Using ExploitDB and Metasploit for Vulnerability Research

When conducting a penetration test there are two types of tools, we can use to help us identify exploits for specific vulnerabilities. These tools are called ExploitDB and Metasploit. ExploitDB tools for vulnerability research is called **`searchsploit`**. For example.

```
$ searchsploit
  Usage: searchsploit [options] term1 [term2] ... [termN]
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
   -c, --case     [Term]      Perform a case-sensitive search.
   -e, --exact    [Term]      Perform an EXACT & order match on exploit title.
   -s, --strict               Perform a strict search.
   -t, --title    [Term]      Search JUST the exploit title.
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

We can use **`searchsploit`** to search for specific vulnerabilities. Critical to the success of this is our ability to identify and profile the target system. So, support that we want to look for a local vulnerability on Windows Server 2003, then we could do the following:

```
$ searchsploit local Windows 2003
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (MS08-066)
                                                         | windows/local/6757.txt
Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (MS11-080)
                                                         | windows/local/18176.py
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

We can now compile, upload and use the exploits as part of a penetration test. Metasploit provides a similar search capability vie the search command. For Example:

```
$ msfconsole
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
msf6 > search
Usage: search [<options>] [<keywords>:<value>]
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
msf6 >
```

Metasploit allows us to search for vulnerabilities in terms of CVE numbers, Bugtraq ID numbers, type of exploit, the platform that the exploit is required to run on. For example:

```
msf6 > search CVE:2009 type:exploit MS09

#  Name               Disclosure Date        Rank.      Check        Description
-  ----               ---------------        ----       -----        -----------
0  exploit/windows/browser/ms09_002_memory_corruption      2009-02-10       normal
No    MS09-002 Microsoft Internet Explorer 7 CFunctionPointer Uninitialized Memory
Corruption
1  exploit/windows/smb/ms09_050_smb2_negotiate_func_index   2009-09-07        good
No        MS09-050  Microsoft  SRV2.SYS  SMB  Negotiate  ProcessID  Function  Table
Dereference
2  exploit/windows/ftp/ms09_053_ftpd_nlst                  2009-08-31       great
No    MS09-053 Microsoft IIS FTP Server NLST Response Overflow
Interact  with  a  module  by  name  or  index.  For  example  info  6,  use  6  or  use
exploit/windows/browser/ms09_043_owc_msdso
msf6 >
```

So, in the above examine we are look for CVE exploits published on 2009 that also Microsoft Security Bulletins published on 2009. Use **`msfconsole`** we can select which exploit we want to use using the **`use`** command.