2 Cyberoffenses: How Criminals Plan Them

Learning Objectives

After reading this chapter, you will be able to:

- Understand different types of cyberattacks.
- Get an overview of the steps involved in planning cybercrime.
- Understand tools used for gathering information about the target.
- Get an overview on social engineering – what and how.
- Learn about the role of cybercafes in cybercrime.
- Understand what cyberstalking is.
- Learn about Botnets and attack vector.
- Get an overview on cloud computing – what and how.

2.1 Introduction

Technology is a "double-edged sword" as it can be used for both good and bad purposes. People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose. Computers and tools available in IT are also no exceptions; like other tool, 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. Are we sure this will never be misused? Figure 2.1 gives us an idea about all those agencies that collect information about the individuals (i.e., Personally Identifiable Information such as date of birth, personal E-Mail address, bank account details and/or credit card details, etc. explained in Section 5.3.1, Chapter 5).

Chapter 1 provided an overview of *hacking*, *industrial espionage*, *network intrusions*, *password sniffing*, *computer viruses*, etc. They are the most commonly occurring crimes that target the computer. Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc. 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. People who commit cybercrimes are known as "Crackers" (Box 2.1).

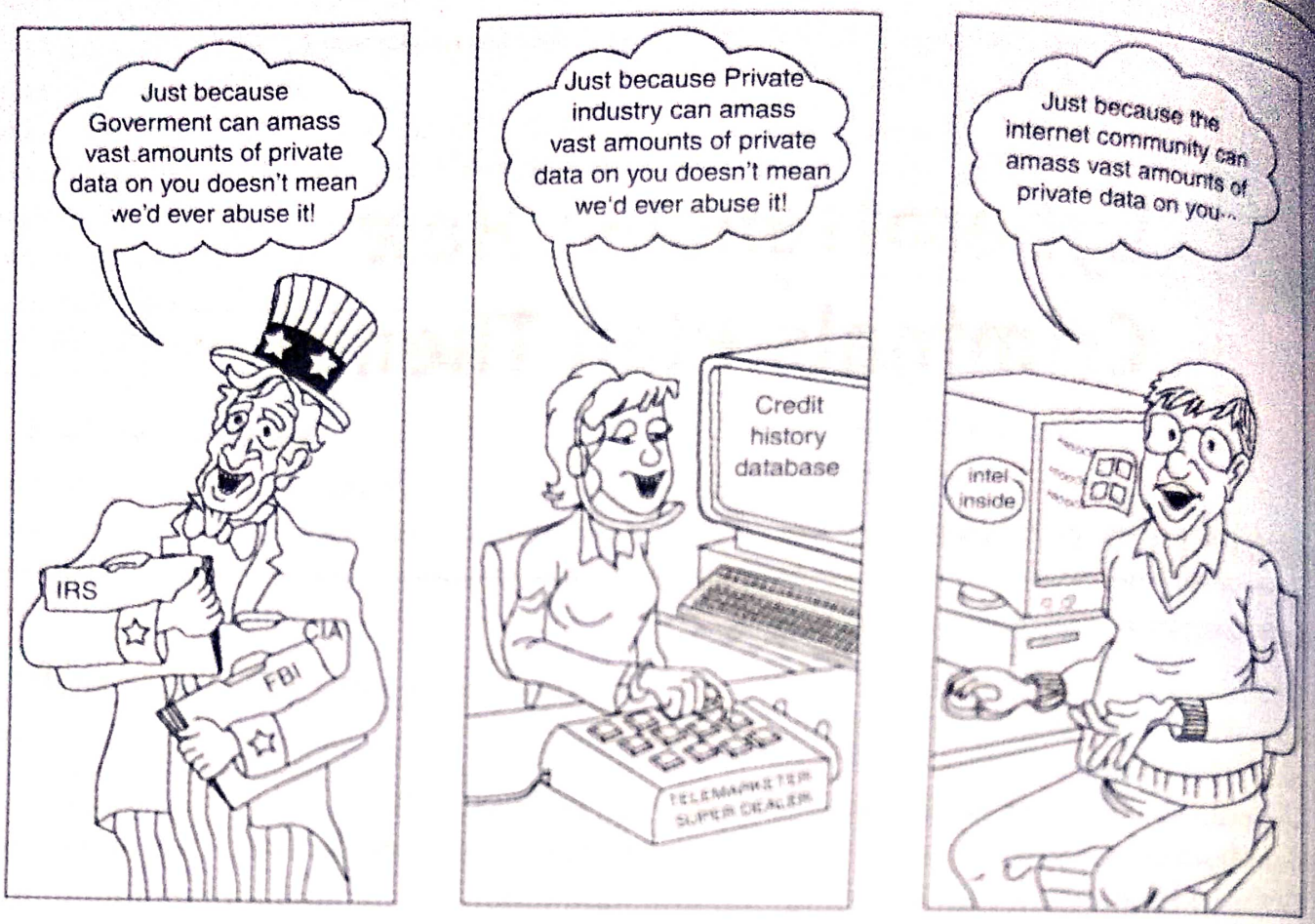

Figure 2.1 We all vouche for keeping your personal information secret!
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

Box 2.1 Hackers, Crackers and Phreakers

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 (refer to Box 2.2).

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.

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.

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: It is program that 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.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2), Wiley India.

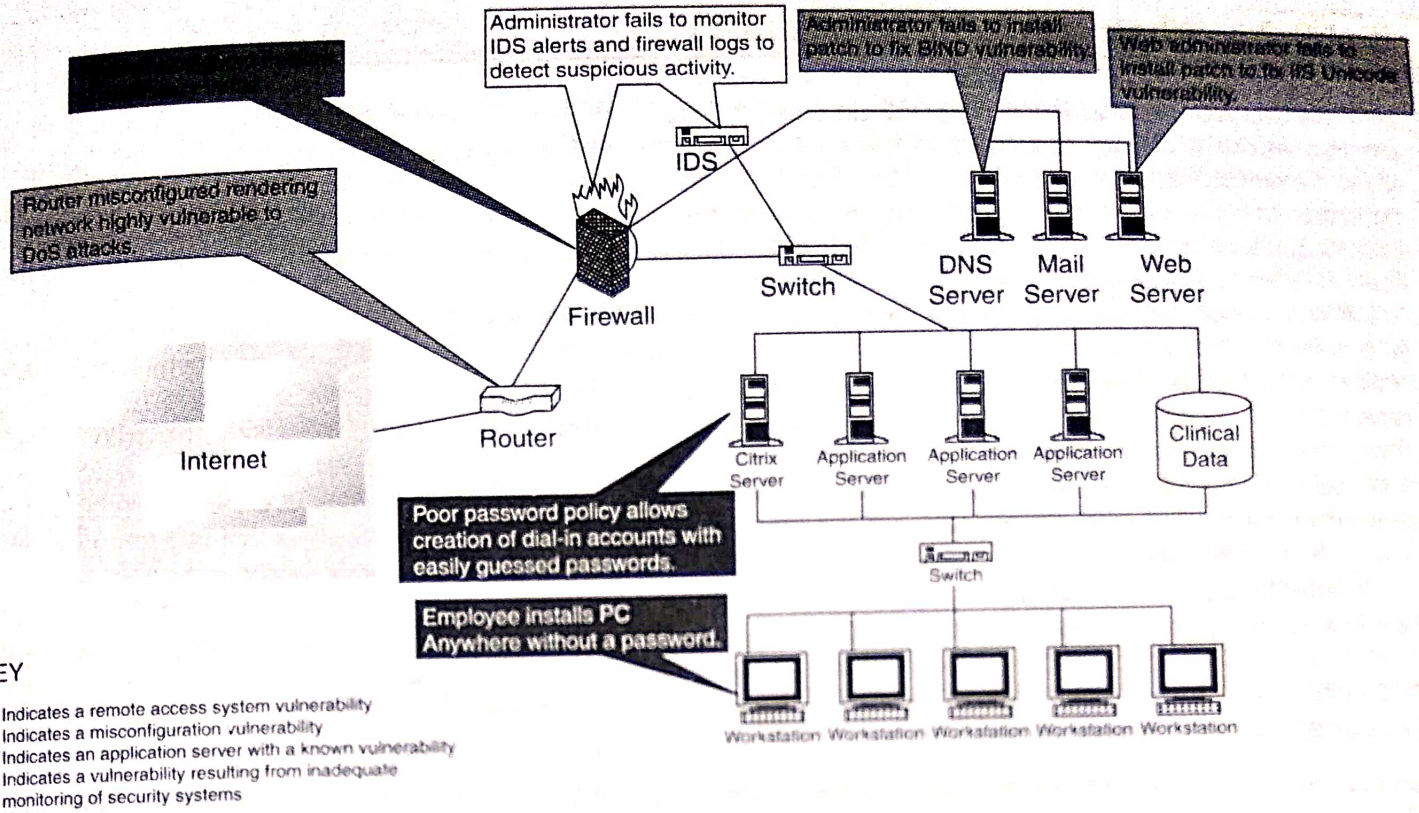

Figure 2.2 Network vulnerabilities – sample network.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 11.6), Wiley India.

An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected. The categories of vulnerabilities that hackers typically search for are the following:

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.

To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

Box 2.2 What Color is Your Hat in the Security World?

When Edward De Bono wrote his epoch making the book *The Six Thinking Hats* most successful concept that helps people to be more productive, focused, and mindfully involved, little did he know that the hats would follow suit in other domains too!! Just read on to discover about the "hats" in security world. And not only that, but also be conscious to know if any of these hats are around you to jeopardize the security of your information assets on the network.

A *black hat* 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 jargon, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

Box 2.2 What Color . . . (*Continued*)

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. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. 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.

A *black hat* will wish to secure his/her own machine whereas a white hat might need to break into a black hat's machine in course of an investigation. What exactly differentiates white hats and black hats is open to interpretation; however, white hats tend to cite altruistic motivations. Usually a black hat is a person who uses his knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or to the manufacturer for correction. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, black hats may work to cause damage maliciously.

Interestingly, this is not all; in the security world, there are hats of other colors too. 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).

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 17.3), Wiley India.

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

As explained in Section 1.5, Chapter 1, cybercrime can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).

1. **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 (explained in Section 1.5.13, Chapter 1), 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.
2. **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.
3. **Crimes targeted at organizations:** Cyberterrorism 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 programs and files or plant programs to get control of the network and/or system (see Box 2.3).

Box 2.3 Patriot Hacking

Patriot hacking[1] 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.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyberattacks like website defacements (explained in Box 1.4, Chapter 1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5.

For detailed information visit www.patriothacking.com

4. **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.
5. **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 (refer to Section 2.4 on "Cyberstalking").

2.2 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. (The custodian of a property can be an individual or an organization; for discussion purpose not mentioned here.) Criminals plan passive and active attacks (see Sections 2.2.2 and 2.2.3 for more details on these topics). 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 breaches of confidentiality.

In addition to the active and passive categories, 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.

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).

2.2.1 Reconnaissance

The literal meaning of "Reconnaissance" is *an act of reconnoitering – explore, often with the goal 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 preattack 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. Let us understand these two phases.

2.2.2 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.

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.

Box 2.4 Tips for Effective Search with "Google" Search Engine

The Google search engine can be used indigenously to perform "Reconnaissance" 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.

Site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within www.google.com. [help site:com] will find pages about help within .com URLs (uniform resource locator). Note that, there should be no space between the "site:" and the domain. This feature is also available through advanced search page, under Advanced Web Search > Domains.

Filetype: This will search within the text of a particular type of file. The file type to search must be typed after the colon.

Link: The query [link:] will list the webpages that have links to the specified webpage. For instance, [link: www.google.com] will list webpages that have links pointing to the Google homepage. Note that there can be no space between the "link:" and the webpage URL. This functionality is also accessible from the advanced search page, under Page Specific Search > Links.

Box 2.4 Tips for . . . (Continued)

Inurl: If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the URL. For instance, [inurl:google search] will return documents that mention the word "google" in their URL, and mention the word "search" anywhere in the document (URL or no). Note that there should be no space between the "inurl:" and the following word. Putting "inurl:" in front of every word in your query is equivalent to putting "allinurl:" in front of your query; this implies [inurl:google inurl:search] is the same as [allinurl: google search].

Cache: If you include other words in the query, Google will highlight those words within the cached document. For instance, [cache: www.google.com web] will show the cached content with the word "web" highlighted. This feature is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the webpage that Google has in its cache. For instance, [cache: www.google.com] will show Google's cache of the Google homepage. Note that there should be no space between the "cache:" and the webpage URL.

Related: The query [related:] will list webpages that are "similar" to a specified webpage. For instance, [related: www.google.com] will list webpages that are similar to the Google homepage. Note that there should be no space between the "related:" and the webpage URL. This feature is also accessible by clicking on the "Similar Pages" link on Google's main results page, and from the advanced search page, under Page Specific Search > Similar.

Info: The query [info:] will present some information that Google has about that webpage. For instance, [info: www.google.com] will show information about the Google homepage. Note that there should be no space between the "info:" and the webpage URL. This feature is also accessible by typing the webpage URL directly into a Google search box.

Define: The query [define:] will provide a definition of the word/phrase you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).

Stocks: If you begin a query with the [stocks:] operator, 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. For instance, [stocks: intc yhoo] will show information about Intel and Yahoo. (Note that you must type the ticker symbols, not the company name.) This feature is also available if you search just on the stock symbols (e.g., [intc yhoo]) and then click on the "Show stock quotes" link on the results page.

Allintitle: If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For instance, [allintitle: google search] will return only documents that have both "google" and "search" in the title. This feature is also available through advanced Search page, under Advanced Web Search > Occurrences.

Intitle: If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word "google" in their title and the word "search" anywhere in the document (title or no). Note that there should be no space between the "intitle:" and the following word. Putting [intitle:] in front of every word in your query is equivalent to putting [allintitle:] at the front of your query; this implies that [intitle:google intitle:search] is the same as [allintitle: google search].

Allinurl: If you start a query with [allinurl:], Google will restrict the results to those with all of the query words in the URL. For instance, [allinurl: google search] will return only documents that have both "google" and "search" in the URL.

Note that [allinurl:] works on words, not on URL components. In particular, it ignores punctuation. Thus, [allinurl: foo/bar] will restrict the results to page with the words "foo" and "bar" in the URL, but won't require that they be separated by a slash within that URL, that they be adjacent, or that they be in that particular word order. There is currently no way to enforce these constraints.

Source: http://www.google.com.tw/help/operators.html

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. The network traffic is sniffed for monitoring the traffic on the network – attacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Along with Google search, various other tools are also used for gathering information about the target victim (Table 2.1).

Table 2.1 | Tools used during passive 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/
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

(Continued)

Table 2.1 | *(Continued)*

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/

Note: IP is Internet Protocol here.

2.2.3 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 suspicion.

Table 2.2 gives the list of tools used for active attacks – some of the tools are also used during "vulnerability assessment" and/or "penetration testing." Refer to Appendix E in CD.

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

(Continued)

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; • 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/

(Contin

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/

(Continued)

Table 2.2 | *(Continued)*

Name of the Tool	*Brief Description*	*Remarks*
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/
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/
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	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.

(Continued)

Table 2.2 | *(Continued)*

Name of the Tool	*Brief Description*	*Remarks*
	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: 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 TCPrewri For further details, visit: http://tcpreplay.synfin.net/trac/
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

Note: IP is Internet Protocol here.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Table 35.2 Wiley India.

2.2.4 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target. The objectiv of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer netwo systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

Box 2.5 Ports and Ports Scanning

A port is an interface on a computer to which one can connect a device. TCP/IP Protocol suite made out of the two protocols, TCP and UDP, is used universally to communicate on the Internet. Each of these has ports 0 through 65536 (i.e., the range is from 2^0 to 2^{16} for binary address calculation). The port numbers are divided into three ranges:

Box 2.5 Ports and Ports . . . (*Continued*)

1. Well-known ports (from 0 to 1023);
2. registered ports;
3. dynamic and/or private ports.

The list of well-known port numbers and short description about the services offered by each of these are provided in Table 2.3.

Table 2.3 | Well-known port numbers

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)
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)		

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 35, p. 774), Wiley India.

Box 2.5 Ports and Ports . . . (Continued)

There are some well-known IP ports (0–999) that require scanning owing to vulnerabilities known about them. In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are preassigned to them by the Internet Assigned Numbers Authority (IANA), an organization working under the auspices of the Internet Architecture Board (IAB), responsible for assigning new Internet-wide IP addresses.

Table 2.3 lists the well-known ports along with the services run on them. Although public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws, and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

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. The important characteristic about these "external ports" is that they are indeed external and visible to the naked eye. Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap (Table 2.2 lists a few vulnerability assessment tools) 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.

Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked. Port scanning is an act of systematically scanning a computer's ports. In technological terms, "port scanning" refers to the act of using various open-ended technologies, tools, and commands to be able to communicate with another remote computer system or network, in a stealth mode, without being apparent, and be able to obtain certain sensitive information about the functions of system and the properties of the hardware and the software being used by the remote systems.

In "*portscan*," a host scans for listening ports on a single target host. In "*portsweep*," a host scans multiple hosts for a specific listening port. 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.

TCP/IP suite of protocols is used to communicate with other computers for specific message formats. Most of these protocols are tied to specific port numbers that are used to transfer particular message formats as data. Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.

1. *Ports 20 and 21 – File Transfer Protocols (FTP) – are used for uploading and downloading of information.*
2. *Port 25 – Simple Mail Transfer Protocol (SMTP) – is used for sending/receiving E-Mails.*
3. *Port 23 – Telnet Protocol – is used to connect directly to a remote host and Internet control message.*
4. *Port 80 – It is used for Hypertext Transfer Protocol (HTTP).*
5. *Internet Control Message Protocol (ICMP) – It does not have a port abstraction and is used for checking network errors, for example, ping.*

Box 2.5 Ports and Ports . . . (*Continued*)

Open ports present two vulnerabilities of which administrators must be wary:

1. Vulnerabilities associated with the program that is delivering the service.
2. 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. There is also the possibility that there are no known vulnerabilities in either the software (program) or the OS at the given time.[2]

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step 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.

Most of the tools listed in Table 2.2 are used for computer network scanning as well.

Usually, most of the attackers consume 90% of the time in scanning, scrutinizing and gathering information on a target and 10% of the time in launching the attack.

2.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password (we will address it in Chapter 4);
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.

2.3 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. It is generally agreed that people are the weak link in security and this principle makes social engineering possible. 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 goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behavior so that