Class: 03 (14 Sep 2024)

Topic:

1. MITRE ATT*ACK Framework
2. Cyber kill chain

https://exposed.lol/ → Check for, is your email address on international black market?

https://haveibeenpwned.com/ → someone has been controlled or compromised

 # Enhanced Incident Detection with thread intelligent

#Miter attack

- MITRE Atta*ck → step by step procedure
- Miter attack base on: 4 step
    - Adversary
    - Threat models
    - Techniques ,300+ technique
    - Mitigating tactics → age thik kora kon path e agabo →18 technique
- Attacker er perspective e miter attack banano hoy
- Three matrix:
    - Enterpricse attack
    - Pre attack
    - Mobile attack
- One password list and one username list: brute force check user and password
- https://mitre-attack.github.io/attack-navigator/ -- scanning ip for find vulnerability
- https://attack.mitre.org/ →matrices →ICS→View on the ATT&CK® Navigator →

- sudo -i for root
- nmap use for find ip details
- nmap – help
- netdiscover –i eth0 → for find all pc which connect with eth0 net
    - nmap –sC –sV –Pn –A target-ipaddress →Scanning IP blocks
- https://web-check.as93.net/ → to find website vulnerability (best web site)
- load balancer— 100jn heat korle sobaik 10 second kore dewa,load balancer jei server idle oitak onno serverk dey
- tinyurl.com/junivgift03
- malware is a software or program
- Zero-day Exploit – recently discover vulnerability

- C2 (Command and Control)

#Need to basic for Cyber Security

- Networking
- System
    - Administration
    - Hardware
- Software development

#Job sector

- Vendors
- Banks
- Financial orgs
- Others

#Certificates

- https://www.isc2.org/certifications/cissp --> most demandable certificate in usa/Europe → odit certificate
- https://www.comptia.org/
- https://www.offsec.com/ → oscp certificate best. best from all course
- https://mile2.com/
- https://www.eccouncil.org/ ceh certification need for beginners