Cyberoffenses: How Criminals Plan Them

Objectives

- Understand different types of attack
- Overview of steps involved in planning cybercrime.
- Overview of Social Engineering- What and how.
- Role of Cybercafés in cybercrime.
- Cyberstalking.
- Botnets and Attack Vector.
- Overview on Cloud Computing.

Hackers, Crackers and Phreakers

- Hacker: 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.
- Brute Force Hacking: It is a techniques used to find password or encryption keys. This technique involves trying every possible combination of letters, numbers etc. until the code is broken.

Hackers, Crackers and Phreakers

- Crackers: A cracker is a person who breaks into a computers. Cracker should not be confused with hackers. Some of their crimes include vandalism, theft and snooping in unauthorized areas.
- Phreaking: This is an infamous art of breaking into phone or other communication system.

Attackers and their Profile

Attacker	Skill Level	Motivation
Hacker	High	Improve Security
Cracker	High	Harm System
Script Kiddie	Low	Gain recognition
Spy	High	Earn money
Employee	Varies	Varies
Cyber terrorist	High	Support ideology

Categories of Cybercrime

- Cyber crimes can be categorized based on:
  - The target of crime and
  - Whether the crime occurs as a single event or as a series of events.
- Crimes Targeted at Individuals: The goal is to exploit human weakness, these crimes include financial frauds, sale of non existent or stolen items, child pornography, Copyright violation, harassment etc.

Categories of Cybercrime

- Crimes targeted at property: This include stealing mobile devices such as cell phone, laptop and PDAs, Removable media etc.
- Crimes targeted at organization: Attackers 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 problems and files 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.
- Series of Events: This involves attacker interacting with the victims repetitively. For example attacker interacts with the victims on the phone and/or via chat rooms to establish relationship and then they exploit the relationship.

How Criminals plan the attack

How Criminals plan the attack

- Criminals use many tools to locate the vulnerabilities of their target. The target can be an individual or an organization. Criminals plan active or passive plan.
- In addition to active or passive categories attacks can be categorized as either inside or outside.

Inside Attacker

- 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.

Outside Attack

- An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or outsider, who is indirectly associated with the organization. It is attempted through the internet or a remote access connection. Following phases are involved in planning cybecrime:
  - Reconnaissance (Investigation)
  - Scanning and Scrutinizing (Examining) the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
  - Launching an attack.

Reconnaissance

- The literal meaning of “Reconnaissance” is an act investigation often with the goal of finding something or somebody to gain information about an enemy.
- In the world of hacking reconnaissance phase begins with ***“Footprinting”*** – this is the preparation toward preattack. Footprinting gives vulnerabilities and provides a judgments about possible exploitation of those vulnerabilities.
- An attacker attempts to gather the information in two phases: Passive and Active attack.

Passive Attack

- A passive attack involves gathering information about a target without his/her knowledge.
- It can be as simple as watching a building to identify what time employees enter the building premises.
- Network sniffing is an another means of passive attack where network traffic is sniffed for monitoring the traffic on the network- attacker watches the flow of data to see what time certain transaction take place and where the traffic is going.

Active Attack

- An active attack involves inquiring the network to discover individual host 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***" .
- This provides confirmation to an attacker about security measures.

Scanning and Scrutinizing Gathered Information

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

TCP/IP Port Scanning

Category	Number Range	Description	Example
Well-known port numbers	0–1023	Reserved for the most universal applications	25-Simple Mail Transfer Protocol (SMTP)
Registered port numbers	1024–49151	Other applications that are not as widely used	1026-Calendar access protocol
Private port numbers	49152–65535	Used for private applications in a particular organization	Any applications

Table 9-5 TCP/IP port categories

Port Scanners

- If an attacker knows a specific port is used, that port could be probed for weakness
- **Port scanner**
  - Used to search a system for port vulnerabilities that could be used in an attack
  - Determines the state of a port to know what applications are running and could be exploited
- Three port states:
  - Open, closed, and blocked

Port Scanner

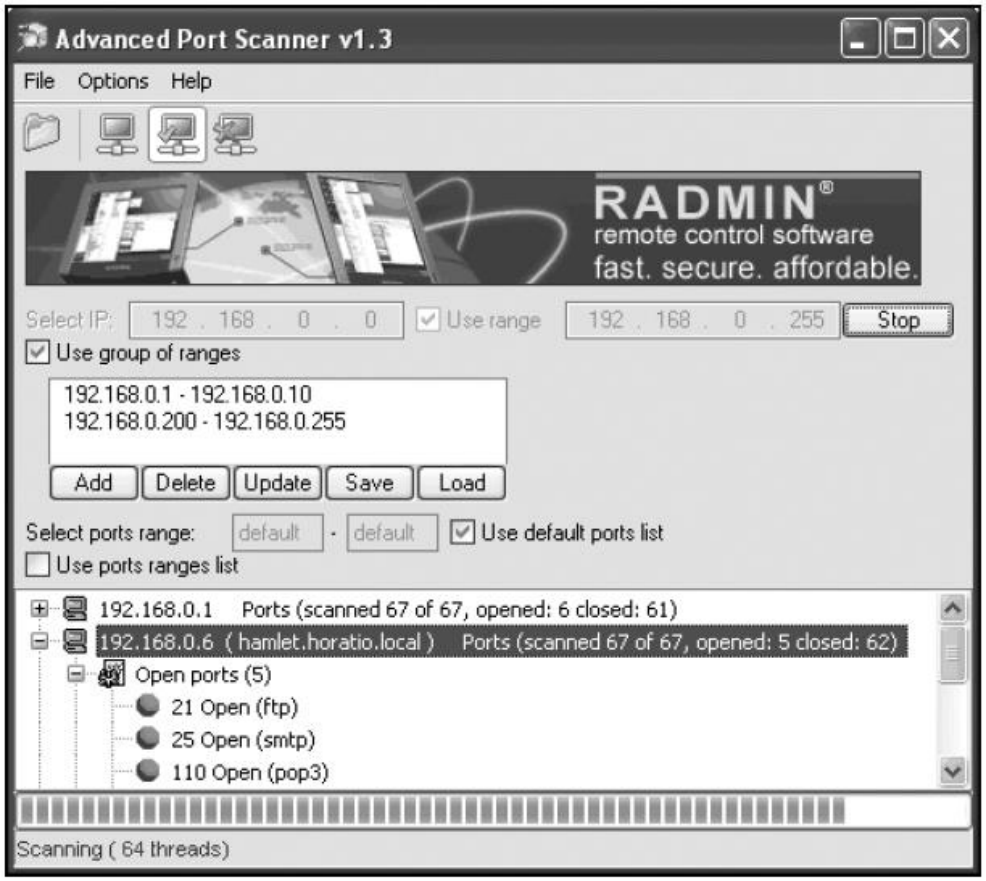


Figure 9-3 Port scanner

Social Engineering

- Social Engineering is a “technique to influence” people to obtain the information or perform some action.
- A social engineer usually uses telecommunication or internet to do something that is against the security/ policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationship with insiders.

Social Engineering

- 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 people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.

Social Engineering Example

- Maria, a customer service representative, receives a telephone call from someone claiming to be a client. This person has a thick accent that makes his speech hard to understand. Maria asks him to respond to a series of ID authentication questions to ensure that he is an approved client. However, when asked a question, the caller mumbles his response with an accent and the representative cannot understand him. Too embarrassed to keep asking him to repeat his answer, Maria finally provides him with the password.

Social Engineering Example

- The help desk at a large corporation is overwhelmed by the number of telephone calls it receives after a virus attacks. Ari is a help desk technician and receives a frantic call from a user who identifies himself as Frank, a company vice president. Frank says that an office assistant has been unable to complete and send him a critical report because of the virus and is now going home sick. Frank must have that office assistant's network password so he can finish the report, which is due by the end of the day. Because Ari is worn out from the virus attack and has more calls coming in, he looks up the password and gives it to Frank. Ari does not know that Frank is not an employee, but an outsider who now can easily access the company's computer system.

Social Engineering Example

- Natasha, a contract programmer at a financial institution, drives past a security guard who recognizes her and waves her into the building. However, the guard does not realize that Natasha's contract was terminated the previous week. Once inside, Natasha pretends that she is performing an audit and questions a new employee, who willingly gives her the information she requests. Natasha then uses that information to transfer over $10 million to her foreign bank account

Classification of Social Engineering

- Human-Based Social Engineering : Human-based social engineering refers to person-to-person interaction to get the required/desired information.
  - Impersonating an employee or valid user
  - Posing as an important user
  - Using a third person
  - Calling technical support
  - Shoulder Surfing
  - Dumpster Diving

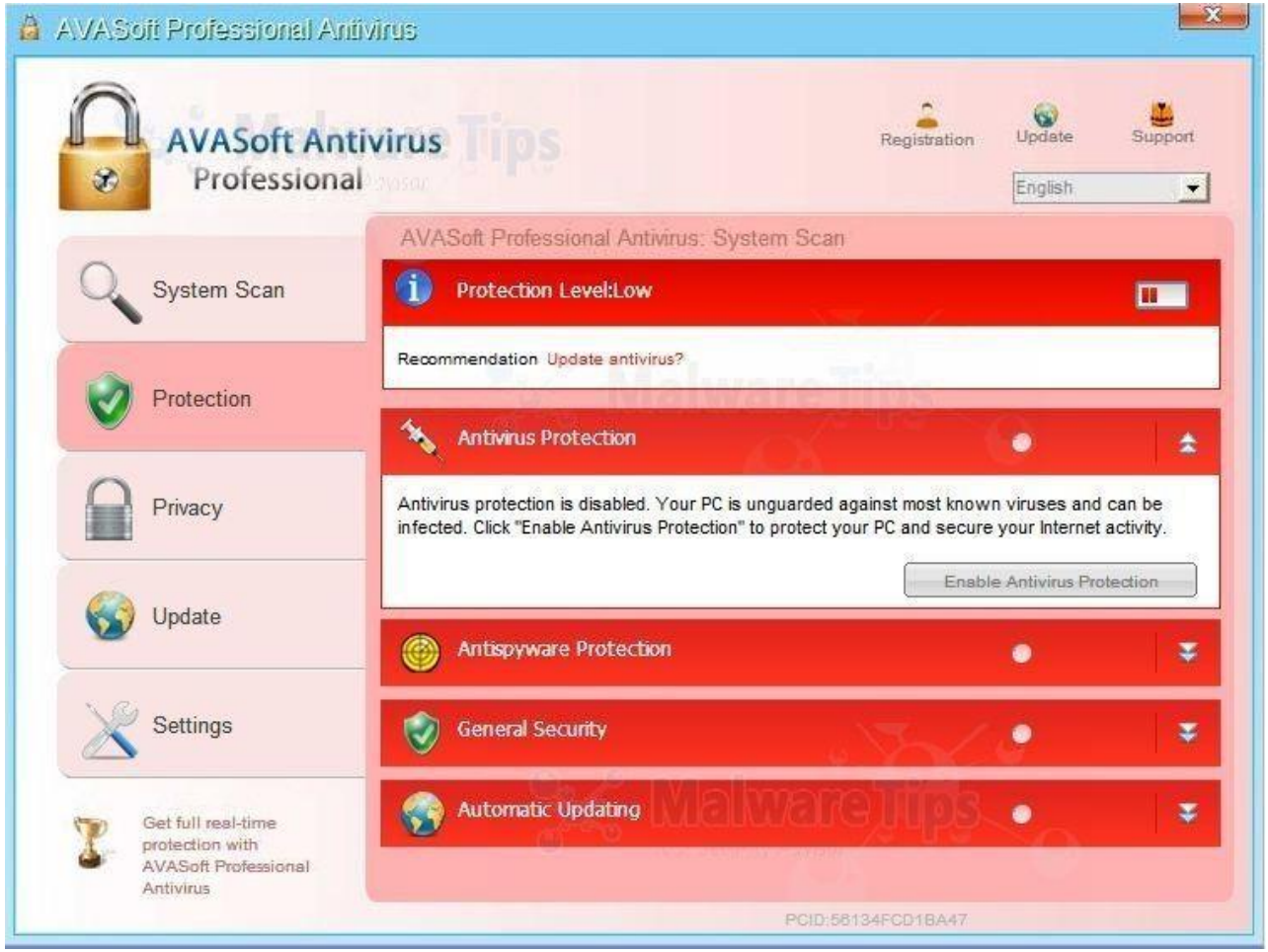
Shoulder Surfing

Dumpster Diving

Classification of Social Engineering

- Computer-Based Social Engineering: It refers to get the required/desired information using computer software/internet. For example sending a fake mail to a user and asking him/her to re-enter a password in a web page to confirm it.
  - Fake E-mail
  - E-mail attachment
  - Pop-up Windows

Example Pop-up



Social Engineering Statistics

- As per Microsoft Corporation research in 2007 there is an increase in the number of security attacks designed to steal PI. According to FBI survey on average 41% of security related losses are direct result of employees stealing information from their company.

Cyberstalking

Cyberstalking

- Cyberstalking has been defined as the use of information and communications technology, particularly the internet, by and individual or group of individuals to harass another individual or group of individuals.
- Cyberstalking refers to use of internet and/or other electronic communication devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly for following a person, visiting a person's home and/or business place.

Types of Stalkers

- Online Stalkers: Stalker aim to start the interaction with the victim directly with the help of the internet (E-mail and chat rooms). They makes sure that the victim recognizes the attack attempted on him/her. Stalker may use a third party person to harass the victim.

Types of Stalkers

- Offline Stalkers: The stalkers may begin the attack using traditional methods such as following the victim, watching daily routine of victim, gather information of victim through internet etc.

Cases Reported on Cyberstalking

- The majority of cyberstlkers are men and majority of their victims are women. In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate and neighbor.

How Stalking Works

- Gathering Personal Information of the victim
- Establish a connection.
- Keep on sending repeated mail
- Posting personal information on web site
- Call victim (Harass/Blackmailing)

Cybercafe and Cybercrimes

- In past several years, many instances have been reported in India, where cybercafés are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank password and subsequent fraudulent withdrawal of money have also happened through cybercafés.

Cybercafe and Cybercrimes

- Survey in one the metropolitan city in India
  - Pirated Software are installed in computers
  - Antivirus are not updated
  - Several cafes have installed the software called “Deep Freeze”
  - AMC is not updated
  - Unwanted stuff are not blocked
  - Owners are not aware about cyber security/Law
  - Government/State Police (Cyber Cell Wing) do not seem to provide IT Governance guidelines to café owners

Tips for Safety and Security

- Always Logout
- Stay with the computer
- Clear history and temporary files
- Be Alert
- Avoid online financial transaction
- Change Passwords
- Virtual Keyboard
- Security Warning

Virtual Keyboard

Botnet

- Bot is an automated program for doing some particular task, often over a network.
- In simple word, a Bot is simply automated computer program through which one can gain control of your computer by infecting them with virus
- Your computer may be a part of botnet even though it seems working normally.

Security Parameters

- Use antivirus and anti- spyware and keep it up to date
- Set the OS to download and install security patches automatically.
- Use a firewall to protect the system from hacking attacks while it is connected on the internet.
- Disconnect from the internet when you are away from your computer
- Check regularly the folder in your mailbox
- Take an immediate action if your system is infected.

Attack Vector

- An attack vector is a path or means by which an attacker can gain access to a computer or to a network server to deliver a ***payload*** or malicious outcome.
- Attack vector enable attackers to exploit system vulnerabilities.

Payload means malicious activity that the attack performs

Attack Vector

- To some extent attack vector can be protected using firewalls and antivirus but no method is totally attack proof.

Zero-Day Attack

- A zero day is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e. undisclosed to the software vendors and software users).
- A zero day attack is launched just on or before the first or “zeroth” day of vendor awareness.

Zero Day Emergency Response Team (ZERT)

- This is a group of software engineers who work to release non-vendor patches for zero day exploits.

Attack Vector Example

- Attack by E-Mail
- Attachments
- Attack by deception
- Hackers
- Heedless guests
- Attack of Worms
- Malicious macros
- Foist ware (Sneak ware)
- Viruses

Attack by deception

- Deception is aimed at the user/operator as vulnerable entry point.
- Social engineering and hoaxes are other forms of deception that are often an attack vector.

Heedless guests (Attack by Webpage)

- Counterfeit websites are used to extract personal information. Such websites are very much like the genuine websites.

Foist ware

- Foist ware is the software that adds hidden components to the system cleverly.
- Spyware is the most common form of foistware.

Malicious Macros

- Microsoft word and excel are some of the examples that allows macros, these macros can also be used for malicious purposes.

Cloud Computing

- Cloud computing is internet based development and use of computer technology. Characteristics of cloud computing are:
  - It is sold on demand
  - It is elastic in term of usage
  - The service is fully managed by the provider
- Prime area of risk in cloud computing is protection of user data.

Why Cloud Computing

- Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one users computer.
- It could bring hardware cost down.
- Organization do not have to buy a set of software license for every employee and the storage devices take up space.

Why Cloud Computing

- Organization do not have to rent a physical space to store servers and database. Storage and digital devices take up space.
- Organization would be able to save money on IT support

Cloud Computing

- Public Cloud: Sells services to anyone
- Private Cloud: Like a proprietary network that supplies the hosted services to limited number of people.
- Virtual Cloud: When a service provider uses public cloud resources to create a private cloud, the result is called a virtual private cloud.