THE ART OF HACKING

A GUIDE TO INTRODUCE YOU TO THE WORD OF CYBERSECUIRTY

HACKING
NINJA

This is the guide that will make sure you have a **hard start** in hacking and you don’t have to spend countless hours researching stuff.

Research is Great but a good **direction** is always needed.

What This guide contains:

1. Step by step guide to help you put on a **path** of learning to hack.
2. How to have a side income by **bug bounty hunting**.
3. What are different **sources** you must follow to learn about interesting things in this domain?
4. I will explain terms in **easy** language.
5. Famous attack vectors.
6. Some famous hacks of the world.
7. Myths busted.
8. All information is given with further reading. (**Links**)
9. How are other fields of computer science interacting with it ?

Who is this for :

1. Anyone who wants to learn hacking.
2. Anyone who thinks he/she is misguided by the internet
3. Anyone who wants to explore the world of compute networking / ethical hacking

What this guide is not?

1. This is not a tutorial, this is a guide. This will tell you what to do and where to find the resources to do it.
2. This guide is not a complete hacker’s playbook.
3. This is not “how to hack insta” guides.

Lets clear some things first, this is not a guide that will make you a hacking wizard in a day or two. Hacking is a skill that needs **years to practice** and this guide will put you on the right track.

If you are here to know how to hack someone’s account then again **kindly don't read this**.

If you are passionate about computer systems in general and problem solving then you are the one who should read this.

This does not contain tutorials but it's just a guide that will tell you what's what and where you can learn.

Hacking IS computer networking nothing more, nothing less.

It's not magic but it comes close to it.

FAQ

I don’t know a lot about computer science, Can I still learn ethical hacking?

Sure you can!! Anybody can learn anything! You just need consistency and a love for hacking. Follow this guide and you will be in love with it in no time.

I don’t have a good computer, Can I still hack?

Most intelligent hacks don’t need that much power or networking power. You can even launch attacks from your phones!!

What is hacking?

Hacking is a layman term for computer networking. It is basically finding loopholes / things you can take advantage of, in a system and take the control of a victim machine.

What is ethical hacking?

Detectives have to think like thieves to catch them. That's why cybersecurity testers have to think like a hacker to prevent hacks from happening. The people who only use the power of hacking for good are ethical hackers.

What is Penetration Testing?

It is basically running automated tests and providing test results for the company and providing reports on what to do to fix the loop holes they have found in the particular software / hardware.

How to use this guide?

- Read it once for an overall idea of learning to hack.
- Then I have given links everywhere, go through them. Not once but twice.
- And just follow this guide and become a good hacker and **remember all good hackers are life hackers.**

There are 2 ways you can go about learning to hack.

You can be a script kiddie and just grab tools from the web and run scripts off the github.

By this you can hack the things that have been hacked before, essentially which have exploits lying on the internet.

But you will not be able to create your own exploits and you will not be able to modify these tools to your specific needs .

So In my humble opinion learn, learn, learn and practice, practice and practice!

Lets clear some terms that cyber security people use:

1. **Victim**: the person on which the attack has been done / is going on.
2. **Vulnerability**: It is something in a program that can be taken advantage of.
3. **Exploit**: It is a software that takes advantage of the vulnerability.
4. **Persistence**: It doesn't matter whether a computer restarts, the program will be running on startup. That is called persistence.
5. **Backdoor**: It is something that stays on the software even without the knowledge of the victim and can be used to gain unauthorised access to their devices.
6. **Packet**: data packed in a nice format sent over the internet.
7. **Bruteforce**: just try everything and hope something will be hacked. (not intelligent but works if you have strong computers and network)
8. **Attack vector**: A way in which a hacker hack.
9. **Botnet:** computers hijacked by hackers to perform coordinated attacks.
10. **Firewall:** hardware / software that protects a device from cyber attacks.
11. **Attack surface:** different ways in which an attack can be performed. If ways increase, so does the attack surface.

This list is not exhaustive by any chance. But this is enough by now as we move forward I will try to explain each and every term. If you don't understand a term, well google it!!

Why learn a programming language ?

It is the language of the computers. If you ever wanted to customize tools or better make your own ones. You need several programming languages in your toolbox.

If you learn one, you can easily switch to another in no time.

Pick any:

1. **Python**: this is easy to learn and has many libraries but it lacks speed.
2. **C++**: this is speed.
3. **C**: this is more speed.
4. **Assembly**: This is the best speed one can have if you don't know how to program in binary (that is everybody). you need this for malware analysis and reverse engineering.

And It doesn't really matter which language you learn, you can change them in no time and choice of language is not important but your skills are.

Then you should learn how computers **think** (and how you think)

Data structures and algorithms

You don't need to have mastery in this subject, just learn the basics. Just know what queues, stacks, graphs are and how different algorithms like searching, sorting, dynamic algos' work. This will make your brain think in computer terms and you will be able to think of ways in which a hacker thinks!

OS, DBMS, Computer Networks

Again, you don't need PHD's in this. Just learn basic things like how OS works, what are different components of it and how they interact with each other. How data is stored and retrieved etc. Learning about computer networks is essential for any hacker as you will be dealing with networks mostly.

This will clear your basics about how computers work and you will have an overview of how things work in a computer. Before knowing how to hack it is essential that you know how the system works.

Then you may be wondering where are those tools people learn and scripts on github?

Well tools should be used to automate things. They are just a means to an end. They are not a substitute for a hacker. If that was a case you wouldn't be reading this, Right? Tools are just an extension of you, the hacker. Learn the basic ones but concentrate on learning about concepts.

These tools are essential for anyone who wants to safeguard anybody:

1. **John the reaper**: is one of the most popular password crackers of all time.
2. **Metasploit**: is actually a repository of all exploits that have been found and hopefully patched. It is also a tool that compiles those exploits and these can be deployed easily on devices.
3. **Nmap**: It's basically a scanning tool that tells you which devices are on the network and which ports are open on them.
4. **Wireshark**: it is a packet sniffing tool, what it does basically grabs whatever packet is moving through its network.
5. **Burp Suite**: this is one of the best web penetration packages out there. It basically does every test it can on a website and gives you a report.

6. **Ettercap:** this is used for MITM attacks.
7. **Aircrack-ng**: Wifi hacking tool.
8. **SQLmap:** used for testing sql injection on website
9. **WPscan:** wordpress site testing

These are just basic tools that you should be familiar with. There are many tools out there and many improvements upon these. But these are the most important ones. Exploration is the key for any hacker. Explore the cyber universe!!

Android hacking Tools:

There has been a rise in hacking by handheld devices like android.But android is just a linux system that does not have the required packages for hacking. But termux changed it all.

Termux: It is a built upon your android linux terminal and provides you with all these great tools and it comes as close to an actual linux terminal as one can. Sometimes many scripts out there will be compatible with this terminal. Just check their dependencies and OS requirements.

Fing: It is by far the best scanning tool for android

I am not including apps like wifi connect they are not hacking tools, they are just apps that don't work or are just a repo of keys that work by bruteforce.

Basic Hacking Methods:

1. **SS7**: It is an amazing hack that targets mobile networks and grabs important stuff. This is a great article:
   https://medium.com/@vasanthavanan59439/ss7-the-deadliest-attack-6423de7fe8c0

2. **Wps pixie attack:** It takes advantage of a vulnerability in wps enabled wifis. Read more at:
   https://security.stackexchange.com/questions/149178/what-is-pixie-dust-attack-on-router

3. **DDoS:** you just send random requests to a system in the hope that the system will be crashed. https://portswigger.net/daily-swig/what-is-ddos-a-complete-guide

4. **MITM:** man in the middle attack, you basically trick someone into connecting to your device and making them communicate through your device and then you can capture packets and take a look at what they are doing and grab their important stuff. Wikipedia is great for reading about stuff (not just for school projects) :

https://en.wikipedia.org/wiki/Man-in-the-middle_attack

5. **Phishing and Pharming:** in phishing, you send a url to a person and trick him/her into thinking that it is the actual website and they give their important stuff.
   Pharming does the same thing but with changing DNS records. There are many techniques similar to phishing. But the basic idea is that you pose as if you are someone else and get information you need
   https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing

6. **SQL injection:** basically you inject some code into a website and get some information about there databases. That is very dangerous if you think about it. That database can contain passwords and payment information and so on.
   https://portswigger.net/web-security/sql-injection

7. **XSS attack:** this is similar to sql injection as in this a hacker injects js scripts not sql queries. By this you can do all kinds of things.
   https://owasp.org/www-community/attacks/xss/

8. **Social engineering:** Humans are the weakest link in any system. Social engineering is one of the best hacks and one of the easiest to perform. This infographic is great:
   https://blog.knowbe4.com/social-engineering-101-18-ways-to-hack-a-human-infographic

9. **Zero-day exploit:** A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. Basically these are new security flaws that gets discovered.

The key to learn hacking or anything for that matter is to research well. After learning computer concepts, languages, tools and basic attacking methods you should be ready to actually hack stuff.

And practise is what you should do now.

Do CTF's

What are those?

Catch the flags are competitions where you hack a vulnerable machine. These are the places where you will hone your skills and will become a real hacker.

This is a great website for that: https://www.hackthebox.eu/

Now lets see some great hacks of the past!

Famous Hacks

2008 cyberattack on United States

It was the "worst breach of U.S. military computers in history". The defense against the attack was named "Operation Buckshot Yankee". It led to the creation of the United States Cyber Command.

https://en.wikipedia.org/wiki/2008_cyberattack_on_United_States

Ghostnet

is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009. The operation is likely associated with an Advanced Persistent Threat. Its command and control infrastructure is based mainly in the People's Republic of China and GhostNet has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City were compromised.

https://en.wikipedia.org/wiki/GhostNet

WannaCry ransomware attack

It was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life.

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Now lets see how different fields of computer domain are interacting with cybersecurity.

Machine Learning in cybersecurity

ML are basically algorithms that take input and output and make rules for it. It is different from general algorithms as those are defined by humans. These automatically find the functions to reach that output from that input.

Ml is used for password cracking, finding vulnerabilities easily and quickly and much more
https://github.com/jivoi/awesome-ml-for-cybersecurity
https://github.com/antoinedelplace/Cyberattack-Detection

Blockchain and cybersecurity

Blockchain is basically a ledger / something that stores and is immutable, that is it can't be changed. That is amazing because we can now trust data placed somewhere on the internet.

https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/#6b7187713ac3

Quantum computing and cybersecurity

In general computing there are 2 bits 1's and 0's. In quantum computing, every bit has a probability of being 1 or 0 and every bit has every value with some probability (I don't understand this) . The basic threat to cybersecurity is that these computers can compute way faster than normal computers. Therefore can crack encryption keys and fail cybersecurity. But this will be decades for now and by then we will have a solution for this.

How can you earn by bursting bugs?

My friend of mine encountered a very simple bug (XSS) in a very famous company (that can not be named) and was awarded 30 dollars for it!!

Websites and applications have very common bugs that can be found by any beginner who just knows the simple terms and strategies

What you really need is persistence and consistency and that's all. You can earn 100's of $'s per month at least and there is no limit.
Basically you have to stress test the website apply every strategy to hack it and then report the company and they will reward you for helping them patch the application

These are the famous platforms:
https://www.hackerone.com/
https://www.bugcrowd.com/

Every famous company has a bug bounty program. Check their site.

Resources:

Websites:

http://netsec.ws/
https://owasp.org/
https://github.com/infoslack/awesome-web-hacking
http://www.phrack.org/
https://www.2600.com/

Subreddits:

/r/netsec
/r/AskNetsec
/r/netsecstudents
/r/hacking
/r/blackhat
/r/howtohack
/r/security
/r/Information_Security
/r/cybersecurity
/r/pwned
/r/Defcon
r/CompTIA (for Security+)
r/ccna (for CCNA and CCNA Security, also r/ccnp for CCNP)
r/CEH (for CEH)
r/cissp (Certified Information Systems Security Professional)
r/oscp

Youtube:

https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w
https://www.youtube.com/channel/UC0ZTPkdxlAKf-V33tqXwi3Q
https://www.youtube.com/channel/UCgTNupxATBfWmfehv21ym-g