14/09/24

* Mitre attack framework: based on-

1. Adversary/attacker behaviors

2. Threat models

3. Techniques (300+)

4. Mitigation tactics (18 tactics)

* Mitre attack matrices

( We can search for type of mitre attack techniques by google search)

Commands:

sudo –i (for root)

nmap (to find ip details)

nmap – help (to find help for a specific attribute)

netdiscover –i eth0 (to find all pc which connect with eth0 net)

nmap –sC –sV –Pn –A target-ipaddress (Scanning IP blocks)

* To check the weakness of any website - <https://web-check.as93.net>
* Load balancer
* If there is no dns security, web defacement is possible

\*\*\*\* tryhackme- best for beginners in cybersecurity, account must have

Acc details : [zarin.teresa10@gmail.com](mailto:zarin.teresa10@gmail.com)

Pass : same as other accounts

\*\*\*\* osint framework : osint is an interesting topic

Courses:

\*\*\*\* CompTIA courses - network+

\*\*\*\* CISSP

\*\*\*\* EC council : CEH course