

The background of the slide features a person wearing a dark hoodie, seen from the chest up, with their hands on a keyboard. The person's face is obscured by the hood. The background is a dark blue-grey color with a faint world map. Overlaid on the map are vertical columns of binary code (0s and 1s) and various numbers (0-9) and symbols (like \$, %, &, @, #, !, ~, ^, &copy;, &reg;, &trade;) in a light green or teal color. The overall theme is digital and cyber-related.

# CYBER OFFENSES:

How criminals plan them

# Unit 2: Learning Objectives

- 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
- Learn about the role of cybercafe in cybercrime
- Understand what is cyberstalking
- Learn about botnet and attack vector
- Get an overview of cloud computing

# Few Definitions

- Hacker
- Brute force hacking
- Cracker
- Cracker Tools
- Phreaking
- War dialer

# Hacker

- A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them
- 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.
- Many sites supply crackers with programs that allow them to crack computers.
- Some of these programs contain dictionaries for guessing passwords

# Cracker Tools

- These are programs used to break into computers.
- Cracker Tools include
  - *Password crackers*
  - *Trojans*
  - *Viruses*
  - *Worms*

Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does there need to be user action for it to spread?	Yes	No	Yes



## ■ Phreaking

- *This is a notorious action of breaking into phone or other communication system.*

## ■ War Dialer

- *A war dialer is a computer program used to identify the **phone numbers** that can successfully make a connection with a computer modem.*

# Introduction

- Cybercriminals use the World Wide Web and Internet to an optimal level for an illegal activities.
- These criminals take the advantage of the wide spread lack of awareness about cybercrimes and cyberlaws among people who are constantly using the IT infrastructure for official and personal purposes.
- Attacker exploit the network vulnerability.

# Categories of vulnerabilities that hackers typically search for:

1. Inadequate border protection
2. Remote access servers(RASs)
3. Application servers
4. Misconfigured systems and systems with default configurations.

# What color is your Hat in the security world?



# What color is your Hat in the security world?

- **Black Hat** - Just like in the old westerns, these are the bad guys. A black hat is a cracker or a dark side hacker.



# What color is your Hat in the security world?

- **White Hat** – While black hats use their skill for malicious purposes, white hats are ethical hackers **use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks.**



# What color is your Hat in the security world?



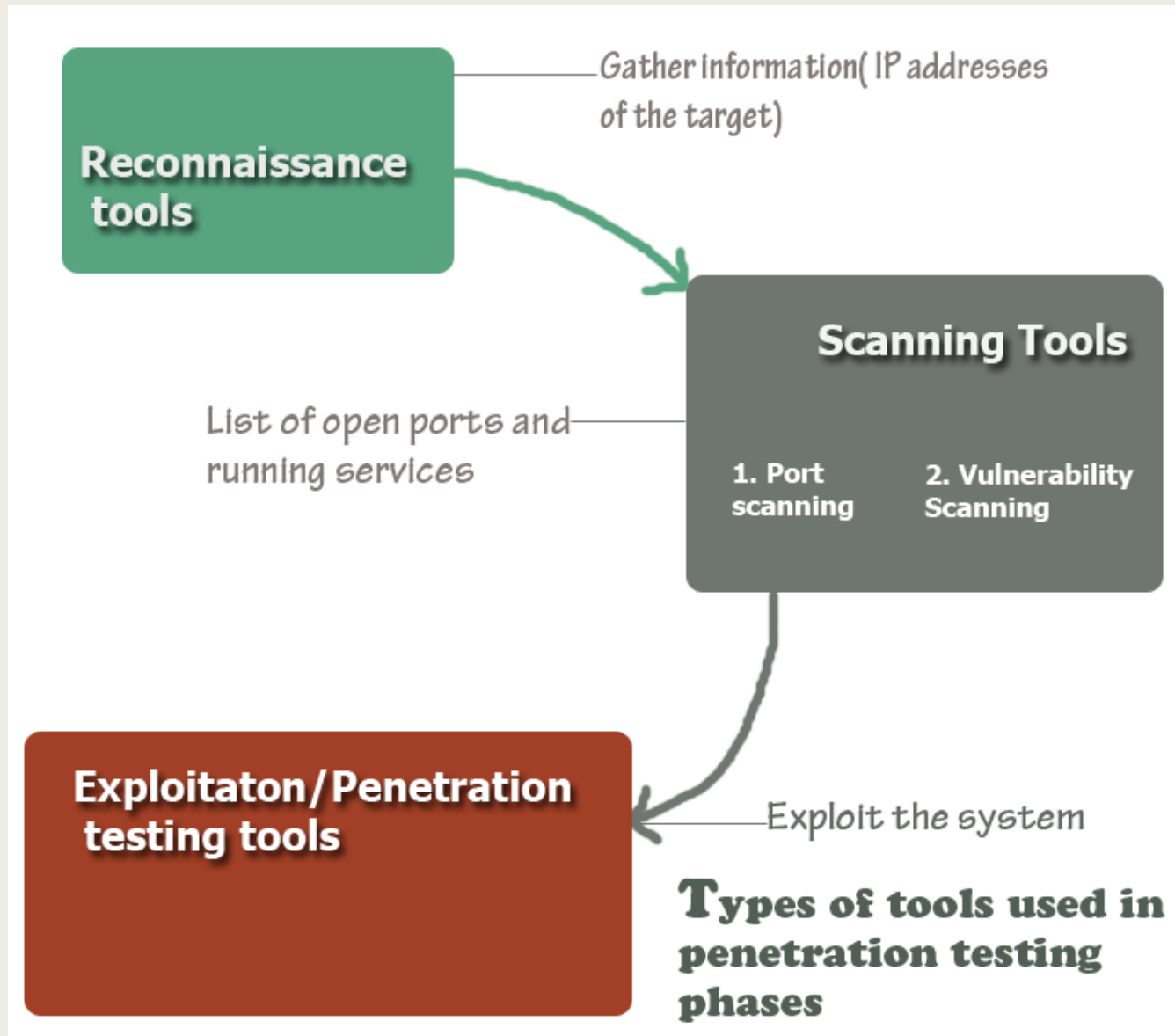
- **Gray Hat** – A gray hat, as you would imagine, is a bit of a white hat/black hat hybrid.
- Thankfully, like white hats, **their mission is not to do damage to a system or network, but to expose flaws in system security.**
- The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data:



# Categories of Cybercrime

- Target of the crime
  - *Crimes targeted at individuals*
  - *Crimes targeted at property*
  - *Crimes targeted at organizations*
  - *Crimes targeted at society*
  - *Crimes emanating from usenet newsgroup*
  
- Whether the crime occurs as a single event or as a series of events.
  - *Single event cybercrime: hacking or fraud*
  - *Series of events: cyberstalking*

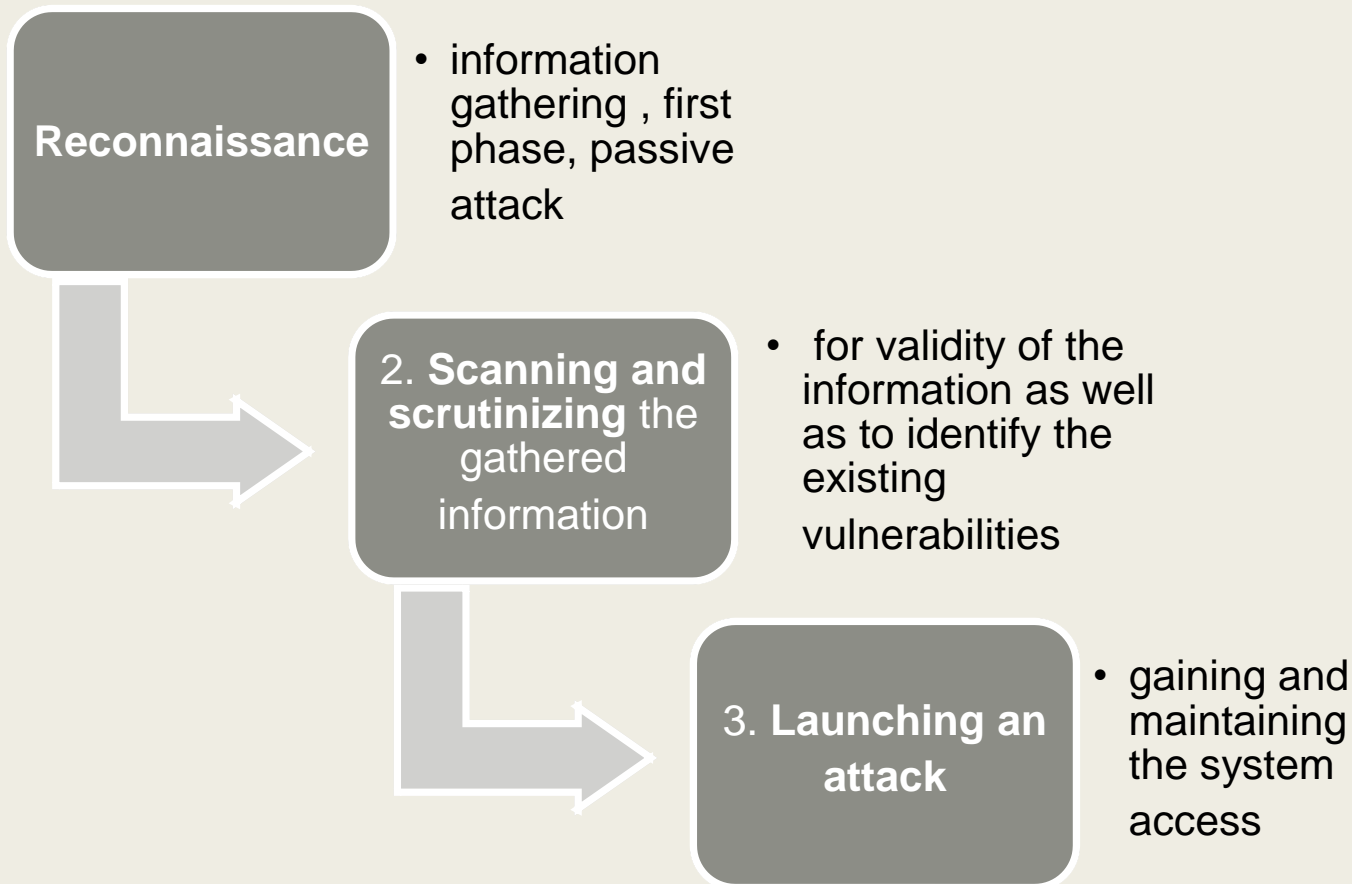
# How criminals Plan the Attacks



# How criminals Plan the Attacks



Phases involved in planning cybercrime:



# Types of attacks:

## ■ Active attack

- *Used to alter system*
- *Affects the availability, integrity and authenticity of data*

## ■ Passive attack

- *Attempts to gain information about the target*
- *Leads to breaches of confidentiality*

## ■ Inside attack

- *Attack originating and/or attempted within the security perimeter of an organization*
- *Gains access to more resources than expected.*

## ■ Outside attack

- *Is attempted by a source outside the security perimeter,*
- *May be an insider or an outsider , who is indirectly associated with the organization*
- *Attempted through internet or remote access connection*

# Reconnaissance

- A reconnaissance attack occurs when an adversary tries to learn information about your network
- **Reconnaissance** is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
- **Reconnaissance** is also known as information gathering
- Is the preparatory phase to understand the system, its networking ports and services and other aspects of security, that are needful for launching the attack

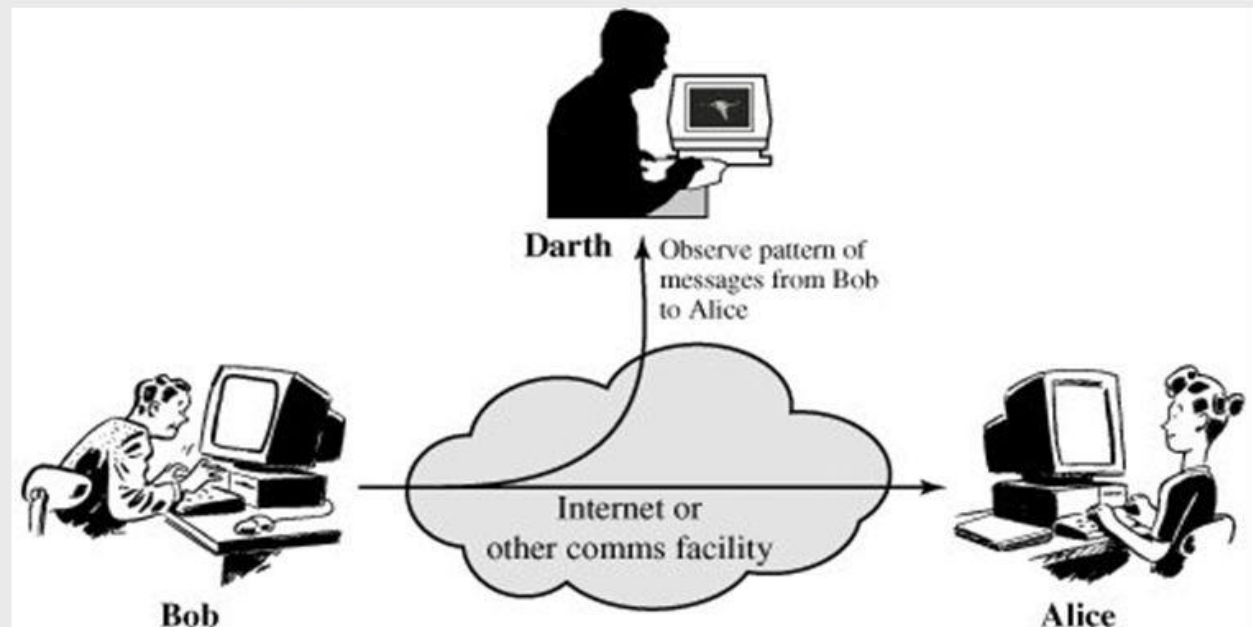
- An attacker attempts to gather information in two phases
  1. *Passive attacks*
  2. *Active attacks*

# Passive attacks

## Passive Attacks

---

### ◆ Traffic analysis



# Passive attacks

1. Involves gathering information about the target without his/ her knowledge.
2. **Google or yahoo search:** to locate information about employees
3. Surfing online community group: **facebook**; to gain information about an individual
4. **Organizations website:** for personnel directory or information about key employees; used in social engineering attack to reach the target
5. **Blogs, newsgroups, press releases, etc**
6. **Going through job postings**
7. Network sniffing: information on Internet Protocol address ranges, hidden servers or networks or services on the system



# Tools used during passive attacks


1. CheckUserNames
2. Google earth
3. Internet Archive: permanent access for researchers , historians and scholars to historical collections
4. Professional community: linkedIn
5. People Search
6. Domain Name Confirmation
7. WHOIS
8. Nslookup
9. Dnsstuff

# Tools used during passive attacks

- 9. Traceroute
- 10. VisualRoute Trace
- 11. eMailTrackerPro
- 12. HTTrack

# Tools used during passive attacks

checkusernames.com/?username=sanketdesai



Check the use of your brand or username on 160 Social Networks:

To check the availability of your username on over 500 social networks check out our new, updated site at: [KnowEm.com](http://KnowEm.com).

KnowEm also offers a **Premium Service** which will create profiles for you on up to 300 popular social media sites.

Facebook

Twitter

LinkedIn

Buffer

Hootsuite

You Tube <a href="#">Not Available</a>	Live Leak <a href="#">Not Available</a>	APSense <a href="#">Not Available</a>	Intense Debate <a href="#">Not Available</a>
Wikipedia <a href="#">Not Available</a>	Zimbio <a href="#">Available</a>	Folkd <a href="#">Available</a>	Design Float <a href="#">Not Available</a>
Linked In <a href="#">Not Available</a>	Houzz <a href="#">Not Available</a>	Watt Pad <a href="#">Not Available</a>	Stock Twits Oops, Error!
Twitter <a href="#">Not Available</a>	My Space <a href="#">Available</a>	Empire Avenue Oops, Error!	Fotki <a href="#">Available</a>
Ebay <a href="#">Not Available</a>	Game Spot Oops, Error!	Spark People <a href="#">Available</a>	Trend Hunter <a href="#">Not Available</a>
Tumblr <a href="#">Not Available</a>	Cracked Oops, Error!	N4G Oops, Error!	Ads Of The World <a href="#">Available</a>
Pinterest <a href="#">Not Available</a>	Behance <a href="#">Not Available</a>	Veoh <a href="#">Not Available</a>	Eventful Oops, Error!
Blogger <a href="#">Not Available</a>	Sky Rock <a href="#">Available</a>	Ebaums World <a href="#">Not Available</a>	Tiny Chat Oops, Error!
Imgur <a href="#">Not Available</a>	Viadeo <a href="#">Not Available</a>	Dzone Links <a href="#">Not Available</a>	Shock Wave <a href="#">Available</a>
Flickr <a href="#">Not Available</a>	We Heart It <a href="#">Available</a>	Mouth Shut <a href="#">Available</a>	Active Rain <a href="#">Not Available</a>
Word Press <a href="#">Not Available</a>	Fan Pop <a href="#">Available</a>	Yuku <a href="#">Available</a>	Destructoid Oops, Error!
Daily Motion <a href="#">Not Available</a>	Dreams Time Oops, Error!	Fark <a href="#">Available</a>	Boonex <a href="#">Available</a>
Reddit <a href="#">Not Available</a>	I Can Has Cheezburger? Oops, Error!	Blog Talk Radio Oops, Error!	Tech Dirt Oops, Error!
CNET Oops, Error!	Meta Cafe Oops, Error!	Zedge <a href="#">Not Available</a>	Jigsy <a href="#">Available</a>
Vimeo <a href="#">Not Available</a>	Last FM Oops, Error!	Dat Piff Oops, Error!	The Hype Machine <a href="#">Available</a>
Slide Share <a href="#">Not Available</a>	Hi5 <a href="#">Not Available</a>	Wonder How To <a href="#">Available</a>	Moby Picture <a href="#">Available</a>
Deviant Art Oops, Error!	The Motley Fool <a href="#">Available</a>	Crunchy Roll Oops, Error!	Wall Inside <a href="#">Not Available</a>
Live Journal <a href="#">Not Available</a>	Fixya Oops, Error!	8 Tracks Oops, Error!	Programmable Web Oops, Error!
Yelp <a href="#">Not Available</a>	Kongregate <a href="#">Not Available</a>	Red Bubble <a href="#">Not Available</a>	All My Faves <a href="#">Not Available</a>
Wikia <a href="#">Available</a>		BitLy <a href="#">Not Available</a>	

..csv

meetingAttendanc....csv

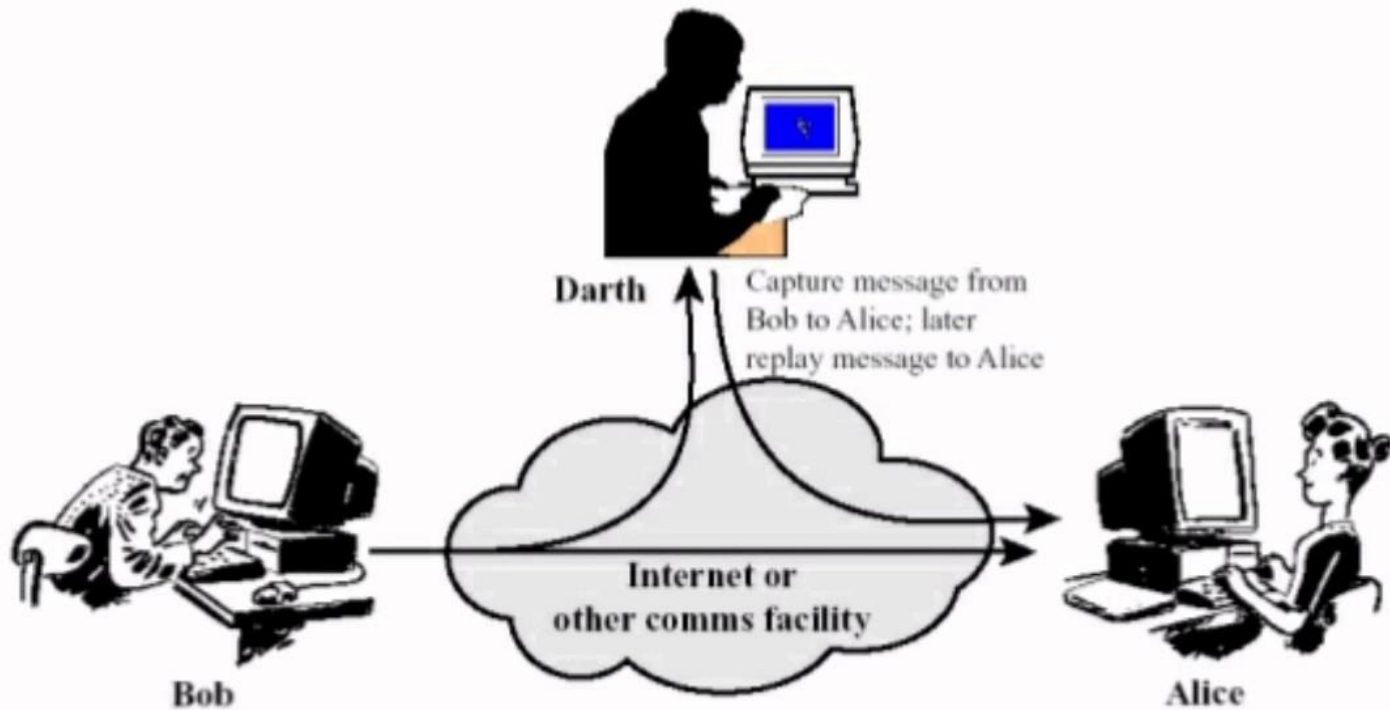
SBL\_WEEK 2\_HARS....pdf

SBL\_WEEK 2\_HARS....pdf

SBL\_WEEK 2\_HARS....pdf

# Active Attacks

## Active Attacks: Replay



# Active Attacks

- Rattling the doorknobs/ Active reconnaissance
- Involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- Can provide confirmation to an attacker about security measures in place.

# Tools used during active attacks

1. Arphound
2. Arping
3. Bing
4. Bugtraq
5. Dig
6. DNStacer
7. Dsniff
8. Filesnarf
9. FindSMB

# Tools used during active attacks

10. Hmap

11. Hping

12. Hunt

13. Netcat

14. Nmap

15. TCPdump

16. TCPReplay

- **Words of Caution:** never try to use the above mentioned tools in a network or system without authorization from the proper authority.
- The intention of the PPT is to help the students/ engineers/ professionals who also wants to learn and develop a career in cyber security.





- After gathering solid information about the target, the next step is to start scanning the target system.

# Scanning and Scrutinizing gathered information

- Is a key step to examine intelligently while gathering information about the target.
- The objectives are:
  1. Port scanning
  2. Network scanning
  3. Vulnerability scanning

# What is Port Scanning?

- The act of systematically scanning a computer's ports.
- Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer.
- There are, however, software products that can stop a port scanner from doing any damage to your system.

# Port Scanning (Few points)

- A port is an interface on a computer to which one can connect a device.
- At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.
- The most common protocols that use port numbers, are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

- Each port handles different application traffic.
- Port 80, for example, handles normal HTTP web traffic, while port 443 handles HTTPS encrypted web traffic. Sending email is always done over port 25, while receiving it is completed over port 110.
- Each of these has ports 0 → 65535 ( $2^0$  to  $2^{16}$  binary calculation)
- The Port numbers are divided into 3 ranges
  - *Well known ports (from 0 to 1023)*
  - *Registered ports*
  - *Dynamic and/or private ports*

# Port scan

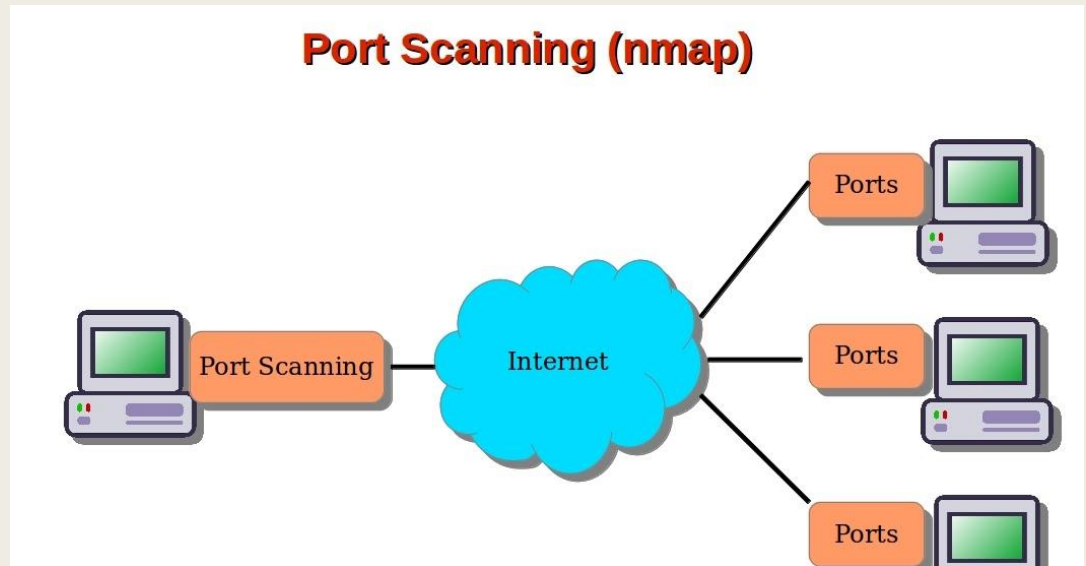
- a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- The result of a scan on a port is usually generalised into one of the following categories:
  1. Open or accepted
  2. Closed or not listening
  3. Filtered or blocked.

# Types of port scans:

- **vanilla:** the scanner attempts to connect to all 65,535 ports
- **strobe:** a more focused scan looking only for known services to exploit
- **fragmented packets:** the scanner sends packet fragments that get through simple packet filters in a firewall
- **UDP:** the scanner looks for open UDP ports
- **sweep:** the scanner connects to the same port on more than one machine
- **FTP bounce:** the scanner goes through an FTP server in order to disguise the source of the scan
- **stealth scan:** the scanner blocks the scanned computer from recording the port scan activities.

# Scanning Tools used ....

1. Nmap- This tool creates a complete list of opened ports in your target.
2. Nessus
3. Nexpose





Port number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

- Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer.

```
root@kali:~# nmap -sS 192.168.28.129
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-02-22 11:07 EST
```

```
Nmap scan report for 192.168.28.129
```

```
Host is up (0.00032s latency).
```

```
Not shown: 991 closed ports
```

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

139/tcp	open	netbios-ssn
---------	------	-------------

143/tcp	open	imap
---------	------	------

443/tcp	open	https
---------	------	-------

445/tcp	open	microsoft-ds
---------	------	--------------

5001/tcp	open	complex-link
----------	------	--------------

8080/tcp	open	http-proxy
----------	------	------------

8081/tcp	open	blackice-icecap
----------	------	-----------------

```
MAC Address: 00:0C:29:0B:B0:26 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

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

## Port Scanning Responses

**1 Open, Accepted:**  
The computer responds and asks if there is anything it can do for you.

**2 Closed, Not Listening:**  
The computer responds that "This port is currently in use and unavailable at this time."

**3 Filtered, Dropped, Blocked:**  
The computer doesn't even bother to respond, it has no time for shenanigans.



```
root@kali:~# nmap -sS 192.168.1.130 -p 22,80,139
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-08 10:04 EDT
Nmap scan report for 192.168.1.130
Host is up (0.00033s latency).

PORT      STATE      SERVICE
22/tcp    closed     ssh
80/tcp    open       http
139/tcp   filtered   netbios-ssn
MAC Address: 00:0C:29:13:56:E7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds
```

# Step 2: Scanning and Scrutinizing

## Phase 2: Scrutinizing

- Scrutinizing is always called “Enumeration” in the hacking world.
- The objective behind this is to identify:
  - *The valid user accounts/ groups*
  - *Network resources*
  - *OS and different applications that are running on the OS*

Usually most of the attackers consume **90%** of the time in scanning, scrutinizing and gathering information on a target

&

**10%** of the time in launching the attack

# 3. Launching an Attack (Gaining and Maintaining the System Access)

- After scanning and scrutinizing, the attack is launched using the following steps:
  1. Crack the password
  2. Exploit the privileges
  3. Execute the malicious command/ applications
  4. Hide the files
  5. Cover the track – delete access logs, so that there is no trail illicit activity.

# SOCIAL ENGINEERING

The clever manipulation  
of the natural human  
tendency to trust.

# What is Social Engineering?

- *Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders*
  - Example: Calling a user and pretending to be someone from service desk, working on a network issue and then asking questions like username password and so on.





# Kevin Mitnick

## Famous Social Engineer Hacker

- *Went to prison for hacking*
- *Became ethical hacker*



# Kevin Mitnick - *Art of Deception*:

- *"People inherently want to be helpful and therefore are easily duped"*
- *"They assume a level of trust in order to avoid conflict"*
- *"It's all about gaining access to information that people think is innocuous when it isn't"*
- *Here a nice voice on the phone, we want to be helpful*
- *Social engineering cannot be blocked by technology alone*

# Live Example



- *Convinced friend that I would help fix their computer*
- *People inherently want to trust and will believe someone when they want to be helpful*
- *Fixed minor problems on the computer and secretly installed remote control software*
- *Now I have **total access** to their computer through **ultravnc viewer***

# Classification of Social Engineering

- Human Based Social Engineering (Quid Pro Quo)
  - *Impersonating an employee or valid user*
  - *Posing as an important person*
  - *Using a third person*
  - *Calling as a Technical support personnel*
  - *Shoulder surfing*
  - *Dumpster diving*
- Computer Based Social Engineering
  - *Fake E-mails*
  - *E-mail attachments*
  - *Pop up windows*

# Human Based Social Engineering

- It refers to person-to-person interaction to get the required/desired information

## 1. Impersonating an employee or valid user

- *Posing oneself as an employee of same organisation*
- *Let someone into the building who forgot his/her badge etc*

## 2. Posing as an important person

- *CEO or a high level manager who needs immediate assistance to gain access to the system.*

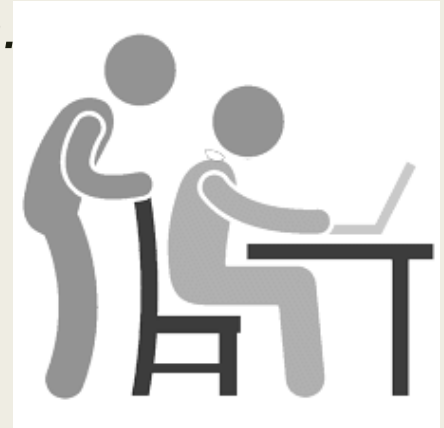
## 3. Using a third person

- *Trick works when the supposed personnel is on vacation or cannot be contacted for verification*

## 4. Calling as Technical Support

## 5. Shoulder surfing

- *It is a technique of gathering information such as usernames and passwords by watching over a person's shoulders while he/she logs into the system.*



## 6. Dumpster diving

- *It involves looking in the trash for information written on pieces of paper or computer printouts.*



# Computer Based Social Engineering

- Computer Based social engineering refers to an
- attempt made to get the required/ desired information by using computer software/ Internet.
- 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 emails to numerous users such that the user finds it as a legitimate mail. This activity is also called 'Phishing'
  - *Phishing Email:*

**From:** Microsoft office365 Team [<mailto:cyh11241@lausd.net>]  
**Sent:** Monday, September 25, 2017 1:39 PM  
**To:**  
**Subject:** Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify


[Verify Now](#)

Microsoft Security Assistant  
[Microsoft office365 Team!](#) ©2017 All Rights Reserved

# Phishing Email

**From:** Bank of America <crvdqi@comcast.net>  
**Subject:** Notification Irregular Activity  
**Date:** September 23, 2014 3:44:42 PM PDT  
**To:** Undisclosed recipients :  
**Reply-To:** crvdqi@comcast.net

---

**Bank of America** 

**Online Banking Alert**  
Would be capitalized

**Dear member:** ←

We detected unusual activity on your Bank of America debit card on **09/22/2014**.  
For your protection, please verify this activity so you can continue making debit card transactions without interruption.

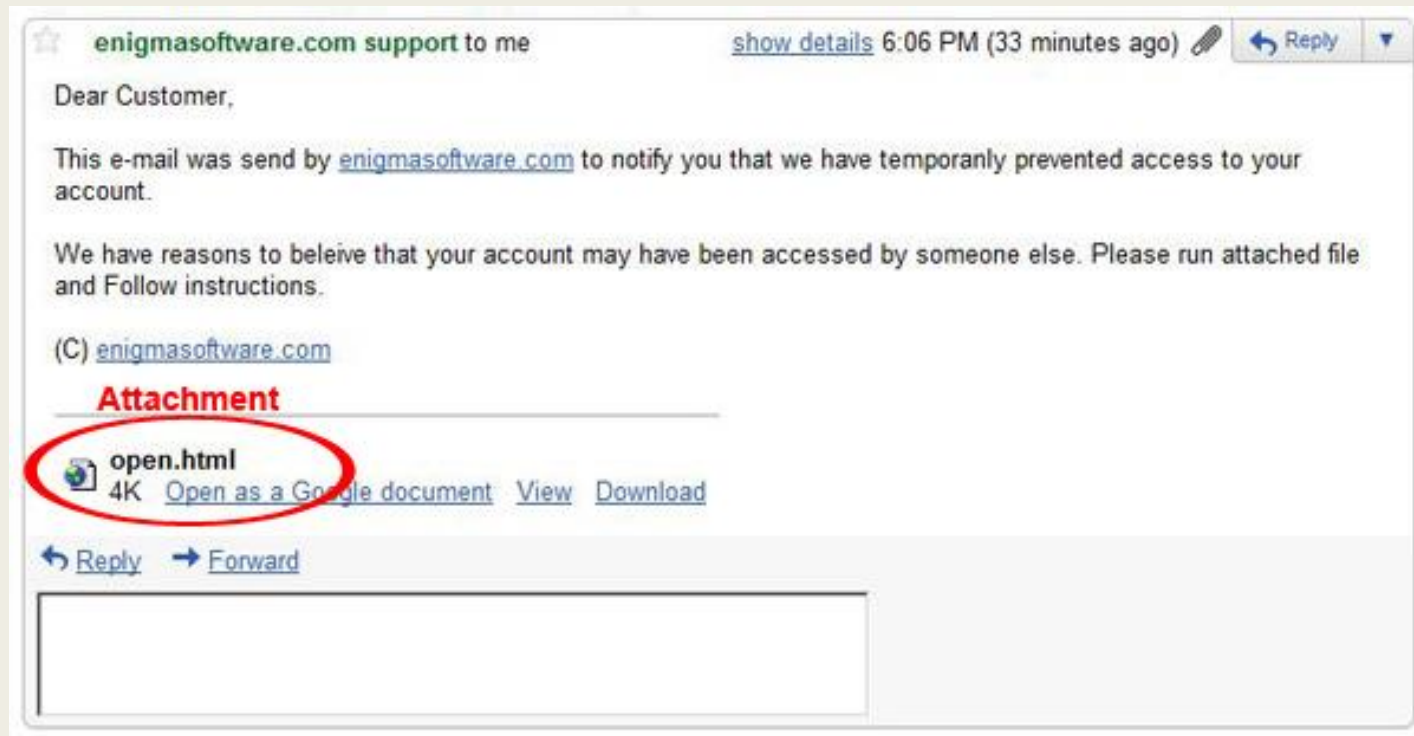
**Please sign in to** your account at <https://www.bankofamerica.com> ←  
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.  
If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error  
<http://bit.do/ghsdfhgdsd>

© 2014 Bank of America Corporation. All rights reserved.

## 2. Email attachments:

- *Used to send malicious code to a victim's system*
- *Eg: Virus, Trojans etc are used as attachments*



### 3. Pop up window

- *Pop up window with special offers or free stuff can encourage an user to unintentionally install malicious software.*



# Weakest Link?

- *No matter how strong your:*
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software
- ***You** are the **weakest link** in computer security!*
  - People are more vulnerable than computers
- *"The weakest link in the security chain is the human element" -Kevin Mitnick*



# Ways to Prevent Social Engineering

## Training

- *User Awareness*
  - User knows that **giving out certain information is bad**
- ***Military** requires Cyber Transportation to hold*
  - **Security Plus Certification**
- ***Policies***
  - Employees are **not allowed to divulge private information**
  - **Prevents employees from being socially pressured or tricked**

# Ways to Prevent Social Engineering Cont..

- *3rd Party test - **Ethical Hacker***
  - Have a third party come to your company and attempted to **hack into your network**
  - 3rd party will attempt to **glean information from employees using social engineering**
  - Helps **detect problems** **people** have with security
- ***Be suspicious** of unsolicited phone calls, visits, or email messages from individuals asking about internal information*
- ***Do not provide personal information**, information about the company(such as internal network) unless authority of person is verified*

# General Safety



- *Before transmitting personal information over the internet, check the **connection is secure** and check the **url is correct***
- *If unsure if an email message is legitimate, **contact the person or company by another means** to verify*
- *Be **aware** when interacting with anything that needs protected*
  - The smallest information could compromise what you're protecting



# Social Engineering Video

[illegible]

# Cyberstalking

- **Cyberstalking** is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization.
- It may include false accusations, defamation, slander and libel.
- It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

# Cyberstalking

- Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group.
- A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.
- Cyberstalking messages differ from ordinary spam in that a cyberstalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

# Types of Stalkers

- online Stalkers
- offline stalkers.
- Both are criminal offenses.
- Both are motivated by a desire to control, intimidate or influence a victim.
- A stalker may be an online stranger or a person whom the target knows. He may be unknown and have involvement of other people online who do not even know the target.

# How stalking works?

1. Personal information gathering about the victim.
2. Establish a contact with the victim through telephone/ cell phone. – start threatening or harassing
3. Establish a contact with the victim through E-mail.
4. Keep sending repeated E-mails asking for various kinds of favors or threaten the victim.
5. Post victim's personal information on any website related to illicit services.
6. Whosoever comes across the information, start calling the victim on the given contact details, asking for wrong services.
7. Some stalkers may subscribe/ register E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim start receiving such kind of unsolicited E-Mails

# Cybercafe and Cybercrimes



- An **Internet café** or **cybercafé** is a place which provides Internet access to the public, usually for a fee.
- According to Nielsen Survey on the profile of cybercafes users in India:
  1. 37% of the total population use cybercafes
  2. 90% of this were males in age group 15-35 years
  3. 52% graduates and post graduates
  4. > 50% were students

Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

# Role of Cybercafe

- used for either real or false terrorist communication.
- for stealing bank passwords, fraudulent withdrawal of money
  - *Keyloggers or spywares*
  - *Shoulder surfing*
- For sending obscene mails to harass people.
- They are not network service providers according to ITA2000
- They are responsible for “due diligence”



# Illegal activities observed in Cybercafes

- Pirated softwares: OS, browser, Office
- Antiviruse software not updated
- Annual Maintenance Contract(AMC): not in place
  - *Is a risk bez a cybercriminal can install Malacious code for criminal activities without any interruption*
- Pornographic websites and similar websites are not blocked
- Owners have less awareness about IT Security and IT Governance.
- IT Governance guide lines are not provided by cyber cell wing
- No periodic visits to cybercafes by Cyber cell wing( state police) or Cybercafe association

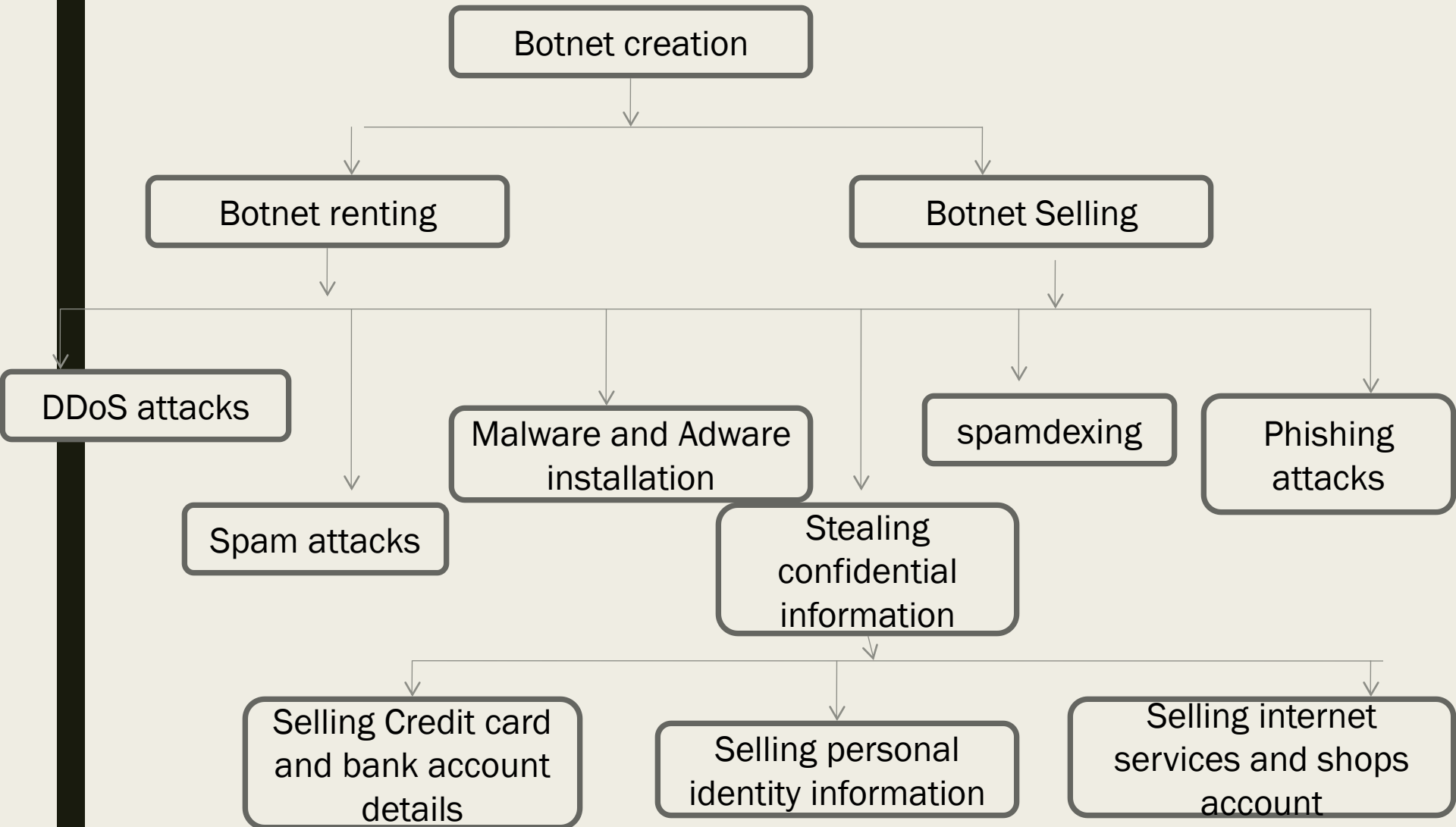
# Safety and security measures while using the computer in Cyber Cafe

1. Always Logout:  
*do not save login information through automatic login information*
2. Stay with the computer
3. Clear History and temporary files
4. Be alert:  
*don't be a victim of Shoulder surfing*
5. Avoid Online Financial Transaction
6. Change passwords
7. Virtual Keyboards
8. Security warnings

# Botnets: The fuel for Cybercrime

- Bot: “ an automated program for doing some particular task, often over a network”
- A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.
- Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.
- Most computers compromised in this way are home-based.
- According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet

# Botnet used for gainful purposes



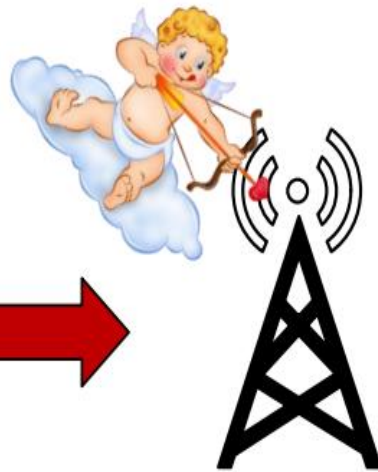
# Ways to secure the system

- Use antivirus and anti-spyware
- Install updates
- Use firewall
- Disconnect internet when not in use
- Don't trust free downloads
- Check regularly inbox and sent items
- Take immediate action if system is infected

# ATTACK VECTORS



Terminal



Access Point



Radius

# Attack vector

- An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, 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 anti-virus software can block attack vectors.
- But no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.



- If vulnerabilities are the entry points, then attack vectors are the ways attackers can launch their assaults or try to infiltrate the building.
- In the broadest sense, the purpose of the attack vectors is to implant a piece of code that makes use of a vulnerability. This code is called the ***payload***, and attack vectors vary in how a payload is implanted.
- 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.

# Different ways to launch Attack Vectors:

- Attack by E-Mail
- Attachments
- Attack by deception: social engineering/ hoaxes
- Hackers
- Heedless guests (attack by webpage)
- Attack of the worms
- Malicious macros
- Foistware/ sneakware
- viruses

# Attack Vector

- An attack vector is a path or means by which an attacker can gain access to a computer or to network server to deliver a payload. ( malicious code )
- Attacker vector include virus , E-mail attachment, web page, pop up window, instant message , chat room .
- To some extend , attack vector can be blocked using firewalls and antivirus.
- List of attack vector
  1. Attack by email.
  2. Attachment.
  - 3.Attack by deception (Social Engineering)
  4. Hackers
  5. Heedless guest (attack by webpage ) : attacker make fake website to extract personal information , such website look genuine .

# Attack Vector

## 6. Attack of the worms.

Many worms are delivered as E mail attachment.

## 7. Malicious macros : MS word and MS excel. (malicious macro is a macro virus that replaces normal macros with a virus)

## 8. Foistware : Foistware is the software that adds hidden components to the system on the sly (smartly or clever). It is bundle with attractive software.



# Attack Vector

## 9. Virus

- *A virus is a type of malicious software that when, executed, replicates itself by modifying other computer programs and inserting its own code.*

# Cloud Computing

- Cloud computing is a practice of using a network of remote servers hosted on the Internet to store, manage and process data, rather than at local server or a personal computer.
- It doesn't store any data on the HD of the computer

# Types of clouds

- There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.
- 1. Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
- 2. Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.
- 3. Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
- 4. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

# Top Cloud computing service providers:

1. Amazon web services
2. Kamatera
3. Digital ocean
4. Rackspace
5. MassiveGrid
6. Alibabacloud
7. Liquidweb
8. Microsoft Azure
9. Google Cloud platform
10. Vmware
11. Salesforce
12. Oracle cloud
13. Dell Cloud
14. Verizon Cloud
15. IBM Cloud
16. Open Nebula
17. Navisite
18. Pivotal
19. Cloudsigma
20. Limestone
21. Quadranet



# Advantage of Cloud computing.

1. Application and data can be access from anywhere at any time.
2. Data not held on a HD on user's computer.
3. Hardware cost comes down. But one would need internet connection.
4. Organization do not have to buy set of software / software licenses for every employee.
5. Organization do not have to rent a physical space to store servers and databases.
6. Organization can save money on IT support.

# Difference between Cloud service and Traditional hosting:

1. It is sold on demand- typically by the minute or hour.
2. It is elastic in terms of usage – an user can have as much as or as little as his need of service
3. The service is fully managed by the provider – a user just needs PC and internet connection.

# Types of Service

1. Infrastructure-as-a-service(IaaS) – provides virtual servers.
2. Platform-as-a-service(PaaS) – provides s/w development tools to develop new apps. Eg: Google apps
3. Software-as-a-service(SaaS) – Customer can directly only use the applications. Eg: Twitter, Gmail

# Best examples of Cloud

C	1	Pinterest	
	2	Spotify	
	3	Netflix	
	4	Siri, Alexa, Google Assistant	Cloud based NL intelligent bots
	5	Skype, Whatsapp	Cloud infrastructure
	6	Salesforce, Hubspot, Marketo	Business management app
	7	Dropbox, Google drive, Amazon S3	Cloud backup solution
	8	Amazon Lumberyard	Mobile Game Development Tool
	9	Loadstorm, Blazemeter	Testing tools
	10	Hadoop, Cassandra, HPC	Open source big data tools
	11	Facebook, LinkedIn, My space, Twitter	Social Networking

# Cyber crime and Cloud Computing

- Prime area of risk – protection of user data
- The risks are as follows
  - *Elevated user access*
  - *Regulatory compliance*
  - *Location of data*
  - *Segregation of data*
  - *Recovery of data*
  - *Difficult to trace illegal activity – customers logging in/out*
  - *Long term viability*

# Threats Associated with Cloud Computing

- Data breach
- Data ownership and control
- Data Loss
- Malicious attacks
- Insider Threat
- Shared space

# Safety measures against threats to Cloud Computing

- Backing up of data
- Understanding the cloud service provider's service agreement
- Updating backups created
- Password protection
- Two –step authentication
- Encryption and decryption
- Disciplined online behaviour
- Not storing sensitive information on cloud servers