CEH v13 Practical Notes

Unlock The Hacker's Mind
Module Wise Mastery

Simplified, Sorted, and Supercharged for Aspiring Hackers!

By

Lukman Nadaf

Welcome to the World of Ethical Hacking

Welcome, Cyber Warriors!

Greetings to all curious minds, passionate geeks, and rising stars of the hacker community! If you've ever dreamt of diving into the thrilling world of ethical hacking, uncovering hidden vulnerabilities, and mastering the art of cybersecurity, you're at the right place.

This isn't just a set of notes—it's your hacker's manual, your companion in the journey to becoming a Certified Ethical Hacker. Think of it as a treasure map, guiding you to uncover secrets, gain control (ethically!), and secure systems like a pro.

Why this guide?

To simplify the complex.
To ensure you learn by doing.
To make ethical hacking as exciting as it truly is.
Whether you're new to hacking or polishing your skills, these notes are here to empower you with the commands, tools, and mindset you need to succeed.

Remember: Hacking is a responsibility, not a rebellion. Use your skills for good, stay curious, and always be ready to learn!

Let's hack the future—together!

What’s Inside This Treasure Trove?

Welcome to your ultimate guide to mastering **ethical hacking**! This isn’t just a collection of notes—it’s a powerful, action-packed roadmap that transforms complex CEH v13 concepts into practical skills. Whether you're a beginner or brushing up on your skills, this guide has something for you. Here's what you’ll gain:

1. ***Hands-On Expertise***: Dive straight into the world of hacking with detailed practicals for every concept. No fluff, just actionable steps to learn by doing.
2. ***Command Mastery***: Master the most essential commands and tools used by ethical hackers. Each command is explained and demonstrated to make it simple and effective.
3. ***Comprehensive Knowledge***: Cover every module of CEH v13, from the basics of reconnaissance to advanced exploitation techniques, ensuring no stone is left unturned.
4. ***Real-World Scenarios***: Understand how hackers operate in the real world and how to counter their tactics with real-world examples and practical applications.
5. ***Strategic Thinking***: Learn to think like a hacker—discover vulnerabilities, exploit them, and secure them, building a solid foundation of offensive and defensive skills.
6. ***Career-Ready Skills***: By the end of this guide, you’ll not only master the CEH syllabus but also be ready to apply these skills in real-world cybersecurity roles.

This isn’t just a guide; it’s your secret weapon to step into the ethical hacking community with confidence. Packed with challenges, tips, and insights, this guide will push you to go beyond the basics and truly master the art of hacking.

So, gear up, dive in, and let the journey to ethical hacking mastery begin!

Module - 01

Introduction to Ethical Hacking

Module 1: Introduction to Ethical Hacking

In this module, we'll cover the basics of ethical hacking, the hacking phases, and essential terms that you need to know to embark on your journey as a Certified Ethical Hacker (CEH).
Note: This chapter is more about laying the foundation and understanding the concepts—practicals will come right after in the next modules, so let's keep this short and exciting!

What is Ethical Hacking?

Ethical hacking refers to the process of intentionally probing a system for vulnerabilities in a controlled, authorized manner to identify weaknesses before malicious hackers can exploit them. The main goal is securing systems, not compromising them.

Why Ethical Hacking is Important

Identify vulnerabilities: Protect systems from real hackers.
Prevent data breaches: Guard sensitive information.
Strengthen defences: Ensure that the system is fortified against attacks.

Types of Hackers

White Hat Hackers: Ethical hackers who work for the good of the system (you, the ethical hacker).
Black Hat Hackers: Malicious hackers who exploit systems for personal gain.
Gray Hat Hackers: Hackers who may sometimes cross legal lines but without malicious intent.

The Phases of Hacking

Ethical hacking follows a systematic process, known as the *ethical hacking lifecycle*. Here are the main stages:

1. **Reconnaissance:**
   - The hacker collects information about the target system.
   - This can be active (direct interaction with the system) or passive (gathering info from public sources).
2. **Scanning:**
   - This phase involves identifying live hosts, open ports, and services running on the system.
   - Tools: nmap, netdiscover.
3. **Enumeration:**
   - Extracting detailed information such as user accounts, shares, and services.
   - Tools: enum4linux, snmp-check.
4. **Gaining Access:**
   - The hacker attempts to exploit the discovered vulnerabilities to gain access to the system.
   - Tools: Metasploit, Hydra.

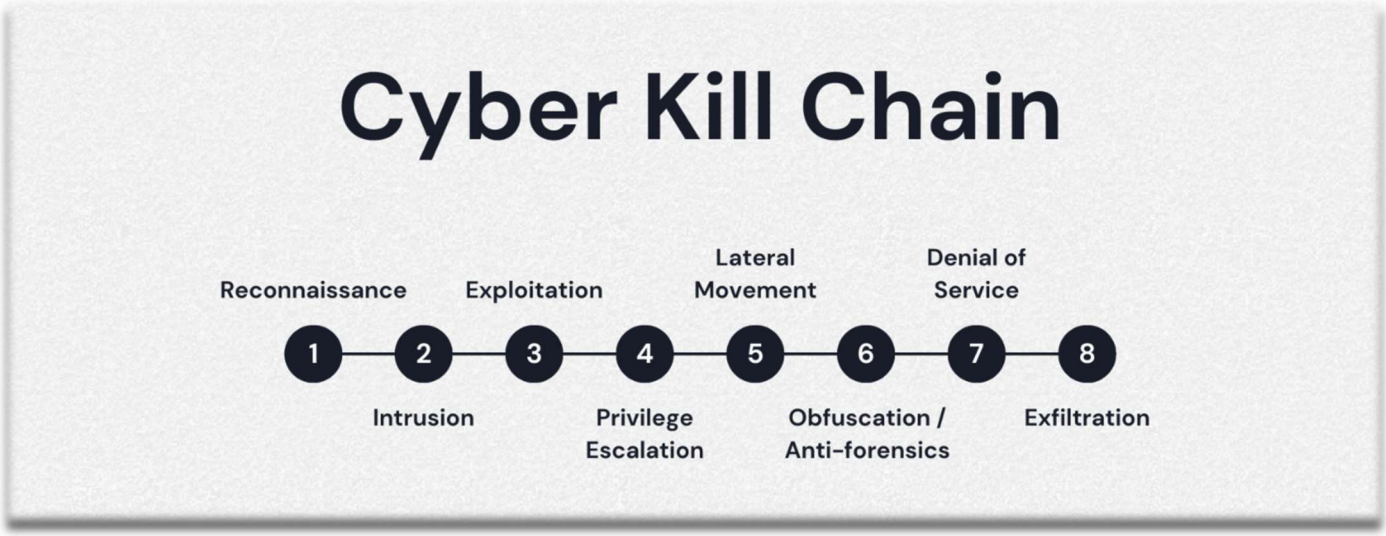
5. **Maintaining Access:**
   - Once access is gained, the hacker may create a backdoor for future entry.
   - Tools: Netcat, Metasploit.
6. **Covering Tracks:**
   - The final phase is about erasing logs and traces to avoid detection.
   - Tools: Clearev, Rootkit Hunter

For Real-World Hackers: The Cyber Kill Chain and MITRE ATT&CK Frameworks

As a hacker operating in the real world, you know that cybersecurity is more than just tools and commands—it's about strategy, precision, and understanding your target. Two critical frameworks that every hacker should master are the **Cyber Kill Chain** and **MITRE ATT&CK**. These frameworks break down the art and science of hacking into structured phases, giving you the edge in understanding and emulating attack scenarios.

The Cyber Kill Chain:

Developed by Lockheed Martin, the **Cyber Kill Chain** is a seven-step framework that outlines the lifecycle of a cyberattack, from preparation to execution. Here's what each phase means to a hacker:



1. **Reconnaissance**
   - **Goal**: Gather intelligence about your target.
   - **Real-World Use**: Use OSINT tools, scan networks, and map out vulnerabilities.
   - *Tools*: Nmap, Shodan, Maltego.
2. **Weaponization**
   - **Goal**: Craft your exploit. Combine malware with a delivery method.
   - **Real-World Use**: Write custom payloads or tweak existing ones to evade detection.
   - *Tools*: msfvenom, Veil, Python.
3. **Delivery**
   - **Goal**: Deliver the weapon to the target via phishing, USB drops, or direct access.

- **Real-World Use**: Choose the most effective vector based on reconnaissance.
- *Tools*: Social engineering, email spoofing, PowerShell scripts.

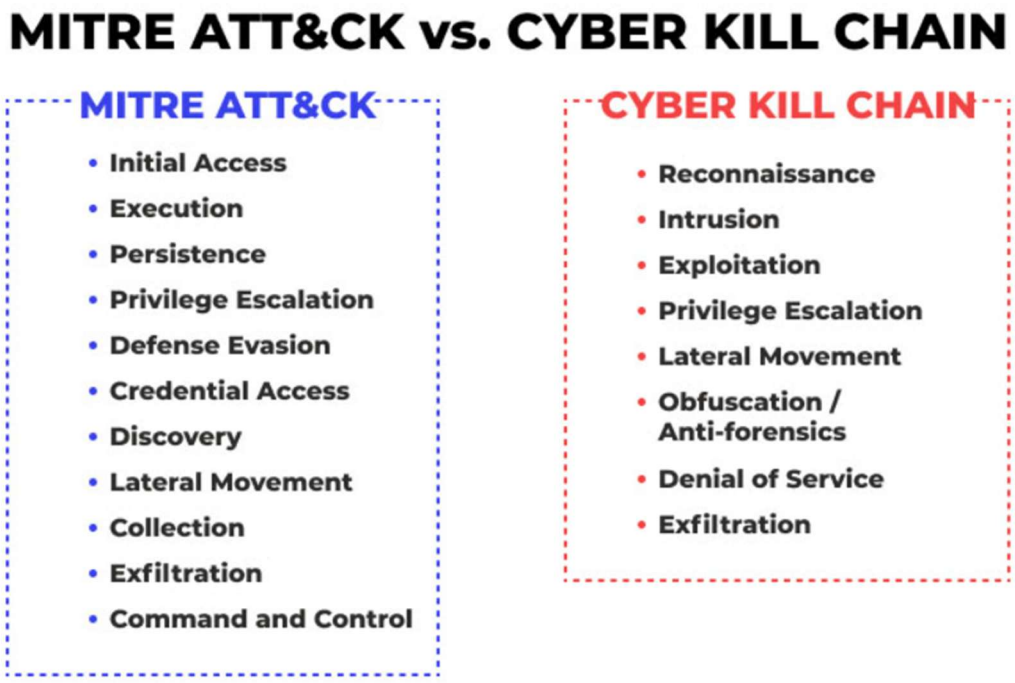
4. **Exploitation**
   - **Goal**: Trigger the payload to exploit the vulnerability.
   - **Real-World Use**: Execute exploits with precision to gain initial access.
   - *Tools*: Metasploit, ExploitDB scripts.
5. **Installation**
   - **Goal**: Install backdoors or malware to maintain access.
   - **Real-World Use**: Drop persistent shells or RATs for ongoing control.
   - *Tools*: Cobalt Strike, Empire, Netcat.
6. **Command & Control (C2)**
   - **Goal**: Establish a secure communication channel.
   - **Real-World Use**: Use stealthy techniques to avoid detection while controlling compromised systems.
   - *Tools*: C2 frameworks like Sliver, Covenant.
7. **Actions on Objectives**
   - **Goal**: Achieve your ultimate objective, whether it's data exfiltration, sabotage, or lateral movement.
   - **Real-World Use**: Execute final operations while maintaining stealth.
   - *Tools*: Mimikatz, BloodHound, Rclone.

MITRE ATT&CK:

The **MITRE ATT&CK Framework** is a comprehensive knowledge base that categorizes tactics and techniques used by adversaries across various platforms. It's an invaluable resource for understanding how attacks unfold in the real world.

1. **Tactics**
   - These represent the **why** of an attack—the adversary's objectives at each stage.
   - *Examples*: Initial Access, Privilege Escalation, Defense Evasion.
2. **Techniques**
   - These describe the **how** of an attack—the specific methods used to achieve the objectives.
   - *Examples*: Phishing (Initial Access), Credential Dumping (Privilege Escalation), Obfuscated Files (Defense Evasion).
3. **Sub-Techniques**
   - These are detailed variations of techniques, showing granular execution methods.
4. **Real-World Application for Hackers**
   - **Planning**: Use the framework to emulate real-world APT tactics in red team exercises.
   - **Execution**: Map your techniques to the ATT&CK matrix to identify and refine your approach.
   - **Defense Evasion**: Learn how defenders detect and respond, and craft your payloads to bypass these measures.

MITRE ATT&CK Navigator is a fantastic tool for visualizing your attack flow and identifying gaps in your methodology.



Let's Get Ready for the Fun Stuff!

Now that you have an understanding of the basics, *it's time to get into the real action!* From the next module onward, we'll dive into actual practicals like scanning networks, exploiting vulnerabilities, and more. So, buckle up—you're about to start your hands-on journey with ethical hacking!

Module - 02

Footprinting and Reconnaissance

Module 2: Footprinting and Reconnaissance

So lets start from information gathering. Information gathering is the initial phase of Hacking we can say!

During this phase we use lots of different types of techeniques and tools to collect usefull and meaningfull information about the target.

Reconnaissance, Footprinting and Enumeration these are the techniques we can use in order to gather information about target as much as posible.
Lets understand each one by one…

Information Gathering:
Information gathering is an umbrella term nothing but collecting data about target as much as posible in order to create attack vecters.

Info gathering is a Broad Process, It is the overarching term for collecting any kind of data about the target which includes all activities like footprinting, reconnaissance, and enumeration.

Information gathering Types:
There are two ways via which we can gather information about target, one is active and another one is passive way.

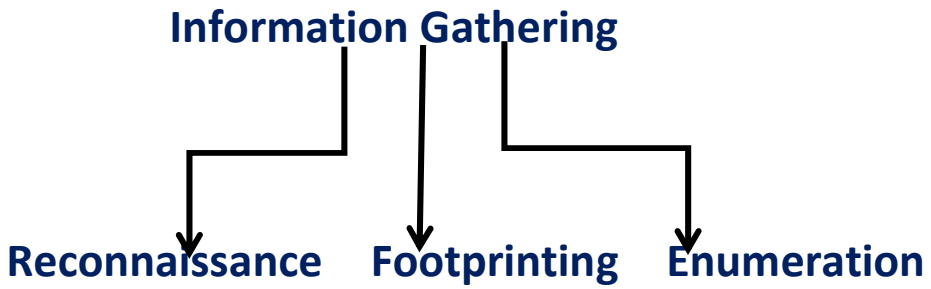
1. ***Active Information Gathering:***
   - Collecting information about target by connecting to target itself is known as active information gathering.
   - If we are having direct connection with our target to collect information then it is active way of gathering information

2. ***Passive Information Gathering:***
   - Collecting information without connecting the target directly is called passive information gathering.
   - In this way of gathering information we collects data from other resources present there on the internet, we use google like search engines and some time we use multiple tools.

Footprinting:
Footprinting is a Specific Subset of Information Gathering which Focuses on mapping and profiling the target and it is **Passive by Nature** Often done without interacting directly with the target, such as using public records or Google Dorks.
To create a map of target infrastructure we use this process of information gathering.

Reconnaissance:
Reconnaissance is a Phase of Hacking which Refers to the initial stage where data is collected to prepare for an attack.
Includes Footprinting It combines both passive (indirect) and active (direct) methods to gather information.
Its main Goal is to Identify potential vulnerabilities and weaknesses for the next steps in the hacking process.

Enumeration:
Enumeration is a "Post-Scanning Phase" which Starts once live systems and open ports have been identified during scanning.
Active Interaction: Involves direct engagement with the target system to extract detailed and specific data.
Its main objective is to Retrieve usernames, machine names, shared resources, and other critical information.
We will discuse about Enumeration more in a separate chapter.



so in this module we will extract information about the target organization that include, but not limited to:

- **Organization information** Employee details, address and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information.
- **System Information** operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

LAB 01: Perform Footprinting Through Search Engines

Task 01: Information Gathering using Advanced Google Hacking Techniques!!!

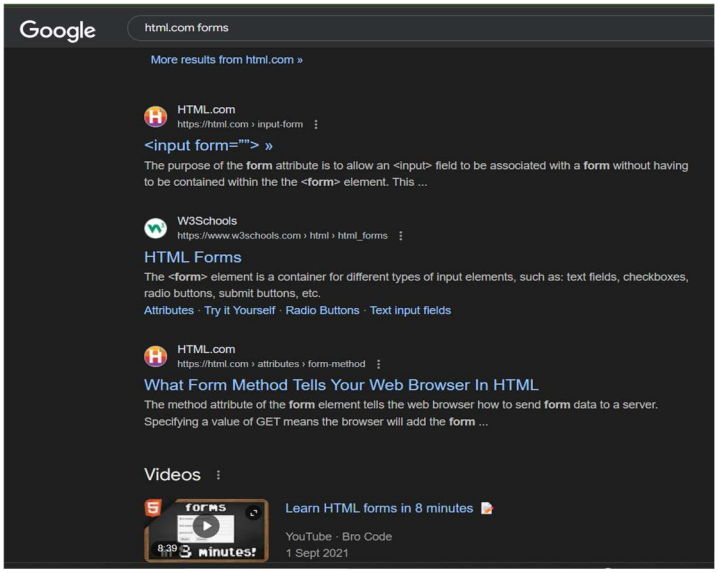
Google Dorks:
Google Dorks are advanced search techniques that use specialized operators to find specific and often hidden information on the internet.

generally what happens, when we search something on google like search engines it will brings lots of data which has similar keywords in urls or in titles, but mostly you will get lots of irrelevant information as well.
so google dorks helps you to get exact what you want

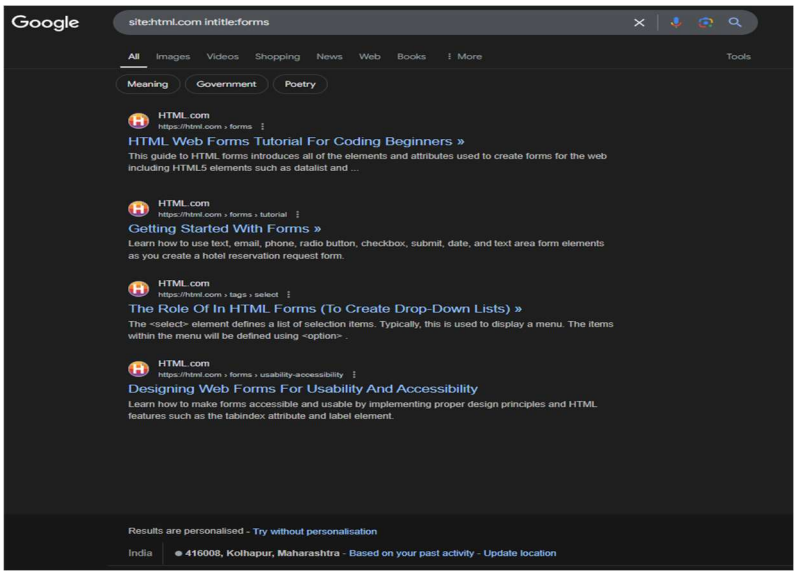
Some google dorks:

Site: To fech data from a specific site only then we can use this dork.

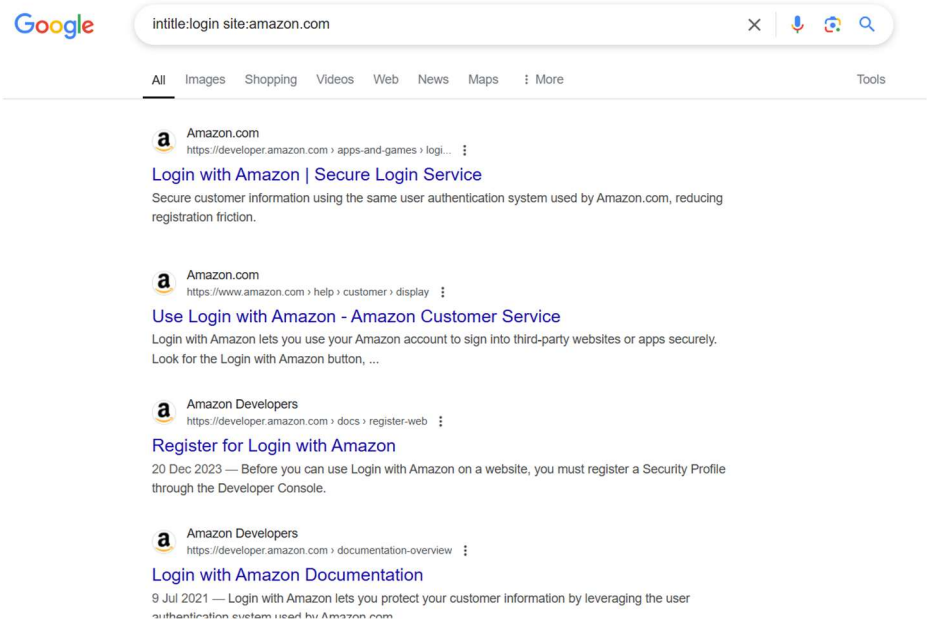
Simple search: html.com forms intitle:forms



search with google dorks: site:html.com intitle:forms



Intitle: Intitle dork helps to find out all posts and links where the specific searched query there in title of google searches.



Here are some google dorks which helps lot in bug bounty!!!

1. **Finding Sensitive Files:**
   - *filetype:pdf inurl:"confidential"*
   - *filetype:xls | filetype:xlsx inurl:"salary"*
   - *filetype:doc | filetype:docx "password"*
   - *intitle:"index of" "backup"*

2. **Discovering Login Pages:**
   - *inurl:adminlogin*
   - *inurl:login.jsp*
   - *intitle:"Admin Login"*
   - *inurl:/admin/ intitle:login*

3. **Exposed Databases**
   - *filetype:sql "password"*
   - *inurl:phpmyadmin/index.php*
   - *inurl:"/wp-admin/setup-config.php"*
   - *intitle:"phpinfo" "mysql"*

4. **Detecting Security Cameras**
   - *intitle:"Live View / - AXIS" | intitle:"Live View / - D-Link"*
   - *inurl:/view.shtml*
   - *inurl:/video.cgi*
   - *intitle:"Network Camera" inurl:"main.cgi"*

5. **Finding Email IDs**
   - *intext:"@gmail.com" OR intext:"@yahoo.com" OR intext:"@outlook.com"*
   - *"email" intext:"*.*@*.*"*
   - *site:linkedin.com "gmail.com"*

6. **Vulnerable Websites**
   - *inurl:"id=" & intext:"sql syntax error"*
   - *inurl:"search.php?q=" & intext:"sql"*
   - *intitle:"Welcome to Joomla!" inurl:"/administrator"*
   - *inurl:index.php?option=com_*

7. **Exposed Configuration Files**
   - *filetype:env "DB_PASSWORD"*
   - *filetype:json "AWS_SECRET_ACCESS_KEY"*
   - *filetype:xml inurl:config*
   - *filetype:conf inurl:apache*

8. **Default Credentials**
   - *intitle:"index of /" "ftpconfig"*
   - *intitle:"index of /" "ssh_config"*
   - *intitle:"index of /" "passwd"*

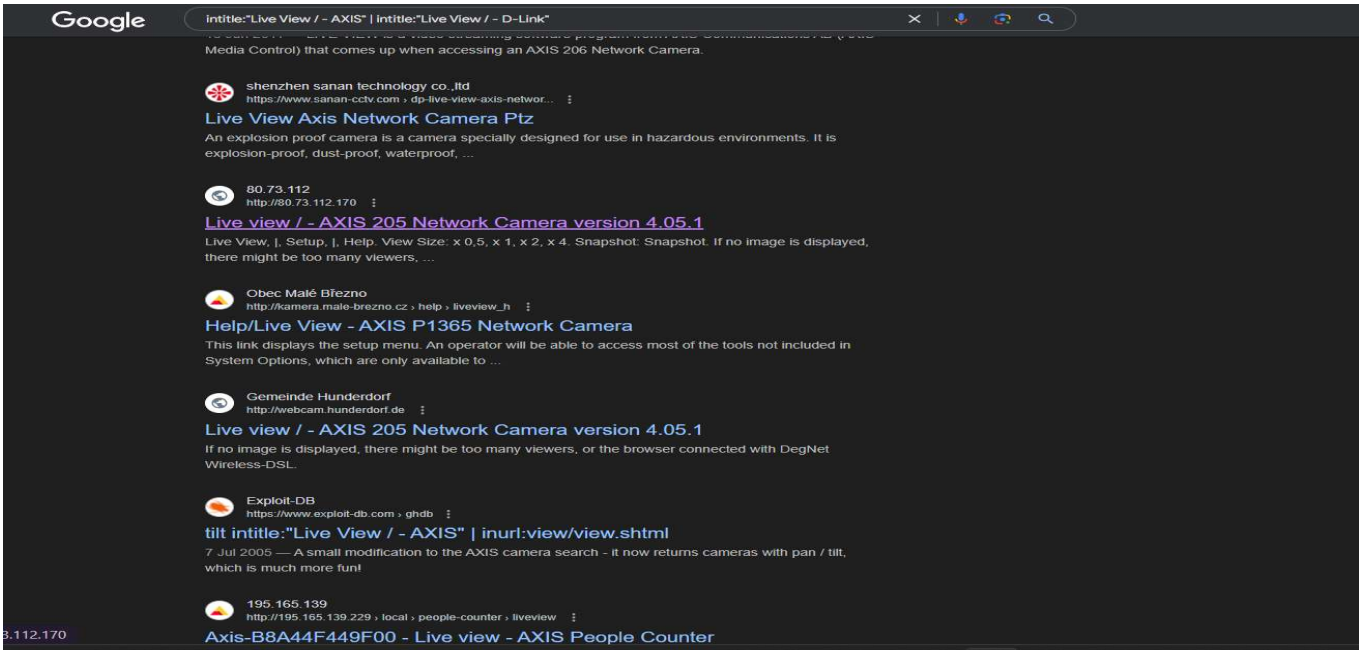
9. IoT Devices

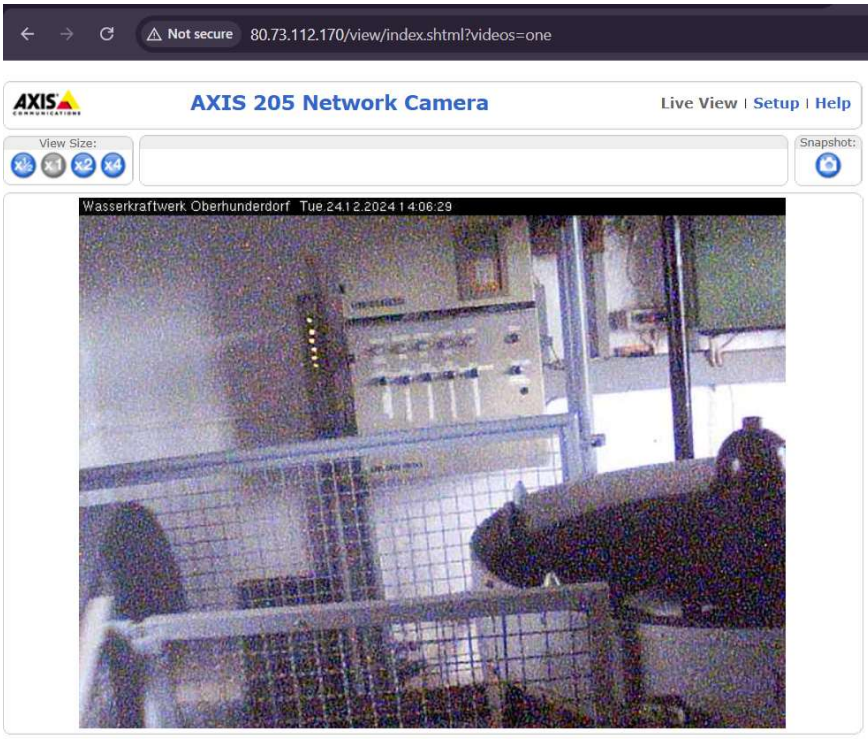
- *intitle:"netcam" inurl:"/webcam.html"*
- *intitle:"Index of /" "IP camera"*
- *inurl:"/dvr.cgi" OR inurl:"/config/"*

10. Discover Public APIs

- *filetype:json inurl:api*
- *"api_key" filetype:json*
- *"Authorization: Bearer" filetype:json*

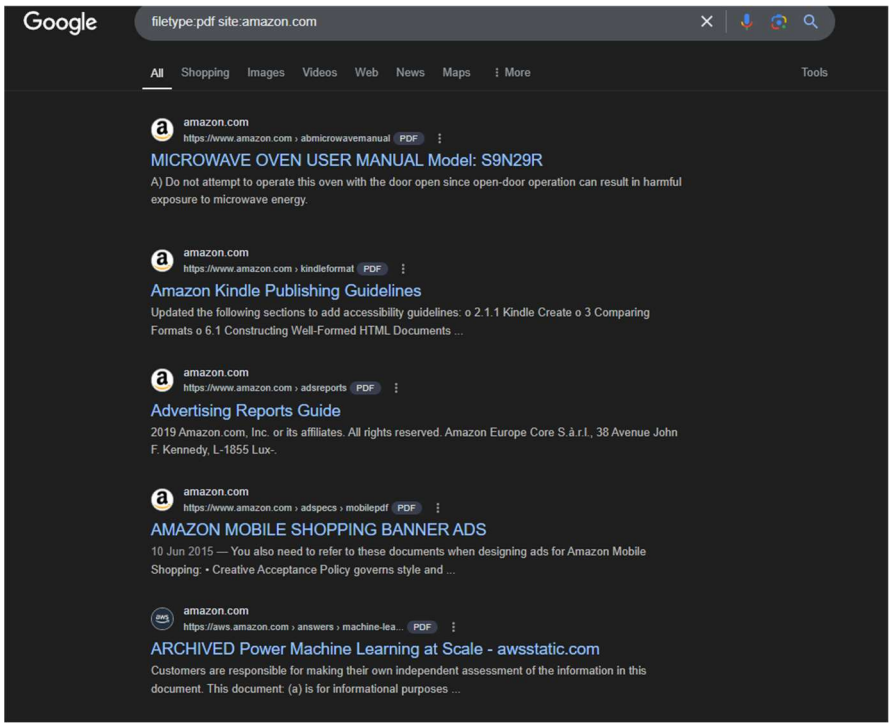
Example : intitle:"Live View / - AXIS" | intitle:"Live View / - D-Link"





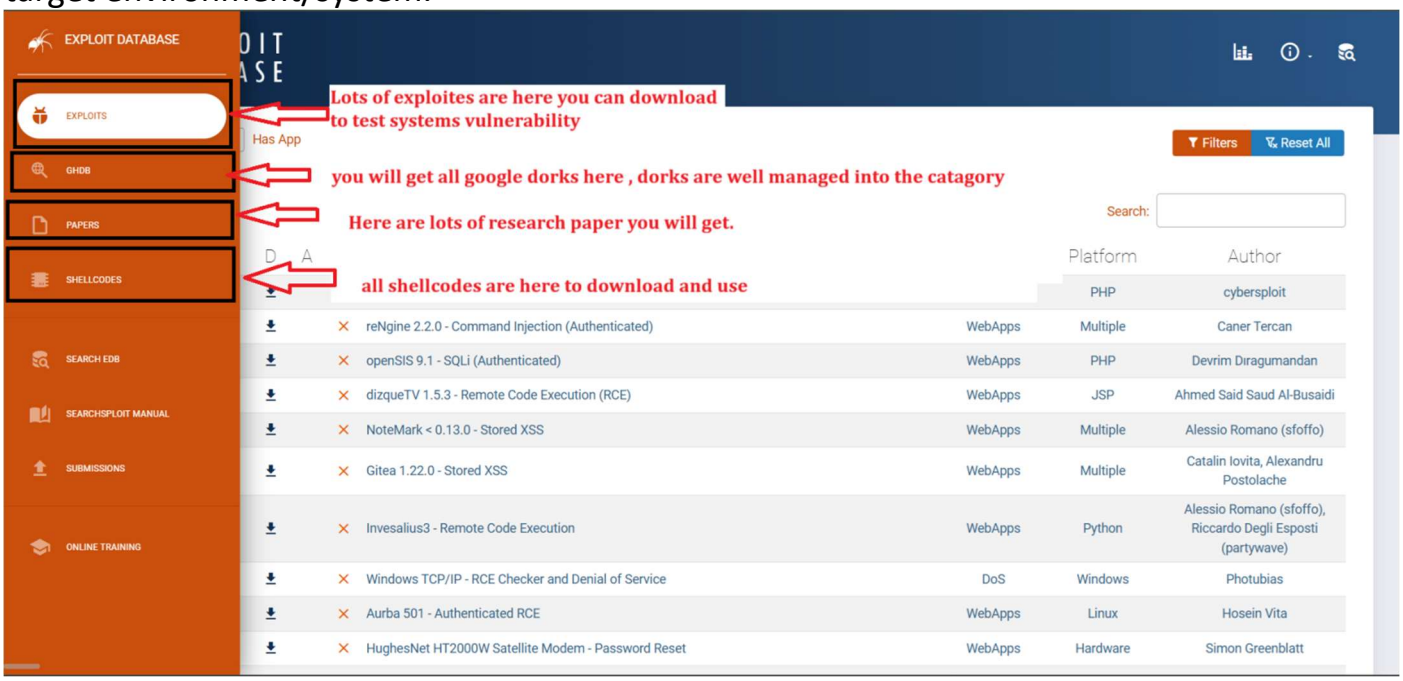
We can access
live AXIS footage

filetype: This operator helps you to access specific files only
As you can see every result providing the pdf file associated with amazon.com site only!

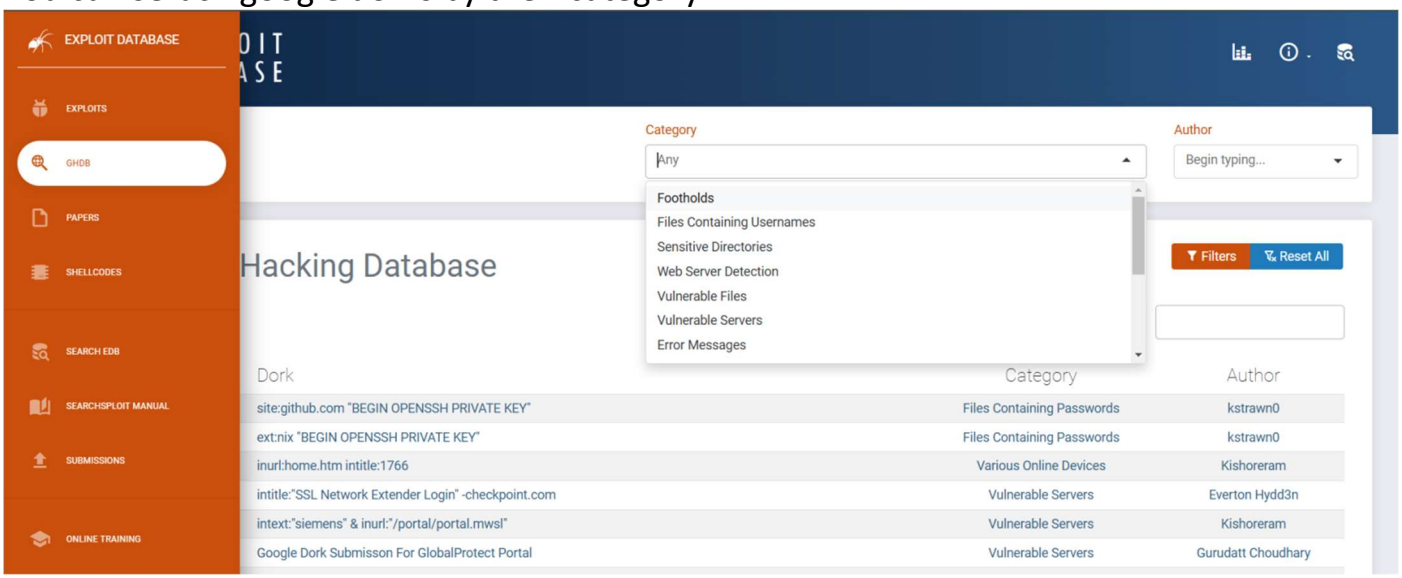


This is the power of google dorks! Each search engine has its own engine dorks to make searches easy and eleminate irrelevency!

GHDB:
We can also use ***Google Hacking Database(GHDB)*** which provides you not only the google dorks but the malwares, research papers, shellcodes and many more things to pentest your target environment/system.



Now main section here is GHDB where you ll get all dorks!
You can serach google dorks by their category

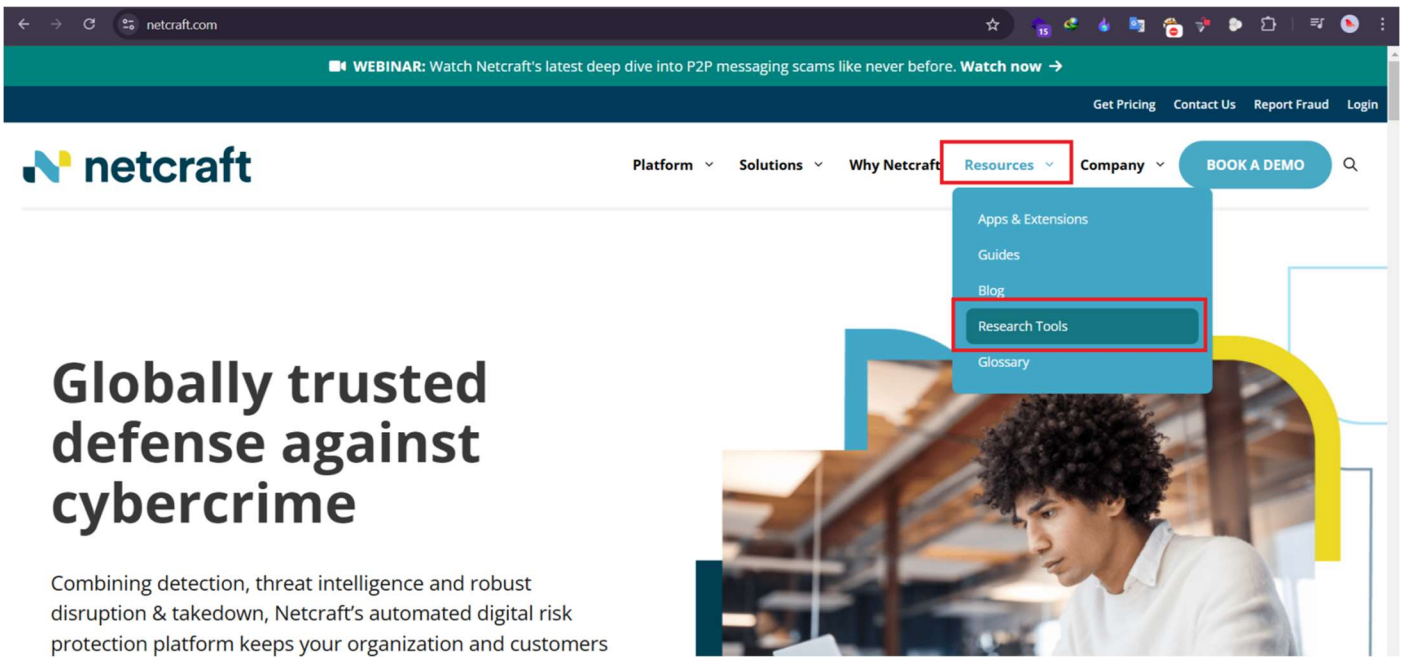


LAB 02: Perform Footprinting Through Internet Research Services

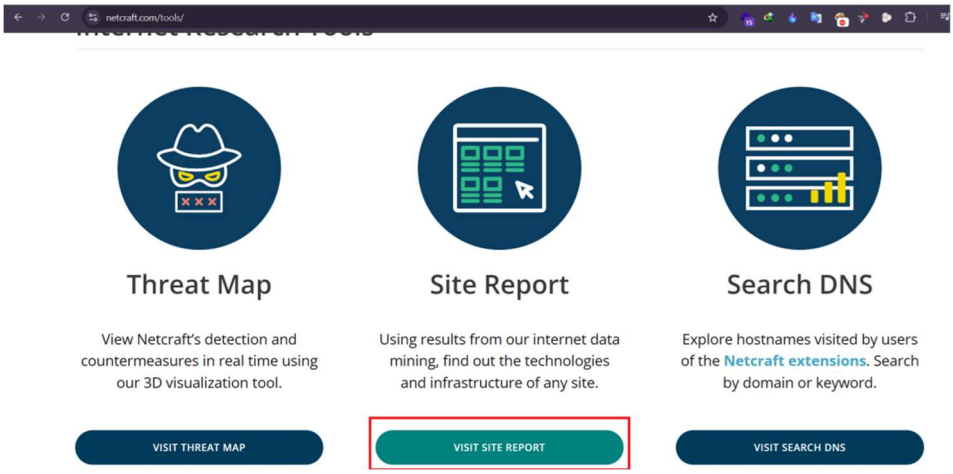
Task 1: Find the Company's Domains, Subdomains, and Hosts using Netcraft and DNSdumpster

1. Using Netcraft

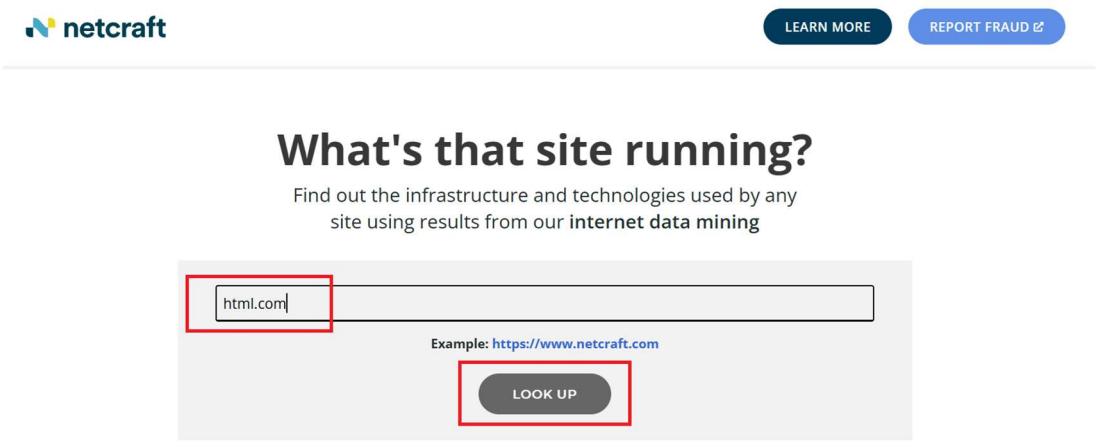
- Go to the site > Resources > Research Tools



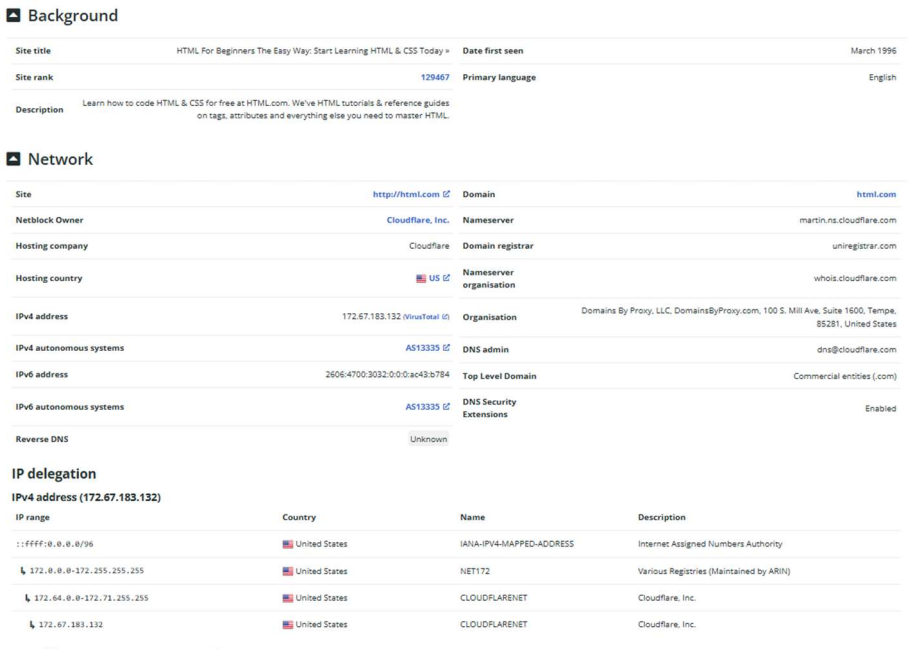
- Then open site report

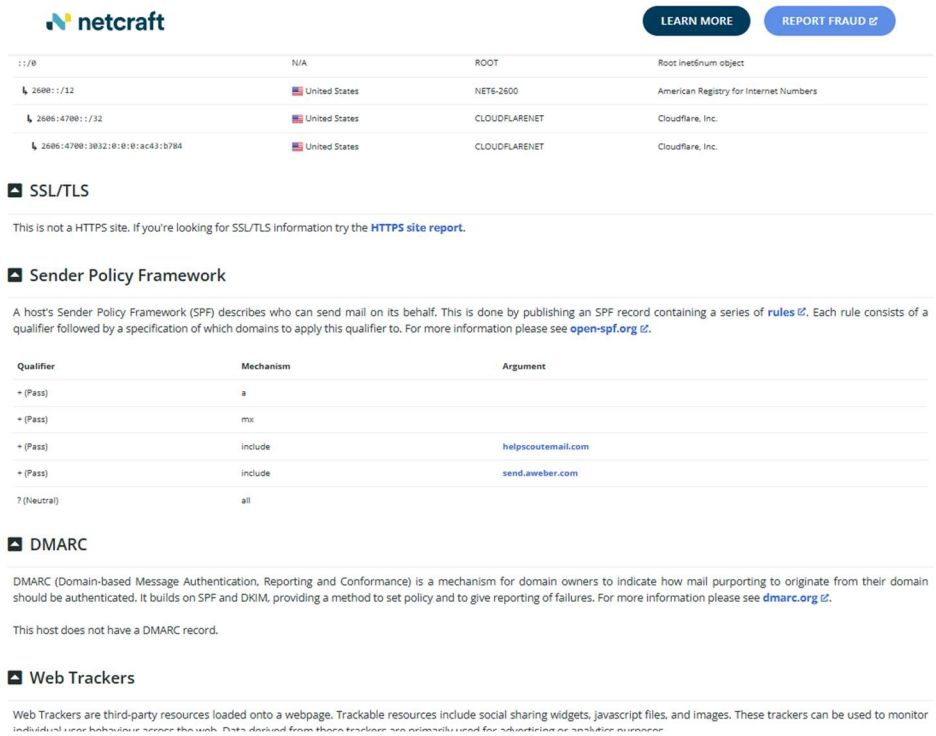


- Then click to the lookup button

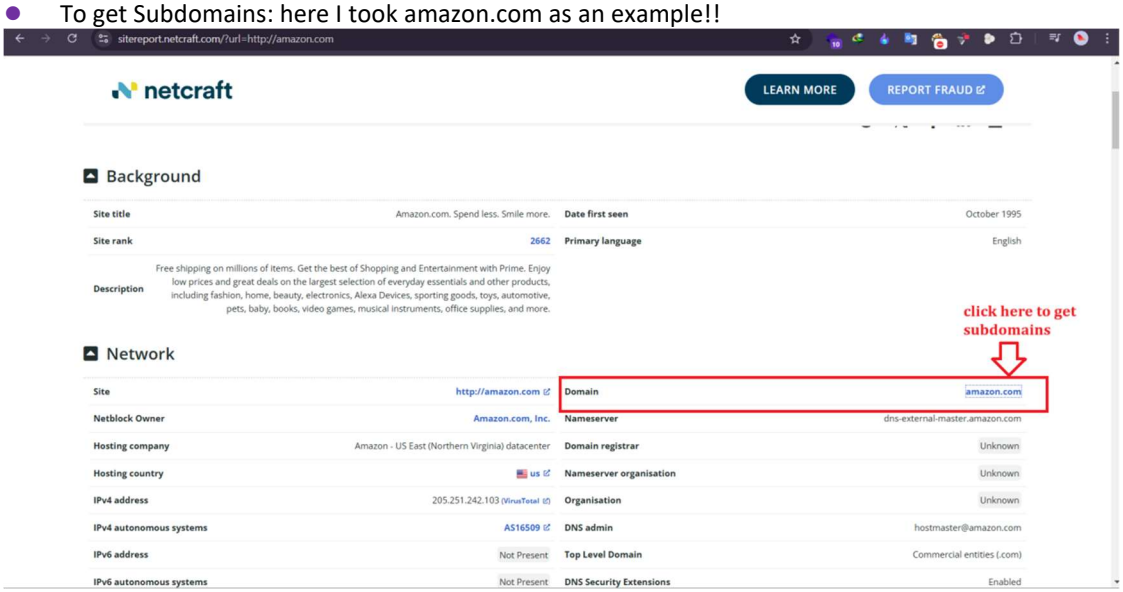


- We will get site report here!!

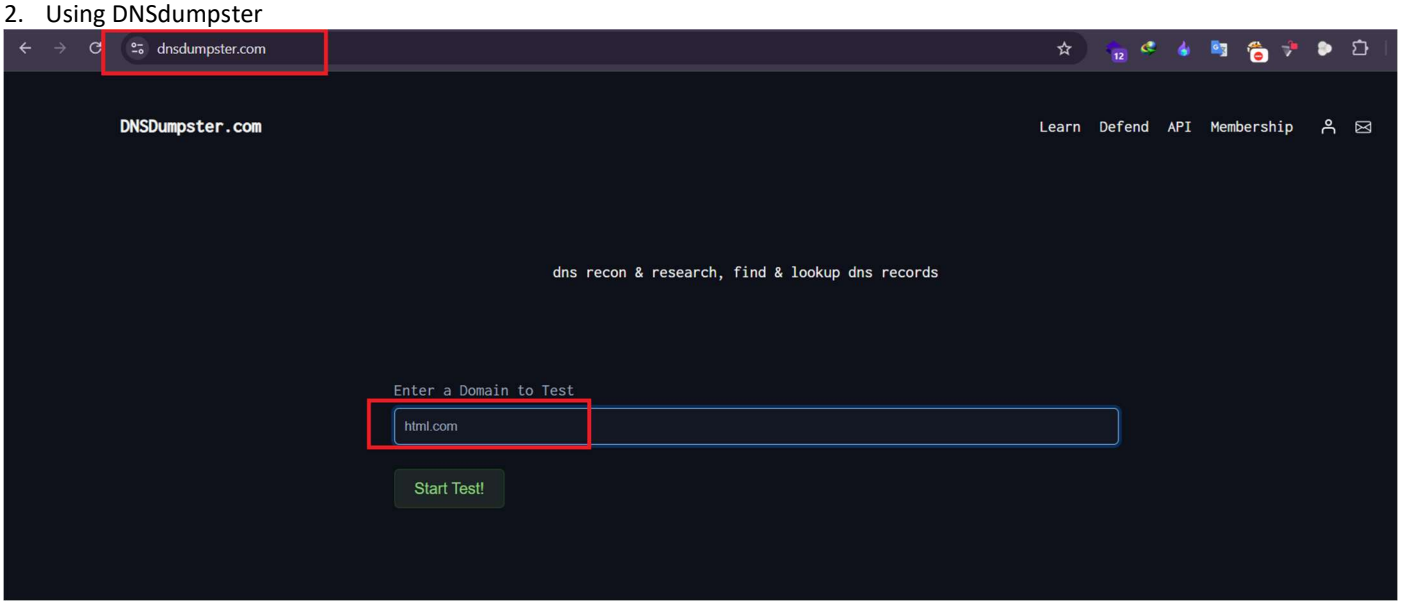




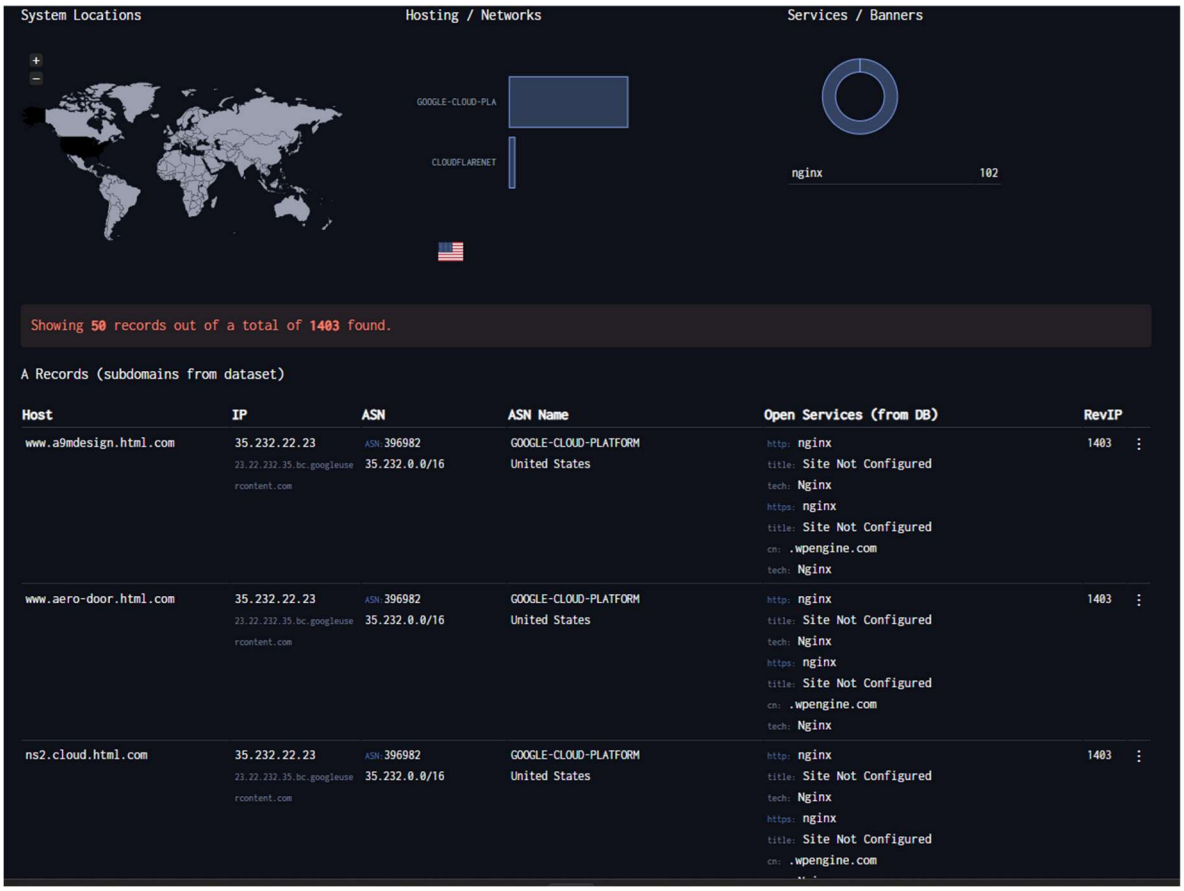
- To get Subdomains: here I took amazon.com as an example!!



2. Using DNSdumpster



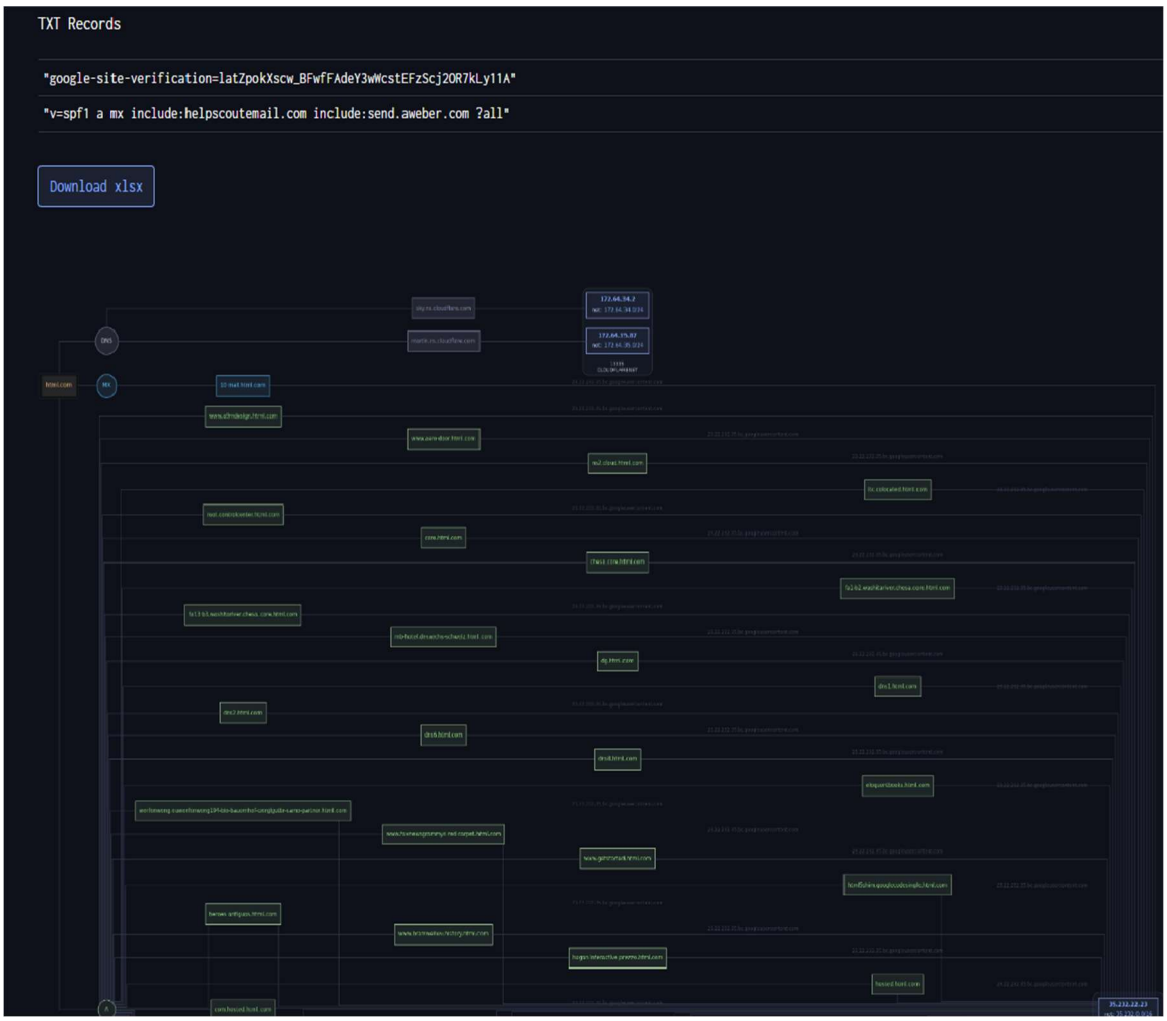
Result:


System Locations
Hosting / Networks
Services / Banners
GOOGLE-CLOUD-PLA
CLOUDFLARENET
nginx 102
Showing 50 records out of a total of 1403 found.
A Records (subdomains from dataset)
Host IP ASN ASN Name Open Services (from DB) RevIP
www.a9mdesign.html.com 35.232.22.23 23.22.232.35.bc.googleuse rcontent.com ASN:396982 35.232.0.0/16 GOOGLE-CLOUD-PLATFORM United States http: nginx title: Site Not Configured tech: Nginx https: nginx title: Site Not Configured cn: .wpengine.com tech: Nginx 1403
www.aero-door.html.com 35.232.22.23 23.22.232.35.bc.googleuse rcontent.com ASN:396982 35.232.0.0/16 GOOGLE-CLOUD-PLATFORM United States http: nginx title: Site Not Configured tech: Nginx https: nginx title: Site Not Configured cn: .wpengine.com tech: Nginx 1403
ns2.cloud.html.com 35.232.22.23 23.22.232.35.bc.googleuse rcontent.com ASN:396982 35.232.0.0/16 GOOGLE-CLOUD-PLATFORM United States http: nginx title: Site Not Configured tech: Nginx https: nginx title: Site Not Configured cn: .wpengine.com 1403

.

.

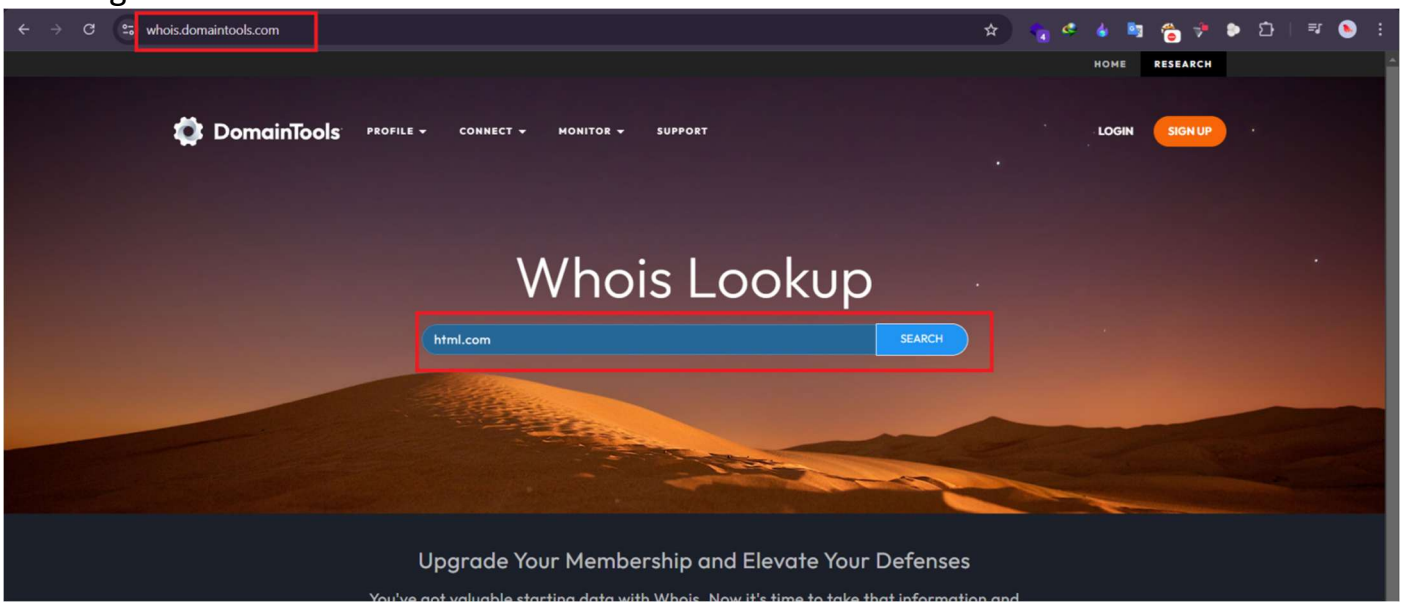
.


TXT Records
"google-site-verification=latZpokXscw_BFwfFAdeY3wWcstEFzScj2OR7kLy11A"
"v=spf1 a mx include:helpscoutemail.com include:send.aweber.com ?all"
Download xlsx

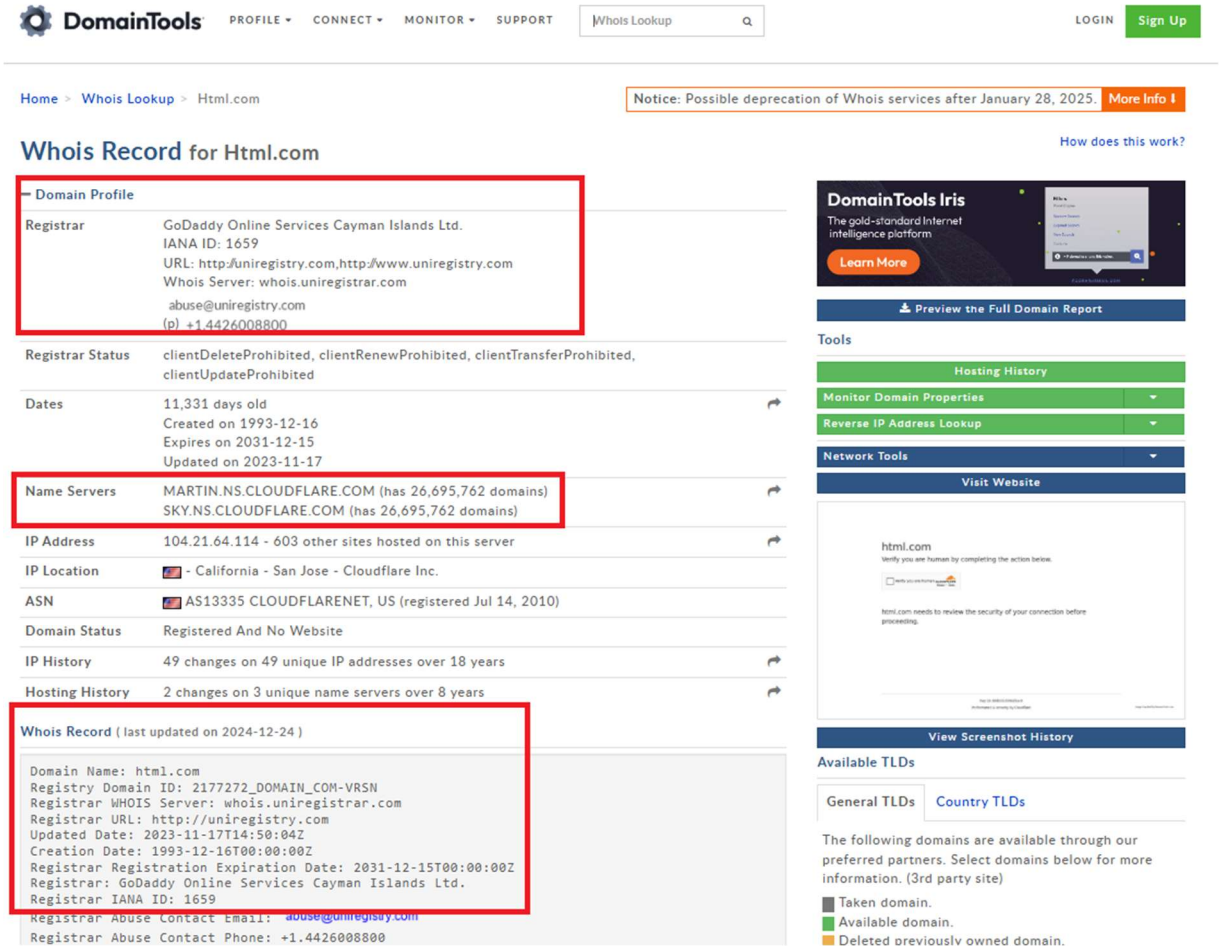
To get more informaion about target DNS ; check out my previous post

LAB 03: Perform Whois Footprinting

1. Using DomainTools



Result:



We can also use SmartWhois to get records

LAB 04: Perform DNS Footprinting

I have covered each and every topic in my DNS Pentesting Notes so to know more about it, just go and check it out |link

LAB 05: Perform Network Footprinting

Task 1: Network Tracrouting in windows and linux machine

- Open Windows Command Prompt and hit command “tracert html.com”

Output:

```
C:\Users\91937>tracert html.com

Tracing route to html.com [104.21.64.114]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  RTK_GW.domain.name [192.168.101.1]
  2     2 ms     2 ms     3 ms  103.93.97.66
  3    10 ms    13 ms    31 ms  103.93.97.90
  4    13 ms    12 ms    11 ms  10.200.200.9
  5     *        *        *     Request timed out.
  6    12 ms    11 ms    13 ms  14.143.171.25.static-pune.vsnl.net.in [14.143.171.25]
  7    21 ms    16 ms    17 ms  172.28.118.237
  8    16 ms    15 ms    15 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  9   225 ms   139 ms   139 ms  if-ae-2-2.tcore2.mlv-mumbai.as6453.net [180.87.38.2]
 10   171 ms   201 ms   201 ms  if-bundle-12-2.qcore4.ldn-london.as6453.net [180.87.39.21]
 11   190 ms     *      247 ms  195.219.213.138
 12   180 ms   202 ms   201 ms  195.219.213.131
 13   183 ms   201 ms   201 ms  104.21.64.114

Trace complete.

C:\Users\91937>
```

- we can do the same at linux also; just run the command “traceroute yoursite.com”

```
┌──(pentestplayer㉿Lucky)-[~]
└─$ traceroute google.com
traceroute to google.com (142.250.71.110), 30 hops max, 60 byte packets
 1  _gateway (192.168.101.1)  5.746 ms  5.390 ms  5.131 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Point 1

Point 2

This means that the target system could not be reached

- Point 1: 142.250.71.110 is the ip of target that which it has obtained by using the reverse DNS look up.
- Point 2: 30 hops means that traceroute will only route the first 30 routes between your system and the victim’s system.

Wrapping Up: Information Gathering & Reconnaissance

Congratulations! You've just completed one of the most critical modules in ethical hacking—**Information Gathering and Reconnaissance**. By now, you should have a solid understanding of how to lay the foundation for any hacking or penetration testing engagement. This module wasn't just about tools or commands—it was about strategy, mindset, and precision.

Here's a quick recap of what we've covered:

1. **Understanding the Basics**:
    - Differentiated between information gathering, reconnaissance, footprinting, and enumeration.
    - Explored how each phase contributes to identifying potential vulnerabilities.
2. **OSINT (Open-Source Intelligence)**:
    - Leveraged tools like Maltego, Google Dorking, and Shodan to gather public information.
    - Understood how to use advanced search operators to find sensitive data.
3. **Passive vs. Active Reconnaissance**:
    - Learned the subtle difference between passive methods (e.g., Whois lookups) and active techniques (e.g., scanning networks).
    - Practiced blending into the background while collecting crucial data.
4. **Network Scanning and Enumeration**:
    - Used Nmap, Netcat, and Nikto to identify live hosts, open ports, and services running on the target.
    - Performed banner grabbing and service fingerprinting to gather detailed insights.
5. **Social Engineering Recon**:
    - Observed how human interactions can provide information just as valuable as technical exploits.

Why This Module Matters

The success of every ethical hacking operation depends on how well you perform this phase. You've now mastered the ability to:

- Identify high-value targets and their vulnerabilities.
- Understand the importance of stealth and evasion.
- Lay the groundwork for advanced exploitation techniques.

What's Next?

Now that you've gathered intelligence, it's time to put that knowledge to work. In the upcoming modules, we'll dive into **exploitation, vulnerability assessment, and more advanced techniques.** Get ready to turn theory into action as we escalate from information gathering to real-world attacks.

Final Thought

Remember, the best hackers are not just tool users—they're strategists. Reconnaissance is about seeing the bigger picture and piecing it together. Keep practicing, stay curious, and continue to refine your skills.

Let’s move forward to the next phase of your ethical hacking journey—it only gets more exciting from here! 🚀