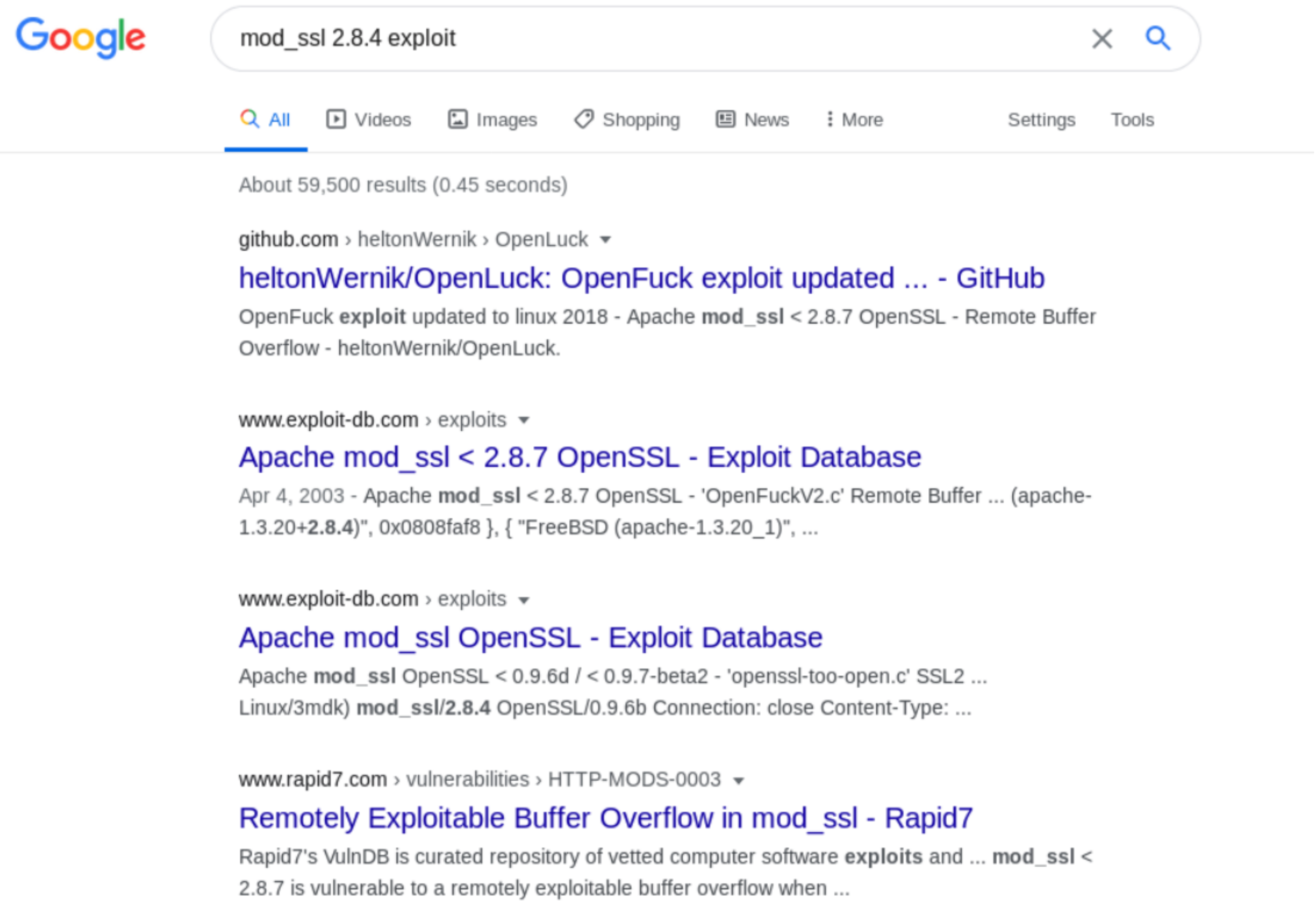
Identifying and Researching Potential Vulnerabilities

From our scanning and enumeration of the Kioptrix machine we have found the following key information:

```
80/443 - Open - 192.168.229.133
Default webpage - Apache - PHP
Information Disclosure - 404 page
information Disclosure - server headers disclose version information

80/tcp open http        Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4
OpenSSL/0.9.6b)

mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow
which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2002-0082, OSVDB-756.

SMB
Unix (Samba 2.2.1a)

Webalizer Version 2.01 - http://192.168.229.133/usage/usage_201911.html

SSH
OpenSSH 2.9p2
```

Let's do some research on `mod_ssl 2.8.4` with a simple google search as shown below:



About 59,500 results (0.45 seconds)

github.com › heltonWernik › OpenLuck

heltonWernik/OpenLuck: OpenFuck exploit updated ... - GitHub

OpenFuck **exploit** updated to linux 2018 - Apache **mod_ssl** < 2.8.7 OpenSSL - Remote Buffer Overflow - heltonWernik/OpenLuck.

www.exploit-db.com › exploits

Apache mod_ssl < 2.8.7 OpenSSL - Exploit Database

Apr 4, 2003 - Apache **mod_ssl** < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer ... (apache-1.3.20+**2.8.4**)", 0x0808faf8 }, { "FreeBSD (apache-1.3.20_1)", ...

www.exploit-db.com › exploits

Apache mod_ssl OpenSSL - Exploit Database

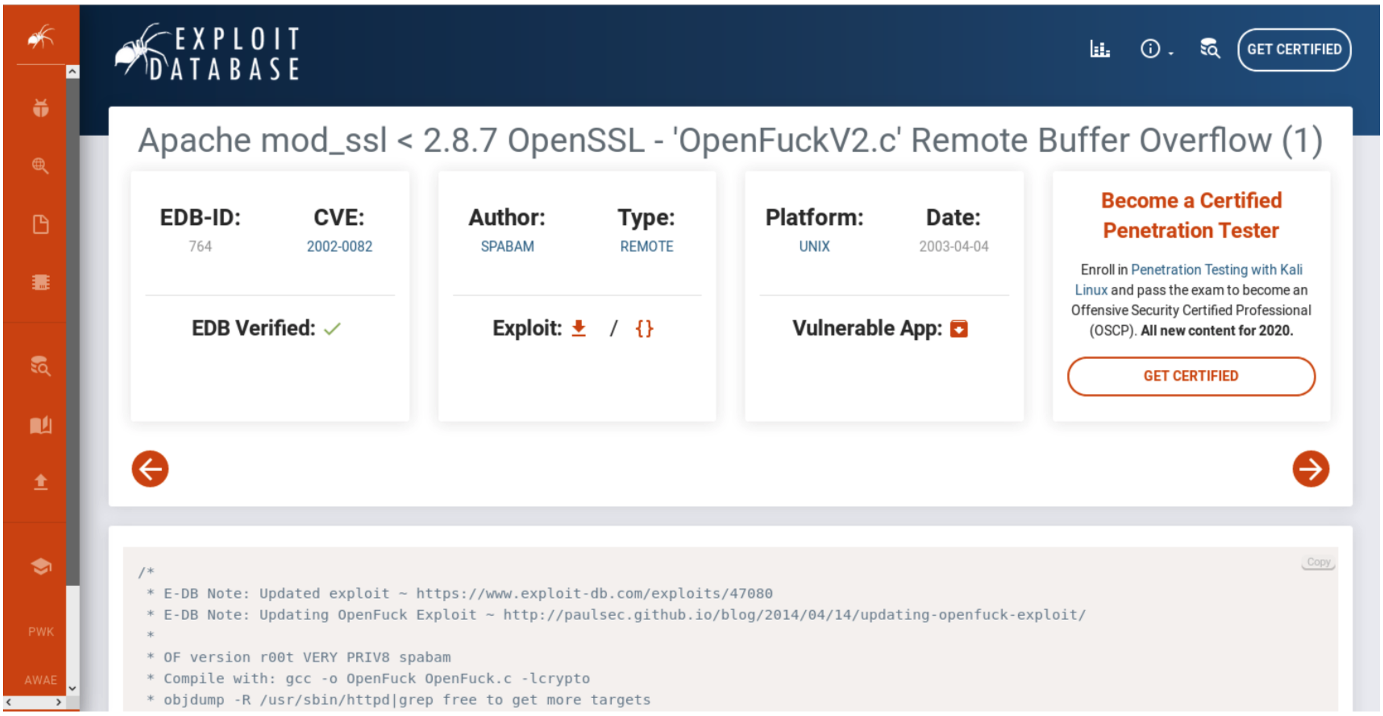
Apache **mod_ssl** OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 ... Linux/3mdk) **mod_ssl/2.8.4** OpenSSL/0.9.6b Connection: close Content-Type: ...

www.rapid7.com › vulnerabilities › HTTP-MODS-0003

Remotely Exploitable Buffer Overflow in mod_ssl - Rapid7

Rapid7's VulnDB is curated repository of vetted computer software **exploits** and ... **mod_ssl** < 2.8.7 is vulnerable to a remotely exploitable buffer overflow when ...

Exploit-db is a good resource to start with. It also includes the exploit code so we can review the code and try to make sense of it.



Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
764	2002-0082	SPABAM	REMOTE	UNIX	2003-04-04
EDB Verified: ✓		Exploit: ⬇ / {}		Vulnerable App:	

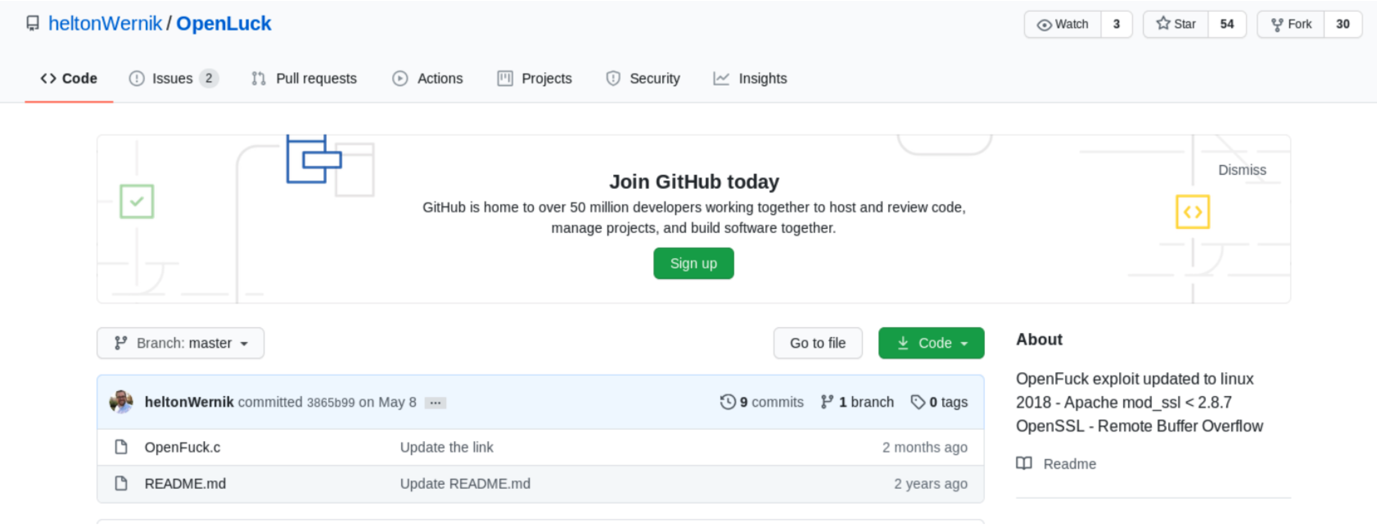
Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). **All new content for 2020.**

GET CERTIFIED

```
/*
 * E-DB Note: Updated exploit ~ https://www.exploit-db.com/exploits/47080
 * E-DB Note: Updating OpenFuck Exploit ~ http://paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
 *
 * OF version r00t VERY PRIV8 spabam
 * Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
 * objdump -R /usr/sbin/httpd|grep free to get more targets
```

We will also look at the github resource which is also good as well (shown below):



Join GitHub today

GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

heltonWernik committed 3865b99 on May 8 · 9 commits · 1 branch · 0 tags

OpenFuck.c	Update the link	2 months ago
README.md	Update README.md	2 years ago

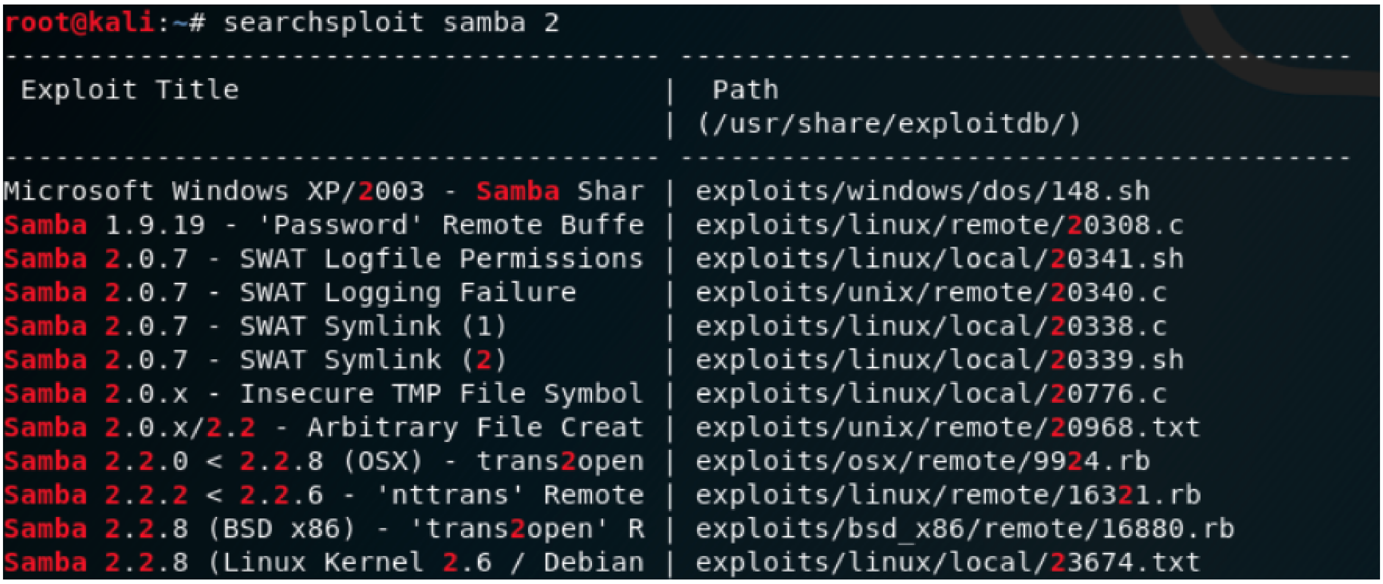
About

OpenFuck exploit updated to linux 2018 - Apache mod_ssl < 2.8.7 OpenSSL - Remote Buffer Overflow

We can also do a google search for `Apache httpd 1.3.20`. We will find a `cvedetails` resource. If the score of the vulnerability is red or tending to red/orange, it is likely vulnerable.

Another resource we can use is `Rapid7`.

We can also do some research in the terminal using a tool called `searchsploit`. Searchsploit is an "offline" version of Exploit-db as shown below:



```
root@kali:~# searchsploit samba 2
--------------------------------------- ----------------------------------------
 Exploit Title                         |  Path
                                       | (/usr/share/exploitdb/)
--------------------------------------- ----------------------------------------
Microsoft Windows XP/2003 - Samba Shar | exploits/windows/dos/148.sh
Samba 1.9.19 - 'Password' Remote Buffe | exploits/linux/remote/20308.c
Samba 2.0.7 - SWAT Logfile Permissions | exploits/linux/local/20341.sh
Samba 2.0.7 - SWAT Logging Failure     | exploits/unix/remote/20340.c
Samba 2.0.7 - SWAT Symlink (1)         | exploits/linux/local/20338.c
Samba 2.0.7 - SWAT Symlink (2)         | exploits/linux/local/20339.sh
Samba 2.0.x - Insecure TMP File Symbol | exploits/linux/local/20776.c
Samba 2.0.x/2.2 - Arbitrary File Creat | exploits/unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open | exploits/osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote | exploits/linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' R | exploits/bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian | exploits/linux/local/23674.txt
```

TIP: when using searchsploit, do not be too specific with your search terms.