

AD AND AZURE AD ASSESSMENT TOOLS

V0.91

TABLE OF CONTENTS

Assessment VM	4
Create and Prepare a VM	4
Install OS	8
BloodHound (AD + Azure Assessment)	8
Prepare Assessment Client (Windows).....	8
BloodHound – Configuration (Windows).....	10
AD: SharpHound – Run (Windows).....	11
AD Pre-requisites	11
Run SharpHound to collect data.....	12
Run SharpHound to collect Session data.....	12
Azure: AzureHound.....	12
Pre-Requisites	12
AzureHound – Run (Windows)	13
Load Data (Windows)	13
View Graph	14
Create AD Excel Report (Windows)	14
Pre-requisites	14
Create Report	15
Create Tiering Report	15
Pre-requisites	15
Create Report	16
Create Jupyter Notebook Report (AD + Azure)	17
Pre-requisites	17
Open Report	18
Cypher Queries (Azure)	19
PingCastle (AD Assessment).....	20
Pre-requisites	20
Create Report	20
adalanche(AD Assessment).....	20
Pre-requisites.....	20
Run Adalanche	21

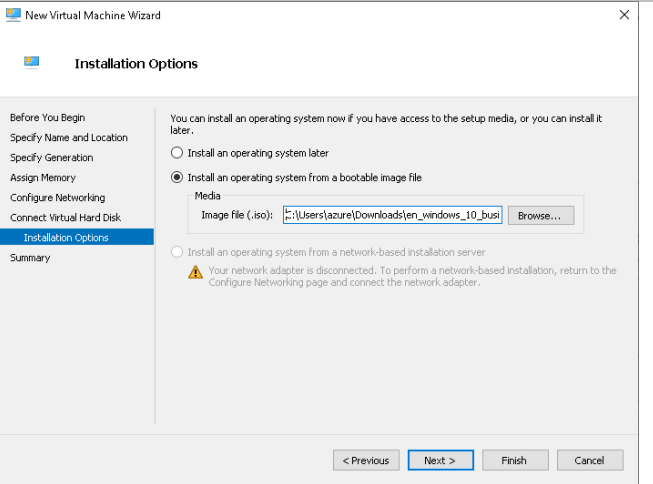
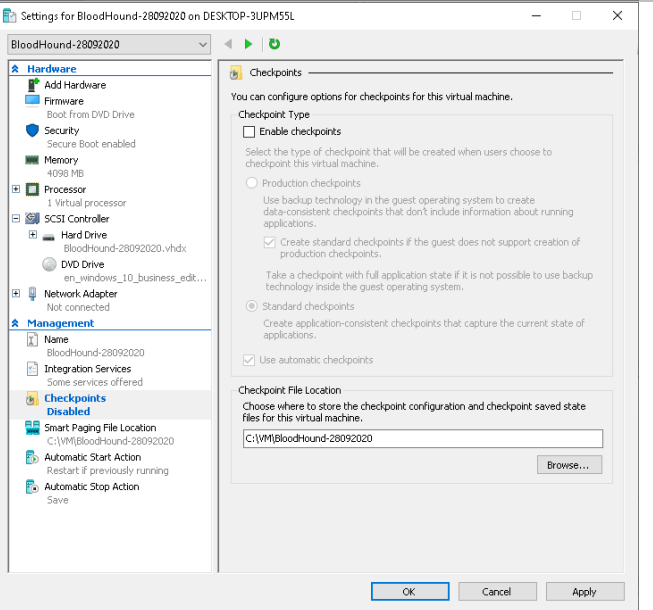
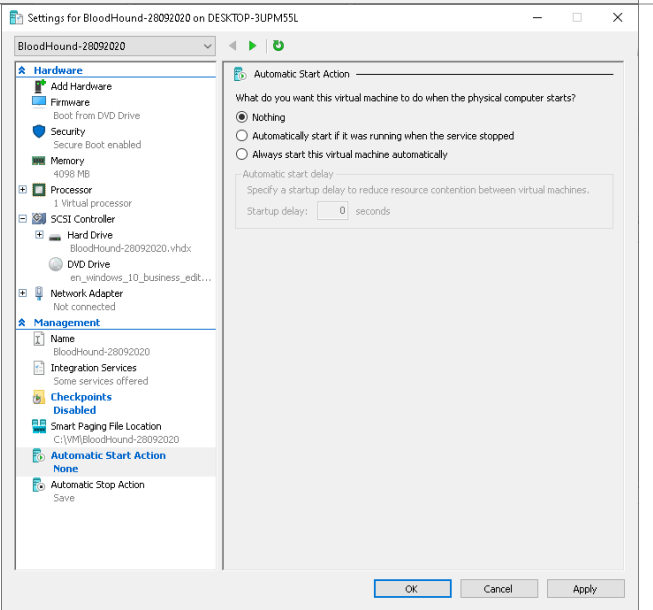
Analyse Data	21
ROADTools (Azure Assessment)	21
AzureAD / Azure Pre-requisites	21
Prepare Assessment Client (Windows).....	21
Run RoadRecon (Windows)	22
View Data with RoadRecon UI	22
Export Data to BloodHound.....	23
Stormspotter (Azure Assessment).....	23
AzureAD / Azure Pre-requisites	23
Prepare Assessment Client (Windows - Docker)	23
Prepare Assessment Client (Windows – Without Docker)	24
Run Stormcollector	25
Load Data (Windows)	26
Review Graph.....	26
Cypher Queries	26
AzureADAssessment	27
Prepare Assessment Client	27
Run AzureADAssessment.....	27
Run AzureADAssessment on Hybrid Components	28
Microsoft Defender for Identity	28
Lateral movement Report.....	28
References.....	28

ASSESSMENT VM

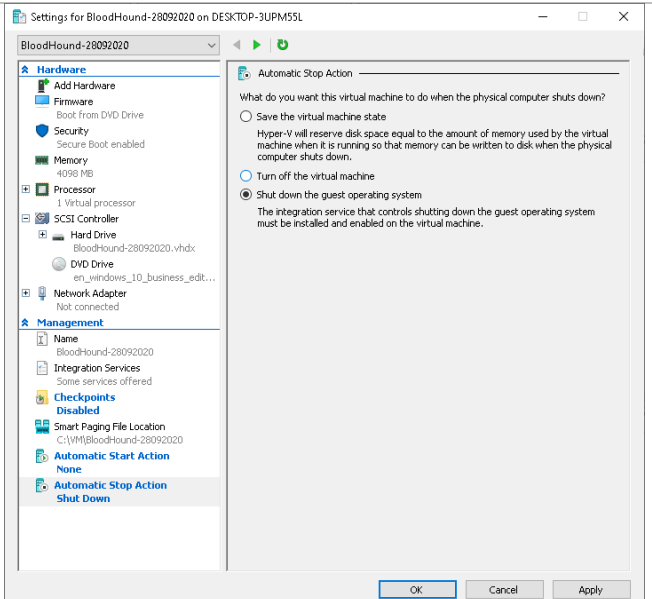
Create and Prepare a VM

	<div><div>New Virtual Machine Wizard</div><div><div>Before You Begin</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.</p><p>To create a virtual machine, do one of the following:</p><ul style="list-style-type: none">Click Finish to create a virtual machine that is configured with default values.Click Next to create a virtual machine with a custom configuration.<p><input type="checkbox"/> Do not show this page again</p><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Specify Name and Location</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>Choose a name and location for this virtual machine.</p><p>The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.</p><p>Name: <input type="text" value="BloodHound-28092020"/></p><p>You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.</p><p><input checked="" type="checkbox"/> Store the virtual machine in a different location</p><p>Location: <input type="text" value="C:\VM\"/> <input data-bbox="1305 1093 1369 1115" type="button" value="Browse..."/></p><p>⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.</p><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Specify Generation</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>Choose the generation of this virtual machine.</p><p><input type="radio"/> Generation 1</p><p>This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.</p><p><input checked="" type="radio"/> Generation 2</p><p>This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.</p><p>⚠ Once a virtual machine has been created, you cannot change its generation.</p><p>More about virtual machine generation support</p><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div></div>

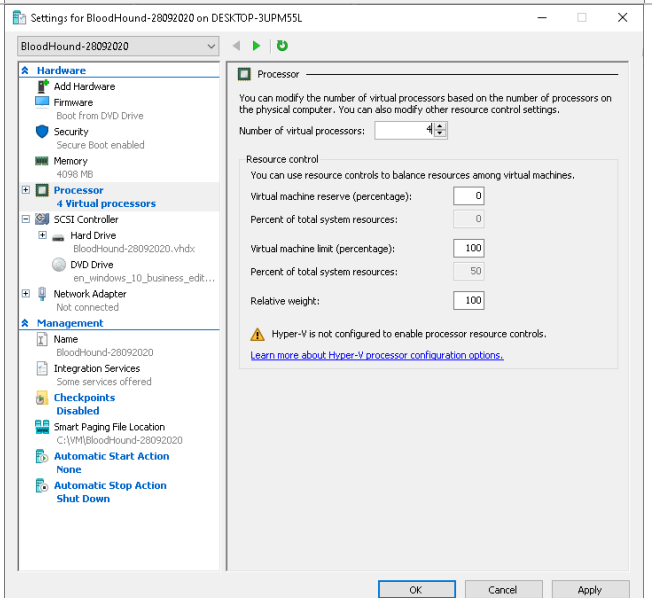
	<div><div>New Virtual Machine Wizard</div><div><div>Assign Memory</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.</div><div>Startup memory: 4096 MB</div><div><input type="checkbox"/> Use Dynamic Memory for this virtual machine.</div><div><div>When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.</div></div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
Chose "Not Connected" for the moment	<div><div>New Virtual Machine Wizard</div><div><div>Configure Networking</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.</div><div>Connection: Not Connected</div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Connect Virtual Hard Disk</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.</div><div><input checked="" type="radio"/> Create a virtual hard disk</div><div>Use this option to create a VHDX dynamically expanding virtual hard disk.</div><div><div>Name: BloodHound-28092020.vhdx</div><div>Location: C:\VM\BloodHound-28092020\Virtual Hard Disks\ Browse...</div><div>Size: 40 GB (Maximum: 64 TB)</div></div><div><input type="radio"/> Use an existing virtual hard disk</div><div>Use this option to attach an existing VHDX virtual hard disk.</div><div><div>Location: C:\VM\ Browse...</div></div><div><input type="radio"/> Attach a virtual hard disk later</div><div>Use this option to skip this step now and attach an existing virtual hard disk later.</div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>

	
Checkpoints: Disable Checkpoints (Optional)	
Automatic Start Action: Turn off Automatically start	

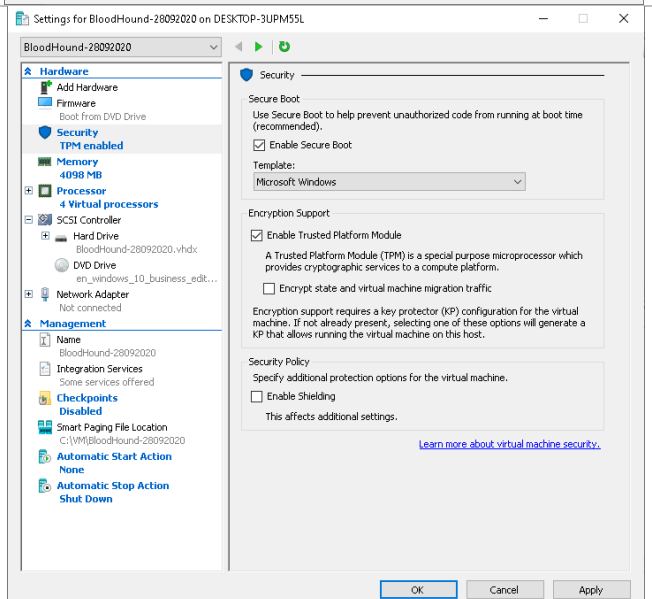
Automatic Stop Action: Shut down the guest operating system



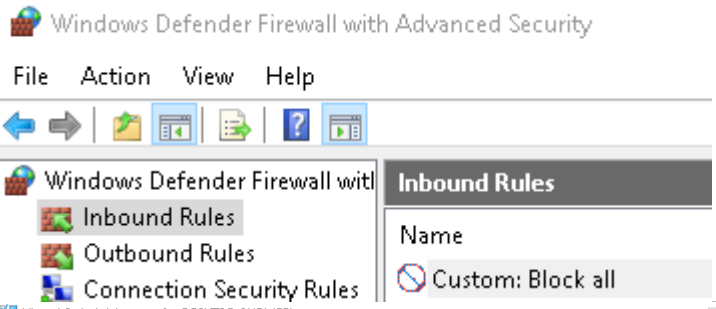
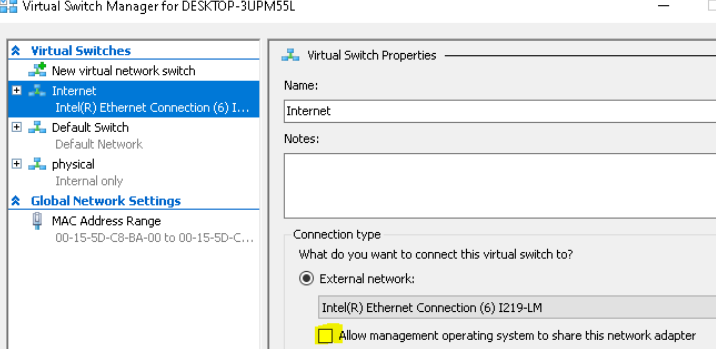
Processor:
Switch to 4 virtual CPU's (depends on the machine)



Security: Enable Secure Boot and Enable TPM



Install OS

Detach any Network Cable (No Internet Connection required at this stage)	
Install Windows OS (Most recent version)	
Create an inbound rule a block all the traffic	
If a VM is used, assign a dedicated VM Switch and don't share it with the host.	
Install Security Updates	Disconnect after update is complete. Exposure to the Network must be as minimal as possible.

BLOODHOUND (AD + AZURE ASSESSMENT)

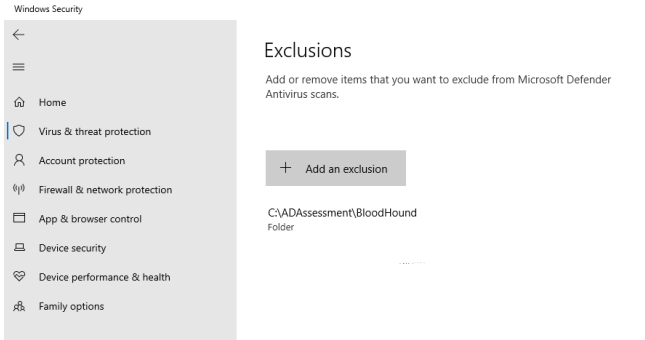
BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a C# data collector (@harmj0y; @_wald0; @CptJesus;, n.d.).

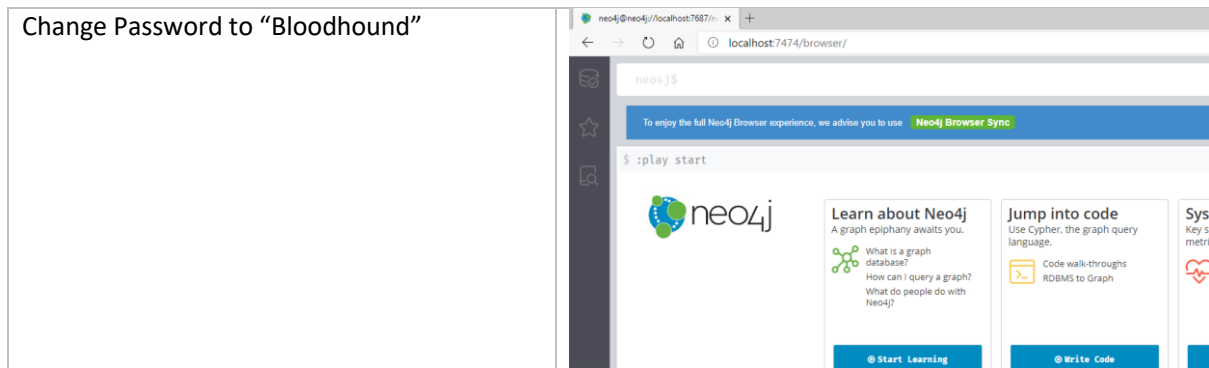
Prepare Assessment Client (Windows)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

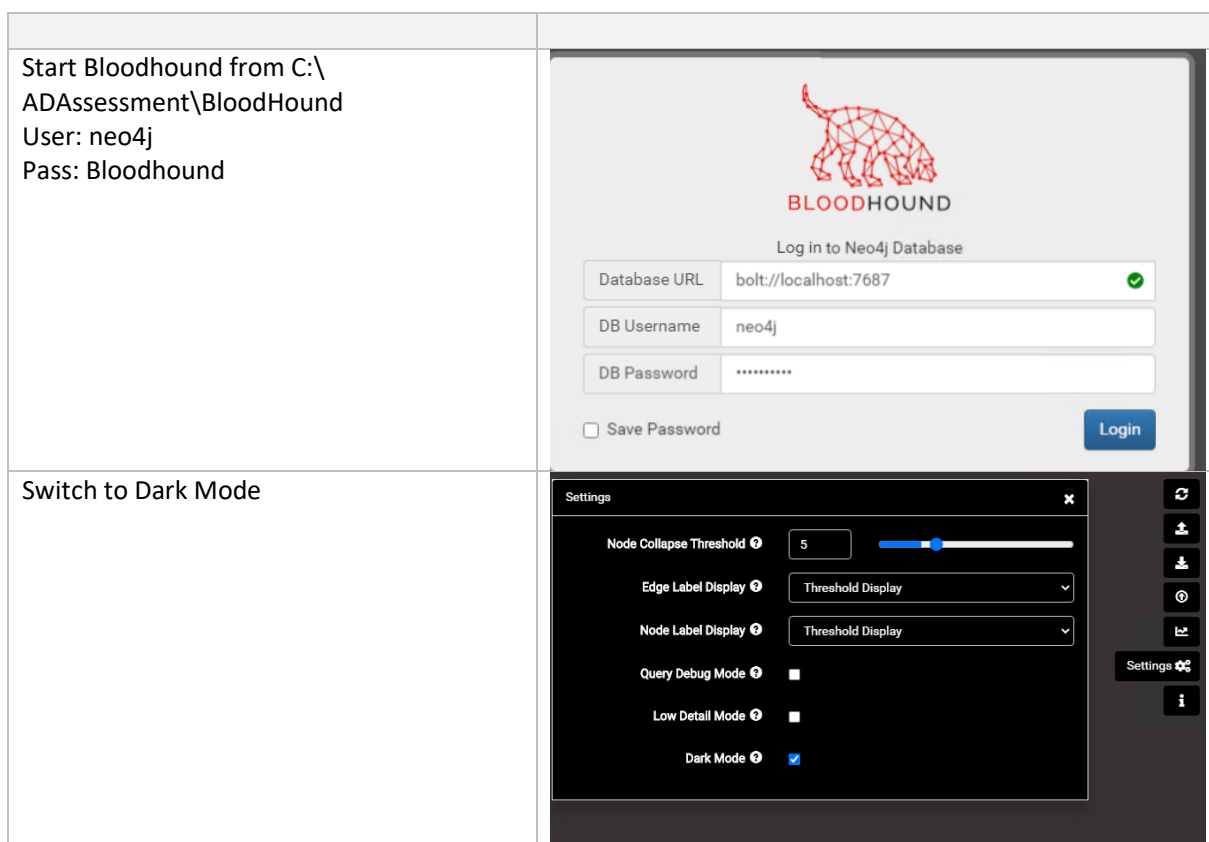
See First Chapter for VM preparation: Assessment VM

Create a C:\ADAssessment directory	
Create a C:\ADAssessment\BloodHound directory	

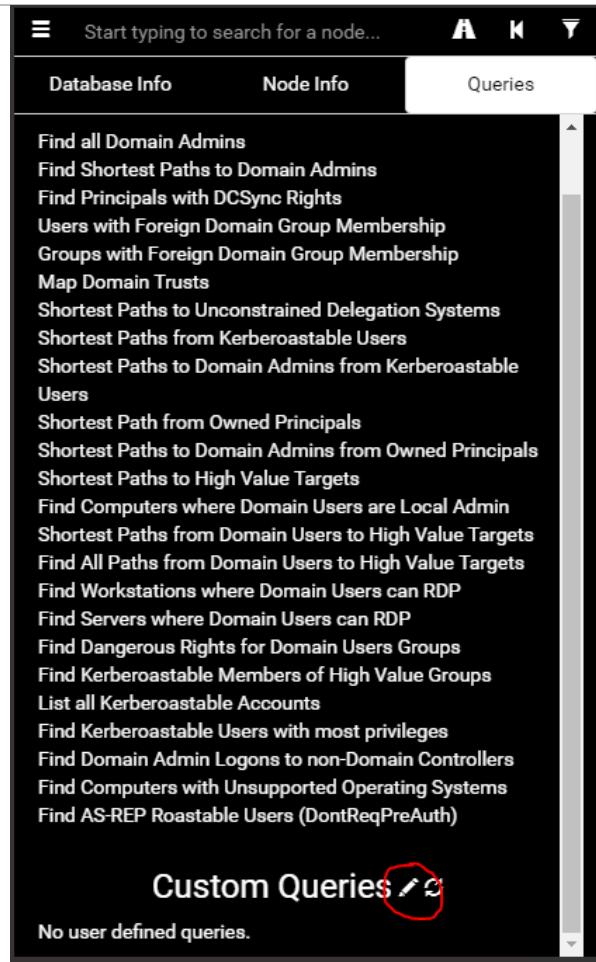
<p>Create a Defender exclusion for the Folder.</p> <p>Virus & Threat protection settings > Exclusions: C:\ADAssessment\BloodHound</p>	
<p>Create folder: C:\ADAssessment\source</p> <p>You can place all the following source files into that folder</p>	
Download Neo4j Community Edition database engine	https://neo4j.com/download-center/#community
Download the latest version of the BloodHound GUI + Source Code	Releases · BloodHoundAD/BloodHound (github.com)
Download CustomFilter	Bloodhound-Custom-Queries/customqueries.json at master · hausec/Bloodhound-Custom-Queries (github.com)
Download Zulu JDK 11	Java Download Java 8, Java 11, Java 13 - Linux, Windows & macOS (azul.com) 
Install Zulu JDK	
Extract Bloodhound binaries to C:\ADAssessment\BloodHound	
Extract neo4j into the C:\ADAssessment\BloodHound directory	
Open cmd	
Change folder to: C:\ADAssessment\BloodHound directory\neo4j...	
Run: Neo4j.bat install-service net start neo4j	<pre>PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> .\Neo4j Neo4j service installed PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> net sta The Neo4j Graph Database - neo4j service is starting. The Neo4j Graph Database - neo4j service was started successfully</pre>
<p>Open the administrative web interface in the browser by going to http://localhost:7474</p> <p>➔ Username: neo4j ➔ Password: neo4j</p>	



BloodHound – Configuration (Windows)



Load CustomFilters



Copy content of downloaded customqueries file to opened editor

Or copy file to:

C:\Users\<user>\AppData\Roaming\bloodhound

AD: SharpHound – Run (Windows)

AD PRE-REQUISITES

Create a temporary assessment user in AD	
User Right: Domain User	
SAM-R: If possible assign temporary rights to the user to read SAM-R from all available Clients in the network.	

RUN SHARPHOUND TO COLLECT DATA

Open CMD
cd C:\ADAssessment\Bloodhound\resources\app\Collectors
SharpHound.exe --domain <domain name> --CollectionMethod All, GPOLocalGroup
If the assessment client is not domain joined:
runas /user:<domain>\adassessment /netonly cmd

RUN SHARPHOUND TO COLLECT SESSION DATA

<https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html#the-session-loop-collection-method>

Open CMD	
cd C:\ADAssessment\Bloodhound\resources\app\Collectors	
SharpHound.exe --domain <domain name> --CollectionMethod Session --Loop --Loopduration 03:00:00	3h Loop to collect only session data
Before loading the data decompress the main zip file (e.g. 20201014101654_BloodHoundLoopResults.zip) to get the result zip files. Import of the main zip file will not work.	

Azure: AzureHound

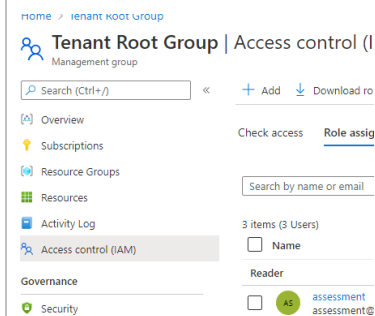
PRE-REQUISITES

<https://bloodhound.readthedocs.io/en/latest/index.html#collect-your-first-dataset>

Open Powershell as Administrator
Run: [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 Set-ExecutionPolicy bypass
Install Azure CLI Install-Module -Name Az -Scope CurrentUser -Repository PSGallery -Force
Install AzureAD Powershell Module Install-Module AzureAD -Scope CurrentUser -Repository PSGallery -Force
Import AzureHound Modules Import-Module C:\ADAssessment\Bloodhound\resources\app\Collectors\AzureHound.ps1
Create a temporary assessment user in Azure AD

Assign the Azure AD Role via PIM or permanent: Global Reader

Assign the Reader Azure Role via PIM to the Tenant Root group

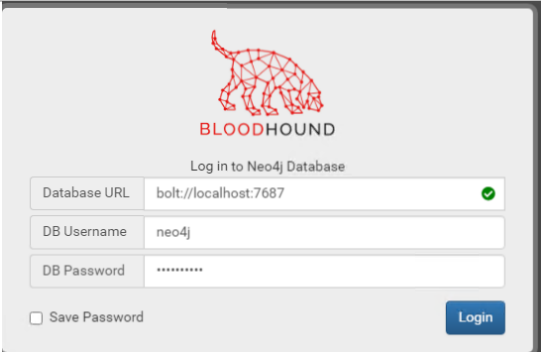



AZUREHOUND – RUN (WINDOWS)

Open Powershell as Administrator	
login to Azure PowerShell	
Connect -AzAccount	
Login zu Azure AD	
Connect -AzureAD	
OPTIONAL: It is also possible to steal the access tokens from a compromised machine if that machine has been used to login to Azure PowerShell before. Copy the existing files: <code>C:\users\[Username]\.azure\AzureRmContextSettings.json</code> <code>C:\users\[Username]\.azure\TokenCache.dat</code> And place them in your own .azure folder. Re-launch PowerShell and the token will now be used.	
Run <code>Import-Module</code> <code>C:\ADAssessment\Bloodhound\resources\app\Collectors\AzureHound.ps1</code> <code>Invoke-AzureHound -TenantId <TenantID> -OutputDirectory</code> <code>C:\ADAssessment\Bloodhound\resources\app\Collectors</code>	

Load Data (Windows)

--	--

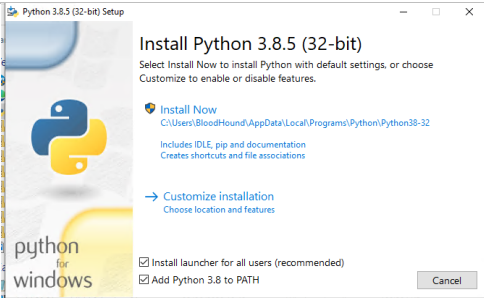
<p>Start Bloodhound from C:\ADAssessment\BloodHound</p> <p>User: neo4j</p> <p>Pass: Bloodhound</p>	
<p>Once Bloodhound has logged in, you will have a huge blank window. We need to load data into this.</p> <p>Click Upload Data</p> <p>Select the zip file collected by Sharphound or AzureHound.</p> <p><datetime>_azurecollection.zip</p> <p><datetime>_BloodHound.zip</p>	
Wait till the data is imported	
Mark all T0 services as High Value Target:	AADConnect, ADFS, etc.
Right click -> High Value	

View Graph

Open:	
C:\ADAssessment\Bloodhound\BloodHound.exe	

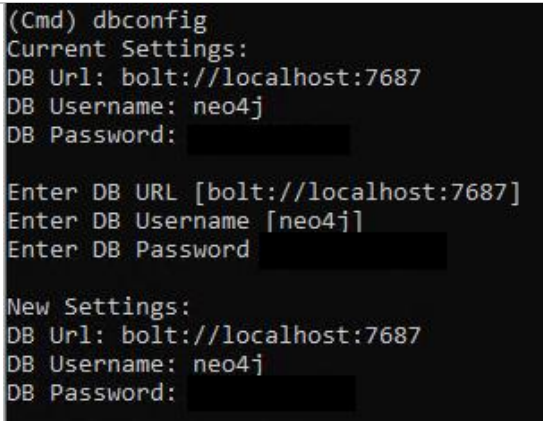
Create AD Excel Report (Windows)

PRE-REQUISITES

Download Python (https://www.python.org/downloads)	
Install Python	
Open CMD and install the following modules:	
<code>pip install neo4j</code>	

<p>pip install openpyxl</p> <p>If behind a proxy add at the end:</p> <p>--proxy https://<proxyserver>:<port></p>	
<p>Download BloodHound Analytics Python file from:</p> <p>Bloodhound/bloodhoundanalytics.py at main · m8r1us/Bloodhound · GitHub</p> <p>Save to:</p> <p>C:\ADAssessment\Report</p>	<p>Script made for neo4j >=V4.0</p>

CREATE REPORT

Run:	
cd C:\ADAssessment\Report	
python bloodhoundanalytics.py <domain>	
Type:	
dbconfig	
Check the connection settings	 <pre>(Cmd) dbconfig Current Settings: DB Url: bolt://localhost:7687 DB Username: neo4j DB Password: Enter DB URL [bolt://localhost:7687] Enter DB Username [neo4j] Enter DB Password New Settings: DB Url: bolt://localhost:7687 DB Username: neo4j DB Password:</pre>
Type:	
Connect	
Type:	
startanalysis	
Excel is required to open the file	

Create Tiering Report

Identify the attack paths in BloodHound breaking your AD tiering (Knudsen, 2021).

<https://improsec.com/tech-blog/improhound-identify-ad-tiering-violations>

PRE-REQUISITES

<p>Download APOC Version which is matching the installed neo4j version:</p> <p>Releases · neo4j-contrib/neo4j-apoc-procedures (github.com)</p>
--

Version Compatibility Matrix:

<https://github.com/neo4j-contrib/neo4j-apoc-procedures#version-compatibility-matrix>

Copy the **apoc-x.x.x.x-all.jar** to C:\ADAssessment\BloodHound\neo4j...\plugins\

Open the neo4j.conf file under:

C:\ADAssessment\BloodHound\neo4j...\conf\

Edit neo4j.conf to allow unrestricted APOC access by adding

dbms.security.procedures.unrestricted=apoc.*

after the following line:

#dbms.security.procedures.unrestricted=my.extensions.example,my.procedures.*

Restart Neo4j

net stop neo4j && net start neo4j

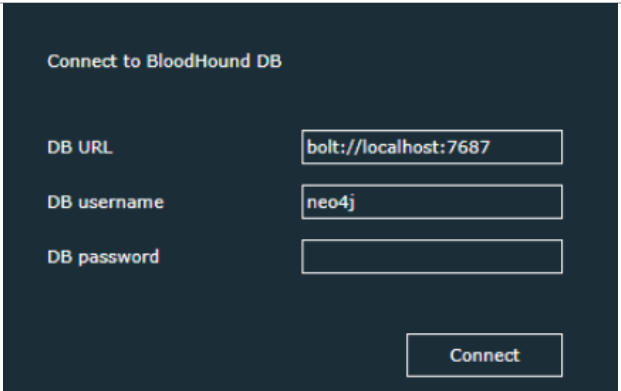
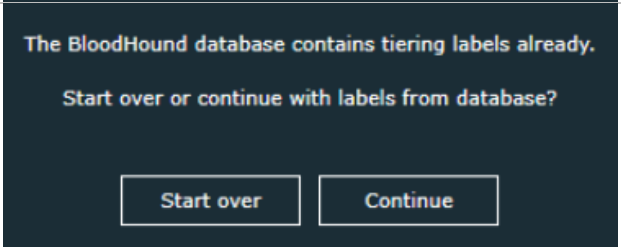
Download the latest release of ImproHound.exe in Windows (x64) to

C:\ADAssessment\ImproHound

[Releases · improsec/ImproHound \(github.com\)](#)

Or review the code and compile C# application.

CREATE REPORT

Run ImproHound.exe	
Connect to the Database Enter the database credentials and establish a connection. It is the same credentials you use in BloodHound GUI.	
Select Start over	

Set the correct tiering labels for your OU structure.

Set children to tier

If you select a domain or an AD container, you can click 'Set children to tier' to set all children (recursively) to the tier level of the given domain/container.

Set members to tier

If you select a group, you can click 'Set children to tier' to set all members (recursively) to the tier level of the given group.

Set tier for GPOs

If you click 'Set tier for GPOs' each GPO will have their tier level set to the tier level of the OU with highest tier (closest to zero) which the GPO is linked to. GPOs not linked to an OU will not have their tier level changed.

Delete tiering

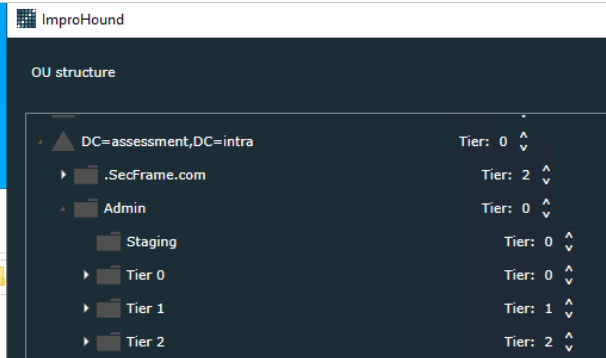
All tier labels and ImproHound created nodes in the BloodHound database will be deleted.

Press **"Get tiering violations"**

Two CSV files are generated as output:

adobjects-[timestamp].csv: All AD objects and which tier they are in.

tiering-violations-[timestamp].csv: The tiering violations.



Create Jupyter Notebook Report (AD + Azure)

Report is based on the blog post from Rodriguez (2019).

Jupyter: [Installation — JupyterLab 3.0.16 documentation](#)

Plots: [plotly/plotly.py: The interactive graphing library for Python \(includes Plotly Express\) \(github.com\)](#)

PRE-REQUISITES

Download Python (if not already done) (https://www.python.org/downloads)	
Install NPM: Node.js (nodejs.org)	

Open cmd as admin and run:

```
pip install jupyterlab
pip install py2neo
pip install altair
pip install pandas
pip install psutil
npm install --save plotlywidget
jupyter labextension install jupyterlab-plotly@4.14.3
```

If behind a proxy add at the end for pi:

```
--proxy http://<proxyserver>:<port>
```

For npm:

```
npm config set http-proxy=http://<proxyserver>:<port>
npm config set https-proxy=http://<proxyserver>:<port>
```

Create folder C:\ADAssessment\Reports

Download bloodhound_report.ipynb and bloodhound_Azure_report.ipynb from:

[m8r1us/Bloodhound: AD Assessment scripts \(github.com\)](https://github.com/m8r1us/Bloodhound-AD-Assessment-scripts)

and save the file to the Reports folder.

OPEN REPORT

Open cmd as admin and run:

```
cd C:\ADAssessment\Reports
jupyter-lab
```

A browser should have opened automatically otherwise go to:

<http://localhost:8888/lab/workspaces>

Double-click or right click to open the bloodhound_report.ipynb or the bloodhound_Azure_report.ipynb file

Change the connection string in step 2 accordingly.

Initialize BloodHound neo4j Database Connection

```
[2]: g = Graph("bolt://localhost:7687", auth=("neo4j", "Bloodhound"))
[2]: Graph
```

Neo4j connection URL
See: <http://localhost:7474/browser/>

DB user Password

Change the Domain to the domain to assess

Domain to assess

```
[3]: domain = "ASSESSMENT.INTRA"
```

Change the Azure Tenant to your Tenant

Press the restart kernel button	<div> <div>▶▶</div> <div>Restart Kernel?</div> <div>Do you want to restart the current kernel? All variables will be lost.</div> <div> <div>Cancel</div> <div>Restart</div> </div> </div>
---------------------------------	---

Cypher Queries (Azure)

Return All Azure Users that are part of the 'Global Administrator' Role	MATCH p =(n)-[r:AZGlobalAdmin*1..]->(m) RETURN p
Return All On-Prem users with edges to Azure	MATCH p=(m:User)-[r:AZResetPassword AZOwns AZUserAccessAdministrator AZContributor AZAddMembers AZGlobalAdmin AZVMContributor AZOwnsAZAvereContributor]->(n) WHERE m.objectid CONTAINS 'S-1-5-21' RETURN p
Find all paths to an Azure VM	MATCH p = (n)-[r]->(g:AZVM) RETURN p
Find all paths to an Azure KeyVault	MATCH p = (n)-[r]->(g:AZKeyVault) RETURN p
Return All Azure Users and their Groups	MATCH p=(m:AZUser)-[r:MemberOf]->(n) WHERE NOT m.objectid CONTAINS 'S-1-5-' RETURN p
Return All Azure AD Groups that are synchronized with On-Premise AD	MATCH (n:Group) WHERE n.objectid CONTAINS 'S-1-5-' AND n.azsyncid IS NOT NULL RETURN n
Find all Privileged Service Principals	MATCH p = (g:AZServicePrincipal)-[r]->(n) RETURN p
Find all Owners of Azure Applications	MATCH p = (n)-[r:AZOwns]->(g:AZApp) RETURN p
Return All Azure Users (Console)	MATCH (n:AZUser) return n.azname
Return All Azure Applications	MATCH (n:AZApp) return n.objectid
Return All Azure Devices	MATCH (n:AZDevice) return n.name
Return All Azure Groups	MATCH (n:AZGroup) return n.name
Return all Azure Key Vaults	MATCH (n:AZKeyVault) return n.name
Return all Azure Resource Groups	MATCH (n:AZResourceGroup) return n.name
Return all Azure Service Principals	MATCH (n:AZServicePrincipal) return n.objectid
Return all Azure Virtual Machines	MATCH (n:AZVM) return n.name
Find All Principals with the 'Contributor' role	MATCH p = (n)-[r:AZContributor]->(g) RETURN p

PINGCASTLE (AD ASSESSMENT)

Ping Castle is a tool designed to assess quickly the Active Directory security level with a methodology based on risk assessment and a maturity framework. It does not aim at a perfect evaluation but rather as an efficiency compromise (PingCastle, n.d.).

PRE-REQUISITES

Download or compile PingCastle from:	
vletoux/pingcastle: PingCastle - Get Active Directory Security at 80% in 20% of the time (github.com)	
or	
Home - PingCastle	
Create a PingCastle folder under: C:\ADAssessment	
Create a user that has only Domain User rights	

CREATE REPORT

Run PingCastle.exe from C:\ADAssessment\PingCastle with the created assessment domain user.	
If the assessment client is not domain joined:	
<code>runas /user:<domain>\adassessment /netonly cmd</code>	
Choose Healthcheck	
Define the domain to check	
Wait for the report creation under C:\ADAssessment\PingCastle	

ADALANCHE(AD ASSESSMENT)

adalanche gives instant results, showing you what permissions users and groups have in an Active Directory. It is useful for visualizing and exploring who can take over accounts, machines or the entire domain, and can be used to find and show misconfigurations (Lars Karlslund, n.d.).

Pre-requisites

Download adalanche:	
lkarlsund/adalanche: Active Directory ACL Visualizer and Explorer - who's really Domain Admin? (github.com)	
Install go 1.17	
Downloads - go.dev	
<code>cd adalanche-master</code>	
Windows: <code>build.cmd</code>	
Linux/OSX: <code>./build.sh</code>	
Create a temp. assessment user in AD	

Run Adalanche

Run: <code>adalanche collect activedirectory</code>	
By default, adalanche uses LDAPS. Use “--ignorecert” to switch to LDAP in a Lab environment.	
Use “--help” to find out more about the default collection options before collecting data from AD.	
If the assessment client is not domain joined: <code>runas /user:<domain>\adassessment /netonly cmd</code> or <code>adalanche collect activedirectory --domain contoso.local --username adasement --password YourPassword</code>	

Analyse Data

Run: <code>adalanche analyze</code>	
-------------------------------------	--

ROADTOOLS (AZURE ASSESSMENT)

ROADtools is a framework to interact with Azure AD. It currently consists of a library (roadlib) and the ROADrecon Azure AD exploration tool (Jan, n.d.).

[dirkjanm/ROADtools: The Azure AD exploration framework. \(github.com\)](https://github.com/dirkjanm/ROADtools)

AzureAD / Azure Pre-requisites

Create a temporary assessment user in Azure AD	
Assign the Azure AD Role via PIM: Global Reader	
Assign the Reader Azure Role via PIM for Azure.	

Prepare Assessment Client (Windows)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

Create a folder: <code>C:\AzureAssessment</code>	
Create a folder: <code>C:\AzureAssessment\roadtools</code>	
Create a folder: <code>C:\AzureAssessment\sources</code>	
You can place all the following source files into that folder	
Download Python (https://www.python.org/downloads)	
Install Python	
Install Microsoft C++ Build Tools	

https://visualstudio.microsoft.com/thank-you-downloading-visual-studio/?sku=BuildTools&rel=16	
Download Roadtools from: Pipelines - Run 20210527.1 artifacts (azure.com) Or: dirkjanm/ROADtools: The Azure AD exploration framework. (github.com)	
Extract ROADtools.zip to: C:\AzureAssessment\roadtools\roadlib C:\AzureAssessment\roadtools\roadrecon	
Open cmd	
Run: Cd C:\AzureAssessment\roadtools pip install pipenv pipenv install roadlib/ pipenv install roadrecon/	

Run RoadRecon (Windows)

Open cmd Run: Cd C:\AzureAssessment\roadtools pipenv shell	
Use the created Azure AD Account Run: Roadrecon auth --device-code	
Run: Roadrecon gather	
Create Conditional Access Rule dump Run: Roadrecon plugin policies	

View Data with RoadRecon UI

Open cmd	
Cd C:\AzureAssessment\roadtools pipenv shell	
Roadrecon-gui	
Open Browser	

Export Data to BloodHound

Use the new Bloodhound Version with integrated Azure AD support (AzureHound).

Download the following repository https://github.com/dirkjanm/Bloodhound-AzureAD	
Extract to AzureAssessment\	
Download and install neo4j Community Edition (Follow installation guide from Bloodhound)	
pip install neo4j-driver	
Open Cmd	
Cd C:\AzureAssessment\roadtools Pipenv shell Roadrecon plugin bloodhound	
Download NodeJS/NPM (https://www.npmjs.com/get-npm)	
Open Cmd	
cd AzureAssessment\BloodHound-AzureAD-master NPM install NPM run dev	
The application could be also compiled to an exe.	
Open the URL:	
Control +R if blank screen for refresh	
Import SharpHound Data	

STORMSPOTTER (AZURE ASSESSMENT)

Stormspotter creates an “attack graph” of the resources in an Azure subscription. It enables red teams and pentesters to visualize the attack surface and pivot opportunities within a tenant, and supercharges your defenders to quickly orient and prioritize incident response work (Microsoft Azure Red Team, n.d.).

<https://github.com/Azure/Stormspotter>

AzureAD / Azure Pre-requisites

Create a temporary assessment user in Azure AD	
Assign the Azure AD Role via PIM: Global Reader	
Assign the Reader Azure Role via PIM for Azure.	

Prepare Assessment Client (Windows - Docker)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

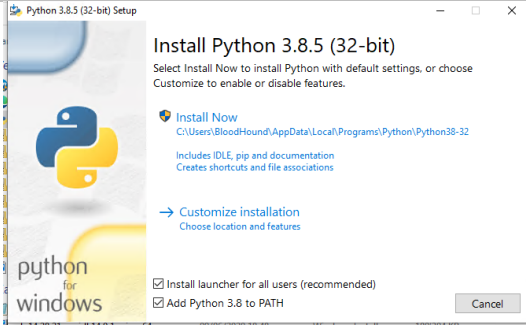
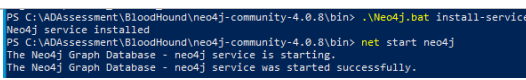
<https://github.com/Azure/Stormspotter#with-docker>

--	--

Download and Install Docker (Follow the instruction to Install WSL2) Docker Desktop for Mac and Windows Docker	
git clone https://github.com/Azure/Stormspotter	
Adjust ports etc. in the docker-compose.yaml if required. (Conflict with installed neo4j version)	
docker-compose up	

Prepare Assessment Client (Windows – Without Docker)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

Create a folder: C:\AzureAssessment	
Create a folder: C:\AzureAssessment\stormspotter	
Create folder: C:\AzureAssessment\source	
You can place all the following source files into that folder	
Download Python (https://www.python.org/downloads)	
Install Python 3.8.0 (https://www.python.org/ftp/python/3.8.0/python-3.8.0-amd64.exe)	
Download NodeJS/NPM (node-v14.17.0-x64) (https://www.npmjs.com/get-npm)	
Install NPM (NodeJS)	
Download Zulu JDK 11 (https://www.azul.com/downloads/zulu-community/?architecture=x86-64-bit&package=jdk)	
Install Zulu JDK	
Download Neo4j (https://neo4j.com/download-center/#community)	
Extract neo4j into the C:\AzureAssessment\Stormspotter directory	
Open cmd	
Change folder to: C:\AzureAssessment\Stormspotter\neo4j-community-4.2.6\bin	
Run: Neo4j.bat install-service net start neo4j	


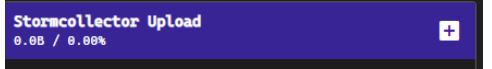
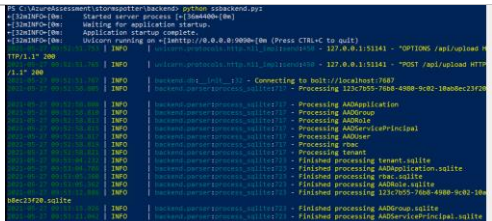
Open the administrative web interface in the browser by going to http://localhost:7474	
Username: neo4j Password: neo4j	
Change Password to "stormspotter"	
Download Stormspotter (Releases · Azure/Stormspotter (github.com))	
Extract C:\AzureAssessment\stormspotter	
Install az cli powershell (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli)	
Install Fronted reuirements Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa npm install -g @quasar/cli	

Run Stormcollector

Open separate CMD and RUN: cd C:\AzureAssessment\Stormspotter\stormcollector Run to show the help menu: python sscollector.pyz -h Common options for all authentication types python sscollector.pyz cli python sscollector.pyz spn -t <tenant> -c <clientID> -s <clientSecret> --cloud: Specify a different Azure Cloud (GERMAN, CHINA, USGOV) --config: Specify a custom configuration for cloud environments --azure: Only enumerate Azure Resource Manager resources --aad: Only enumerate Azure Active Directory --subs: Subscriptions you wish to scan. Multiple subscriptions can be added as a space delimited list. --nosubs: Subscriptions you wish to exclude. Multiple subscriptions can be excluded as a space delimited list. --json: Convert SQLite output to JSON (WARNING: STORMSPOTTER ONLY PARSES SQLITE FORMAT) This option is useful if you want to parse the output for reasons other than Stormspotter. --ssl-cert: Specify an SSL cert for Stormcollector to use for requests. Not a common option --backfill: Perform AAD enumeration only for object IDs associated with RBAC enumeration. Only applicable when --azure is specified.	
Run to collect data by using the created azure assessment account: Az login python sscollector.pyz cli	

--	--

Load Data (Windows)

Start Frontend -> Open CMD	
Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa quasar serve -p 9091 --history	
Start Backend -> open CMD (Required for uploading data)	
Run: cd C:\AzureAssessment\stormspotter\backend python ssbackend.pyz	
Open: http://localhost:9091	
Upload to Stormcollector Upload -> results_<date>.zip	
Files collected are in the folder: C:\AzureAssessment\stormspotter\stormcollector*.zip	
Check upload status in the Backend CMD Window	

Review Graph

Start Frontend -> Open CMD	
Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa quasar serve -p 9091 --history	
Open in Edge http://localhost:9091	

Cypher Queries

Show ServicePrincipal Relationships	MATCH (a)-[r]-(t) Where a.type ="AADServicePrincipal" RETURN *
-------------------------------------	---

Show all Global Administrators	MATCH (a:AADRole)<-[r:MemberOf]-(t) WHERE a.name = 'Global Administrator' RETURN *
Show all AAD Roles	MATCH (a:AADRole) RETURN *
Show full Tenant Relationships aka Christmastree	MATCH (a)-[r]-(t) Return *

AZUREADASSESSMENT

Azure Assessment script which creates two powerbi reports (Microsoft, n.d.)

[GitHub - AzureAD/AzureADAssessment: Tooling for assessing an Azure AD tenant state and configuration](#)

Prepare Assessment Client

Create a folder:	
C:\AzureAssessment	
Create a folder:	
C:\AzureAssessment\AzureADAssessment	
Open Powershell and run: Install-module msal.ps Install-Module AzureADAssessment -Force <i>! If there are msal.ps install errors follow the on-screen recommendations and try again to install msal.ps before installing the AzureADAssessment module.</i> ## If you have already installed the module, run the following instead to ensure you have the latest version. Update-Module AzureADAssessment -Force	
Install PowerBi Download Microsoft Power BI Desktop from Official Microsoft Download Center	

Run AzureADAssessment

Use the created Azure AD Assessment Account cd C:\AzureAssessment\AzureADAssessment Connect-AADAssessment Invoke-AADAssessmentDataCollection "C:\AzureAssessment\AzureADAssessment"	
Create PowerBI Report Complete-AADAssessmentReports AzureADAssessmentData-<TenantName>.onmicrosoft.com.zip -OutputDirectory "C:\AzureAssessment\AzureADAssessment" Open PowerBi Template AzureADAssessment.pbix	
In the popup provide the path to the Results folder:	

C:\AzureAssessment\AzureADAssessment\AzureADAssessmentData-<tenant>.onmicrosoft.com\AAD-<tenant>.onmicrosoft.com	
--	--


Run AzureADAssessment on Hybrid Components

Export Portable Module	
Export-AADAssessmentPortableModule "C:\AzureAssessment\AzureADAssessment"	
Import the module on each server running hybrid components.	
Import-Module "C:\AzureADAssessment\AzureADAssessmentPortable.psm1"	
Export Data into a single output package.	
Invoke-AADAssessmentHybridDataCollection "C:\AzureAssessment\AzureADAssessment"	

MICROSOFT DEFENDER FOR IDENTITY


Lateral movement Report

Goto <https://portal.atp.azure.com/> > Reports and create a "lateral movement paths to sensitive accounts" report:

 Lateral movements paths to sensitive accounts
Sensitive accounts at risk of being compromised through lateral movement techniques


From

06/15/2021



To

06/22/2021



Download

REFERENCES

@harmj0y; @_wald0; @CptJesus; (n.d.). Bloodhound.

Jan, D. (n.d.). ROADtools. Retrieved from <https://github.com/dirkjanm/ROADtools>

Knudsen, J. B. (2021). ImproHound. Retrieved from <https://github.com/improsec/ImproHound>

Microsoft. (n.d.). Microsoft Azure AD Assessment. Retrieved from <https://github.com/AzureAD/AzureADAssessment>

Microsoft Azure Red Team. (n.d.). Stormspotter. Retrieved from <https://github.com/Azure/Stormspotter>

PingCastle. (n.d.). PingCastle. Retrieved from <https://www.pingcastle.com/>

Rodriguez, R. (2019). Jupyter Notebooks for BloodHound Analytics and Alternative Visualizations. Retrieved from <https://medium.com/threat-hunters-forge/jupyter-notebooks-for-bloodhound-analytics-and-alternative-visualizations-9543c2df576a>

Lars Karlslund. (n.d). adalanche. Retrieved from <https://github.com/lkarlslund/adalanche>