Week Lab 7 Evasion Techniques  
CIS 450  
Krutarth Panchal

## Section 1: Anti-malware Scanning (AMSI) Bypass

AMSI is an interface on which applications or services can scan script for malicious usage. If a signature of script is registered by AMSI antimalware service provider, it will be blocked by Windows Defender. Since AMSI relies on being loaded within the process executing the actual script, techniques to break or patch specific functions within amsci.dll are well known.   
  
In this section 1 of the lab, we will try to bypass through Downgrading, amsiInitFailed, and AMSI.fail.  
  
First, we’ll start with installing DotNet v2.0 SP1 and downloading Mimikatz payload as guided in Lab walkthrough  
   
A computer screen shot of a blue screen

Description automatically generatedFig 1.1  
A blue screen with red text

Description automatically generated  
Fig 1.2

We have invoking Mimikatz.ps1 but as we can see from Fig 1.1 it failed and was detected by Static and dynamic analysis of Windows defender and also the command *amsiutils* also failed to run Fig1.2.

A screenshot of a computer error

Description automatically generated  
Fig 1.3  
Here we downgrading and choosing to use PowerShell version 2 and re-running amsiutils as shown in Fig 1.3 but it not running and is blocked again.

A computer screen shot of a blue screen

Description automatically generated  
Fig 1.4

We turned off “Real-time protection” before importing Mimikats module into Powershell v2 session. Turned on “Real-time protection” back and attempted to Invoke Mimikats payload and this time is worked successful thereby evading ASMI as shown in Fig1.4.

A screen shot of a computer error

Description automatically generated  
Fig 1.5

Here we tried “raw” payload through PowerShell v3(with AV enabled). It was blocked by antivirus as seen in Fig 1.5.

A computer screen with red text

Description automatically generated  
Fig 1.6

This time I tried to obtain base-64 value of AmsiUtils & amsiInitFailed using the command used in Fig 1.6.

A screen shot of a computer

Description automatically generated  
Fig 1.7

Now we inserted converted text into our script as shown in Fig 1.7

A blue screen with red text

Description automatically generated  
Fig 1.8

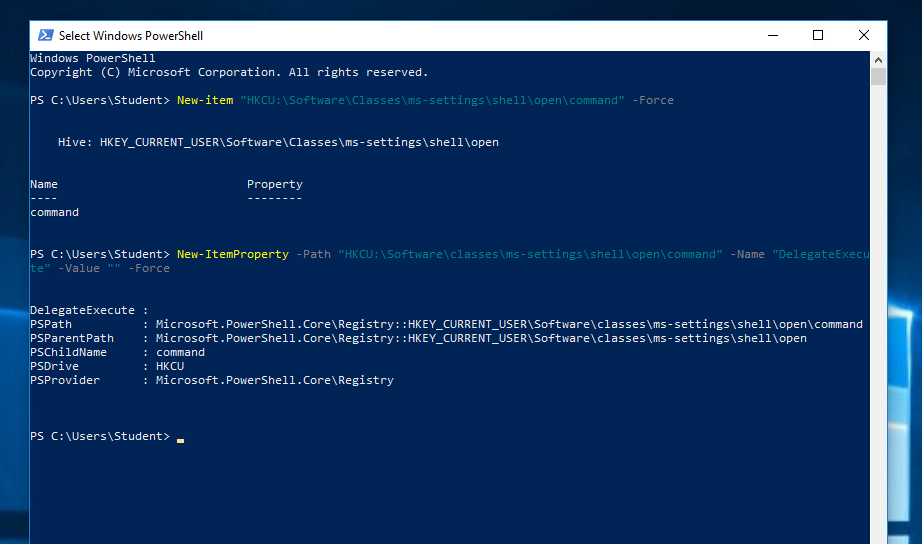
I attempted to run *amsiutils* to verify if bypass was successful, but in my case it was still blocked by the Antivirus. ☹

This technique prevents AMSI scanning capability for the current process by setting “amsiInitFailed” flag but in our instance it did not work according to Lab.

## Section 2: User Account Control (UAC) Bypass

The purpose of the User Account Control (UAC) is to make sure that certain changes are made only with the approval from the administrator, if not approved by administrator they action will not be executed and the Windows will remain unchanged.

In Section 2 part of the lab we will attempt to Bypass the User Account Control (UAC)

  
Fig 2.1

As shown in the figure the command is executed to modify the registry.

A blue screen with white text

Description automatically generated  
Fig 2.2

As shown in the fig 2.2, command is created to open a command prompt without triggering the UAC.

A screenshot of a computer

Description automatically generated  
Fig 2.3

Bypass command is executed using *fodhelper* as shown in the fig 2.3 and our Command prompt shell cmd.exe with Admin privileges has successfully opened up bypassing the User Account Control. Section 2 is a success!

## Section 3: ExecutionPolicy Bypass

An execution Policy is part of PowerShell security strategy. It determines whether you can load configuration files like your PowerShell profile or run scripts by checking they are digitally signed or not.  
  
Section 3 part of the lab is an attempt to bypass PowerShell’s ExecutionPolicy.

A screenshot of a computer

Description automatically generated  
Fig 3.1

We have run the command as shown in Fig 3.1 to set the Execution Policy to be On. Also, we have verified it.

A screenshot of a computer

Description automatically generated  
Fig 3.2

As shown in the fig 3.2 I have created a message.ps1 file and attempted to run it and what we see is that Execution Policy we prior set is in place and has blocked our attempt to run the python file.

A blue screen with white text

Description automatically generated  
Fig 3.3

By using the command shown in the Fig 3.3 we have bypassed through read and redirect. And as you can see “Mile-2” shows as success.

A computer screen shot of a program

Description automatically generated  
Fig 3.4

As shown in the Fig 3.4, by using EncodedCommand we have bypassed the execution policy as our message “Mile2” shows in success.

A blue screen with white text

Description automatically generated  
Fig 3.5

Lastly, as we in Fig 3.5 by using Invoke-Expression we again bypass Execution policy as our message “Mile-2” is seen again.

## Questions:

1. What is MimiKatz used for in pen testing or attacks?

Ans: Mimikatz is a tool that is commonly used by hackers and security professionals to extract sensitive information, such as passwords and credentials, from a system’s memory. It is typically used to gain unauthorized access to networks, systems, or applications or to perform other malicious activities, such as privilege escalation or lateral movement within a network.

1. What are three techniques that a pen tester can try to bypass AMSI?

Ans: a. Downgrading   
 b. amsiInitFailed  
 c. AMSI.fail

1. What does User Account Control do on a Windows system?

Ans: The purpose of the User Account Control (UAC) is to make sure that certain changes are made only with the approval from the administrator, if not approved by administrator they action will not be executed and the Windows will remain unchanged.

1. One has to hack the Windows system in order to disable UAC. (T or F)

Ans: False. Disabling User Account Control (UAC) is a built-in function in Windows, however it's not recommended as it can weaken your computer's security.

1. What scripting application can one use to implement an ExecutionPolicy Bypass?

Ans: Read and redirect, Encoded command and Invoke-expression can be used in scripting application to implement ExecutionPolicy bypass.

---------------------------------------End of Lab----------------------------------------------------------