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

DATE

text box for password

<input type = "password" />

---

text box with excesting words

<input type = "text" value = "
Enter your name "/>

Big text box creation

<textarea>

</textarea>

it spawns a big text box you can drag and resize.

---

text area with rows and colombs

<textarea rows = "10"
cols = "30"></textarea>

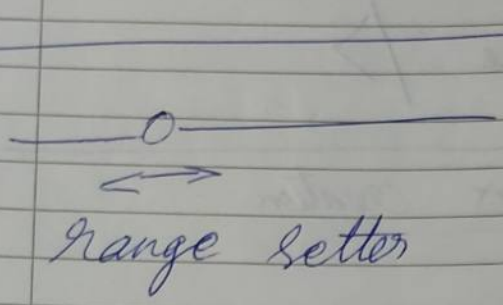
it spans a text boxes as table.

you can enter here the reading which is permanent

Input for date

<input type = "date" />

Input for email ↓ replaced with "email"



range setter ↓ replaced by range

uplode file as input ↓ replaced by "file".

input type checkbox ↓ Replaced by "Checkbox"

Radio button is same as check box

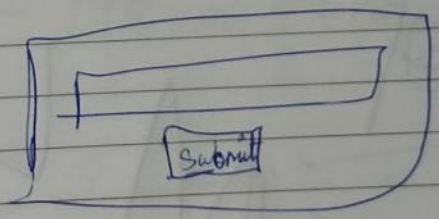
if you want to be clicked on a radio singe button then use this

<input name = "define a common name"
type = "radio" />
<input name "define a common name"
type = "radio" >

=> define a common name should be same for both radio button.

---

to create submit button



<input type = "submit" />

more input type can be searched online.

DATE

to save the inputs use form

```
<form>
<input type = "text" />
</form>
```

---

iframes. → you see a other website on you :

```
<iframe >src "http://www.google.com"></iframe>
if you cant see the web site this message will be displayed
```

→ you can resize with width etc.

End of HTML

PAGE

7:27

form

/>

website

.com/">

message

etc.

PAGE

6

OS for us

DATE

→ Arch Strike — all tools avable free
→ Pen too Linux — Best for cracking
→ network security tool kit → 125 open source tools
→ Deft linux → used by you and tools
→ Wifi Slax → Best for wireless attacks
→ Samurai web → unseen
→ Bug trap → penetration
→ Back Box → "
→ Parrort Security ~~OS~~ → highly customizable
→ Kali Linux - king

→ Fedora security → fast for Beginner
→ Blackarch - 1900 tools + 400 → fast → ~~hard~~ hard

King
kali
Linux

We Select

classmate

PAGE

Yotug 35:34.

DATE

(7) Python.

Order does matter.

You can use use GoTo in python.

eg to know the ~~place of the~~ position of alphabet in a string eg

a = "cosmo"

~~print (p.o. Index~~

~~print~~ print (phrase.Index ("c"))

it will print '0' because

0 1 2 3 4
c o s m o

If you can use a word also

you can replace the words using

a = "Crang Robbery"

Print (a. replace ("Crang", "Group"))

to convert from int to string or any

a = "55"

print (str(a) + "it is string now")

classmate

PAGE

to print the abso
absolute value
and showing the p
print (abs (
it will print 5

to print power
print (pow(
>> 16.

to print the
print (max
>> 6

to print
print (min
>> 4

classmate

DATE

to print the absolute value of any number
absolute value is nothing but removing the sign
and showing the positive value

```
print (abs (-5))
```

it will print 5

to print power of a number

```
print (pow( 4, 2)
```

>> 16.

to print the largest value of two numbers

```
print (max (4, 6))
```

>> 6

to print small value

```
print (min (4, 6))
```

>> 4

DATE

Same for round value

print (round (4.89))

>> 5

to round the value at the lowest point

print (floor (3.7))

>> 3

to round the value with ~~big~~ next high value

print (ceil (3.7)

>> 4

to find ~~Sqa~~ Squareroot

~~print~~ print (sqrt (4))

>> 2

to print the correct input

DATE

to concordinate two lists or to join two list to gether one after one to one use

a = [4, 8, 6, 7, 8]

b = [1, 2, 3, 9]

a.extend(b)

>> [4, 8, 6, 7, 8, 1, 2, 3, 9]

to add an Item in the list

a.append(10)

>> [4, 8, 6, 7, 8, 10]

to insert the value inBetween

a.append(0, 11) — Value

position

>> [11, 4, 8, 6, 7, 8, 10]

to remove a element

a.remove(11)

>> [4, 8, 6, 7, 8, 10]

DATE

to clear the list

a.clear() // this will returns an empty list

// to find the position the stored data use index

to find the repeated value of a same data use .count

a = ["asd", "apple", "can", "can", bug"]

print(a.count("can"))

>>2

to sort the list in assending alphabetical order.

print(a.sort())

>> [apple, asd, bug, can, can]

// or you can use to numbers also

classmate

PAGE

to reverse

a = [1,

a.rev

>> [4,3,2,

to create a

a2 = a.

>> [1,2

you can creat

a list or lis

Error handeling

this is used

try:

a = int(i

Print(a)

Except:

Print("

classmate

3:04:30.

DATE

to reverse the order of the list

a = [1, 2, 3, 4]

a.reverse()

>> [4, 3, 2, 1]

to create a copy of a list

a2 = a.copy()

>> [1, 2, 3, 4]

you can create a list inside a tuple or tuple inside a list or list inside list or tuple inside tuple

Error handeling

this is used when we have error eg

try:

a = int(input("enter a number"))

Print(a)

Except:

Print ["invalid input enter a number").

PAGE

classmate

output

When you input a string it does not able to convert it into integer at that line, it usualy shows error but now it will excute except:

⇒ Enter a number A to

⇒ Invalid input eata a valid number.

There are many types of exception like

10/0 - Division error

int a = "cat" value error

you can catch a particular type of error and show in different places

---

code: # this is zero division error

try:

a = 10/0 # it will catch only a division error

~~a = int (input~~

a = int (input ("enter a num"))

except:

except Z

this is an

errors to

print (" yo

output

you cant

valide erro

try: #

a = int

print

except

print

output

Enta a

enter

except:

except ZeroDivisionError:

this is an inbuilt error there are many types of errors to specify a particular type.

print ("you cant divide by zero")

Output

You cant divide by zero

Valide error

try: # it will get only the value error

a = int (input ("Enter a number"))

print (a)

except Value error:

print ("enter a valid number")

Output

Enter a number asd

enter a valid number

3:13:38

→ you can store errors in a variable

```
code:
try:
    a = 10/0
Except as err:
  print (err)
## it will print the type of #errors
output.
Division by Zero
```

---

reading files

```
# to open a file
open ("location", "r") → read
 "       "        "w" → write
 "       "        "a" → append.
 "       "        "r+" → Read and write
```

opening and clo
employe — file
employe — file

to check the
or not
e = open (
print (e. re
output
True

e = open
print (e.
e. close()
output
false

opening and closeing a file

```
employe_file = open("c:\\Built\employe.txt","r")
employe_file.close()
```

to cheack Wether the file is readable or not

```
e = open("c\\a\b.text","r")
print(e.readable())
e.close()
```

output

True

```
e = open("c\\a\b.txt""w")
print(e.readable())
e.close()
```

output

false.

DATE

to print all Data from a file
use read

```
a= open("a.txt","r")
print(a.read())
a.close()
```

---

to print a particular line

same program but read is replaced by readline() # not readlines()

```
readline()
```

write multiple ~~for~~ times to print ~~multiple~~ multiple line.

---

to print a particular line 2nd or any other position line use readlines()[ ]

```
print(a.readlines()[3])
# read lines not read line
```

3:28:19

DATE

a → append → adding additional data to the end of the file

e = open ("emp.text", "a")

e.write ("\nToby - human resource")

e.close()

you can use "W" but it will erase all data and from first it will write

google search list of modules in python

We should install more external modules.

How to Check pip

CMD

>> pip -- version

>> pip install "the required module"

eg >> pip install Py game.

PAGE

classmate

Pg 170.

Constructor

DATE

def __init__(self)

→ it is good to use Vitural Box or to use Cheap computer.

→ That point is grate because you are not damageing the real system.

→ while testing a hacking tool we could break the System

→ using ~~not~~ ~~with~~ Virtual box does not leaks the original data. we can visit unsafe web.

---

types to get access

1) network hacking → fidel ~~path~~
2) Gaining access → getaccess
3) post Exploitation → ~~use~~ what to do after
4) website hacking

classmate

PAGE

DATE

hacking

going access to the system which you should not have access to

types.

Kali Details

→ you have multiple work space.

→ Ctrl + Alt to navigate

Terminal and commands.

1) gui → might have bugs so using cmd or terminal is best.

Basics.

pwd → current directory print address

eg pwd

c// asd / c / downloads

ls → all directory in the current folder.

cd → open file

eg cd /download → opens downloads.

PAGE

classmate

DATE

to go back the main directory
type
cd ..

---

help → man
eg :
man ls // it will show usages of ls
// a how to use ls command text
// diff file will be opend.

Press Q to exit

---

to clear the screen by pressing clear.

---

press tab to make the half word. to become full.

---

ctrl + c to kill the program

PAGE

apt - get
the programs.
where apt
store to get

apt-g. apt
the programs
it
eg

apt-g
// this is to
to upgrade it.
where apt
install - s to
terminators
used here
terminator is San

classmate

DATE

apt-get update -> // is to upgrade the programme.

Where ~~apt-get~~ apt-get is the store to get program

~~apt-g~~ g. apt-get is allows us to install the programs So we can upgrade or install it

eg

apt-get install terminator

// this is to install the terminator software or to upgrade it.

where apt-get

install -> key to install

terminator -> upgraded version of terminal used here

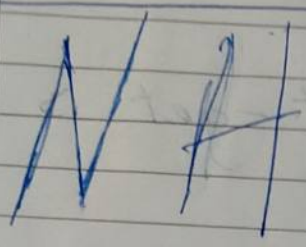
terminator is same as terminal but we

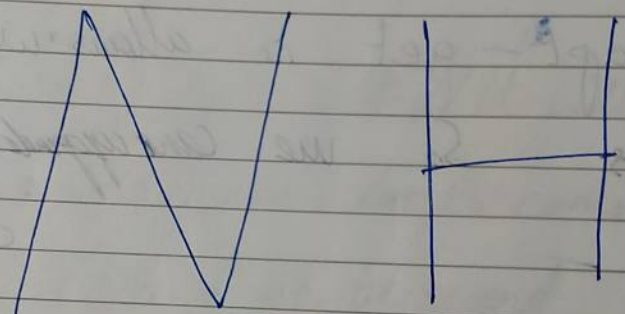
PAGE

classmate

DATE

use multiple windows and multiple





NH → Network Hacking every main computer use need in the field of hacking is in network.

PGP → Pore Grain Access Post.

SQL

SQL

Find

find

it s

desired

1) pisces - Fe
2) taurus -
3) Virgo -
4) Scorpio - O
5) Cancer -
6) Capricoan

classmate

8 9

DATE

~~Find~~

find 4 dead people → desi mard, desi aurath, firangi mard
firangi aurath FB, Insta, gmail account,
Create a ~~hotmail acc~~ 4 whats app fake acc.

A I ~~[illegible]~~ 7

its a type of coding which is desined with many conditions

---

1) pisces – Feb 20 – march 20 Koushik ~~odd even~~ even odd
2) taurus – April 21 – may 20 bapu ~~20 24~~
3) Vir Go – Aug 24 – Sep 23 Bala ~~odd even~~ 24 20
4) Scorpio – Oct 24 – November 22 bum 24 – 20.
5) cancer – june 22 – July 22 madan
6) capricoan – Dec ~~[illegible]~~ 22 – Jan 21 China

~~Dr Srinavasen Bsatrik@gmail.com~~

(10) (11) (12)

Run

1) head up not full up
2) 90° elbow
2) arms should not cross, forward movement is ga
3) hips stright dont move
4) do not bend
5) Do stretch

Rock climbing

1) find center of gravity and bring it in feet
2)

Good manners

1) eyes up
2) Smile
3) Stay Straight (sholders back)
4) hand Shake with & Web (Shake)
5) eye contact
6) full response.

classmate

PAGE

13 Cancer

Colors

yellow, pink - orange / Bluish-green

Stone

pearl, yellow Topaz and red coral

number

1, 4, 3, 7, 9

dis dd

Self-inflicted pain

---

aquarius

(14)

C++

DATE

how to define a module

Syntax

// defining it

```
#ifndef  module_name_H
#define  module_name_H

Class B
{
   function C(){}
};

// ~~calling it~~ you can define another fun. outside the ;
#include "module_name.h"

B::C()
{
}
```

// Calling the module.

```
#include <stdio.h>
#include "module_name.h"
int main()
{
module_name objectname;
return 0;
}
```

// You can use the module and functions inside it

&& - and you can use in the if, while, for, do-while etc.

|| - Or operator

DATE

C++

last left = 3:04:46

C Standard library

this contains a function called rand used for printing a random number

~~#include <cstdlib~~

#include <cstdlib.h>

// declaration of the c standard libra

~~#~~//

the program to generate a random numb

#include<iostream.h>

#include<cstdlib.h>

void main()

{ cout<< rand(); }

PAGE

a program t
a dice

#include <
#include <
int main
{ for(int
{ co
}
}

but this
Same Random
~~call~~ recalled

eg run 1

5
4
1
2
3

classmate

A program to generate a dice game

```
#include <iostream>
#include <cstdlib.h>
int main()
{  for(int x=0; x=<25; x++)
   {  cout << 1+(rand()%6) << \n(or)
                              << endl;
   }
}
```

---

but this has a disadvantage it displays same random number when it is recalled.

eg

Run 1	Run 2	Run 3
5	5	5
4	4	4
1	1	1
2	2	2
3	3	3

} Same.

DATE

sets rand function

Syntax

Srand (5); → // the number can be fill

what does this function does this

function does selects a sets

sets inside the random func

eg

set 1	set 2	set 3
1	5	8
2	2	5
5	1	2
9	5	9
3	3	
8	7	8
	6	1

header file

void main

{

for (int

for

output

set 1

1

2

6

5

3

4

classmate

~~Used~~ using Srand in the dice program

```
header files
void main ()
{
   ~~Srand (43);~~
  for (int x x=1; x<25 ; xx++)
  ~~int y~~ { Srand (xx); cout<<"set xx;
    for (int x =1 ; x<25 ; x++)
      { cout << 1+ (rand ()%6) <<\n;
      }
  }
```

output

set 1	Set 2	Set3	.... Set24
1	4	3	2
2	4	1	2
6	1	4	2
5	6	6	4
3	5	3	5
4			

Still every time we run it truely not random we can make truely random by adding time

We can access # include <time.h> this allows us to access time time() // this is the function time(0) is used to access sec dice program using time() :

header files +

#include ~~<time>~~ <ctime.h>

```
int main()
{ Srand ( time (0)) ;
for ( int x=1; x<25 ; x++):
 {
   cout << 1 + (rand()% 6) <<
 }
```

DATE

now the paput is truely random

vid

3 : 13 : 00.

How to have multiple ~~type~~ data type once in C++

Syntax

header files

template < class name of your data type >

Eg

header file

template < class memo >

void main ()

{ memo a ; // initialization

} // this can be used as anything

classmate memo takes place at int, float, double etc...

PAGE

eg

header files
template <class first, class second>
first Smaller (first a, second b)
// this can be used for functions also
{ return (a < b ? a : b); }

int main()
{ int x = 89;
double y = 5.6;
cout << Smaller (x, y) <<
endl;
}

7:29:00

Exception hand
(error hand
Syntax
try { }
catch (in
{ messag

eg
int main()
{ try { in
in
in

catch (int
{ cout

}

classmate

PAGE

DATE

Exception handeling in C++
(error handeling)

Syntax

```
try { throw error_number (or) name. ; }
catch ( int varible)
  { message or program }.
```

eg

```
int main ()
{ try { int momAge = 50;
        int sonage = 34;
        if (sonesonage > momage)
          { throw 99;
          }
}
catch (int x)
  { cout << "son is older than mom" <<
    x;
}
```

PAGE

classmate

(15) (16)

output

Son is ~~odd~~ older than mom,

Error number 99

That Rudde

Secret name

UN-US

Bit coin :

→ crypto wallet, this is safe and the Inform~~ation~~ lies within the crypto wallet.

→ no one asks the private key, its like pin

→ may copy of transation is stored in many computer

(17) (18)

→ The balance can~~not~~

Anonymous

→ You can use

→ onion router

→ proxy

↓

Fire blasting com

→ do not re size

→ Tails or ~~Cube~~ qub~~es~~

→ American Spys

→ Tulli - ~~Coun~~

→ Europol,

→ Euard ~~for~~ Sno

→ Browsing history

→ good is there

classmate

17 18

DATE

Cons

→ The balance can be seen by every one

Anonymous.

→ You can use VPN
→ onion routers.
→ proxy

+ Blasting combo

Fire blasting combo

→ do not resize the window, you can be traced
→ Tails or ~~Cube~~ qubes.

Da WEB

→ American Spys are here
→ Tulli - ~~Cous~~ Customs,
→ Europol, Interpol
→ Euard ~~Sor~~ Snow din Speach
→ Browsing history of celebrity is available
→ good is there, there is a idea that cannot be killed

} Kal cha

classmate

PAGE

DATE

- $ Psycolob, is unable
- Crime is ~~easy~~ but we have to Stop
- → if you have gone to Dark web you cant return
- → Casino we can find more criminals
- ~~bb~~ * # ||| # * . . . | . . # #
- → ~~##~~ known link is dead dead
- → unknown is truth Drark
- → Copa kabana is a bread of animal
- → Mariyana's web, → no one has read all treasure is here
- → In the Surface web the URL gets into @IP So you can access Website
- → Same find the Surfer. So we can get
- Smoke web
- → how can you tell the word is a dark web.
- ⇒ marianas web

classmate

PAGE

(20) (21)

hackers

→ jugadu

→ Git hub, F

other websites

hackers Bujan

→ they buy

→

to learn

→ Sim Swap

→ social engineer

→ Li linux

→ Brute force

→ cloud h

→ Python

→ ~~Cross~~ CrossS

→ API

→ Click jack

classmate

9 (20) (21)

DATE

Hackers

→ jugadu

→ Git hub, Python Script is usable for hacking other websites

Hackers buying products

→ they buy used or refurbished products

⇒

to learn

→ Sim Swap

→ Social engineering

⇒ Linux

→ Brute force

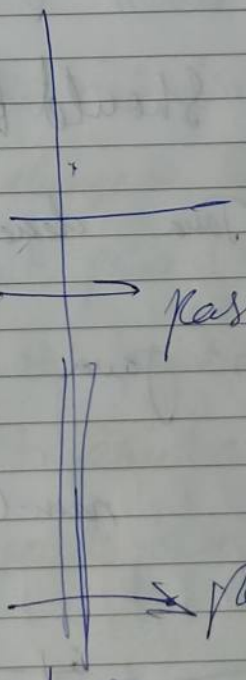
→ cloud hi

⇒ Python

→ ~~Cms~~ CMSs, word press, VPS

→ API

→ Click jacking



PAGE

classmate

22

DATE

→ Stay away from carding products
→ fishing (fake website) →
→ telegram → pass
→ PGP encryption. → pass
→ Back track
→ Freaking. → Frekers.

Java

JDK should be Downloaded

JDK – Java development kit

Function in java

return type nam() { . . .
}

~~return types → void~~

main function is main
class is mandatory

return types
→ void
// comment
// it is case
first program

~~public~~

package
public class M
· public static
// main function show
Syste
Syste
// print is use
// print ln is
}
}

classmate

PAGE

DATE

Return types

→ Void

// Comment line

// it is case Sensitive

first program to print hellow world

~~function~~

package com.package // already written

public class Main { // here main has 'M' as caps

public static void main (String [] args) {

// main function should always be Static

System.out.print ("10") ; // to print all

System.out.println ("hello world");

// print is used to print other data Structure

// print ln is used to print the lines

}

}

18:32

PAGE

classmate

22

DATE

Java was developed by James gosling in 1995 at Sun micro system

25:20

Java

Varible declaration same as in C++

=> we can print the varble like in C++

Varble data types

byte → 1 Byte [-128, 127)

Short → 2 Byte [-32K, 32000]

int → 4 Byte [-2B, 2B]

long → 8 Byts

float

double

classmate

PAGE

1) Tailor series

2) [cos u residue

Conture theorem

↓

~~Laurent~~ Conture ∫

conture intergration

Step 1 → write

2 → Subsitute z =

$\cos\theta = \frac{z^2+1}{2z}$

Subsitute this values

once Subsitute

of the ∫ and pu

1 ~~Laplace~~ ~~Sum~~

z - alpha = z -

classmate

DATE

1) Taylor Series

2) Cos u residue theorem (or)
Contour Theorem only one will be asked.

↓

Contour ∫

Contour integration

Step 1 → write the given problem

2 → Substitute $z = e^{i\theta}$, $d\theta = \frac{dz}{iz}$

$\cos\theta = \frac{z^2+1}{2z}$ $\sin\theta = \frac{z^2-1}{2zi}$

Substitute this values in the given problem once substituted remove the limit of the ∫ and put C alone

1

$z - \text{alpha} = z -$

4 problems

PAGE

classmate

in long.

ber "L"

'L'

56, 789L;

3

how to use boolean type of varble

Syntax

Varible name

boolean ~~isMale~~ = true / false ;

eg

boolean isMale = false;

byte is used normally as int.

Char are same as C++

34 : 28

hack on

- Kar ~~Qfoo~~ key containe a chip

→ Adreno is a micro computer.

classmate

PAGE

DATE

Java

Reference data types These are the data type like

→ Dates

→ Sort message

→ These types of data are stored in different modules.

eg

```
// printing the date
package com.package;

import java.util.Date;
    // We are importing a module which
// contains a class which is used to declare
// date
public class Main {
    public static void main(String[] args
```

classmate

PAGE

varible

char character.

boolean true / false

how to store a long number in long

Syntax

long varble_name = long number "L"

L = letter 'L'

eg

long views = 3_123_456_789L

how to represent a float

Same but F is used here

eg

float price = 10.99F

classmate

PAGE

how to use boolean type

Syntax

boolean ~~isEligible~~ varible name =

eg

boolean isMale = false;

byte is used normally

Char are sm

34 :

hack on

→ Car key

→ Adrenno is a micro

classmate

```
byte age = 30;
Date now = new Date();
// here Date is acting like int, float etc
// now is the varible name and new is the object
// here and Date() is the function
System.out.println(now);
}
}
```

This prints the date

output

Tue may 21 13:09:55 PDT 2019

Pointers in Java

Code:

```
package com.package;
import java.awt.*;
public class Main {
  public static void main(String[] args) {
```

DATE

~~point point~~

Point point1 = new Point(x:1);

Point point2 = point1;

// here Point acts like the datatype new point gives new point and point2 is the pointer

here Point 1 and point2 both are pointers and x:1 ⇒ x=1, y:1 ⇒ y=1

// the x and y can be accessed by point1

Point1.x = 2;

System.out.println(point2);

}

}

classmate

PAGE

output

Java.awt.point[x=2, y=1]

// in the point 2 and Point 2 the address is stored

String operations in Java

code:

```
package Com.CodeWithMosh;
public class Main {
    public static void main (String[] args) {
        String message = "hello world";
// where String is a datatype and message is
// a variable and hello word is the message
// to print the streng
        System.out.println (message);
// to concartinate
        message = "hello world" message + "!!"
        System.out.println (message);
```

DATE

```
// to check end with
message . endsWith
System.out.println(message.end
                    with ("!!"));
// to check starts with
System.out.println(message.
                    startsWith("!!"));
// to get length of the String
System.out.println(message.length());
// to get the portion of given letters in the
// String
System.out.println(message.Index
                    ("H"));
// Similarly we can replace(e, H) etc
// Similarly the we can convert to lower case and
// upper case by
// toLowerCase(), toUpperCase()
```

classmate

PAGE

```
// we can delet
// unwanted like
// converted into
// trim() ; it
// to print Doble
pac
String message
System.out.pr
// it prints he
// Similarly with
// and newline
}
}
```

array in

new is the

data type

classmate

// we can delet the space which is
// unwanted like 5 or more space can be
// converted into 1 space
// trim() ; is the function used here
// to print Doble Quotes = \"

```
String message = "Hello \"mosh\"";
System.out.println(message);
//it prints hello "mosh"
//Similarly with back Shash.
//and newline is same., tab space too....
}
}
```

---

array in the Java

new is the keyword to modify the existing data type.

// arrays in Java are same but

import java.util.Arrays;

// this package contains some array functions

// but you can create an array without

// this also this is used to print array in

// a String etc...

public class Main {

public static void main (String [] args) {

int [] numbers = new int [5];

number [0] = 1;

numbers [1] = 2;

// it can be printed one by one

System.out.println (numbers(1));

// or fully in to String.

~~Arrays.toString~~

System.out.println (Arrays.toString (numbers

}

}

classmate

PAGE

output is

2 [1, 2, 0, 0, 0]

other types of declaration of array

```
public static void main (String [] args) {

int [ ] numbers = {2, 3, 5, 1, 4};
// we can sort the array in order
// before using this function import java.
//                          util.Arrays;
//
// then
Array.Sort(numbers);
System.out.println(Arrays.toString(numbers));
}
}
```

output

[1, 2, 3, 4, 5]

DATE

// to print multi dimensional array

public static...main(){

int[][] ma = new int[2][3];

ma[0][0] = 1;

Sy.o.println(Arrays.deepToString(...

// any multidimensional array can be print...

// Other method to declar array

main(){

int[][] numbers = {{1,2,3},...

~~numbers[0][0] = 1;~~

Sys.out.println(Arrays.deepToString(numbers));

}

}

output

[[1, 2, 3], [4, 5, 6]]

classmate

PAGE

DATE

// how to declare a variable that doesn't changes its value

pi = 3.14F;

final float pi = 3.14F;

pi = 1; // This throws a error because

// final is the key word used to declare

// a variable that does not changes its value

1:03:00

Arithmetic operations are same from C++ including a++; a--;

1:13:00

//how to convert string into an integer.

PAGE

classmate

String x = "1"

int y = integer.parseint (x)+2;

System.out.println(y))

}

}

}

// here x is converted into int

Same for float, Double dt

int y = float.parseFloat (x)

int y = Double.parseDouble (x)

1:14:00

Math operations

Math functions

Sy.out.print

//output is 1

Sy.out.println

//output is 2

Sy.out.print

//output 1

Sy.out.pr

//the output

Sy.out.pri

//output

Sy.out.pr

//this prints

//output is

classmate

classmate

PAGE

Math functions ()

```
Sy. out . print ln (math. round (1.1F))
//output is 1
Sy. out . println (math. ceil (1.1F));
//output is 2
Sy. out . println (math. floor (1.1F));
//output is 1
Sy . out . println (Math . max (1,2));
//the output is 2
Sy. out . println (math. min (1,2));
//output is 1
Sy. out . println (math. random ());
//this prints a random number
//output is 0.45986016012
```

~~ttthant~~ want a 2 digit
Random number

```
1)
2)  Syst.out.println(math.
3)                  random()*100);
4)
```

output := 21.61 24

```
5)
6)  // if you want a whole number,
7)
8)  Sys:out.println(math.round(math.
9)
```

output is 21

```
10)
11) // (or)
    int result = (int)(math.random()*
13) Sy.out.println(result);
14) }
15) }
```

1:19:00 //

Switch, for, if etc are same.

input statement

```
int number = Scanner.nextInt();
```

2:00:00

2:08:00

Completed.

(25) Android edureka new playlist

7:46

18:00

→ to start a new application

→ Start a new application development

→ write application name.

→ activity is an empty frame.

→ layout is an arrangement.

↓

Buttons etc Box, B Scroll etc. ...

UI ↑

→ more like VB.

40:00

classmate

PAGE

Social

1) Victim 1 Gopi

Purpose → Basics of

First appear

2 5

after 5:

2) Victim 2 Kitty

annie, Subject →

do people believe the

Timing of

Timing of Sonia

Timing of Grea

classmate

Social engineering

1) Victum 1 Gopi ~~[redacted]~~ thambi passed
Purpose → Basics of social engineering

First official hacking Begining date
25 | Apiral | 2020
after 5:00 Pm Via Social engineering

2) Victum 2 kitty minion, featherless angle, piku, annie, subject → female purpose - Education how do people believe the strangers

Timing of Last - girl - ~~[redacted]~~ I wake up - 5:00

Timing of Sonia Jason - 7:30 - 10:00

Timing of real me - ∞.

classmate PAGE

29

DATE

Introduction to clue hunt.

1) Victim I

Objectives

→ find clue from tick tock

→ find Sister clue.

→ find family members.

→ find location

→ Social ingeneering in Insta

→ day 1 likes

→ ~~after~~ 3rd day Nourish Social talk

→ intro caly. copy information from

→ Write the account mess detail in

→ find the family in other medium of Social media and

→ pack other.

→ find answer.

→ Blocker her to be cause the Social objective Lesson ends her. and real technology hacking

→ Delete tick tock, and any other means of Social media.

victims → cousin

is Col — me

Kavitha

name → harini

gender → Doubt.

tik tok → acc

location clues

typed tree,

School →

secondary

to learn

→ Digital

Vitins → Cousin ~~or own Sister~~ insta acc name is Cal — me — champion and the karate Karathey

name → harinisekar (anukutty)

gender → Doubt.

tik tok → acct name → @ harini_karate_girl

location clues → Bamboo ~~Special~~ Special typed tree, native location is ~~coya~~ Coimbatore

School → GRG matriculation higher secondary School IV Std A sec

to learn

→ Digital foot point

~~Gmail~~ 

1) → to doo as a hacker
2) → encrypted ~~email~~ emails should be
3) → understand proton mail.
4) → use all encrypted Software and
5) → Buy a iphone.
6) → use Linux
7) → Do not have any photos.
8) → use Tor network and fuck google
9) → know to extract geo data from photo
10) → whats apps save and apple is Safe
11) → But the phone is not.
12) → delete all google account
13) → delete all microsoft and other account which contains private information
14) → create a proton mail
15) → Get anonymous gmail with different password.

classmate

DATE

→ Buy a laptop
encrypted it
→ never connect
any personal em
battery should b
any personal d
→ buy a electr
and
→ buy an mouse

classmate

should be

ftware and

h google.
data from photo
pple is Safe

d other account whi

sit with different

PAGE

DATE

. → Buy a laptop only for UR purpose and encrypted it

→ never connect that encrypted laptop to any personal emails or turn on ~~video~~ and the battery should be removable and dont put any personal items.

→ buy a electric bike for commercial purpose and

→ buy an manual petrol bike for UR.

classmate

32 33

DATE

hackers plant.

1) mal ware
2) proliferation
3) Viruses (∞ computer virus)
4) Ransom ware
5) worms (computer virus)
6) trojan horses
7) root kits
8) back door
9) evasion
10) Antimalware (Anti virus)

Deadly computer Infections

1) SQL Slammer / Sapphire ☆☆
2) Melissa Virus ☆☆
3) Anna Kournikova
4) Sircam
5) CODE Red & Code Red II ☆☆☆
6) Conficker Worm ☆☆☆
7) Blackenergy - 1, 2, 3

PAGE

7) Telebot and
7) I love you
8) So Big ☆
9) Mydoom ☆
10) ~~Stucks~~ net
11) home depot
12) Span hors
13) Distributed
14) ebay ~~play~~ p
15) OSX / RS
16) Stoam
17) Sasser
18) poison I
19) 00 mpa
20) jig saw
21) Crypto m
22) Ceiber
23) Spora
24) J

TeleBoT and Grey Energy

DATE

7) I love you ☆☆☆

8) So Big ☆☆

9) Mydoom ☆☆☆

10) ~~Stucks net attack~~ Stuxnet ☆☆☆

11) home depot credit card attack

12) Spam horse attack

13) Distributed denal service DDOS

14) ~~ebay play~~ physhing.

15) OSX/RS plug.A Trojan

16) Storm worm ☆

17) Sasser & netsky ☆

18) PoisonIvy ☆

19) OO mpa ÷ Loo mpa [aka Leap.A]

20) jig saw

21) Crypto mix

22) Cerber

23) Spora

24) Jaff
classmate

PAGE

PAGE

DATE

25) Nemucod
26) Cryasis
27) Loclay
28) Wana cry
29) Not petya
30) Donzi Buddy
31) Butter ~~fly~~ fly on Desktop
32) ~~no titags~~ motitags
33) memz virus
34) Jerusalem
35) Solar Sunrise
36) Brain
37) Explorer . Zip
38) Auto run
39) Fizzer
40) Sircam
41) magistor
42) ~~Storm~~ metropolton police virus

classmate

PAGE

34)
43) Nimda
44) Alureon
45) Klez
46) CIH
47) Blaster
48) morris.
49) Agent . btz
50) Win32 Fake
51) Zeus
52) Cryptolocker.
3) Kms, keygen
4) Botnet army
5) Anti and v
1) B.it defender.
2) AVIra
3) Avast
4) AVg
5) Kaspersky
6) Quick heal.

classmate

43) Nimda
44) Alureon (TDSS)
45) Klez
46) CIH
47) Blaster
48) Morris.
49) Agent.btz
50) Win32 Fake Sysdef.
51) Zeus
52) Cryptolocker.
53) Kms, Keygens, Crack etc. Root kits
54) Botnet army.
55) Anti and uncle US

Free	Paid
1) Bit defender.	1) Avast
2) AVIra	2) Norton
3) Avast	3) Web root.
4) AVG	4) Bit defender.
5) Kaspersky.	5) Kasper Sky
6) Quick heal.	6) AVG
	7) McAfee

To install for interpreter

To install for in ubuntu.

Search in Internet.

Virtual box.

→ the free software you can just download many os.

→ it needs bios setup.

Detail Secrets of linux (Remakes)

→ Kali linux → Debian os + Tools

→ Back Box → Ubuntu + Tools

→ parrot security os → Debian + Tools

→ DEFT linux → Standalone linux

→ Samurai web Testing framework } → X "

→ Network security Tool kit → "

→ Black Arch linux → Arch linux + Too

→ Cyborg hawk → Ubuntu linux

classmate

PAGE

→ Gnoach Trach

→ Node Zero →

Comparison of

1) parrot security o

2) Kali

3) Bto Back Box

4) other os are

Required OS

1) windows, Kube

2) Back Box or

4) parrot security

Defaults

→ Labanta Defaul

→ virtual box os

classmate

→ Gnach Track → ubUntu

→ Node Zero → Ubantu

Comparison of top hacking os

1) parrot Security os aswom

2) kali Gali

3) ~~Bto~~ Back Box. nasom

4) other os are shit

Requirred OS for hacking

1) windows, which we want to test.

2) Back Box or any linux which we want to test

4) parrot security os

Defaults

→ Lebantu Defaut OS

→ Virtual box OS

Arch linux + Tools

Ubutu

PAGE

classmate

38

CEH

DATE

1) → Command line
2) → proxy chains
3) → macchanger
4) → wireless penetrating testing
5) → Aircrack-ng

1) command line Essentials
→ leafpad is a text editor
→ Cd - Change directory - open file
→ Pwd - current working dir
→ ls - list of files
→ nano list.txt → it creates new text file called list.
→ cp - copy
→ mv - move
→ cat
→ less

→ grep
→ echo
→ touch
→ mkdir
→ chown.
→ chmod
→ rm - to remove.
→ man + help

12:00.

how to copy a file
cp filename.ext
→ rm is file location
→ rm file.txt.
→ mv is same as copy.

classmate

PAGE

classmate

ls.

- open ~~any~~ file

creates new text file called

DATE

→ grep
→ echo
→ touch
→ mk dir
→ chown.
→ chmod
→ rm - to remove. file delet
→ man + help

12:00.

how to copy a file (using) in terminal

cp filename.extension /location/

→ rm is ~~same as~~ copy used in that particular file location

→ rm file.txt.

→ mv is same as cp but it moves the file not copy.

PAGE

classmate

20:00

→ Ctal + l or clear it clear the window

→ ~~Grep~~ grep → does filter the content

eg if in help you want a particular word

usage ~~use~~ you can use it

eg

mv --help | grep v

→ echo is like print

→ touch is used to create a file

eg touch name.txt

(or) ~~multi~~ multiple files

→ touch file1 file2 file3

// it creates many files

→ mk dir // used to make directory

mk dir file name.

classmate

PAGE

32

Proxy Cha

classmate

39

→ Go back to one file
Cd.. is used here.

→ Chown is used make access able to the owner from root to all people etc.

→ Chmod is used to change the mood of the file eg Readable
Writable
Executable

→ You can force a file to be removed by
rm -f filename // command
man // manual command.

32:44

Proxy Chains.

→ proxy chains are like tor but not tor it is simply number of proxy you can enable it by

open terminal

nano/etc/proxychains.conf

you can enable the proxy by deleting the comment line

types of chains in proxy

~~Static~~

dynamic chain

→ you have to add .Socks.5 at proxy list.

→ you can get free proxy by scarching the list

Ma

→ arp -a

to see which

us

→ if config

→ mac changer

→ macchange

Tool

to change

→ macch

→ Crontab

this tool

eg while

address,

Maccchanger

→ arp -a this command is used to see which device is connected to us

→ ifconfig is same

→ macchanger --help

→ macchanger -s eth0

O - Zero
O - O Alphabet

tool → Show → to Show current and permanent mac address

To change random mac address

→ macchanger -r eth0

→ Crontab

this tool is used to Shedule the things eg while booting automatically change the mac address, open prefox etc...

PAGE

classmate

how to run the DATE

maccharger tool when the system gets reboot (restart) using crontab

→ @reboot ~~mach~~ macchanger -r eth0

Ctrl + x to exit

) before it select the editor press (2) in most case

When the crontab editor is ~~open~~ opend the editor will explain many things about crontab.

the reboot in the linux can be done in terminal by

→ reboot // command.

57:

yet to be continu

Crunch

this tool is used

word list to do br

→ you can use

→ command

- crunch m

eg crunch

57:

classmate PAGE

classmate

57:33

yet to be continued

Crunch

this tool is used to ~~install~~ create a word list to do brute force attack.

→ you can use crunch by

→ command

- crunch minimum length maximum length characters

eg crunch 3 5 abc

57:33.

Kali Linux

1) how to install man in the middle framework.

inter →

apt-get install ~~mitmf~~ mitmf

and for many uses see help of framework

2) how to install Root kit hunter on Kali linux

inter →

apt-get install Rkhunter.

→ Same

3) how to install tor and proxy chains

inter →

// for tor

apt-get install tor

// for proxy chains

leafpad (or) nano /etc/proxychains.conf

Then config as known
after saving the folder

inter →

→ Service tor Start
~~(tord)~~

~~5) Install java~~

6) To install lazy kali (first install git)

inter →

→ cd ~~Desktop~~

↳ Sudo git clone https://github.com/~~the~~ thelnin/Lazykali-and-Hackpack.git

(or)

→ Sudo git clone http://github.com/asismelach sroinas/Iscript.git

(or)

Search net.

→ cd lscript

→ Chmod +x install.sh

→ ./install.sh

to run it

• inter →

l.

7) to install Git

inter →

→ Sudo dnf install git-all

(or)

→ Sudo apt install git-all

8) to install the Screen recorder in linux

inter →

→ apt-get install recordmydesktop

no space.

8) how to install and configure free VPN
- See SSTecTutorials

9) how to install fire wall

~~inter~~

apt-get install → (agi) Ok
inter

→ agi gufw

43) adrino fun fact

→ adrino uses C program to run program

→ potentio meter is use the controle the power of the ~~electricity~~ / variable resister is used to controle the amount of electricity flow.

44) IOT

→ connet all devices and hacking is made possible

→ micro controllers are used here like Raspberry pi

→ Sensor are used they could be vunerable.

Raspberry pi uses python

eg program to ~~publish~~

import RPi.GPIO

↓

This are the pins by side

Same as arduino. But has many disadvantage and advantage.

Ethical hacking once again

1) When we open any os you should install Kali Sources.list repository
→ to install this go to kali docx
→ and click on Kali Sources.list repository
→ copy the command and paste it in the file /etc/apt/sources.list with nano mode and paste there in the documentation.
→ and then save.

→ Then update the

~~apt~~ → apt

apt install

(or)

→ use # apt

and dont

→ copy the new

→ ~~type # apt~~

→ type # apt in

version)

→ Then reboot.

→ then # apt

→ Then update the system by

~~apt~~ → apt update

apt install linux-headers-$(uname -r)

(or) if this does not work

→ use # apt install linux-headers-*
and dont continue

→ copy the new version of header and

→ ~~type # apt install linux-headers-~~

→ type # apt install linux-image-(paste the newer version)

→ Then reboot.

→ then # apt install linux-headers-$(uname -r)

DATE

→ you can simply create py thon program first you create ~~your~~ a using nano

→ to change mode use chmod command
w r x

eg chmod +x program.py

→ to make it executable ./filename.

eg ./program.py

→ Commands to try

1 Pwd
2 cd
3 ls
4 -la => ls -la
5 touch
6 rm
7 mk dir
8 clear
9 cd..

classmate

PAGE

10) whoami
11) chmod
12) cat
13) grep
14) echo
15) history
16) cp
17) mv
18) man
19) locate
20 nano
21 S
22 Shut do
23 reboot
24 PS
25 top
26 ctrl
27 uname

classm

10) who am i

11) ~~sudo~~ chmod +x

12) cat

13) grep

14) echo

15) history

16) cp

17) mv to chang name, location

18) man

19) locate

20 nano

21 ~~sudo~~ Shut down

22 Shut down -C → to cancel

23 Reboot

24 PS → process running in cir dir.

25 top → Shows all process

26 ctrl + x or +y → no command key

27 uname -a

28) man

29) uname → to show the type of os

30) man uname

31) ifconfig → linux , ipconfig → windows

32) net Stat

33) net State -nr

34) net Stat -antp

35) net Stat -ntp

36) ~~update~~ apt update

37) apt-get update

38) apt-get upgrade

39) exit

words that Should be known by us.

1) foot printing → geting the imformation a comp or the clent.

2) Scanning and enumeration → with out attacking know there data etc. OS etc.. using n map our map network.

3) System hacking → entering into the system through back door etc..., upload, like picture, Bag Stories etc.

4) malware. → program that damage your computer.

worms
Trojans
virus
} popular.

5) Sniffing → sniffing the packages

6) Social engineering → attacking the user (or) people

7) Denial of Service → crash website (or) pc.

8) SQL & XSS

9) Wifi hacking.

10) Phising, mobile hacking. apple and anroid.

11) cryptography.

12) Phising

Addition tools before the linux:

→ remove the logs if error occurs

→ apt install git

→ using the git hub install instashell using

eg

git clone "the website link"

→ apt install tilix → terminator type

→ apt-get install tor.

→ to start tor → # service tor Start.

tostop → # service tor Stop.

how to use mac Changer 0-Zero

1) to See the current and permenet mac address.

macchanger -s eth0

macchanger --help for more info

When we reboot the permenent mac address came to action.

Foot printing

Foot printing

Types

→ Active foot printing

requires intration between

→ passive foot printing

Social engineering, ph

Google hacking

In ula Scans

This Scans the webs

eg code :-

inurl: "index.ph

// ula can be explo

More updates

Just search in g

it will show co

or exploit da

classmate

PAGE

classmate

Foot printing

Foot printing

Types

- Active foot printing

requires interaction between target

- passive foot printing

Social engineering, public information

Google hacking

Inurl scan

This scans the websites url.

eg code :-

inurl: "index.php? id=" #// This types of

url can be exploited using SQL injection

more updates

Just search in google "google hacking database"

it will show commands.

or exploit database

DATE

Nicto

→ for more info use help

→ Do research on these tools

in this help is —H not small -h

Who is tool

to get a detail of a company or a website.

The harvester

if the tool does not work find the location and run.

Shodown

SHODAN

→ search or IP and enter IP if its valid then it will get displayed Ok

Dig

→ Dig is used

Ip or DNS

→ Zone tra

eg: Dig

Zone

A - I

AAAA

NS -

Zone

dig

d

→ Same

→ #

DATE

→ Dig is used for Zone transfer attack or getting more Ip or DNS data.

→ Zone transfer → Replicates you as slave to the master.

eg: Dig google.com #for details

Zone transfering

A - IPV4 Address

AAAA - IPV6 Adress

NS - named Server.

Zone transfer

dig axfr website // get help

dnsenum

→ Same as Dig but. // learn by yourself

→ # dnsenum --help

PAGE

classmate

MEtaSPOlitable

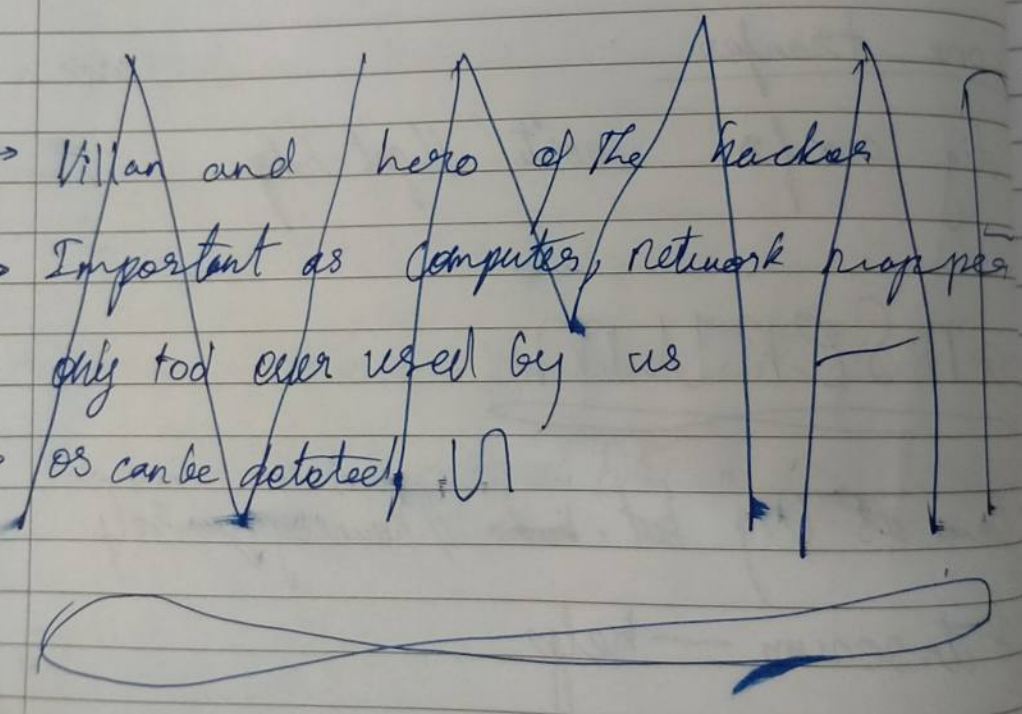
→ ~~use~~ first download it

→ it is a portable virtual machine, which is used to attacks and scann the attacks

→ Don not connet to the network locally.

→ it is a linux machine

→ use it as a victum and attack it



→ Villan and hero of the hackers

→ Important as computer, network mapper

→ only tod ever used by us

→ OS can be detected in it

→ nmap --help for more help.

classmate

PAGE

The protocalls that

→ DCP

→ UDP

→ ICMP

→ CTP

nmap is by default used

~~Nmap~~ nmap

The bunch of

→ Major IP this are blocked.

nS lookup

it gives the

→ curl is

the ip addre

→ # curl ip

and location

classmate

The protocalls that can be used

→ DCP
→ UDP
→ ICMP
→ CTP

nmap → by default Scans 1000 ports which is commonly used

~~Nmap~~ nmap

The bunch of options will be printed

→ major IP this is a website where the ipaddress are blocked.

nslookup "Ipaddress" (or) "website"

it gives the name of the server.

→ curl is a tool used to find the the name of the ip address

→ # curl ipinfo.io/ "Ipadderess"

and location is also find.

DATE

→ Ip locator in google, this website is used to locate Ip address.

→ nmap.org you can practice

→ nmap with Gui is Zenmap

TCP

→ Layer 1 :- Software (Application layer)

→ Layer 2 :- Transport layer

→ Layer 3 :- Internet layer

→ Layer 4 :- network layer (local)

~~mordern~~ . mordern tells who is visit where.

 → Data

 → Packet

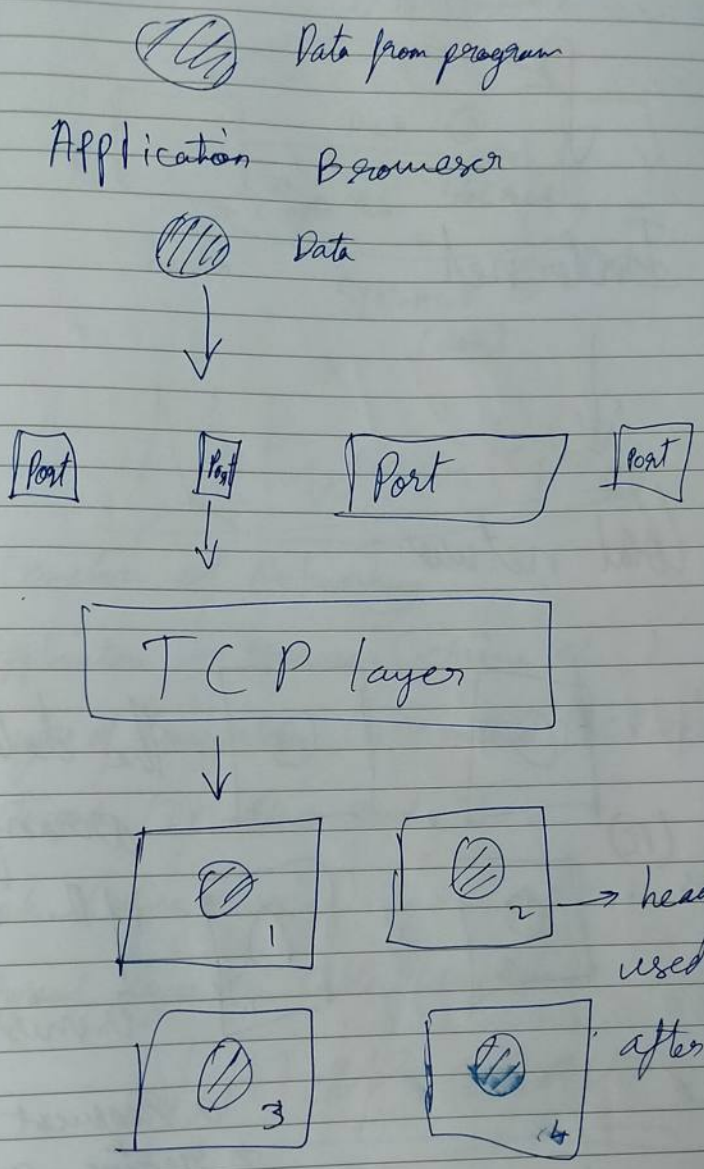
 → Packet with data and header

CLASSMATE

PAGE

Gui TCP/IP

DATE



PAGE

classmate

DATE

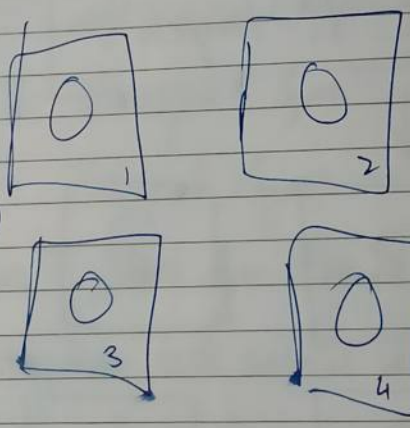
↓

Internet

↓

↓

local networ



Mac address (PC)

The data →
arrange →
if the da →
is missi →

a request is
to receive agai

6

classmate

PAGE

SYN

Ack

Hacker

SYN

Netw

Structure of Networ

→ Application → Processe

→ Types of transportation

→ Network (IP address

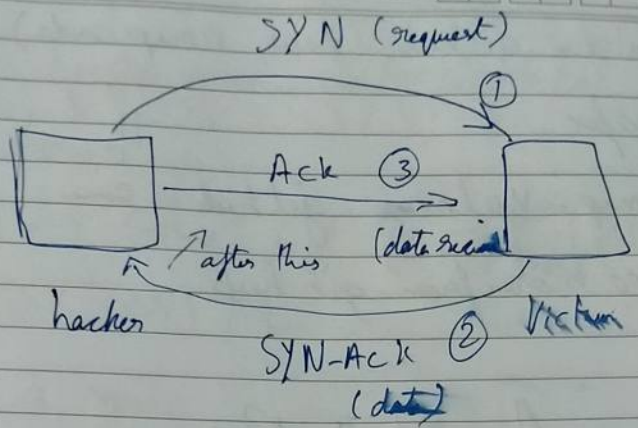
→ Link (wire or wi

→ Physical layer (ca

NM

→ See the scr

classmate



Networking

Structure of Networking

→ Application → Browser (chrome etc.)

→ Types of Transportation (UDP method, TCP method)

→ Network (IP address sending)

→ Link (wire or wifi)

→ Physical layer (cable) (modem)

Nmap again

→ see the scripts in nmap.

downloads

DATE

→ Vulscan github (new nmap code) Search in firefox.

→ nmap-vulners github (same)

→ See more from git hub.

AMAP

→ Same as Nmap Explore.

OWASP

→ this is used to test web Application.

→ install in ~~ubu~~ virtual box

→ install the first one.

→ ~~Com~~ Copy the ipadress in your browser.

→ you will get an idea

Network page

HTTP - hyper te

easy to hack

HTTPS → Some

like SSL (or)

→ cookie is mai

COO

→ these are the

id the prim

about it.

Bu

→ this is pre insta

→ used for prog

→ you can open

→ we can mo

→ the prog

→ install burpsu

→ you can get it in

Network pages

HTTP - Hyper text Transfer protocol
easy to decode

HTTPS -> Some but encryption is used
like SSL (or) TLS

-> Cookie is main

Cookies

-> These are the small data packets stored in the users id the privacy can be breached please don't attack.

Burp Suit

-> This is pre installed Gui program
-> used for proxy - Hacks etc., Brute force, decoder etc.
-> by you can open in cmd or start.
-> we can modify our own packets.
-> The proxy setting should be used both Burpsuit and Firefox
-> install burpsuit trusted certificate
-> you can get it in http://burp

→ and import the certificate

→ you can edit the header and the value.

What web

→ this used to know more about web technology details.. what web - help

dirb

→ it finds hidden pages of a websites

→ it Brute forces the webservers.

hydra

Brute force attacks in web

- help.

→ Copy the path from Burpsuit

→ See video

classmate

PAGE

Session hij

→ flaw in cookie

→ Stealing the information

Session fixa

→ flaw in link

→ when the web unique user user so login.

hijacking the

→ Zoom links

SQL In

1) command inj basic common

classmate

DATE

Session hijacking

→ flaw in cookie.

→ Stealing the information while exchanging the information

Session fixation

→ flaw in link

→ when the web server creates unique id for unique user it only interacts with particular id not user so that unique link can be accessed without login.

hijacking the session

→ Zoom links. eg.

SQL Injection

1) command injection

basic commands. for linux & windows.

DATE

1) net cat

2) "nc" is the word for terminal

3) Blind command injection

4) → Same like command injection

5) → to check whether the Blind command can be executed ping twice

6)

7) Wire Shark

8)

9) Shell Shock

10) msf console

11) SQL Injection.

3) Commands in SQL

1) Create	5) Delete
2) Select	6) Drop
3) Update	
4) Insert	

classmate

PAGE

Data base
Collection

Relational
Related ta
Non rela
opposite

for SQL yo

→ DNS -
→ it maps
→ all DNS
Share Conne

classmate

Database

Collection of Data which can be used

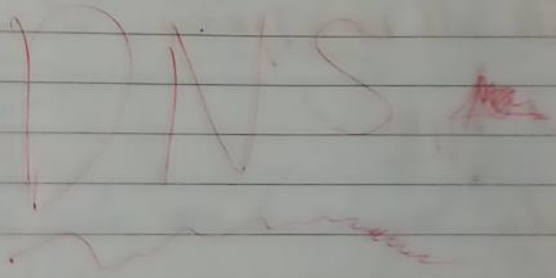
Relational Database

Related tables

Non Realational database

opposite

for SQL you should install mySQL or related software



- DNS - Domain name System
- it maps domain name with ipaddress
- all DNS server does not has every ips and they share connect the information for security purpose

DATE

DNS components

→ Name Space

eg

921.58.101 = google.com (they are called name space)
IP address

→ Client

We are the clients ask web names ip

→ Servers

it holeds all name spaces.

Record types

1) A record

→ it maps IP address

Tools for DNS

→ Ping

→ nslookup

→ Dig → dig

DATE

DNS spoofing

learn it.

DNS Sec

learn it.

Nat Vs Briged Vs host only

JS

Variables → These value can be changed in the programs.

Constants → These values cannot be changed.

Literals → Directly providing the value in the program

It is a mixture of variables and constant

Variables

Syntax

let variable_name = "value"; // Same as C

PAGE

classmate

DATE

Constant

Syntax

Const variablename = "value";

operator preference is same like a

~~Del~~

Delecting an varible ~~or~~ object or anything

Delete is ke keyword.

Syntax

~~del~~ delete varblename or constant nam or object

Array eg

Constant a1 = [1,2,3,4];

const a2 = [1, 2, null, 4, "jue"];

//Array can have many array.

~~Constte~~ const a4 = [[1,2,3], "babu", 2];

classmate

PAGE

Date object

Syntax

// I +

→ Const now = n

Console.log (no

// this prints

// II +

Const dt

console.log

// II +

Const dt

console.

// prints y

if else

if else is so

classmate

DATE

Date object

Syntax

// I +

→ const now = new Date ();

console.log (now);

// this prints current time

// II +

const dt = new Date (2018, 9, 12);

year month Date

console.log (dt);

// II +

const dt = new Date (2018, 9, 12, 15, 0);

year month Date hour min

console.log (dt);

// prints year, month, Date, hour, min.

if else

if else is same.

PAGE

classmate

DATE

Switch Statement

Same.

while

Same

do while

for loop

Same.

for in loop

same as python

for of loop

Same as in loop but in loop prints index but it prints the value of the variable

Type of

Same.

Print in console using Console.log("")

classmate

PAGE

DATE

if-else

Same

Conditional operator

Same.

Break

Same

Function declaration

→ function "function name" (~~parameters~~ parameters) { actionblock;

return (parameter);

}

Function call

function name (parameters)

Anonymous function

You can hide a function inside a varible

index

PAGE

classmate

eg

Syntax

```
const f = function () {
    Statements }

f(); // calling a function
```

You can declare it in a ~~tuple also.~~ dictonary also.

1) Arrow notation

eg

Syntax

~~con~~ with out arrow

```
const f1 = function () { return "hey"; }
```

with arrow

```
const f1 = () => "hy";
// both are same.
```

classmate

PAGE

DATE

2) another eg: without

const f2 = function (arg) { return "hey"; }

with

const f2 = arg1 => "hey";

3) another eg

without

const f3 = function (arg1, arg2) { return arg1 * arg2; }

with

const f3 = (arg1, arg2) => arg1 * arg2;

this keyword.

~~Not~~ return function

~~when~~ when the function executes the return value can ~~be~~ be a function

array

classmate Same.

PAGE

How to add an element in the array

```
const arr = [2, 3, 4];
console.log(arr);
// output 2, 3, 4
console.log(arr.push(5));
console.log(arr)
// output 2, 3, 4, 5.

console.log(arr.pop());
// to remove the last element.
console.log(arr)
// output 2, 3, 4
console.log(arr.unshift(1));
console.log(arr);
// adds an element at begning
// output 1, 2, 3, 4
console.log(arr.shift());
console.log(arr)
// to remove the first element
output 2, 3, 4,
```

concat()

```
const arr=
console.log(
// output -
console.log
// many elem
// output.
```

Slice()

```
eg
const ar
console.
// Starts
// output
console
// start
// output
// all ar
```

concat()

```
const arr=[1,2,3];
console.log(arr);
//output -1,2,3
Console.log(arr.concat(4,5,6));
//many elements can be added in the array
//output. 1,2,3,4,5,6.
```

Slice()

eg

```
const arr2=[1,2,3,4,5];
console.log(arr2.slice(2));
// Starts from 2nd element
//output. 3,4,5
console.log(arr2.slice(2,4));
// start from 2 element and ends with 5th
//output 3,4
//all same like python
```

ents to be added

given order.

to be removed
er 1

PAGE

Object creation

DATE

The object is created by use of variable

Class creation.

Syntax

```
class model {
  constructor () {
  }
}
const obj 1 = new model();
const obj 2 = new model();
```

Error handeling :

```
try {
    Statements
}
catch (e) {
  console.log - Statements
}
```

PAGE

classmate

SQL Injection

DATE

Create
Select
update
Insert
Delete
Drop
From
where
Syntax
eg
Select column from tablename where condition
eg
Select names from products where name='n
-- comment line
/* comment line */
→ to Check the website is vernerable to SQL p
" ' "
↓
apostrophe if this show error
it is vernerable.

classmate

PAGE

tools to be

→ all hacking to
→ apt-get ins
→ pip3 install
→ pip3 all
tools to

→ XSS e.g.
→ ~~XXS~~ XSS

MIM

Man In mi

PC Victim

classmate

SQL Injection

DATE

Create
Select
~~Upda~~ update
Insert
Delete
Drop
From
where

Syntax

eg

Select column from tablename where condition

eg

Select names from products where name='mi

-- comment line

/* comment line */

→ To check the website is vulnerable to SQL p

" , "

↓

apostrophe if this show error

it is vulnerable.

classmate

PAGE

tools to be Insta

→ all hacking tools

→ apt-get install p

→ pip3 install xc

→ pip3 all hack

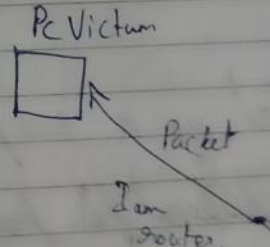
tools to learn

→ XSSer, dift

→ ~~xxf~~ XSS-Sni

MIMA

Man In middle



classmate

tools to be Install

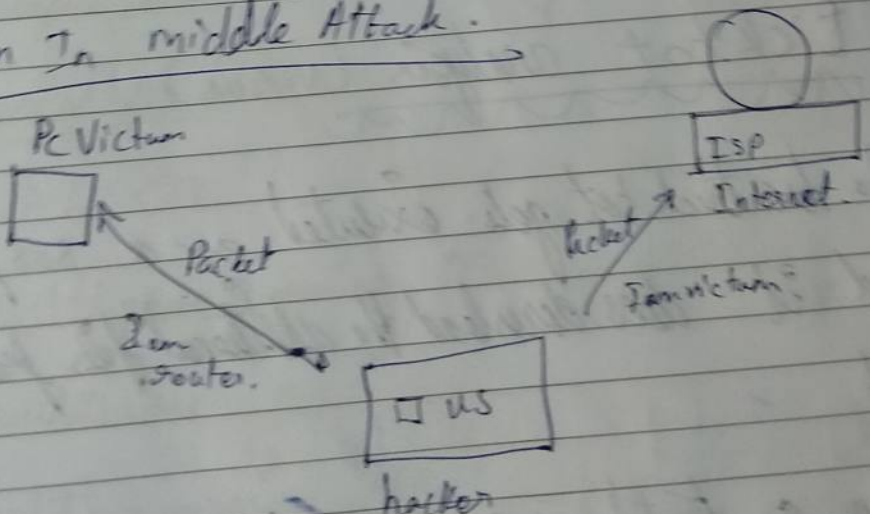
→ all hacking tools from github.
→ apt-get install python3-pip
→ pip3 install xcat
→ pip3 all hacking tools, apache 2

tools to learn

→ XSSer, dift net, ettercap with Gnaindra
→ ~~XSS~~ XSS-Sniper - Github download.

MIMA

Man In middle Attack.



DATE

tools to be install

→ ~~mitm~~ mitmf ; Github

→ and install all requirements for mitmf

by → pip install -r requirments.txt.

→ wine

→ dpkg --add-architecture i386

→ apt-get update

→ apt-get install wine32

→ python 2.7.14 for windows x86 MSI

→ wine msiexec /i python-2.7.14.msi

→ ngrok download

tick bot analysis (virus)

→ The ~~the~~ trick bot gets exicuted as a subp

and it does download the additional files fr

web

→ then a trusted program is turned on and the

trusted program runs in process hollowing

classmate

PAGE

→ the trusted program

mode and after every

replace the code in that

→ using some tools we

process modified etc..

→ inject DLL64_

Credentials.

→ if network transfer is

→ https://github.com

OS

→ a interface between

types of OS

→ Batch OS

→ Multiprogramming

→ multitasking OS

→ multiprocessing

→ Real time OS

classmate

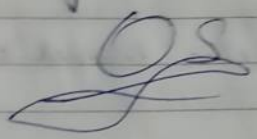
→ the trusted program goes into suspended mode and after every data gets load the virus replace the code in that program. and runs

→ using some tools we can see the files added the process modified etc ..

→ inject DI64_ configs → this is stealing Banking credentials.

→ if network transfer is not encrypted in network transfer.

→ https://github.com/hasherezade



→ a interface between human and computer hardware.

types of OS

→ Batch OS

→ Multiprogramming OS

→ multitasking OS

→ multiprocessing OS

→ Real time OS

DATE

Websites to be known :

→ owasp

→ nmap

→ hackus

→ Hack me.

Cmd

→ dir = ls

→ cd = cd.

→ help → this is like manual or help

eg help dir

help cd.

→ mkdir = mkdir.

→ rmdir = rm - for folders.

→ move = mv

→ copy = cp

→ ren → is used to rename a file or anything

eg :- ren cat.txt cats.txt

classmate

PAGE

The cat file

→ Del = rm

→ * = all.

→ echo = ec

→ type = cat

echo usage

create a new

echo hel

modify the

echo b

→ & = ;

→ && =

→ || →

→ | →

→ Set = le

→ System in

classmate

DATE

The cat file will become Cats file

→ Del = Rm . for files

→ * = all.

→ echo = echo

→ type = cat.

Echo usage

create a new file

echo hello world > File.txt

modify the exting file

echo bye bro >> file.txt

→ & = ;

→ && = &&

→ || → only one command is run.

→ | → outputs are compined.

→ Set = let. (Java Script)

→ System info → Shows details about ur system

PAGE

classmate

→ copy any content to the clip board
eg

~~Systeminfo~~

ipconfig | clip

→ driverquery → gives list of drivers in your pc.

→ -V = -V

→ ~~tas~~ tasklist → shows current task

→ tree → shows the path of files.

→ fc → used to compare files
eg

fc 1x1.txt 1x2.txt

→ Shutdown -s = Shutdown

→ Shutdown -c = Shutdown -a
(in aux) (windows)

→ ciper → used to encrypt files.
eg

to encrypt
eg: cipher

to decrypt
eg: cipher

for more use

→ taskkill → to

→ ping = ping

→ tracert
eg tra

→ pathping →
eg pathping

→ ipconfig =

→ arp - a

→ Nslookup =

→ F7 → histor

→ ctrl + c =

→

to encrypt

eg:- cipher /e File.txt

to decrypt

eg:- cipher /d File.txt

for more use help

→ taskkill → to kill task

→ ping = ping.

→ tracert → use and c

eg tracert 8.8.8.8

→ pathping → use and c

eg pathping 8.8.8.8

→ ipconfig = ifconfig.

→ arp -a = arp -a.

→ Nslookup = Nslookup (used to find domine ip or web)

→ F7 → history of command

→ Ctrl+c = Ctrl+c.

→

Information gathering

(Websites)

→ use DomainTools.com or whois.net

→ use pipl (person)

Creating a malware

→ Things that malware does.

1) Create a connection with our server.
2) Create a shell function
3) Automatically start program when machine is reboot
4) Start / Stop / Spawn other programs
5) Navigate through different directories
6) able to restart it self within a period of time
7) Implement keylogger to our backdoor

C program modules to be learnt.

1) Stdio.h	4) winsock2.h
2) Stdlib.h	5) windows.h
3) Unistd.h	6) winuser.h
	7) wininet.h
	8) string.h
	9) sys/types.h

tools to be

→ bee logger

→ F Society

→ apt-get

⇒ " "

→ SSL Strip

the new

~~said~~ iso

→ Ruby

→ Bash

→ Rootkit

→ Digital forensics

→ See Parrot OS

→ IDA

~~→ practi~~

DATE

7) wininet.h
9) string.h
11) sys/types.h
8) windows X.h
10) sys/stat.h

tools to be Downloaded.

→ bee logger → Git hub.
→ F society → Git hub.
→ apt-get install chkrootkit
⇒ " " " rkhunter
→ SSL Strip (man in middle), Metasploitable 3.

the new careers to be learnt

→ ~~Said ISO~~ Shell Scripting
→ Ruby
→ Bash
→ Root kit
→ Digital forensics
→ See Parrot OS site.
→ IDA
→ ~~Practical~~

PAGE

CLASSMATE

Things before deploying the Root kit

DATE

→ Check whether it already exists on the target

→ Check whether the target is virtual machine

→ Check the location

→ Disable antivirus

→ make a loadable Kernal program

→ Examine the process list

Places where we can download virus

→ VirusShare.com

→ Malware - Traffic - Analysis.Net

→ github → Shadow brokers.

→ Disassembler and assembly-level debugger

→ Basics of reverse engineering

→ how to set up a safe malware analysis lab

classmate

PAGE

MSDN

msdn.microso

Exp

XSS A

→ it takes advan

Request by ash

XSS Request

→ Tricks a logged-

Request to a

→ Request is sent by

→ Can be difficult t

→ Also called one cli

classmate

MSDN

msdn.microsoft.com

Experience

Learn

XSS Attack

→ it takes advantage by submitting unexpected request by using commands or programs etc..

XSS Request forgery

→ Tricks a logged-on victim's browser to send a request to a vulnerable web application

→ Request is sent by the victim, not the attacker

→ Can be difficult to detect.

→ Also called one click vulnerability

W- Website , A- App) t - tool, Th - Github owasp

DATE

→ hellbound. hackers - W

→ McAfee HacMe Sites - W

→ hacme Bank - W

→ hacme Bank for android - A

→ HacMe Books - W

→ Hack me Casino - W

→ Hacme Shipping - W

→ Hacme travel - W

→ mutillidae - W - t

→ Over the wire - W

→ Owasp juice Shop project - W → github.

→ peruggia - W - t

→ Root me - W

→ Try 2 hack - W → gitand some web

→ Vicnum - W - t

→ Web Goat - W - t - Git

→ hack.me - W

→ hack the Box - W

PAGE

classmate

DATE

→ CTF 365 - w

1) → hacking lab - OS - T
2) → Pwnable.kr
3) → Smash the stack
4) → microcorruption
5) → w3challs
6) → PWNO
7) → PVIA
8) → CTF time
9) → Juice Shop
10) → hackademic
11) → hackxor
→ Bodgeit Store
13) → Enigma group
14) → hackyourself first.troyhunt.com
15) → Slaue hack.com
→ peruggia
→ github.com/psiinon/bodgeit

classmate

PAGE

Penetrati
→ metasp
→ Penetrat
→ Open w
→ pentes
→ penet
→ XSS -
→ Open
Manu
→ MITM
&
Explo
→ Shell
- Shell
→ Shell
→ Exp

class

DATE

Penetration testing resources

- → metasploit unleashed
- → Penetration testing Execution Standard (PTES).
- → Open web Application. Security project (owasp)
- → pentest - wiki
- → penetration-testing Framework. (PTF)
- → XSS - payloads
- → Open Source Security testing methodology manual. (OSSTMM).
- → MITRE's Adversarial. Tactics, Techniques & knowledge (ATT&CK)

Exploit Development

- → Shell code Tutorial - tutorial on how to write shell code.
- → Shellcode Examples - shellcodes database
- → Exploit writing tutorials - same as name.

PAGE

classmate

DATE

OSINT Resources

→ OSINT framework - OSINT tracking to
→ intel techniques - osint tools
→ Net Bootcamp OSINT Tools - OSINT
→ wigle.net → information about network

Social Fengineering Resources

→ Social Engineering Framework

Lock picking Resources

→ Schuyler Towne channel
→ bosniabill
→ /r/lockpicking

Operating System Resources

→ Security related operating systems
Rawsec
→ Best Linux penetration testing Distribute
@@ Cyber punk

→ Security @ Dist
→ Cuckoo -
→ Computer Aided I
(CAINE)
→ Digital Evidenc
→ Tails

Hacking tools

OS

→ parrot, kali

Dockers for p

docker pull
↓
Same for all
gbhackers.

multi - para

→ metasploit
→ Armitage
→ Faraday

classmate

PAGE

classmate

→ Security @ Distrowatch

→ Cuckoo -

→ Computer Aided investigative Environment (CAINE)

→ Digital Evidence & Forensics toolkit (DEFT)

→ Tails

Hacking tools

OS

→ parrot, kali

Dockers for penetration testing

docker pull owasp/zap2docker-stable

↓ Same for all

wpscanteam/wpscan

etc.... See

gbhackers.com/hacking-tool-list/

Multi-paradigm Frameworks

→ metasploit

→ Armitage

→ Faraday

classmate

→ Exploit pack

→ Pupy

Vulnerability Scanners

→ Nexpose

→ Nessus

→ OpenVas

→ Vuls

Static Analyzers.

→ Brakeman

→ Cppcheck

→ FindBugs

→ Sobelow

→ bandit

Web Scanners

→ Nikto

→ Arachni

→ W3af

→ Wapiti

→ Sec Apps

→ Web Reaver

→ WPScan

→ Cms-ex

→ JoomScan

→ AcsTIS

Tools typ

→ Network

→ Wireless

→ Transport

→ Web Exp

→ Hex Edit

→ File

→ Defense

→ hash Cra

→ windows

→ GNU/Linux

DATE

- Wapiti
- Sec Apps
- Web Reaver.
- WPScan
- Cms-explorer
- Joomscan
- AcsTIS

Tools types

- Network tools
- Wireless network hacking tools
- Transport layer security tools
- Web Exploitation.
- Hex Editors
- File Format analysis tools
- Defense Evasion tools.
- Hash Cracking tools.
- Windows utilities
- GNU/Linux Utilities

PAGE

classmate

→ MacOS Utilities
→ DDOS tools
→ Social Engineering tools
→ OSINT Tools
→ Anonymity tools
→ Reverse Engineering tools
→ Physical Acess tools
→ Side-channel tools
→ CTF tools
→ pentesation testing Report templates

Security courses :

→ Offensive Security testing
→ Sans Security training
→ open Security training
→ CTF Field Guide
→ ARizona Cyber warfare Range
→ Cybrary
→ Computer Security Student

→ European union information Se
Database of Vu

→ see on
https://gb

drone

→ drone Sploit
→ Cyper punk -

hackable Site

→ hack yourself
~~→ Stare~~
→ bonsai-sec.

→ windows 8
→ you can use
or USB

DATE

than your known . P: or . C: cl.

---

windows password cmd

net user → this command is used.

to find users list :

net & user Administrator user *

→ to change pass

---

open windows Explorer

cl. P:/ my softwares

Start

Tool

~~softwares~~ to be download

→ Safenugget → Github → Scan. Vulnerable pa

Scanner.

↓

Safe Nuget.

→ web chlarling → learn.

classmate

PAGE

MITM Th

ARP (ADD Re

→ Simple protocol

machine to I

Beelogger is

→ Beelogger is a to

keylogger.

→ it sends key Stro

→ Find it from

VEI

→ it is a fun

back door

→ to download it

→ and goto

→ and run Veil

classmate

DATE

MITM Theory

ARP (ADDress Resolution protocal)

→ Simple protocal used to map ip address of a machine to its mac address

→ Beelogger is a tool in the Linux used to create keyloggers.

→ it sends key strokes from gamil.

→ Find it from Git hub

VEIL

→ it is a framework which allows to create a back door

→ to download it goto git hub VEIL Framework

→ and goto Config directory and run Setup.sh

→ and run Veil.py

classmate

PAGE

MITMF

→ to install it get it from git.
→ it is used Mitm attacks
→ first install requirements
→ by :- pip install -r requirements.txt
→ follow the instructions given on github
then

→

Post - connection Attacks :
(Information gathering)

→ Discover all devices on the network
→ Display their
1) Ip add
2) mac add
3) OS
4) Open ports.

classmate

PAGE

5) Running Services etc -
etc. This can be done by ~~nmap~~, net scanner
& net discover, nmap

how to use net discover

→ net dicover --help

→ net discover -r (range of Ip address)

eg= 10.0.0.1/24

∴ it means 10.0.0.1 - 10.0.0.24

Press Q to Quit the program.

or

→ net discover -i eth0

FSociety

→ install it from GitHub

→ it is collection of tools.

Root kit Cheaker

DATE

Rootkit checker

→ in windows install the newest notron antivirus

→ Root kits are the virus or malware which hide in Root Kernel code. and attacks very deep

→ it is very important and difficult to detect

→ in linux use

1) Chkrootkit

2) Rkhunter

→ Chk Rootkit — help

→ ~~sudo~~ apt ~~install~~ -get install ~~RKhunter~~ rkhunter.

→ Rkhunter -help.

→ to perform Scan. and update it frequently.

→ sudo rkhunter -C -C

→ this is like antivirus but you have to manually Delete the files

classmate

PAGE

Who is look up : we web browser

→ you can gater information on the Domine, website

1) DNS Staff

2) Net Craft.

→ plase Sing the domine primarily cheack

→ 1) DNS Stuff // youhave tools online so you can do etc

→ this is not a tool. it is a website

Key logger

THE LAB

→ The plase where we can practice because we want to run a malicous Software you can't run on original OS on original computer you may break it

→ so we need virtual machine

DATE

Typical Network

Information gathering

- IP
- Domine name
- Technologies used
- other websites on the same servies.
- DNS Records
- files / Sub-domains / directories
- Scanning the websites
- use a program to discover the Sub domines

SETUP BURP SUITE

- first cheack the Burpsuite is installed
- Enable proxy of the Burpsuite
- and enter the proxy in the Browser
- first install or upgrade Burpsuite
- the Defaut Inter face is 127.0.0.1 at port 8080

classmate

PAGE

- the Burp suite
- Websites like
- download the
- your Brows
- to install CA
- turn on pro
- Just type
- CA Cert
- Download
- Thats it.
- and dont for
- exting th
- off.

M A

- these are th
- Physi

classmate

→ the Burp suite proxy will not run higher Security websites like google, in order to run it download the trusted certificate and install it in your Browser.

→ to install CA, turn on the Burp suite and then turn on proxy and turn off "intercept" and just type "burpsuite" in url's and download CA certificates from "CA T", and add the Downloaded certificate by pressing import and that's it.

→ and dont forget to turn off the burpsuite before exiting the browser it will show that the server is off.

MAC Address Changer

→ these are the address which is kept from by manufacturer

→ Physical, → Permanent, → Unique

DATE

Why change the mac Address

→ increase anonymity

⇒ Ryan can Bypass the filters

→ hide the identity

how to change Maccadress

⇒ ifconfig (interface) down

eth0

WlanO

// this command is to ~~change the~~ turn off the ~~net~~ device

→ ifconfig (interface) hw ether (mac address

eg:- 00:11:22:33:

→ ifconfig eth0 up

(OR)

classmate

PAGE

macchanger

macchanger

~~how to~~

How

0x0

→ use pip

→ then pyinstalle

// this creates

Ett

→ Arator tool fo

→ Built in Sn

→ dns spoofing

classmate

macchanger

macchanger -r eth0

~~sudo~~

How to convert py into exe

→ use pip install pyinstaller.

→ then pyinstaller python_progame.py --onefile

// this creates that executable in one file.

Etter Cap

→ Another tool for mitm attacks

→ Built in Sniffer

→ dns spoofing etc.

→ Before using the ettercap which is preinstalled

→ nano . /etc/ettercap/etter.conf

Remove # below

if use ip tables.

ec_uid=0

ec_gid=0

→ and Save !

→ etter cap --help.

The harvester

→ this gather the emails So we can do engineering

→ To run it type

the harvester (no Space)

DATE

NMAP - 2 on nmap

- → huge Security Scanner
- → IP range cabe
- → open ports
- → Running Services
- → Operating System
- → connected clients etc....

Nmap --help.

Proxy Chains

- → file location
- → etc/proxychains.conf
- → run proxy chain

proxychains firefox www.duckduckgo.com

- → dnsleaks.com for you working.

PAGE

classmate

DATE

Metasploit

→ to start it by "msf console"

→ the modules of this tools are saved in

→ = /usr/share/metasploit-framework/modules

Phy Pro to Change to run

~~Mac address~~

Comm
in Cl
or
termi

→ The program should exicute the terminal commands

→ Sub process is the module which allowes to run commands in linux and windows.

→ Syntax

import subprocess

subprocess.call("command", shell = True)

To see ifconfig DATE

Eg:-

Import Subprocess as s

~~Subpro~~ s.call ("ifconfig", shell = True)

HYdra for internal network hacking

→ use x hydra → Gui of hydra

→ do a nmap Scan to check the open ports.

→ Then open x hydra etc.

Back Doors → Reverse connection

→ ~~Lis~~ Listening for incoming connections on a specific port

→ net cat can be use

Exploit XSS

→ all the attacks are performed using Dvwa

Level 1 Low Security

eg <script> alert(1)</script>

Level 2 Medium Security

eg * changing a single char capital etc.

<ScRipt> alert(1) </ScRIpt>

Level 3 High Security

using orther tags you can perform attacks

eg:- <body onload = alert(1)> </body>

Level 4 Impossible

find your self

SQL Injection

Using SQL MAP

These Shortc
at security l
→ the Burp Suit
request.
→ then the requ
by converting
→ and use the

→ use crack

Anos

→ get it from git
→ these are pre
→ go to help.

These stunts are performed under DVWA at security level low or medium

→ the Burp Suit proxy is used to capture the request.

→ then the request txt is pasted in sqlmap by converting into txt document

→ and use the help to do some action

Cracking

→ use crack station website.

AnonSurf

→ get it from github

→ these are proxies to browse the dark net.

→ go to help..

Tor

DATE

- → modified version of firefox
- → fully patched
- → disable plug ins
- → enable private plugins
- → disable Java Scripts

Verify the tor

in windows

- → ~~Tour~~ download tor browser and its signature
- → Download GPg.4 win (install it)
- → open cmd
- → itorproject.org/docs/verify
- → copy the code from it paste it in cmd
- → type → @ gpg.exe --fingerprint (input and compare the finger print in the and cmd

classmate

PAGE

- → you have vid
- → type → gpg.exe
- Apple
- → See vid
- Linux
- → See vid
- Tor
- → Do not
- Bridge
- → use bridge
- → use plu
- → tor bridg
- → download
- → email
- → the bridge
- → use v pr

classmate

→ you have vid watch it.

→ type → gpg.exe --verify tor-(setup) tor(sig)

Apple

→ See vid

Linux

→ See vid

Tor

→ Do not maximise the window

~~Bridge in tor~~

→ use bridge if tor is not working

→ use plug in even if bridge is not working.

→ ~~tor~~ bridge.torproject.org ~~/options~~ options

→ download bridge with a pluggable transport.

or Send

→ email to. bridge@torproject.org.

→ the bridge will be downloaded, copy the bridge

→ use vpn with it.

DATE

how to use a good VPN

→ The VPN Should be reputable
→ avoid free VPN
→ Make Sure they keep no logs.
→ use HTTPS everywhere.

how to have a fully secured Tor connection

→ HTTPS every where + VPN +
Tor + Bridges with plugins + TLS
→ Create your own VPN

Tips for tor

→ ~~Add~~ never use tor In full screen.
→ check for updates.
→ drag to increase the size
→ go to options
→ privacy and . Security
→ never remember history
→ Block trackers
→ Block popup windows

classmate

PAGE

→ wa
→ prev
→ Sec
→ Blo
→ Blo
→ wa
→

Tails.

→ it is a live
→ the default con
→ it leaves no
→ once the com
→ do not use
→ Ctrl + Alt +
→ Same as all

classmate

→ warn when browsers install addons
→ prevent accessibility services
→ Security Safest
→ Block dangerous and deceptive content
→ Block dangerous downloads
→ warn you about unwanted software
→ Test with panopticlick.eff.org
→ panopticlick

Tails.

→ it is a live operating system
→ the default connection is by tor.
→ it leaves no traces.
→ once the computer is restarted the traces are erased.
→ do not use Tails in virtual box or vm ware.
→ Ctrl + Alt + ↓ new work Space (second desktop)
→ Same as all linux

DATE

→ Tails is a volatile os nothing is stored after restart

→ Same as for browser.

Enabling presistence in Tails

→ Start Applications → tails → config presistence

→ put pass prase.

→ Select options

→ Restart.

~~→~~ More on tails

→ The tor browser in tails will only share access to folder called tor browser.

→ Tails has a addition browser called unsafe browser which the internet directly

→ The unsafe browser is used to access local network

→ ~~Google~~, fake

→ in Duck Duck go mention onion to get dark web

→ Do not use links, copy and paste url in onion

classmate

PAGE

Darknet Search engin

→ Duck Duck go (clear n

→ not Evil (Dark)

→ tourch. (Dark)

→ ahmia (for) (Dark)

→ hidden wiki (cl

→ dark fail (Clear

→ deep web sub

Reddit

(C

→ dread (Dark)

→ hidden answers

→ For Stalker - the

// it is used

// email that can

classmate

DATE

Dark net Search engines

→ Duck Duck go (clear net) (Dark net)

→ not Evil (Dark) (Quality)

→ tourch (Dark)

→ ahmia (Jaw) (Dark)

→ hidden wiki (contains broken links and Scams be carfull) (Clear) (Dark)

→ dark fail (clear) (Dark)

→ deep web sub reddit (clear) (or) (r/deepweb)

reddit

↓

type with URL

↑

(r/onions)

(clear)

→ dread (Dark)

→ hidden answers (Dark) (guard of deep.)

→ For stolen - the fake id generator

// it is used to generate fake information and

// email that can be used.

PAGE

classmate

Temporary Accounts. - Email

→ Temp mail Address. com (clear)

→ GUERRILLAMAIL . COM (Dark) (Clear)

//use ~~Scrambled~~ address.

Private permanent emails

	opens	Sender of emails
→ proton mail	(clear) (Dark) →	(clear) (Dark)
→ Elude	(Dark) →	((lear) (Dark)
→ Tor Box	(Dark) →	(Dark)
→ Xmpp		

XMPP

→ list of Server that can be Searched on git hub

→ It is like ~~Gmail~~ email provider but it is instant ~~messaging~~ tool

→ you can create

→ using tails

→ add ur accou

→ if you want

link from lo

tab.

→ use OTR

→ Tools →

✓ Enable pr

✓ Automat

✓ Require

✓ Don't l

press not

→ and verify

Fil

→ you can create a email on any server and
→ using tails it has a pegion application.
→ add ur account in it and fill informations
→ if you want onion service then copy paste the onion link from last server in pegion app. in connect service tab.
→ use OTR for communication it encrypts
→ Tools → Plugins → OTR (off the Record)
✓ Enable private mess
✓ Automatinticiate privat mess
✓ Require pri mess
✓ Don't log.
press not private (or) OTR
→ and verify your buddy.

File management

File Manag

→ Remove identifying Information
→ Securely delete the data
→ Securely wipe and encrypt the Storage

META Data

→ each file has meta data such as
  → the creator
  → programme used to create it
→ time etc ...

→ the meta data can be cleared in files by Right click

fire for file

File

→ fire for Se
→ Send. fire for
(

Cuses Java

→ onion Sha
(right click
using to

Wipe

HDD
→ Simply de
to delet it
→ files has
→ it only mov

~~fire for file Send~~

File Sending methods

- ~~fire for Send.com~~
→ Send.firefox.com (not that trustable)
~~→~~ (Security level → low & medium)
(uses java script)

→ Onion Share (app built in tails) (uses tor)
(right click) (uses an onion link) (access only using tor) (Sensitive files can be Shared.)

Wipe data or erase a storage

HDD
→ Simply deleting just shows that the file is in active
to delet it completly
→ files has inbuilt option called wipe
→ it only works on harddisk not in usb etc..

O = Zero

DATE

→ number of passes 2 is good for new hard d...
3 8 for more security
1 is waste.

→ it does not work on SSD or USB or etc...

→ Right click on windows can do it

SSD

→ destroy the SSD is best

→ or format and encrypt.

→ application → utilities → Disks

→ Select the partition

~~Delet the Se~~ format the partion 

Erase = overwrite with O

type = any ~~Fipe~~ type (your option)

name = any name (your option)

to encrypt it (more secure)

Erase = over write with O

Type = LUKS + Ext4 (encrypted)

classmate

PAGE

DATE

for new hard drive

or etc....

if

disks

etion)

ion)

secure)

ted)

PAGE

name = any

DATE

password = any

(only usable in tails)

(Brute force can be used to open it)

Encryption

⇒ this a method of converting useful data into gobrish which is understand by only some people

PGP

⇒ Very strong public key encryption

⇒ un broken

⇒ Encrypts all files

Symmetric encryption

→ Same key encryption

→ any body has the key can decrypt it.

classmate

PAGE

DATE

A Symetric encryption

→ 2 different key are used

→ one key is public key that is used to encrypt but this key cannot decrypt

→ another key is private key it is used to decrypt.

Manual encryption in Fails

→ Applications → utilities → pass word and keys → Gnupg keys → + (or) (File → new) PGP Key → continue → (fill name and Email all should be fake) → Aduance key option → Encryption type = Rsa, Key Strength = 4096 Expiration date (as wish) → Create. → (fill passw → Ok

Share the public key

in (GnuPg keys Tab) → File → Export → (Select → (Change pgp key → Armored PGP keys)

classmate

PAGE

→ Export →

- Go to the file location where you saved and share the file in email, onion share etc.. (or) open in txt format copy text and as message

at the receiver end

* how to use others public key.

→ if text is sent copy it in text editor and save it as .txt → .asc

→ if the file is sent download it as a asc file

→ then go to Gnupg keys page → File import → (select the file) → import.

→ you can see new key in . Gnpg keys tab you can verify the finger print etc...

Encryption using public key (text)

→ open a text editor → type message → copy → clipboard → Sign/Encryption clipboard with public keys. → (select the public key) → ok

→ open another txt editor → right click → paste and → copy the txt → send via email or onion etc...

DATE

decryption using private key (text)

→ copy the received txt in email etc..

→ [clipboard] clipboard → Decrypt / verify clipboard →

password = (ur password) → ok → (output).

~~Sing~~ Sign the message

→ to verify the file is from a real person we sign the

→ to verify whether the message is modified

Sending

→ text editor → type message → copy → [clipboard] clipboard →

Sing / Encrypt ..... → Select the person. →

Sign message as = (urs) → password = (urs) → ok

ok ~~→ paste~~

→ in the text editor → paste. → Send the pas

message (share)

PAGE

DATE

Recieving

→ Copy the message → clipboard → Decrypt/Verify ... → enter password → you can see ~~then to~~ Sender info and message.

for files (~~Files~~)

Sender

→ Select the file → right click → encrypt → select the keys. (optional signature) → OK → password = (urs) → OK

→ you can see new Image in same folder → share it

Reciver

→ download the file → right click → open with decrypt file → enter pass word → OK → open the new file and see → ✓ if it was sign you will recive notification that it has been verified

Just Siging

→ select file → right click → Sign → select the ~~file~~ key → Share it. (image and sign)

PAGE

classmate

Verifying Sign

→ Stored Image and sign download → Right click Signature → open with verified Signature

Tips

→ You can upload the key to a Server

→ You can download a key from a Server using email → name etc...

→ Verify the finger print

Crypto currency

→ Same like normal transation

→ one form can be ~~can~~ changed to another.

→ private and anonous.

→ Works on block chain

→ anyone has the record of our transation can calculate the money you have.

Wallets crypto currency

Applications → Electrum Bitcoin wallet

[wns = your choice] DATE

update the Electrum → by → electrum.org
→ downloads → linux → save it → save signature
→ download public key → import the download key
→ open with verify signature (signature download) →
if it is valid → ~~Run Electrum in portable~~ →
→ ~~change the~~ copy the electrum app in persistance →
change setting as executable → run → name = (wns)
→ Standard wallet → next → create a new seed
→ next → Segwit (or) legacy → note the seed
(Secured) (durable)
So you can ~~see~~ recover ur wallet → password
= (wns) → next

Ways to get Bit coin

~~[illegible]~~

→ mine it yourself
→ powerful computer required → complex
→ Expensive → Very anonymous.
→ time consuming

PAGE

classmate

→ using an exanchange + Tumbler/mixer
→ complicated
→ not anonymous
→ Bit coin ATMs
→ peer to peer (with cash)
Bit coin exchange
→ Bitcoin.org
→ Coin base.com
→ Coinatm radar.com
→ If the address starts with 3 it is segwit address
→ 1 for legacy

Sending and receiving Bitcoins

→ never send your money to illegal accounts

DATE

→ Copy address from receive ~~area~~ tab
→ paste it in send tab → enter pass word
→ it will take time

Mixer and tumbler

→ See more in Duck Duck go. com
→ bit coin-laudry. com (free) [not that ~~Secure~~ Safe]
→ Bitmix (onion) (charge) (fast)
→ mixtum (most anonymous) (time delay) (onion) (costly)

~~to~~

mixtum

→ Send yor recive address
→ Send money
→ wait.
→ ~~you~~ you have dependon mixtum website to keep yours Secret-

PAGE

classmate

DATE

Monero

→ like bit coin monero is Decentralised
→ unlike bit coin monero is private
→ untraceable and unlinkable transations.

→ go to.
Web. getmonero. org.
→ download the linux setup, verify
→ verify using hash using Gtkhash
→ Gtkhash
→ Select the file → ~~compare~~ hash
Compare the hash using ctrl+F in browser.
→ Open Gtk has in application utilities
→ Change the mod
→ execute using linux terminal.
→ Select language
→ use advance mode

DATE

- create a new wallet
- ~~se~~ full details → next → ~~set default port~~
- set password → connect a node (second option) (first option is resource hungry). → monero world.com/#nodes → ~~cop~~ copy a node and paste it and port → next → open wallet and similar to electrum

how to login after restart fails

- go to the location → open start gui → select the language → advance mode. → restore wallet from keys (or) open the file of the wallet. → password → use custom settings → node → paste the node again and port

PAGE

DATE

how to buy monero Anonymously

→ mine it your self (secure)

→ using an exchange

  → with normal currencies

  → with crypto

→ Atms

→ peer to peer.

→ web.getmonero.org.

atm is same as bit coin site

Crypto exchange.

→ ~~Chas~~ cash → Bit → monero

Cash → monero → Bit

Bit → monero → Bit → monero → etc.

Bit

linked

→ monero →

anonymous)

→ web.g

→ Morph to

→ note the

donation.

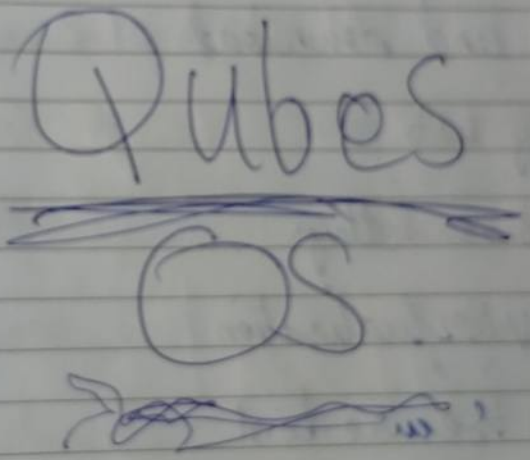
→ you can't

→ it d

Cannot

D.4 → monero (more secure)
linked list broken.

- Monero → monero → monero (make it more anonymous)
- web.getmonero.org
- Morph token
- 20
- note the minimum amount or else it acts as donation.



- you can't be private if you are not secure
- it creates different virtual partition that cannot access from one partition.

DATE

→ Qubes OS uses compartmentalization
→ different domains are created
→ every partition has own spaces.
→ it is very resource consuming
→ all are same as tails only difference it uses compartmentalization
→ it can be a live or main O.S
* Downloade and use
→ verify and download.
→ Copy usb
→ change bios settings
Enable virtualisation
Disable secure boot
Set boot to legacy
Boot from usb
→ Go to boot Select usb.

→ test option should be used

; open installer → english → continue → installation destination → select usb or harddrive → format → encrypt → put passprase → Begin install → create user → Finish

~~live mode~~ 2 USB is required

one as setup → one as OS instlen

reboot ✓

⇒ ~~yo~~ use ; t you can understand.

⇒ Ctrl + Shift + C → global clipboard.

→ Ctrl + ~~Ctrl~~ Shift + V → Global paste

⇒ defaut network is direct not tor

→ anon - whonix → this connects to tor defaut.

→ you can change. Sysnet → Sys-whonix

by Qube manager.

⇒ you can clone it by right click on. ✓

Soft ware to be install on linux

→ Synaptic
apt-get install Synaptic.

153) Important python libraries modules

→ win sound
→ main
→ url lib
→ xml pc. Server, xmlpc. client
→ xml
→ profile, Cprofile

→ win reg
→ web browser
→ tty
→ tkinter
→ time it
→ time
→ temp file
→ telnet
→ tar file
→ Syslog
→ Sysco
→ Sys
→ SS/ S
→ Spw
→ sock
→ Smt
→ Smt
→ site

- winreg → signal → ftplib
- web browser → random → email
- tty → pwd → dis
- tkinter → ~~ppt~~ pty → curses
- timeit → poplib → crypt
- time → pdb → codeop
- tempfile → os → cmd
- telnetlib → msvcrt → ~~as~~ asyncio
- tarfile → msilib → asyncore
- syslog → ~~mail~~ mail cap → ssl
- sysconfig → ~~mailbox~~ mail box → socket
- sys → 2to3 → module.python (not a module)
- ~~ssl~~ SSL → ipaddress
- spwd → imaplib → Beginners guide
- socketserver → http → Developers guide
- smtplib → html → python.org
- smtpd → hashlib → CV2 (screen record)
- site → getpass

DATE

Maltego

→ This tool is used for information gathering

→ it is a Gui discover by your self.

No Distribute

→ This is a web site which is used to check whether your antivirus gets detected or not.

→ nodistribute.com

The FAT Rat

→ it is same as veil

→ download it in Github

→ run setup.sh

classmate

PAGE

Empire

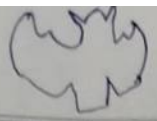
- Same as veil and fat rat.
- download it from Git hub
- run setup → install
- Give password.
- Create a listener

Z logger

- download this from GitHub
- it is a key logger creator

LaZagne

- download in github



DATE

Bat → exe

→ download .bat → exe Software from
→ www.f2ko.de/en/b2e.php
// no caps is used
→ Download and install using time
→ Invisible programes can be created

Icon Archive

→ used to download Icons
→ Iconvert → to convert Image to Icon
Image 256 X 256.
→ Bat → exe Set Icon

Right to left override

→ Zaid.pdf.exe → exe.fdp.diaz

- in app called Characters
- Right to left override
- copy
- paste
- deliver the word as zip.

Auto IT

- learn
- used to create exe
- less detectable

MS Office

- you can run codes in a normal word etc MS office applications
- only VBA code is run
- using empire → uselstager → windows macro → info → set options (ur options) →

→ copy the code
→ create a new macro
→ Save as word 97-2003
→ Tell the person to enable the content when its opened
→ Check whether the program is detected
→ use download and activate if emplike is detected

Auto Scan

→ download it from
http://autoscan-network.com/download/
→ download for linux
→ extract it
→ add 32bit compatibility
→ # dpkg --- add-architecture i386
→ #apt-get update
→ #apt-get install libc6:i386

Q? install using wine ??

32 bit arch

- dpkg --add-architecture i386
- apt-get update
- apt-get upgrade
- apt-get install libc6:i386

Arp Spoof

- Inbuilt in kali
- man Arp for more details
- eg :- arpspoof -i wlan0 -t 192.168.1.6 192.168.1.1

fool pc → windows, modem

fool modem → 192.168.1.1, 192.168.1.6

Server site attack

FTP attacks

→ using Zenmap discover open ports
→ google the service
→ see how to exploit it
→ like a login cheat

Back Door using metasploit

→ Rapid 7 makes it possible
→ msfconsole → runs the metasploit
→ help - show help.
→ show [Somethings]
→ use [Somethings]

- set [option] [value] → "Know"
- exploit → runs the current task.
- use nmap and use it
- search online

Metasploit

Community (Gui)

→ download it from =
https://www.rapid7.com/product/metasploit/metasploit-community-registration.

→ Change the permission to executable JSP

→ Run installer

→ once metasploit community is installed
// # Service metasploit start

→ go to https://localhost:3790 in a browser → enter your product key

→ u can perform PSQL and all attacks

Defence

Nexpose

→ Download it from . http://www.rapid7.com/products/nexpose/compare-downloads.jsp

→ try all products.

→ before installing Stop psql
service postgresql Stop

→ execute the setup.

→ follow internet → modify all

usage

→ before running
service postgresql Stop

→ # ~~chsc~~ sudo su

→ # ./nsc.sh

→ copy the url

→ login

enter the product key

Gui (no prob)

this can be used to generate the reports

CSS

Gimp

→ P - paint brush

→ n → pencil

→ play bro.

bash

types

→ Z Shell C Shell

→ k shell KSh → Korn Shell

→ bash Shell etc

→ TCSh

→ Sh

DATE

Kernel

→ controls hardware and software

→ it is a program which loads the system to be b...

→ OS = Kernal + Shell

→ Software = Shell + application

Shell

→ ~~echo~~ how to find

→ echo $0 ⇒ tell what type of shell

→ cat /etc/shells ⇒ available shells.

→ ~~etc~~ cat /etc/passwd ⇒ your shell

Shell Script

→ Programming

Types of Shells

→ Dos = MS Dos = has Gui (except MS...

→ Gnome = has Gui

→ KDE = has Gui

0 - zero

DATE

Sh = command line

bash

csh and tcsh (Stay away from it)

ksh (advance)

Starting a Shell (open terminal)

find the current shell

$ echo $0

you can start Sh Shell by

$ sh

$ echo $0 //(verify)

$ exit //(to exit)

$ → C Shell

$ csh

$ exit

→ ksh

$ ksh

$ exit

PAGE

classmate

Script file permission

→ permission only for ~~root~~ . Sudo su

chmod +x . script-name

→ permission for all

chmod a+x script-name

→ Checking permission

Define shell

→ #i/bin/bash

→ use vi (or) nano (or) ~~subli~~ plume

Scripting.

// hellow world program

• #!/bin/bash

echo

echo hello world

echo

basic

#!/bin

echo

echo

echo

~~echo~~

echo

~~ech~~

echo

who

echo

date

echo

cal

echo

touch

echo

echo

basic task Scripts

#!/bin/bash

echo

echo this script will run few basic task like

echo pwd =

~~echo~~ ~~ls~~ pwd

echo ~~who~~ ~~ami~~ ls =

~~ech~~ ls

echo whoami =

who ami

echo date

date

echo cal

cal

echo Creation of 3 files with message

touch a.txt

echo this is a message ~~>touch~~ >> a.txt

echo print the message

cat a.txt
echo "that's all"
echo

Debuging

→ press Esc
: (enter the line number)

→ press Esc // to quit and save
: x

→ press Esc // to just quit
: q

Basic administration task program

```
#!/bin/bash
# echo
echo "Admin tasks"
echo
top # this checks the system usage
```


top | head -
echo
df -h
echo
uptime # di
echo
iostat
echo
free -m
echo
#
Usage of
#!/bin/b
p=`pw
l=`ls`
w=`wh
d=`dat
c="ca

top | head -10 # gives top lines of sys usage

echo

df -h

echo

uptime # displays when the sys was started on.

echo

iostat

echo

free -m # checks free memory

echo

#

Usage of variables

#!/bin/bash

p=`pwd`

l=`ls`

wi=`who am i`

d=`date`

c="cal 2018"

echo
$ p
$ l
$ wi
$ od
$ c

Input Output

```
#program to print name
echo
echo Enter your name
echo
read name
echo
echo $name , hello
a=`hostname` #it is pre defined who is log
echo
echo this is $a computer.
```

C = Baba #no ' colon is use because it is
// value not a Key word.

Conditional Scripts

if else → if ... then ... else

= = ⇒ -eq ⇒ = =

-e => if the file exist

if then Scripts

Check variable

```
# !/bin/bash
. Count = 100
if [ $count -eq 100]
then
    echo count is 100
else
    echo count is not 100
fi
```

Syntax

```
if [condition]
then
    Statements
else
    Statements
fi  #Determineds end of the Statements.
```

Check if the file error.txt exist

```
#!/bin/bash
clear
if [ -e /home/iafzal/error.txt ]
then
    echo "file exist"
else
    echo "file does not exist"
fi
```

Check if a

```
#!/bin/bash
a=' date '
if [ "$a"
then
    echo
else
    ech
fi
```

yes or

```
echo "
read
echo
if ["
then
echo
```

Check if a varible value is monday.

```
#!/bin/bash
a=`date | awk '{print $1}'`
if [ "$a" == Mon ]
then
        echo today is $a
else
        echo today is not monday, $a
fi
```

yes or know

```
echo "Do you love Bada"
read like
echo
if [ "$like" == y ]
then
echo you are cool
```

elif [" $like" = n]
then
echo you should try Beef
else
echo nikal lowday paheli fursat may
echo nikal

fi # ends here

Comparison operators

-eq ⇒ equal for numbers
== ⇒ equal for letters
-ne ⇒ not equal for numbers
!= ⇒ not equal for letters
-lt ⇒ lesses than
-le ⇒ lesser than or equal to
-gt ⇒ greater than
-ge ⇒ greater than or equal to.

file operations

-s ⇒ file exist and not empty

-f ⇒ file exist and not a directory (folder)

-d ⇒ directory (folder) exist.

-x ⇒ whether file is executable

-w ⇒ " " " writeable

-r ⇒ " " " readable

Note

⇒ if [Condition]

↳ space ↲

Same for elif.

⇒ you should be case sensitive

⇒ you should be space sensitive

Case Scripts

Syntax

```
#! /bin/bash
echo statement
read input
   case $input in
choice 1) Statement ;;
choice 2) Statement ;;
choice 3) Statement ;;
*) default Statement ;;
esac
```

eg

Command running using case

#! bin bash
echo
echo
echo
echo a
echo b
read
case
a) date;
b) ps;
c) pwd;
d) up
*)
esac

```
#! /bin/bash
echo
echo pls choose one of the options below
echo .
echo 'a = Display Date and time
echo 'b = files and dir '
"      'c = list of users logged in'
"      'd = check sys'cmd time'
read choice
case $choice in
a) date ;;
b) ps ;;
c) pwd ;;
d) uptime ;;
*) invalid echo no choice
esac
```

esac means → end of script and case

0 = zero DATE

Exit Status

→ when a program gets executed successfully it returns 0 it can be used to run next command

eg: if update is done upgrade it.

echo $?

0 # means last command was success

1 # minor problem

2 # Serious problem

3 # everything else - error.

eg of usage

Sudo apt update data

if [$? -eq 0]

then

Sudo apt upgrade

fi

which →

Cat usage

Cat

print

Cat <

lines

a

prints

if (($

#!

which → this shows the path.

: ' → multiline comments.

Cat usage

Cat file name

~~print~~ prints the text inside the file

Cat << a

'lines

a

prints multiple line

if (($c < 9))

DATE

and , or , not

and

if ["$age" -gt 18] && ["$age" -lt

if [["$age" -gt 18 && "$age" -lt 40]]

if["$age" -gt 18 && "$age" -lt

if ["$age -gt 18 -a "$age" -lt 4

→ all are same for and operator

for or , it can be replaced by

|| , -o

classmate

PAGE

while

```
#/bin/bash
number=1
n=0
while [ $n -lt 10 ]
do
        echo "$n"
        number=$((n+1))
done
```

until

```
number=1
until [ $number -ge 10 ]
do
        echo $number
        number=$((number+1))
done
```

both are same but
different loops

for

```
for i in 1, 2, 3, 4, 5
do
    echo $i
done
```

```
for i in {0.... 20}
do
    echo $i
done
```

```
for i in {0..20..2}
    #{start .. ending .. increment}
do
    echo $i
done
```

```
for ((i=0; i<5; i++))
do
    echo $i
done
```

break and continue

break is directly used

```
if (condition)
then
    Statement
    break (or) continue
fi
```

break exits loop
continue skips particular condition

Arguments

while executing $0 $1 $2

```
# ./do.bash arg1 arg2 arg3
```

args is pre defined

args = ("$@")

unlimited arguments

echo $@ # prints all arguments

echo $# # prints no of arguments

Exporting Varible

ds.sh

message = "hello"

export message # the message varible is exported.

./secondscript.sh

arithmetic operations

$((n1+n2))

$((n2*-n2))

$((n3/n4))

$((n4*n5))

$((n5%n6))

use of -n = new line

DATE

1:20:35

hex → Deci

using Bash → bc → calculator

#! /bin/bash

echo "Enter Hex number of your choice"

read hex

echo -n "the decimal value of $hex is:

echo "obase=10; ibase=16; $hex" | bc

bc

$hex "/bc

function declaration

Syntax :- function funcname()
{ statements }

eg function echobash()
{ echo bash }

PAGE

classmate

DATE

Calling a function by its name

1:58:40

Email using ssmtp

→ Lower the Security apps ~~ong~~ in google

→ Sudo apt install ssmtp

→ --help.

Curl direct download

→ usage man curl

→ usage curl --help

→ curl "url." -O# url should download

classmate

PAGE

curl "url" -O # to download it is #current directory

curl "url" -O file name # downloads in a new file ↓

curl "curl" > location # a specific location (local directory)

grep

→ Sudo apt update | grep completed.

→ --help

→ man.

Objectives

→ try to make ping command.

→ use cron. and email it or notify

CRON

→ go to the directory where the script is
→ crontab -e #in that script dir.
o enter
min hour day of month month day of week

Syntax

min hour day of month month day of week location of script

eg

24 20 * * * /home/run.sh
> file to save in location

#* = run every day weekdate ...

One page at time

Syntax ⇒ cmd | more.

⇒ Chown or chgrp change ownership

bash

For loops

Read number with sleep (time delay)

```
for i in (1..10)
do
    echo $i
    Sleep . 1 . # reads . 1 number per sec
done.
```

Combining the 2 or more files

- cat file1 file2 file3 > file4

Split 1 in to multiple file

Split -l 300 file.txt file2.txt

output will be

file2.txta

file2.txtb . . .

Copy file to a remote host.

→ Ftp is used or scp is used.

Script.

```
#! /bin/bash
# This is a script to copy file to remote host.
~~for i in ip range~~
ip=(192.168.1 ..192.168.22)
for i in ip
do
    scp Somefile ~~Some file~~ $i:/tmp
done
# (OR)

for i in PC1 PC2 PC3
do
    scp ~~Some file~~ Somefile $i:/tmp
done.
#pc1, PC2, PC3 has IPs of computer.
```

Linux file Editors

DATE

- Vi → ed → ex → emacs
- pico → Vim

Keys used in Vi

Esc - Escape out of any mode

i - insert

r = replace

d = delete

:q! = quit without saving

:x" = Save and quit

System Utility Commands

- date # displays date
- uptime # displays when was System turned on
- hostname # " host name
- ~~uname~~ uname # " type of OS
- which

PAGE

classmate

→ Cal # calendar
→ bc # calculator.

Aliases

→ it is used to cut down the big commands into small

→ eg

alias ls = "ls -al
alias pl = "pwd ; ls"
// tell = "who ami ; hostname ; pwd";
// dir = "ls -l | grep "d"
// Wpa = "chmod a+w"

Ftp

Command usage

Ftp Ftp. ip. Com # com, s required # if, it is on website

Terminal commands

1. clear
2. Exit
3. Script
4. Su
5. Sudo Su
6. Su username

Power Shell

→ Bat + cmd + terminal + Bash ++ Powershell (unique)
= power Shell

→ get -host # this gives Details of ur shell
→ get -help # help
→ get -process # prosser list
→ get -Command # all command list
→ get -~~alias~~ alias # all alternative cmd

Android Studio

DATE

Observation

from here you should observe and attack Power is the out come of all Power.

classmate

PAGE

observation.

DATE

~~Calss~~ Class of IP

in binary

	First byte
A	0
B	10
C	110
D	1110
E	1111

in decimal notation

	First bite	
A	0 to 127	Big
B	128 to 191	medium
C	192 to 223	local
D	224 to 239	multicasting
E	240 to 255	Research

PAGE

DATE

for a 1st bit 2nd bit 3rd 4th

A 1st net | host 2nd 3rd 4th

B net 1st 2nd | 3rd 4th host

C net IP 1st 2nd 3rd | host 4th

D full address

E full address

Defaut Sub net mask

Subnet mask for a

255 . 0 . 0 . 0

B

255 . 0 . 0 . 0

255

classmate

PAGE

C

25

Router

A N

C

DATE

255:255.255.0

Router finds the type of address by AND operation.

PAGE

classmate