Let's grade

19-8-21

Day 1: Introd^ to cyber security

"Providing security to cyber assets"

- Y CS is required?
- How to protect ourselves from cyber attacks
- Some terminology
- Various cyber attacks?

Terminologies:

→ Hacker:

White hat - find security faults & solves

black hat - misuse every → fully hacker

grey hat - partially hack

→ Exploit:

Virus ransomware & worm

→ Vulnerability

→ Threat

→ DoS - Denial of Service

→ Bruteforce - username known but not password

Various Cyber attacks

→ Malware, Phishing, password attack, DDoS

Threat map

Termux → android app

Networking & Cryptography

OSI model

65535 ports — transport layer

1024 — s/m reserved services

TCP and UDP

TCP - Conne^ oriented

UDP - Connectionless (no ack)
Live streams

TCP FTP - File transfer protocol → ftp IP (21)
TCP - SH - secure shell → ssh username@IP (22)
TCP - SMTP - Simple mail transfer protocol (25)
TCP - HTTP - website (80)
TCP - HTTPS (443)
TCP - SMB (445)
53 - TCP/UDP - DNS

Assignment:
1) Install kali linux in parrot - virtual box VMware
2) Look for basic Linux commands

Cloudflare - ports (brainc)
N/w layer - IP addr - temporary
router/access pt, Computers, mobile phones
IPV4 & IPV6 - 192.168.0.1 142.250.67.206
2^{32} IP addr in IPV4 (7billion)
NAT - N/w addr transl'
public & private in NAT
Data link layer - MAC addr - hard coded
Linux - ip a - android (Wireshark) → ip MAC addr tells device info
windows - ipconfig/all
Physical layer - bits

Cryptography
Encryption - plain text to cipher text
Description - reverse

1) Symmetric key cryptography - one key (private)
2) A - " - " - " - or public key crypt

MD5 Hash generator

Day-2

* Active & Passive Recon → "info gathering"
* Google dorking (Passive Recon) → free available

inurl:login site:tesla.com

if site:tesla.com
ii) inurl
iii) intext
iv) filetype

filetype: ppt/txt
robot.txt
capture the flag stuff

Sathvik site:linkedin.com
:- delete or don't show linked in profile

google-hacking database (GHDB)

root@kali :~# cewl -scan -t (for

* OSINT - Passive
- profil3r (dragging person)

root@kali :~# sudo apt install python3-pip
or
pip3 install profil3r
profil3r --help
profil3r -p sai sathvik
↓
select selectors
↓
select domain (Social media)
(spaces to select & enter to run)

* Website Info
# Whatweb tesla.com
* Wappalyzer → Extension (gives info of website) built on
* whois lookup → enter IP addr (who is lookup on website) visitor

4. website footprinting
- website technology
- finding IP
- whois lookup
- subdomain: tesla.com & shop.tesla.com is a subdomain

#sublist3r -d tesla.com (to find subdomains)
- finding emails

#theHarvester -- help
#theHarvester -d tesla.com
#theHarvester -d tesla.com
#if don't work

hunter.io
type tesla.com

Scanning: Scanning for vulnerabilities
- looking for files or folders in a website

#
discovered → github.com
↓
copy url & paste in terminal

#. git clone url (paste)
#. Nmap (Network mapper) : (to scan)

- Nikto
#nikto -- help
vulnerability scanners
nessus
netsparker
acunetix

bug bounty,
play live capture the flag

. digital forensics
big bounty hunting

4. Web
- website technology
- finding IP
- who is lookup
- subdomain: tesla.com → shop.tesla.com is a subdomain

#sublist3r -d tesla.com (to find subdomains)
- finding emails

#theHarvester -- help
#theHarvester -d tesla.com
; if don't work

hunter.io
type tesla.com

Scanning: scanning for vulnerabilities
- looking for files or folders in a website

#
dirsearch → github.com
↓
copy url & paste in terminal

#: git clone url(paste)
#: Nmap (Network mapper) : (to scan)
Watch Nmap

- Nikto
#nikto -- help
vulnerability scanners
nessus
net sparker
acunetix

bug bounty,
play live capture the flag

. digital forensics
bug bounty hunting

Day 3

Exploitation:

* Exploitation
  - metasploit owned by rapid 7 website
    1. Msfvenom :- tool helps in creating virus or exploits
    2. Msfconsole :- " " in communicate

arp-scan -l

copy ip addr

ping ip addr (to check online or not)

1 Msfvenom - creating exploits
(1) Bind shell : we are connecting to target
(2) Reverse shell : Target connecting us

Protectn:

1. Passwords
   pswd Manager : lastpass & bitwarden
   2FA : 2 factor authenticate
2. Antivirus

~~Comptia~~ Security +

try hackme

hack box