

The Plan:

- Enumerate Azure AD using Stormspotter

Auth'd Recon

Let's leverage Stormspotter to enumerate this Active Directory environment by first authenticating to Azure:

```
cd /shared
cnoio_stormspotter-client
```

We should see output similar to the following:

```
root@ip-10-0-1-241:/shared# cnoio_stormspotter-client
Unable to find image 'cnoio/stormspotter-client:latest' locally latest: Pulling from cnoio/stormspotter-client
...
Status: Downloaded newer image for cnoio/stormspotter-client:latest
root@b30c7bd18fe2:/#
```

Next run the "az login" command to log into azure via the cli:

```
az login
```

We should see output similar to the following:

```
root@b30c7bd18fe2:/# az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code E7DQWLAKY to authenticate.
```

Follow the link <https://microsoft.com/devicelogin> to authenticate using your padawan credentials

- Username (### is your student number): padawan###@traintestrepeatstage2sec.onmicrosoft.com
- Password: h0w1N0w2BROWN321COW

We should see output similar to the following once we are fully authenticated via the Azure CLI:

```
root@abbfdeb45ea4:/shared# az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code EAGBDHTEN to authenticate.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "5f1661aa-cb2e-47bb-b1cd-d2bc432974a5",
    "id": "74078d2e-d4de-4ca7-ad70-282472836afa",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Pay-As-You-Go",
    "state": "Enabled",
    "tenantId": "5f1661aa-cb2e-47bb-b1cd-d2bc432974a5",
    "user": {
      "name": "padawan001@traintestrepeatstage2sec.onmicrosoft.com",
      "type": "user"
    }
  }
]
```

Next, we will enumerate Azure AD:

```
cd /shared
python3 /StormSpotter/stormcollector/sscollector.pyz cli --azure
```

```

root@abbfdeb45ea4:/shared# az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code EAGBDHTEN to authenticate.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "5f1661aa-cb2e-47bb-b1cd-d2bc432974a5",
    "id": "74078d2e-d4de-4ca7-ad70-282472836afa",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Pay-As-You-Go",
    "state": "Enabled",
    "tenantId": "5f1661aa-cb2e-47bb-b1cd-d2bc432974a5",
    "user": {
      "name": "padawan001@traintestrepeatstage2sec.onmicrosoft.com",
      "type": "user"
    }
  }
]
root@abbfdeb45ea4:/shared# python3 /StormSpotter/stormcollector/sscollector.pyz cli
2021-07-24 16:19:58.853 | INFO | stormcollector.auth: get_resource_creds_from_cli:73 - Authenticating to login.microsoftonline.com with CLI credentials.
2021-07-24 16:19:58.853 | INFO | stormcollector.aad: query_aad:186 - Checking access for Azure AD: https://graph.windows.net
2021-07-24 16:19:58.854 | INFO | stormcollector.arm: query_arm:128 - Starting enumeration for ARM - https://management.azure.com
2021-07-24 16:19:59.966 | INFO | stormcollector.arm: query_arm:136 - Enumerating subscription and resource groups for tenant 5f1661aa-cb2e-47bb-b1cd-d2bc432974a5
2021-07-24 16:20:00.619 | INFO | stormcollector.arm: query_management_certs:97 - Enumerating management certs for subscription: 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:00.619 | WARNING | stormcollector.arm: query_management_certs:105 - Forbidden: Cannot enumerate management certs for 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:00.619 | INFO | stormcollector.arm: query_rbac:75 - Enumerating rbac permissions for subscription: 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:13.007 | INFO | stormcollector.arm: query_rbac:91 - Finishing rbac permissions for subscription: 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:13.007 | INFO | stormcollector.aad: query_aad:234 - Starting enumeration for Azure AD: https://graph.windows.net
2021-07-24 16:20:13.013 | INFO | stormcollector.aad: query_objects:77 - Starting query for AADUser
2021-07-24 16:20:13.013 | INFO | stormcollector.aad: query_objects:77 - Starting query for AADServicePrincipal
2021-07-24 16:20:13.013 | INFO | stormcollector.aad: query_objects:77 - Starting query for AADApplication
2021-07-24 16:20:13.013 | INFO | stormcollector.aad: query_objects:77 - Starting query for AADRole
2021-07-24 16:20:13.013 | INFO | stormcollector.aad: query_objects:77 - Starting query for AADGroup
2021-07-24 16:20:13.290 | INFO | stormcollector.arm: query_subscription:49 - Querying for resources in subscription - 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:14.676 | INFO | stormcollector.aad: query_objects:109 - Finished query for AADGroup
2021-07-24 16:20:14.888 | INFO | stormcollector.aad: query_objects:109 - Finished query for AADUser
2021-07-24 16:20:15.136 | INFO | stormcollector.aad: query_objects:109 - Finished query for AADRole
2021-07-24 16:20:16.247 | INFO | stormcollector.aad: query_objects:109 - Finished query for AADApplication
2021-07-24 16:20:20.763 | INFO | stormcollector.arm: query_subscription:70 - Finished querying - 74078d2e-d4de-4ca7-ad70-282472836afa
2021-07-24 16:20:37.923 | INFO | stormcollector.aad: query_objects:109 - Finished query for AADServicePrincipal
2021-07-24 16:20:37.923 | INFO | main:main:120 - --- COMPLETE: 39.070257902145386 seconds. ---
2021-07-24 16:20:37.924 | INFO | main:main:122 - Zipping up output...
2021-07-24 16:20:37.941 | INFO | main:main:124 - OUTPUT: /shared/results_20210724-161958.zip
root@abbfdeb45ea4:/shared#

```

Note: Stormspotter collector sometimes hangs and/or is throttled while querying Azure graph. If this happens, wait a minute and try again. If it still fails, use the results file [here SIMS-CC-FILEBASES/results_20210725-201429.zip?canvass=download=1](https://github.com/0x09b/Stormspotter/blob/master/results/20210725-201429.zip?canvass=download=1)

Once we see output similar to the following...

```

root@b30c7bd18fe2:/shared# python3 /StormSpotter/stormcollector/sscollector.pyz cli --azure
2021-07-31 20:00:36.010 | INFO | stormcollector.auth: get_resource_creds_from_cli:73 - Authenticating to login.microsoftonline.com with CLI credentials.
2021-07-31 20:01:07.338 | INFO | main:main:124 - OUTPUT: /shared/results_20210731-200035.zip
root@b30c7bd18fe2:/shared#

```

Next exit out of the docker container via the following command...

exit

We should see output similar to the following...

```

root@b30c7bd18fe2:/shared# exit
exit
root@ip-10-0-1-241:/shared#

```

Now we can analyze the results via the web interface for Stormspotter.

Start the web interface with the following command:

```

cnoio_stormspotter

```

We should see output similar to the following...

```

Starting stormspotter_stormspotter-neo4j_1 ... done
Starting stormspotter_stormspotter-frontend_1 ... done
Starting stormspotter_stormspotter-backend_1 ... done
Attaching to stormspotter_stormspotter-neo4j_1, stormspotter_stormspotter-frontend_1, stormspotter_stormspotter-backend_1
stormspotter-neo4j_1 | Selecting JVM - Version:11.0.12, Name:OpenJDK 64-Bit Server VM, Vendor:Oracle Corporation
stormspotter-frontend_1 | Quasar CLI..... v1.2.1
stormspotter-frontend_1 | Listening at..... http://61c9b7fffadf:9091
stormspotter-frontend_1 | Web server root.... /usr/src/app
stormspotter-frontend_1 | Gzip..... enabled
stormspotter-frontend_1 | Cache (max-age).... 86400
stormspotter-frontend_1 | Micro-cache..... 1s
stormspotter-frontend_1 | History mode..... enabled
stormspotter-frontend_1 | Index file..... index.html
stormspotter-backend_1 | INFO: Started server process [1]
stormspotter-backend_1 | INFO: Waiting for application startup.
stormspotter-backend_1 | INFO: Application startup complete.
stormspotter-backend_1 | INFO: Uvicorn running on http://0.0.0.0:9090 (Press CTRL+C to quit)
stormspotter-neo4j_1 | Changed password for user 'neo4j'.
stormspotter-neo4j_1 | 2021-07-24 16:48:37.308+0000 INFO Starting...
stormspotter-neo4j_1 | 2021-07-24 16:48:38.239+0000 INFO ===== Neo4j 4.3.2 =====
stormspotter-neo4j_1 | 2021-07-24 16:48:38.745+0000 INFO org.neo4j.internal.kernel.api.security.AbstractSecurityLog$SecurityLogLine@69d021c1
stormspotter-neo4j_1 | 2021-07-24 16:48:38.745+0000 INFO org.neo4j.internal.kernel.api.security.AbstractSecurityLog$SecurityLogLine@6d5508a5
stormspotter-neo4j_1 | 2021-07-24 16:48:38.864+0000 INFO Bolt enabled on 0.0.0.0:7687.
stormspotter-neo4j_1 | 2021-07-24 16:48:39.287+0000 INFO Remote interface available at http://localhost:7474/
stormspotter-neo4j_1 | 2021-07-24 16:48:39.289+0000 INFO Started.

```

Open a second SSH session to your Public EC2's Instance.

Determine your Public EC2's Instance's Internet IP Address:

```
curl ipcurl.net/n
```

We should see output similar to the following (e.g. the IP Address of our Public EC2 instance is 3.129.90.235):

```
root@ip-10-0-1-241:~# curl ipcurl.net/n
3.129.90.235
root@ip-10-0-1-241:~#
```

You will need to find the file name of the output file created from StormSpotter...

We can use the following command to find it...

```
ls -alF /shared/results_*.zip
```

We should see output similar to the following...

```
root@ip-10-0-1-241:~# ls -alF /shared/results_*.zip
-rw-r--r-- 1 root root 24107 Jul 31 20:01 /shared/results_20210731-200035.zip
root@ip-10-0-1-241:~#
```

Upload the results file to the Stormspotter API using the following command (replace "results_20210801-202634.zip" with the results file you created earlier with Stormspotter collector)

```
curl -F 'upload=@/shared/results_20210801-202634.zip' http://localhost:9090/api/upload
```

We should see output similar to the following:

```
root@ip-10-0-1-241:~# curl -F 'upload=@/shared/results_20210731-200035.zip' http://localhost:9090/api/upload
```

```
{"status": "Upload Success"}
```

```
root@ip-10-0-1-241:~#
```

And then browse to the web interface (replacing ip.ip.ip with your EC2 instance's public IP address e.g. 3.129.90.235):

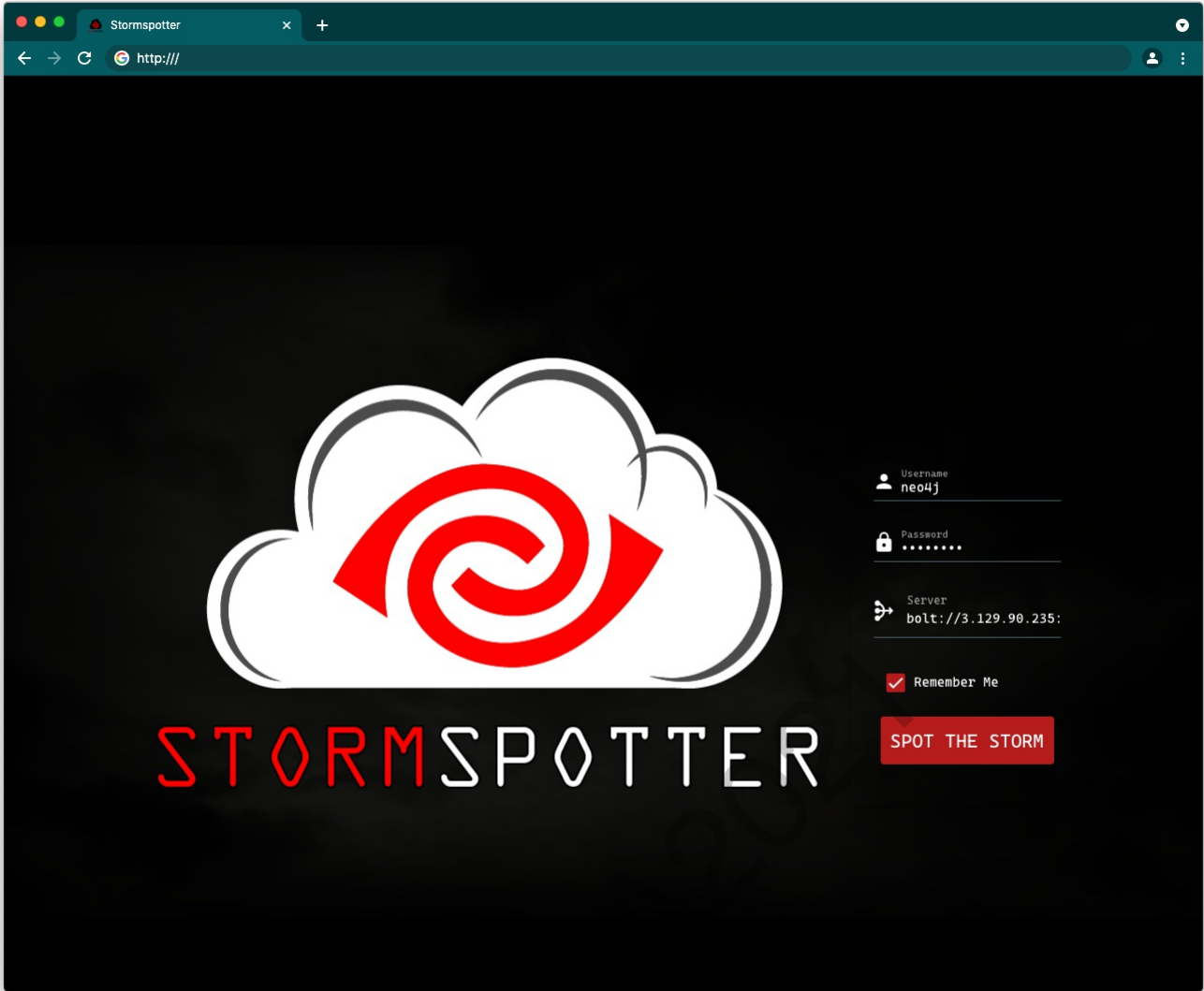
```
http://ip.ip.ip:9091/
```

Login using:

- Username: neo4j
- Password: password
- Server: bolt://ip.ip.ip:7687

NOTE: Make sure to change localhost to your public IP in the server field!

BHUSA2021



DATABASE
INFO
QUERIES

Database Stats

Database	bolt://localhost:7687
User	neo4j

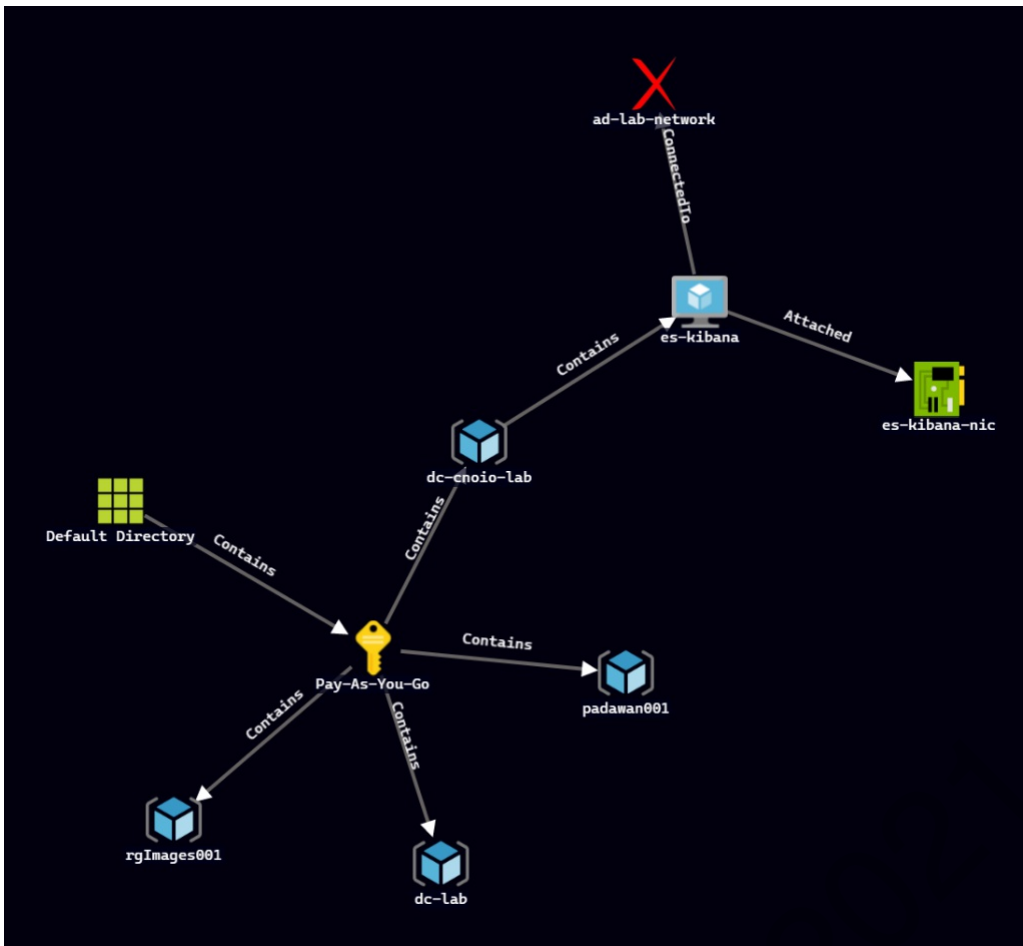
Node Summary

Node Type	Count
AAObject	42
AzureResource	2
Disk	6
IpConfiguration	5
NetworkInterface	5
NetworkSecurityGroup	3
PublicIp	5
ResourceGroup	4
Rule	7
StorageAccount	1
Subscription	1
Tenant	1

Stormcollector Upload 0.00 / 0.00%

From the interface, you can click on nodes (icons) and expand relationships between objects

We should see output similar to the following:



References:

- <https://www.synacktiv.com/en/publications/azure-ad-introduction-for-red-teamers.html>
- <https://github.com/LMGsec/o365creeper>
- <https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/#:-:text=Password%20spraying%20is%20an%20attack,account%20by%20guessing%20the%20password.>
- <https://www.coalfire.com/The-Coalfire-Blog/March-2019/Password-Spraying-What-to-Do-and-How-to-Avoid-It>
- <https://www.youtube.com/watch?v=SG2ibjuzRJM>

BHUSAZ