

【Exploit】SearchSploit

SearchSploit 是一個命令行搜索工具，用於在本地系統上搜索 Exploit Database 存檔。這個存檔預設包含在 Kali Linux 中的 exploitdb 包中。我們建議在進行任何評估之前更新該包，以確保安裝了最新的攻擊代碼。可以使用以下命令更新該包：

```
kali@kali:~$ sudo apt update && sudo apt install exploitdb
[sudo] password for kali:
...
The following packages will be upgraded:
  exploitdb
...
Setting up exploitdb (20220526-0kali1) ...
...
```

上述命令將更新本地 Exploit Database 存檔的副本，存放在 /usr/share/exploitdb/ 目錄下。該目錄分為兩個主要部分，即 exploits 和 shellcodes。/usr/share/exploitdb/ 目錄包含每個 exploits 和 shellcodes 子目錄的 CSV 文件。每個 CSV 文件包含其相應子目錄中所有文件的文件信息。這些 CSV 文件包含與 Exploit DB 網站相似的信息，如 EDB-ID、標題、作者、平台等，這些信息我們之前已經介紹過。

當我們重定向到 exploits 目錄時，我們會找到許多子目錄，其中包含所有的攻擊。這些子目錄是根據操作系統、架構、腳本語言等進行分類的。例如，linux 子目錄包含所有與 Linux 相關的攻擊。

```
kali@kali:~$ ls -l /usr/share/exploitdb/exploits
aix
alpha
android
arm
ashx
asp
aspx
atheos
beos
bsd
bsd_x86
cfm
cgi
freebsd
freebsd_x86
...
```

手動搜索 Exploit Database 絕對不是理想的方法，特別是考慮到存檔中的大量攻擊。這就是 searchsploit 工具派上用場的地方。

我們可以在命令行中運行 searchsploit，而無需使用任何參數來顯示其用法：

```
kali@kali:~$ searchsploit
Usage: searchsploit [options] term1 [term2] ... [termN]
...
```

就內建例子來看，searchsploit 允許我們通過提供的不同搜索選項作為參數進行整個存檔的搜索並顯示結果。

```
=====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | json_pp

For more examples, see the manual: https://www.exploit-db.com/searchsploit
```

這些選項允許我們縮小搜索範圍、更改輸出格式、更新 exploitdb 套件等。

```
=====
```

```
Options
=====
## Search Terms
-c, --case [Term]    Perform a case-sensitive search (Default is inSEnsITive)
-e, --exact [Term]   Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "-t"]
                    e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
-s, --strict          Perform a strict search, so input values must exist, disabling fuzzy search for version range
                    e.g. "1.1" would not be detected in "1.0 < 1.3")
-t, --title [Term]   Search JUST the exploit title (Default is title AND the file's path)
                    --exclude="term"    Remove values from results. By using "|" to separate, you can chain multiple values
                    e.g. --exclude="term1|term2|term3"

## Output
-j, --json [Term]    Show result in JSON format
-o, --overflow [Term] Exploit titles are allowed to overflow their columns
-p, --path [EDB-ID]  Show the full path to an exploit (and also copies the path to the clipboard if possible)
-v, --verbose        Display more information in output
-w, --www [Term]     Show URLs to Exploit-DB.com rather than the local path
                    --id                Display the EDB-ID value rather than local path
                    --colour           Disable colour highlighting in search results
...
```

最後，幫助菜單的「Notes」部分揭示了一些有用的搜索提示。

```
=====
Notes
=====
* You can use any number of search terms
* By default, search terms are not case-sensitive, ordering is irrelevant, and will search between version ranges
* Use '-c' if you wish to reduce results by case-sensitive searching
* And/Or '-e' if you wish to filter results by using an exact match
* And/Or '-s' if you wish to look for an exact version match
* Use '-t' to exclude the file's path to filter the search results
* Remove false positives (especially when searching using numbers - i.e. versions)
* When using '--nmap', adding '-v' (verbose), it will search for even more combinations
* When updating or displaying help, search terms will be ignored
```

例如，我們可以使用以下語法搜索針對 Windows 操作系統上的 SMB 服務的所有可用遠程攻擊：

```
kali@kali:~$ searchsploit remote smb microsoft windows
```

Exploit Title	Path
Microsoft DNS RPC Service - 'extractQuotedChar()' Remote Overflow 'SMB' (MS07-029) (Metasploit)	windows/remote/16366.rb
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	windows/remote/43970.rb
Microsoft Windows - 'SMBGhost' Remote Code Execution	windows/remote/48537.py
Microsoft Windows - 'srv2.sys' SMB Code Execution (Python) (MS09-050)	windows/remote/40280.py
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050)	windows/remote/14674.txt
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050) (Metasploit)	windows/remote/16363.rb
Microsoft Windows - SMB Relay Code Execution (MS08-068) (Metasploit)	windows/remote/16360.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	windows/dos/41891.rb
Microsoft Windows - SmbRelay3 NTLM Replay (MS08-068)	windows/remote/7125.txt
Microsoft Windows 2000/XP - SMB Authentication Remote Overflow	windows/remote/20.txt
Microsoft Windows 2003 SP2 - 'ERRATICGOPHER' SMB Remote Code Execution	windows/remote/41929.py
Microsoft Windows 2003 SP2 - 'RRAS' SMB Remote Code Execution	windows/remote/44616.py
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows/remote/42315.py

```
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/42030.py
Microsoft Windows 95/Windows for Workgroups - 'smbclient' Directory Traversal | windows/remote/20371.txt
Microsoft Windows NT 4.0 SP5 / Terminal Server 4.0 - 'Pass the Hash' with Modified SMB Client | windows/remote/19197.txt
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py
Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death (MS07-063) | windows/dos/9594.txt
-----
Shellcodes: No Results
Papers: No Results
```

具有搜索參數的攻擊將顯示在輸出中。為了演示，假設我們希望在參與過程中使用上面突出顯示的兩個攻擊。為了演示，假設我們枚舉了兩個對 SMBGhost 和 EternalBlue 漏洞易受攻擊的 SMB 伺服器。

如果需要修改攻擊，我們可以使用 `-m` 選項將攻擊複製到當前工作目錄。將攻擊複製到當前工作目錄的好處是更容易組織在參與過程中使用的攻擊並將其與正在測試的系統相關聯。

所有本地攻擊在釋放新的 exploitdb 套件時都會被覆蓋，因此在原始位置修改攻擊會導致我們損失這些更改。

讓我們使用 `-m` 選項複製這兩個攻擊。我們可以使用這些攻擊的路徑或 EDB-ID 進行複製，這些 ID 可以在其路徑名稱中找到。

```
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
```

我們想要的攻擊現在已複製到我們當前的工作目錄中。第一個命令執行複製了攻擊文件，第二個命令執行複製了攻擊，通過其 EDB-ID 進行標識。

🕒 修訂版本 #1

★ 由 treeman 建立於 11 🍀🍀🍀🍀 2023 00:49:55

✍ 由 treeman 更新於 7 🍀@🍀🍀 2024 19:30:26