**Date: 14 September 2024**

**Mentor: Arabi Sir**

**Topics:**

1. MITRE ATTACK framework
2. Cyber kill chain

**Websites:**

1. exposed.lol (Check mail address if it is on international black market or not)
2. haveibeenpwned.com (for control & compromise)
3. attack.mitre.com
4. webcheck.as 93.net (to check website vulnerability) Best website.
5. eccouncil.org (CEH certification, best for beginners)
6. comptia.org(network)
7. mike2
8. isc2
9. Tryhackme (must account, practice)
10. Offsec.com (oscp certificate best from all course)

**Mitre Attack Analysis:**

Step by step attack methodology. The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective.

Attacker er perspective theke mitre attack banana hoy.

**Key Components:**

1. Adversary /attacker behavior
2. Threat models
3. Techniques (Approx 300+ techniques)
4. Mitigation tactics (Approx 18 tactics)

**Matrices:** 3 matrices

1. Enterprise attack
2. Pre attack
3. Mobile attack

**Command:**

$ sudo –i (root e jawar jonno)

$ nmap --help (shob command pawa jay)

$ ipconfig (current ip address & details pawar jonno)

$ apt install netdiscover (netdiscover install)

$ netdiscover –I eth0 (Lan er shob connected PC dekhabe)

$ nmap (target ip, eg:192.168.172.2)

$ nmap –sC (target ip) (Script run korbe)

$ nmap –sV (target ip) (Version check)

$ nmap –Pn (target ip) (Ping korbe)

$ nmap –A (target ip) (Machine er OS identification)

* load balancer— 100jn heat korle sobaik 10 second kore dewa, load balancer jei server idle oitak onno serverk dey

**Should Have Knowledge:**

1. Networking
2. System

* Administration
* Hardware

1. Software.

**Question:**

1. Login failure er reason? Ans: (T1110)
2. Malware, Phishing? Ans: Software program
3. Zero-day exploit? Ans: Recently discover vulnerability
4. C2? Ans: Command & Control.

**Job Sectors:**

1. Vendors
2. Banks
3. Financial orgs (bkash, nogod)
4. Others.