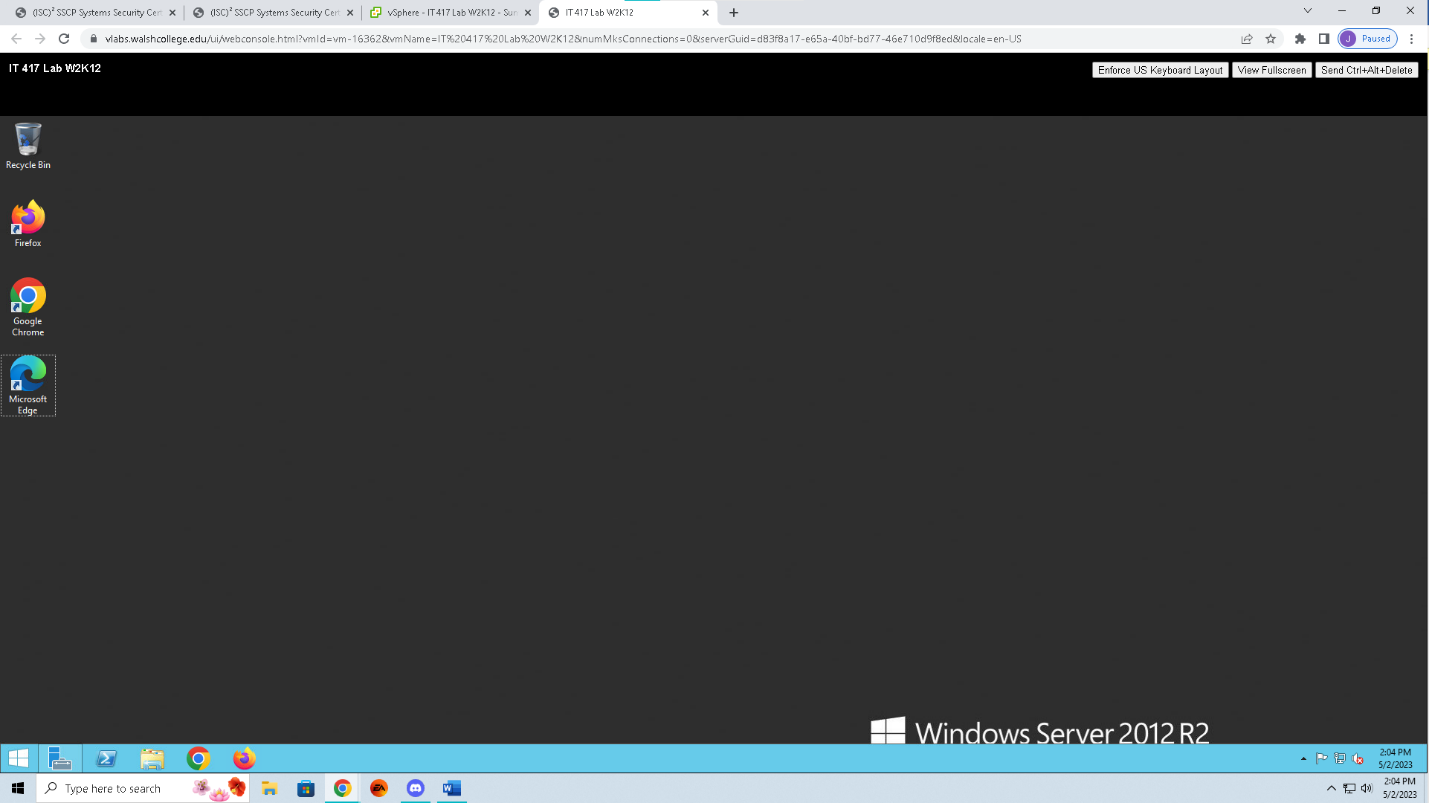
Jordan Schalter

IT417 A.Toma

Assignment4

2/3/2023

Q19.



Q25.

A screenshot of a computer

Description automatically generated

Q30.

A screenshot of a computer

Description automatically generated

Q43.

A screenshot of a computer

Description automatically generated

Q 49A.

Graphical user interface, text, application

Description automatically generated

b. Who is the author? Why would this be important?

WIN-INQ5OLTON31\Administrator. This is important to note, because if there is not supposed to be an admin with that name then you obviously know that it may be malicious intent.

c. What are the triggers?

If I recall correctly, the triggers from the lab (I am no longer on the lab and away from my home computer at the moment) will nuke the C drive on the last day of the month at around 6:30am.

d. What are the Actions? Why would the location be important? How could you search this folder for its contents? How could you pivot?

The actions are that the C drive will be wiped, this is important since the C drive holds the operating system and could jeopardize the entire system if the action triggers.

e. What are the Conditions?

At the end of every month, the C drive will be wiped at 6:30 in the morning.

f. What are the settings?

The settings show what will happen and how the explosion will be executed.

Q50.

A screenshot of a computer

Description automatically generated

Q53.

A screenshot of a computer

Description automatically generated

Q55.

A screenshot of a computer

Description automatically generated

Q55-2

A screenshot of a computer

Description automatically generated

Q58.

A screenshot of a computer

Description automatically generated

Q59.A

A screenshot of a computer

Description automatically generated

b. What do they represent?

They represent .exe or other operations that are running or runnable on the system.

c. What information can you see when you open one?

When the service was started if it is running, how long the service has been running, the author of the service and if it belongs to the local system or if it as .exe that is run through the network.

d. What information is helpful on the General tab?

General information on the services.

e. Any other tabs?

There are other tabs but, I will have to go back to them as I had an emergency situation last night and I cannot get into Vlabs at the moment as I originally planned on doing to answer these short answer questions.

Q61.

A screenshot of a computer

Description automatically generated

Q62.

A screenshot of a computer

Description automatically generated with medium confidence

Q63.

A screenshot of a computer

Description automatically generated