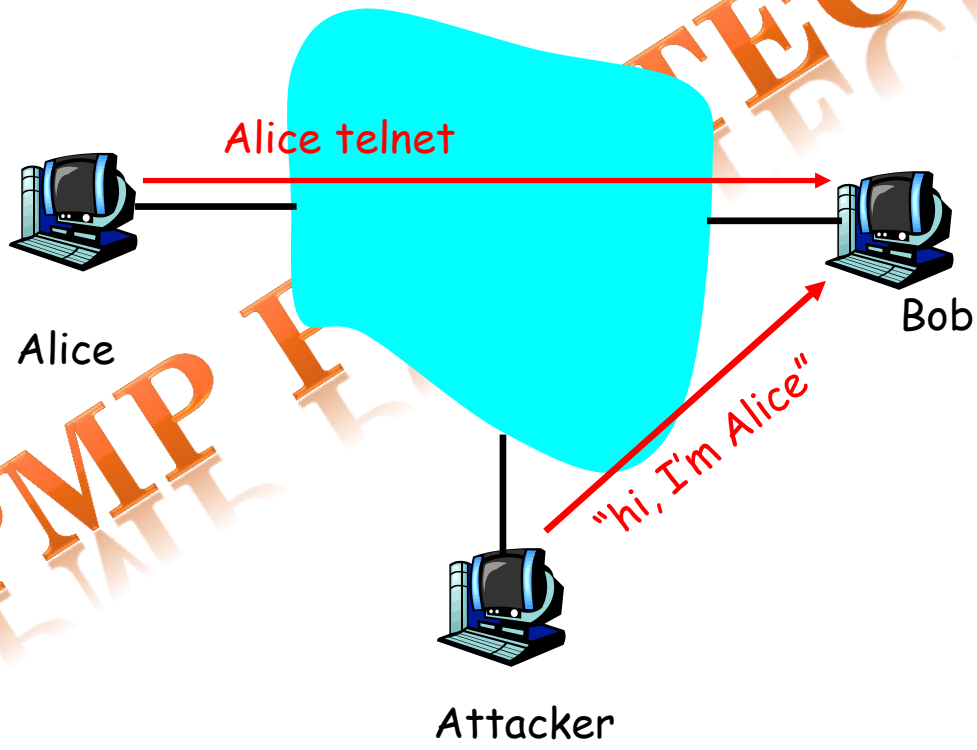

Original Connection
Victim
Web Server
MITM Connection
Attacker

MESSAGE REPLAY

- 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 an instruction to transfer funds from a bank account into one under the control of an attacker. This could be foiled by confirmation of the freshness of a message.

TCP/IP Hacking

- Take control of one side of a TCP connection
- Combination of sniffing and spoofing



Session hijacking: The details

- Attacker is on segment where traffic passes from Alice to Bob
  - Attacker sniffs packets
  - Sees TCP packets between Bob and Alice and their sequence numbers
- Attacker jumps in, sending TCP packets to Bob; source IP address = Alice's IP address
  - Bob now obeys commands sent by attacker, thinking they were sent by Alice
- Principal defense: encyrption
  - Attacker does not have keys to encrypt and insert meaningful traffic

Session Hijacking Tools

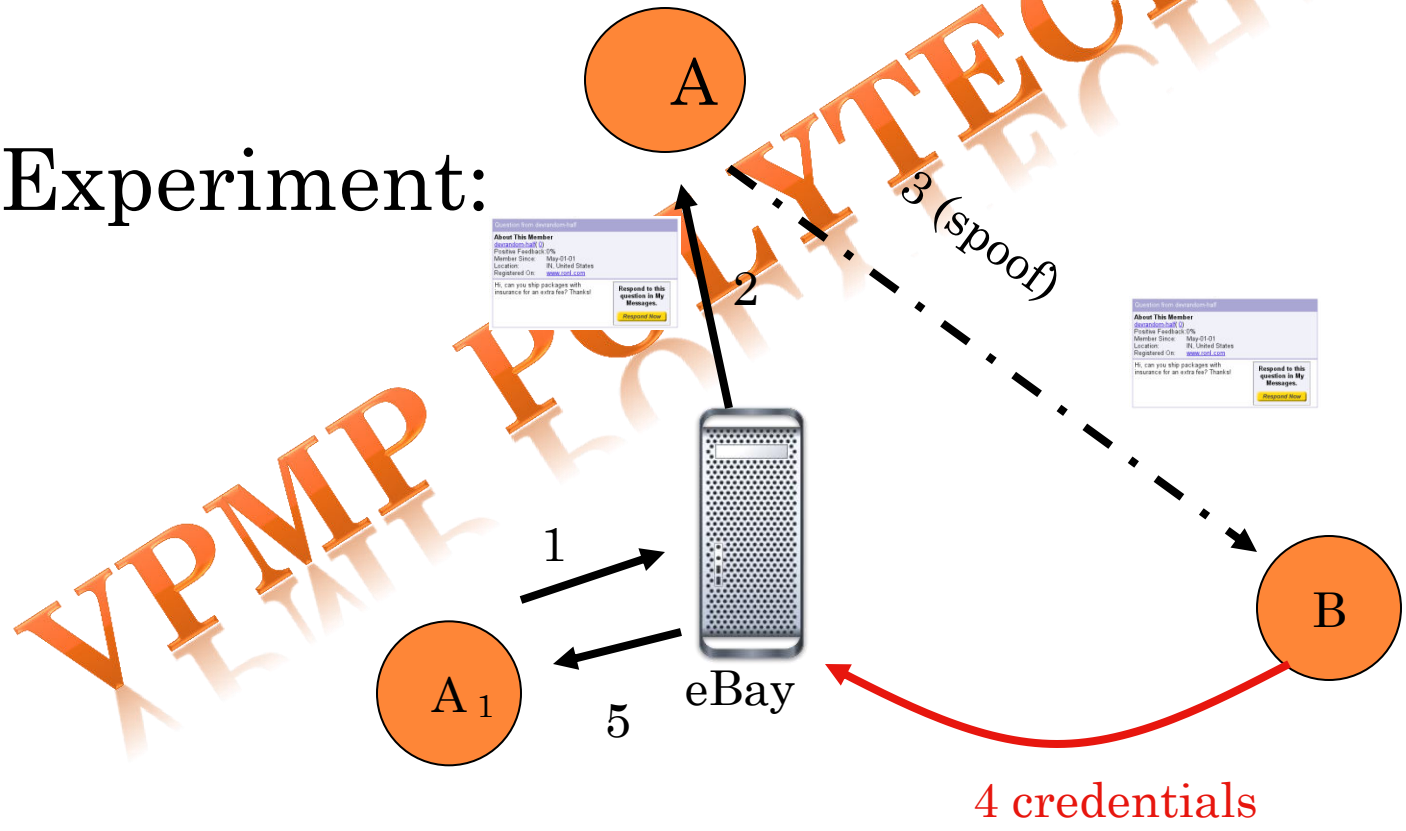
- Hunt
  - http://ihackers.co/hunt-session-hijacking-tool/
  - Provides ARP poisoning
- Netcat
  - General purpose widget
  - Very popular

Phishing Attack

- In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal.
- The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into 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 and password and then tries that information on the real site.

CONTINUE…

Experiment:



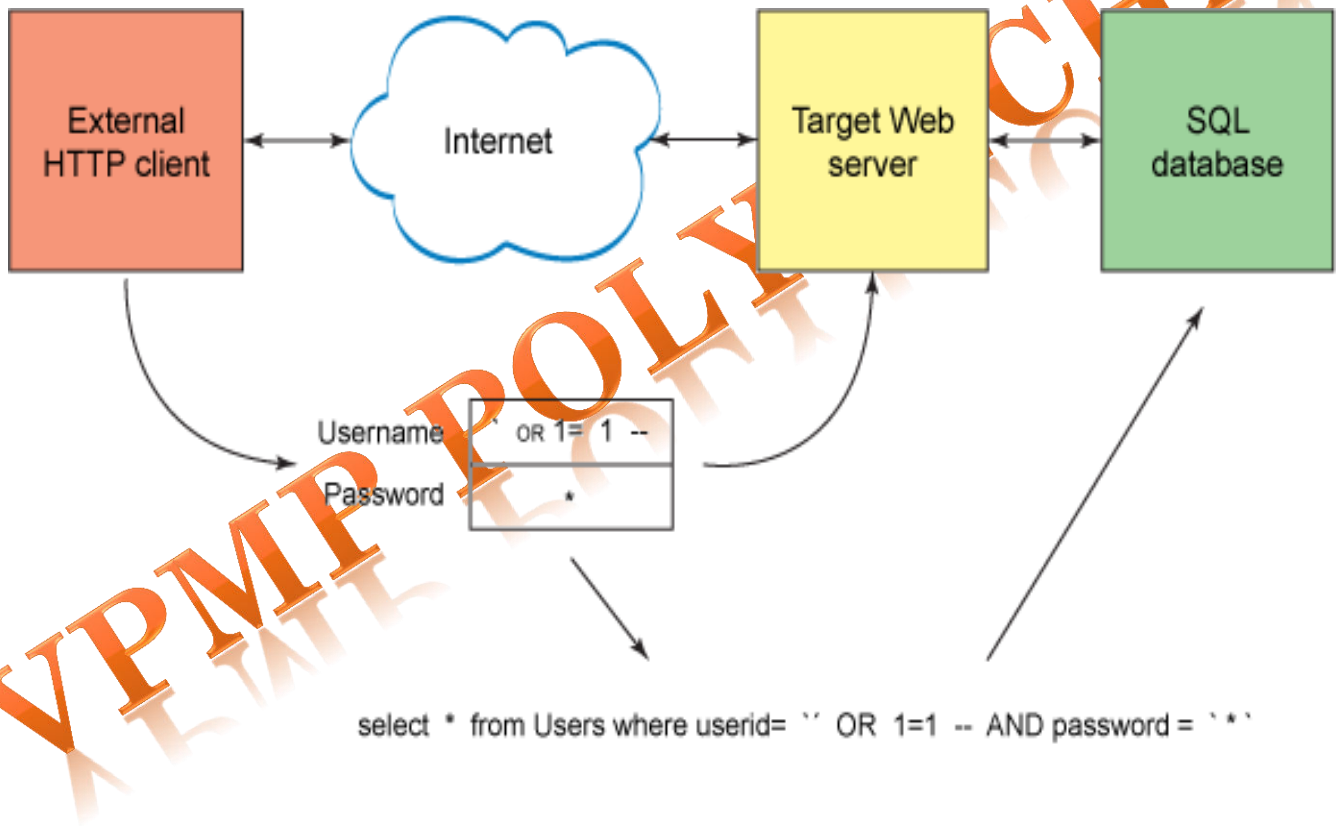
SQL Injection

- SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input.
- Injected SQL commands can alter SQL statement and compromise the security of a web application.
- When SQL is used to display data on a web page, it is common to let web users input their own search values.
- Since SQL statements are text only, it is easy, with a little piece of computer code, to dynamically change SQL statements to provide the user with selected data:

CONTINUE…

- **Server Code**
- txtUserId = getRequestString("UserId");
  txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
- The example above, creates a select statement by adding a variable (txtUserId) to a select string. The variable is fetched from the user input (Request) to the page.

Simple SQL injection attack figure



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 does not distribute malicious codes until the specified date is reached.
- 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.

VIRUSES

- A VIRUS is a small program written to alter the way a computer operates, without permission or knowledge of the user.
- Two Criteria:
  - it must execute itself.
  - It must replicate itself.
- Five categories:
  - File infector viruses
  - Boot sector viruses
  - Master-boot record viruses
  - Multi partite viruses
  - Macro viruses

CONTINUE…

- File infector viruses: It infects program files such as .exe, .com.
- Boot sector viruses: It infects the system area of disk like boot record on hard disk.
- Master-boot record viruses: It saves a copy of master boot record in a different location.
- Multi partite viruses: It infects both, program files as well as boot records.
- Macro viruses: It infects data files like Microsoft excel, word, access, power point files.