MALWARE REVERSE ENGINEERING AND CYBER ATTRIBUTION :

- **Updates the package list and upgrades all installed packages on your system :**

```
sudo apt update
sudo apt upgrade
```

- **Installs necessary dependencies including Python, development libraries, database systems (MongoDB, PostgreSQL), and VirtualBox for running virtual machines.**

```
sudo apt-get install python python-pip python-dev libffi-dev libssl-dev -y

sudo apt-get install python-virtualenv python-setuptools -y

sudo apt-get install libjpeg-dev zlib1g-dev swig -y

sudo apt-get install mongodb -y

sudo apt-get install postgresql libpq-dev -y

sudo apt install virtualbox -y

sudo apt-get install tcpdump apparmor-utils -y
```

- **Creates a new user named cuckoo without a password, which will run the Cuckoo processes.**

```
sudo adduser --disabled-password --gecos "" cuckoo
```

- **Configures the tcpdump tool (used for network packet capturing) to run with the necessary privileges. The cuckoo user is added to the pcap group to manage packet capturing.**

```
sudo groupadd pcap
sudo usermod -a -G pcap cuckoo
sudo chgrp pcap /usr/sbin/tcpdump
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

- **Verifies the capabilities set for tcpdump and disables AppArmor restrictions on it, allowing it to capture packets without interference.**

```
getcap /usr/sbin/tcpdump
sudo aa-disable /usr/sbin/tcpdump
```

- **Installs swig and m2crypto, which are necessary for building Python bindings for Cuckoo.**

```
sudo apt-get install swig
sudo pip install m2crypto
```

- **Adds the cuckoo user to the vboxusers group, allowing it to manage VirtualBox VMs.**

```
sudo usermod -a -G vboxusers cuckoo
```

- **Switches to the cuckoo user to set up the virtual environment**

```
sudo su cuckoo
```

- **Setting Up Virtual Environment:**

```
sudo apt-get update && sudo apt-get -y install virtualenv
sudo apt-get -y install virtualenvwrapper
```

- **Installs Python 3's pip, sets up auto-completion for pip, and installs virtualenvwrapper locally for the user.**

```
sudo apt-get -y install python3-pip
pip3 completion --bash >> ~/.bashrc
pip3 install --user virtualenvwrapper
```

- **Create Cuckoo Virtual Environment:**

Creates a virtual environment for Cuckoo using Python 2.7 and installs Cuckoo within it.

```
source ~/.bashrc
mkvirtualenv -p python2.7 cuckoo-test
pip install -U pip setuptools
pip install -U cuckoo
```

- **Setting Up the Windows Virtual Machine** :

Downloads a Windows 7 ISO, creates a mount point, and mounts the ISO for installation.

```
sudo wget https://cuckoo.sh/win7ultimate.iso
sudo mkdir /mnt/win7
sudo chown cuckoo:cuckoo /mnt/win7/
sudo mount -o ro,loop win7ultimate.iso /mnt/win7
```

- **Installs additional dependencies for building and running the virtual machine environment.**

```
sudo apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage
sudo apt-get -y install zlib1g-dev libjpeg-dev
sudo apt-get -y install python-pip python-virtualenv python-setuptools swig
```

- **Installs vmcloak, a tool for automating the setup of virtual machines for Cuckoo.**

```
pip install -U vmcloak
```

- **Creating and Configuring the Virtual Machine:**

Configures a Windows 7 virtual machine, installs dependencies like Internet Explorer 11, and takes a snapshot for later use in analysis.

```
vmcloak-vboxnet0
vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048
vmcloak clone win7x64base win7x64cuckoo
vmcloak list deps
vmcloak install win7x64cuckoo ie11
vmcloak snapshot --count 1 win7x64cuckoo 192.168.56.101
vmcloak list vms
```

- **Interacting with Cuckoo Sandbox:**

```
cuckoo init
cuckoo community
```

- **Running Cuckoo Sandbox :**

```
cuckoo rooter --sudo --group opensecure
cuckoo web --host 127.0.0.1 --port 8080
```

It Starts the Cuckoo Sandbox services, including the rooter (network routing) and the web interface on localhost for accessing the Cuckoo dashboard.