

기	안	결	재
Dohyeon Kim		Nikolay Akatyev	

협조 :

Interim Report

<13th Digital Forensics 김도현(Dohyeon Kim) / ☎ 2226, '24. 08. 13(Tue)>

☐ 목 표 : detection_evasion

☐ 목 차

1. Set Analysis Environment

- 1-1 AWS CLI
- 1-2 CloudGoat
- 1-3 Terraform

Interim Report

<13th Digital Forensics 김도현(Dohyeon Kim) / ☎ 2226, '24. 08. 13(Tue)>

1. Set Analysis Environment

❏ AWS CLI

- First, I need to install AWS CLI in Ubuntu Virtual Machine(WSL 2).

```
dhDESKTOP-AQ7PH80:/mnt/c/Users/Administrator$ sudo snap install curl
[sudo] password for dh:
curl 8.1.2 from Ubuntu (ubuntu) installed
dhDESKTOP-AQ7PH80:/mnt/c/Users/Administrator$ curl
curl -try 'curl -help' on 'curl --manual' for more information
dhDESKTOP-AQ7PH80:/mnt/c/Users/Administrator$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscli2.zip"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload    Total   Spent    Left   Speed
100 57.9M 100 57.9M    0     0 1157K      0  0:00:51  0:00:51 --:--:-- 2001k
dhDESKTOP-AQ7PH80:/mnt/c/Users/Administrator$ sudo ./aws/install
[sudo] password for dh:
```

❏ CloudGoat

- Install CloudGoat in Ubuntu Virtual Machine(WSL 2).

[illegible]

❑ Terraform

- Install Terraform in Ubuntu Virtual Machine(WSL 2).

```
66 packages can be upgraded. Run 'apt list --upgradable' to see them.
dh@DESKTOP-AQ7PM80: /mnt/c/Users/Administrator$ sudo apt-get install terraform
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  terraform
0 upgraded, 1 newly installed, 0 to remove and 66 not upgraded.
Need to get 28.0 MB of archives.
After this operation, 89.0 MB of additional disk space will be used.
Get:1 https://apt.releases.hashicorp.com jammy/main amd64 terraform amd64 1.9.4-1 [28.0 MB]
Fetched 28.0 MB in 16s (1778 kB/s)
Selecting previously unselected package terraform.
(Reading database ... 25068 files and directories currently installed.)
Preparing to unpack .../terraform_1.9.4-1_amd64.deb ...
Unpacking terraform (1.9.4-1) ...
Setting up terraform (1.9.4-1) ...
dh@DESKTOP-AQ7PM80: /mnt/c/Users/Administrator$
```

- Then, I need to prepare python environment and install CloudGoat dependencies.

```
Downloading sqllite-utf16-3.27-py3-none-any.whl (167 kB)
Collecting jmespath[2.0.8, >=0.7.1]
Downloading jmespath-1.0.1-py3-none-any.whl (20 kB)
Collecting s3transfer[0.8.1, >=0.5.0, <0.10.0]
Downloading s3transfer-0.10.2-py3-none-any.whl (102 kB)
Collecting boto3[boto3-1.34.154, >=1.34.154]
Downloading boto3-1.34.154-py3-none-any.whl (12.5 MB)
Collecting charset-normalizer[4.0.0]
Downloading charset-normalizer-3.2.0-py3-none-any.whl (69 kB)
Collecting certifi[2024.7.4]
Downloading certifi-2024.7.4-py3-none-any.whl (166 kB)
Collecting urllib3[2.0.7, >=2.0.0, <3.0.0]
Downloading urllib3-2.0.7-py3-none-any.whl (122 kB)
Collecting python-dateutil[2.9.0.post0, >=2.9.0, <3.0.0]
Downloading python_dateutil-2.9.0.post0-py3-none-any.whl (249 kB)
Collecting click-default-group[2.2.0]
Downloading click_default_group-1.2.4-py2.py3-none-any.whl (4.1 kB)
Collecting click
Downloading click-8.1.7-py3-none-any.whl (97 kB)
Collecting sqllite-fts4
Downloading sqllite-fts4-1.0.3-py3-none-any.whl (10.8 kB)
Collecting tabulate
Downloading tabulate-0.9.0-py3-none-any.whl (135 kB)
Collecting plugin
Downloading plugin-1.5.0-py3-none-any.whl (20 kB)
Collecting six[1.16.0, >=1.16.0, <2.0.0]
Downloading six-1.16.0-py3-none-any.whl (11 kB)
Installing collected packages: sqllite-fts4, sqllite-utf16, urllib3, tabulate, six, PyYAML, plugin, jmespath, idna, click, charset-normalizer, certifi, arpcomplete, requests, python-dateutil, click-default-group, sqllite-fts4, boto3, s3transfer, s3transfer, boto3
Successfully installed arpcomplete-3.2.0 boto3-1.34.154 boto3core-1.34.154 certifi-2024.7.4 charset-normalizer-3.2.0 click-8.1.7 click-default-group-1.2.4 idna-3.7 jmespath-1.0.1 plugin-1.5.0 python-dateutil-2.9.0.post0 requests-2.31.0 s3transfer-0.10.2 six-1.16.0 sqllite-fts4-1.0.3 sqllite-utf16-3.27 tabulate-0.9.0 urllib3-2.0.7
```