6/12/23

Security

- Introduction to computer Security
  Goodrich & Tamassia

Attacks vs Defense
Red vs Blue

Top 10 cyber attacks:

- **Estnia cyber attack:**

Denial of Service (DOS) → this attacks Availability

[একটা computer থেকে অনেক গুলো thread এ বিভিন্ন port দিয়ে অনেক hit করে]

TCP session : Identify → Flow identify করা।
- → Source IP
- → Sourse Port
- → Dest IP
- → Dest Port

→ Port change করে করে ~~same~~ request করা, (65535 ports)

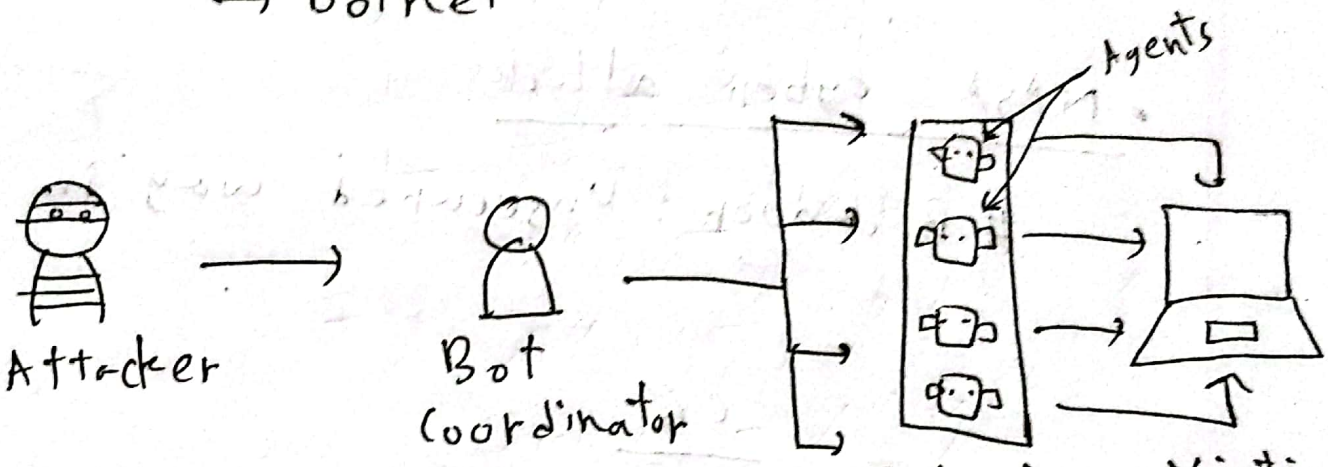
→ Active concurrent session → কতগুলো session একসাথে কাজ করতে পারে।

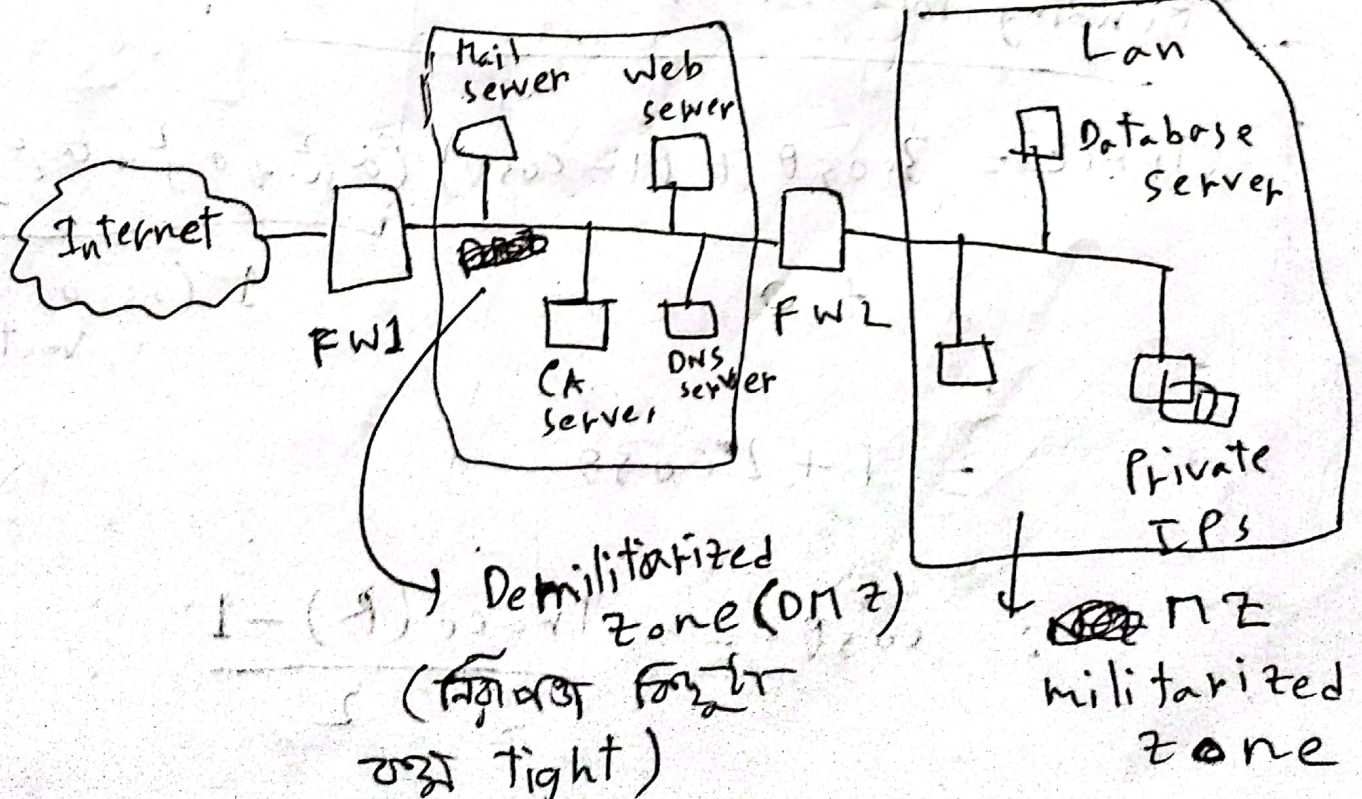
Firewall: can block all packets from an IP.

Distributed Denial of Service (DDOS)

→ IP change করতে করতে শেষ করে দেয়।

→ Botnet



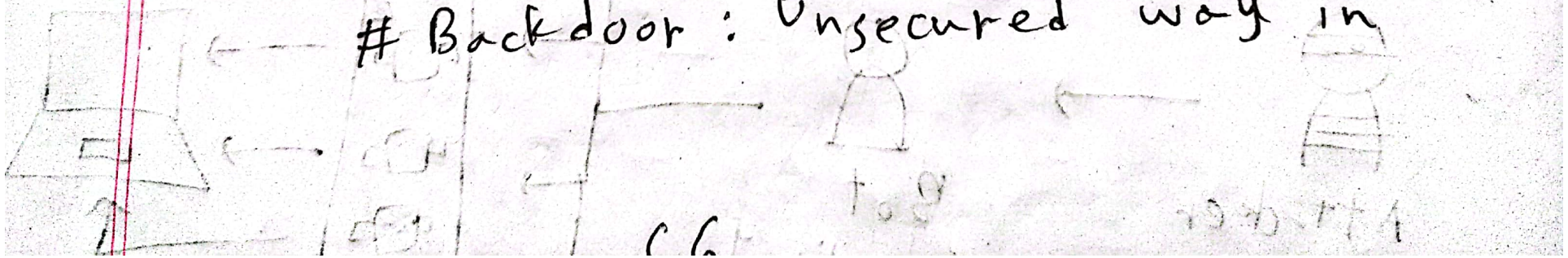


- Firewall ও inside থেকে outside ও check হয় না, outside থেকে inside ও check হয়।

- Ukraine Power grid Cyber attack

- NASA cyber attack

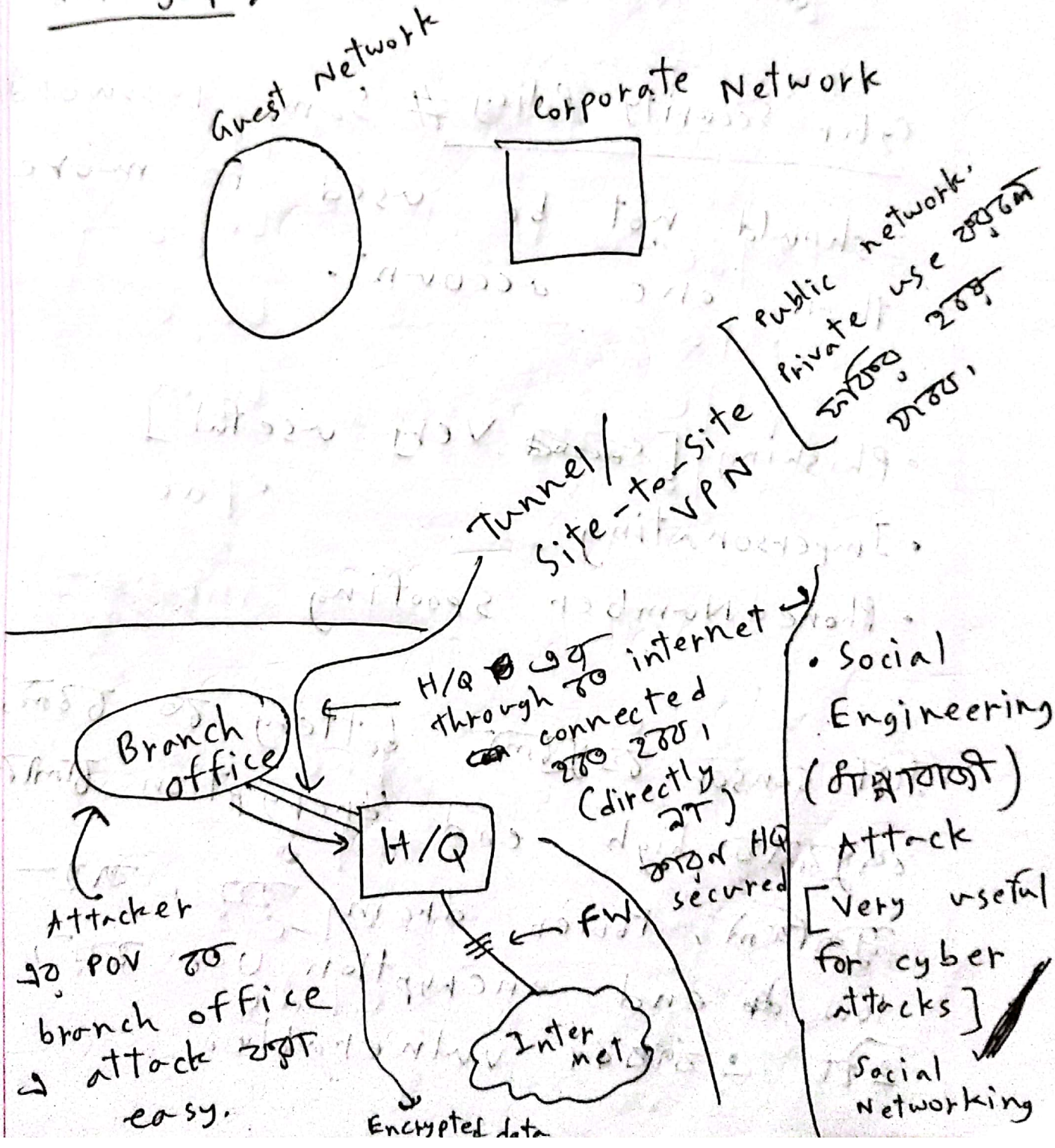
Backdoor : Unsecured way in



10/12/23

Security

- Critical infrastructure (CI) → [illegible] attack [illegible] [illegible] [illegible] [illegible], [Like Bangladesh bank, in pov of Bangladesh]
- **Air-gap:**



Attacker [illegible] pov [illegible] branch office → attack [illegible] easy.

• Stress marketing → কিছু সময়ের জন্য সময় না দিয়ে সিদ্ধান্ত বলা, (deadline ছুঁড়ে দেয়া)

Cyber Security Policy # Same password should not be used in more than one account.

• Phishing [Very useful]
• Impersonating
• Phone Number Spoofing

• IOT sensor গুলোতে battery কম থাকে, সেন্সরগুলোয় high end encryption চালালে ঝামেলা, Power drain হয়। তাই low end encryption use হয়। এটা এ কারণে vulnerable.

দুই account একজন
করলে problem.

- Maker → checker

একজন
entry
করবে

Approve
করবে

~~Bank~~ ~~check~~

[Bank এ transaction
এ use হয়]

Security

Security Goals

CIA → Confidentiality Integrity
Availability

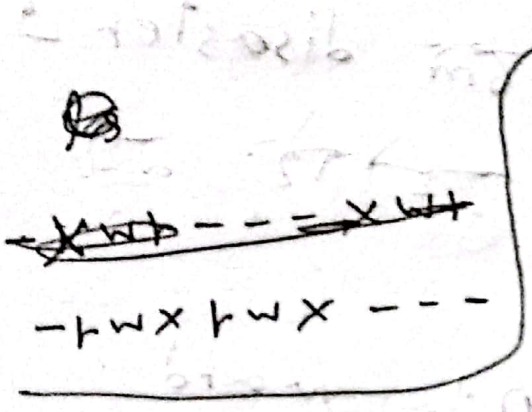
Security trade off Usability

Dos and Don'ts:

virus Os এ কু
করলে হলে যায়,
/ Privilege
এ হলে যায়, তবে
delete ও হয়ে যায় না,
Rootkit

Crypto-analysis → key ছাড়া decryption এর প্রচেষ্টা।

Tools for confidentiality → Access Control.



Authentication

you know
you have
you are

Authorization

grant select on Customer to Alice

↳ Alice customer table read করতে পারবে এবং write করতে পারবে না।

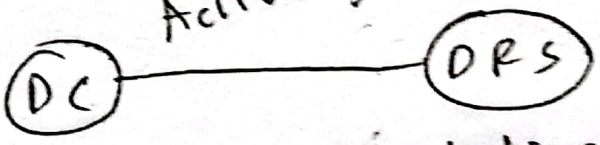
faraday cages → Electromagnetic signals cannot enter or exit the enclosure.

DC → Data Center

DRS → Disaster Recovery Site

Backup always আলাদা location এ থাকতে হয়, যাতে কোন disaster এ main আর backup দুইটাই নষ্ট না হয়।

Active guard / Data guard



Active ⟷ Active

DC down হলে DRS কাজ করতে শুরু করবে, (Hot Standby)

↓
দুই backup মধ্যে Sync থাকতে হবে!

Hot
warm
Cold

Active ⟷ Passive

↑
এই active থাকতে কিছু সময় লাগবে। (Cold standby)

• Availability বাড়ালে খরচ ও বাড়বে।

Security

13/12/23

Anonymity

Ways

- Aggregating data (sums or average)
- Mixing
- Proxies
- Pseudonyms

Attacks

Eavesdropping

{Avoid hostile countries while data communication} → Alt route, satellite link (প্রচলন মুছনা satellite এর set — Satellite constellation)

* How GPS satellite

* NTTN Nationwide Telecommunication Transmission Network

Man in the middle (MITM)

Alice --- Trudy

Trudy --- Bob

Denial of Service

Masquerading

Repudiation

Spoofing

IP-spoofing

MAC-spoofing

DNS-spoofing

DHCP-spoofing

DHCP → ~~Default~~ Default Gateway জানে
→ IP জানে
→ আরও অনেক কিছু জানে.

fail-safe → default configuration should have a conservative protection scheme

many SW has issues because → Trust (আমরা ভাবলাম এরা বন্ধুত্ব হয়েছিল) Relationship

•Complete Mediation (প্রতিটি access আসার পর কিনা আগে check হচ্ছে access দেয়া [using some policy])

America → Embassy on another country [security by obscurity can be used

America → Public n/c [cannot be used. Need open design

17/12/23

Security

- Separation of privilege
- Least Privilege
- Least Common Mechanism
- Psychological acceptability
- Work Factor

* Wanna Cry → Ransomware ***

- Compromise recording
  - → রেকর্ড: হামলা, যাতে ঘটনা ঘটলে সময় জানা যায়, চুরি হয়েছে, যে করেছে etc.
  - → যতটা আবশ্যক (Policy এর উপর depend করে)

* It audit → Team, যারা policy কিনা সেগুলো মানা হচ্ছে ~~investigate~~ inspect করে।

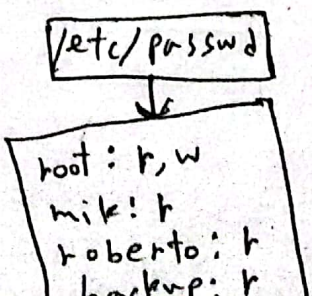
↳ Internal audit → organisation এর employee রাই audit করে।
External audit → বাইরের কোন team এসে audit করে।

- Access Control
File protection → permission manage করা যাতে অন্য কেউ কিছু করতে না পারে।

Access matrix

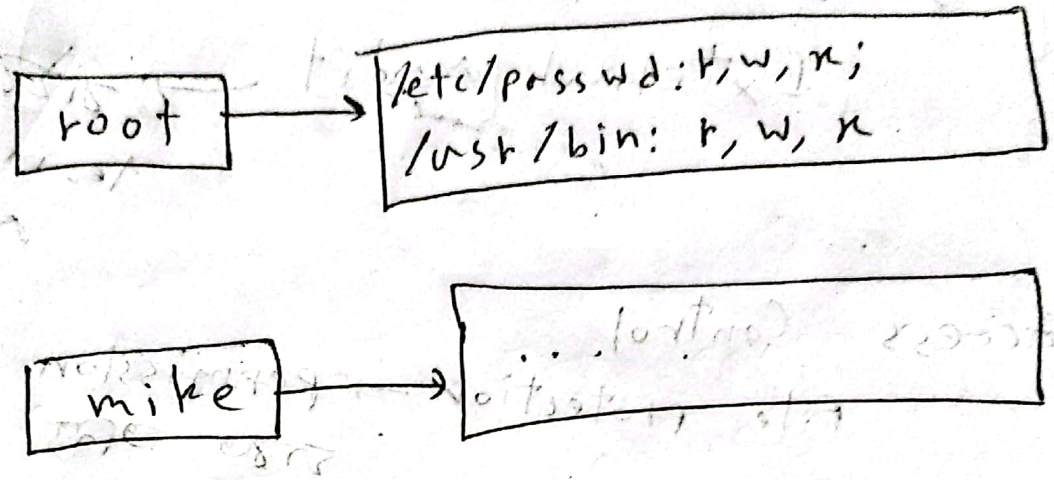
	/etc/passwd	/usr/bin/	/r/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec

* Access Control Lists

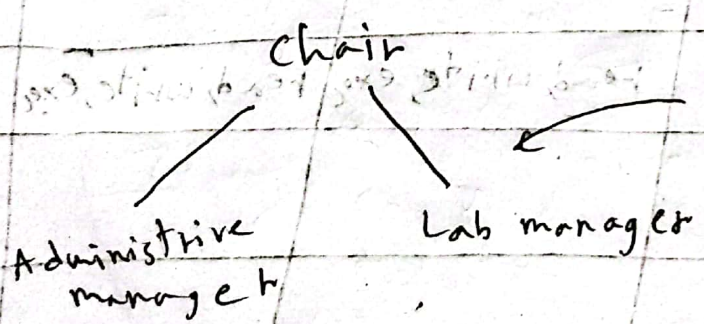


Association rule in AI

Capabilities



RAC → Role-based Access Control



Lab manager এর উপর access chair ও পাবে

এতে distrust তৈরির সম্ভাবনা একটু কম হয়ে যায়।

Security

- টাকা যখন চাইলেই তোলা হয় না,

- second এ অনেকগুলো password ~~attack~~ attempt হলে বুঝতে হবে, Password attack. (Normally minute এ 3-4 টা attempt হতে আসুক)

Password attacking tools

- John the ripper
- Hydra

- raw socket → Full Frame build করতে পারবে।

- কোনো website এ 4 password attempt/min এ exceed করলেই account lock হয়ে যায়। (আবার ২ঘণ্টা) তখন 5 min sleep করতে হয়।

[Password related problem]

Computer Forensics

- Preserving, identifying, extracting, documenting, interpreting data on a computer.

(Many steps)

• Used to obtain potential legal evidence.

Antiforensic:

→ Criminal তারা forensic বিভ্রান্ত করে, তাই তথ্য চুরি, ধ্বংস করতে তথ্য না দেয়।

• Oxygen forensics

→ Computer running থাকলে power backup দিয়ে RAM on থাকতে হবে, RAM থেকে ডাটা, দরকার extract করতে হবে।

→ Write-blocker use করে HDD থেকে data নিতে, Hash ও করতে হবে,

Forensic ⟷ Antiforensic
Armstrace

20/12/2

Security

Identification

Running → RAM copy করতে হবে,
Hard Drive copy করতে হবে,

Standby (Password লাগবে)

Mobile → 1. Seize

2. Mobile forensic kit, তিন্ন jack দিয়ে connect করে lock bypass করা যায়,
→ (অনেক সময় connector পাওয়া যায় না, (Iphone এর lock খুবই tough)

[Or অনেক সময় brute force attack দিয়ে]

3. Contacts & call-log
4. Contents দেখা
5. Browsing history / email
6. Social media
7. ROM & SD card copy নিতে হবে,

• Minimum দুইটি copy. main টা HQ তে রাখা,

এক copy নিরাপদ স্থানে সংরক্ষিত, দ্বিতীয় copy নিয়ে কাজ করতে হবে।

Analysis :

- Browsing history
- Downloads
- Documents

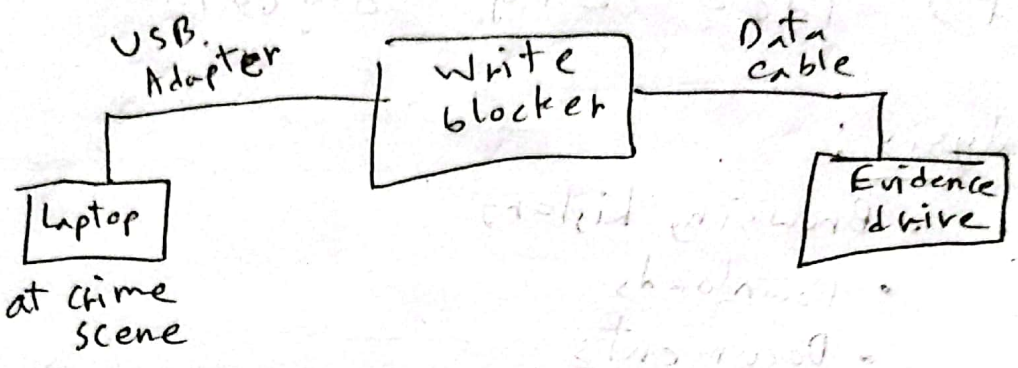
[Autopsy] [FTK imager] [Cellebrite - mobile]
open source

[Volatile → For Volatile storage]

→ Device নিয়ে image করার সময় hash calculate করতে নিশ্চয় থাকতে হবে।

Chain of Custody → যখন কাজ Custody করলি, Custody transfer এর সময়ও hash মিলানো হয়।

- Priority by Volatility



- Recovering deleted file.

  zeroize → 0 দিয়ে overrite করা,

  Defragment

Undeleted files, deleted, windows registry, print spool files, Hibernation files, Temp files, slack space, swap files, Internet browsing histories, Alternate or hidden partitions, removable media.

Temporarily save করত print এর জন্য।

FS এ block এর আকার ছোট হলে কম্পিউটার, এমনকি ছোট ফাইল FS এ রাখা যায় না।

8/1/24

Security

Steganography, Cryptography, file name/extension change, hidden tracks, deleted files.

Anti-forensic:

File-System security

- DAC (Discretionary Access Control)

Closed policy → by default no access, (white list) প্রয়োজন অনুযায়ী access দেয়া হয়।

Open policy → by-default all access, (black list) প্রয়োজন অনুযায়ী permission প্রত্যাহার হয়।

Hacker → Low privilege → Privilege escalation করে root হয়ে যায়।

Security

user	grp	others
rwx	rwx	rwx
rws	rws	[illegible]

→ এটাও হয়, হয়তো থাকে

rws → executable + set user id
[যেটা run করবো, consider হবে যেন owner run করছে]

→ নিজের password change এর জন্য

→ অন্যদের জন্য sudo লাগবে। (root এর password দিতে হয়)

sudo → gives the privilege of root

/etc/passwd → stores all password (mainly details. password থাকে shadow file এ)

[root user এর normal user হিসেবে account থাকে, তবে root privilege পাওয়ার জন্য sudo দিতে।]

rwS → set user id but not executable. (Not useful)

passwd format and shadow file format দেখানো হবে।

~~user:x:~~

Salt:

Bob → CSE-BUET
alice → CSE-BUET

Without salt
Bob: 1Hashed$
alice: 1Hashed$

same. অর্থাৎ এদের দুজনের পাসওয়ার্ডও same. Privacy breach.

salt থাকলে password এর সাথে salt add করে hashing করে। এজন্য হ্যাশ মিলবে না।