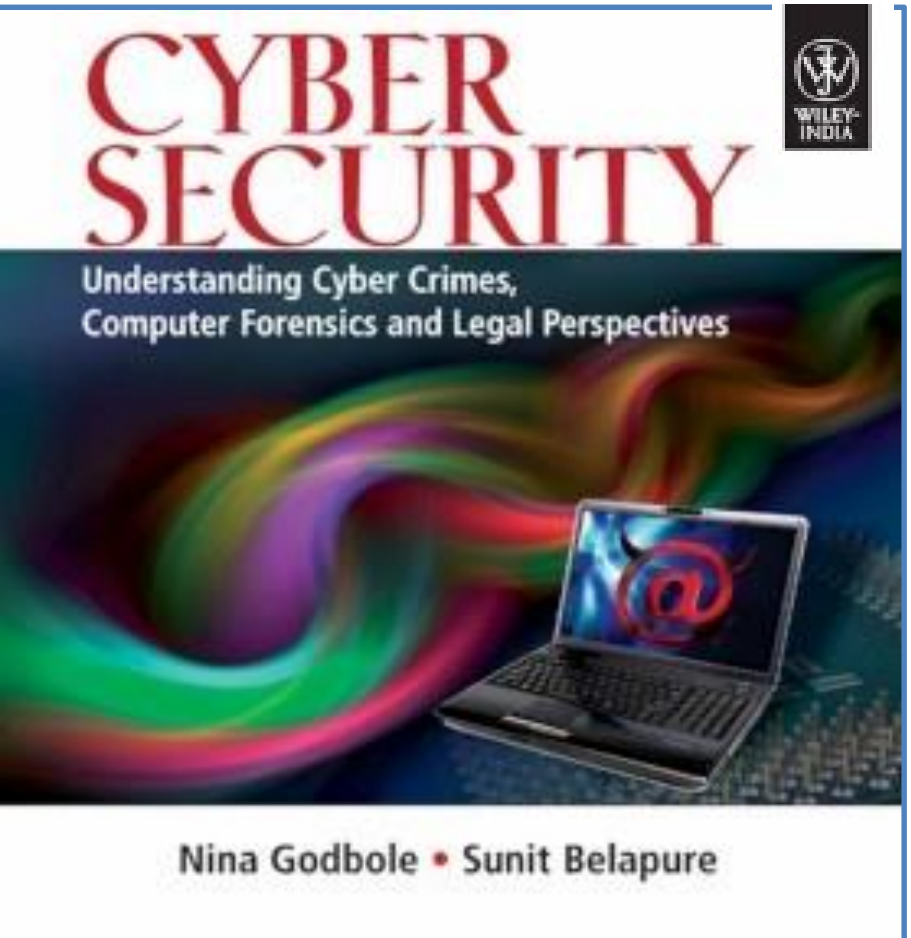
Unit-3

Tools and Methods Used in Cybercrime

Chapter 4
Tools and Methods Used in Cybercrime



Introduction

As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it.

The basic stages of an attack are:

1. Initial uncovering:

i. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means.

ii. In the second step, the attacker uncovers as much information as possible on the company's internal network.

2. Network probe: A "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool is used to discover exactly which services are running on the target system.

3. Crossing the line toward electronic crime (E-crime): Now the attacker is toward committing what is technically a "computer crime" by exploiting possible holes on the target system.

4. Capturing the network: At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily.

5. Grab the data: Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network.

6. Covering tracks: This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

Proxy Servers and Anonymizers

- *Proxy server* is a computer on a network which acts as an intermediary for connections with other computers on that network.
- A proxy server has following purposes:

1. Keep the systems behind the curtain.
2. Speed up access to a resource (through "caching").
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.

- *An anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.

Phishing

Phishing is a fake or false e-mail which can infect systems with in addition to stealing personal and financial data.

How Phishing Works?

Phishers work in the following ways: (1) Planning (decide the target), (2) Setup (create methods for delivering the message and to collect the data about the target), (3) **Attack (**phisher sends a phony message**), (4) Collection (**record the information of victims**), (5) Identity theft and fraud (**use the information that they have gathered to make illegal purchases or commit fraud**).**

Password Cracking

Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system. Examples of guessable passwords include:

1. Blank (none);
2. the words like “password,” “passcode” and “admin”;
3. series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwertyuiop;
4. user’s name or login name;
5. name of user’s friend/relative/pet;
6. user’s birthplace or date of birth, or a relative’s or a friend’s;
7. user’s vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

Online Attacks

- The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."
- It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.

Offline Attacks

- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

Strong, Weak and Random Passwords

- A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords.
- A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it.

Random Passwords

- Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters.
- The general guidelines applicable to the password policies are:

Keyloggers and Spywares

- Keystroke logging- practice of noting (or logging) the keys struck on a keyboard.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior.
- It can be classified as **software keylogger** and **hardware keylogger**.

Software Keyloggers

- Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work.

Hardware Keyloggers

- Hardware keyloggers are small hardware devices connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.
  1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
  2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs.
  3. Prevents Internet banking frauds.
  4. It prevents ID theft.
  5. It secures E-Mail and instant messaging/chatting.

Spywares

- Spyware is malicious software secretly installed on the user's personal computer.
- Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

Virus and Worms

Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself.
Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

Types of Viruses

Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. Boot sector viruses
2. Program viruses
3. Multipartite viruses
4. Stealth viruses
5. Polymorphic viruses
6. Macroviruses
7. Active X and Java Control

- A **computer worm** is a self-replicating malware computer program which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention

Trojan Horse

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.
- Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet.
    - Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
    - On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- An attackers often use backdoors that they detect or install themselves as part of an exploit.
- In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.

How to Protect from Trojan Horses and Backdoors

1. Stay away from suspect websites/weblinks
2. Surf on the Web cautiously
3. Install antivirus/Trojan remover software

Steganography

- It is a method that attempts to hide the existence of a message or communication.
- The word "steganography" comes from the two Greek words: *steganos* meaning "covered" and *graphein* meaning "to write" that means "concealed writing."

Steganalysis

- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

DoS and DDoS Attacks

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

DoS Attacks

- The attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.
  1. Flood a network with traffic, thereby preventing legitimate network traffic.
  2. Disrupt connections between two systems, thereby preventing access to a service.
  3. Prevent a particular individual from accessing a service.
  4. Disrupt service to a specific system or person.

DDoS Attacks

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack.
- A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent.

How to Protect from DoS/DDoS Attacks

1. Implement router filters.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system’s performance and establish baselines for ordinary activity
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

SQL Injection

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- Attackers target the SQL servers – common database servers used by many organizations to store confidential data.
- During an SQL injection attack, Malicious Code is inserted into a web form field or the website's code to make a system execute a command shell or other arbitrary commands.
- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.

Blind SQL Injection

- Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
- The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.

Using SQL injections, attackers can:
1. Obtain some basic information if the purpose of the attack is reconnaissance
2. May gain access to the database by obtaining username and their password
3. Add new data to the database
4. Modify data currently in the database

How to Prevent SQL Injection Attacks
SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**
2. **Modify error reports**
3. **Other preventions**

- The default system accounts for SQL server 2000 should never be used.
- Isolate database server and web server. Both should reside on different machines.
- Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

Buffer Overflow

- Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.
- As buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Types of Buffer Overflow

Stack-Based Buffer Overflow

- Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer.
- The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting.

NOPs

- NOP or NOOP (no operation performed) is an assembly language which enables the developer to force memory alignment to act as a place holder to be replaced by active instructions later on in program development.
- NOP opcode can be used to form an NOP slide, which allows code to execute when the exact value of the instruction pointer is indeterminate.

Heap Buffer Overflow

- Heap buffer overflow occurs in the heap data area when an application copies more data into a buffer than the buffer was designed to contain.

How to Minimize Buffer Overflow

The following methods will definitely help to minimize such attacks:

1. Assessment of secure code manually
2. Disable stack execution
3. Compiler tools
4. Dynamic run-time checks
5. Various tools are used to detect/defend buffer overflow

Attacks on Wireless Networks

- Even when people travel, they still need to work.
- The employee is no longer tied to an office location and is, in effect, "boundaryless."

The following are different types of "mobile workers":

1. Tethered/remote worker
2. Roaming user
3. Nomad
4. Road warrior

- Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs.
- Wireless networks are generally composed of two basic elements:
  (a) access points (APs)
  (b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other (see Fig. 1).

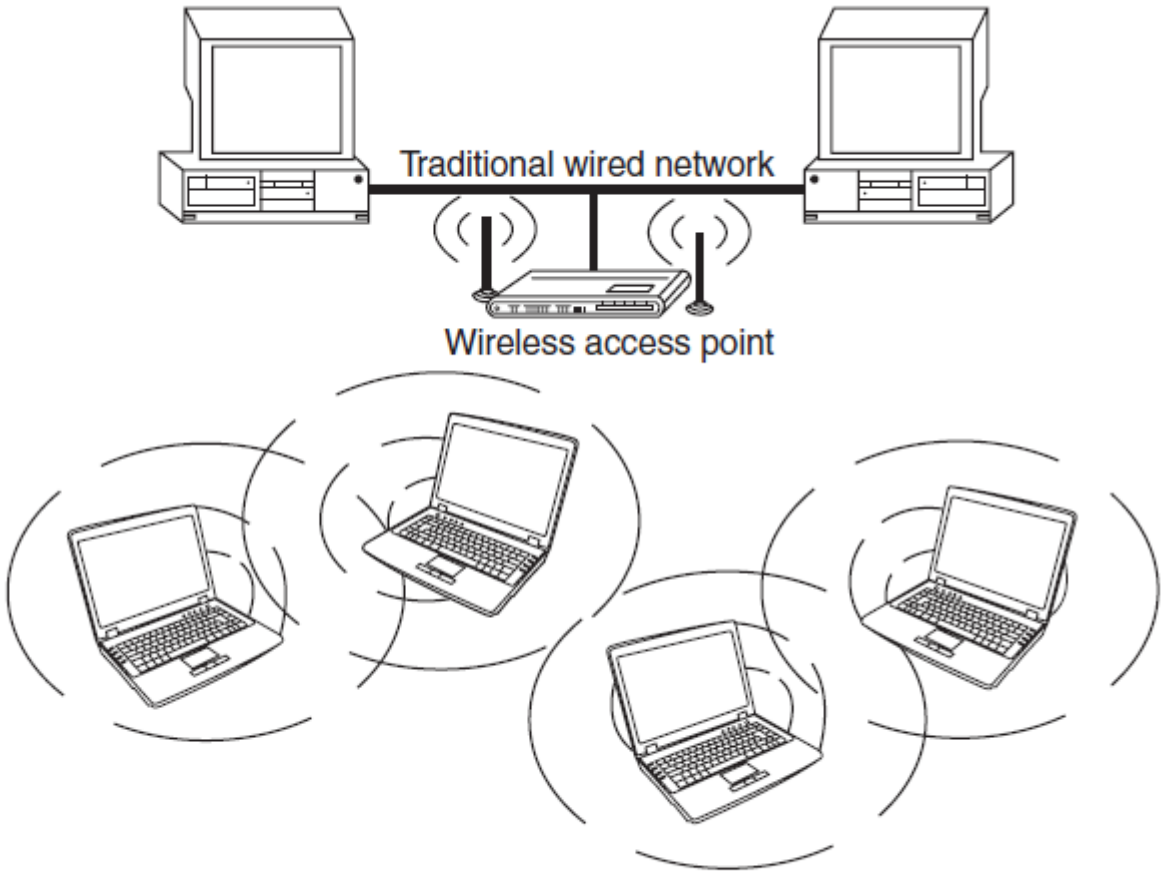


Figure 1 | Wireless networks.

Traditional Techniques of Attacks on Wireless Networks

- Penetration of a wireless network through unauthorized access is termed as wireless cracking.
- There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.
    1. Sniffing
    2. Spoofing
    3. Denial of service (DoS)
    4. Man-in-the-middle attack (MITM)
    5. Encryption cracking

Theft of Internet Hours and Wi-Fi-based Frauds and Misuses

- Wireless network into homes enables the Internet on the finger tip of home users.
- In case, unfortunately, he/she visits a malicious webpage, the router is exposed for an attack.
- As the networks become stronger and more prevalent, more of the signals are available outside the home of the subscriber, spilling over into neighbor's apartments, hallways and the street.

- Be careful with use of WAPs; when you are using a WAP to gain access to computer on a network
- be aware of the local laws/legislations where you are doing it because things can become dangerous from security and privacy as well legal perspective.

How to Secure the Wireless Networks

Following summarized steps will help to improve and strengthen the security of wireless network:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.

   WEP stands for Wired Equivalent Privacy, and WPA stands for Wireless Protected Access. WPA2 is the second version of the WPA standard. Using some encryption is always better than using none, but WEP is the least secure of these standards, and you should not use it if you can avoid it.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade router's firmware periodically.

Questions

- What are the basic stages of an attack?
- What is proxy server? Describe its functions
- Describe the process of password cracking.
- How can keyloggers be used to commit a cybercrime?
- Describe online attacks, offline attacks, strong passwords, random passwords
- What is the difference between a virus and a worm?

Questions

- What is SQL injection and what are the different counter measures to prevent the attack?
- How to Protect from DoS/DDoS Attacks? Explain in detail
- Differentiate between hoax mails and spam.
- Explain with a diagram about Attacks on Wireless Networks.
- Explain the difference between Trojan horses and backdoors?
- How to Secure the Wireless Net
- Explain in detail on Theft of Internet Hours and Wi-Fi-based Frauds and Misuses