Locating Public Exploits

One of the essential skills for any ethical hacker and penetration tester is the ability to locate and analyze public exploits. Public exploits are those that have been discovered, documented, and made available to the public, often through online repositories, forums, or databases.

1. Online Exploit Resources

At first, we have some online exploits resources and databases.

- **Exploit DB** - https://www.exploit-db.com

ExploitDB is an online database maintained by the Offsensive Security, the same folks that are behind Kali Linux which we are using. So, Exploit-DB contains a massive collection of real-world exploits and proof-of-concept code for various software vulnerabilities. It serves as a repository where we as a security researchers, ethical hackers, and penetration testers can find and study publicly available exploits.

- **Packet Storm** - https://packetstormsecurity.com/

There is another one called Packet Storm, It is also an online resource that serves as a library or database of computer security tools, exploits, advisories, and other information related to vulnerabilities and cyber threats.

- **Github** - Be cautious with the exploits

The third one we have is Github which is like a very famous website, if we are into the software development circle then you must have heard of it. Those of you who dont know, so GitHub is a website that provides an online space where you can store all the project files (chapters, code, images etc.) in one place. Think of it like a shared folder or locker that everyone can access.

Taking it as a online exploit resource, we can find many public exploits or POC of vulnerabilities from different authors and it is one of my favoruite place to find exploits.

But whenever you are downloading any exploit code on your machine from github that you will run against the target. Make sure, it is validated and has ample amount of stars.

- **Google Search Operators** - We can use the following search query to locate vulnerabilities affecting the *Microsoft Edge* browser and limit the results to only those exploits that are hosted on the Exploit Database website.

```
firefox --search "Microsoft Edge site:exploit-db.com"
```

---

2. Offline Exploit Resources

Now lets talk about some offline exploit resources. There is a fantastic tool called searchsploit which uses the exploit DB database but offline. Lets see how it works.

Searchsploit

- First lets Install and update the exploitdb package. So that we can use it with its full power and capabilites.

```
sudo apt update && sudo apt install exploitdb
```

- List all the file inside the exploit database.

```
kali@kali:~$ ls -1 /usr/share/exploitdb/
exploits
files_exploits.csv
files_shellcodes.csv
shellcodes
```

- The exploits are arranges as per the platform.

```
kali@kali:~$ ls -1 /usr/share/exploitdb/exploits
aix
alpha
android
arm
ashx
```

```
asp
aspx
atheos
beos
bsd
bsd_x86
cfm
cgi
freebsd
freebsd_x86
```

- Search for the exploit using searchsploit.

```
searchsploit remote smb microsoft windows
```

- Copy the exploit to the current working directory either by exploit path or EDB ID.

```
kali@kali:~$ searchsploit -m windows/remote/48537.py

  Exploit: Microsoft Windows - 'SMBGhost' Remote Code Execution
      URL: https://www.exploit-db.com/exploits/48537
     Path: /usr/share/exploitdb/exploits/windows/remote/48537.py
File Type: Python script, ASCII text executable, with very long lines
(343)

Copied to: /home/kali/48537.py

kali@kali:~$ searchsploit -m 42031
  Exploit: Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code
Execution (MS17-010)
      URL: https://www.exploit-db.com/exploits/42031
     Path: /usr/share/exploitdb/exploits/windows/remote/42031.py
File Type: Python script, ASCII text executable

Copied to: /home/kali/42031.py
```

---

3. Nmap NSE Scripts

At last, we have Nmap NSE exploit scripts.

So we have already seen the capabilities of nmap in our previous modules. But Nmap also has some exploitation scripts that can be used in order to not just scan but also exploit the target.

- Check for NSE scripts that can be used for exploitation.

```
grep Exploits /usr/share/nmap/scripts/*.nse
```

- Display information about the particular nmap NSE exploit script.

```
nmap --script-help=clamav-exec.nse
```

These are primarily some old exploits in this list and i would not recommend using them directly on the target without knowing the aftermath of the script. But keeping this option in your arsenal while searching for exploits is a must, in my opinion.
