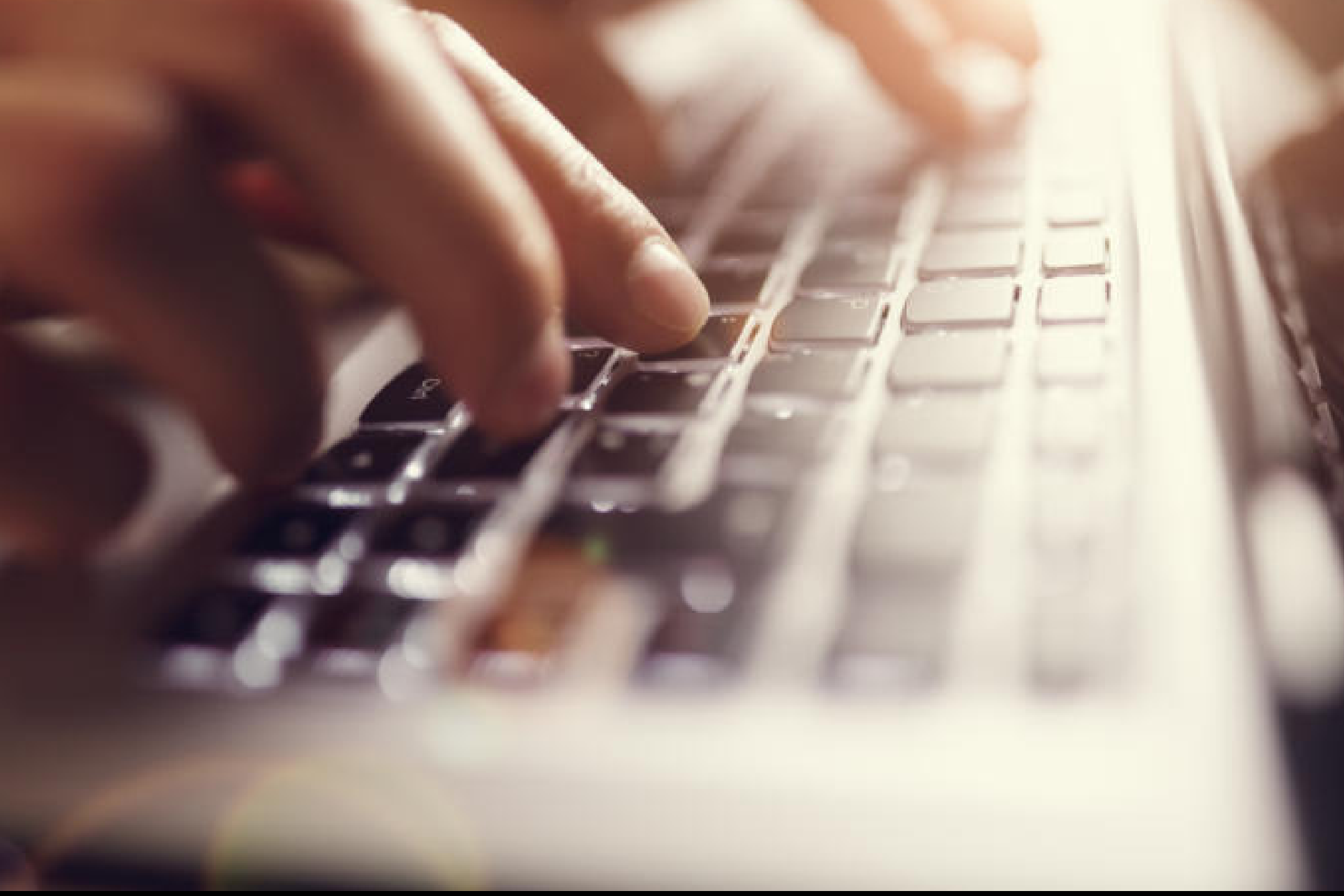
Password hacking

Team Nikist

KEYLOGGERS

Hello everyone, In this eBook, we are going to learn hacking and counter-measures to protect ourselves from the attack of hackers. In the chapter first, we will learn about key loggers and ratting. Key loggers are basically software to monitor, track and save the key strokes that are pressed on the device in which it is installed. This needs to be installed directly or indirectly in the device.

Many key logging software are available for free over the internet for windows, Mac, Android and iOS. Anyone can easily download them from there.



Key loggers save each and every keystroke that is pressed on that device, the text that is copied and paste and even all the web addresses that are visited and the running applications also. And they deliver all those data to you on your email too.

It is very easy to install key loggers. Just download and install it as you setup any other app. And you can even hide key logger, so that it is not visible on the system and not even in the installed softwares list.

You can determine that keylogger is installed in your system if you closely monitor the program files in the C drive. Any folder that you are unable to recognize can be keylogger software. You can delete that folder to stop its functioning. You should definitely check after you have given any other access into your system, either for repair or something.

There are many more features available if you buy the advanced versions of those software. Like capturing emails and screenshots also. Software like mspy.com are available to install keyloggers on android and iOS.

You can also hack someone's whatsapp. For this you can install mspy and hide it from the device of that person. You will be provided access to call logs, messages, contacts, battery level, Wifi access etc.

So, Beware of such software as you can also be hacked using the same software. So first protect yourself from it, then hack into anyone's account.

You should not access any of your banks, Gmail, face book or any other account from public computers or anyone else's computer. You should first secure yourself from this type of software. In your android device, you will have root it and then search for key logger software through the file explorer using any root system app. You can also guess passwords, to know more about some guessing tips, head on to our next chapter.

2

GUESSING

In the last chapter, you read all about key loggers, now in this one, we will see how we can guess someone's password. Most of the people use very general passwords so that they do not forget, and also because they aren't much creative as the young minds.

Research says, the most common password around the globe may be 123456, qwerty, abcd, password, abcd123, letmein, dragon, iloveyou, trustno1, monkey, baseball, sunshine, welcome, 123123, ninja, Ashley, Jesus, football, mustang and many more.

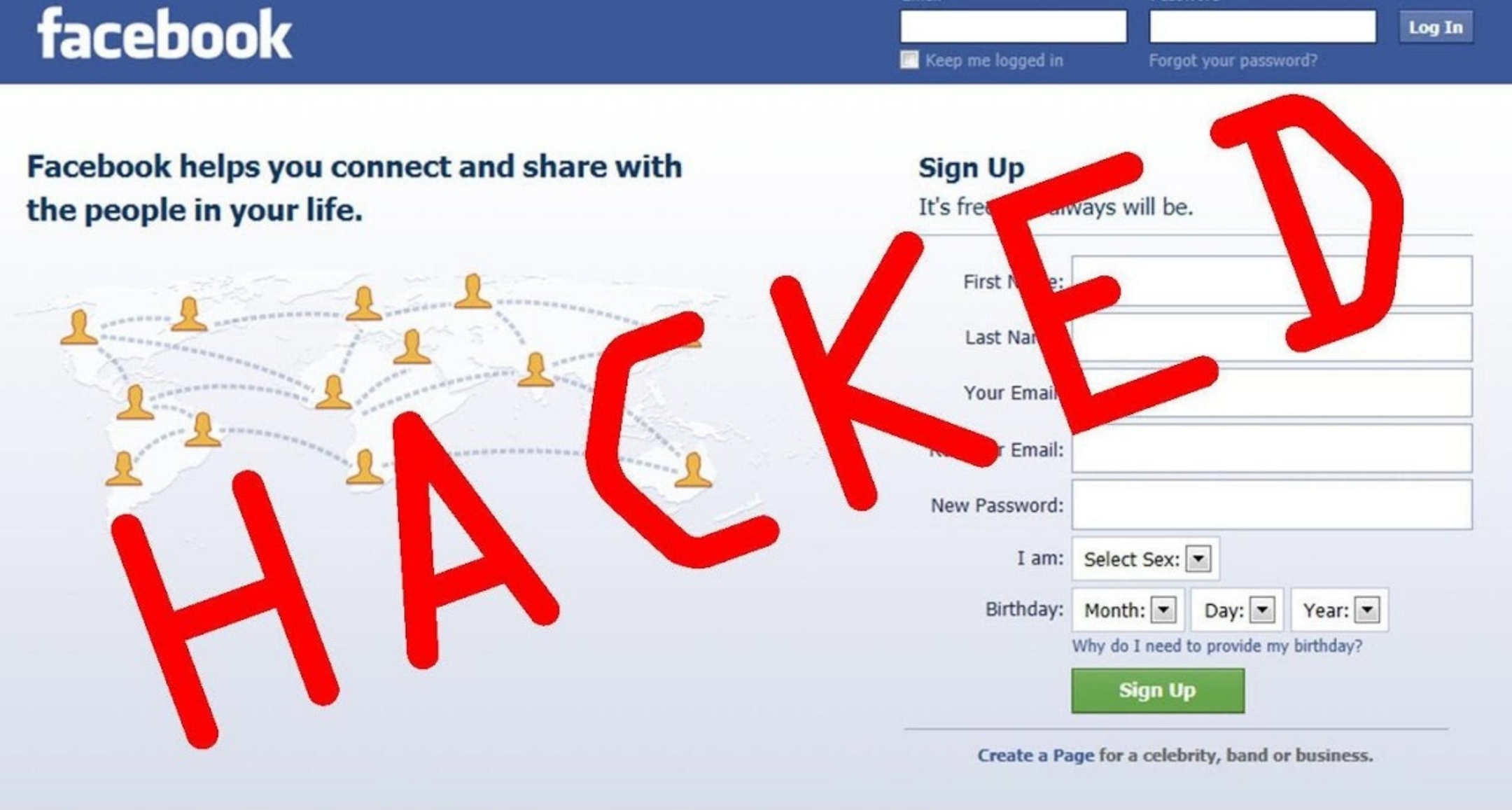
People also set their passwords based on their personal information, like their date of birth, phone number, pet's name, spouse name, spouse's date of birth or phone number, anniversaries, where they live, favorite TV show, best friend, favorite character etc.

For guessing any password, you need to know some tricks, as there are more than 50% chances that it will have one or more vowels. If it has a number in it, it can be 1 or 2, and will be at the end. Any capital letter will be in the beginning, generally followed by a vowel. So, Make sure, you do not set such a password which is this easy to guess, as just like you, there are many people out there to hack your account too.

BRUTE FORCE ATTACK

Now let's learn about brute force, it is a trial and error method to decrypt any encrypted data like password, PIN numbers etc. For this you have to install software, Kali Linux is a powerful tool used for brute force and phishing.

It can be easily downloaded over the internet, as per your system. Plugin pen drive with at least 4GB of space and Install it with PowerISO Software; it is also available for free on the internet and boot with the USB drive and in few minutes, it will be ready to use.



To hack Facebook, in the kali Linux software install python mechanize from the terminal by apt-get install command, once installed, keep facebook.py as home directory by python facebook.py command. Now enter username, email or phone number of the account you want to hack, and attach the link of a separate txt file, which have all possible password for that account. Now as the process starts, it will try all the passwords and will give you the correct password for that account.

But beware; you can also be a victim such type of password attacks. What you can do is, change your passwords regularly, and avoid keeping very easy and guessable passwords, keep your passwords strong by using combination of special characters and numbers. Keep it in your mind, and do not write down it anywhere just to remember it. Enable notification settings for Facebook, for preventing brute force attacks. Be alert and conserve yourself, as your safety should be the first priority. Now continue to our next chapter to know more about brute forcing. See you there.

```
AVE_CONFIG_H -I. -I. -I../../in
 -pipe -O2 -march=native -D_LA
r-arith -Wbad-function-cast -Wm
 -march=native -c file.c  -fPIC

le x86_64-pc-linux-gnu-gcc  -DH
nclude  -I./ref  -I/usr/include
Wall -Wmissing-prototypes -Wpoi
rations -Wnested-externs  -pipe
est -f 'sel.c' || echo './'`sel

AVE_CONFIG_H -I. -I. -I../../in
 -pipe -O2 -march=native -D_LA
r-arith -Wbad-function-cast -Wm
 -march=native -c sel.c  -fPIC

le x86_64-pc-linux-gnu-gcc  -DH
nclude  -I./ref  -I/usr/include
Wall -Wmissing-prototypes -Wpoi
rations -Wnested-externs  -pipe
lo `test -f 'sel-gram.c' || ech

AVE_CONFIG_H -I. -I. -I../../in
 -pipe -O2 -march=native -D_LA
r-arith -Wbad-function-cast -Wm
 -march=native -c sel-gram.c  -
```

```
  1  [||||||||||||||||||||     6
  2  [|||||||                  2
Mem[||||||||||||||||||103/2
Swp[|                      7/153

  PID USER      PRI  NI  VIRT
 7583 paludisbu  20   0  8652
   72 root      20   0 19132
  271 tureba    20   0 23928
14177 paludisbu  20   0  6952
12147 root      20   0  480M
16659 tureba    20   0 14272
14030 paludisbu  20   0  6980
  235 tureba    20   0 76444
 7584 root      20   0  118M
  994 tureba    20   0 29212
26696 root      20   0  118M
F1Help  F2Setup  F3SearchF4Filt
```

```
README                 autom4te.cache
Rules                  build
[11:04:40|1023] (tureba@exbull
tre)
[11:04:46|1024] (tureba@exbull
mpi)
AUTHORS    Makefile.am
Doxyfile   Makefile.in
HACKING    Makefile.ompi-rules
INSTALL    NEWS
LICENSE    README
Makefile   README.JAVA.txt
[11:04:46|1025] (tureba@exbull
mpi)
[11:07:11|1025] (tureba@exbull
1025][11:07:32|1025] (tureba@e
5 ~/om[11:[11:09:44|1025] (tur
[11:09:52|1025] (tureba@exbull
```

```
ative"
ive"
sh <<   9% :   1:  1
```

3

BRUTE FORCE

From the last chapter, you got an overview about brute force; here we will discuss it in more detail. So, in simple words, brute force is a hit and trial technique used by applications to decode passwords and pins. To learn hacking through brute force, all you need is a laptop with 1.5 GHz processing speed, a secured Wi-Fi network, and a Kali Linux OS, which you already know by now.

Now, you can also hack Wi-Fi passwords using brute force, for this, you have to boot into Kali Linux software using your bootable pen drive, after pressing F10 or whatever your system requires, while booting the system. In the terminal, To get the wireless card interface name, run command iwconfig, mostly you can get it by name wlan0. Now put the wlan0 in monitor mode using airmon-ng start command, It will give you the monitor mode interface (mostly mon0).

Now to find the BSSID (Basic Service Set ID) of the router, use command airodomp-ng wlan0, a list will appear and when you find the router which you want to hack, stop refreshing of the list by CTRL+C. Copy that BSSID and use it with the command reaver -i mon0 -b (BSSID) -vv. Now let the reaver hack the password for you. Take rest as this process can take time from 4 to 12 hours also, it depends on the strength of the password. After the completion of this process, you will get access to the password of that Wi-Fi network.

Yes, it is this easy to crack any Wi-Fi passwords, But, you do not have to worry you can easily save your router from this type of brute force attack. What you have to do is to check whether your router supports WPS, If not, then it is better but if yes, you can disable the WPS on your route. You can also filter the list of MAC addresses of the devices which you want to connect to your router, but that is not a foolproof idea as MAC address spoofing can also be done to imitate a device connected to that router.

You can also use DD-WRT Linux based firmware to protect wireless routers and access points. You can check if this software supports your router, as this has many benefits, it not only protects your router from being hacked but also monitors your data usage and boosts its speed, and a lot of more advanced features.

And for preventing brute force on face book and Gmail, you know what you have to do, just turn on message notification, so that you get to know if someone tries to hack your accounts password. One more thing you should always keep in mind is that always keep strong passwords, make combinations of numbers, capital letters and special characters.

Always be safe, as there are many different ways by which you can be hacked by any professional or unprofessional hacker. Never click on links from email or other sources, as they can be duplicate also. To learn more about phishing, tune in to our next chapter.

PHISHING

Now after reading about brute force in the last chapter, Let us discuss phishing here. In simple words, phishing is a technique used by hackers to steal your confidential information like bank account details; passwords etc, by making you type this information in a spurious website that is especially designed to hack your information.

You already know from the previous chapter that what all you need for brute force and phishing. In phishing, you have to make a clone webpage exactly same as the webpage, in which you want the victim to enter his/her credentials.

Now, In the kali Linux software, go to applications, then kali Linux, then exploitation tools, then social engineering toolkit and finally se toolkit. From the displayed menu, select social engineering attacks and then website attack vectors and then credentials harvester attack method.

Now select site cloner, and enter your system's IP address, then it will ask you URL to be cloned (any page can be cloned, irrespective of the language in which it is written), write the URL of the page that you want to clone & press enter. In a little bit, our fishnet is ready.

While cloning a webpage make sure that you enter the original IP address, not the local one, to get it, check that your computer is connected to a Wi-Fi network. One more thing, you can change the language of the cloned website, while you enter URL write lang=en or any other language initials to get your cloned website in that particular language.

Now create a eye catching email that will attract your victim to the website and link the cloned website's link in that message and send it to the victim. Now if the victim open that link and enter his/her credentials in that page, you will get all the information in the terminal, that was entered in that page.

because one can easily retrace an IP

address in the URL. You can purchase domain name similar to the website's name that you want to clone and use for phishing. This is going to help you to distract the victim as you will mention a similar URL in place of the original web address of that particular webpage. You can also use free hosting services like my 3gb.com that provide free services which are enough to host your clone website. You just have to register in the website.

You can also use Google adwords for phishing. By using it whenever the victim searches for facebook or any other website, your spurious webpage's link will be displayed in the first place, that you have created using the Google adwords. It is very easy to create account on Google Adwords. Most of the people ignore the actual web address and just click on the first link. After the victim arrives on the fraud webpage, the credentials that he /she enters will be saved and displayed to you.

You should be aware of such frauds, as you are smart enough to recognize the difference between the original and the fake links. Always check the connection to be secured, it should be https not just http. Always check spellings in the link, if it is suspicious, do not enter any confidential information. Never set same passwords for every account. Phishing emails are easy to recognize, Avoid opening those suspicious email links. Now move on to our next chapter for information on social engineering. See you there.

5

SOCIAL ENGINEERING

So, now you probably know everything about phishing. Now we will learn something new. The art of manipulating people in order to divulge confidential and personal information such as bank account details or password from individuals, by tricking them so that it can be used for deceitful crimes, is social engineering.

Social engineering basically can be done through humans or computers. Have you ever got a call from someone saying he/she is a bank manager and want your credit card details to activate your card or cross check your account? Yes, this is a part of human based social engineering.

It basically requires collecting personal information through interaction and building trust or fear. Acting as a reputed and legitimate end user and ask for confidential information. So, keep a sharp lookout on this kind of fraud calls and persons and never share your bank account details, credit card details or any other confidential information with anyone.

The second is computer based social engineering. In this, we just use computers instead of humans to manipulate people to get privileged information. The most common source is messaging or chatting. It is very easy to use the information shared while chatting with a person, to hack into the facebook, Gmail or other social media accounts.

You can use the person's email id, then go to forgot password, it will ask you send a verification code either on your mobile number or email address, select the option where it says that you no longer have access to these, then it will ask you to add a new number or email address, for confirmation it will ask you a security question, whose answer you can easily get through social engineering and now you easily have the access to that person's account.

You can easily be prevented by the attacks of social engineering, only if you are aware of such type of frauds. Aware your family, friends and colleagues about the frauds happening through social engineering. You should also change your password periodically and keep strong passwords.

Enable the feature of account blocking after three unsuccessful attempts. Do not share a lot of information about yourself with anyone you don't know, avoid such people if you have any doubt that he/she is asking you a lot of personal questions. Do not set same passwords for all of your account. Always check the URL of the website before entering any confidential information, make sure it is a HTTPS connection.

Phishing emails can be easily guessed as they will always show urgency, the email link will be unsecure (http) and there may be many spelling mistakes in the URL. So, avoid clicking on any such fraud email links. However, somehow you can get affected by social engineering. But it is better protecting yourself from such hacking attacks.

Well, some human user to make an exception to the rules for what they believe is a good reason. Commonly exploited simple emotions, and an example of how each is exploited, include:

- Greed:- A promise you'll get something very valuable if you do this one thing
- Lust:- An offer to look at a sexy picture you just have to see
- Empathy:- An appeal for help from someone impersonating someone you know
- Curiosity:- Notice of something you just have to know, read, or see
- Vanity:- Isn't this a great picture of you?

These emotions are frequently used to get a computer user to perform a seemingly innocuous action, such as logging into an online account or following an Internet URL from an e-mail or instant messaging client. The actual action is one of installing malicious software on their computer or divulging sensitive information. Of course, there are more complex emotions exploited by more sophisticated social engineers.

While sending someone an instant message with a link that says "I love this photo of you" is a straightforward appeal to their vanity, getting a secretary to fax you an internal contact list or a tech support agent to reset a password for you is quite a different matter. Attacks of this nature generally attempt to exploit more complex aspects of human behavior, such as

• A desire to be helpfu:-l “If you’re not busy, would you please copy this file from this CD to this USB flash drive for me?” Most of us are taught from an early age to be friendly and helpful. We take this attitude with us to the workplace.

• Authority/conflict avoidance:- “If you don’t let me use the conference room to email this report to Mr. Amit, it’ll cost the company a lot of money and you your job.” If the social engineer looks authoritative and unapproachable, the target usually takes the easy way out by doing what’s asked of them and avoiding a conflict.

- Social proof:- “Hey look, my company has a Facebook group and a lot of people I know have joined.” If others are doing it, people feel more comfortable doing something they wouldn’t normally do alone.

No matter what emotional button the attacker is attempting to push, the premise is always the same: the intended victim will not sense the risk of their action or guess the real intentions of the attacker until it's too late or, in many cases, not at all.

Because the intended victims in these cases most often are working on computers inside of the target company network, getting them to run a remote access program or otherwise grant you remote access directly or indirectly can be the fast track to obtaining targeted sensitive data during a penetration test.

6

CARDING

In this chapter, we are going to know all about carding. So first of all what is carding?

Carding is generally a fraud associated with all your plastic money like credit cards, debit cards and ATM cards. It is a completely illegal act. Anyone can use your money in your bank account if they get the details of your credit or debit card like the card number and the CVV code. It is not necessary that if it is your card then only you can have the access to your account.

Now what exactly happens is some people who are known to be carders, has a whole database that has the information of a large amount of people's card details.

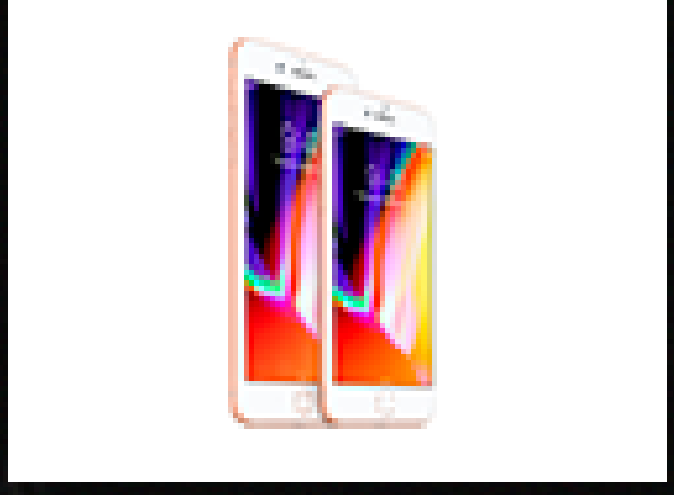
These databases are prepared by hackers who trace or steal the card details of people through any of the different means either by calling you from a fake number and profile and ask you to verify your card details or use some software that will scan your card details when you swipe it in any machine for payments and save a large amount of information as credit card dumps.

Using these details the carder will buy things online from a false identity and then sell them for cheap prices. You may have heard of such offers that you can get iphones in just ten thousand or any other good mobile in a price that is very low than the original price. All this is done through carding.

iPhone 8

по предзаказу

279$	339$
64 gb	256 gb
2 шт.	2 шт.
за 529$	за 649$



iPhone 8 Plus

по предзаказу

319$	379$
64 gb	256 gb
2 шт.	2 шт.
за 599$	за 719$

iPhone 7

в наличии

219$	259$
32 gb	128 gb
2 шт.	2 шт.
за 399$	за 489$

If you ever get a message saying that you can get any of the products in a very low cost at an advance payment of only 500, 1000 or so. Never ever believe this and do not pay any amount to anyone who says you so as you will become a victim of this credit card theft.

Protect yourself from these kinds of frauds and never believe any type of advertisements that sell you branded products at a cheaper rate. Always take care when you swipe your card in any shop, make sure that the swipe machine is a proper branded machine. If you have any doubts, ask the shopkeeper immediately, never hand over your card to the shopkeeper as it is possible that he may try to memorize your card details.

Never enter your credit card details on the web without ensuring the security of that webpage. Always recheck the URL of that website and the connection protocol should always be https. However there is no problem in entering your details onto a trusted website but you should always be alert in these cases.

So, always be aware of such fraud that are happening around you and prevent yourself from becoming a victim. As there are many hackers out there looking for an opportunity to steal your card details.

This is all about the basics of carding. Head on to our next chapter to learn how you can do carding.

7 HOW TO DO CARDING?

In the last chapter we have seen what is carding and now we know what carders do and how your plastic money is not safe in the market. In this chapter we will see how to do carding. What tips and tricks the hackers use to steal your card details and how this black market is increasing day by day with the advancement of technology.

As we know by now, Hackers create a large database which contains the card details of thousands of people. And the carders buy these from them in order to perform carding.

It is a completely illegal act but still there are many websites who sell credit card information to carders and in those websites, carders do not have any guarantee about how much money will be there in the card. One of such websites is “UniCC” It sells credit card information in various prices like 10 to 50 dollars.

Now, Basic things that you need if you want to try carding are a computer, you can also use mobile phones for carding but using a computer is more safer. A CC Cleaner, it is a tool used to clean the browsing history, cookies and flash cookies, caches and temp files. A Mac address changer, to spoof Mac address of your computer, Socks, it's used to hide your original location and help you maintain a fake location according to the credit card to make payments successful. A remote Desktop Protocol (RDP), A Drop, it's a service to get shipping address of the credit card and finally credit card details.

Now to start, first of all setup socks in your Firefox browser, this can be done in advances settings by manual proxy configuration. Make sure you use socks as per the location of the credit card.

Now create a fake email id similar to the name of the credit card holder. Make sure you do not use disposable mails. Now run RDP or change the Mac address with the help of Mac address changer. Run the CC cleaner to delete all cache and temp files. Again set up sock in the Firefox and check whether your IP is changed according to the location of the Credit card holder.

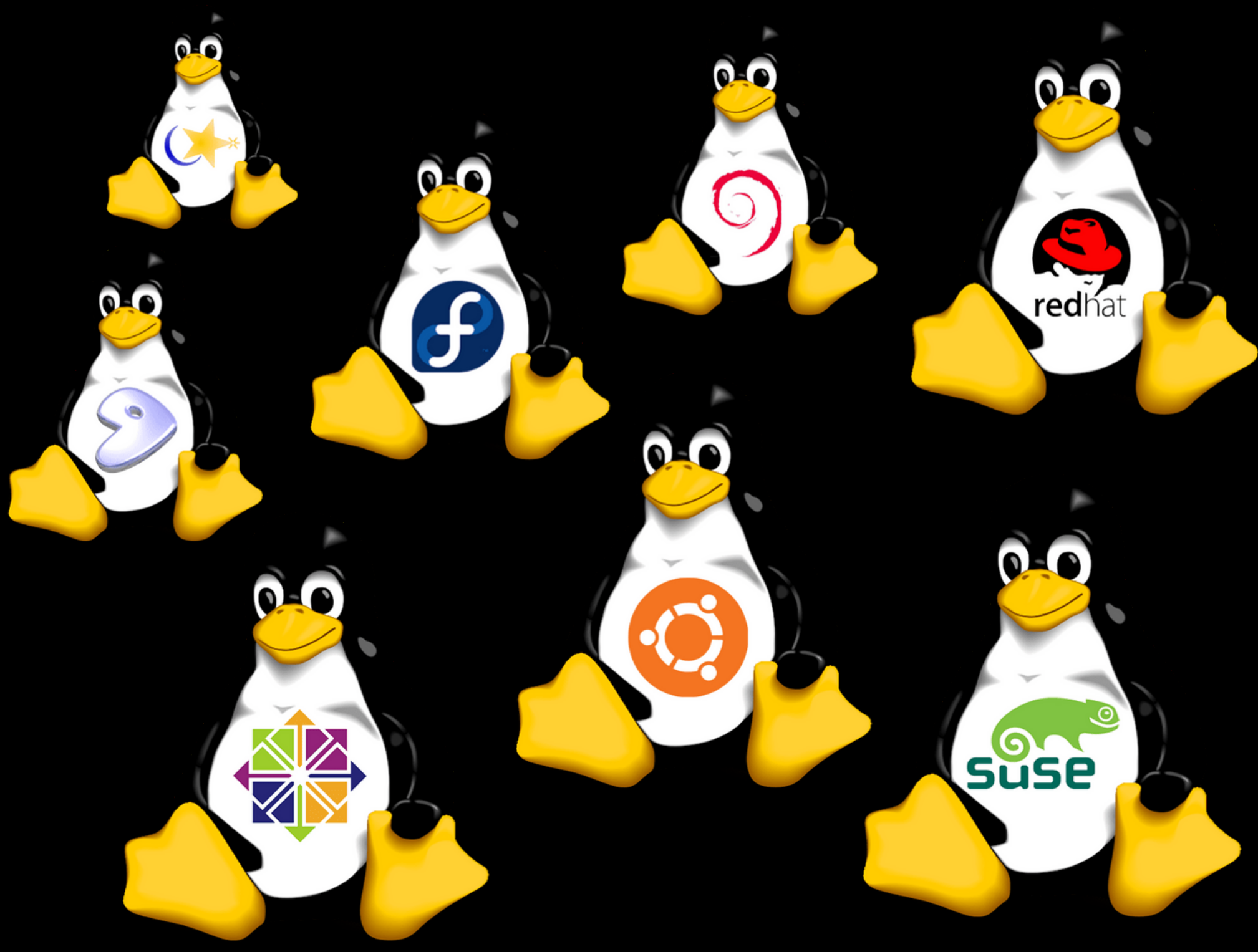
Now open any local online store (from the same country) and register yourself with the name of cardholder and email that you created for carding. Add any product in your cart. Never make large transactions on your first order.

In shipping address, enter the address you want to get the delivery. Now in payment option, choose credit card for payment and enter the details which you got from the credit card, in billing address, enter the address of the credit card holder.

Now your order will be placed. Wait for the order to arrive, if the delivery boy asks for any identity proof, be prepared with a fake id.

Never use your original identity to receive order.

So this is how carding is done. It is a completely illegal and a punishable offense. You can get on to a lot of trouble if you are caught doing carding. We do not promote such crime. The information here is only for educational purpose.



Basic Linux Exploits

Why study exploits? Ethical hackers should study exploits to understand if a vulnerability is exploitable. Sometimes security professionals will mistakenly believe and publish the statement: "The vulnerability is not exploitable." The black hat hackers know otherwise.

They know that just because one person could not find an exploit to the vulnerability, that doesn't mean someone else won't find it. It is all a matter of time and skill level. Therefore, gray hat, ethical hackers must understand how to exploit vulnerabilities and check for themselves. In the process, they may need to produce proof of concept code to demonstrate to the vendor that the vulnerability is exploitable and needs to be fixed.

Stack Operations

The stack is one of the most interesting capabilities of an operating system. The concept of a stack can best be explained by comparing it to the stack of lunch trays in your school cafeteria. When you put a tray on the stack, the tray that was previously on top of the stack is covered up. When you take a tray from the stack, you take the tray from the top of the stack, which happens to be the last one put on.

More formally, in computer science terms, the stack is a data structure that has the quality of a first in, last out (FILO) queue. The process of putting items on the stack is called a push and is done in the assembly code language with the push command. Likewise, the process of taking an item from the stack is called a pop and is accomplished with the pop command in assembly language code. In memory, each process maintains its own stack within the stack segment of memory.

Remember, the stack grows backward from the highest memory addresses to the lowest. Two important registers deal with the stack: extended base pointer (ebp) and extended stack pointer (esp). As Figure 11-1 indicates, the ebp register is the base of the current stack frame of a process (higher address). The esp register always points to the top of the stack (lower address)

The end!!!!

Thankyou for reading!!
please dm us your review in our insta page