

Cybersecurity

Cuckoo Lab



Cuckoo Lab

- Materials needed
 - Kali Virtual Machine
- Software Tools
 - Cuckoo (Online file analyzer)



Objectives Covered

- Security+ Objectives (SY0-601)
 - Objective 4.1 – Given a scenario, use the appropriate tool to assess organizational security
 - Network reconnaissance and discovery
 - Cuckoo



What is Cuckoo?

- Sandboxed environment that a person can put a file into
 - Find out how it will act in the isolated environment
 - Does the file contain malware?
 - Test before putting on an actual system or network
 - Keeps the network or system safe from potential malware



The Cuckoo Lab

- Setup the VM environment
- Locate Files
- Test the Files
- View the Results



Setup Environment

- Log into your range
- Open the Kali Linux Environment
 - You should be on your Kali Linux Desktop
 - Open a new Terminal

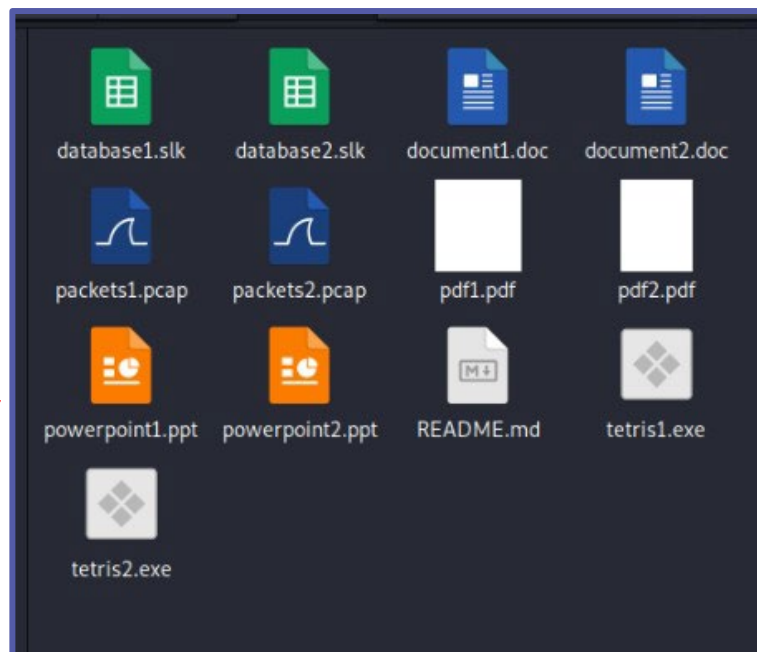


Test the Files

- Open the Home folder
 - Navigate to CourseFiles → Cybersecurity → cuckoo-lab
 - You should see 13 files in the folder with 6 pairs
- Each pair contains a normal file and a malware file
- Pick a pair to test

Please Note: If doing this with multiple groups, assign different pairs to different groups

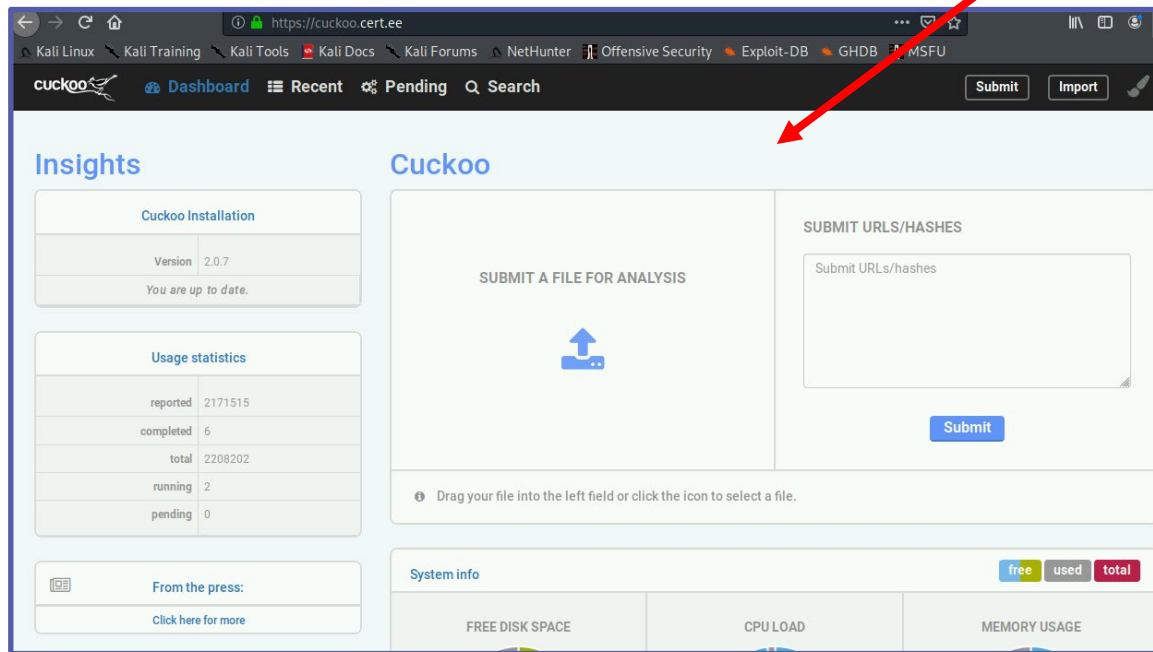
**6 pairs of files
in the Cuckoo
folder**



Test the Files

- Open the Web Browser
- Go to the following website:
<https://cuckoo.cert.ee>

Cuckoo's
online file
analyzer



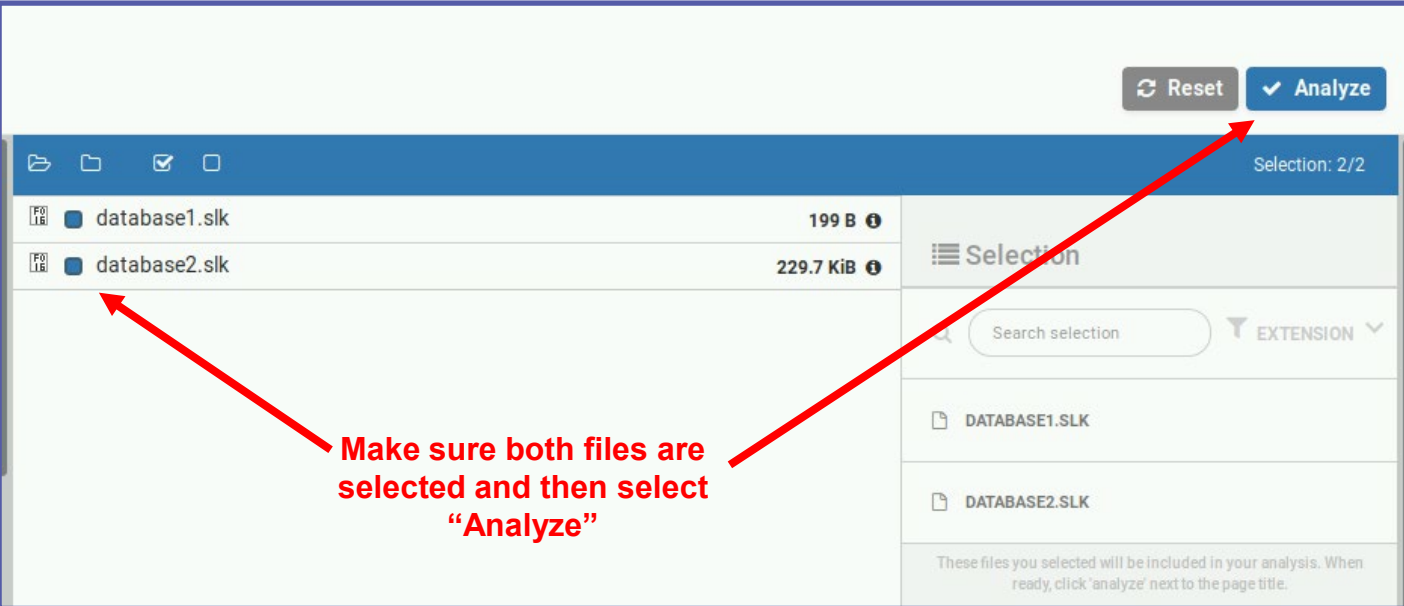
The screenshot shows the Cuckoo online file analyzer web interface. The browser address bar displays <https://cuckoo.cert.ee>. The page features a navigation bar with 'Dashboard', 'Recent', 'Pending', and 'Search' options, along with 'Submit' and 'Import' buttons. The main content area is divided into several sections:

- Insights:** A table showing Cuckoo Installation (Version 2.0.7, 'You are up to date.') and Usage statistics (reported: 2171515, completed: 6, total: 2208202, running: 2, pending: 0).
- Cuckoo:** A central area with a 'SUBMIT A FILE FOR ANALYSIS' button and a file upload icon. Below it, a note says 'Drag your file into the left field or click the icon to select a file.'
- SUBMIT URLS/HASHES:** A text input field for 'Submit URLs/Hashes' and a 'Submit' button.
- System info:** A section with a progress indicator (free, used, total) and three sub-sections: 'FREE DISK SPACE', 'CPU LOAD', and 'MEMORY USAGE'.



Test the Files

- Drag and drop a pair of files into the “SUBMIT A FILE FOR ANALYSIS” box
- Once they are uploaded, select “Analyze”



The screenshot shows a file upload interface. At the top right, there are two buttons: "Reset" and "Analyze". The "Analyze" button is highlighted with a red arrow. Below the buttons is a table of selected files. The table has two rows: "database1.slk" (199 B) and "database2.slk" (229.7 KiB). Both files have a blue selection checkbox that is checked. A red arrow points to the "Analyze" button, and another red arrow points to the checked checkboxes. A red text box in the center of the screenshot reads: "Make sure both files are selected and then select 'Analyze'".

File Name	Size
database1.slk	199 B
database2.slk	229.7 KiB

Selection: 2/2

Selection

Search selection EXTENSION

DATABASE1.SLK

DATABASE2.SLK

These files you selected will be included in your analysis. When ready, click 'analyze' next to the page title.



Test the Files

- The files should start processing

The files are running in the Cuckoo environment and being analyzed

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
2210824	📅 17/05/2021 ⌚ 17:15	database1.slk	xls	● running
2210825	📅 17/05/2021 ⌚ 17:15	database2.slk	xls	● running
Done				

“running” - files are being executed in the Cuckoo environment

“completed” - files are done being ran in the environment and are being analyzed

“reported” - the files are done being analyzed and a report has been made

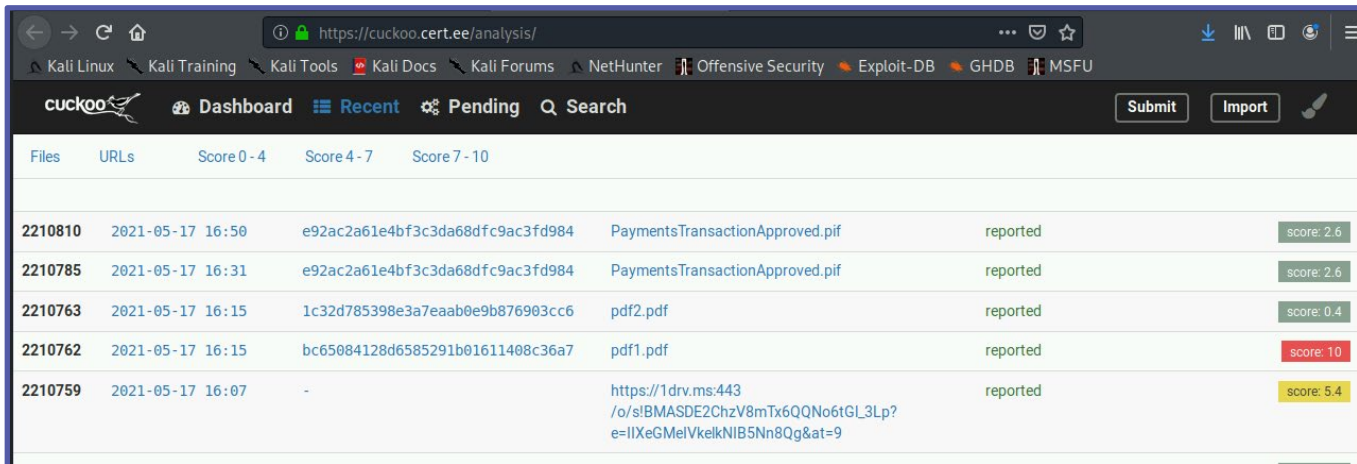
✓ reported
● completed
● completed
✓ reported

Please Note: This process could take up to 10 or more minutes to complete



View the Results

- While the test is running, open the following webpage in another tab
 - <https://cuckoo.cert.ee/analysis>
 - Leave the tab with the test running open



The screenshot shows a web browser window with the URL <https://cuckoo.cert.ee/analysis/>. The page displays a table of analysis results with columns for Files, URLs, and scores. The table contains five rows of data, each representing a different file or URL that has been analyzed. The scores range from 0.4 to 10.0, with a score of 10.0 indicating a high level of detection.

Files	URLs	Score 0 - 4	Score 4 - 7	Score 7 - 10
2210810	2021-05-17 16:50	e92ac2a61e4bf3c3da68dfc9ac3fd984	PaymentsTransactionApproved.pif	reported score: 2.6
2210785	2021-05-17 16:31	e92ac2a61e4bf3c3da68dfc9ac3fd984	PaymentsTransactionApproved.pif	reported score: 2.6
2210763	2021-05-17 16:15	1c32d785398e3a7eaab0e9b876903cc6	pdf2.pdf	reported score: 0.4
2210762	2021-05-17 16:15	bc65084128d6585291b01611408c36a7	pdf1.pdf	reported score: 10
2210759	2021-05-17 16:07	-	https://1drv.ms/443/o/s!BMA5DE2ChzV8mTx6QQNo6tGL3Lp?e=IIXeGMelVkelkNIB5Nn8Qg&at=9	reported score: 5.4



These are all the files being tested in the online Cuckoo environment. The pair of files you have tested will appear here when the report has been reported.

View the Results

- Open a report

ID	Date	Time	File Name	URL	Status	Score
2210695	2021-05-17	14:52	ca6aebcfd1af4967d5c4de3585c30685	unnamed.desc	reported	score: 1.4
2210694	2021-05-17	14:51	f79718a58a72f1a5eb0e7b6af9c0b100	PagoXinterbancario.pdf.gz	reported	score: 7
2210693	2021-05-17			http://aaaenterpriser.co.za/sharesecureupdate/UKDOV.html	reported	score: 5
2210692	2021-05-17		35978d2	cfc39b9dc7b0bd60_dvrHelper	reported	score: 2.9
2210691	2021-05-17		7d5a2c0	logo_small.desc	reported	score: 1.4
2210690	2021-05-17			http://203.159.80.188/bin.sh	reported	score: 9
2210689	2021-05-17		35978d2	cfc3	reported	score: 9

- Open Link in New Tab
- Open Link in New Window
- Open Link in New Private Window
- Bookmark This Link
- Save Link As...
- Save Link to Pocket
- Copy Link Location
- Search Google for "2021-05-17 14:5..."

Right-click the URL here and then select "Open Link in New Tab"

You should see the Summary page for this file open

Summary

File PagoXinterbancario.pdf.gz

Score: 7.0 out of 10!

This file is very suspicious, with a score of 7.0 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

Feedback: Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Property	Value
Size	565.7KB
Type	RAR archive data, v5
MD5	f79718a58a72f1a5eb0e7b6af9c0b100
SHA1	9d2926d8ecfaf88dbc7f12ac137d5937825e51be
SHA256	3c3b9858357e2241c7af40987b3e1886e476e8066c1c0323d854f057a818e788
SHA512	Show SHA512
CRC32	0BAB0E3F
ssdeep	None
Yara	None matched

What all is reported on the Summary page? Scroll down to view more!



View the Results

- When both of your tests shows **reported**
- View the results of the tests
 - Refresh the analysis page
- Which file was the malware?

packets1.pcap	reported	score: 3.3
packets2.pcap	reported	score: 10

The score ranges from 0-10, where 0 is a “safe” file while 10 is a potentially “dangerous” file*. Here, packets2.pcap would be the malware since its score was a 10.

*Please Note: While Cuckoo runs a lot of tests on a file, it does not always report correctly. Sometimes, the application might report a virus as a safe file and vice versa.

