**SOP OF WINDOWS PASSWORD HACKING**

**METHOD 2: HOW TO CRACK WINDOWS 10 PASSWORD AND ENTER THE SYSTEM USING THE FAKELOGINSCREEN TOOL**

In this method we are going to use FakeLogonScreen, a fantastic utility to steal or hack Windows 10 password.

[Now in this method we will be creating a very simple payload that might get detected by the Windows Defender, so to complete this practical/method we need to turn off the defender in our target Windows 10 machine.]

Attacker Machine: Kali Linux [LHOST]

Text

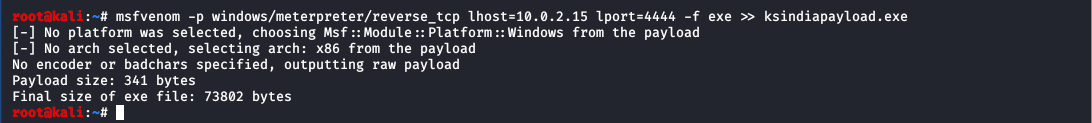
Description automatically generated

Target machine: Windows 10 [RHOST]

Text

Description automatically generated

**Step 1**: We will create a [malicious payload by using msfvenom tool](https://www.ehacking.net/2020/04/how-to-hack-an-android-phone-using-metasploit-msfvenom-in-kali-linux.html) according to the information acquired by the target system. We will set lhost to our Kali’s IP i.e., 10.0.2.15, and set lport as 4444. We will generate a payload as an executable file so that it easily gets executed on the target machine.



**Step 2**: The payload with name “ksindiapayload.exe” will be generated and you can find it in the home directory.

A screenshot of a computer

Description automatically generated with medium confidence

**Step 3**: The most crucial stage is to get the target download this malicious payload. In real-life scenarios, an attacker can use different social engineering techniques and let the target user to download this malicious file into his system. For practical demonstration, we will share the payload with the Windows machine via web server (Apache server).

**Step 3a**: For this we will start the apache service:

Graphical user interface, text

Description automatically generated

**Step 3b**: Now go to the directory /var/www/html and then you can create a new directory here and name it “ksindia\_share”. Now put the data (the payload we created) that you want the Windows 10 machine to access here.

Graphical user interface, application

Description automatically generated

**Step 3c**: We can access shared content on both OS (Linux & Windows), to access the content, first open the browser window (any browser like Chrome,Firefox,IE etc) and type IP Address of the kali machine in Address bar and add /ksindia\_share to it to access the data in that particular directory.

So basically, we will be typing 10.0.2.15/ksindia\_share.

Graphical user interface, text, application, email

Description automatically generated

**Step 4**: Now to listen to the incoming connection from the exploited system (Windows 10) we will use the Metasploit framework.

**Step 4a**: Start msfconsole:

A picture containing graphical user interface

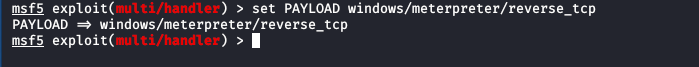
Description automatically generated

**Step 4b**: Start the multi handler:

Shape

Description automatically generated with medium confidence

**Step 4c**: Set the payload as windows/meterpreter/reverse\_tcp:



**Step 4d**: Show options:

Text

Description automatically generated

**Step 4e**: Set the LHOST as 10.0.2.15 (your system IP) and LPORT as 4444

Text

Description automatically generated with medium confidence

**Step 4f**: After configuring it all, just run the exploit, go back to the Windows machine, and run the executable, i.e., ‘payload.exe’. This will quickly get us a meterpreter session.

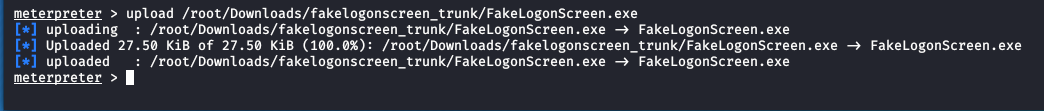
Text

Description automatically generated

**Step 5**: Now that we have got a meterpreter session we will upload the executable.

Step 5a: We will upload the FakeLogonScreen executable that we will download from:

<https://github.com/bitsadmin/fakelogonscreen/releases>



**Step 5b**: After that, get the shell access and run FakeLogonScreen.exe as showing be:

Graphical user interface, text

Description automatically generated

**Step 5c**: And YAYY!! At the target machine, all the running windows would get closed, and the logon screen would pop up, asking the credentials and appears it as a legitimate window. The user would not hesitate for a second to enter his credentials and get his work back.

A screenshot of a video game

Description automatically generated with medium confidence

**Step 5d**: To check the strength of this tool, we will be entering the wrong password. [And this will show the error “The password is incorrect, try again.” This is the strength of FakeLogonScreen tool that enforces a target to enter his correct password. The user has no choice other than that to enter his password.]

A screenshot of a video game

Description automatically generated with medium confidence

**Step 5e**: Let us enter the correct password, and you will get your standard window as nothing happened before.

Graphical user interface, text

Description automatically generated

**Step 5f**: This also showing the FakeLogonScreen works similar to a keylogger. The attacker would easily monitor all the logs and could grab the correct password of the target user.

Text

Description automatically generated