DNAMIC ANALYSIS USER GUIDE

Author	Release Version	Date Created
Joe Garcia	1.0.1	2020-01-27

Table of Contents

1 INSTALLATION

1.1 Windows

1. Download & install the latest version of Python 3 for Windows executable installer.
2. Download the source code zip of the latest DNAmic Analysis release.
3. Unpack the source code zip file and start a command prompt from within the directory.
4. **pip3 install -r requirements.txt**
5. Run the application with valid arguments as outlined in the Usage section below.

1.2 Linux

1.2.1 RHEL/CentOS

1. Install EPEL Release repository:
   sudo yum install epel-release -y
2. Install Python 3.6 from EPEL:
   sudo yum install python36 -y
3. Upgrade pip to latest version:
   sudo python3 -m pip install –upgrade pip
4. Clone GitHub repository for DNAmic Analysis:
   git clone https://github.com/infamousjoeg/DNAmicAnalysis.git
5. Change directory to the newly cloned GitHub repo directory:
   cd DNAmicAnalysis/
6. Install requirements.txt dependencies:
   sudo python3 -m pip install -r requirements.txt
7. Run DNAmicAnalysis with proper arguments as outlined in the Usage section below.

1.2.2 Ubuntu/Debian

1. Install Python 3.6:
   sudo apt install python3.6 -y
2. Install pip for Python 3.6:
   sudo python36 -m ensurepip
3. Upgrade pip to latest version:
   sudo python36 -m pip install --upgrade pip
4. Clone the GitHub repository for DNAmic Analysis:
   git clone https://github.com/infamousjoeg/DNAmicAnalysis.git
5. Change directory to the newly cloned GitHub repo directory:

cd DNAmicAnalysis/

6. Install requirements.txt dependencies:
   python36 -m pip install -r requirements.txt
7. Run DNAmicAnalysis with proper arguments as outlined in the Usage section below.

1.2.3 MacOS

1. Install the latest Python 3:
   brew install python
2. Clone GitHub repository for DNAmic Analysis:
   git clone https://github.com/infamousjoeg/DNAmicAnalysis.git
3. Change directory to the newly clone GitHub repo directory:
   cd DNAmicAnalysis/
4. Install requirements.txt dependencies:
   pip3 install -r requirements.txt
5. Run DNAmicAnalysis with proper arguments as outlined in the Usage section below.

2 USAGE

2.1 Pre-Requisites

- A DNA database file from a CyberArk Discovery & Audit (DNA) scan
  > Must NOT be obfuscated
  > To disable auto-deletion of the DNA db file, open **dna.exe.config** and edit:
  DeleteDB=yes to **DeleteDB=no**

2.2 Create Configuration Template

- A configuration template must be created for DNAmic Analysis to use for analysis.
- You should create one configuration template per customer account.
- You should keep all configuration templates in the **config/** directory located in the root directory where **DNAmicAnalysis.py** exists.

1. Copy **config/template_config.yml** and rename it to something like **customer_config.yml**.

2. Update the values within the YAML config file to match those given to you by the customer for the scan analysis.
   a. **database_file**
      i. The path where the DNA database file is located on the local filesystem.

ii. The file path can be in Linux or Windows format.

b. domain

i. A domain name that is included in the scan.

ii. This is for your protection to ensure analysis is being done on the proper customer scan.

c. account_regex

i. service_account

1. A YAML array containing the naming convention used in the scan for service accounts.
2. **^** is the wildcard character. **svc^** will look for accounts starting with **svc**. **^service** will look for accounts ending with **service**. **^svc^** will look for accounts starting, ending, or containing **service**.

ii. **admin_account**

1. A YAML array containing the naming convention used in the scan for admin accounts (domain, personal privileged, etc).
2. **^** is the wildcard character. **a_^** will look for accounts starting with **a_**. **^admin** will look for accounts ending with **admin**. **^admin^** will look for accounts starting, ending, or containing **admin**.

d. **include_disabled_accts**

i. Yes or no on whether you want to include disabled accounts in the report. (I recommend keeping no.)

e. test_mode

i. For testing only.

f. scan_datetime

i. override

1. Yes or no on whether to override detecting scan datetime from the DNA database filename and use **manual_scan_datetime** below instead.

ii. manual_scan_datetime

1. Use 24h format for the time.
2. Example: **2019-05-21 20:47:43**

2.2.1 Example Configuration Template

2.2.1.1 config/customer_config.yml

```
---
# path to where the DNA database file is located
database_file: /Users/joegarcia/Git/infamousjoeg/DNAmicAnalysis/data/test/DNA_2019-05-21_08-57-43-PM.db
# domain name of one scanned domain that can be detected
domain: cyberarkdemo.com
# privileged account patterns to match
account_regex:
  service_account:
    - svc^
    - ^service
  admin_account:
    - adm^
    - ^admin
# yes or no: whether to include disabled accounts in metrics
include_disabled_accts: no
# yes or no: activate test mode... do not adjust unless you
  # know what you are doing
test_mode: yes
# DNA scan date & time settings
scan_datetime:
  # yes or no: override the timestamped DNA.db filename with the manual_scan_datetime
  override: yes
  # Use 24-hour format for the time e.g. 2019-05-21 20:57:43 for 08:57:43 PM
  manual_scan_datetime: "2019-05-21 20:57:43"
```

2.3 Run DNAmicAnalysis.py

2.3.1 Windows

- python.exe not in **$PATH**:

  > **python.exe DNAmicAnalysis.py customer_config.yml**

- python.exe in **$PATH**:

  > **.\DNAmicAnalysis.py customer_config.yml**

2.3.2 *Nix or MacOS

- **./DNAmicAnalysis.py customer_config.yml**

3 OUTPUT

3.1 Excel Workbook

A Microsoft Excel workbook is created in the **reports/** directory where **DNAmicAnalysis.py** was ran from. It contains all the metric data needed for analysis and includes the relevant underlying data, as well.

3.2 Logs

A log file is generated at every runtime in **logs/** that includes every action taken by DNAmic Analysis. If an error occurs, this is a good place to start troubleshooting.

4 SUPPORT

E-Mail PASProgramsOffice@cyberark.com and be sure to include the log file from **logs/** that was generated during the analysis and any relevant screenshots.