Cyber Security

Name : Zannat Hossain Tamim

Class Number : 03

Date : 14 Sep 2024

Topic:

1. MITRE ATT\*ACK Framework

2. Cyber kill chain

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

<https://haveibeenpwned.com/> à someone has been controlled or compromised

**# Enhanced Incident Detection with thread intelligent**

**#Miter attack**

· MITRE Atta\*ck à step by step procedure

· Miter atta\*ck base on: 4 step

o **Adversary** : The framework tracks their methods, such as how they gain access, move within networks, and steal data, to help organizations defend against these threats​

o **Threat models:** gaining access, exploiting vulnerabilities

o Techniques ,300+ technique

o Mitigating tactics à age thik kora kon path e agabo à18 technique

· Attacker er perspective e miter attack banano hoy

· Three matrix:

o Enterpricse attack

o Pre attack

o 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/> àmatrices àICSà[View on the ATT&CK® Navigator](https://mitre-attack.github.io/attack-navigator/) à

· sudo –i à for root

· nmap à use for find ip details

· nmap – help à find help for specific attribute

· netdiscover –i eth0 à for find all pc which connect with eth0 net

o nmap –sC –sV –Pn –A target-ipaddress àScanning IP blocks

· <https://web-check.as93.net/> à 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 à gift

· malware is a software or program

· Zero-day Exploit – recently discover vulnerability

· C2 (Command and Control)

#Need to basic for Cyber Security

· Networking

· System

o Administration

o Hardware

· Software development

#Job sector

· Vendors

· Banks

· Financial orgs à tk bsi,bank bade onno financial orgs

· Others

#certificates

· <https://www.isc2.org/certifications/cissp> --> most demandable certificate in usa/Europe à odit certificate

· <https://www.comptia.org/>

· <https://www.offsec.com/> à oscp certificate best. best from all course

· <https://mile2.com/>

· <https://www.eccouncil.org/> ceh certification need for beginners

·