# 🛡️ Day 9 – Ethical Hacking

## 🔍 Topic: Finding Exploits

## 📌 Overview

After performing port scanning and service detection using tools like nmap, the next step in penetration testing is identifying known vulnerabilities or exploits for the services and software versions running on a target system. This process is often called exploit enumeration.  
  
The goal is to map the discovered service/version to a known CVE (Common Vulnerabilities and Exposures) and find a corresponding public exploit to further investigate or weaponize.

## 🔧 Tools Used

|  |  |
| --- | --- |
| Tool | Purpose |
| nmap | Port scanning and service version detection |
| Exploit-DB | Public exploit database (offline & online) |
| Rapid7 | Online vulnerability research and exploit frameworks (e.g., Metasploit) |
| GitHub | Open-source exploits and POCs |
| searchsploit | Offline tool to search for public exploits locally |
| mousepad | To view exploit code files |

## 🔍 Step-by-Step Process

### ✅ 1. Scan the Target with Nmap

We use Nmap to discover open ports and detect service versions:

**nmap -sS -sV <target-ip>**

- -sS: SYN scan (stealthy TCP scan)  
- -sV: Service version detection  
  
Example Output Snippet:  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)  
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))  
  
These versions are crucial for the next phase — searching for exploits.

### ✅ 2. Search for Exploits Manually (Online)

Once you have the version numbers (e.g., Apache 2.4.18), head to online resources:

#### 🔹 A. Exploit-DB

Website: https://www.exploit-db.com  
Purpose: Official and community-contributed public exploits and CVEs.  
Search for:  
Apache 2.4.18 exploit

#### 🔹 B. Rapid7 / Metasploit Framework

Website: https://www.rapid7.com/db/  
Purpose: Search CVEs, modules, and exploit POCs for Metasploit.  
Try keywords like:  
Apache 2.4.18  
OpenSSH 7.2p2

#### 🔹 C. GitHub

Search real-world, often working exploits from researchers or hackers.  
Use:  
site:github.com "Apache 2.4.18 exploit"

### ✅ 3. Use Searchsploit (Offline)

#### 🔸 What is searchsploit?

A command-line tool included in Kali Linux that searches the local copy of the Exploit-DB.  
Works offline.  
Faster and efficient for quick vulnerability lookup.

Example Usage:  
searchsploit Apache 2.4.18  
  
You may get outputs like:  
Apache HTTP Server 2.4.18 - mod\_http2 Denial of Service (DoS) | linux/dos/40002.txt  
Apache 2.4.18 - Remote Code Execution | linux/remote/12345.py

### ✅ 4. Download Exploit for Offline Use

Once you see a relevant exploit from searchsploit, copy its path and use the -m flag to copy it to your local directory.  
  
Example:  
searchsploit -m linux/remote/12345.py  
  
Now you can see it locally in your folder.

### ✅ 5. Read or Edit the Exploit Code

Use any text editor to view or modify the code (we use mousepad here):  
mousepad 12345.py  
  
Or you can use nano, vim, or gedit.

## 📁 Important Concepts

|  |  |
| --- | --- |
| Concept | Explanation |
| CVE | Public identifier for known vulnerabilities |
| PoC | Proof-of-Concept code that demonstrates exploitability |
| RCE / LFI / XSS / DoS | Types of attacks: Remote Code Exec, File Inclusion, Cross-site, Denial |
| Privilege Escalation | Gaining higher system access (e.g., root access via exploit) |
| Public Exploit | Exploit code available to the public for known vulnerabilities |

## 📌 Best Practices

- Always verify that the exploit version exactly matches the target.  
- Analyze PoC code before running it.  
- Prefer trusted sources: Exploit-DB, Rapid7, GitHub (official repos).  
- Use sandbox or VM environment for testing exploits (e.g., Metasploitable2, TryHackMe, VulnHub).

## 🧪 Example: Full Flow

1. Scan:  
nmap -sS -sV 10.10.98.129  
  
2. Found: Apache 2.4.18  
  
3. Run:  
searchsploit Apache 2.4.18  
  
4. Copy exploit:  
searchsploit -m linux/remote/12345.py  
  
5. View:  
mousepad 12345.py

## ✅ Summary Table

|  |  |  |
| --- | --- | --- |
| Step | Tool / Action | Example Command |
| Scan Target | nmap | nmap -sS -sV 10.10.98.129 |
| Search Online | Exploit-DB / Rapid7 / GitHub | Search "Apache 2.4.18 exploit" |
| Search Offline | searchsploit | searchsploit Apache 2.4.18 |
| Copy Exploit File | searchsploit -m <path> | searchsploit -m linux/remote/12345.py |
| View/Modify Code | mousepad, nano, vim | mousepad 12345.py |

## 🧠 Conclusion

Finding and analyzing exploits is a critical skill in ethical hacking. After fingerprinting services using Nmap, tools like Searchsploit, Exploit-DB, Rapid7, and GitHub help in mapping services to known vulnerabilities.  
  
This knowledge helps security professionals and bug bounty hunters to assess risks, exploit responsibly in labs, and patch or report vulnerabilities effectively.