**Introduction to Cuckoo Sandbox**

1. **Introduction**

Cuckoo is an open-source automated malware analysis system.

It’s used to automatically run and analyze files and collect comprehensive analysis results that outline what the malware does while running inside an isolated operating system.

It can retrieve the following types of results:

* Traces of calls performed by all processes spawned by the malware.
* Files being created, deleted and downloaded by the malware during its execution.
* Memory dumps of the malware processes.
* Network traffic trace in PCAP format.
* Screenshots taken during the execution of the malware.
* Full memory dumps of the machines.

This is a guide on how to set up Cuckoo Sandbox and run the first malware analysis test.

1. **Hardware requirements**

CPU: 2 cores minimum

RAM: 4 GB minimum

Storage: 100 GB minimum

1. **Prerequisites materials**
2. VMWare Workstation 17: <https://softwareupdate.vmware.com/cds/vmw-desktop/ws/>
3. Linux 18.04 (later versions will not work with this guide): <https://releases.ubuntu.com/18.04/>
4. **Installation overview**
5. Setup Ubuntu virtual machine

In this section, an Ubuntu virtual machine will be deployed with specific configurations and custom modifications. These configurations are crucial because the Ubuntu VM will host and manage a nested virtual machine, which will run Cuckoo Sandbox. Cuckoo Sandbox will handle the execution of Portable Executable (PE) files in this nested VM, ensuring that potentially malicious files are contained within a secure, isolated environment.

The nested virtualization setup is essential for maintaining security while performing malware analysis, allowing the system to run and analyze executable files without risking the integrity of the host machine.

1. Install and upgrade required dependencies for Cuckoo Sandbox

Before setting up Cuckoo Sandbox, it is essential to install and upgrade all the required dependencies to ensure smooth operation. The dependencies include various software libraries, tools, and Python packages that Cuckoo Sandbox relies on for functionality, including network monitoring, malware analysis, and process isolation. These dependencies can be divided into system-level packages, Python packages, and virtualization tools.

1. Setup virtual environment for Cuckoo Sandbox

A virtual environment provides a dedicated space where all Python libraries, tools, and configurations required by Cuckoo Sandbox can be installed independently. This helps prevent conflicts between different software versions, ensuring that Cuckoo runs in a controlled and consistent environment.

1. Create a Windows virtual machine inside Ubuntu virtual machine

In this guide, Windows 7 will be installed within VirtualBox. This section will prepare the system to mount and access the Windows 7 ISO and install essential packages and libraries required for the configuration of Cuckoo Sandbox.

This Windows version is often used as the guest operating system in Cuckoo Sandbox environments because it is a common target for many types of malware, especially older or legacy malware. Many malware samples are specifically designed to exploit vulnerabilities in older versions of Windows, including Windows 7, which was widely used before its end-of-life. Even though Windows 7 is no longer officially supported by Microsoft, it remains a valuable platform for malware analysis because it allows analysts to study how malware interacts with an unpatched, older system.

1. Cuckoo initialization and configuration

In this section, the Cuckoo Sandbox system is initialized and configured to ensure proper operation and integration with the virtual environment. After installing all necessary dependencies and setting up the virtual environment, Cuckoo must be initialized to create the basic configuration files and directory structure needed for it to function.

1. Cuckoo Sandbox first analysis

The first analysis in Cuckoo Sandbox typically involves testing the setup with a known benign malware test file, such as the **EICAR test file**. The EICAR file is a harmless, standardized file that is often used to verify the detection and behavior of antivirus systems and malware analysis environments. This test ensures that Cuckoo Sandbox has been properly configured and is capable of executing and analyzing files inside the virtual machine.

1. **Installation details**

**1. Setup Ubuntu virtual machine**

Install **VMWare Workstation 17** then restart if required and start it. The user interface will be like the following image:

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động

On the menu bar, choose **File à New Virtual Machine (Ctrl + N)**

A screenshot of a computer

Description automatically generated

Then, choose **Custom** configuration mode. For the Hardware compatibility, choose **ESXi 7.0**

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

Assume that the prerequisite materials are all downloaded, on this next step, choose the **.iso disc image file**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

Next, enter VM credentials; in this guide, **cuckoo** will be used as the username

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

Then, specify the desired path as the **location** of the virtual machine and Allocate the **processors numbers** and **memory**. In this guide, for the best performance, recommended settings of 4 processors – 4096MB RAM or 2 processors – 2048MB RAM.

A screenshot of a computer

Description automatically generated

Afterwards, specify options for Network, I/O and Virtual Disk type. In this guide, the VM will be using these configs:

* **NAT (network address translation)**: allows the virtual machine to access the external network by sharing the host's IP address without needing additional configuration.
* **LSI Logic (SCSI controller):** provides good compatibility with different operating systems.
* **SCSI (virtual disk type):** supports more devices than IDE (up to 15 devices per controller), making it more scalable for virtual machines that need multiple disk drives or higher disk performance.

Set the option to **Use network address translation (NAT)**, and follow with **LSI Logic** and **SCSI**

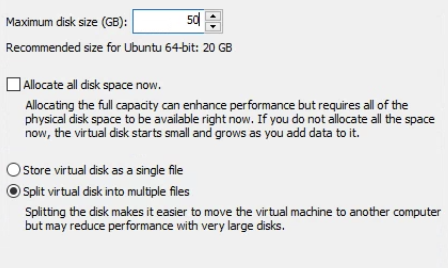
A screenshot of a computer

Description automatically generated Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự độngA screenshot of a computer

Description automatically generated

Create a new virtual disk to store the OS and data inside it. It is recommended to set the disk volume to be 50GB (this virtual machine will hold another virtual machine)



Then, leave other configurations as default by keep clicking on Next button until the **overview** system pops up

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

The next steps makes sure that the deployed virtual machine will be able to handle **nested virtual machine** (As cuckoo will be using another virtual machine to execute PE files)

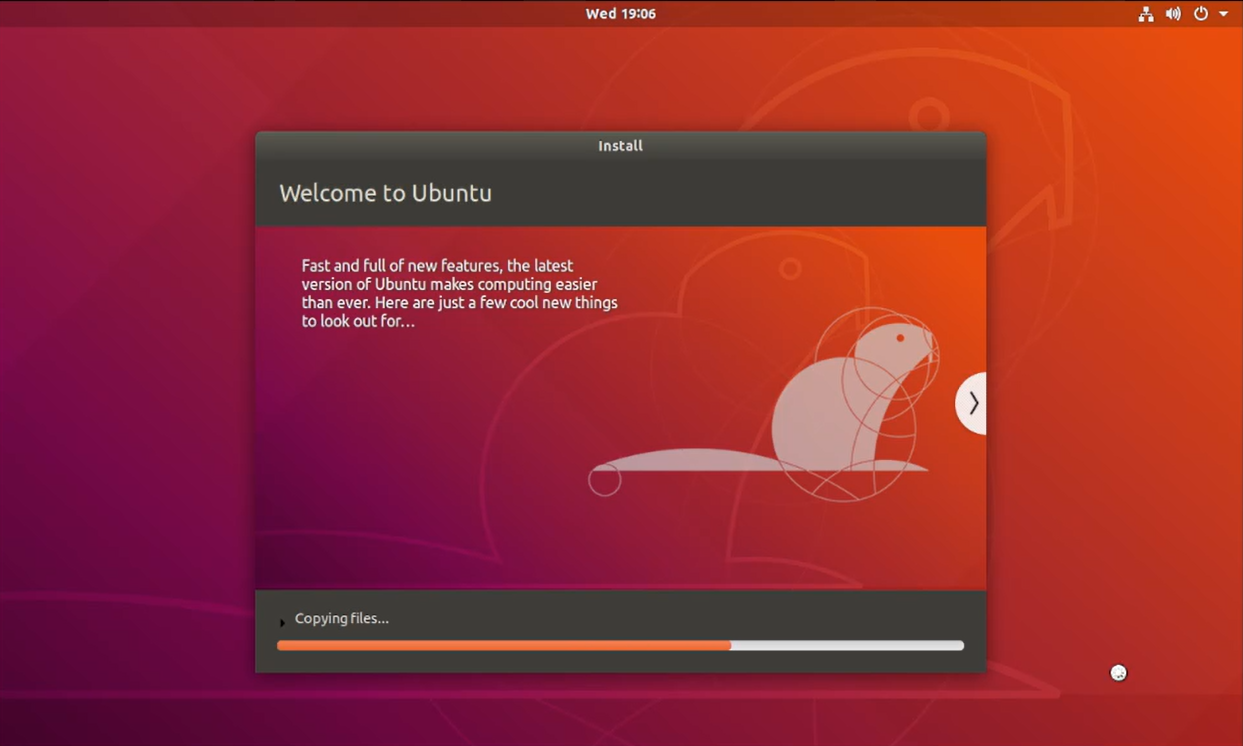
After successfully creating the VM, a new machine icon will pop up on the left side bar, right-click à **Settings**

A screenshot of a computer

Description automatically generated

In the menu bar, choose **Processors**, enable the option **Virtualize Intel VT-x/EPT or AMD-V/RVI**. Then click OK to enable **nested virtualization.**

Now, it is possible to start the configured virtual machine, proceed to **start** it and wait for a while for the OS to be fully functional.



**2**. **Install and upgrade required dependencies for Cuckoo Sandbox**

Update the package list on the Ubuntu system to ensure that all the latest versions of software packages and libraries are available.

1. sudo apt update

2.

3. sudo apt upgrade

Install **System-Level Dependencies:** Cuckoo Sandbox requires several system-level dependencies for its operation. These include tools for process analysis, networking, and system libraries. The following command installs these essential packages:

5. sudo apt-get install python python-pip python-dev libffi-dev libssl-dev -y

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

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

8. sudo apt-get install mongodb -y

9. sudo apt-get install postgresql libpq-dev -y

10. sudo apt install virtualbox -y

11. sudo apt-get install tcpdump apparmor-utils -y

Cuckoo Sandbox requires the ability to capture and analyze network traffic. The following commands enable non-root users to use **tcpdump**, which is crucial for network monitoring:

12. sudo groupadd pcap

13. sudo usermod -a -G pcap cuckoo

14. sudo chgrp pcap /usr/sbin/tcpdump

15. sudo setcap cap\_net\_raw,cap\_net\_admin=eip /usr/sbin/tcpdump

16. ------check capabilities-------

17. getcap /usr/sbin/tcpdump

18. sudo aa-disable /usr/sbin/tcpdump

Then, add the current user to the virtualbox user group (enables the current user to run virtualbox)

19. sudo apt-get install swig

20. sudo pip install m2crypto==0.38.0

21. -------add the user named "cuckoo" to the group "vboxusers"--------

22. sudo usermod -a -G vboxusers cuckoo

**3. Setup virtual environment for Cuckoo Sandbox**

Initialize a bash script to create a new virtual environment for running Cuckoo Sandbox

23. cd /opt/

24. sudo nano cuckoo-setup-virtualenv.sh

Paste this script into the file **nano command line interface**:

#!/usr/bin/env bash

# NOTES: Run this script as: sudo -u <USERNAME> cuckoo-setup-virtualenv.sh

# install virtualenv

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

# install virtualenvwrapper

sudo apt-get -y install virtualenvwrapper

echo "source /usr/share/virtualenvwrapper/virtualenvwrapper.sh" >> ~/.bashrc

# install pip for python3

sudo apt-get -y install python3-pip

# turn on bash auto-complete for pip

pip3 completion --bash >> ~/.bashrc

# avoid installing with root

pip3 install --user virtualenvwrapper

echo "export VIRTUALENVWRAPPER\_PYTHON=/usr/bin/python3" >> ~/.bashrc

echo "source ~/.local/bin/virtualenvwrapper.sh" >> ~/.bashrc

export WORKON\_HOME=~/.virtualenvs

echo "export WORKON\_HOME=~/.virtualenvs" >> ~/.bashrc

echo "export PIP\_VIRTUALENV\_BASE=~/.virtualenvs" >> ~/.bashrc

To be able to execute the script, its permission must be modified, then execute it to initialize the virtual environment to bashrc.

25. sudo chmod +x cuckoo-setup-virtualenv.sh

26. sudo -u cuckoo ./cuckoo-setup-virtualenv.sh

27. source ~/.bashrc

Create a virtual environment name for Cuckoo Sandbox and install Cuckoo Sandbox with python pip. **cuckoo-test** will be used as the name for virtual environment

28. mkvirtualenv -p python2.7 cuckoo-test

29. pip install -U pip setuptools

30. pip install -U cuckoo

After executing the above commands, a denotion of **(cuckoo-test)** will be prepended into the terminal, indicating that it is currently executing commands in virtual environment



**4. Create a Windows virtual machine inside Ubuntu virtual machine**

A Windows 7 virtual machine will be installed as the execution environment for Cuckoo Sandbox. A direct download link has already been stated in the following commands, it can be changed if there is any error in executing this command

31. sudo wget https://ss2.softlay.com/files/en\_windows\_7\_ultimate\_x64\_dvd.iso

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

After having downloaded the windows file, create a directory **/mnt/win7** to serve as a mount point for the Windows 7 ISO. This directory will be used to access the contents of the ISO as if it were a physical disk.

32. sudo mkdir /mnt/win7

Changes the ownership of the **/mnt/win7** directory to the user **cuckoo** and the group **cuckoo**. This ensures that the **cuckoo** user has the appropriate permissions to **manage** and **access** the **directory** where the ISO will be mounted.

33. sudo chown cuckoo:cuckoo /mnt/win7/

Mount the Windows 7 ISO file (**en\_windows\_7\_ultimate\_x64\_dvd.iso**) to the **/mnt/win7** directory in **read-only** mode (-o ro). The loop option allows the ISO to be mounted as if it were a physical disk, providing access to the contents of the ISO image from the mounted directory. The mounted ISO can then be used to install Windows 7 in a virtual machine.

34. sudo mount -o ro,loop en\_windows\_7\_ultimate\_x64\_dvd.iso /mnt/win7

Install or upgrade some dependencies to setup **vmcloak** (tool specifically designed for automating the creation and configuration of Windows virtual machines for use in malware analysis environments, particularly with Cuckoo Sandbox)

35. sudo apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage

36. sudo apt-get -y install zlib1g-dev libjpeg-dev

37. sudo apt-get -y install python-pip python-virtualenv python-setuptools swig

38. pip install -U vmcloak

Create a **VirtualBox host-only network** named vboxnet0 to set up networking between the host machine (where VirtualBox is running) and the guest virtual machines created by VMCloak

39. vmcloak-vboxnet0

Specify the number of cpus and ramsize of the Windows VM. This is recommended to be **half of Ubuntu** virtual machine hardware specifications (in this guide, 2 cpus and 2048MB RAM since the Ubuntu VM is 4 cpus and 4096MB RAM), then initialize the setup process of Windows VM. A message will appear to show the state.

40. vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thông tin

Mô tả được tạo tự động

From there, open another terminal, and execute the command **virtualbox** to start VirtualBox. Then click **Show** to observe the setup part of Windows 7. This process should take ~5-10 minutes.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

Ảnh có chứa văn bản, máy tính, phần mềm, ảnh chụp màn hình

Mô tả được tạo tự động

Wait until the terminal shows **Added image u’win7x64base’ to the repository.**

This message indicates the successful installation of Windows 7 machine.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

The following command will list the **bundles** that **can be installed** on this machine. There are many bundles, and the more bundles, the more activities the malware will perform.

41. vmcloak list deps

In this guide, **winrar** bundle is installed for testing purpose only.

42. vmcloak install win7x64cuckoo winrar

Take a **snapshot** of the machine in order not need to re-do the time-consuming setup part.

43. vmcloak snapshot --count 1 win7x64cuckoo 192.168.56.101

The next command will list out all available VMs that have been installed

44. vmcloak list vms

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, thông tin

Mô tả được tạo tự động

**2 IP addresses** indicate successful installation in this guide.

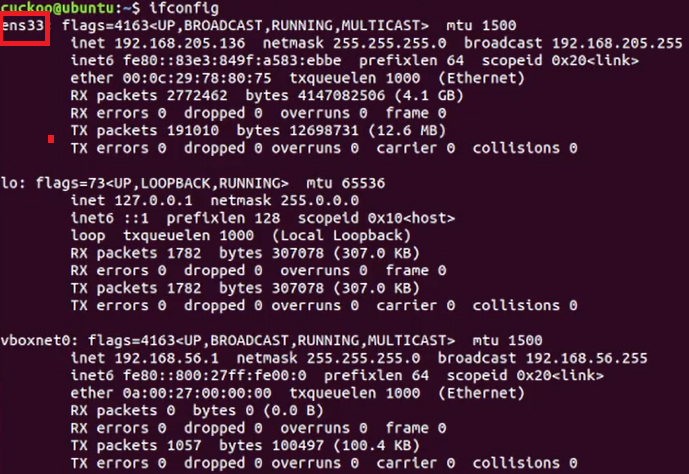
**5. Cuckoo initialization and configuration**

Install net-tools package to execute **ifconfig** command

45. sudo apt install net-tools

46. ifconfig

By executing **ifconfig**, network interface that is being used will be searched. Its pattern starts with **ens**, in this case, **ens33.**

****

Setup IP forwarding to forward packets from forwarding for VirtualBox's host-only network (vboxnet0) to another network interface.

47. sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1

48. sudo sysctl -w net.ipv4.conf.\*interface name\*.forwarding=1

If a **restart** is taken, this **sysctl configuration** will be **lost** (reset). Therefore, this can be **automatically done at startup time** by doing the followings:

49. sudo nano /etc/sysctl.conf

And **append** the following parts to the configuration file

50. sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1

51. sudo sysctl -w net.ipv4.conf.\*interface name\*.forwarding=1

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Configure **iptables** for the virtual machine. This guide will be using **192.168.56.0/24** subnet (VirtualBox host-only network).

This rule allows VMs in the 192.168.56.0/24 network to access the internet or another network via the host machine’s outgoing network interface. It hides the source IP addresses of the VMs and makes them appear as if they are coming from the host's IP.

52. sudo iptables -t nat -A POSTROUTING -o \*interface name\* -s 192.168.56.0/24 -j MASQUERADE

This blocks all forwarded traffic. Only traffic explicitly allowed by subsequent rules will be forwarded. This is a security measure to ensure that only trusted or required traffic is forwarded.

53. sudo iptables -P FORWARD DROP

These rules allows traffic that is part of existing connections to be forwarded, ensuring that once a connection is, the traffic is permitted to continue without being blocked and allows traffic originating from the 192.168.56.0/24 subnet to be forwarded to other networks, such as the internet or the host network.

54. sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

55. sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT

Then, execute the following command to check current **iptables** rules

56. sudo iptables -vnL

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

If the output of the terminal is like so, then above part is perfectly handled.

Open a new terminal and attach the virtual environment **cuckoo-test**, then download rules from community github to Ubuntu local virtual machine

57. workon cuckoo-test

58. cuckoo init

59. cuckoo community

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Start cuckoo rooter in a new router, inside **cuckoo-test** virtual environment using **cuckoo rooter --sudo --group cuckoo**

Remember, the **cuckoo** at the end indicates the machine’s username.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Get back to the previous terminal, execute **cd /home/cuckoo/.cuckoo/conf**

From there, we will modify some configuration files.

Start a bash loop that reads the output from the vmcloak list vms command and automatically **adds each virtual machine listed to Cuckoo Sandbox**

1. while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(vmcloak list vms

Modify Cuckoo’s Virtual Box configuration by deleting redundant virtual machine settings (since we will only use one virtual machine instance for Cuckoo Sandbox)

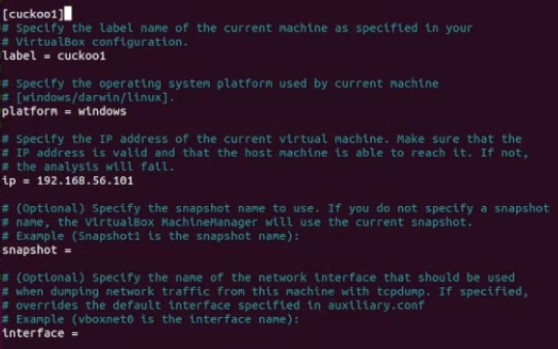
1. nano virtualbox.conf

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, Đồ họa

Mô tả được tạo tự động

Proceed to delete the cuckoo1 in machines variable

The result will be **machines = 192.168.56.1011**



Delete the whole block of **cuckoo1** machine until there is only the **192.168.56.1011** left, then proceed to save the file.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Execute **nano routing.conf** to modify routing configuration file. Only need to change the **internet** variable to the machine’s internet interface, in this case **ens33.**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Lastly, execute **nano reporting.conf** and set mongodb **enabled = yes** to enable logging with mongodb.

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, thiết kế

Mô tả được tạo tự động

After having configured all required files, start cuckoo by executing **cuckoo** command.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Open a new terminal with cuckoo-test virtual environment (**workon cuckoo-test)**, start cuckoo web version:

1. cuckoo web --host 127.0.0.1 --port 8080

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Cuckoo Sandbox web version can now be acccessed, simply go to Firefox, enter **127.0.0.1:8080** as the link. Here is how the dashboard looks like

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Trang web

Mô tả được tạo tự động

**6. Cuckoo Sandbox first analysis**

For testing, **Eicar Malware test file** is being used. Simply go to <https://www.eicar.org/download-anti-malware-testfile/> and download the file.

In this guide, the .**zip** file at the download page is used to analyzed

A screenshot of a computer

Description automatically generated

Drag the file into the box, wait for a while and settings as the following image. Then click **Analyze**

A screen shot of a computer

Description automatically generated

Ảnh có chứa phần mềm, văn bản, Biểu tượng máy tính, Trang web

Mô tả được tạo tự động

When getting to the dashboard, it shows that the file is being scanned, denoted by **running**

Ảnh có chứa văn bản, biên lai, ảnh chụp màn hình, hàng

Mô tả được tạo tự động

Wait until it is marked as **completed**. Then go to **Recent**, click the most recent date to get the analysis report

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

The **Summary** is being displayed, and different analysis in the toolbar on left side bar.

There is also an option to export the analysis for deeper understanding.

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết kế

Mô tả được tạo tự động