Name:Hayden Cordeiro
BECOMPS
RollNo:05

DON BOSCO INSTITUTE OF TECHNOLOGY, MUMBAI - 400 070
Department of Computer Engg. & Info. Technology
(Academic Year ODD Semester 2021 – 2022)

Course Code and Name : ILO 7016 - Cyber Security and Laws (BE Sem VII)

ASSIGNMENT NO.: 02

Q1. Explain the difference between passive and active attack.

Active attack	Passive attack
Information is modified.	Information remains unchanged.
Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
It does not check for loopholes or vulnerabilities	It scans the ports and network in the search of loopholes and vulnerabilities
It is difficult to prevent networks from active attack.	Passive attacks can be prevented
Attacker needs to have physical control of the media or network.	Attacker merely needs to observe the communication in the media or network.
It can be easily detected.	It cannot be easily detected

Q2. What is social engineering? Explain each type of social engineering in detail.
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions. Scams based on social engineering are built around how people think and act.
Classification of Social Engineering:

- **Human Based Social Engineering:** Human based social engineering refers to person-to-person interaction to get impersonating an employee or valid user, posing as an important user, using a third person, calling technical support, dumpster diving

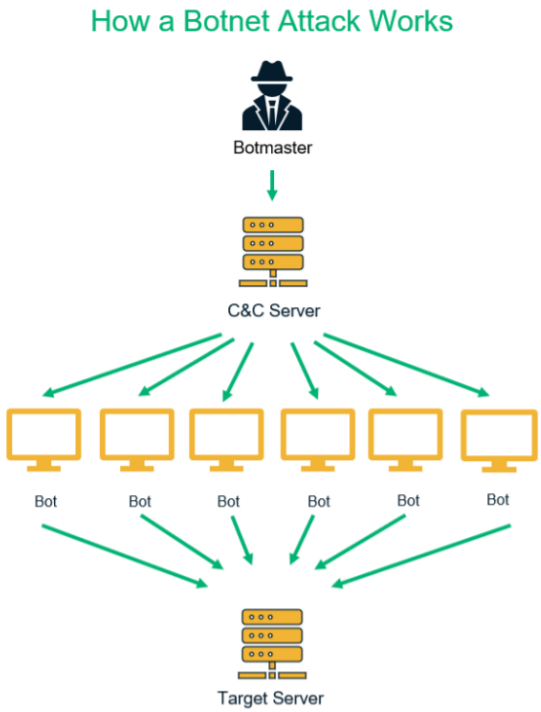
- **Computer Based Social Engineering:** Computer-based social engineering refers to an attempt made to get the required information by using computer software/internet. Fake Email ,email attachments, pop-up windows

Q3. What is cyberstalking?

- Stalking is an “act or process of following a victim silently – trying to approach somebody or something”.
- Cyberstalking has been defined as the use of information and communications technology of individuals to harass another individual.
- Cyberstalking doesn’t have to involve direct communication, and some victims may not even realize they are being stalked online.
- Perpetrators can monitor victims through various methods and use the information gathered for crimes like identity theft.
- In some cases, the line between cyberspace and real life can become blurred.
- Attackers can collect your personal data, contact your friends and attempt to harass you offline.
- Cyberstalkers often start small. Over time, the messages may become systematic, sustained and repetitive and take on an increasingly intimidating or frightening tone.

Q4. What is a botnet? How does it work? OR How do viruses get disseminated? Explain with Diagram.

- A botnet is “an automated program for doing some particular task, over a network”.
- The Term Botnet is used for the collection of software that runs autonomously and automatically.
- Botnets are exploited for various purposes, including denial-of-service attacks, creation or misuse of SMTP mail relays for spam, click fraud, and financial information such as credit card numbers.
- A botnet attack is a type of cyber attack that uses a botnet as part of its strategy



How a Botnet Works?
Phase 1: Recruiting New Hosts to Join Botnet Army
Phishing emails, Malicious websites, Vulnerability exploits.
Phase 2: Establishing Communication Between the Host Device & Bot Herder
Client-Server Network, Peer-to-Peer Botnet Network.
Phase 3: Using Botnet Malware for Cyber Attacks
Distributed Denial of Service (DDoS) Attacks, Brute Force Attacks, Data Theft, Spreading Malware, Crypto Mining, Fake Traffic

Q5. What is Attack Vector? How different attacks are launched with attack vectors.
In cybersecurity, an attack vector is a method of achieving unauthorized network access to launch a cyber attack.
Attack vectors allow cybercriminals to exploit system vulnerabilities to gain access to sensitive data, personally identifiable information (PII), and other valuable information accessible after a data breach.
An attack vector is a method of gaining unauthorized access to a network or computer system. In general, attack vectors can be split into:
Passive attack vector exploits
Passive attack vector exploits are attempts to gain access or make use of information from the system but do not affect system resources, such as typosquatting, phishing and other social engineering based attacks.
Active attack vector exploits

Active attack vector exploits are attempts to alter a system or affect its operation such as malware, exploiting unpatched vulnerabilities, email spoofing, man-in-the-middle attacks, domain hijacking and ransomware.

Common types of attack vectors

1. Compromised credentials

Usernames and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams and by malware.

2. Weak credentials

Weak passwords and reused passwords mean one data breach can result in many more.

3. Malicious insiders

Disgruntled employees can expose private information or provide information about company specific vulnerabilities.

4. Missing or poor encryption

Common encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks

5. Misconfiguration

Misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure or AWS, or using default credentials can lead to data breaches and data leaks,

6. Ransomware

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid,

7. Phishing

Phishing is a social engineering technique where the target is contacted by email, telephone or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing sensitive data, credentials or personally identifiable information (PII).

8. Vulnerabilities

New vulnerabilities are added to CVE every day and zero-day vulnerabilities are found just as often.

9. Brute force

Brute force attacks are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works.

10. Distributed Denial of Service (DDoS)

The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.

11. SQL injections

An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't.

12. Trojans

Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread by infected email attachments or fake software.

13. Cross-site scripting (XSS)

XSS attacks involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors.

14. Session hijacking

When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.
15. Man-in-the-middle attacks
Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic
16. Third and fourth-party vendors
The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your data

Q6. What is cloud computing? List and explain the type of services of cloud computing services?
The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

There are the following operations that we can do using cloud computing:

Developing new applications and services
Storage, back up, and recovery of data
Hosting blogs and websites
Delivery of software on demand
Analysis of data
Streaming videos and audios
The wide range of services offered by cloud computing companies can be categorized into three basic types:
Infrastructure as a Service (IaaS).
IaaS provides users access to raw computing resources such processing power, data storage capacity, and networking, in the context of a secure data center.
Platform as a Service (PaaS).
Geared toward software development teams, PaaS offerings provide computing and storage infrastructure and also a development platform layer, with components such as web servers, database management systems, and software development kits (SDKs) for various programming languages.
Software as a Service (SaaS).
SaaS providers offer application-level services tailored to a wide variety of business needs, such as customer relationship management (CRM), marketing automation, or business analytics.

Q7. What is cloud computing? Explain types of cloud and also list the advantages of cloud computing.
The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

There are the following operations that we can do using cloud computing:

- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios

Advantages:
1) Back-up and restore data
Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.
2) Improved collaboration
Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.
3) Excellent accessibility
Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.
4) Low maintenance cost
Cloud computing reduces both hardware and software maintenance costs for organizations.
5) Mobility
Cloud computing allows us to easily access all cloud data via mobile.
6) IServices in the pay-per-use model
Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of the service.
7) Unlimited storage capacity
Cloud offers us a huge amount of storage capacity for storing our important data such as documents, images, audio, video, etc. in one place.
8) Data security
Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

Q8. Explain cloud computing and cybercrime
Cloud Computing:
The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.
There are the following operations that we can do using cloud computing:
Developing new applications and services
Storage, back up, and recovery of data
Hosting blogs and websites
Delivery of software on demand
Analysis of data
Streaming videos and audios

The characteristics of cloud computing are given below:

1) Agility

The cloud works in a distributed computing environment. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the chances of infrastructure failure are minimum.

3) High Scalability

Cloud offers "on-demand" provisioning of resources on a large scale, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.

5) Device and Location Independence

Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

6) Maintenance

Maintenance of cloud computing applications is easier, since they do not need to be installed on each user's computer and can be accessed from different places. So, it reduces the cost also.

7) Low Cost

By using cloud computing, the cost will be reduced because to take the services of cloud computing, IT companies need not set their own infrastructure and pay-as-per usage of resources.

8) Services in the pay-per-use mode

Application Programming Interfaces (APIs) are provided to the users so that they can access services on the cloud by using these APIs and pay the charges as per the usage of services.

Cybercrime:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cybercrime

Here are some specific examples of the different types of cybercrime:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.

- Cyber Extortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyber extortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyber Espionage (where hackers access government or company data).