Installing, using and Blocking a Malware - Based Backdoor

(CompTIA Security + SY – 601)

Objectives:

To analyze potential indicators in order to determine the type of attack

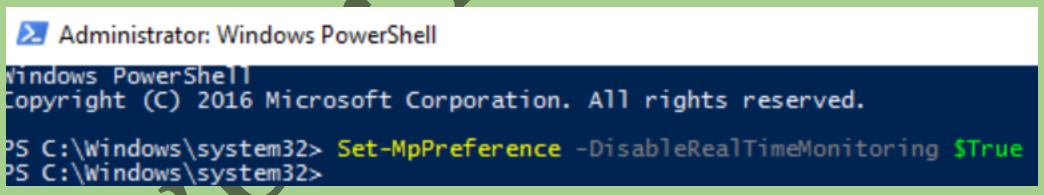
Resources:

1. Windows Virtual Machine VM
2. ODYSSEUS with a Backdoor Malware
3. Angry IP ort scanner

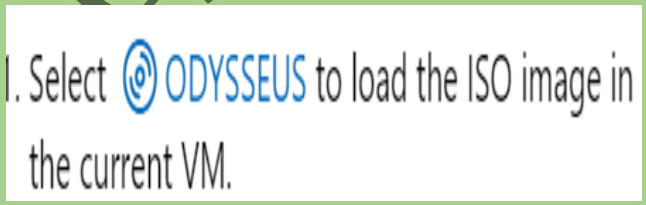
Instructions:

1. Log in to the MS1 in the Windows virtual Machine VM
2. Select start and right-click Windows Powershell and Run as administrator
3. When prompted select Yes to confirm UAC

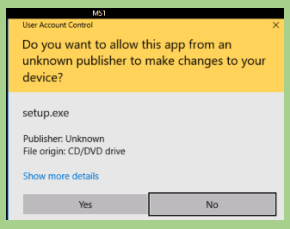
4. Type the following and press Enter
5. Type the following command



6. Close the Powershell window
7. Select the ODYSSEUS to load the ISO image in the current VM

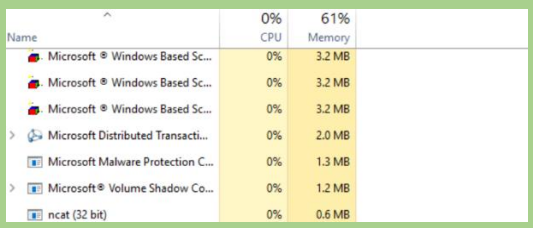


8. In the MS1 VM window click the notification and then Select Run setup.exe

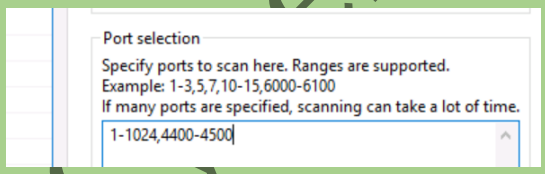


9. If necessary, select show more details
10. You would normally proceed but for this activity select Yes
11. When Installation is complete you will see to new icons in the desktop. Open either SimpleHash or SimpleSalter shortcuts from the desktop

12. Close the utility window
13. Right-click the taskbar and select the Task Manager, if necessary, select More details to view the full interface

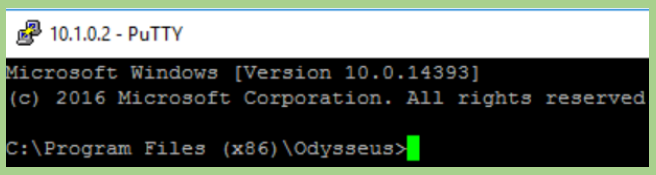


14. Close the Task Manager
15. Log in to the DC1 in the Windows virtual Machine VM
16. From the desktop open the AngryIP shortcut
17. In the ip range box type 10.1.0.2
18. Select the preference icon to open the Preferences dialog box
19. Select the ports tab and enter T-1024, 4400, 4500

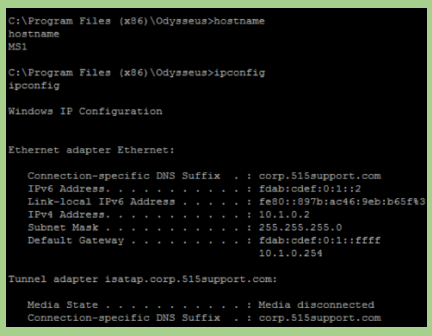


20. Select start to begin the scan
21. When the scan is complete, select close
22. Close the AngryIP scanner window

23. On the DC1 VM double click the PUTTY icon in the LABFILES folder



24. In the Host name box type 10.1.0.2 and in the port, box enter 4450
25. In the saved session box type MS1then select the save button
26. Select Open after a few second you will be connected to the command prompt on MS1
27. Run the following commands to confirm your remote connections:



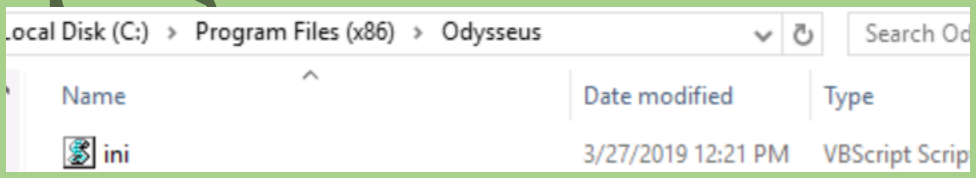
28. Run the following command to create a user account named mal on the remote server

```
C:\Program Files (x86)\Odysseus>net user /add mal Pa$$w0rd
net user /add mal Pa$$w0rd
The command completed successfully.
```

29. Run the following command to add the mal user to the local administrator group

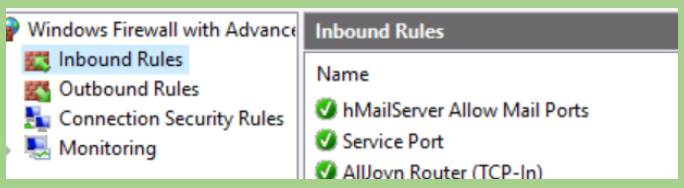
```
C:\Program Files (x86)\Odysseus>net localgroup administrators mal /add
net localgroup administrators mal /add
The command completed successfully.
```

30. Leave the PUTTY window open
31. Switch back to the MS1 on the Windows Virtual Machine
32. Using the File Explorer browse and note the ini.vbs file



33. Open the ini.vbs file and note the actions that the script performs
34. Close the script file and use the File Explorer to delete it
35. Open the Task Manager

36. Select the processes tab in the Task Manager and then right-click on the ncat (32bit) process and end Task
37. Select start then type firewall with advanced security and the open the Firewall with advanced security link that appears
38. Select the Inbound Rules node



39. Double click the rule added by the trojan, select Disable Rule and delete it

Observations:

1. The ODYSSEUS backdoor malware was loaded and installed on the MS1 Windows VM.
2. The Angry IP Scanner identified the target IP range and open ports.
3. A remote connection was successfully established using PUTTY.
4. A new user account named 'mal' was created and added to the local administrator group.
5. The ini.vbs script was examined and deleted to stop the malware's actions.
6. The ncat process associated with the malware was terminated.
7. The malicious inbound firewall rule created by the trojan was disabled and deleted.

Results:

1. Successful identification of target IP and open ports using Angry IP Scanner.
2. Establishment of a remote connection to the MS1 VM.
3. Creation and administrative elevation of a new user account, confirming remote access capabilities.
4. Successful termination of the ncat process and deletion of the ini.vbs script, effectively neutralizing the malware.
5. Disabling and removal of the malicious firewall rule, restoring network security.

Conclusion:

The lab effectively demonstrated the installation, usage, and mitigation of a malware-based backdoor. Key skills acquired included configuring network scans, establishing remote connections, identifying and terminating malicious processes, and modifying firewall rules to block malware.

Future Work:

Future work should involve deeper exploration of advanced malware analysis techniques, developing strategies for proactive threat detection, and enhancing defensive measures to prevent similar attacks. Additionally, integrating more sophisticated malware and defensive scenarios will further solidify practical cybersecurity skills.