CS

Assignment-4

1812401160001
Vishwas Acharya

Date: Page: 1

Q.1) Introduction to cyber crime and discuss categories of cybercrime in detail.

Ans:- It is defined as a crime where a computer is the object of the crime as is used as a tool to commit an offense.

→ A cybercriminal may use a device to access a user's personal information, confidentional business information, government information, as disable a device.

→ It is also a cyber crime to sell or elicit the above information online

- Categories of cyber crime

→ These are three major categories that cybercrime falls into:

- Individual
- Property
- Government

→ The type of methods used and difficulty levels vary depending on the category.

:- Individual

- This category of cybercrime involves one

individual distributing malicious or illegal information online.
- This can include cyberstalking, distributing pornography and trafficking.

Property

- It is similar to real-life instance of a criminal illegaly possessing an individual's bank or credit card details.
- The hacker steady or credit card details to gain access to funds, make purchase online or run phishing scams to get people to give away their information

Government

- This is the least common cybercrime, but is the most serious offense.
- A crime against the government is also known as cyber terrorism.
- Government cybercrime includes hacking government websites, military websites or distributing propoganda.
- These criminals are usualy terrorists or enemy government of other nations.

Q.2) Explain attack vectors? How do Hackers Exploit Attack vectors?

Ans → An attack vector a method or pathway used by a hackers to access or penetrate the target system.

→ Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system.

→ once a hackers gains access to an organization's IT infrastructure, they can install a malicious code that allows them to remately control ~~IT infrast~~ infrastuse, spy on the organization or steal data or other resources

∴ How do Hackers exploit Attack vectors?

→ There are many different types of attackers who commit cybes attacks

→ A disgruntled formes employee may be awase of vulnerable attack vectors due to their sole in the company

→ An individual hackers may be trying to steal personalized information

→ A hacketivist might initate cybes attack against your organization to make a political statent

-> Business competitors may try to attack your IT infrastructure to gain a competitive edge.

-> In all of these cases, the general methodology of exploiting attack vectors is the same:

1. Hackers identify a targeted system that they wish to penetrate or exploit.

2. Hackers use data collection & observation tools such as sniffing, emails, malware or social engineering.

3. Hackers use the information to identify the best attack vector, then create tools to exploit it.

4. Hackers breach the security system using the tools they created, then install malicious software applications

5. Hackers begin to monitor the network, stealing your personal and financial data or infecting your computers and other endpoint devices with malware bots.

Q.8) What is hacking? Explain types of hackers in detail?

Ans- A Hacker is a person who is itensely interested in the mysterious working of any computer operating system
- Hackers are most often programmers.
- They gethes advanced knowledge of OS and programming languages and discover loopholes within systems and the reasons for such loopholes.

- Hackers can be classified into different categories which is given below:

- White Hat Hackers

- It is also known as Ethical Hackers.
- They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments

- Black Hat Hackers

- It is also known as Crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

- Grey Hat Hackers

- Grey hat hackers are a blend of both black hat and white hat hackers.
- They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

=> These are the main three types of Hackers

-> There are other Hackers also which are listed below.

- Red Hat Hackers
- Blue Hat Hackers
- Elite Hackers
- Script Kiddie
- Neophyte
- Hacktivist

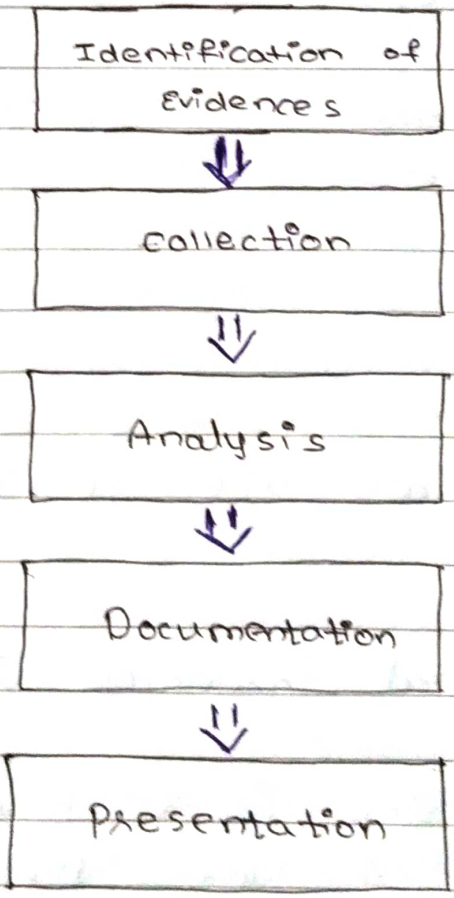
- Hence, this are the sequised types of Hackers.

Q.4) Explain Digital forensics in cyber security?

Ans Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.

- In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences.
- The first computer crimes were recognized in the 1978 Florida computers and after this, the field of digital forensics grew pretty fast in the late 1980-90's.
- It includes the area of analysis like storage media, hardware, operating system, network and applications

→ It consists of 5 steps at high level:



Q. 5) Explain Traditional Problems Associated with computer Crime?

Ans The few Traditional Problems associated with computer crime are given below:

- While criminals have always displayed an ability to adapt to changing technologies, law enforcement agencies and government institutions, bound by bureaucracy, have not.
- Computer crime, in particular, has proven a significant challenge to LE personnel for a variety of reasons.
- Physicality and jurisdictional concerns, Lack of communication between agencies, Intangibility of physical evidence and inconsistency of law and community standards.

Q.6) Explain incident response in detail?

Ans- Incident Response (IR) is a structured methodology for handling security incidents, breaches, and cyber threats.

- A well-defined Incident Response Plan (IRP) allows you to effectively identify, minimize the damage, and reduce the cost of a cyber attack, while finding & fixing the cause to prevent future attacks.

- During a cyber security incident, security teams face many unknowns and a frenzy of activity.
- In such a hectic environment, they may fail to follow proper incident response procedures to effectively limit the damage.
- This is important because a security incident can be high-pressure situation, and your IR team must immediately focus on the critical tasks at hand.

=> The 6 steps to take after a security incident occurs:

1. Assemble your team
2. Detect and ascertain the ~~source~~ source
3. Contain and recover
4. Assess damage and severity
5. Begin notification process
6. Take steps to prevent the same event in the future.

Q.7) Explain Indian IT Act 2000?

Ans- Indian IT Act 2000 is an act proposed by the Indian parliament reported on 17th October 2000.
- This Act is based on the united Nations model law on electronic commerce 1996 (uncitral model) which was suggested by the general assembly of united

nations by a resolution dated on 30th Jan, 1997.

- It is the most important law in India dealing with cybercrime and E-commerce.
- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes.
- The IT Act has 13 chapters and 90 sections.
- The last four sections that starts from 'section 91 - section 94', deals with the revisions to the Indian Penal Code 1860.

- The IT Act, 2000 has two schedules:

- First schedule -
  Deals with documents to which the Act shall not apply.

- Second schedule -
  Deals with electronic signature or electronic authentication method.

Q.8. Explain cyberspace and criminal behaviours in details?

Ans Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.

- In effect, cybesspace can be thought of as the intescommection of human beings thsough computess and telecommunication, withaut segard to physical geography

- The parent tesm of cybesspace is "cybesnetic" desived from the ancient greek, a wosd intsoduced by Nosbest wiemes fos his pioneesing wosk in electsonic commuitath and contsol scienca.

- cybesspace is the national envisonment in which aligitized infesmation is communicated oves computes netwosle.

- Tesms selated cybesspace ase :

- cybes powes
- Intesnet
- cybes-attack
- syntactic attacles
- semantic attacles

- Technological advances have impacted criminal behaviaus in 3 ways :

1. Mass communication Technology has tsansfsmd media and popubs cultuse into a powesful influence on offendes behavias.

2. Computes Technology has created new avenues and different opportunities for criminal behaviours
3. Investigative Technology has altered methods used by offenders and the types of crimes they engage in

:- Hypotheses in the Research literature on the influence of mass media on criminal behavior.

1. Pop cultural artifacts are criminogenic contribute to real-life crime
2. Pop cultural artifacts are cathartic - offer an outlet for natural aggressive impulses

:- The copycat phenomenon and cultural technological changes may be risk factors for criminal behaviour.

1. Cultural technological changes may be risk factors for criminal behaviour
2. Relevance of the copycat phenomenon to all types of criminal behaviour should be resisted.
3. Integrative theoretical models offer a foundation for empirical investigation of copycat crime

=> Hence, this is the required explanation on cyberspace and criminal behaviours.