CYBER OFFENSES: HOW CRIMINALS PLAN THEM:

INTRODUCTION
HOW CRIMINALS PLAN THE ATTACKS
SOCIAL ENGINEERING
CYBER STALKING
CYBER CAFE AND CYBERCRIMES
BOTNETS: THE FUEL FOR CYBERCRIME
ATTACK VECTOR
CLOUD COMPUTING

UNIT-2

INTRODUCTION

- Technology is a "double-edged sword" as it can be used for both good and bad purposes.
- Computers and tools available in IT are also no exceptions; like other cool, they are used as either target of offense or means for committing an offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders with "false sense of anonymity"; without realizing, we seem to pass on tremendous amount of information about ourselves.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyberlaws among the people who are constantly using the IT infrastructure for official and personal purposes.

INTRODUCTION (CONT..)

INTRODUCTION (CONT...)

- **Hacker:** A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers.
- **Brute force hacking**: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.
- **Cracker**: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.

INTRODUCTION (CONT...)

- **Cracking:** It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called “phreaking”). These sites usually display warnings such as “These files are illegal; we are not responsible for what you do with them.”

- **Cracker tools:** These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.

INTRODUCTION (CONT...)

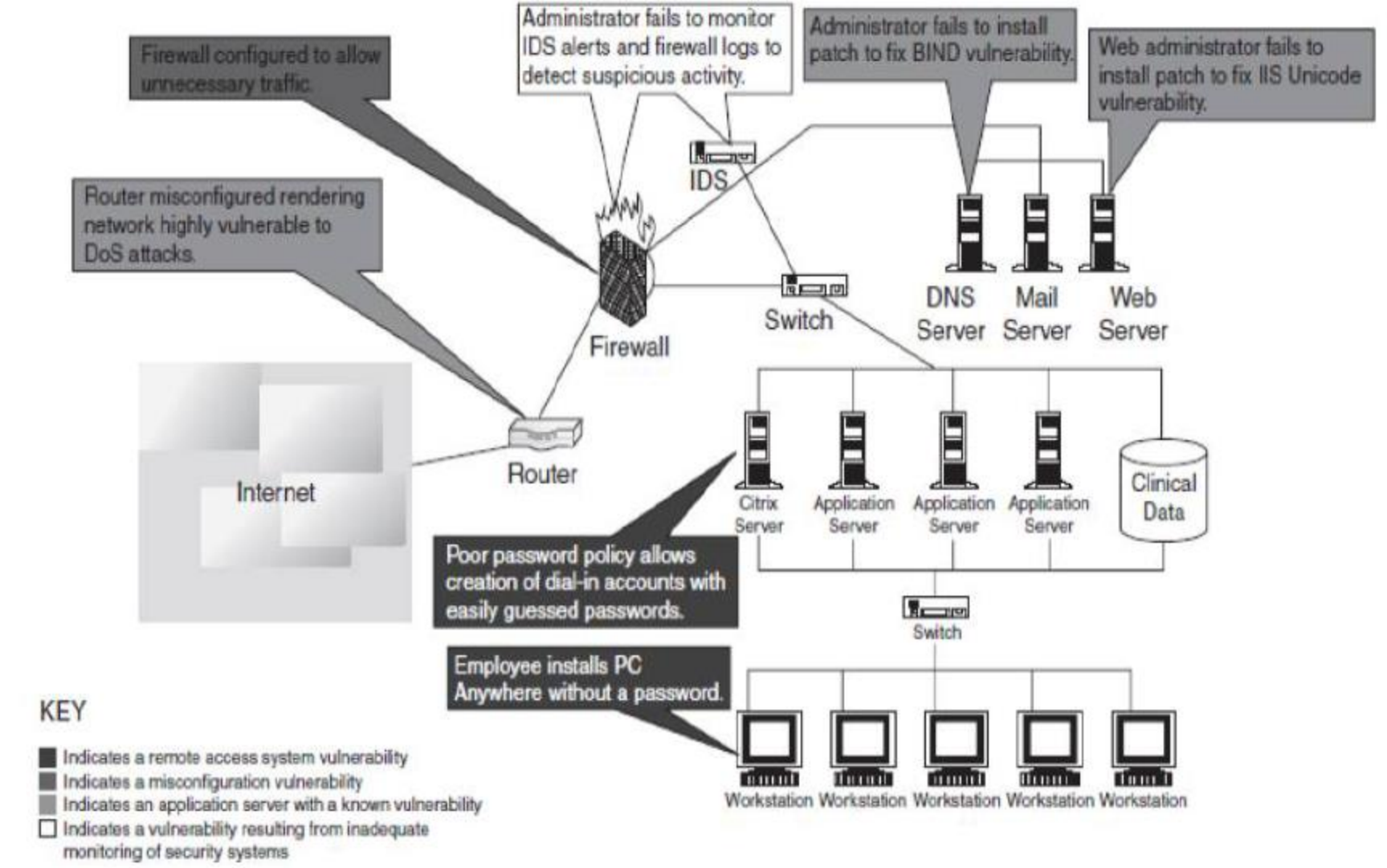
- **Phreaking:** This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

- **War dialer:** Program automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in. An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.

INTRODUCTION (CONT…)

- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection (border as in the sense of network periphery);
  - remote access servers (RASs) with weak access controls;
  - application servers with well-known exploits;
  - misconfigured systems and systems with default configurations.

INTRODUCTION (CONT...)



INTRODUCTION (CONT...)

- A **black hat hacker** is also called a “cracker” or “dark side hacker.” Such a person is a malicious or **criminal hacker**. Typically, the term “cracker” is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of “hacker” can be much broader. The name comes from the opposite of “white hat hackers.”

- A **white hat hacker** is considered an ethical hacker. In the realm of IT, a “white hat hacker” is a person who is ethically opposed to the abuse of computer systems. As a simplified explanation, a “white hat” generally focuses on securing IT systems, whereas a “black hat” (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

INTRODUCTION (CONT...)

- A **brown hat hacker** is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

CATEGORIES OF CYBERCRIME

- Cybercrime can be categorized based on the following:
  - The target of the crime and
  - Whether the crime occurs as a single event or as a series of events.

- Cybercrime can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).
- **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography, copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.

CATEGORIES OF CYBERCRIME

- **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.

- **Crimes targeted at organizations**: Cyber terrorism is one of the distinct crimes against organizations/ governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the rograms and fi les or plant programs to get control of the network and/or system

CATEGORIES OF CYBERCRIME

- **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.

- **Series of events:** This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

CATEGORIES OF CYBERCRIME

- **Patriot hacking** also known as Digital Warfare, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat. Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

HOW CRIMINALS PLAN THE ATTACKS

- Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- **Active attacks** are usually used to alter the system (i.e., computer network) whereas **passive attacks** attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to violation of confidentiality.
- Attacks can be categorized as either inside or outside.
- An attack originating and/or attempted within the security perimeter of an organization is an **inside attack**; it is usually attempted by an "insider" who gains access to more resources than expected. An **outside attack** is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

HOW CRIMINALS PLAN THE ATTACKS

- The following phases are 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).

HOW CRIMINALS PLAN THE ATTACKS

Phase-1: Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

- The literal meaning of "Reconnaissance" is an **act of finding something or somebody (especially to gain information about an enemy or potential enemy**).
- In the world of "hacking," reconnaissance phase begins with "Footprinting" – this is the preparation toward pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack. Thus, an attacker attempts to gather information in two phases: passive and active attacks.

HOW CRIMINALS PLAN THE ATTACKS

Passive Attacks:

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises.
- However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information
  - Google or Yahoo search: People search to locate information about employees.
  - Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
  - 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
  - Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
  - 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 its network.

HOW CRIMINALS PLAN THE ATTACKS

Tips for Effective Search with “Google" Search Engine:

- The Google search engine con be used indigenously to perform "Reconnoissonce" phase of an attack. The following commands can be used effectively in the Google search engine.
- http://groups.google.com : This site can be used to search the Google newsgroups.

HOW CRIMINALS PLAN THE ATTACKS

Search Technique/Keyword	Description
Site	Google will restrict the results to those websites in the given domain. Ex. site:www.google.com
Filetype	This will search within the text of o particular type of file. Ex. filetype:rtf galway
Link	will list the webpages that have links to the specified webpage. Ex. link: www.google.com
inurl	Google will restrict the results to documents containing that word in the URL. Ex. inurl:google search
Cache	Google will highlight those words within the cached document. ex. cache: www.google.com web
Related	The query will list webpages that are "similar" to a specified webpage. Ex. related:www.google.com

HOW CRIMINALS PLAN THE ATTACKS

Search Technique/Keyword	Description
Info	will present some information that Google has about that webpage. Ex. info: www.google.com
Define	will provide a definition of the word/phrase you enter after it, gathered from various online sources. Ex. define:cybersecurity
Stocks	Google will treat the rest of the query terms as stock ticker symbols and will link to a page showing stock information for those symbols. Ex. stocks: intc yhoo
Allintltle	Google will restrict the results to those with all of the query words in the title. Ex. allintille: google search
Intltle	Google will restrict the results to documents containing that word in the title. Ex. . intille:google search
Allinurl	Google will restrict the results to those with all of the query words in the URL. Ex. allinurl: google search

HOW CRIMINALS PLAN THE ATTACKS

- Network sniffing is another means of passive attack to yield useful information such as Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network.
- Along with Google search, various other tools are also used for gathering information about the target/victim.

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

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
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/

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

Active Attacks:

- An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called “Rattling the doorknobs” or “Active reconnaissance.” Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

HOW CRIMINALS PLAN THE 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

HOW CRIMINALS PLAN THE ATTACKS

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

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

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; • hping can also be useful to students that are learning TCP/IP.	This is open-source software. For additional technical details, visit: http://www.hping.org/

HOW CRIMINALS PLAN THE ATTACKS

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/

HOW CRIMINALS PLAN THE ATTACKS

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

HOW CRIMINALS PLAN THE ATTACKS

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/
Pathchar	This is a network tool for inferring the characteristics of Internet paths, including Layer 3 hops, bandwidth capacity, and autonomous system information.	For further details, visit: http://ee.lbl.gov/
Ping	This is a standard network utility to send ICMP packets to a target host.	For further details, visit: http://www.controlscan.com/auditingtools.html#
ScanSSH	This supports scanning a list of addresses and networks for open proxies, SSH Protocol servers, and Web and SMTP servers. Where possible, it displays the version number of the running services. ScanSSH supports the following features: • Variable scanning speed: per default, ScanSSH sends out 100 probes per second; • open proxy detection; • random sampling: it is possible to randomly sample hosts on the Internet.	The first version of the ScanSSH Protocol scanner was released in September 2000. For further details and downloading the current version, visit: http://www.monkey.org/~provos/scanssh/

HOW CRIMINALS PLAN THE ATTACKS

SMBclient	This helps a client to talk to an SMB (Samba, Windows File Sharing) server. Operations include getting files from the server, putting files on the server, retrieving directory information, and much more. It is an open-source/free software suite that has, since 1992, provided file and print services to all types of SMB/common Internet file system (CIFS) clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License.	
SMTPscan	This is a tool to determine the type and version of a remote Simple Mail Transfer Protocol (SMTP) mail server based on active probing and analyzing error codes of the target SMTP server.	For further details, visit: http://www.greyhats.org/outils/smtpscan/
TCPdump	It is a network tool for the protocol packet capture and dumper program.	For further details, visit: http://ee.lbl.gov/

HOW CRIMINALS PLAN THE ATTACKS

TCPreplay

This is a utility to read captured TCPdump/pcap data and "replay" it back onto the network at arbitrary speeds.

TCPreplay is a suite of licensed tools written by Aaron Turner for Unix operating systems. It gives you the ability to use previously captured traffic to test a variety of network devices. It allows you to classify traffic as client or server; rewrite open system interconnection (OSI) Layers 2, 3 and 4 headers; and finally replay the traffic back onto the network and through other devices such as switches, routers, firewalls, network-based intrusion detection system (NIDS), and intrusion prevention system (IPS).

TCPreplay supports both single and dual NIC modes for testing both sniffing and inline devices.

TCPreplay is used by numerous firewalls, IDS, IPS, and other networking vendors, enterprises, universities, laboratories, and open-source projects.

TCPreplay suite includes the following tools:

- TCPprep: It is a multi-pass packet capture (pcap) file preprocessor which determines packets as client or server and creates cache files used by TCPreplay and TCPrewrite.
- TCPrewrite: It is a pcap file editor which rewrites TCP/IP and Layer 2 packet headers.
- TCPreplay: It replays pcap files at arbitrary speeds onto the network.
- TCPreplay-edit: It replays and edits pcap files at arbitrary speeds onto the network.
- TCPbridge: It bridges two network segments with the power of TCPrewrite.

For further details, visit:
http://tcpreplay.synfin.net/trac/

HOW CRIMINALS PLAN THE ATTACKS

THC-Amap	This is a scanner to remotely fingerprint and identify network applications and services.	For further details, visit: http://freeworld.thc.org/releases.php
Traceroute	This is a standard network utility to trace the logical path to a target host by sending ICMP or UDP packets with incrementing tunneled transport layer security (TTLs).	For further details, visit: http://ee.lbl.gov/
URLsnarf	This is a network auditing tool to capture HTTP traffic on a local subnet.	For further details, visit: http://monkey.org/~dugsong/dsniff/
XProbe2	This is a tool employing several techniques to actively fingerprint the operating system of a target host.	For further details, visit: http://www.sys-security.com/html/projects/X.html

HOW CRIMINALS PLAN THE ATTACKS

Phase-2: Scanning and Scrutinizing Gathered Information

- Scanning is a key step to examine intelligently while gathering information about the target.
- The objectives of scanning are as follows:
  1. Port scanning: Identify open/close ports and services.
  2. Network scanning: Understand IP Addresses and related information about the computer network systems.
  3. Vulnerability scanning: Understand the existing weaknesses in the system.

HOW CRIMINALS PLAN THE ATTACKS

- **Ports and Ports Scanning**
- A port is an interface on a computer to which one can connect to device. TCP/IP Protocol suite made out of the two protocols, TCP and UDP, is used universally to communicate on the Internet. The port numbers ore divided into three ranges:
  - Well-known ports (from 0 to 1023)
  - Registered ports (from 1024 to 49151)
  - Dynamic and/or private ports (from 49152 to 65535)

HOW CRIMINALS PLAN THE ATTACKS

Port Number	*Port Description*	*Port Number*	*Port Description*
1	TCP port service multiplexer (TCPMUX)	118	Structured query language (SQL) services
5	Remote job entry (RJE)	119	NNTP (Newsgroup)
7	ECHO	137	NetBIOS name service
18	Message Send Protocol (MSP)	139	NetBIOS datagram service
20	FTP – Data	143	Internet Message Access Protocol (IMAP)
21	FTP – Control	150	NetBIOS session service
22	Secure shell (SSH) remote log-in protocol	156	SQL server
23	Telnet	161	Simple Network Management Protocol (SNMP)
25	Simple Mail Transfer Protocol (SMTP)	179	Border Gateway Protocol (BGP)
29	MSG ICP	190	Gateway Access Control Protocol (GACP)

HOW CRIMINALS PLAN THE ATTACKS

37	Time	194	Internet relay chat (IRC)
42	Nameserv (host name server)	197	Directory location service (DLS)
43	WHOIS	389	Lightweight Directory Access Protocol (LDAP)
49	Log-in (log-in host protocol)	396	Novell netware over IP
53	Domain name system (DNS)	443	Secure Hypertext Transfer Protocol (S-HTTP)
69	Trivial File Transfer Protocol (TFTP)	444	Simple Network Paging Protocol (SNPP)
70	Gopher services	445	Microsoft-DS
79	Finger	458	Apple quick time
80	HTTP	546	DHCP client
103	X.400 Standard	547	DHCP server
108	SNA gateway access server	563	SNEWS
109	POP2	569	MSN
110	POP3	1080	Socks
115	Simple File Transfer Protocol (SFTP)		

HOW CRIMINALS PLAN THE ATTACKS

- **Port Scanning**
- A "port" is a place where information goes into and out of a computer and so, with port scanning, one can identify open doors to a computer. Ports are basically entry/exit points that any computer has, to be able to communicate with external machines.
- Each computer is enabled with three or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner, and other peripherals.
- Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap offer an automated mechanism for an attacker to not only scan the system to find out what ports are "open" (meaning being used), but also help to identify what operating system (OS) is being used by the system.

HOW CRIMINALS PLAN THE ATTACKS

- The result of a scan on a port is usually generalized into one of the following three categories:

  1. **Open or accepted:** The host sent a reply Indicating that a service is listening on the port.

  2. **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.

  3. **Filtered or blocked:** There was no reply from the host.

- Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.
- Open ports present two vulnerabilities of which administrators must be wary:
  - Vulnerabilities associated with the program that is delivering the service.
  - Vulnerabilities associated with the OS that is running on the host.
- Closed ports present only the latter of the two vulnerabilities that open ports do.
- Blocked ports do not present any reasonable vulnerabilities.

HOW CRIMINALS PLAN THE ATTACKS

- **The scrutinizing phase** is always called "enumeration" in the hacking world. The objective behind this is to identify:

  1. The valid user accounts or groups;
  2. network resources and/or shared resources;
  3. OS and different applications that are running on the OS.

HOW CRIMINALS PLAN THE ATTACKS

Phase-3: Attack (Gaining and Maintaining the System Access)

- After the scanning and enumeration, the attack is launched using the following steps:
  1. Crack the password.
  2. exploit the privileges.
  3. execute the malicious commands/applications.
  4. hide the files (if required).
  5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

SOCIAL ENGINEERING

- Social engineering is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.
- The sign of truly successful social engineers is that they receive information without any suspicion.

SOCIAL ENGINEERING

Mr. Joshi: Hello?
The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.
Mr. Joshi: Ohh … okay. I will be at my home by then, anyway.
Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?
Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?
Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?
Mr. Joshi: My password is "ABCD1965," all characters in upper case.
Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.
Mr. Joshi: Thank you. Bye.
Caller: Bye and have a nice day.

CLASSIFICATION OF SOCIAL ENGINEERING

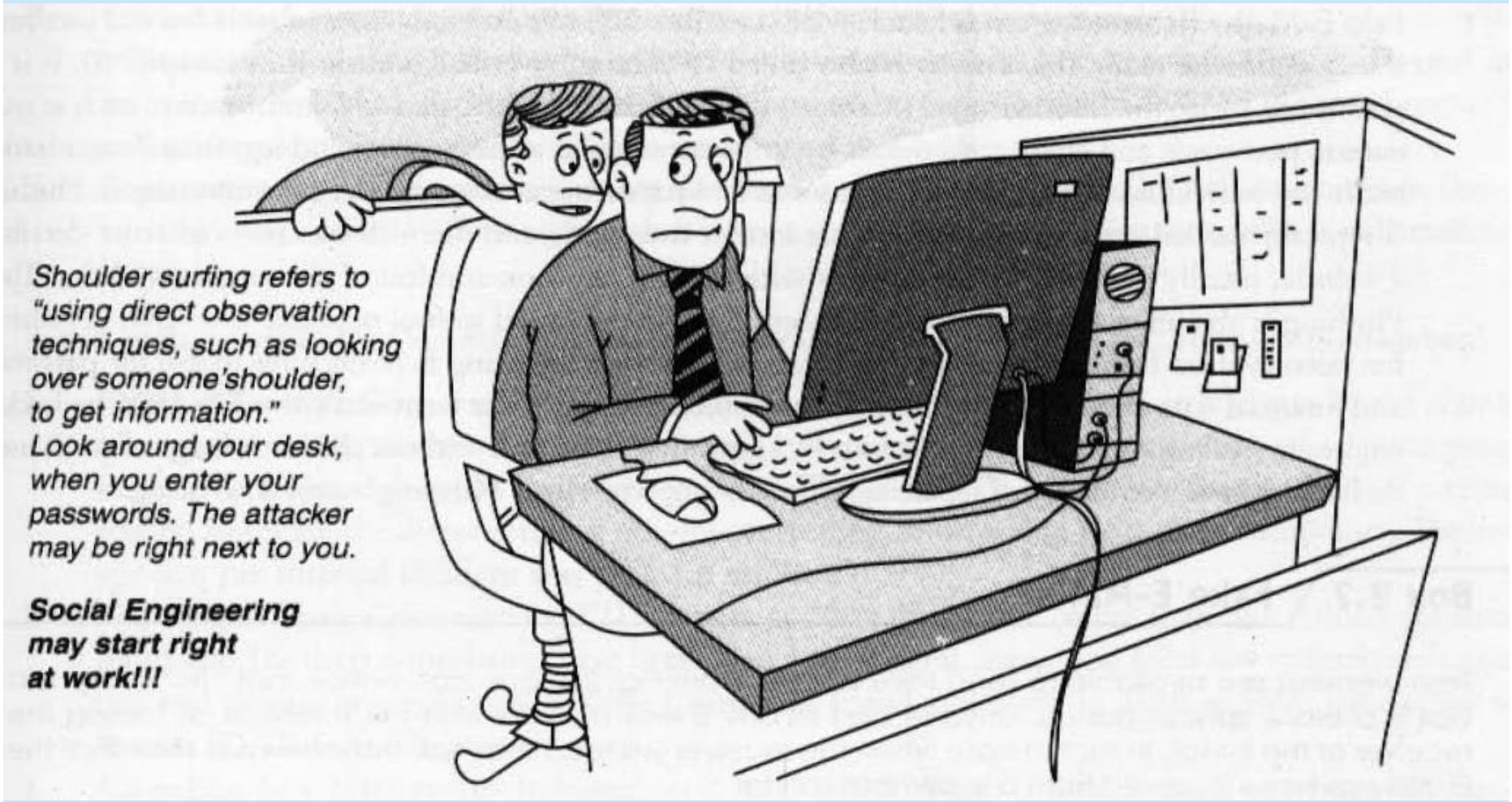
Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.
- **1. Impersonating an employee or valid user:** "Impersonation" is perhaps the greatest technique used by social engineers to deceive people. Ex: forgot ID and access to building.
- **2. Posing as an important user**: The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
- **3. Using a third person:** An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

CLASSIFICATION OF SOCIAL ENGINEERING

- **4. Calling technical support**: Calling the technical support for assistance is a classic social engineering example.
- **5. Shoulder surfing**: It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
- **6. Dumpster diving:** It involves looking in the trash for information written on pieces of paper or computer printouts. It is also called dumpstering, binning, trashing, garbing or garbage gleaning. "Scavenging" is another term to describe these habits. In the UK, the practice is referred to as " binning" or "skipping" and the person doing it is a "binner" or a "skipper."

CLASSIFICATION OF SOCIAL ENGINEERING



Shoulder Surfing

CLASSIFICATION OF SOCIAL ENGINEERING

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet. For example, sending a fake E-Mail to the user and asking him/her to re-enter a password in a webpage to confirm it.
- **1. Fake E-Mails**: The attacker sends fake E-Mails to users in such that the user finds it as a real e-mail. This activity is also called “Phishing”. It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as usernames, passwords and credit card details by impersonating as a trustworthy and legitimate organization or an individual.
- **2. E-Mail attachments**: E-Mail attachments are used to send malicious code to a victim’s system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.
- **3. Pop-up windows:** Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software

CYBER STALKING

- The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.”
- Cyber stalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person’s home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person’s property.

CYBER STALKING

Types of Stalkers

1. Online stalkers:

- They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.

2. Offline stalkers:

- The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet. The victim is not aware that the Internet has been used to perpetuate an attack against them.

CYBER STALKING

How Stalking Works?

It is seen that stalking works in the following ways:

- 1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
- 2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
- 3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
- 4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

CYBER STALKING

- 5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
- 6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone no's), asking for sexual services or relationships.
- 7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

CYBER STALKING

Cyber Bullying

- The National Crime Prevention Council defines *Cyber bullying* as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."
- www.StopCyberbullying.org. on expert organization dedicated to Internet safety, security, and privacy defines cyber bullying as "a situation when a child, tween or teen is repeatedly 'tormented, threatened. harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween or teen using text messaging, E-Mail, instant messaging or any other type of digital technology."
- The practice of cyber bullying is not limited to children and while the behavior is identified by the some definition in adults. the distinction In age groups is referred to as cyber stalking or cyber harassment when perpetrated by adults toward adults.

CYBER CAFE AND CYBERCRIMES

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.
  - First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
  - Second, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

CYBER CAFE AND CYBERCRIMES

- Indian Information Technology Act (ITA) 2000, does not define cybercafes and interprets cybercafes as “network service providers” referred to under the Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:
- 1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
- 2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
- 3. Several cybercafes had installed the software called “Deep Freeze” for protecting the computers from prospective malware attacks. **Deep Freeze** can wipe out the details of all activities carried out on the computer when one clicks on the “restart” button. Such practices present challenges to the police or crime investigators when they visit the cybercafes.

CYBER CAFE AND CYBERCRIMES

- 4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down.
- 5. Pornographic websites and other similar websites with indecent contents are not blocked.
- 6. Cyber cafe owners have very less awareness about IT Security and IT Governance.
- 7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cyber cafe owners.
- 8. Cyber cafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cyber cafes – one of the cyber cafe owners whom we interviewed expressed a view that the police will not visit a cyber cafe unless criminal activity is registered by filing an First Information Report (FIR). Cyber cafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cyber cafes across India.

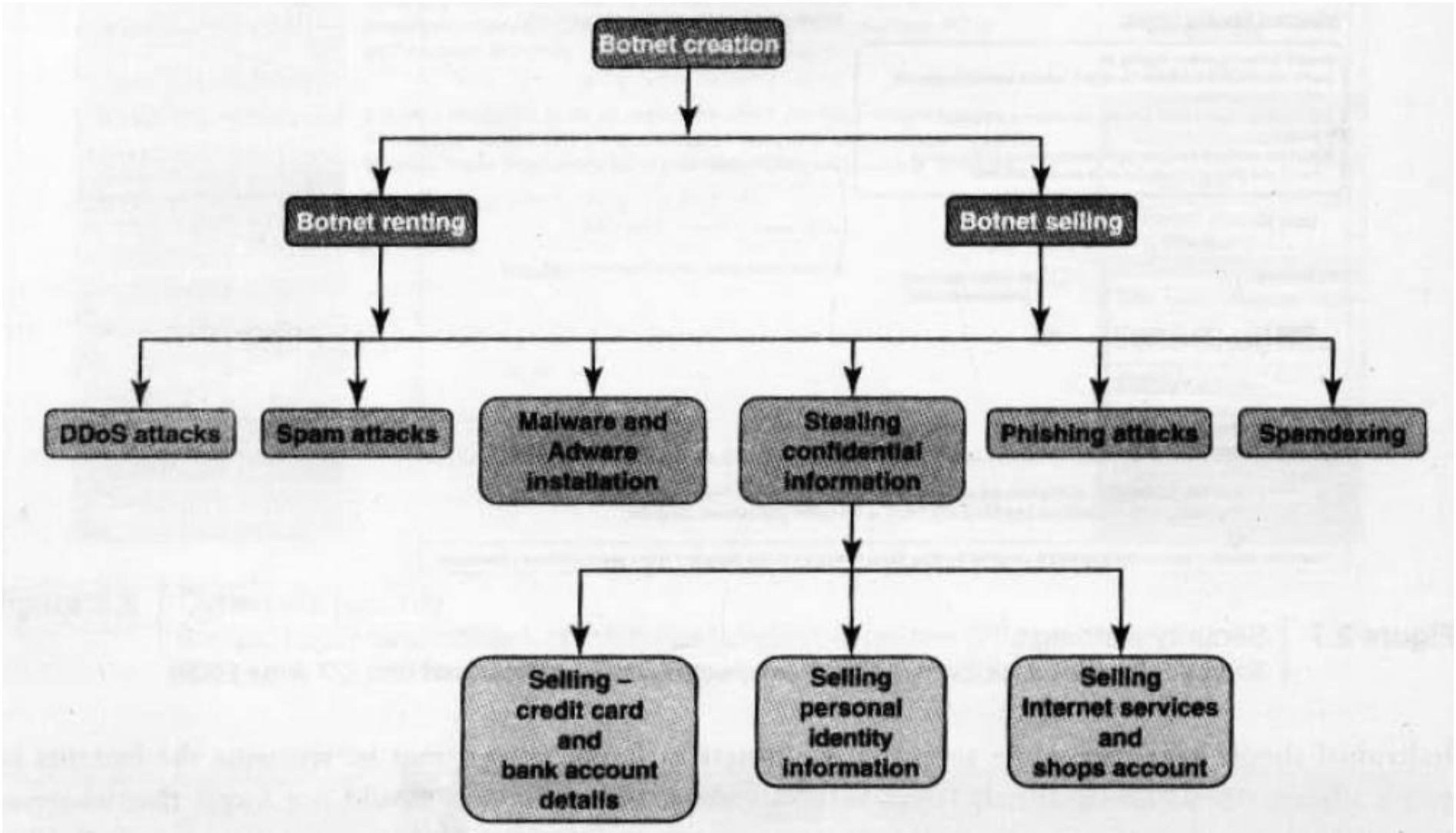
- Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout**
2. **Stay with the computer**
3. **Clear history and temporary files**
4. **Be alert**
5. **Avoid online financial transactions**
6. **Change passwords**
7. **Use Virtual keyboard**
8. **Security warnings**

BOTNETS: THE FUEL FOR CYBERCRIME

- The dictionary meaning of Bot is “(computing) an automated program for doing some particular task, often over a network.”
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically. The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users’ knowledge.
- “Zombie networks” have become a source of income for entire groups of cybercriminals. If someone wants to start a “business” and has no programming skills, there are plenty of “Bot for sale” offers on forums. ‘encryption of these programs’ code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet.

BOTNETS: THE FUEL FOR CYBERCRIME



BOTNETS: THE FUEL FOR CYBERCRIME

- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer:
5. Downloading the freeware only from websites that are known and trustworthy.
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
7. Take an immediate action if your system is infected.

ATTACK VECTOR

- An “attack vector” is a path, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors enable attackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.
- To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

ATTACK VECTOR

- In the technical terms, payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles.
- The attack vectors described here are how most of them are launched.
- **1. Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.

ATTACK VECTOR

- **2. Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
- **3. Attack by deception**: Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering are other forms of deception that are often an attack vector too.
- **4. Hackers**: Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use variety of hacking tools, heuristics, Cyberoffenses: How and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

ATTACK VECTOR

- **5. Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
- **6. Attack of the worms**: Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.
- **7. Malicious macros**: Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart(IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.

ATTACK VECTOR

- **8. Foistware (sneakware)**: Foistware is the software that adds hidden components to the system with cunning nature. Spyware is the most common form of foistware. Foistware is partial- legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some “revenue opportunity” that the foistware has set up.
- **9. Viruses**: These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

CLOUD COMPUTING

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.
- Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which make it easier for cybercriminals to attack these systems.
- Cloud computing is Internet (“cloud”)-based development and use of computer technology (“computing”).
- The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- Cloud computing is a term used for hosted services delivered over the Internet.

CLOUD COMPUTING

- A cloud service has three distinct characteristics which differentiate it from traditional hosting:
  1. It is sold on demand – typically by the minute or the hour;
  2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
  3. The service is fully managed by the provider – a user just needs PC and Internet connection.
- Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

CLOUD COMPUTING

Why Cloud Computing?

- The cloud computing has following advantages.

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every

employee and the organizations could pay a metered fee to a cloud computing company.

4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware. The cloud computing services can be either private or public.

CLOUD COMPUTING

Sr. No.	*Service Providers*	*Weblink*
1.	**Amazon:** It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	**3Tera:** It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	**Force.com:** It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	**Appistry-Cloud Computing Middleware:** It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	**Microsoft Live Mesh:** This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	https://www.mesh.com/Welcome/default.aspx
6.	**AppNexus:** This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.	http://www.appnexus.com/

CLOUD COMPUTING

Sr. No.	*Service Providers*	*Weblink*
7.	**Flexiscale:** It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	**GoogleApp Engine:** This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	**GoGrid:** It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	**Terremark Enterprise Cloud:** It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

CLOUD COMPUTING

Types of Services

- Services provided by cloud computing are as follows:

  1. Infrastructure-as-a-service (IaaS): It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.

  2. Platform-as-a-service (PaaS): It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. Google Apps is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.

  3. Software-as-a-service (SaaS): It is the broadest market. In this case, the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

CLOUD COMPUTING

Cybercrime and Cloud Computing

- Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years.
- Risks associated with cloud computing environment are as follows:

1. Elevated user access-Any data processed outside the organization brings with it an inherent level of risk

2. Regulatory compliance-Cloud computing service providers are not able and/or not willing to undergo external assessments.

3. Location of the data-User doesn't know where the data is stored or in which country it is hosted.

4. Segregation of data-Data of one organization is scattered in different locations

5. Recovery of the data-In case of any disaster, availability of the services and data is critical.

6. Information security- violation reports Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity

7. Long-term viability- In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.