

MDM
full disk encryption
file
DLP

} data in rest

transmit : encryption in Transmit

firewall , VPN ^{SSL/TLS} protocol

etc.

attack

OSI security architecture.

7 layers.

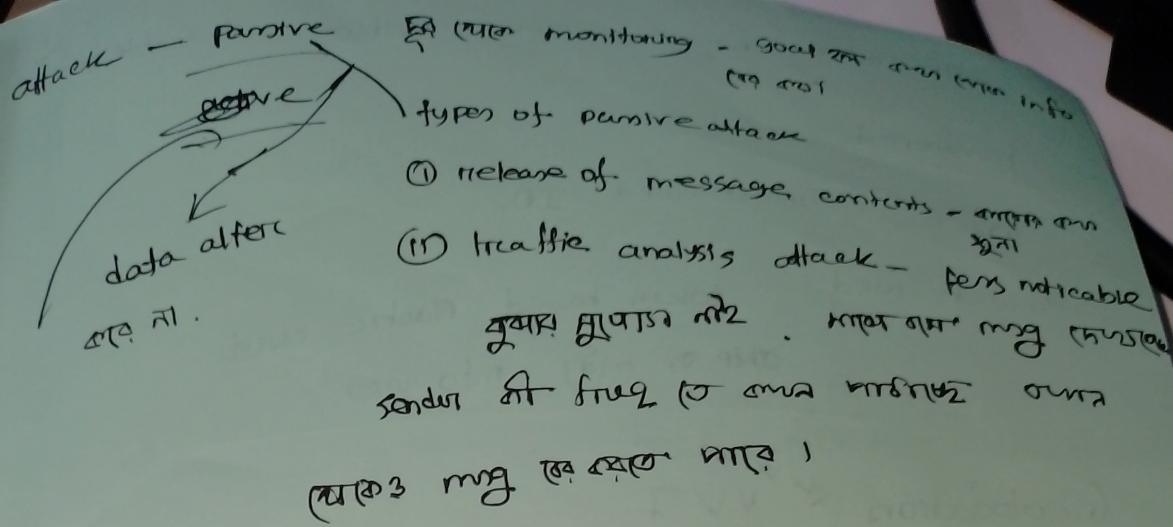
- ① Physical layer - data transmit
- ② Data link " error free (parity bit check) check
phy. & mac
- ③ Net : routing
- ④ Transport layer - TCP port & reliable transmit
ensure acc.
- ⑤ session layer - communication establish

presentation - encryption

Application - HTTP FTP ^{etc service}

Security services - counter attack,

Attack and mechanism



Active attack : false data generate ରିପୋର୍ଟ

4 types of active attack
① masquerade attack.

/ ଅଧିକାରୀ ହୁଏ କରିବାରେ ଦେଇବାରେ

କରିବାରେ ପରିବର୍ତ୍ତନ କରିବାରେ ଏବଂ ଏକ ମହିଳା ହୁଏ କରିବାରେ

ଏବଂ ଏକ ମହିଳା ହୁଏ କରିବାରେ

ଏବଂ ଏକ ମହିଳା ହୁଏ କରିବାରେ

② replay attack - typical attack

retransmit info

1

2

③ modification of msg → 3

change ଏବଂ ତାର ମ୍ୟାଗ୍

④ Denial of service → service off କରିବାରେ

authentication strong AI cent system vulnerable etc

password

Token - Smart card, ID,

Smart card - token based plastic card
chip on card info user

Geolocation ~~VVT~~ - ~~जागृति~~ country specific user

Keystroke -

Keystroke authentication - typing pattern detection

Multifactor authentication -

Mutual authentication - प्राप्तकर्ता निश्चय अपनी identity

- verify me

man in the middle and session hijacking attack

14-9-24

Hacking
cracking

Pegasus - device এর back ground এ যাতে access দেয়
- মাইট্রো-

MITRE ATTACK framework

Cyber kill chain -

ক্লেনচি malicious আমরা কোন বা

gmail , exposed . io

- grid cutter 461 hit এবং
ডায়

been pwned (website)
email pass leak 2212 form
Phish user

attack

Brut

MITRE attack framework

পদ্ধতি একটি অন্তর্ভুক্ত যাকে
attack - incident 2212 র মধ্যে algorithm

MITRE attack framework - step by step attack
free Step by step attack methodology gradually accessible

based on 4 -

- ① adversary behavior
 - ② threat model
 - ③ Techniques
 - ④ Mitigation tactics
(or paths)
- ~~18~~ 300+ technique

~~18~~ optimal

attacker perspective we can analyze 24

3x3 matrices :

① Enterprise attack

② Pre- "

geo (H) mobile "

Brute force attack

এখন মেরে এ অন্তর্বর্তীর ফাইল কেক এবং স্টেজ
এটি একটি brute force attack . জোড়া

login failure brute force attack হচ্ছে এইটি পদ

nmap tools - network mapping এর ভিত্তি

↑ ip, version, vulnerability details
হচ্ছে এইটি ক্ষেত্র

যেমন IP এর দ্রুতগতি এবং স্টেজ

Reconnaissance এর পদ

Sudo - i - ~~root~~ route এ access করে বনানো
root

Ping - machine active ফাইল কেক

net discover - install করো

apt install netdiscover.

192.168.68.137

192.168.68.255 - IP -