Cyber Security

DATE

→ Cyber
→ Introduction to cyber crime
→ Cyber crime definition
→ Cyber space - Examples
→ Cyber squatting
→ Cyber punk
→ Cyber warfare
→ Cyber terrorism — Examples
→ Types of prevalent
→ What is hacking?
→ Devices most vulnerable to hacking

Cyber: Combining forms relating to IT, the internet and virtual reality (cyber fraud and cyber crime)
Introduction: Unrestricted number of free websites, the internet, has undeniably opened a new way of exploitation known as cyber crime.
→ Use of Computers
→ Use of internet
→ World wide web
Examples: Introduction of viruses to vulnerable data networks.
→ Cyber crime: Also known as computer related crime, e-crime, internet crime, hitech crime
Defination: (opposite of physical world) Coined by Willian Gibson
- Cyber space is the environment in which communication over computer network occurs and almost everything or everyone in the one way or the other is connected in it.
- Cyber crime is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

PAGE

PAGE

Your writing partner

Ukraine : Attacked Russia's data

cyber warfare.

DATE

Cyber Space : { Social media platforms eg. facebook, twitter
streaming platforms : Youtube, twitter, netflix
Cloud Services like : Google drive,
Online forums ; Online Games, Email services like Gmail,
Personal websites and blogs, Online education sites }
It describes the virtual space where people used to communicate, share files, consume media and exchange information.

Cyber Squatting :
It is the act by registering, trafficking in or using an internet domain name with the intent of profiting from the good will of a trademark belonging to someone else. (Domain name plays pivotal role in commerce and information exchange)

Laws
- Anti Cyber Squatting Consumer Protection act 1999
- The internet corporation for Assigned names and numbers
- The uniform domain — name dispute resolution policy

Cyber Squatters aim to capitalize on this traffic (network) either through ad revenues, selling counterfeit goods or phishing attempts.

Cyber Punk : Given by Bruce in 1980 → making understand with less info (desperate hackers)
Examples : Comic dialogues
Bruce combined Cyber (the science of replacing human parts with computerised or mechanised) with punk (the aggressive, counter culture, anti establishment movement, music of the late 1970s

Cyber Warfare : (Military Conflict) A series of strategies and cyber attacks against a nation / state causing it significant harm

your writing partner

PAGE

ook, twitter
flix

ces like Gmail,
i sites }
used to
d exchange

using an internet
n the good will
main name plays
change)
99
d numbers
solution policy
(network) either
or phishing

desperate
hackers)

slaving human
punk (the
nt moment,

gies and cyber
ficent harm

PAGE

DATE

This harm could include disruption of vital computer systems upto loss of life.

→ The goal of cyber warfare is to weaken, disrupt or destroy another nation by its assets including civilian infrastructure intended to degrade military capabilities or cause direct harm to the victims.

→ Cyber terrorism : (Terrorism is not done by any approved agency) It is also known as digital terrorism which gives disruptive attacks by recognised or unrecognised terrorist org. against computer systems with the intent of generating alarm, panic or the physical disruption of the information systems.
Examples : Hacking servers to disrupt, communication and steal sensitive information
② attacks on financial institutions
③ viruses to vulnerable data networks.

—Types of prevalent (common types of attacks) :
① Techno crime ② Techno vandalism (like robbery)
Techno crime : use electronic and digitally based technology to attack computer / computer network.
Techno Vandalism : unauthorised access to a computer results in damage to files or programs not so much for profit but for the challenge, intent to destroy or deface.

Hacking : Hacking is refered to misuse of devices like computers, smart phones, tablets, and network to cause damage to or corrupt systems, gather information on users, steal data and document or disrupt data related activities.
Devices most vulnerable to hacking : ① Smart devices (lucrative targets) (get some profit) ② The web cam — hackers use remote access trojan (RAT) or rootkit malware for spying on others.

your writing partner

PAGE

DATE

③ Routers ⑤

④ Email – A malware and ransomeware can be spreaded.
↓ viruses. ↓ blackmailing

⑤ Jail broken phones → it can bypass the app store and go straight to alternative app sources, they can unlock carrier settings enabling you to switch carriers.

Cyber Crime Trend (from 2008)

- Illicit financial gain
- To utilize system resources for computers
- Commercial advantage
- Foreign govt political intrest
- Personal grievances
- unstimted malicious damage
- To demonstrate attacker's skill
- To utilize system and its resources to gain unauthorized accss
- indiscriminate attack (war targets and civilians)
- tampering computer source documents obtaining licensed or digital signature certificate by mis representation or seperation of fac.
- publishing false digital signature certificate
- breach of confidentiality or privacy.

→ Cyber Crime and Information Security

* Information security in India – Cyber security means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorized users to access, use, disclose, disrupt, modification or destruction

Until something can be handled it can't be a crime.

DATE

- Lack of information security gives risk to cyber crime
- IT Act 2008 (Ammendment) → alteration or addition in law made to a constitution or legislative bill or resolution

Botnet (Robot + network)

- A botnet is a network of infected computers that work together to carry out an attacker's goal.
- Botnet is like zombie
- A network of compromised computers is called a botnet and it is called as zombie or bots.
- Among malware or malicious software botnet is the [most widespread and severe threat] several large institutions, govt organisations and also all social media websites like facebook, Twitter etc where every firm associated with the internet become the victim of the malware.

Cyber Criminals — Human / Tech

- A threat can be from insiders (within the organization) or from outsiders (outside the organization). Studies show that 80% of security incidents are coming from insiders and also cyber crime to occur in both human element and technical element.
  - Select a computer as a ~~threat~~ target : attack other computer to perform malicious activities such as spreading viruses, data theft, identity thre-ts
  - Computer as their weapon → Conventional crime : spam
  - Computers as their accessory → To save the stolen or illegal data.

your writing partner

PAGE

DATE

Technopedia : (Explaining cyber criminals)

1) Programmer - write code/program 10) Leaders → Big bosses / large orgy owner
2) Distributor - distribute (and sell stolen data to associated cyber criminals) used by cyber criminals
3) IT Expert - Engineers (Infrastructure), Encryption technologies
4) Hackers - Exploit system applications and make network vulnerable
5) Fraudsters - spam / junk - create and deploy schemes spam and phishing
6) System Host and Providers - sites and servers that passes illegal content
7) Cashiers - Provide account names to cybercriminals and control drop account (latest transaction)
8) Money Mule - manage bank account with wire transfer
9) Tellers - Transfer and launder illegal money via digital and foreign exchange methods.

Cyber Criminals Three Types :

Type I

Hungry for recognition

- Hobby hackers
- IT proffesionals → most threat
- Politically motivated hacker
- Terrorist organisations

Type II

Not interested in recognition

- financially motivated hackers
- psychologically perverts
- State sponsored hackers
- Organised criminals

Type III

Insiders

- Disgruntled or former employees seeking revenge
- Competitors using employees to gain economic advantage to damage or theft

Two types of cyber crime :

① Violent cyber crime
- Cyber terrorism.
- Cyber threat.
- Cyber stalking.
- Cyber hacking.
- Cyber warfare.
- Pornography

② Non violent cyber crime
- Cyber trespass
- Cyber Theft - botnets
- Cyber fraud
- viruses
- worms
- malware
- ransomeware

PAGE

Cybercrime against → Individual, Property, organisation, society, USENET Newsgroup

Against Individuals :
1. Email spoofing → disguised as someone else / fake senders address / forge sender address
2. Phishing, spamming, whishing
3. cyber defamation : act of harassment / harming the reputation of a person by false statement
4. cyber stalking and harassment
5. password sniffing
6. computer sabotage
7. pornographic offensives

Defamation → libel / slander
libel → written statement
slander → oral comment
Two types : file FIR ← 1. cognizable 2. non cognizable (ignored by public annoyance)

Against Property :
1. Credit card fraud
2. Intellectual property crime (IP)
3. Internet time theft → It is used by unofficial individual of the internet hours paid by an org / individual, an unauthorized access during that time

Against Organization :
1. unauthorized users of computer
2. password sniffing
3. DOS attack
4. virus attack or dissemination of viruses
5. email bombing / mail bomb.
6. logic bomb
7. Salami attack / Salami technique (Limiters, bankers, small amounts are stolen by attacker)
8. Trojan horse
9. Data diddling
10. Crimes emanating from usenet news group
11. Industrial spying / espionage
12. computer network intrusion
13. software piracy

Against Society :
1. Forgery
2. Cyber terrorism
3. Webjacking

Crimes emanating from usenet newsgroup :
1. Carry very offensive, harmful, inaccurate, inappropriate materials, cases and posting
2. usenet use group.

DATE

Stalking / harassment

libel is a defammation statement that is written, using pictures / cartoons / photographs in order to disgrace or shame a person or make an ill opinion which are not true

- Slander : oral comment

Salami attack : the practice of stealing small amount of money from large no of account over a period of time where an attack on a computer network which involves the intruder siphoning off small amounts of many from a file and placing them in another file that he/she can access later.
↳ bank account

Trojan horse : stealing and then damage (not able to access) - if removed then file is damaged.

Data diddling - data is altered as it is entered into a computer system (data entry operator / clerks) leading to forging or mis representing. eg Electricity

C&C: command and control : Making use of frequent messages / command.

DATE

Types of botnet :

1) IRC botnet : Internet Relay chat : it acts as the C&C channel The bots receive commands from a centralised IRC server, the commands is in the form of a normal chat message and the limitation of the IRC botnet is that the entire botnet can be collapsed by simply shutting down the IRC server.

ii) Peer to Peer (PtoP) botnet : It is found using the PtoP Protocols and decentralised network of nodes
Its very difficult to shutdown due to its decentralised structure and the bots frequently communicate with each other and send keep alive messages but the limitation of PtoP botnets is that it has a higher latency for data transmission . (Client and Server)

iii) Http botnet :) It is a centralised structure using http protocol to hide their activities, bots used spicific URLs or IP address or addresses to connect to the C&C server at regular intervals but unlike IRC bots, Http bots periodically visit the C&C server to get updates or new commands.

How botnets work?

1) Infection (from bot master or infected machine like bot or zombie)
2) Connection (Comand and Control Server)
3) Control
4) Multiplication (spam, infected websites, social media posts and malware distribution)

PAGE

your writing partner

DATE

Bot Nets (Robot + Network)

— Ex: Flipkart, Amazon, OLX

Bot net communication

1) At first those who want to be bot master finds the target system (Vulnerable System) use popular social engineering technique like phishing to install a small Kbs executable file into it.
2) A small patch has been included in the code making it not visible even with the running background process. A naive user wont even come to know that his/her system became part of a bot army.
3) After infection the bot looks for the channel through which it can communicate with its master
4) Bot master is used to write scripts to run an executable file on different OS.
   Win: Batch pgm Linux: Bash pgm
5) Damage/Deleting? No, only corruption.

The major things that can performed on bots:

1) Web injution: Bot master can inject snippets of code to any secure website that which bot used to visit.
2) Web filters: Here, on a use of a special symbol like ('/') and by the domain name '@' for the screen shot used by bypassing the specific domain
3) Web fakes: Redirection of the web page can be done here.
4) DNS Map: Assign any ip to any domain which the master wants to route to the bot family.

- They help to remove virus and perform Pen (Penetration) test and generally help people understand where there are vulnerab -ities and try to fix them
- Qualifications:
  - Offensive security certified professional (OSCP)
  - Certified Infrastructure tester (CIT)
  - Certified application security tester (CREST)

Black Hat:
- The Black Hat hackers are crackers are the types of people we often hear about whose trying do sell cyber services.

Grey Hat:
- They dont steal information or money nor do they help people out instead they spend most of the time just playing around the systems without doing anything harmful but try to grab the media's attention.

Green Hat:
- Babies of the hacker world (New)

Red Hat:
- Red hat hackers are the vigilants of the hacker's world (Aggressive Hackers)

Blue Hat:
- Blue hat hackers are fairly new to the hacking world but seek revenge on anyone who has made them angry. Use Tools (pre built)

your writing partner

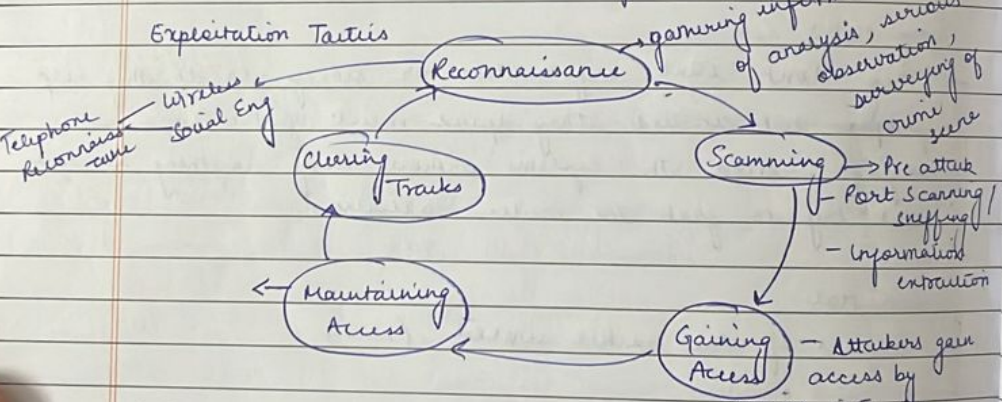
DATE

Cyber Criminals

How Criminals plan?

I Reconnaissance
II Scanning
III Gaining Access
IV Maintaining Access

(Reverse triangle of CIA, court trial)



- Attackers gain access by entering into the remote system through vulnerabilities and exploit them through least privilege, subsequently raising their privilege to administrator level and com
- promise the system using some password cracking tools

Types of Hackers:

1) White Hat :
2) Black Hat
3) Gray Hat
4) Green Hat
5) Red Hat
6) Blue Hat

- White Hat
- They are good guys in hacker's world

PAGE

or insider terms.

Password Sniffing :

- A password sniffer is a software application that scans and records password that are used or broadcasted on a computer or network interface
- It listens to all incoming and outgoing network traffic and records any instance of data / data packet that contains a password.
- Password sniffer installs on a host machine and scans all incoming and outgoing network traffic and it can applied to most network protocols HTTP, FTP, IMAP. (Internet message access protocol)

~~Types of Hackers:~~ Attack Techniques :

There are few cyber attack techniques.

1) Bots
2) Fast flux – change from system to system moving data quickly among the computers to make it difficult to trace the source of malware or phishing websites
3) Zombie Computers – One system affected, affects who network
4) DOS – ① The accessing to a website can be denied
② Flooding a network / server with traffic
5) Skimmers – Skimmers devices steal credit card info / debit card info when the card is swipped through them it is common in public devices.
6) Identity Thief –
7) Social Engineering – Social media platforms

your writing partner

All crackers are hackers

DATE

Hackers Crackers Phreakers

* Hackers :
(1) Very curious about working on any computer software
(2) They are a unit of smart programmers
(3) Have knowledge about Operating system and programming lang
(4) They can exploit and damage or steal knowledge

* Crackers : // Most tough people to handle.
(1) One who breaks into different systems with malicious intent
(2) They carry out activities like making unauthorized access, destroying necessary information, stopping services provided by the server etc.
(3) They can be easily identified because of their actions which is said to be malicious

* Phreakers (Phone + freak)
(1) They gain illegal access to the telephone system.
(2) Break into telephone and make long distance calls
(3) Attack phone systems to obtain free phone access or using the phone line to transmit viruses, access, steal or destroy data
(4) Companies systems and manipulation of data

Software Piracy: (when a software is made for a set of users but others also access the software)

- Software built to protect the privacy of its users
- unauthorized use, copying or distribution of copyrighted software including unauthorized copying of software programs purchased legitimately / legally
- Use of software that is not properly licenced including copying, modifying, distributing or selling the software in the way that offend or conflict copyright law

PAGE