SEPTEMBER 22, 2022 / #HACKING

What is Hacking? The Hacker Methodology Explained

Daniel Iwugo

Time to learn the basics of the splendid art of hacking 👨‍💻👩‍💻.

In this article, you will learn what the hacking process really looks like. And hopefully one day, you'll get to say those famous words: “I’m in”.

Disclaimer: This is for educational purposes only. Please (with a cherry on top), do not use this knowledge to perform illegal activities. I might be one of the white hats to put you in jail someday 🙃. Thank you.

How do Hackers Hack?

Tony Stark attempting to hack S.H.E.I.L.D | Credit: animatedtimes.com

Since you are reading this article, I'll assume that you already know the basics of what hacking is, so let's jump right in.

There really is no general agreed upon process of hacking, in part because there are a few different types of hackers. But, I will tell you the steps the majority of hackers (and I myself) follow.

They are:

1. Reconnaissance
2. Enumeration
3. Exploitation
4. Privilege Escalation
5. Post Exploitation
6. Covering Tracks
7. Report Writing

We'll go through each one in detail so you get a good feel for the process.

Reconnaissance

A neon themed hollywood hacker | Credit: Wallpaperflare.com

Recon (aka footprinting) is the first, longest, and most important step. This entails getting as much information as you can about the target without interacting directly with the target.

Basic OSINT (Open Source Intelligence) skills are a hacker's best friend here.

Quick lesson: OSINT is the collection and analysis of information from public sources in order to gain actionable intelligence. National security agencies, investigative journalists, and hackers legally gather such information in order to create measures, stories, and dossiers, respectively, about targets.

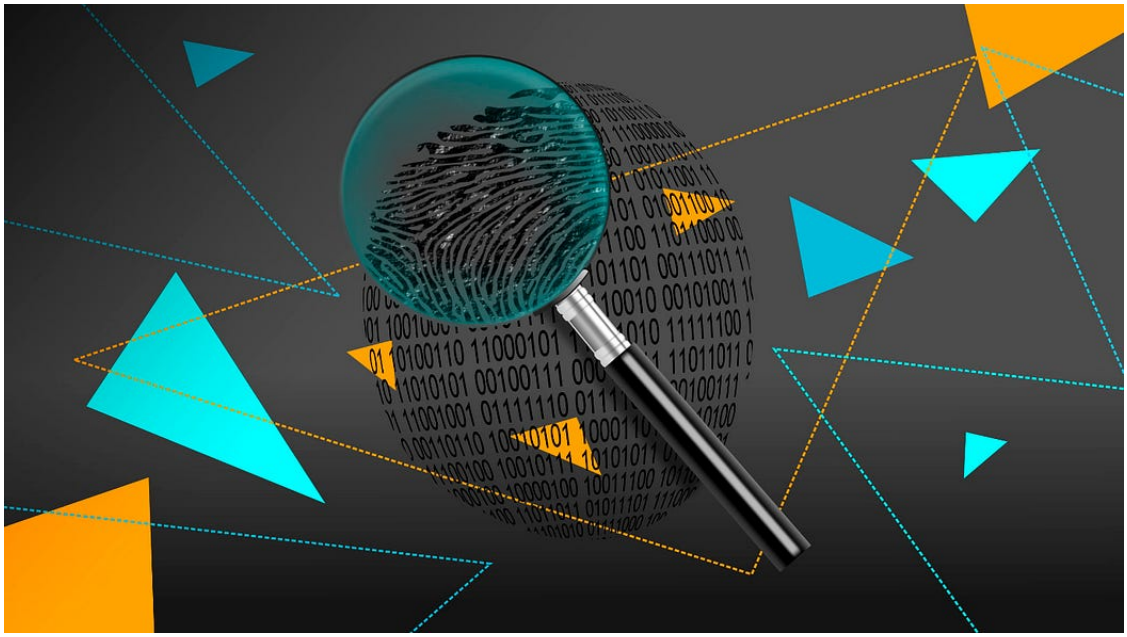
You can find the OSINT framework guide here.

~~doxing~~ would be a good place to start. Doxing in this sense means the use of advanced search techniques to find out more information about a target that you normally wouldn't be able to find using normal methods.

Other resources for recon include:

1. Wikipedia (The biggest encyclopedia to this date)
2. Social Media such as Instagram, Twitter, and Facebook (Best resource for social engineers)
3. who.is (To get information about a website)
4. sublist3r (Lists subdomains publicly available)
5. Media such as newspapers, radio, and television

Enumeration



Magnifying glass over binary ID fingerprint | Credit: Wallpaperflare.com

vulnerability).

Do note, though, that things can get a lot riskier as the target could discover that you are trying to find out information about them, and could put countermeasures in place to hinder you.

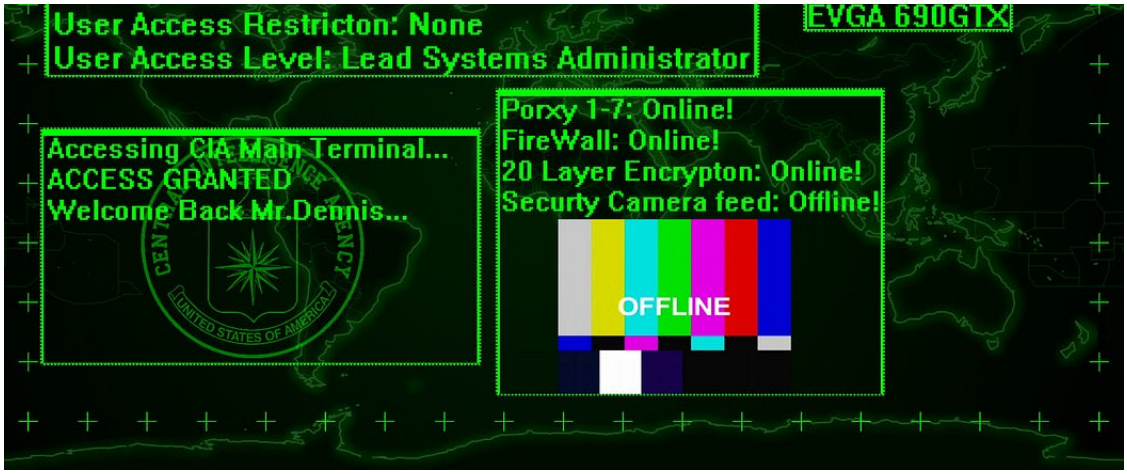
Network enumeration involves port scanning and network mapping. This helps you learn about the target's operating system, open ports, and services being run, along with their version. Nmap (network mapper), burp suite, and exploit-db/searchsploit are common tools you can use for network enumeration.

Tip: Knowing the version of services is a great way to find a vulnerability. Old versions of software may have a known vulnerability which could be on the exploit-db site. You could then use this to perform an exploit.

Physical enumeration involves gaining information through physical means. This could be done via dumpster diving (getting credentials and confidential information from the trash) and social engineering.

Social engineering is quite a broad topic and will get an article of its own later. However, in simple terms, it means hacking humans using manipulative social skills.

Exploitation



A fake terminal access | Credit: Wallpaperflare.com

Exploitation involves gaining access to the target successfully using a vulnerability discovered during enumeration.

A common technique for exploitation is to deliver a payload after taking advantage of the vulnerability. In simple terms, this is finding a hole in the target, and then running code or software that lets you manipulate the system, such as a bash shell.

Infamous vulnerabilities that are commonly exploited are EternalBlue (Windows) and the Apache log4j (web servers) vulnerabilities.

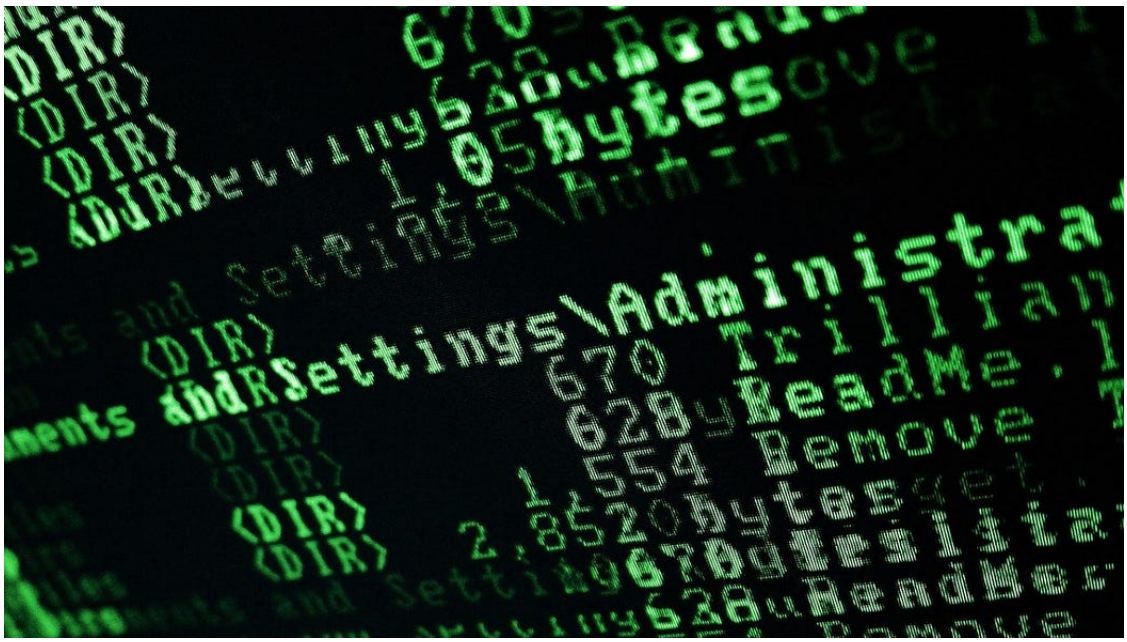
Common tools you can use for exploitation include:

1. Metasploit (The big gun 🔫)
2. Burpsuite (For web applications)
3. Sqlmap (For databases)
4. Msfvenom (Used to create custom payloads)

you access and allow you to manipulate the target.

A very common payload many hackers use is meterpreter. It is a payload by metasploit that allows you to easily transverse the hacked computer.

Privilege Escalation



Random Text with “Administrator” | Credit: Wallpaperflare.com

In order to understand privilege escalation, you need to grasp two concepts:

1. User Accounts
2. Privileges

A User Account is a profile on a computer or network that contains information that's accessed via a username and password.

account, which is the administrator. In contrast, organisations have multiple accounts on a network or computer, with a system administrator having the administrator account and the basic employees having various standard accounts.

Privileges are the permissions that let you write, read and execute files and applications. A standard user doesn't have privileges (permissions) to critical files and applications which we want. However, an administrative account will have privileges for everything.

Escalation is the movement from one user account to another. This could either be vertical or horizontal.

Vertical escalation is when a hacker moves from an account with fewer privileges (standard account) to an account with more privileges (administrative account).

Horizontal escalation is when a hacker moves from one user account to a similar account of the same privilege level in hopes of performing vertical escalation with the new compromised account (standard account to standard account).

The administrative user accounts you would want to target are root (Linux) or Administrator/System (Windows). These accounts have **all** the privileges and are practically a goldmine if you get access to them, as you can take absolute control of the computer.

Techniques to perform privilege escalation include:

1. Password spraying (Reusing passwords)

3. Finding ssh keys (Used for horizontal escalation)
4. Abusing SUID binaries (Taking advantage of misconfigured privileges in Linux)
5. Running tools scripts to look for escalation routes (enum4linux is nice and PEASS-ng has a great suite)

Post-Exploitation

Code with text “malicious virus” | Credit: Wallpaperflare.com

Usually, white hats skip over to the very last step. But I will include this and the next for the sake of knowledge.

Post exploitation is the use of tools with the aim of gaining persistence and obtaining sensitive information from the target computer.

This could be done in a number of ways including:

3. Downloading intellectual property, sensitive information, and Personal Identifiable Information (PII)

Covering Tracks

An Anonymous themed background | Credit: Wallpaperflare.com

This is as simple as it gets, but can be incriminating if there is even a slight mistake. A malicious hacker has to be careful to not leave behind files, scripts, or anything that can be used by a digital forensics expert to track the hacking back to them.

Some basic things to do would be to delete log files and the history file in Linux. The meterpreter payload even has a feature to delete all logs on the Windows Event Manager.

Digital report writing | Credit: Wallpaperflare.com

This is the final step of the hacker methodology. It involves writing down a basic rundown of the entire process you went through above.

There are various formats, but a basic one will include:

1. Vulnerabilities found and their risk level
2. A brief description of how the vulnerabilities were discovered
3. Recommendations on how to remediate the vulnerabilities

Tip: Note taking when hacking is very important. I personally learned this the hard way when doing CTFs (Capture The Flag).

Not only does it make it easier when writing reports, but they also allow you to avoid repeating failed attempts and sort through information easily. They also let you look back on what you've done later on. Taking screenshots is also a great idea.

Alright so let's do a quick recap of the hacker methodology:

1. Reconnaissance
2. Enumeration
3. Exploitation
4. Privilege Escalation
5. Post-Exploitation
6. Covering Tracks
7. Report Writing

Resources to help you practice:

1. Test your knowledge on the hacker methodology
2. Tips on how to protect yourself from hackers
3. More information about OSINT

Acknowledgements

Thanks to Chinaza Nwukwa, Holumidey Mercy, Georgina Awani, and my family for the inspiration, support, and knowledge used put this post together. You guys are the best.

Daniel Iwugo

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet

---