

## 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

Found 1 task(s)

on 1: n.name          n.displayname
-----
KRBGTG@ONEPIECE.LOCAL
SQLSERVICE@ONEPIECE.LOCAL    SQL Service
USOGKEKING@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
AdminGroups.html
AdminGroupsPopulatedCount.csv
AdminsWithoutSensitiveFlag.html.csv
AdminsWithoutSensitiveFlag.html.html
CertificateAuthorities.csv
CertificateAuthorities.html
CertificateTemplateEnrollRights.csv
CertificateTemplateEnrollRights.html
CertificateTemplates.csv
CertificateTemplates_ESC1.html
CertificateTemplates_ESC2.csv
CertificateTemplates_ESC2.html
CertificateTemplates_ESC3.csv
CertificateTemplates_ESC3.html
CertificateTemplates_ESC6.csv
CertificateTemplates_ESC6.html
CertificateTemplates_ESC8.csv
CertificateTemplates_ESC8.html
CertPublishers.html
Computers_LocalAdminEnumeration.csv
Computers_LocalAdminEnumeration.html
Computers_MSSQL.csv
Computers_MSSQL.html
Computers_UnconstrainedDelegation.csv
Computers_UnconstrainedDelegation.html
Computers_UnconstrainedDelegationNonDC.csv
Computers_UnconstrainedDelegationNonDC.html
Computers_WithDescriptions.csv
ConstrainedDelegation-All.html
ConstrainedDelegation-ComputersNonDC.csv
ConstrainedDelegation-ComputersNonDC.html
ConstrainedDelegation-Users.html
ConstrainedDelegation-UsersNonDA.html
DA_Sessions.html
DCOwners.csv
DCOwners-Users.html
DCSyncDirect.csv
DCSyncDirect.html
DCSyncDirectNonDAUsers.csv
DCSyncDirectNonDAUsers.html
DCSyncDirectNonDCComputers.csv
DCSyncDirectNonDCComputers.html
DomainAdmins.html
DomainComputers.csv
DomainComputers.html
DomainControllers.html
DomainControllers_ReadOnly.csv
DomainControllers_ReadOnly.html
DomainGroups.csv
DomainGroups.html
Domains.csv
Domains.html
DomainTrusts.csv
DomainTrusts.html
DomainUsers.csv
DomainUsers.html
EA_Sessions.html
EnterpriseAdmins.html
GMSA_CanReadPassword.csv
GMSA_CanReadPassword.html
GPOCreatorOwners.html
GPO_OU_Links.csv
GPO_OU_Links.html
GPOOwners-Detail.csv
GPOOwners-Detail.html
GPOOwners-NonDA.csv
GPOOwners-NonDA.html
GPOOwners-Summary.csv
GPOOwners-Summary.html
GPOs.csv
GPOs.html
GPOs-NonDA-WithInterestingPermissions.csv
GPOs-NonDA-WithInterestingPermissions.html
Groups_CanResetPasswordsCount.html
Groups-HighValue-members.csv
Groups-HighValue-members.html
HuntComputersWithPassInDescription.html
HuntUsersWithChangeInDescription.html
HuntUsersWithPassInDescription.html
index.html
Kerberoastable_Users.html
LapsDeploymentCount.csv
LapsDeploymentCount.html
LapsDeploymentCount-OS.csv
LapsDeploymentCount-OS.html
LAPSNotEnabled.html
LocalAdmin_Computers_.csv
LocalAdmin_Computers_.html
LocalAdmin_Groups_Count.html
LocalAdmin_Groups_Count.html
LocalAdmins_Groups_Count.html
LocalAdmins_Groups_Count.html
LocalAdmin_Users.html
LocalAdmin_Users.html
OS_Count.html
OS_Count.csv
OS_Unsupported_Count.csv
OS_Unsupported_Count.html
OS_Unsupported.csv
OS_Unsupported.html
OUS_ComputerCount.html
OUS_GroupCount.html
OUS_UserCount.html
Owned-Computers-Groups-DirectDistinct.html
Owned-Computers-Groups.html
Owned-Computers.html
Owned-Groups.html
Owned-Objects-AdminTo-Direct.html
Owned-Objects-GMSARead-Direct.html
Owned-Objects.html
Owned-Objects-MemberOf-Direct.html
Owned-Users-Groups-DirectDistinct.html
Owned-Users-Groups.html
Owned-Users.html
PreWindows2000.html.csv
PreWindows2000.html.html
ProtectedUsers.html
RDPableGroupsCount.html
RDPableGroups.html
Relationships-AuthenticatedUsers.html
Relationships-DomainComputers.html
Relationships-DomainUsers.html
Relationships-Everyone.html
Relationships-PreW2KCA.html
Relationships-Users.html
Reports.zip
SchemaAdmins.html
UserSessionsCount.html
Users_gt006MoOldPasswords.csv
Users_gt006MoOldPasswords.html
Users_gt006MoOldPasswords.csv
Users_gt012MoOldPasswords.html
Users_gt012MoOldPasswords.csv
Users_gt060MoOldPasswords.html
Users_gt060MoOldPasswords.csv
Users_gt120MoOldPasswords.csv
Users_gt120MoOldPasswords.html
Users_gt180MoOldPasswords.csv
Users_gt180MoOldPasswords.html
Users_gt240MoOldPasswords.csv
Users_gt240MoOldPasswords.html
Users_le01D0ldPasswords.csv
Users_le01D0ldPasswords.html
Users_lt07D0ldPasswords.csv
Users_lt07D0ldPasswords.html
Users_lt30D0ldPasswords.csv
Users_lt30D0ldPasswords.html
Users_NeverActive_Enabled.csv
Users_NeverActive_Enabled.html
Users_NeverExpirePasswords.csv
Users_NeverExpirePasswords.html
Users_NotActive120mo.csv
Users_NotActive120mo.html
Users_NotActive12mo.csv
Users_NotActive12mo.html
Users_NotActive60mo.csv
Users_NotActive60mo.html
Users_NotActive60mo.csv
Users_NotActive60mo.html
Users_PasswordNotRequiredNeverSet.html
Users_PasswordNotRequiredNeverSet.html
Users_Sessions_Count.html
Users_Sessions_Count.html
Users_Sessions.html
Users_Sessions.html
Users_UnconstrainedDelegation.csv
Users_UnconstrainedDelegation.html
Users_userpassword.csv
Users_userpassword.html
Workstations_RDP.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
```

file:///opt/PlumHound/PlumHound/reports/index.html

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecNetcat Shell Stabilizati...

Total Rows: 115  
Filtered Rows: 115

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

We can access a lot of data here.