Date :

# B3 U4 Network-Security - II

Cyberthreats → Malicious attempt to damage or disrupt a system.
- ↳ unauthorized access
- ↳ infiltrating
- ↳ stealing

Types of cyber threats
- ↳ Unpatched software, phishing, Trojans, Worms, Advanced Persistent Threats

Cyber Attacks
- ↳ Botnets, Ransomware, DDos, Wiper Attacks, Malware, Man in the middle, IP theft

Counter Measures
- ↳ train your staff members
- ↳ fully updated system and software
- ↳ Ensure endpoint protection for remote devices
- ↳ firewall
- ↳ Always backup data
- ↳ Access management
- ↳ Enable wifi security options
- ↳ Secure Employee personal info.
- ↳ Passwords

Taxonomy of various cyber attacks

Attackers
- → Hacker
- → Hacktivist
- → Groomer
- → Intruder
- → Phisher
- ↳ Social Engineer

Targets
- → OS kernel
- → Network
- → User
- → Organisation
- ↳ Software exploits

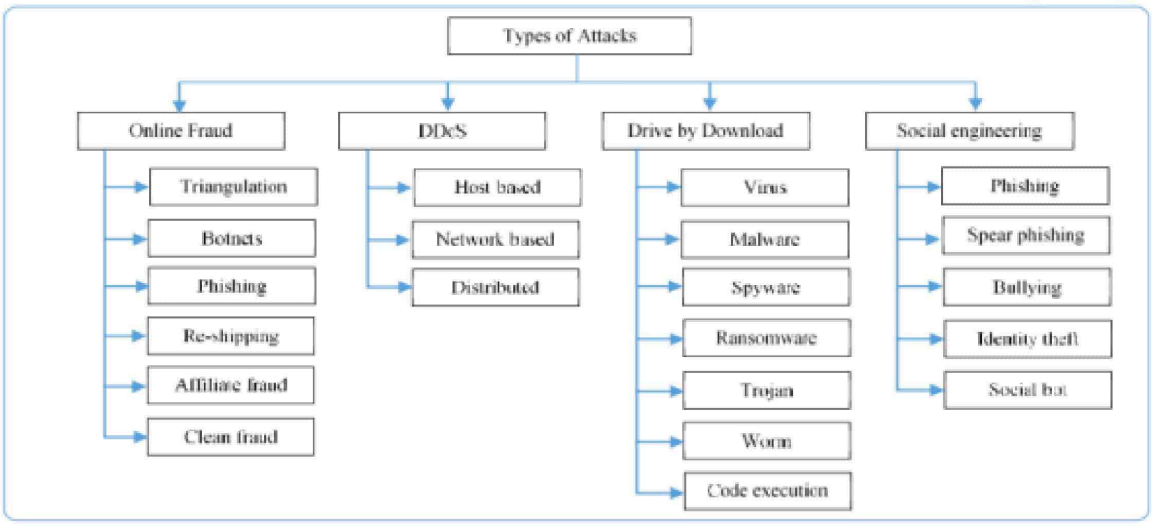



***Figure 1: Classification of Attacks***

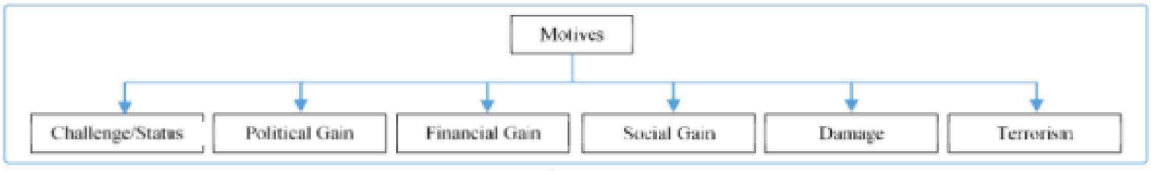



**Figure 4: Motives**

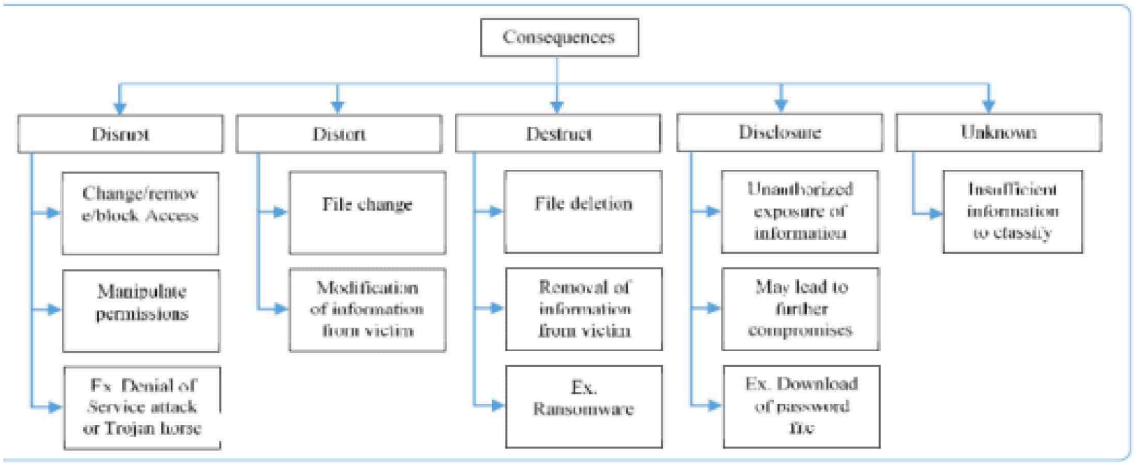



**Figure 5: Consequences**


**Figure 6: Defense Mechanism**

Date : _____

## Virus

Self-replicating, self-executable

(i) Boot sector virus → attack when we start our system
(ii) Browser Hijacker → redirections
(iii) Web Scripting virus → codes written for web pages
(iv) Resident Virus → Resides in memory
(v) polymorphic virus → many forms, hard to detect
(vi) File Infector Virus → infects files
(vii) Multipartite virus → infects program files, boot sector can lead to shut down
(viii) Macro virus → written in same macro language as software applications.

### Prevention

- Use of any trusted Antivirus
- Scan files before & after downloading
- Scan external devices before use
- Don't click on unnecessary links.

## Worm

main functionality to replicate as much as it can infect other systems. exploits the functionality of OS.

(i) Email Worms
(ii) File Sharing Worms
(iii) Crypto worms
(iv) Internet worms
(v) Instant Messaging worms

### Prevention

- Regular updating OS
- use firewalls
- use of any trusted antivirus
- Encrypt data

Date :

## Trojans

everything gets popped-up, identity theft

(i) file sharing websites
(ii) Email Attachments
(iii) Spoofed messages
(iv) Unsecured website
(v) Hacked wifi Networks

### Prevention

- secure services
- VPNs over public wifi
- Use trusted Antiviros with real time protection

## DDos

disrupt the normal traffic of a targeted server.

(i) Flooding Services

System encounters with a lot of traffic which can't be buffered in the server

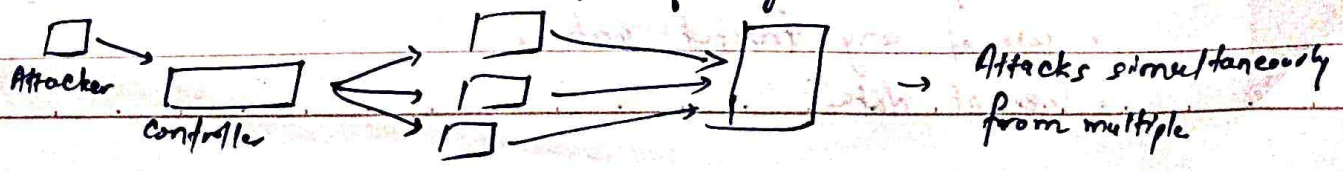
↳ Buffer overflow attacks - increas the traffic, so that buffer can't handle.

↳ ICMP flood - spoofed packets are sent, called ping of death

↳ SYN flood - continuous request made for establishing connection with server, but the handshaking never been completed from attacker side

(ii) Crashing Services

- exploits vulnerabilities to cause system/service crash
- takes advantage of bugs



Date :

## Phishing

establishing fraud comm$^n$ with users which seems to be from an authentic source

Objective :- debit/card info, login details, sensitive info.

## Malwares

once installed on victim's device opens up for breaching the cybersecurity and make devices prone to several threats. for gaining unauthorized access

Diff. malwares :- Viruses, Spyware, Ransomware, Trojan horses

## Diff. categories of malware attacks

1) Exploit kit → malicious toolkits which usually used by attackers to find out loop-holes/ vulnerabilities in victim's system/device

Once found, injects malware

2) Malicious Websites & Driven by-downloads → Malwares on websites.

3) Malvertising → attacks performed using malicious advertising

4) Man in the middle Attack (MiTM) → 3rd person comes in b/w changes info, present nearby such as wifi

5) Man in the browser Attack (MiBM) → through browsers

## Ransom

infect system, encrypts data, demands ransom.

3 steps

- give money asked by attacker & get access. Ex:- Cryptolocker, GoldenEye, Jigsaw.
- Completely remove the malware
- Restart in safe mode

Date : _____

## 2 categories of ransomware

(i) Locker ransomware :- locker, locks, can't open the system unless key provided.
- doesn't affect the files stored.

(ii) Crypto ransomware :-
- exactly opposite to locker.
- attacks on data rather than system.
- countdown for paying

## Vulnerabilities

- weakness/loop holes in system
- exploited by attackers

## Major categories of vulnerabilities

(i) Network vulnerabilities
(ii) OS vulnerabilities
(iii) Human vulnerabilities
(iv) Process vulnerabilities

## Buffer overflow

- caused by constrained resources availability in software development phases.
- where temp. space supported by any software consumed to its defined storage capacity.

### Impacts

(i) Complete system crash
(ii) Access Control
(iii) Additional security concerns

### Common bufferflow attacks

i) Stack based → attacker replaces and send the data req. by app with malicious code

Date :

(ii) heap based :- floods the memory of the program.
(iii) format input string attack :- when program takes input.

## SQL Injection

- A way to intrude into the databases
- try to gain unauthorized access and sensitive info
- simple piece of code to manipulate the database.

### Prevention

- Use a trusted web app firewall
- Use a trusted anti-virus which provides real time security.

## Browser Vulnerabilities

cookies, malwares, plugins

## OS Vulnerabilities

i) Client side vulnerabilities
attacker tries to infiltrate via diff. apps installed
ii) Server side vulnerabilities
SQL injection

Remote Desktop Connection
Remote Desktop Gateway

## Basic Computer Forensics

(i) Cross Drive Analysis :- info distribute, cross examine.
(ii) Live Analysis :- systems are on & in working condition
(iii) Analysis by recovery :- recovering deleted files, file carving
(iv) Stochastic forensics :- used in case of data theft, probability theory
(v) Stenography analysis :- A way to hide the data in image files attackers use this technique to hide pornographic pics of children

Stenography →

forensic team → gets harsh information

Date :

## Recent Cyber Attacks

i) Attack on popular SM website Fb
   ↳ April 2019 → 540 million user data exposed.
   ↳ political firms

ii) Attack on graphic design website CANVA
   ↳ 140 million user's data got exposed.

iii) Attack on servers of MGM hotel
   ↳ 10 million +
   ↳ well known business personals

iv) Attack on zoom video conferencing services
   ↳ Zoombombing during pandemic

v) Attack on WHO
   ↳ COVID, 25000 email addresses.

(vi) Ransomware attack on california university
   ↳ $1.25 million ransom paid.

## Firewalls & Intrusion detection systems (IDS)

Firewalls → • software or hardware or both.
• main obj → to provide access rights to authorized individuals whereas it denies / blocks the permission to unauthorized users.

IDS → • software or hardware or both
• installed on the network or host to detect & report intrusion attempts.

| Firewall | IDS |
|---|---|
| • can't detect security breaches for traffic that doesn't pass through it. | • fully capable of internal security by collecting info from variety of systems |
| • doesn't inspect content of permitted traffic | • keeps a check of overall network |
| • No-man power req. to manage | • Administrator req. |
| • more visible part of a network ↳ vulnerable to attacks. | • very difficult to be spotted in a network. |
| Eg. Huawei, Azure, Glanwire, CrowdSec | Eg. OSSEC, Bro, Snort, Suricata |