Unit 2 Notes

Introduction

- Technology is a double-edged sword
- Target of offense and false sense of anonymity
- Misuse of information
- Agencies collect information about the individuals
- Cyber criminals use WWW and internet for all illegal activities
- Lack of awareness and about cybercrime and cyber laws.
- People who commit cybercrimes are known as **crackers.**

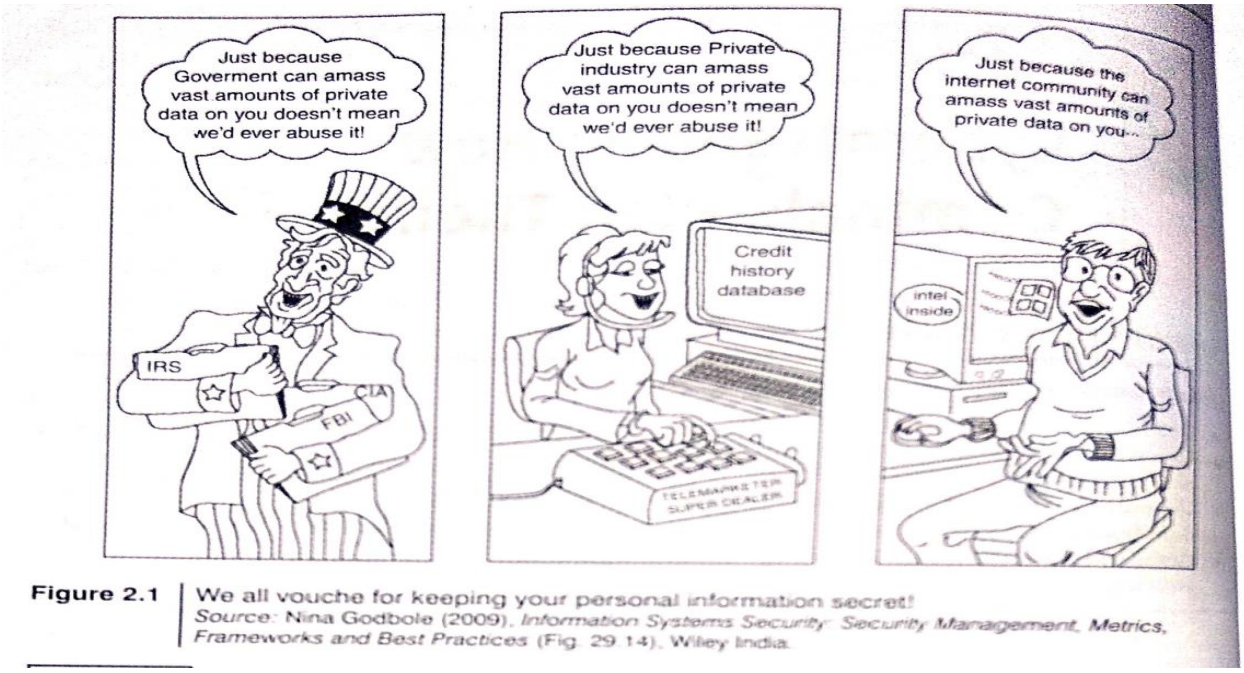
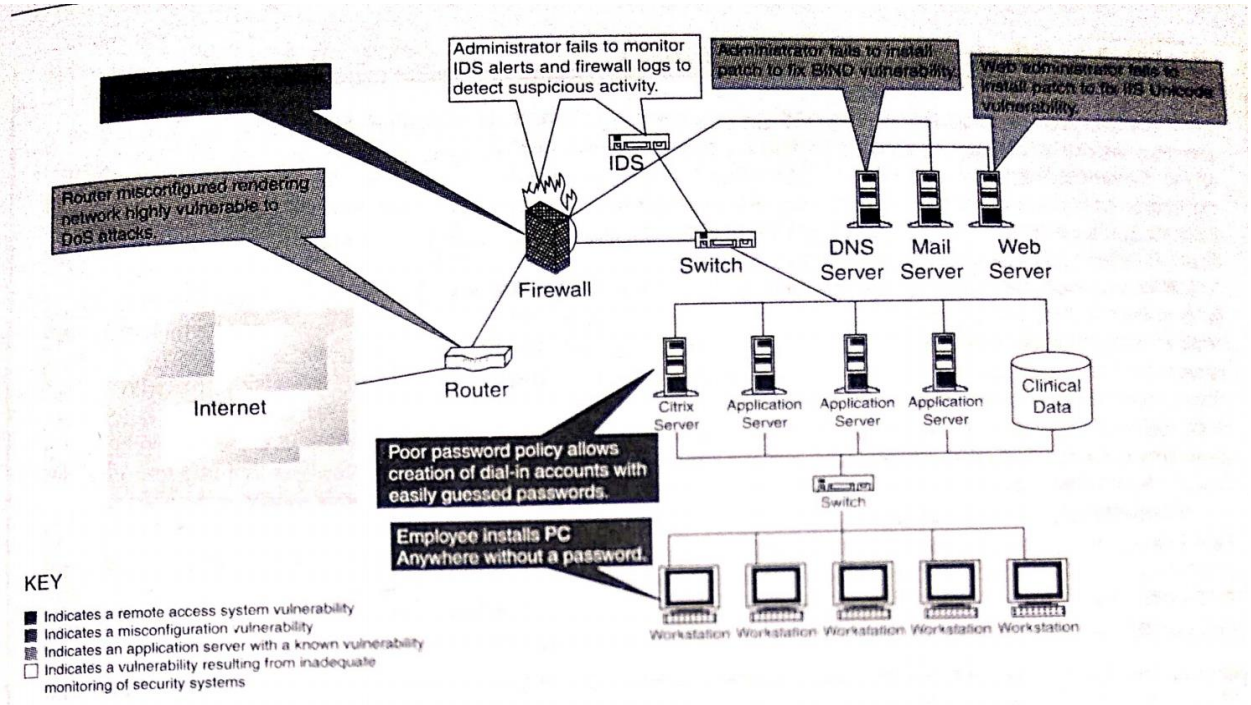


Figure 2.1 We all vouche for keeping your personal information secret!
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

- An attacker would look to exploit the vulnerabilities in the network.
- **Categories of vulnerabilities**

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.



Hackers and crackers

Hackers:

- Person with strong interest in computers and enjoys learning and experimenting
- Very talented and smart people

Crackers:

- Person who breaks into computer
- Crimes include vandalisms, theft and snooping in unauthorized areas

Categories of cybercrime

Cybercrime can be categorized based on

- The target of the crime
- Whether the crime occurs as a single event or as a series of events

1. Crimes targeted at individuals
2. Crimes targeted at property
3. Crimes targeted at organizations
4. Single event of cybercrime
5. Series of events

1. Crimes targeted at individuals

- Human weakness
- Financial frauds
- Child pornography
- Copy right violations
- Harassment

2. Crimes targeted at property

- Stealing devices
- Transmitting harmful programs to destroy the devices

3. Crimes targeted at organizations

- Cyberterrorism
- Attackers (individual / group)
- Usage of computer tools and usage

4. Single event of cybercrime

- It is the single event from the perspective of victim
- Unknowingly opening attachments contain virus
- This is hacking or fraud

5. Series of events

- Attacker interacting with the victims repetitively
- Series of events / demanding
- Cyberstalking

How criminals plan the attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target
- Target can be individual or / and organizations
- Active attack and passive attack
- Inside attack and outside attack

Inside attack: originating or attempted within the security perimeter of an organization.

- **Attempted by insider**
- **Gains access to more resources than expected**

Outside attack: attempted outside the security perimeter of an organization.

- Attempted through internet or remote access connection.

Phases involved in planning cybercrime

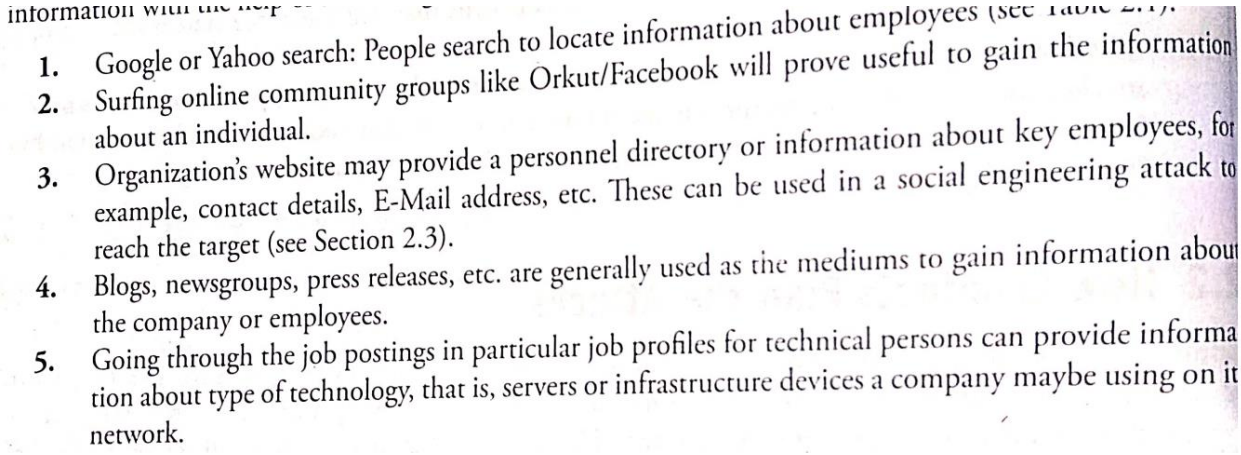
1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

- Is an act of reconnoitering – explore, often with the goal of finding something or somebody.
- Gain information about an enemy or potential enemy.
- Foot printing- gives an overview about the system vulnerability
- Attackers gather the information in two phases
- Passive and active attacks

Passive attacks

- Gathering information about a target without his/her knowledge
- Internet searches or by googling.



information with the help

1. Google or Yahoo search: People search to locate information about employees (see Table 2.1).
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on it network.

Tools used during passive attack

Name of the Tool	*Brief Description*	*Remarks*
Google Earth	Google Earth is a virtual globe, map, and geographic information program. It maps the Earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe. It is available under three different licenses: Google Earth, a free version with limited functionality; Google Earth Plus (discontinued), with additional features; and Google Earth Pro intended for commercial use.	For more details on this tool, visit: http://earth.google.com/ Like "Google Earth," similar details can be obtained from http://www.wikimapia.org/ Indian Space Research Organization (ISRO) unveiled its beta version of Bhuvan (meaning Earth in Sanskrit), a Web-based tool like Google Earth, that promises better 3-D satellite imagery of India than is currently being offered by Google Earth and that too with India-specific features such as weather information and even administrative boundaries of all states and districts, visit: http://bhuvan.nrsc.gov.in/
Internet Archive	The Internet Archive is an Internet library, with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format. It includes texts, audio, moving images, and software as well as archived webpages in our collections.	An attacker gets the information about latest update made to the target's website as well as can dig the information which maybe available in the history (e.g., contact list of executives and higher management officials are always updated). For more details on this tool, visit: http://www.archive.org/index.php
Professional Community	LinkedIn is an interconnected network of experienced professionals from around the world, representing 170 industries and 200 countries.	One can find details about qualified professionals. For more details on this tool, visit: http://www.linkedin.com/
People Search	People Search provides details about personal information: date of birth, residential address, contact number, etc.	To name a few, visit: • http://www.whitepagesinc.com • http://www.intelius.com/ • http://www.whitepages.com/
Domain Name Confirmation	To perform searches for domain names (e.g., website names) using multiple keywords. This helps to enable to find every registered domain name in "com," "net," "org," "edu," "biz," etc.	For more details on this tool, visit: • http://www.namedroppers.com/ • http://www.binarypool.com/bytes.html

Name of the Tool	Brief Description	Remarks
WHOIS	This is a domain registration lookup tool. This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information. WHOIS supports IP address queries and automatically selects the appropriate WHOIS server for IP addresses. This tool will lookup information on a domain, IP address, or a domain registration information. You can select a specific WHOIS server, or you can use the "Default" option which will select a server for you.	For more details on this tool, visit: • http://whois.domaintools.com/ • http://www.whois.net/ • http://www.samspade.org/ For further details of this lookup utility, visit: • http://resellers.tucows.com/opensrs/whois/ • http://www.nsauditor.com/docs/html/tools/Whois.htm
Nslookup	The name nslookup means "name server lookup." The tool is used on Windows and Unix to query domain name system (DNS) servers to find DNS details, including IP addresses of a particular computer and other technical details such as mail exchanger (MX) records for a domain and name server (NS) servers of a domain.	For more details on this tool, visit: • http://www.kloth.net/services/nslookup.php • http://nslookup.downloadsoftware4free.com/
Dnsstuff	Using this tool, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups, etc.	For more details on this tool, visit: http://www.dnsstuff.com/
Traceroute	This is the best tool to find the route (i.e., computer network path) to a target system. It determines the route taken by packets across an IP network.	For more details on this tool, visit: http://www.rjsmith.com/tracerte.html
VisualRoute Trace	This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.	For more details on this tool, visit: http://www.visualware.com/
eMailTrackerPro	eMailTrackerPro analyzes the E-Mail header and provides the IP address of the system that sent the mail.	For more details on this tool, visit: http://www.emailtrackerpro.com/
HTTrack	This tool acts like an offline browser. It can mirror the entire website to a desktop. One can analyze the entire website by being offline.	For more details on this tool, visit: http://www.httrack.com/
Website Watcher	The tool can be used to keep the track of favorite websites for an update. When the website undergoes an update/change, this tool automatically detects it and saves the last two versions onto the desktop.	For more details on this tool, visit: http://www.aignes.com/
Competitive Intelligence	Competitive intelligence can provide information related to almost any product, information on recent industry trends, or information about geopolitical indications. Effective use of competitive intelligence can reveal attack against the website or an industrial espionage.	To name a few, visit: • http://bigital.com/ • http://www.amity.edu/aici/

Active attacks

- **It involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase**
- **Risk of detection and is also called rattling the doorknobs or active reconnaissance**
- **The attacker efforts to change or modify the content of messages.**
- **Active Attack is danger for Integrity as well as availability.**
- **Due to active attack system is always damaged and System resources can be changed.**
- **The most important thing is that, In active attack, Victim gets informed about the attack.**

Tools used during active attack

Table 2.2 | Tools used during active attacks

Name of the Tool	*Brief Description*	*Remarks*
Arphound	This is a tool that listens to all traffic on an Ethernet network interface. It reports IP/media access control (MAC) address pairs as well as events, such as IP conflicts, IP changes and IP addresses with no reverse DNS, various Address Resolution Protocol (ARP) Spoofing and packets not using the expected gateway.	This is open-source software. For more details on this tool and download, visit: http://www.nottale.net/index.php?project=arphound
Arping	This is a network tool that broadcasts ARP packets and receives replies similar to "ping." It is good for mapping a local network and finding used IP space. It broadcasts a "who-has ARP packet" on the network and prints answers. It is very useful when trying to pick an unused IP for a Net to which routing does not exist as yet.	This is open-source software. For more details on this tool and download,visit: http://www.habets.pp.se/synscan/programs.php?prog=arping
Bing	This is used for Bandwidth Ping. It is a point-to-point bandwidth measurement tool based on ping. It can measure raw throughput between any two network links. Bing determines the real (raw as opposed to available or average) throughput on a link by measuring Internet Control Message Protocol (ICMP) echo requests roundtrip times for different packet sizes for each end of the link.	This is open-source software. For installation and usage information, visit: http://ai3.asti.dost.gov.ph/sat/bing.html
Bugtraq	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources.	This software is for free usage. Visit the following site for more details: http://www.securityfocus.com/bid
Dig	This is used to perform detailed queries about DNS records and zones, extracting configuration, and administrative information about a network or domain.	This is open-source software. For additional technical details, visit: http://www.isc.org/index.pl?/sw/bind/
DNStracer	This is a tool to determine the data source for a given DNS server and follow the chain of DNS servers back to the authoritative sources.	This is also open-source software. For additional technical details, visit: http://www.mavetju.org/unix/dnstracer.php

Table 2.2 | (Continued)

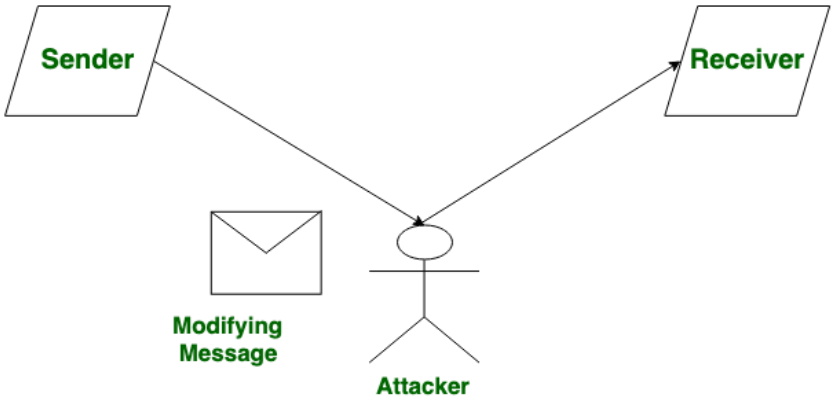
Name of the Tool	*Brief Description*	*Remarks*
Dsniff	This is a network auditing tool to capture username, password, and authentication information on a local subnet.	This is open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
Filesnarf	This is a network auditing tool to capture file transfers and file sharing traffic on a local subnet.	This is also open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
FindSMB	This is used to find and describe server message block (SMB) servers on the local network.	It is open-source software; visit the following site for downloads: http://us3.samba.org/samba/
Fping	This is a utility similar to ping used to perform parallel network discovery.	For this open-source software, visit: http://www.fping.com/
Fragroute	This intercepts, modifies and rewrites egress traffic destined for a specified host, implementing several intrusion detection system (IDS) evasion techniques.	This is another open-source material; visit: http://www.monkey.org/~dugsong/fragroute/
Fragtest	This tests the IP fragment reassembly behavior of the Transmission Control Protocol (TCP) stack on a target. It intercepts, modifies and rewrites egress traffic destined for a specified host, implementing most of the attacks.	For more details on this open-source software, visit: http://www.monkey.org/~dugsong/fragroute/
Hackbot	This is a host exploration tool, simple vulnerability scanner and banner logger.	Another open-source software, whose details can be found at: http://freshmeat.net/projects/hackbot/
Hmap	This is used to obtain detailed fingerprinting of web servers to identify vendor, version, patch level, including modules and much more. *Hmap* is a web server fingerprinting tool.	Details of this open-source software can be found at: http://ujeni.murkyroc.com/hmap/
Hping	This is a TCP/IP packet assembler and analyzer. It can perform firewall ruleset testing, port scanning, network type of service/quality-of-service (TOS/QOS) testing, maximum transmission unit (MTU) discovery, alternate-protocol traceroute, TCP stack auditing, and much more. Using *hping* you can do the following: • Firewall testing; • advanced port scanning; • network testing, using different protocols, TOS, fragmentation; • manual path MTU discovery; • advanced traceroute, under all the supported protocols; • remote OS fingerprinting; • remote uptime guessing; • TCP/IP stacks auditing;	This is open-source software. For additional technical details, visit: http://www.hping.org/

Table 2.2 | (Continued)

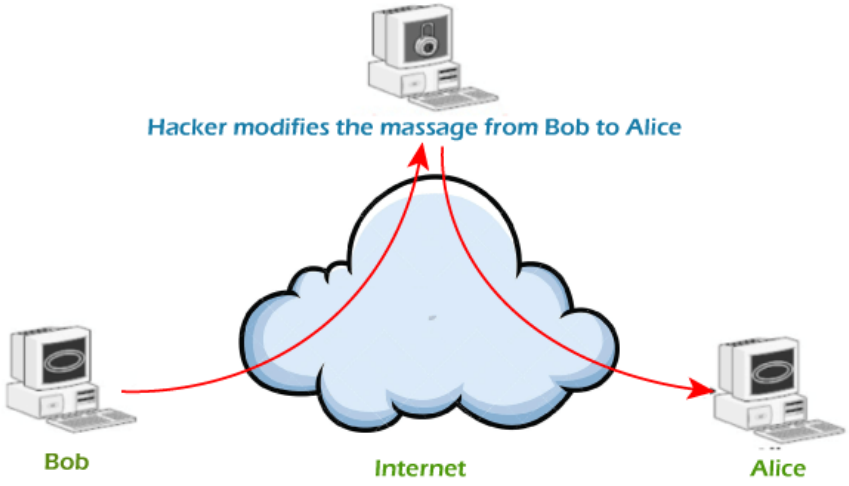
Name of the Tool	Brief Description	Remarks
	Hping works on the following Unix-like systems: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.	
Httping	This is similar to "ping," that is, hping, but for HTTP requests. It shows how long a URL will take to connect, send a request, and receive a reply.	This is open-source software. For additional technical details, visit: http://www.vanheusden.com/httping/
Hunt	This is a tool for exploiting well-known weaknesses in the TCP/IP protocol suite.	This is also open-source software. For additional technical details, visit: http://lin.fsid.cvut.cz/~kra/index.html
Libwhisker	This is an application library designed to assist in scannabilities.	Details of this open-source software can be found at: http://www.wiretrip.net/rfp/lw.asp
Mailsnarf	This is a network auditing tool to capture SMTing for CGI/web vulnerP and POP3 E-Mail traffic (including message headers, bodies, and attachments) on a local subnet.	For this open-source software, you can visit: http://monkey.org/~dugsong/dsniff/
Msgsnarf	This is a network auditing tool to capture instant message (Yahoo, MSN, ICQ, iChat, AIM, and many more) traffic on a local subnet.	Same as above
NBTScan	This is a utility for scanning networks for NetBIOS information. It reports IP address, NetBIOS name, logged-in username, and MAC address.	Details of this open-source material can be found at: http://www.inetcat.org/software/nbtscan.html
Nessus	This is a powerful, fast, and modular security scanner that tests for many thousands of vulnerabilities. ControlScans' system can also be used to create custom Nessus reports.	To know more about this open-source utility, visit: http://www.nessus.org/
Netcat	This is a utility to read and write custom TCP/User Datagram Protocol (UDP) data packets across a network connection for network debugging or exploration.	Explore more details of this open-source utility at: http://www.atstake.com/research/tools/network_utilities/
Nikto	This is a web server vulnerability scanner that tests over 2,600 potentially dangerous files/CGIs on over 625 types of servers. This tool also performs comprehensive tests against web servers for multiple items and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).	Nikto is an open-source web server scanner; visit the following site for more detail: http://www.cirt.net/code/nikto.shtml
Nmap	This is a port scanner, operating system fingerprinter, service/version identifier, and much more. Nmap is designed to rapidly scan large networks.	For details of this open-source software, visit: http://insecure.org/nmap/

Difference between Active Attack and Passive Attack

Active Attacks: Active attacks are the type of attacks in which, The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack.



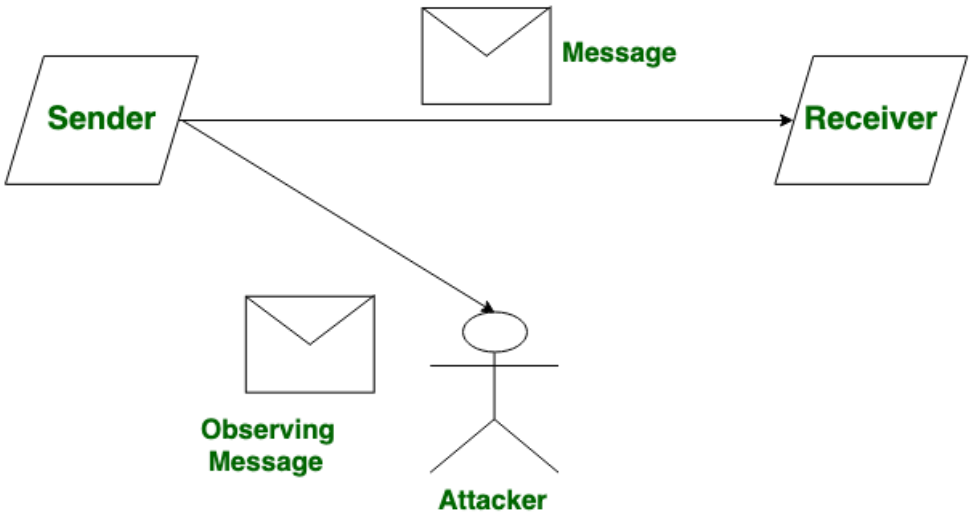
Active Attack



Active Attacks (Modifications of messages)

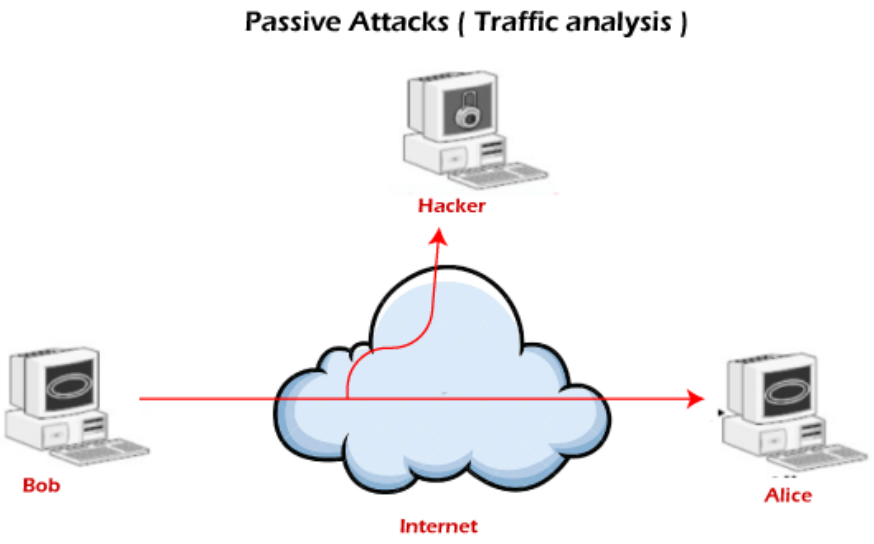
In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for integrity and availability of the message. Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. The system resources can be changed due to active attacks. So, the damage done with active attacks can be harmful to the system and its resources

Passive Attacks: Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is a danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.



Passive Attack

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.



Unlike active attacks, in passive attacks, victims do not get informed about the attack. It is difficult to detect as there is no alteration in the message. Passive attacks can be prevented by using some encryption techniques. We can try the below-listed measures to prevent these attacks

Based on	Active attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to **modify the message's content.**	In passive attacks, the attacker **observes the messages, then copy and save** them and can use it for malicious purposes.
Modification	In an active attack, the attacker **modifies the actual information.**	In passive attacks, **information remains unchanged**.
Victim	In active attacks, the **victim gets notified** about the attack.	Unlike active attacks, in passive attacks, **victims do not get informed** about the attack.
System's impact	The damage done with active attacks can be **harmful to the system and its resources**.	The passive attacks **do not harm the system**.
System resources	In active attacks, the **system resources can be changed.**	In passive attacks, the **system resources remain unchanged.**
Dangerous for	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
Emphasis on	In active attacks, **attention is on detection.**	In active attacks, **attention is on prevention**.
Types	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.
Prevention	Active attacks are **tough to restrict from entering systems or networks**.	Unlike active attacks, **passive attacks are easy to prohibit.**