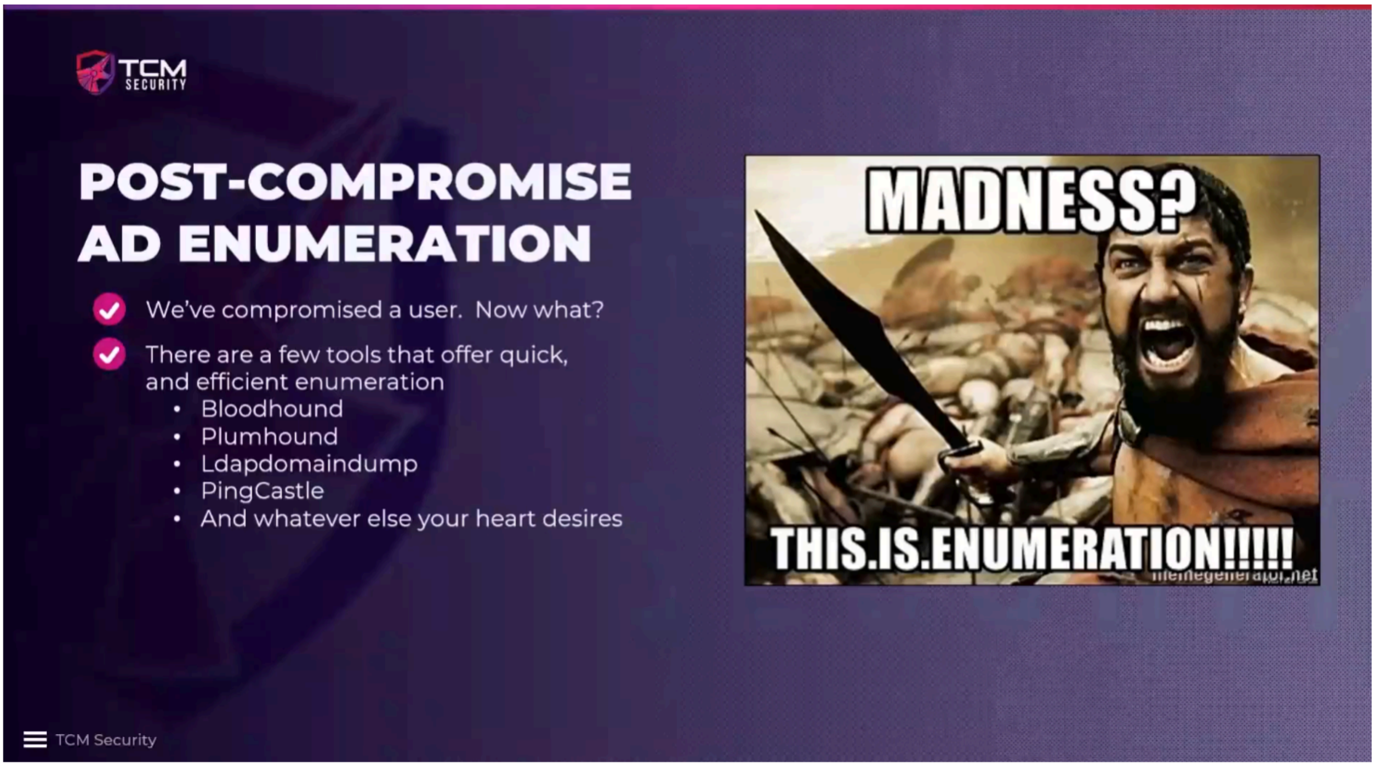
91.0 - Introduction - Post Compromise AD Enumeration



TCM SECURITY

POST-COMPROMISE AD ENUMERATION

- ✓ We've compromised a user. Now what?
- ✓ There are a few tools that offer quick, and efficient enumeration
  - Bloodhound
  - Plumhound
  - Ldapdomaindump
  - PingCastle
  - And whatever else your heart desires

We are going to be learning the how and what tools to use to enumerate an Active Directory Domain Controller machine.

91.1 - ldapdomaindump - Domain Enumeration

We have used this tool before. We used to perform the IPv6 Relay Attack.

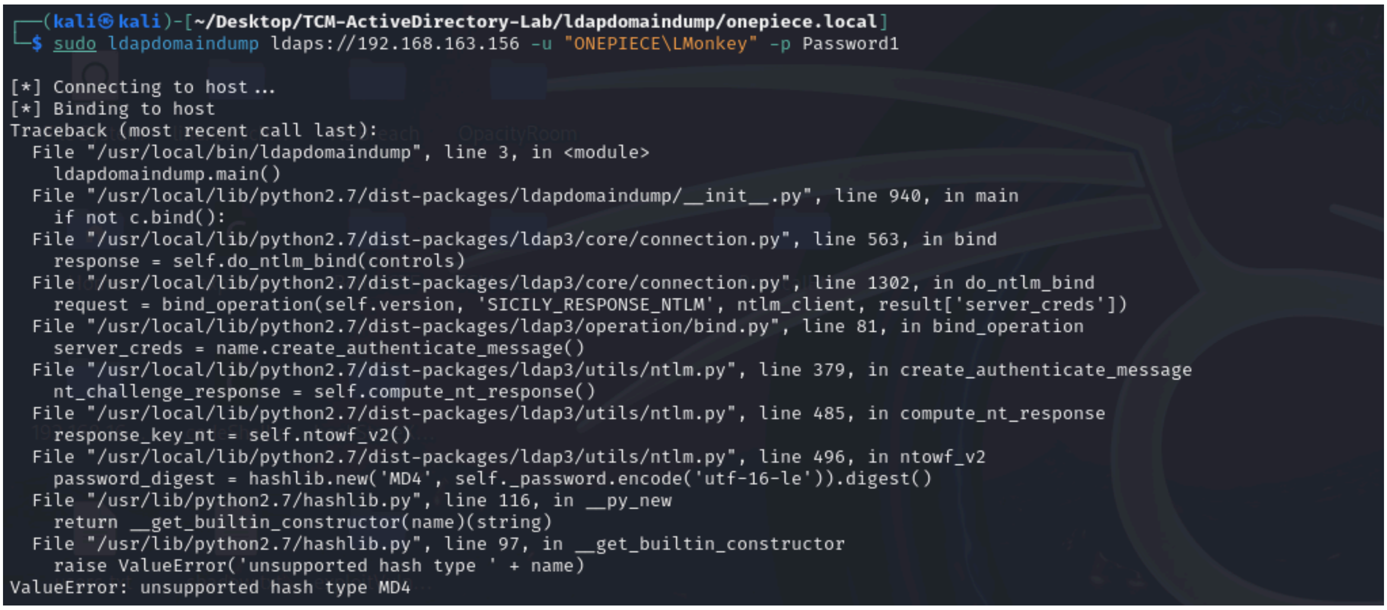
If IPv6 is not possible in the network, this tool will help us with other attacks.

To run this tool in such scenario, we can run this tool as follows:

1 - Create a directory

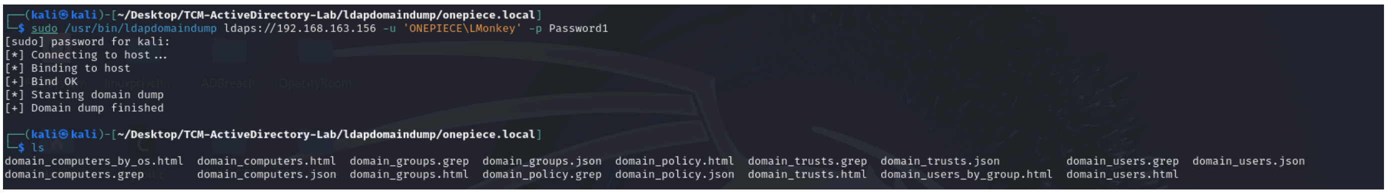
2 - cd into it

3 - Run: "#sudo ldapdomaindump ldaps://DC_IP -u "ONEPIECE\LMonkey" -p Password1"   If we want to output to a specific folder we can use "-o PATH/TO/DIR". if we omit the flag, it will save to the current pwd.



```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
└─$ sudo ldapdomaindump ldaps://192.168.163.156 -u "ONEPIECE\LMonkey" -p Password1

[*] Connecting to host ...
[*] Binding to host
Traceback (most recent call last):
  File "/usr/local/bin/ldapdomaindump", line 3, in <module>
    ldapdomaindump.main()
  File "/usr/local/lib/python2.7/dist-packages/ldapdomaindump/__init__.py", line 940, in main
    if not c.bind():
  File "/usr/local/lib/python2.7/dist-packages/ldap3/core/connection.py", line 563, in bind
    response = self.do_ntlm_bind(controls)
  File "/usr/local/lib/python2.7/dist-packages/ldap3/core/connection.py", line 1302, in do_ntlm_bind
    request = bind_operation(self.version, 'SICILY_RESPONSE_NTLM', ntlm_client, result['server_creds'])
  File "/usr/local/lib/python2.7/dist-packages/ldap3/operation/bind.py", line 81, in bind_operation
    server_creds = name.create_authenticate_message()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 379, in create_authenticate_message
    nt_challenge_response = self.compute_nt_response()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 485, in compute_nt_response
    response_key_nt = self.ntowf_v2()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 496, in ntowf_v2
    password_digest = hashlib.new('MD4', self._password.encode('utf-16-le')).digest()
  File "/usr/lib/python2.7/hashlib.py", line 116, in __py_new
    return __get_builtin_constructor(name)(string)
  File "/usr/lib/python2.7/hashlib.py", line 97, in __get_builtin_constructor
    raise ValueError('unsupported hash type ' + name)
ValueError: unsupported hash type MD4
```

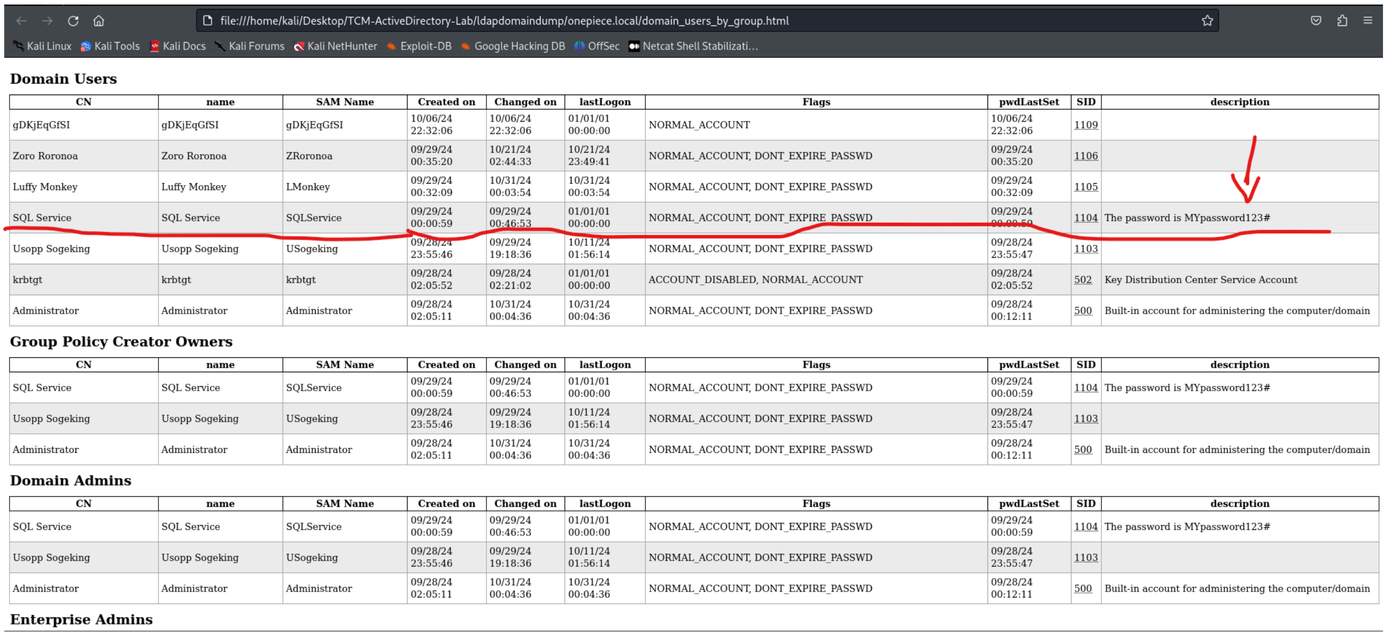
Advised to use the absolute path of the command software.



```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
└─$ sudo /usr/bin/ldapdomaindump ldaps://192.168.163.156 -u 'ONEPIECE\LMonkey' -p Password1
[sudo] password for kali:
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
└─$ ls
domain_computers_by_os.html  domain_computers.html  domain_groups.grep  domain_groups.json  domain_policy.html  domain_trusts.grep  domain_trusts.json          domain_users.grep  domain_users.json
domain_computers.grep        domain_computers.json  domain_groups.html  domain_policy.grep  domain_policy.json  domain_trusts.html  domain_users_by_group.html  domain_users.html
```

It worked!

This is all very good information. Here, we can see the that password of the service Admin account we created, and left in the description is picked up by the ldapdomaindump.



file:///home/kali/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local/domain_users_by_group.html

Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
gDKjEqGfSI	gDKjEqGfSI	gDKjEqGfSI	10/06/24 22:32:06	10/06/24 22:32:06	01/01/01 00:00:00	NORMAL_ACCOUNT	10/06/24 22:32:06	1109	
Zoro Roronoa	Zoro Roronoa	ZRoronoa	09/29/24 00:35:20	10/21/24 02:44:33	10/21/24 23:49:41	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:35:20	1106	
Luffy Monkey	Luffy Monkey	LMonkey	09/29/24 00:32:09	10/31/24 00:03:54	10/31/24 00:03:54	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:32:09	1105	
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is MYpassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
krbtgt	krbtgt	krbtgt	09/28/24 02:05:52	09/28/24 02:21:02	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	09/28/24 02:05:52	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain

Group Policy Creator Owners

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is MYpassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain

Domain Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is MYpassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain

Enterprise Admins

Obviously we are looking for low hanging fruits first. We are looking for domain admin accounts, if account is expired or not, domain users, and much more. All information coming from the dump is going to be valuable.

And this is one method to enumerate Active Directory Domain.

91.2 - Bloodhound - Domain Enumeration

1 - install latest version of bloodhound (#sudo pip install bloodhound)

This will install the latest and greatest. And, if there is not already, it is going to install the ingestors.

2 - Now, we are going to run "#sudo neo4j console". This is required for us to be able to run bloodhound. We are going to be hosting the program on the local host, and a link should show up in the output of the command with the link to the just started service. We can open it and interact with the program through a web browser. The right term is remote interface. So, we have a remote interface that gets spin up for us, so we can use the features of the program. We can right rick and select "open link".

3 - We are going to need to sign in, and set new password for account. The default credentials are user: neo4j , and password: neo4j . Change password to : neo4j1 . We need to have this running in order to run bloodhound. So, keep it running, and move along.

4 - Run "# sudo bloodhound". If you have any data, clear that out.

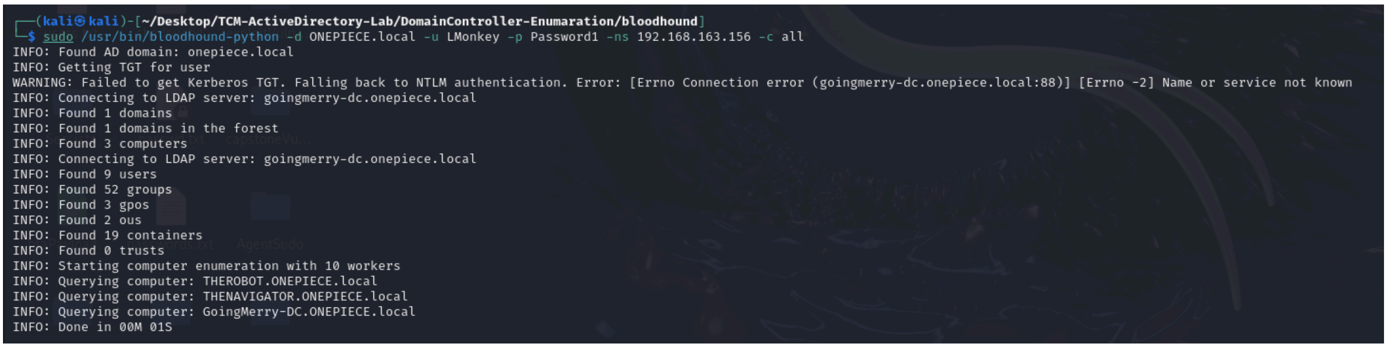
5 - Lets make a directory. "cd" into it.

6 - Run "#sudo bloodhound-python -d ONEPIECE.local -u LMonkey -p Password1 -ns 192.168.163.156 -c all"

This is the command that generates the dump.

-ns for Name Server, which in our case is going to be the Domain Controller IP Address.

-c is what are we collecting. in this case "all".



```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/DomainController-Enumaration/bloodhound]
└─$ sudo /usr/bin/bloodhound-python -d ONEPIECE.local -u LMonkey -p Password1 -ns 192.168.163.156 -c all
INFO: Found AD domain: onepiece.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (goingmerry-dc.onepiece.local:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: goingmerry-dc.onepiece.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: goingmerry-dc.onepiece.local
INFO: Found 9 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: THEROBOT.ONEPIECE.local
INFO: Querying computer: THENAVIGATOR.ONEPIECE.local
INFO: Querying computer: GoingMerry-DC.ONEPIECE.local
INFO: Done in 00M 01S
```

Tadah!

We are going to import all the data into bloodhound.

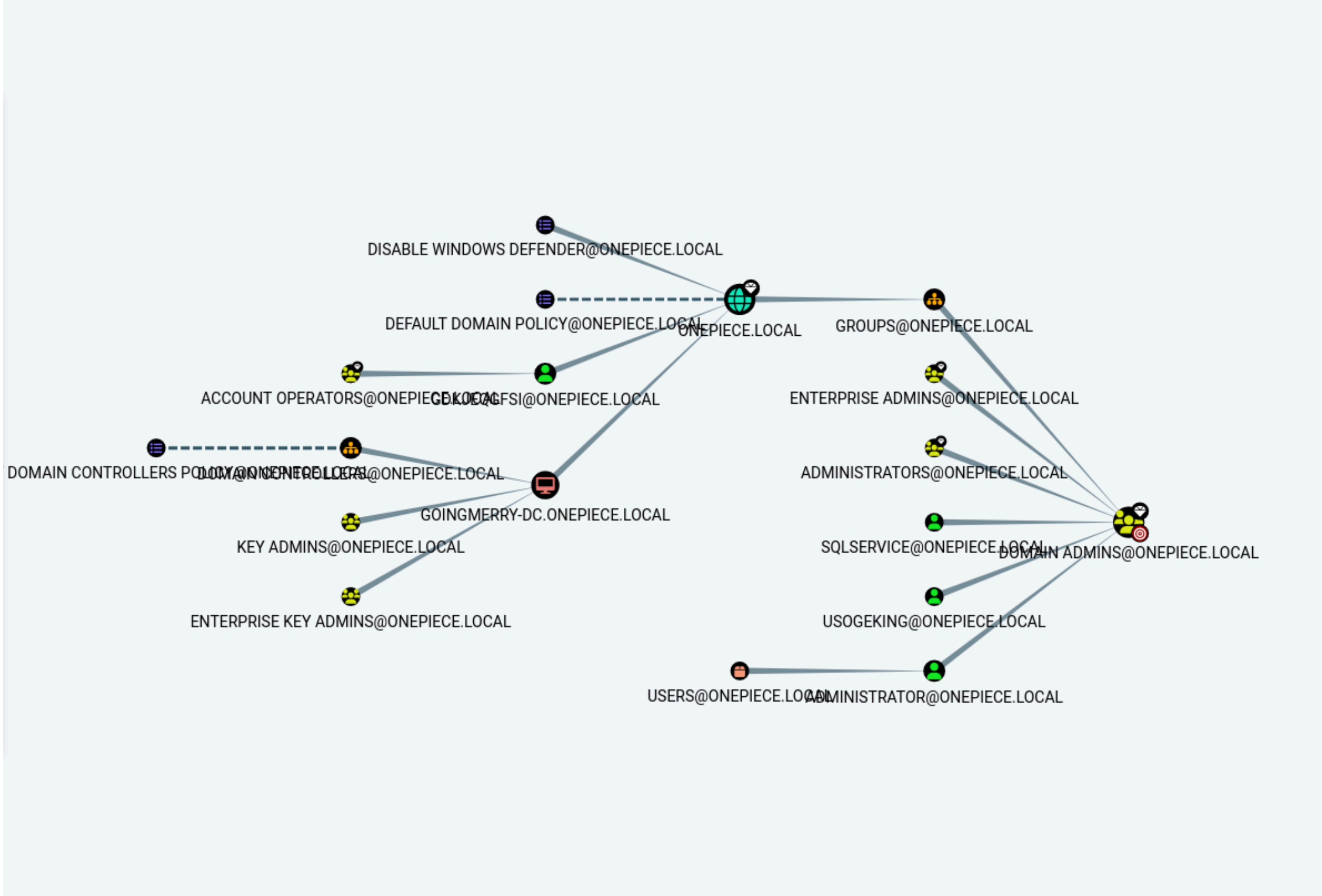
We want to go to bloodhound remote interface > upload data > select all that you want, we can select all of them > open.

The nice thing about Bloodhound is that it generates graphics and it shows the data in a easy to ready format, which allows for a quicker and better understanding of what we are dealing with.

Explore as much as you can.

"Shortest Paths" section under the Analysis tab seems to be really interesting.

"Kerberos Interaction" under the Analysis tab is also very valuable information.


DISABLE WINDOWS DEFENDER@ONEPIECE.LOCAL
DEFAULT DOMAIN POLICY@ONEPIECE.LOCAL
ONEPIECE.LOCAL
GROUPS@ONEPIECE.LOCAL
ACCOUNT OPERATORS@ONEPIECE.LOCAL
GE[illegible]FSI@ONEPIECE.LOCAL
ENTERPRISE ADMINS@ONEPIECE.LOCAL
DOMAIN CONTROLLERS POLICY@ONEPIECE.LOCAL
DOMAIN CONTROLLERS@ONEPIECE.LOCAL
ADMINISTRATORS@ONEPIECE.LOCAL
GOINGMERRY-DC.ONEPIECE.LOCAL
KEY ADMINS@ONEPIECE.LOCAL
SQLSERVICE@ONEPIECE.LOCAL
DOMAIN ADMINS@ONEPIECE.LOCAL
ENTERPRISE KEY ADMINS@ONEPIECE.LOCAL
USOGEKING@ONEPIECE.LOCAL
USERS@ONEPIECE.LOCAL
ADMINISTRATOR@ONEPIECE.LOCAL

Shortest Path to Domain Admin accounts.

91.3 - Plumbhound - Domain Enumeration

1 - We need to leave Bloodhound running for this. So, do not even bother to close it. If you already did, go back, and get it up and running.

2 - Search for Plumhound. Go to the GitHub repo and get the https address to clone it.

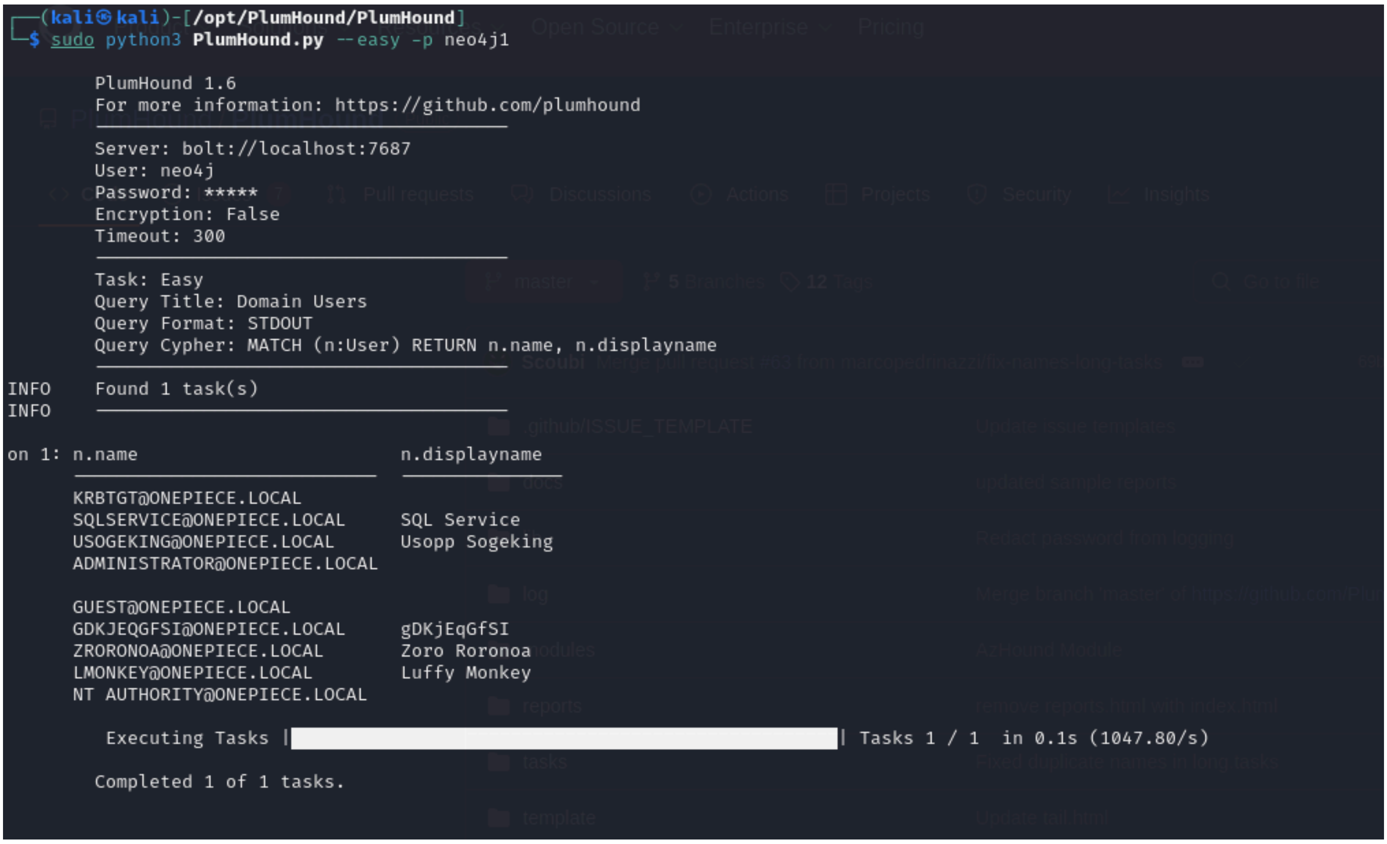
3 - Git and clone the repo. Best to put it under the "/opt" folder. Make new dir, and install the repo in there.

4 - After we downloaded it, we are going to need to install it. To do that we can run "#sudo pip3 install -r requirements.txt" from within the directory which has the downloaded data from the github repo.

Now, we are going to be running the tool.

5 - We can run it by issuing the command "#sudo python3 PlumHound.py --easy -p neo4j1". Remember, we need Bloodhound up and running.

This command will be just a test, that is why we are using --easy. This is just to make sure it is working properly, and we are actually pulling the data from the domain.

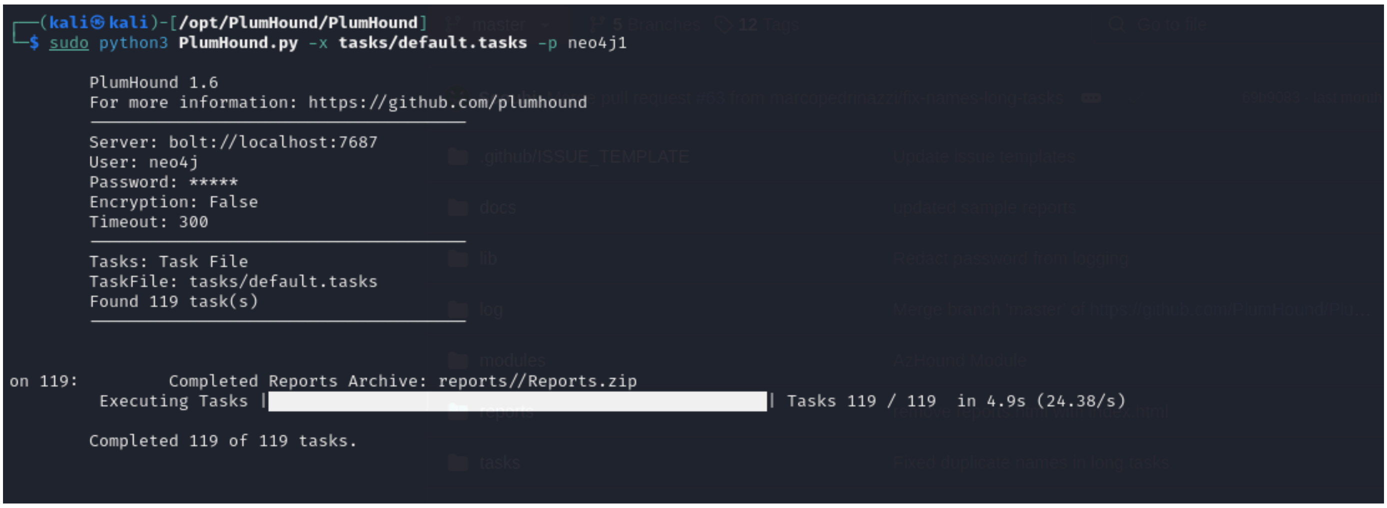


```
┌──(kali㉿kali)-[/opt/PlumHound/PlumHound]
└─$ sudo python3 PlumHound.py --easy -p neo4j1

        PlumHound 1.6
        For more information: https://github.com/plumhound
        ──────────────────────────────────────
        Server: bolt://localhost:7687
        User: neo4j
        Password: *****
        Encryption: False
        Timeout: 300
        ──────────────────────────────────────
        Task: Easy
        Query Title: Domain Users
        Query Format: STDOUT
        Query Cypher: MATCH (n:User) RETURN n.name, n.displayname
        ──────────────────────────────────────
INFO    Found 1 task(s)
INFO    ──────────────────────────────────────

on 1: n.name                        n.displayname
      ───────────────────────────   ──────────────
      KRBTGT@ONEPIECE.LOCAL
      SQLSERVICE@ONEPIECE.LOCAL     SQL Service
      USOGEKING@ONEPIECE.LOCAL      Usopp Sogeking
      ADMINISTRATOR@ONEPIECE.LOCAL

      GUEST@ONEPIECE.LOCAL
      GDKJEQGFSI@ONEPIECE.LOCAL     gDKjEqGfSI
      ZRORONOA@ONEPIECE.LOCAL       Zoro Roronoa
      LMONKEY@ONEPIECE.LOCAL        Luffy Monkey
      NT AUTHORITY@ONEPIECE.LOCAL

         Executing Tasks |██████████████████████████████████████████████████| Tasks 1 / 1  in 0.1s (1047.80/s)

        Completed 1 of 1 tasks.
```

We can see it is working properly.

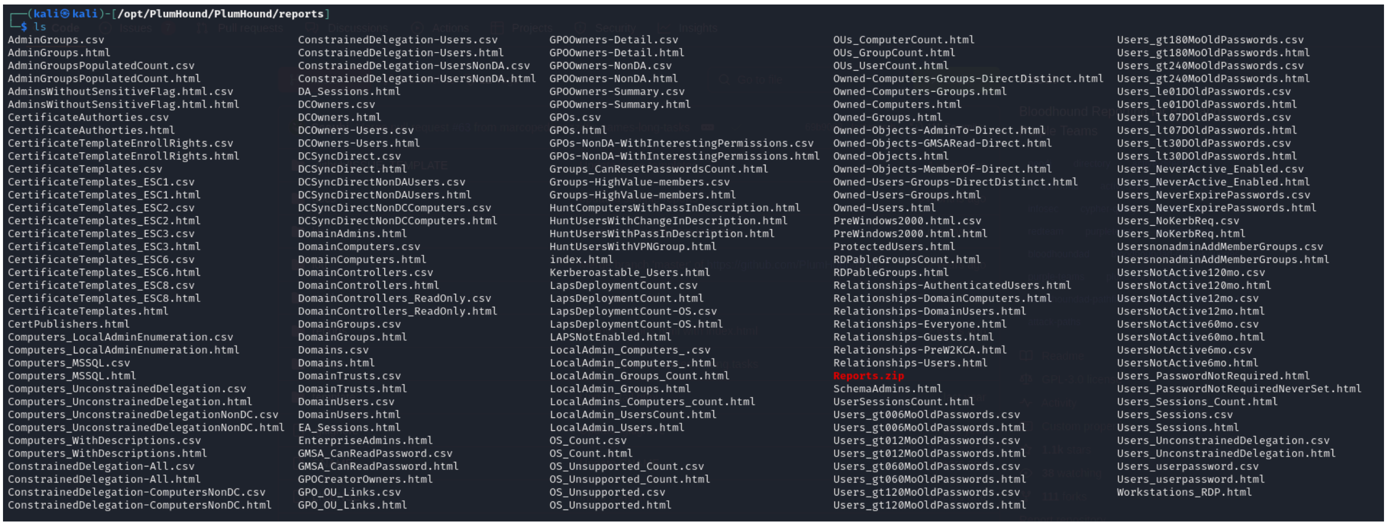
6 - We are going to run "#sudo python3 PlumHound.py -x tasks/default.tasks -p neo4j1"

We can also check the other modules, and features scans we can use in PlumHound.



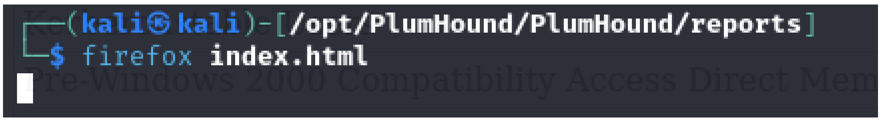
```
┌──(kali㉿kali)-[/opt/PlumHound/PlumHound]
└─$ sudo python3 PlumHound.py -x tasks/default.tasks -p neo4j1

        PlumHound 1.6
        For more information: https://github.com/plumhound
        ──────────────────────────────────────────
        Server: bolt://localhost:7687
        User: neo4j
        Password: *****
        Encryption: False
        Timeout: 300
        ──────────────────────────────────────────
        Tasks: Task File
        TaskFile: tasks/default.tasks
        Found 119 task(s)
        ──────────────────────────────────────────


on 119:         Completed Reports Archive: reports//Reports.zip
         Executing Tasks |██████████████████████████████████████████████| Tasks 119 / 119  in 4.9s (24.38/s)

        Completed 119 of 119 tasks.
```

This will create a folder with all the reports called "reports", and a zip file as well.

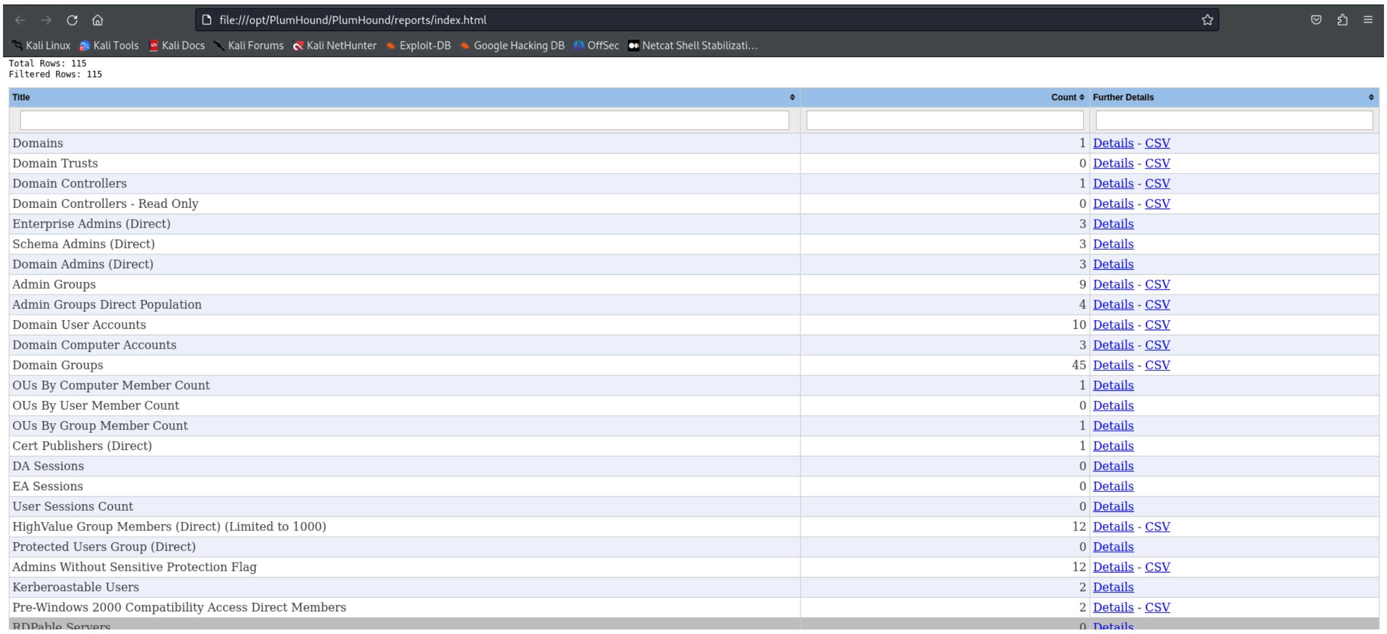


```
┌──(kali㉿kali)-[/opt/PlumHound/PlumHound/reports]
└─$ ls
AdminGroups.csv                              ConstrainedDelegation-Users.csv        GPOOwners-Detail.csv                        OUs_ComputerCount.html                      Users_gt180MoOldPasswords.csv
AdminGroups.html                             ConstrainedDelegation-Users.html       GPOOwners-Detail.html                       OUs_GroupCount.html                         Users_gt180MoOldPasswords.html
AdminGroupsPopulatedCount.csv                ConstrainedDelegation-UsersNonDA.csv   GPOOwners-NonDA.csv                         OUs_UserCount.html                          Users_gt240MoOldPasswords.csv
AdminGroupsPopulatedCount.html               ConstrainedDelegation-UsersNonDA.html  GPOOwners-NonDA.html                        Owned-Computers-Groups-DirectDistinct.html  Users_gt240MoOldPasswords.html
AdminsWithoutSensitiveFlag.html.csv          DA_Sessions.html                       GPOOwners-Summary.csv                       Owned-Computers-Groups.html                 Users_le01DOldPasswords.csv
AdminsWithoutSensitiveFlag.html.html         DCOwners.csv                           GPOOwners-Summary.html                      Owned-Computers.html                        Users_le01DOldPasswords.html
CertificateAuthorties.csv                    DCOwners.html                          GPOs.csv                                    Owned-Groups.html                           Users_lt07DOldPasswords.csv
CertificateAuthorties.html                   DCOwners-Users.csv                     GPOs.html                                   Owned-Objects-AdminTo-Direct.html           Users_lt07DOldPasswords.html
CertificateTemplateEnrollRights.csv          DCOwners-Users.html                    GPOs-NonDA-WithInterestingPermissions.csv   Owned-Objects-GMSARead-Direct.html          Users_lt30DOldPasswords.csv
CertificateTemplateEnrollRights.html         DCSyncDirect.csv                       GPOs-NonDA-WithInterestingPermissions.html  Owned-Objects.html                          Users_lt30DOldPasswords.html
CertificateTemplates.csv                     DCSyncDirect.html                      Groups_CanResetPasswordsCount.html          Owned-Objects-MemberOf-Direct.html          Users_NeverActive_Enabled.csv
CertificateTemplates_ESC1.csv                DCSyncDirectNonDAUsers.csv             Groups-HighValue-members.csv                Owned-Users-Groups-DirectDistinct.html      Users_NeverActive_Enabled.html
CertificateTemplates_ESC1.html               DCSyncDirectNonDAUsers.html            Groups-HighValue-members.html               Owned-Users-Groups.html                     Users_NeverExpirePasswords.csv
CertificateTemplates_ESC2.csv                DCSyncDirectNonDCComputers.csv         HuntComputersWithPassInDescription.html     Owned-Users.html                            Users_NeverExpirePasswords.html
CertificateTemplates_ESC2.html               DCSyncDirectNonDCComputers.html        HuntUsersWithChangeInDescription.html       PreWindows2000.html.csv                     Users_NoKerbReq.csv
CertificateTemplates_ESC3.csv                DomainAdmins.html                      HuntUsersWithPassInDescription.html         PreWindows2000.html.html                    Users_NoKerbReq.html
CertificateTemplates_ESC3.html               DomainComputers.csv                    HuntUsersWithVPNGroup.html                  ProtectedUsers.html                         UsersnonadminAddMemberGroups.csv
CertificateTemplates_ESC6.csv                DomainComputers.html                   index.html                                  RDPableGroupsCount.html                     UsersnonadminAddMemberGroups.html
CertificateTemplates_ESC6.html               DomainControllers.csv                  Kerberoastable_Users.html                   RDPableGroups.html                          UsersNotActive120mo.csv
CertificateTemplates_ESC8.csv                DomainControllers.html                 LapsDeploymentCount.csv                     Relationships-AuthenticatedUsers.html       UsersNotActive120mo.html
CertificateTemplates_ESC8.html               DomainControllers_ReadOnly.csv         LapsDeploymentCount.html                    Relationships-DomainComputers.html          UsersNotActive12mo.csv
CertificateTemplates.html                    DomainControllers_ReadOnly.html        LapsDeploymentCount-OS.csv                  Relationships-DomainUsers.html              UsersNotActive12mo.html
CertPublishers.html                          DomainGroups.csv                       LapsDeploymentCount-OS.html                 Relationships-Everyone.html                 UsersNotActive60mo.csv
Computers_LocalAdminEnumeration.csv          DomainGroups.html                      LAPSNotEnabled.html                         Relationships-Guests.html                   UsersNotActive60mo.html
Computers_LocalAdminEnumeration.html         Domains.csv                            LocalAdmin_Computers_.csv                   Relationships-PreW2KCA.html                 UsersNotActive6mo.csv
Computers_MSSQL.csv                          Domains.html                           LocalAdmin_Computers_.html                  Relationships-Users.html                    UsersNotActive6mo.html
Computers_MSSQL.html                         DomainTrusts.csv                       LocalAdmin_Groups_Count.html                Reports.zip                                 Users_PasswordNotRequired.html
Computers_UnconstrainedDelegation.csv        DomainTrusts.html                      LocalAdmin_Groups.html                      SchemaAdmins.html                           Users_PasswordNotRequiredNeverSet.html
Computers_UnconstrainedDelegation.html       DomainUsers.csv                        LocalAdmins_Computers_count.html            UserSessionsCount.html                      Users_Sessions_Count.html
Computers_UnconstrainedDelegationNonDC.csv   DomainUsers.html                       LocalAdmin_UsersCount.html                  Users_gt006MoOldPasswords.csv               Users_Sessions.csv
Computers_UnconstrainedDelegationNonDC.html  EA_Sessions.html                       LocalAdmin_Users.html                       Users_gt006MoOldPasswords.html              Users_Sessions.html
Computers_WithDescriptions.csv               EnterpriseAdmins.html                  OS_Count.csv                                Users_gt012MoOldPasswords.csv               Users_UnconstrainedDelegation.csv
Computers_WithDescriptions.html              GMSA_CanReadPassword.csv               OS_Count.html                               Users_gt012MoOldPasswords.html              Users_UnconstrainedDelegation.html
ConstrainedDelegation-All.csv                GMSA_CanReadPassword.html              OS_Unsupported_Count.csv                    Users_gt060MoOldPasswords.csv               Users_userpassword.csv
ConstrainedDelegation-All.html               GPOCreatorOwners.html                  OS_Unsupported_Count.html                   Users_gt060MoOldPasswords.html              Users_userpassword.html
ConstrainedDelegation-ComputersNonDC.csv     GPO_OU_Links.csv                       OS_Unsupported.csv                          Users_gt120MoOldPasswords.csv               Workstations_RDP.html
ConstrainedDelegation-ComputersNonDC.html    GPO_OU_Links.html                      OS_Unsupported.html                         Users_gt120MoOldPasswords.html
```

Our best friend here is going to be the "index.html" file, where we can see all the other reports, and access it through a web browser.



```
┌──(kali㉿kali)-[/opt/PlumHound/PlumHound/reports]
└─$ firefox index.html
█
```



```
Total Rows: 115
Filtered Rows: 115
```

Title	Count	Further Details
Domains	1	Details - CSV
Domain Trusts	0	Details - CSV
Domain Controllers	1	Details - CSV
Domain Controllers - Read Only	0	Details - CSV
Enterprise Admins (Direct)	3	Details
Schema Admins (Direct)	3	Details
Domain Admins (Direct)	3	Details
Admin Groups	9	Details - CSV
Admin Groups Direct Population	4	Details - CSV
Domain User Accounts	10	Details - CSV
Domain Computer Accounts	3	Details - CSV
Domain Groups	45	Details - CSV
OUs By Computer Member Count	1	Details
OUs By User Member Count	0	Details
OUs By Group Member Count	1	Details
Cert Publishers (Direct)	1	Details
DA Sessions	0	Details
EA Sessions	0	Details
User Sessions Count	0	Details
HighValue Group Members (Direct) (Limited to 1000)	12	Details - CSV
Protected Users Group (Direct)	0	Details
Admins Without Sensitive Protection Flag	12	Details - CSV
Kerberoastable Users	2	Details
Pre-Windows 2000 Compatibility Access Direct Members	2	Details - CSV
RDPable Servers	0	Details

We can access a lot of data here.

91.4 - PingCastle - Domain Enumeration

For PingCastle, if we are using as a Red team doing an Audit on our own organization, then we do not need the license. But, if we are using it for consulting services or any sort of commercial use, then we need to buy a license in order to use the tool.

We can run it both from the compromised machine, if we have a an local admin account, we can domain join the machine and run it from there. If that is not possible, then there are ways to run it remotely as well.

So, this tool really does a through scan of the Domain, and not only that, it shows us what is the environment weaknesses, like bad password policy, service accounts policy, domain policy, the possible attacks the environment is vulnerable for, and a lot more information on how to hardening the system.