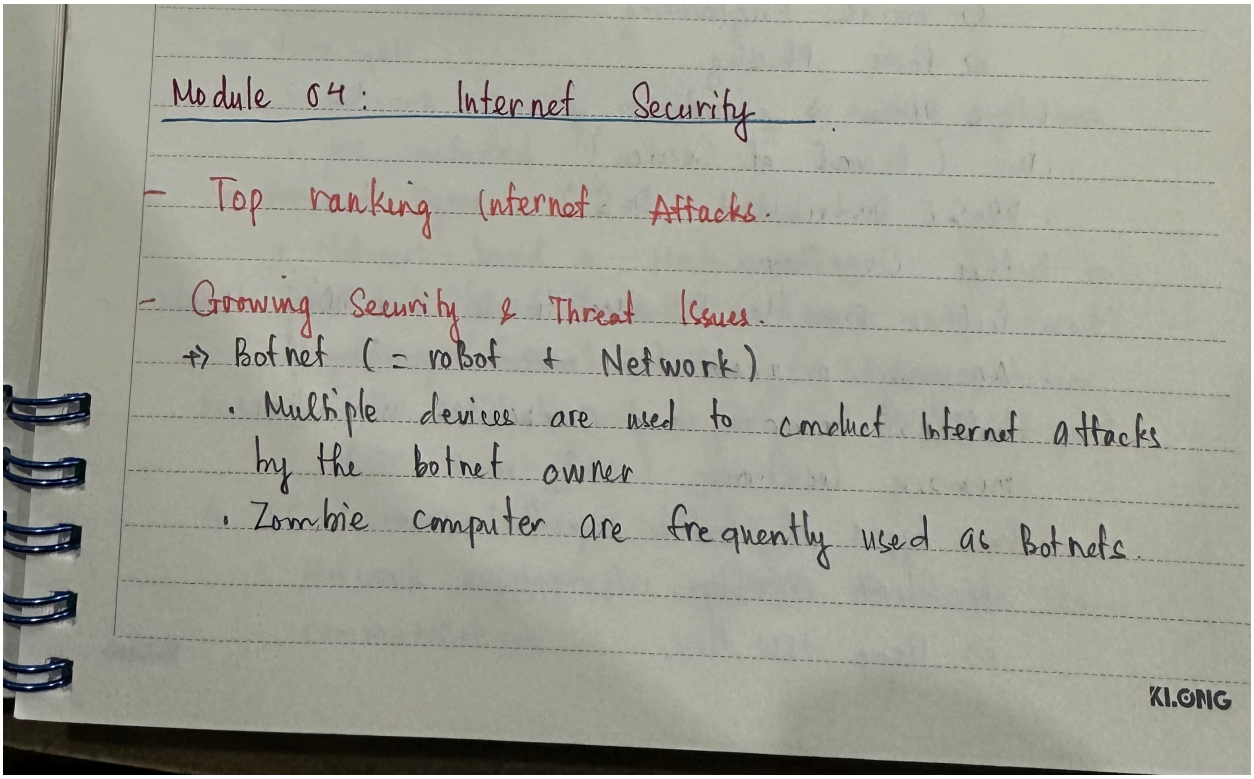
4. Internet Security

Note:



+> Zombie Computer
- Hacker compromised computer connected to the Internet
- Users are commonly unaware
+> Zero - day Vulnerability
+> Browser & Website attacks
+> Repeated attacks
+> Not Reporting breaches & Attacks

— Internet & Cyber Attacks
+> Phishing (Fishing)
- Types of Phishing
1> Spear phishing
2> Clone phishing
3> Whaling
4> Link manipulation
5> Filter Evasion
6> Website Forgery
7> Covert Redirect
8> Social Engineering
9> Phone Phishing
+> DoS & DDoS
- DoS (Denial of Service)
- DDoS (Distributed DoS)
+> Buffer Overflow
- Buffer overflow is used in DoS and DDoS attacks
- Anomaly program (malware) overrun the buffer's boundary and overwrites into adjacent memory locations
- Two types of Buffer overflow
1> Stack overflow
2> Heap over flow

↳ MITM (man-in-the-middle) Attack
- MITM attacker secretly relays and manipulates packets between communicating user/server
- MITM results in active eavesdropping and manipulation of information

↳ SQL Injection

— Internet Security & Protection.

↳ IDS (intrusion detection systems)
- Detection results are reported to the Network Administrator or SIEM system
- False alarms are removed by the alarm filters

↳ IDS System Types
- HIDS (Host IDS)
- NIDS (Network IDS)
- Signature-based IDS
- Anomaly-based IDS

↳ IPS (intrusion detection & prevention system)
- IDS + intrusion counter response system

↳ Firewall

↳ Fire wall
- Network security monitoring & control system
- IDS included

↳ Firewall Types
- Network-based vs Host-based

Network-based firewall : in (LAN, WAN, intranet) gateways (routers, switches) for network protection
Host-based firewall : in computer OS for end point (PC, smart phone) protection

↳ TLS (transport layer security)
- Network cryptographic protocol to enable secure communications

- TLS provides privacy and data integrity between networked applications.

→ WEP & WPA
- WEP (wired equivalent privacy)
  WEP includes Encryption and Authentication techniques
- WPA (wi-fi protected access)
  WPA uses TKIP that dynamically generates new encryption keys for each packet

→ SSH (secure shell)
- cryptography protocol to enable secure services over unsecured networks.
- SSH-2 is commonly supported by all servers