Jordan Schalter

IT417 A.Toma

Lab2

4/19/2023

Q6.

Graphical user interface

Description automatically generated with medium confidence

Q10.

* 1. What is the PID?

A PID (i.e.,**process identification number**) is an identification number that is automatically assigned to each process when it is created on a [Unix](https://www.bing.com/ck/a?!&&p=ab217e433820aab9JmltdHM9MTY4MTg2MjQwMCZpZ3VpZD0wMjBlNGQ5Ny0zYTE3LTZjZGQtMGFiOC01YzZjM2I4MTZkMmQmaW5zaWQ9NTQ3NQ&ptn=3&hsh=3&fclid=020e4d97-3a17-6cdd-0ab8-5c6c3b816d2d&u=a1L3NlYXJjaD9xPVVuaXgmZmlsdGVycz1zaWQlM2FiNTk2NzQxOC00NmQxLTJmN2UtNDcwYi1kMWFmM2NlMThjYzgmZm9ybT1FTlRMTks&ntb=1)-like operating system.

[PID is used to identify processes (linfo.org)](http://www.linfo.org/pid.html#:~:text=A%20PID%20%28i.e.%2C%20process%20identification%20number%29%20is%20an,it%20is%20created%20on%20a%20Unix-like%20operating%20system.)

* 1. In the SVC command output, what are the Services and their relationship to the Image name?

The processes shown are the currently running executables that are being used within the system. I believe that the image name being referred to in the question is referencing the text file, and that is saved as tasklist\_SVC.txt. This text file is an export of the currently running executables.

* 1. How would this be beneficial to the blue team (how would this help you find or determine if something is malicious?

This could be beneficial since if something looks sus and unfamiliar then blue team could further investigate the .exe to confirm if it is malicious or not.

Q12.

Graphical user interface, text

Description automatically generated

Q14.

Graphical user interface, application

Description automatically generated

Q17.

Graphical user interface

Description automatically generated

Q21.

Complete the following: Perform Google searches for a minimum of 5 Event IDs. One of these should be focused on the new user you created in the earlier lab. Look up for each Event ID, provide a definition and how it could be useful in a blue team response effort. (Investigating a possible breach, malware, or compromise.) Hint: the vendor of the log source is typically my first go to. (Submit this answer)

5379 - This is event is new in Windows Server 2019. This event occurs when a user performs a read operation on stored credentials in Credential Manager.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5379#:~:text=This%20is%20event%20is%20new,stored%20credentials%20in%20Credential%20Manager>.

4797 - An attempt was made to query the existence of a blank password for an account.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4797>

4672 - The ID and logon session of the administrator-equivalent user that just logged on.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4672>

4624 - Identifies the account that requested the logon - NOT the user who just logged on.  Subject is usually Null or one of the Service principals and not usually useful information.  See New Logon for who just logged on to the system.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624>

4902 - The Per-user audit policy table was created.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4902

Q24.

1. On your Own, create a cmd that that finds New User Accounts being created (which event ID is this?) and output that file to the desktop. How long ago did you do this, you can adjust your time range accordingly. Open that file and show the new user you created and the corresponding Security Event logs associated with that action on the desktop. (Submit a Screenshot).

Graphical user interface, text, application

Description automatically generated

Q29.

Graphical user interface, text

Description automatically generated

Q29-2.

Graphical user interface, text, application

Description automatically generated

Q30.

Graphical user interface, text, application

Description automatically generated

Q32b.

Graphical user interface, application, Word

Description automatically generated

Q33.

Graphical user interface

Description automatically generated

Q34.

A screenshot of a computer

Description automatically generated with medium confidence

1. Utilizing TCPView, netstat or any command lines in this exercise, review your (or someone’s) Windows machine for suspicious network connections. This is the learning objective of the assignment. Utilizing this lab's commands and instructions you need to be able to answer this question. As the step suggests you can use TCPView as an easier alternative since it is a GUI but missingI challenge you to try and repeat at least 1-2 established connections via the PowerShell command lines that you learned in this lab. Use your favorite whois lookup, I like dnslytics but you can pick whatever whois lookup. Be sure to list out your steps as well. Your response should provide the following in a clear and direct format. I will do one walk through one with you as an example. Submit the table format below with my example. Be sure to include:
   1. Commands/programs utilized
   2. Complete List of Each ESTABLISHED connection (Please use the table below to list connections. If no connections are established, open a web browser with a few tabs and connect to at least 5 Internet sites.)
      1. Program/PID
      2. IP Address (Whois lookup or some other validation)
      3. Valid or Suspicious Connection listing

### Submission

Utilize the table format below to list your ESTABLISHED connections that were reviewed with the details of the columns headers.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Program / method | PID | Local (source) Address/Port | Remote (destination) Address/Port | Valid/Suspicious | Reason/Why |
| netstat -ano | 732 | 192.168.2.202:20225 | 23.227.38.32:80 | Suspicious (don’t trust it) – it collects personal information like names, addresses and credit card information. It is a true social engineering scheme masquerading as a hot sauce website. Sorry was having too much fun here, this should just go into the next column. | IP lookup is owned by shopify, the domain name is redacted. Doing a safe google search with quotes it appears that this seems like a safe website that sells hot sauce. Website looks like it needs some work and the SEO and previews are really lacking. Man, hire a website designer |
| tcpview | 732 | 192.168.2.202:51120 | 23.227.38.32:443 | Valid | Non of the analysis / googlefu found anything malicious |