Tests & Quizzes

Quiz 2

Return to Assessment List

Part 1 of 1 - 4.0/ 5.0 Points

Question 1 of 1

The topic for module 8 is containerization. One aspect of containerization that is commonly used is the idea of "detonating" malware. In other words, you run a piece of malware in a VM to see what it does for analysis. A good example of such a site is malwr.com. Most malware *used to* detect if it was running in a virtual machine. If it was running in a VM, it would then usually exit (assuming that it was being analyzed) to avoid detection.

4.0/ 5.0 Points

Virtualization is also becoming more popular in the enterprise ("VDI" or Virtual Desktop Infrastructure) is becoming very popular. Considering for VDI is becoming more popular, answer the following question: would it behoove a malware author to still exit if they detect that they're running in a virtual machine? Why or why not?

Feel free to use external resources, but add any references that you use.

A VDI is outside the VM and is design in a way that it cannot be seen and be attack by the physical machine.The logical way for a VM to exploited is how the virtual machine is created. There could be exit outside the data vm though the lack of design through the VM, bugs that could be form of exit is memory the host allocate for the VM or attached devices such as bridge network card. Another way for malware to exit is if a user enable shared access between the guest and host machine then it can cause malware to find ways too exploit through the shared access.

Comment: Please put more explanation into your answer

Timezone: America/New_York

- Terms of Use
- Send feedback to the NYU Classes Team
- Powered by Sakai
-

Change Profile Picture

Error removing image

Error uploading image

Upload Choose File No file chosen

Save Cancel Connections ✖ Remove

Search for people ...

View More

My Connections | Pending Connections

You don't have any connnections yet. Search for people above to get started.

You have no pending connections.

←Back to My Connections

Search for people ...

$({cmLoader.getString("connection_manager_no_results")}

Done