

CREATING AND USING INDICATORS OF COMPROMISE

1.Creating an Indicator of Compromise

Created a folder on my windows virtual machine and named it lab11 as shown in the figure below.

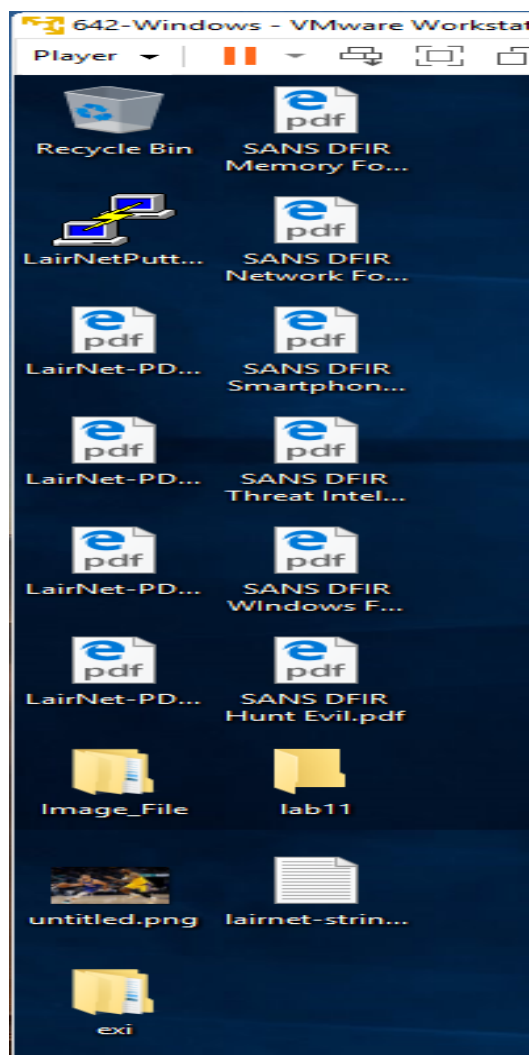


Figure 1/Folder

We launched Mandiant's IOC editor which we used to create a new indicator. After launching the application, we clicked file -> New -> indicator and we prompted with the screen below.

The screenshot shows the IOCe 2.2.0 application window. The title bar reads "IOCe 2.2.0 - C:\Users\student\Desktop\lab11". The menu bar includes "File", "Search", "Tools", and "Help". On the left is a table with columns "N..", "C..", "U..", "S..", and "G..". The first row contains the values "2..", "2..", and "a..". The main area on the right contains a form for a new indicator. The form fields are: "Name" (containing "New Unsavd Indicator"), "Author" (empty), "GUID" (containing "afdfecd4-efd8-4927-a39f-2d6d607be4c1"), "Created" (containing "2024-11-27 18:10:00Z"), and "Modified" (containing "2024-11-27 18:10:00Z"). There is also a "Description" text area. To the right of these fields is a small table with columns "T.." and "R..". Below the form is a section labeled "Add: AND OR Item" with a dropdown menu. At the bottom right is a "Save" button. The status bar at the bottom left shows "Loaded IOCs: 1 | Unsavd IOCs: 1".

Figure 2/new file

We created a new indicator of compromise using the filename of the file under investigation. Indicators of compromise are evidence that an intrusion has happened in an organization's network or endpoint. They are used to identifying when an attack has already compromised a system (Sentinelone, 2023). Then added the author's name as shown in the figure below.

IOCe 2.2.0 - C:\Users\student\Desktop\lab11

File Search Tools Help

| N.. | C.. | U.. | S.. | G.. |
|------|-----|-----|-----|-----|
| L... | 2.. | 2.. | a.. | |

Name: Laimet Trojan

Author: sam

GUID: afdfec4-efd8-4927-a39f-2d6d607be4c1

Created: 2024-11-27 18:10:00Z

Modified: 2024-11-27 18:10:00Z

Description:
The Trojan masquerades as a legitimate instance of PUTTY, however it includes (unwanted) functionality. This malware beacons out to a Command and Control (C2) on port 4444, the default Metasploit port.

Add: AND OR Item

OR
File Name contains Laimet

Save

Loaded IOCs: 1 | Unsaved IOCs: 1

Figure 3/filename

Then we saved the file into our folder that we had created earlier.

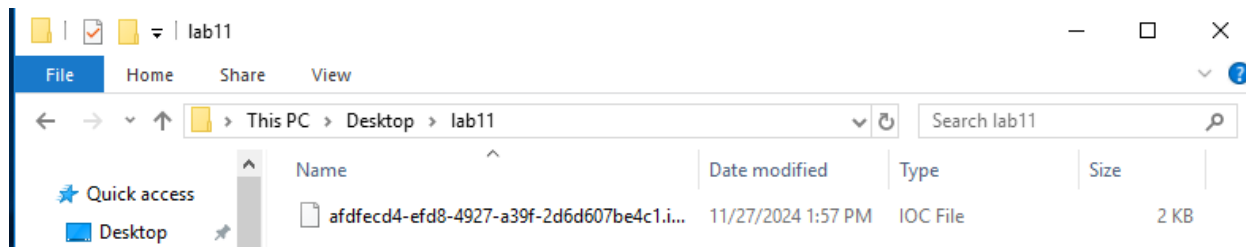


Figure 4/saved

2.Using an Indicator of Compromise

We used Mandiant's Redline application to create a new Indicator of Compromise search collector, then pointed it to the directory we had saved our IOC from our prior steps above. The figure below shows that we imported the IOC file using the Redline application.

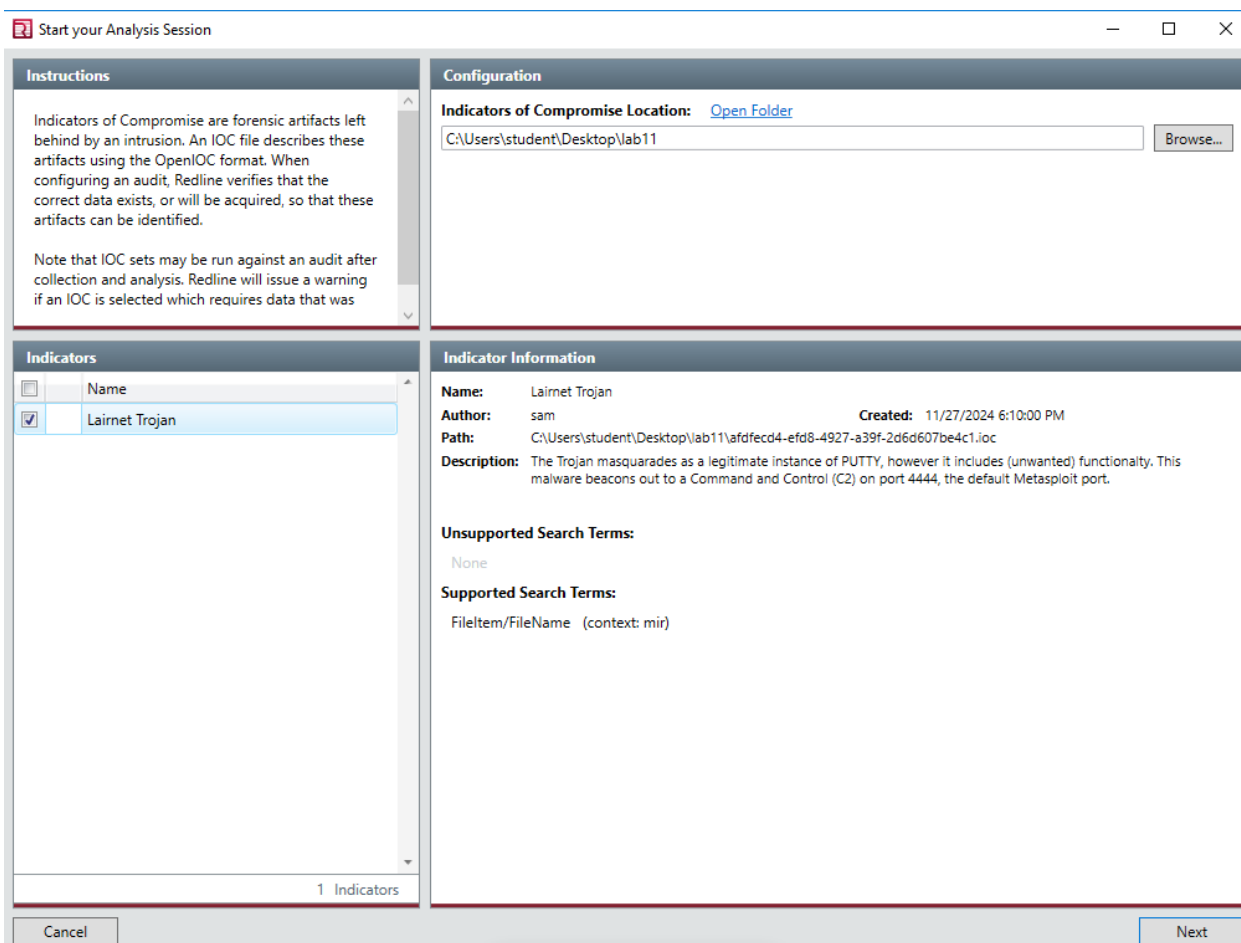


Figure 5/Redline application

We then clicked on edit script to take note of what the application has decided to capture based on the IOC's we had created on the file, and we made sure it did match our prior creation. This was made possible by referring to the file numeration section that is used to list all the files and the directories in file system (Microsoft, 2021).

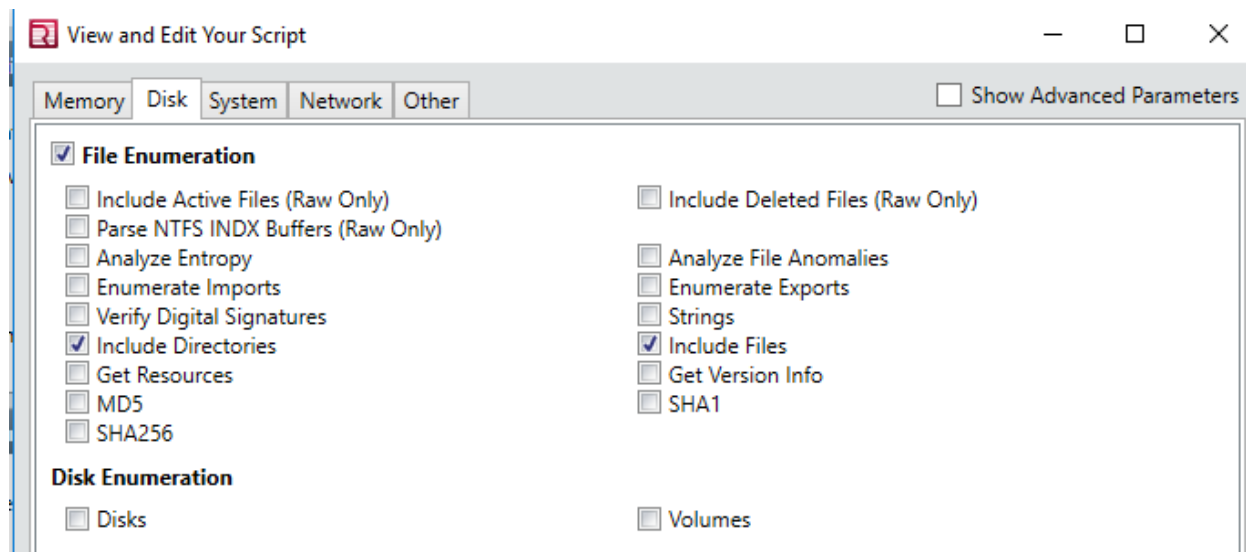


Figure 6/edit

We then saved our collector script to a new directory under the work folder that we had created earlier.

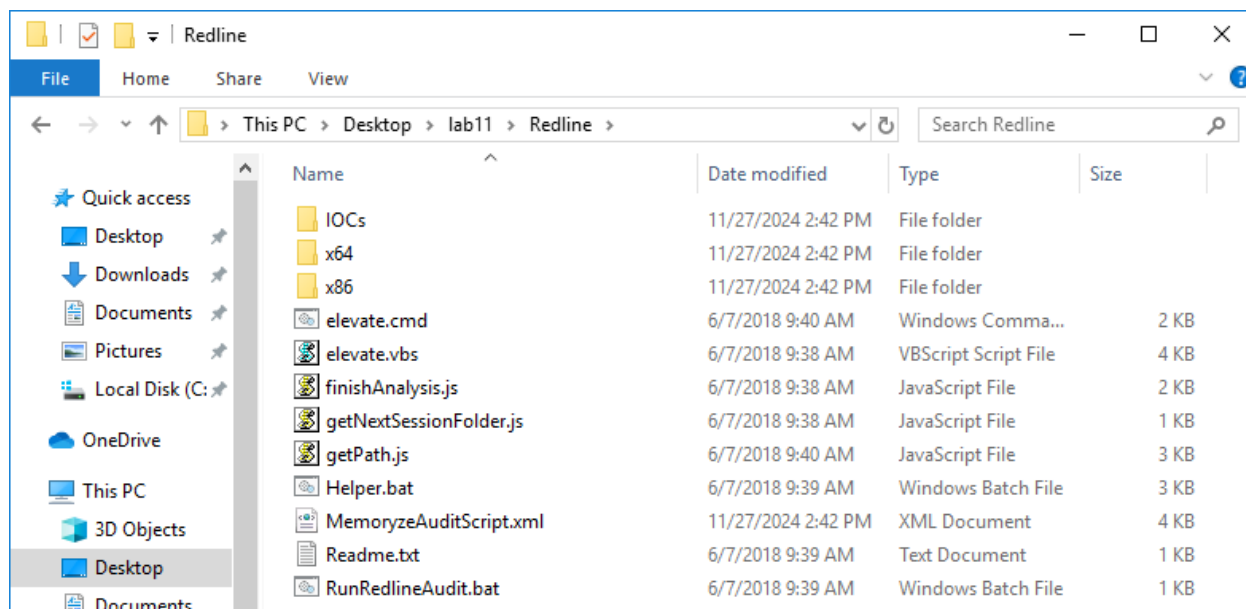


Figure 7/Script

We located and executed the “RunRedlineAudit.bat” file as shown in the figure below

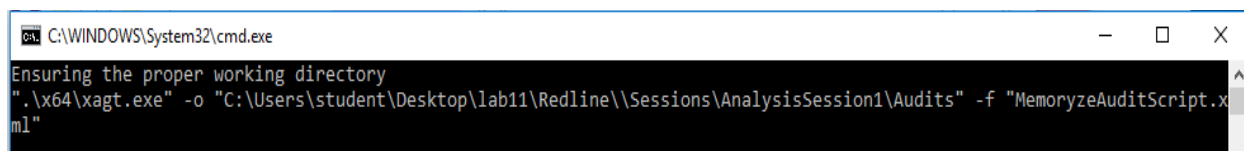


Figure 8/Bash script

After the script running there was a session folder created named “AnalyzeSession1.mans” that we double clicked to open. The Redline application saves the file analysis in a mans format, which can be open either from the Redline Home page or the Redline Launch Page (Ninja, 2016).

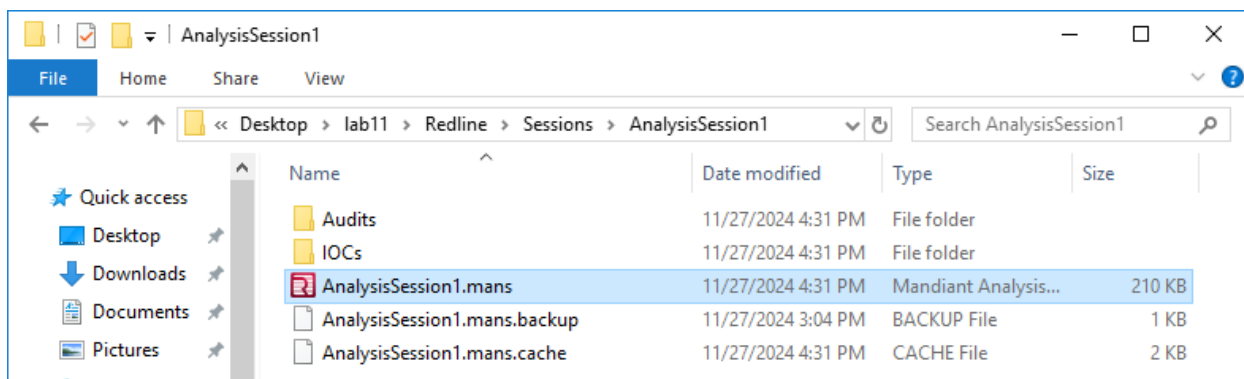


Figure 9/mans

With opening the file, which was ran on the Redline application, an IOC Report tab was created which had the results generated of the search against the IOC file created.

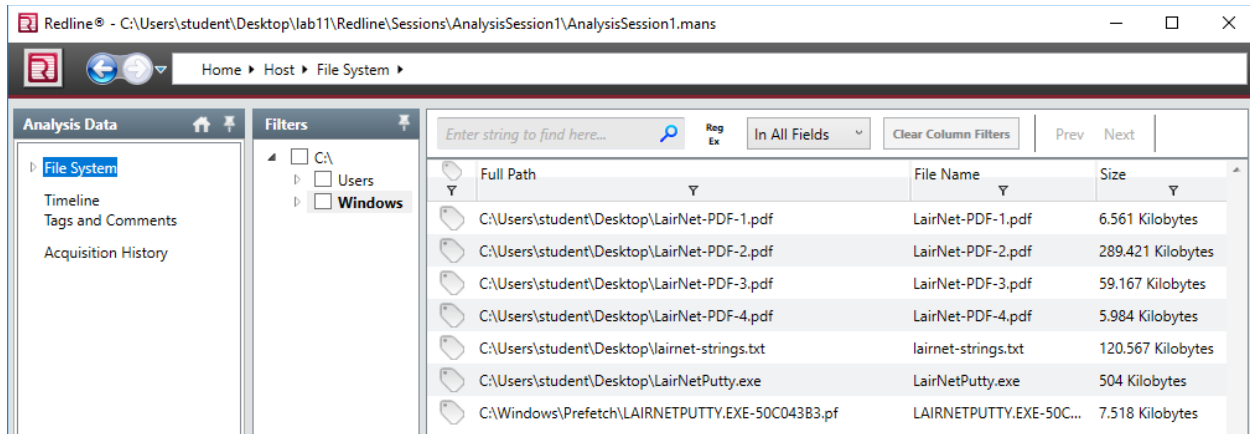


Figure 10/Windows

References

- Microsoft. (2021, September 15). *How to : Enumerate directories and files*. Retrieved from Microsoft learn challenge: <https://learn.microsoft.com/en-us/dotnet/standard/io/how-to-enumerate-directories-and-files>
- Ninja, s. (2016, May 17). *Memory anlaysis using redline*. Retrieved from Infosec: <https://www.infosecinstitute.com/resources/malware-analysis/memory-analysis-using-redline/>
- Sentinelone. (2023, March 11). *What are the indicators of compromise*. Retrieved from Sentinelone: <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-indicators-of-compromise-iocs-a-comprehensive-guide/>