

DNAmic analysis USER GUIDE

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

Table of Contents

[1 Installation 2](#_Toc31022545)

[1.1 Windows 2](#_Toc31022546)

[1.2 Linux 2](#_Toc31022547)

[1.2.1 RHEL/CentOS 2](#_Toc31022548)

[1.2.2 Ubuntu/Debian 2](#_Toc31022549)

[1.2.3 MacOS 3](#_Toc31022550)

[2 Usage 3](#_Toc31022551)

[2.1 Pre-Requisites 3](#_Toc31022552)

[2.2 Create Configuration Template 3](#_Toc31022553)

[2.2.1 Example Configuration Template 4](#_Toc31022554)

[2.3 Run DNAmicAnalysis.py 5](#_Toc31022555)

[2.3.1 Windows 5](#_Toc31022556)

[2.3.2 \*Nix or MacOS 5](#_Toc31022557)

[3 Output 5](#_Toc31022558)

[3.1 Excel Workbook 5](#_Toc31022559)

[3.2 Logs 6](#_Toc31022560)

[4 Support 6](#_Toc31022561)

1. Installation

## Windows

1. Download & install the latest version of [Python 3 for Windows executable installer](https://www.python.org/downloads/).
2. Download the source code zip of the [latest DNAmic Analysis release](https://github.com/infamousjoeg/DNAmicAnalysis/releases).
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](#_Pre-Requisites) section below.

## Linux

### 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**](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](#_Pre-Requisites) section below.

### 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**](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](#_Pre-Requisites) section below.

### 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](#_Pre-Requisites) section below.
6. Usage

## 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**

## 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.
   1. **database\_file**
      1. The path where the DNA database file is located on the local filesystem.
      2. The file path can be in Linux or Windows format.
   2. **domain**
      1. A domain name that is included in the scan.
      2. This is for your protection to ensure analysis is being done on the proper customer scan.
   3. **account\_regex**
      1. **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**.
      2. **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**.
   4. **include\_disabled\_accts**
      1. Yes or no on whether you want to include disabled accounts in the report. (I recommend keeping no.)
   5. **test\_mode**
      1. For testing only.
   6. **scan\_datetime**
      1. **override**
         1. Yes or no on whether to override detecting scan datetime from the DNA database filename and use **manual\_scan\_datetime** below instead.
      2. **manual\_scan\_datetime**
         1. Use 24h format for the time.
         2. Example: **2019-05-21 20:47:43**

### Example Configuration Template

#### 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"**

## Run DNAmicAnalysis.py

### Windows

* python.exe not in **$PATH**:
* **python.exe DNAmicAnalysis.py customer\_config.yml**
* python.exe in **$PATH**:
* **.\DNAmicAnalysis.py customer\_config.yml**

### \*Nix or MacOS

* **./DNAmicAnalysis.py customer\_config.yml**

1. Output

## 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.

## 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.

1. Support

E-Mail [PASProgramsOffice@cyberark.com](mailto:PASProgramsOffice@cyberark.com?subject=[ISSUE]%20DNAmic%20Analysis%20Issue%20Discovered) and be sure to include the log file from [**logs/**](#_Logs) that was generated during the analysis and any relevant screenshots.