S.H.E.L.L.

SECURITY IS AN ILLUSION

Who Are We ?

Secure **H**ack **E**xploit and **L**earn with **L**inux aka S.H.E.L.L is the ethical hacking club of VNIT.

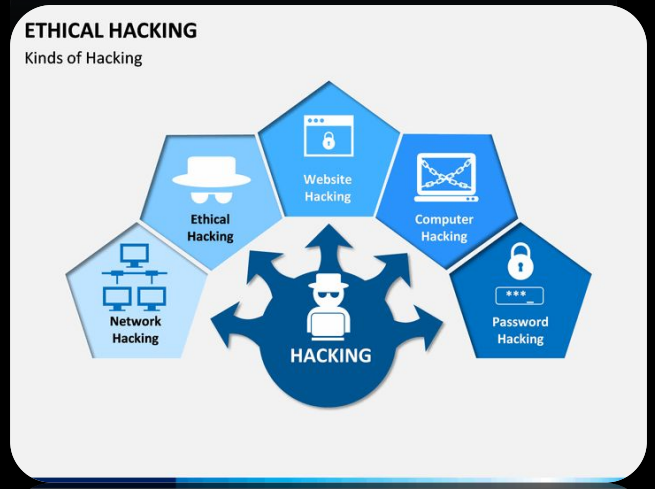
We at S.H.E.L.L. unravel numerous mysteries as we guide our colleagues through various challenges to build a secure future. Buckle up as we ride down the lanes leading us right from the basics of Linux commands to Pwning executables. We host workshops and participate in Capture The Flags to demonstrate and enhance our understanding.

Security is an illusion;
And we are the illusionists.

What is Ethical Hacking ?

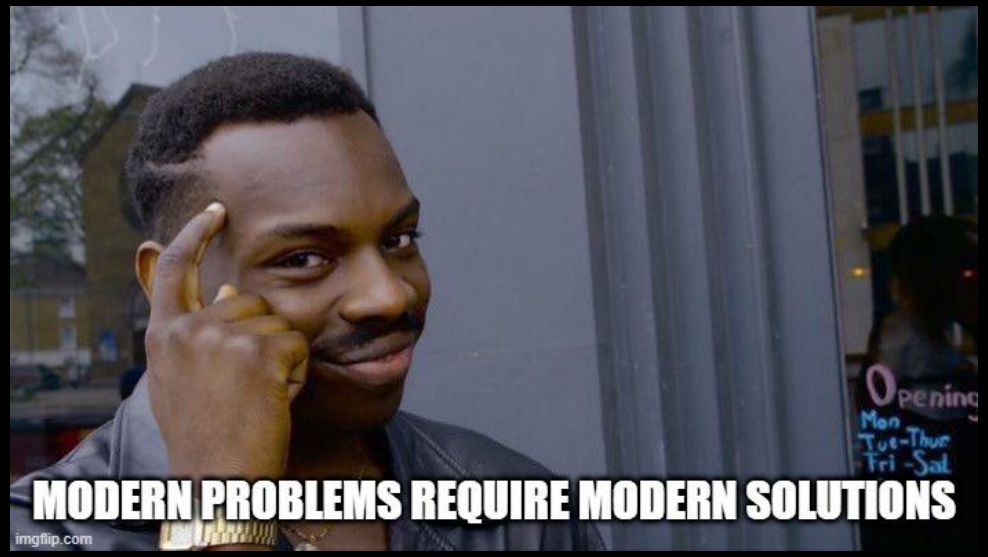
Hacking is an art of identifying weaknesses in computer systems or a network to exploit the security and gain access to personal data of a individual or a corporation.

Accessing someone's data without their permission is a criminal offence. Corporates often hires individuals to find vulnerabilities in their system which is legal .



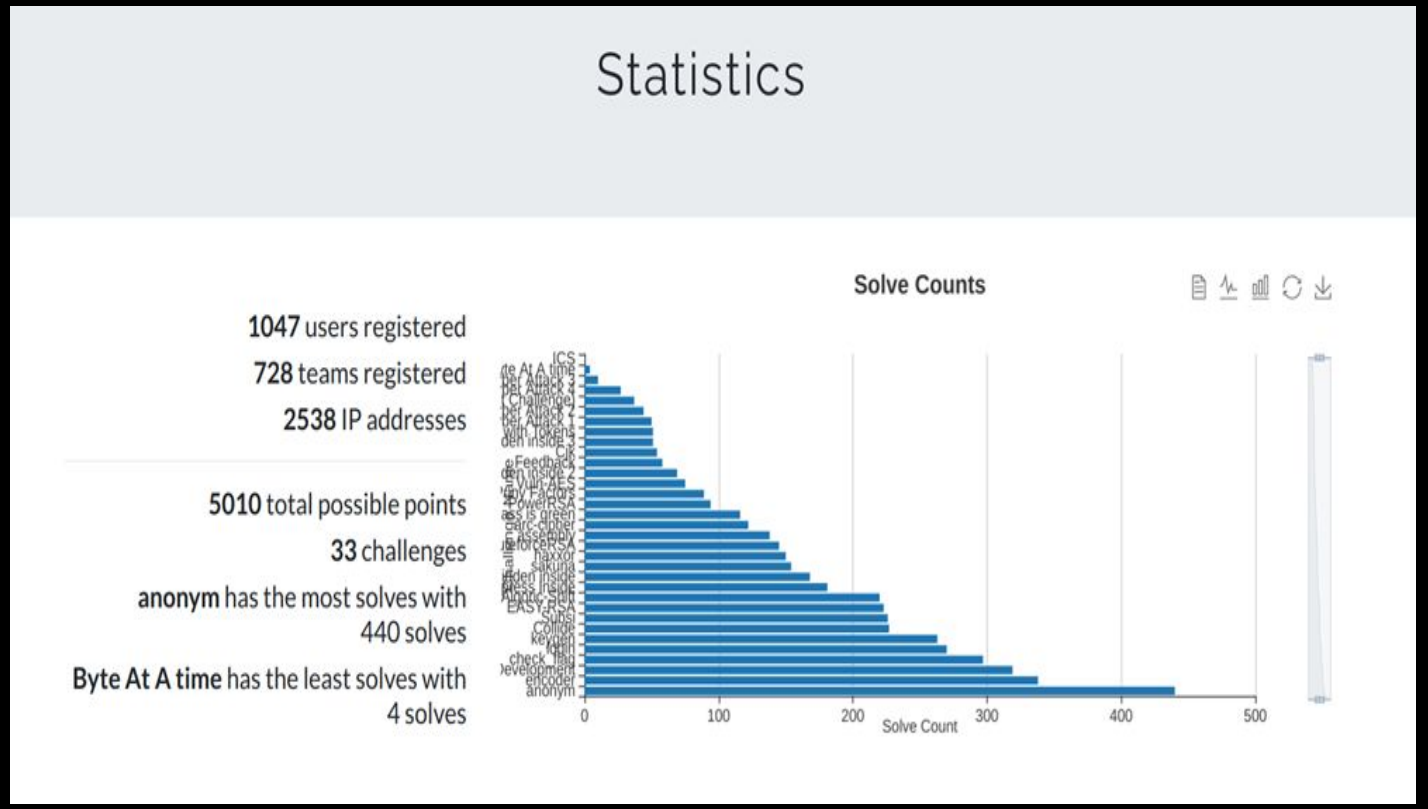
Why should one hack?

In last few years ,cyber threats have been increased which has inflict damages totaling $6 trillion USD globally in 2021.Number of Corporations take security lightly which results
in paying ransomware to cybercriminals . As a result, there are more than 3.5 million (350 % as compared to 8 years ago) jobs vacant in cybersecurity and predicted to boom by 2025.



Events organised by us

- Workshops on different topics of cybersecurity.
- SHELLCTF 2021, A Jeopardy Style CTF-event.



Sponsors

Google Cloud

PentesterLab

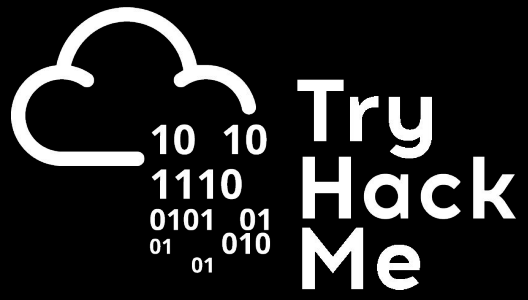
Conferences

How We Learn & Practice

We learn through various courses by great cyber security specialists like TCM

We use platforms like

TryHackMe



Hack The Box

Categories

- Linux Fundamentals.
- Bash scripting & Python.
- Web exploitation.
- Cryptography.
- Reverse Engineering & Binary Exploitation.
- Forensics

Linux Fundamentals

Linux is a family of open-source operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991.

Linux has several distros like ubuntu,kali,arch etc, each providing different features and functionalities.

Linux being open source,and having low requirements make it superior than others.

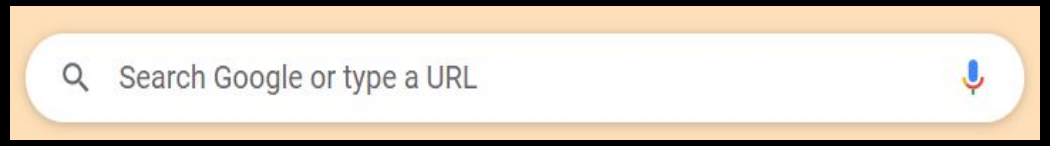
Bash scripting and Python

If you want to write same bunch of codes or commands again and again it would be a tedious task. to remove this tedious labour work we wire python scripts and exploits in bash and reuse it as and when needed.

This skill is useful in every category of hacking, helps you perform a particular task while not appearing suspicious to the Security of the system.

Web

First of all web is a category of cyber security which deals with security of web application (Web application are nothing but website google,facebook,shopping sites, bank sites all comes in web). These vulnerabilities may exist in login form, search bar in various sites, user profile sections, photo/upload options, etc.



Ig everyone is familiar with this search bar. There existed an XSS vulnerability as a result google paid $1000 for person who found this bug.

Next Big software Giant , there existe vulnerability in authentication mechanism, this bug gave ability to fully controller more 1 billion users of it. Team who found was awarded with $15,000 bounty

SCAM

What Ethical Hackers do in web security

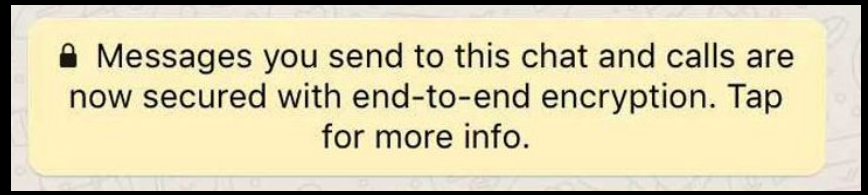
Cryptography

- Cryptography is a technique which converts a plain text into unintelligible text such that no unauthorized person can understand it.
- Job of ethical hacker is to make sure that the algorithm or how we are encrypting the data is not easily breakable with any computational power of our computers.

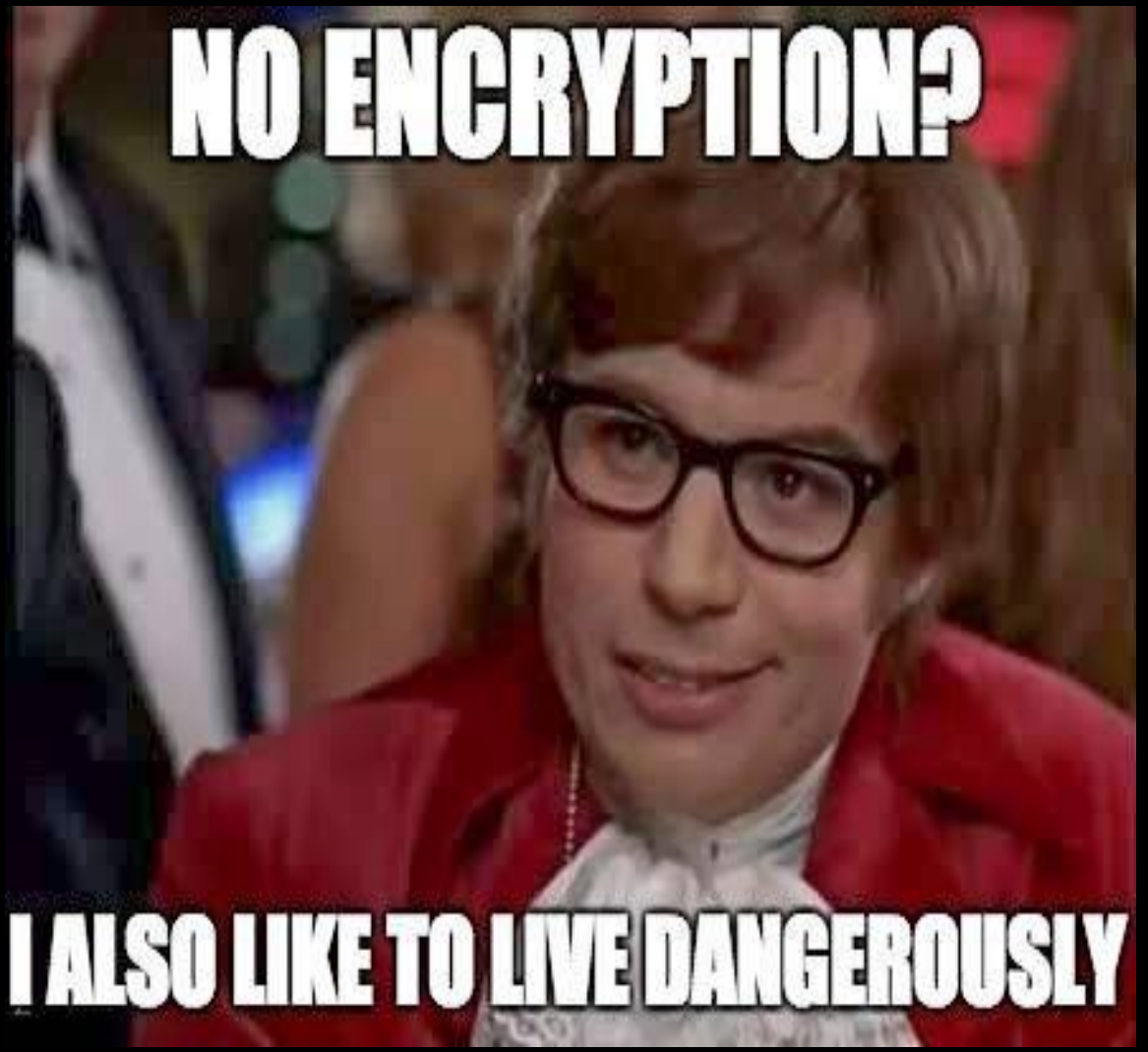
`Caesar Cipher`

```
text   : i use arch btw
shift : 4
cipher: m ywi evgl fxa
```

Real Life Examples




I WILL FIND YOU
AND DECODE THAT MESSAGE


NO ENCRYPTION?
I ALSO LIKE TO LIVE DANGEROUSLY

Reverse Engineering and Binary Exploitation

Reverse engineering (or reversing) involves taking an executable and figuring out the underlying algorithm/software behind it. Useful for finding the purpose of suspicious executables, recovering lost documentation etc.

Binary exploitation (or pwning) works on the principle of turning a weakness into an advantage. It involves finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

A basic program

```c
#include <stdio.h>

int main()
{
    printf("Hello World\n");

    return 0;
}

```

Disassembled exe

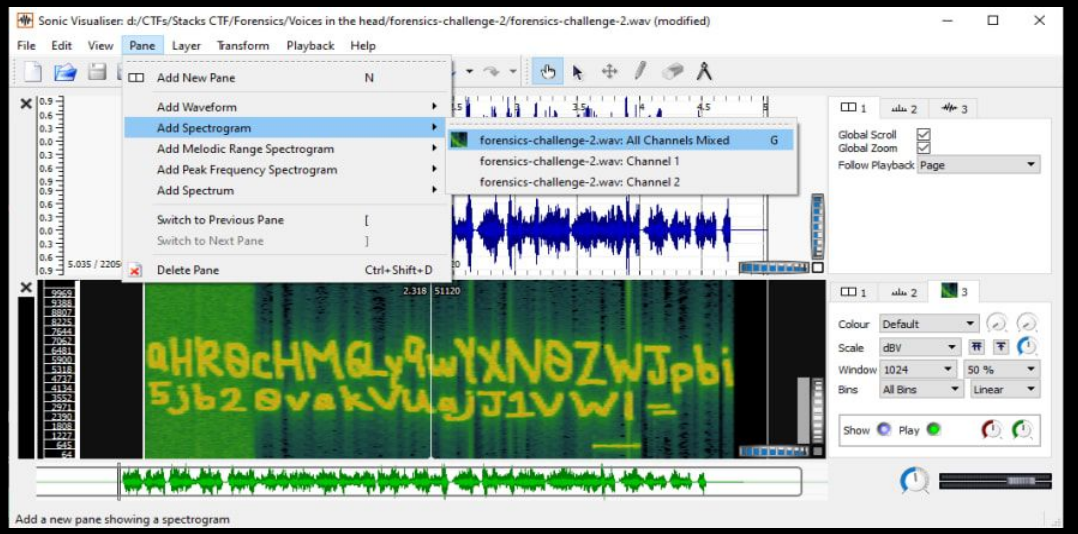
```
Dump of assembler code for function main:
   0x0000000000001149 <+0>:     endbr64
   0x000000000000114d <+4>:     push   rbp
   0x000000000000114e <+5>:     mov    rbp,rsp
   0x0000000000001151 <+8>:     lea    rdi,[rip+0xeac]        # 0x2004
   0x0000000000001158 <+15>:    call   0x1050 <puts@plt>
   0x000000000000115d <+20>:    mov    eax,0x0
   0x0000000000001162 <+25>:    pop    rbp
   0x0000000000001163 <+26>:    ret
End of assembler dump.
```

Decompiled exe

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  puts("Hello World");
  return 0;
}
```

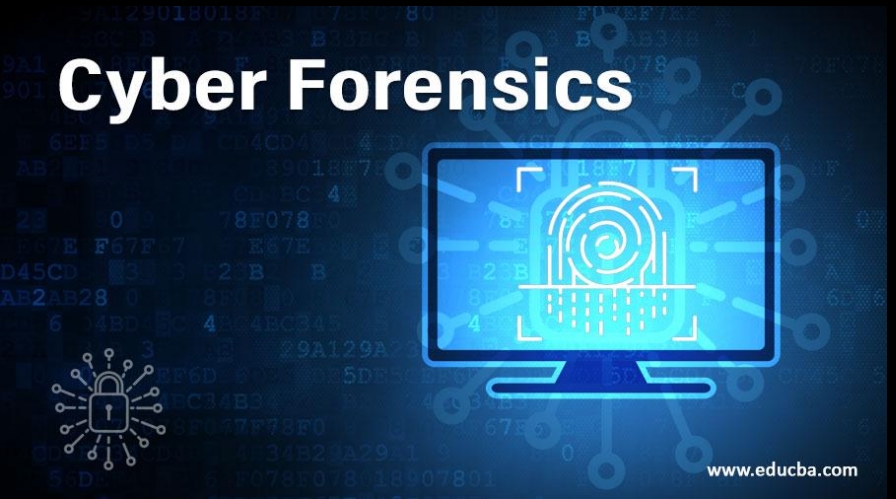
Forensics

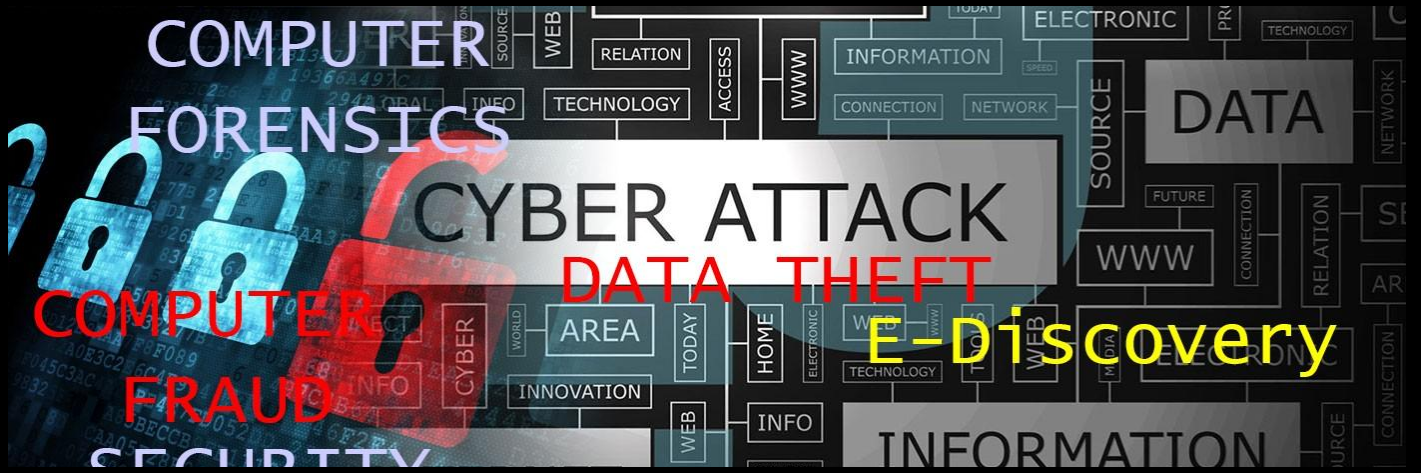
- A field which resembles the working style of Sherlock Holmes. You actually have to dig into things using various tools.
- It has many subdomains like:
  Image forensics ,Data forensics,file format analysis , steganography, memory dump analysis, network capture analysis etc.




What's actually there
what we see
imgflip.com


HACKING DETECTED
RISK ALERT


Cyber Forensics
www.educba.com


COMPUTER FORENSICS
CYBER ATTACK
DATA THEFT
COMPUTER FRAUD
E-Discovery
DATA
INFORMATION
WWW
TECHNOLOGY
NETWORK
CONNECTION
AREA
INNOVATION
SECURITY

How to join shell?

01

We will learn about all fields of cyber-security in depth

Workshop

SHELL CTF 2022

Here you need to apply the concepts you learned in workshops and solve challenges in CTF

02

03

After the CTF, you will be interviewed

Interview

Achievements

- Attempted numerous CTFs all around the year
- 32nd rank in INCTF Nationals .
- 28th in India , 434th worldwide on CTFTime.
- Attended NULLCON 2019CIA Conference (CIACON),
- HITBCyberWeek, DCS2020, Hardwear.io
- Red Team Village,C0c0nv 2020, Hack the
- Capitol 3.0, ICS Security Riscure Hybrid
- Workshop, TryHackCIT Virtual
- Cybersecurity Bootcamp, CTF
- Hackoverflow, ICS Village and so on.

Where you can find us

https://medium.com/shellpwn

https://github.com/S-H-E-L-L

https://ctftime.org/team/65394/

https://in.linkedin.com/company/shell-vnit

Any Questions ?


Are you ready for the thrill?

Thank You
Keep Hacking…