

Описание работы скрипта

Скрипт написан на PowerShell (by Windows).

Скрипт выполняется при запуске с правами пользователя без административных прав.

Шаги выполнения скрипта

1. Присвоение переменным значений принимающего, отправляющего e-mail, периода повторения выполнения скрининга экрана.
2. Определение локальной папки для временного сохранения скриншота для отправки на e-mail принимающего.
3. Старт бесконечного цикла по снятию скриншота, сборки почтового сообщения и отправки его получателю с ранее указанным периодом повторения.
4. Снятие скриншота и сохранение его в том же месте, что и исполняемый скрипт.
5. Сборка почтового сообщения.
6. Отправка сообщения.
7. Удаление ранее сохраненного скриншота освобождая место для нового скриншота.
8. Ожидание указанного периода повторения.
9. Выполнения операций с шага 4 по шаг 8 в бесконечном цикле до момента прерывания процесса исполнения программы из вне.

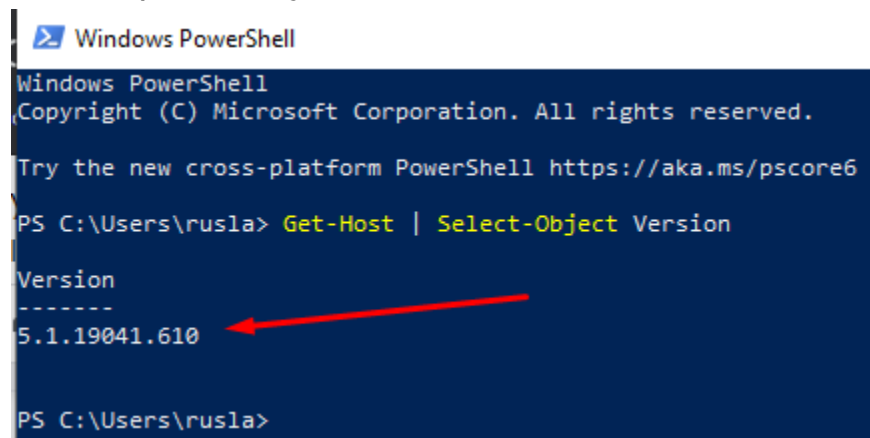
Требования к системе для выполнению скрипта

Операционная система: Windows 8 -10 версии, Windows Server 2012 - 2019 версии

PowerShell окружение: 3 по 7.1

Проверить версию установленную необходимо в консоли PowerShell выполнить команду

Get-Host | Select-Object Version



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\rusla> Get-Host | Select-Object Version

Version
-----
5.1.19041.610

PS C:\Users\rusla>
```

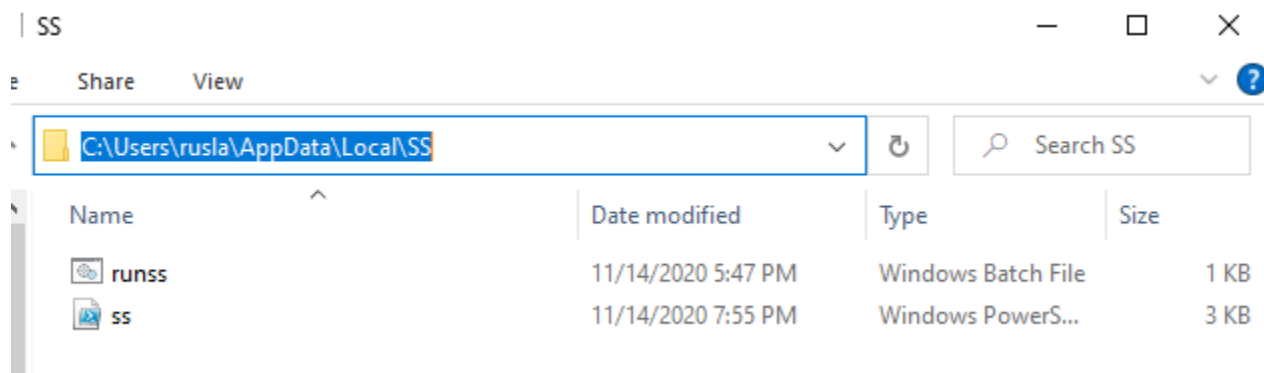
Если PowerShell отсутствует в установленном виде на Windows, то установить руководствуясь ссылкой:
<https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-windows?view=powershell-7.1>

Настройка скрипта и расположение файлов

Расположить файл необходимо в директории доступной аккаунту под которым происходит настройка без административных прав или повышенных привилегий.

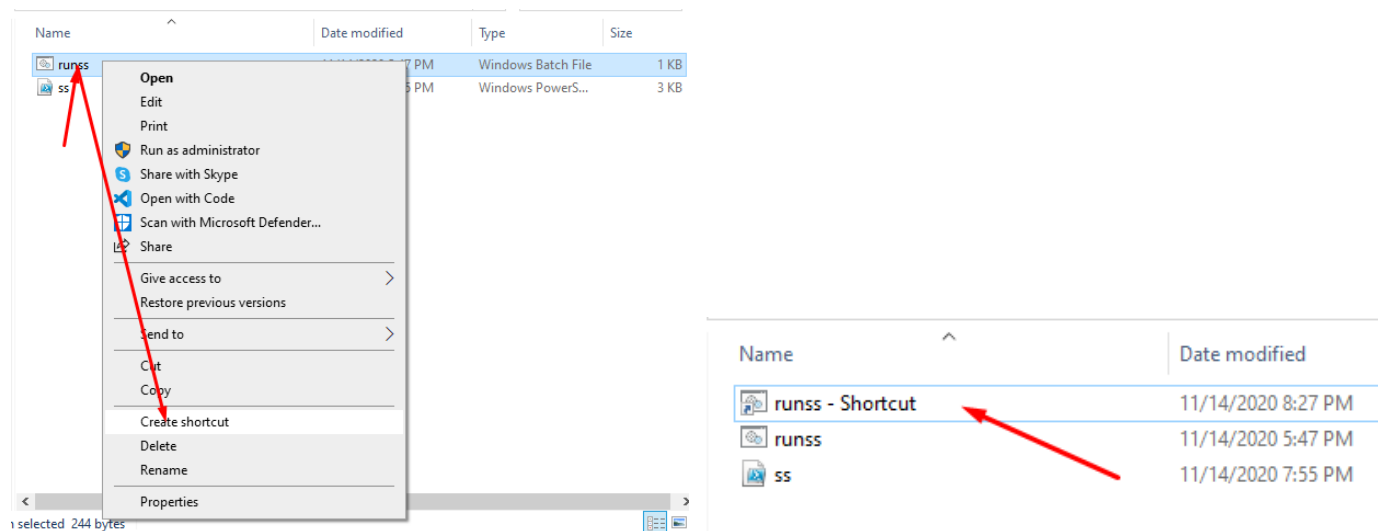
Практический пример

Создать в директории **c:\Users\rusla\AppData\Local** директорию **SS**, где **rusla** это директория аккаунта (учетной записи), чтобы получить полный путь **c:\Users\rusla\AppData\Local\SS**
По этому пути директории расположить файлы **ss.ps1** и **runss.bat**



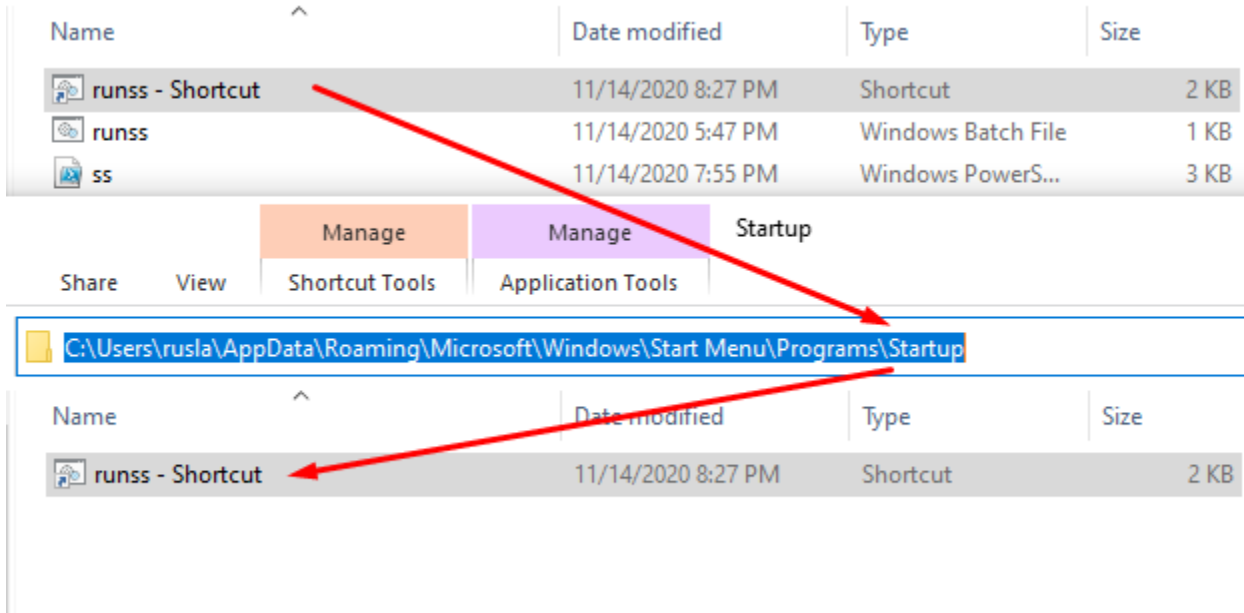
Создать ярлык для файла **runss.bat** и скопировать\перенести его в директорию автозагрузки текущей учетной записи **c:\Users\rusla\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**

Создание ярлыка runss

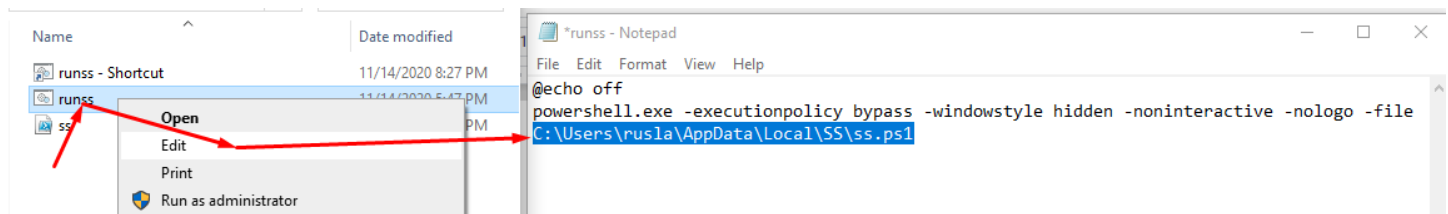


Ярлык runss - Shortcut перенести\скопировать

в папку автозагрузки приложений учетной записи:



Указать актуальный путь к исполняемому скрипту ss.ps1 в файле runss.bat



... -file C:\Users\rusla\AppData\Local\SS\ss.ps1

Указание значений переменных в скрипте ss.ps1

```
c:\> Users > rusla > AppData > Local > SS > ss.ps1 > ...
1  # test execution in cmd to run powershell -ExecutionPolicy Bypass
2  # replace the pathe to the PS script in the XML Task Sheduler co
3  # Enable task, laung task or reboot machine
4  # powershell C:\Users\rusla\AppData\Local\SS\ss.ps1
5
6  #customer settings
7  $MailSubject = "Dell E6230 Desktop Screen Ruslan Dzumaiev"; # u
8  $MailBody = "Some text in the Body"; # up to you
9  $receivermail = "admin@victory-gold.com"; # up to you
10
11
12  # screenshot period in seconds
13  $sleeping = 1800;
14
15  # sender e-mail auth data
16  $MailSender = "screenshot@victory-gold.com";
17  $MailSenderPassword = "gUK&rzZ82w6F";
18  $MailServer = "upp.victory-gold.com";
19  $MailServerPort = "587";
20
```

Переменные и их назначение

#customer settings

\$MailSubject = "Dell E6230 Desktop Screen Ruslan Dzhumaiev"; #

Текст темы отправляемого письма, рекомендовать можно внести текст однозначно идентифицирующий с какой учетной записи\какой рабочей машины пришло письмо

\$MailBody = "Some text in the Body"; #

Текст тела письма для которой нет рекомендаций и вписывается текст по усмотрению

\$receivermail = "admin@gmail.com"; #

Адрес принимающего скриншоты, позволяет через запятую указать нужное количество принимающих адресов, учитывая рекомендацию не указывать более 10 адресов для избежания повышения нагрузки на почтовый сервер или фильтра спам рассылки.

Рекомендую использовать для приема писем почтовые ящики gmail.com, ukr.net и другие бесплатные для исключения переполнения корпоративного принимающего почтового аккаунта по выделенному размеру пространства на сервере.

screenshot period in seconds

\$sleeping = 1800;

Период выполнения скрипта в секундах, где 60 сек = 1 мин, 1800 сек = 30 мин, рекомендовать можно не указывать период менее 30 секунд для избежания переполнения почтового ящика.

Размер 1-го письма до 150 kB (килобайт).

Ниже указаны настройки авторизационных переменных для отправки писем.

Предопределен специально выделенный почтовый аккаунт screenshot@gmail.com для специфических целей этого скрипта. Указать данные можно любого другого на свое усмотрение.

sender e-mail auth data

\$MailSender = "screenshot@gmail.com";

\$MailSenderPassword = "gUKs&rzrsZ82w6F";

\$MailServer = "mail.server..com";

\$MailServerPort = "587";

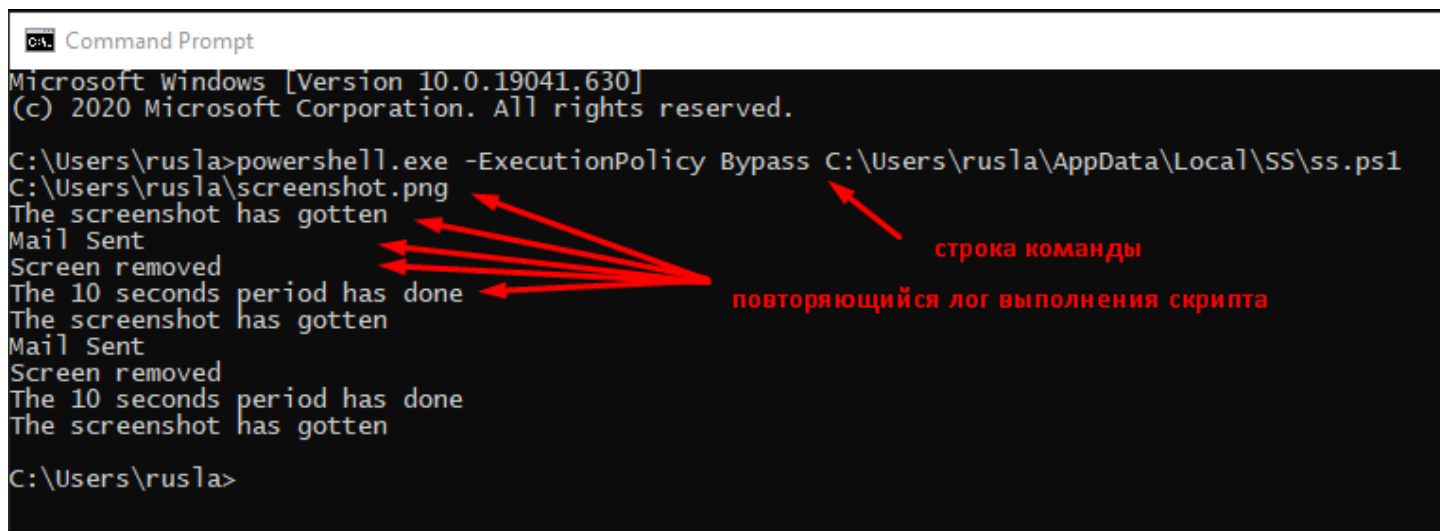
После редакции файлов необходимо их сохранить.

Проверка выполнения скрипта

Тест проводится перед вводом скрипта в эксплуатацию

Запуск скрипта из cmd консоли командой

powershell.exe -ExecutionPolicy Bypass C:\Users\rusla\AppData\Local\SS\ss.ps1 эта команда аналогична в исполняемом bat файле runss.bat, но без аргументов “-windowstyle hidden -noninteractive -nologo -file”, скрывающих окно консоли в которой выполняется, чтобы отследить лог выполнения



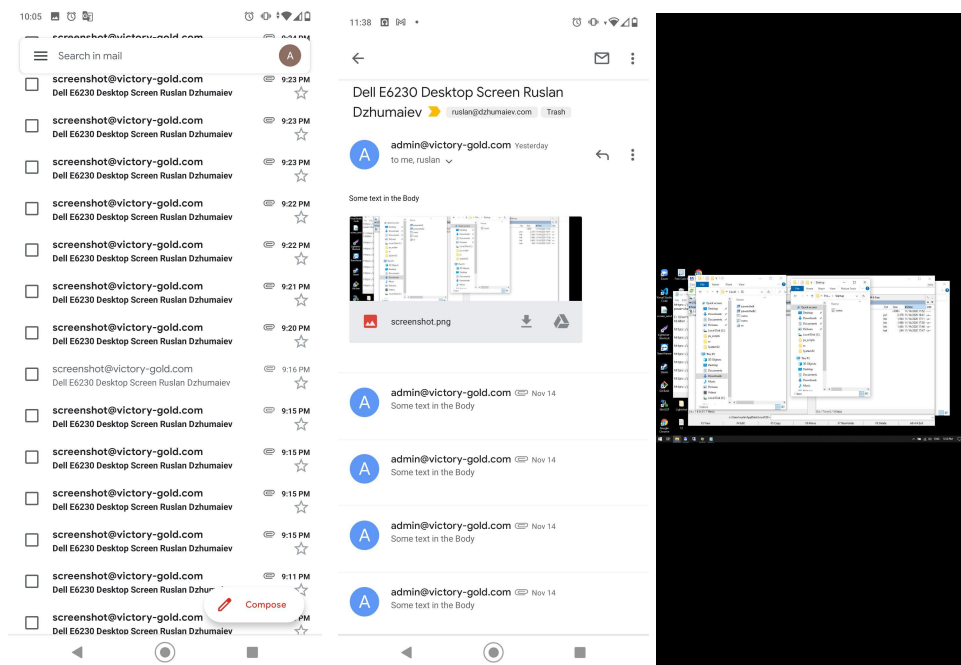
```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\rusla>powershell.exe -ExecutionPolicy Bypass C:\Users\rusla\AppData\Local\SS\ss.ps1
C:\Users\rusla>screenshot.png
The screenshot has gotten
Mail Sent
Screen removed
The 10 seconds period has done
The screenshot has gotten
Mail Sent
Screen removed
The 10 seconds period has done
The screenshot has gotten
C:\Users\rusla>
```

строка команды

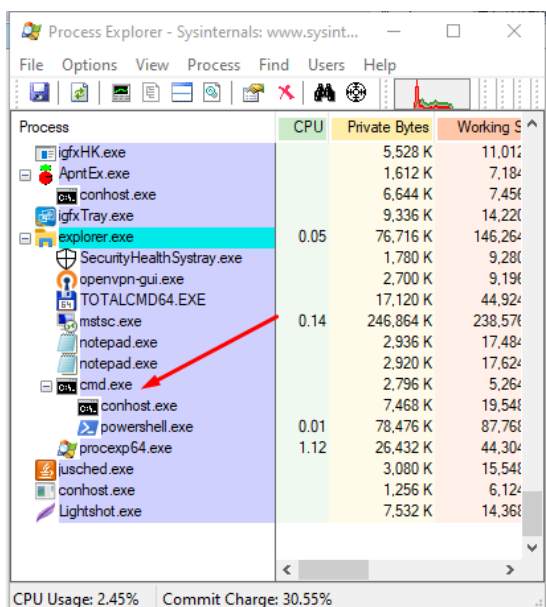
повторяющийся лог выполнения скрипта

В почтовый ящик принимающего придут письма со скриншотами аналогичные этим:



Запуск bat файла для запуска скрипта с унаследованными правами аккаунта

Запустить runss.bat файл двойным кликом мыши в директории `c:\Users\rusla\AppData\Local\SS\`, или с командной строки `c:\Users\rusla\AppData\Local\SS\runss.bat` при этом окно консоли закроется согласно команды внутри runss.bat файла и увидеть процесс запущенный возможно с помощью утилиты Process Explorer <https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>



Так же проконтролировать, что приходят ли письма принимающему адресу и терминировать (удалить) процесс powershell.exe и потом conhost.exe в ветке cmd.exe-conhost.exe-powershell.exe как на скриншоте выше правым кликом мыши на процесс Kill process

Запуск ярлыка (ссылки) на bat файла

Выполняется двойным кликом мыши на ярлыке (ссылке) на runss.bat файл `c:\Users\rusla\AppData\Local\SS\runss - Shortcut.lnk` и так же проконтролировать, что приходят ли письма принимающему адресу и терминировать (удалить) процесс powershell.exe и потом conhost.exe в ветке cmd.exe-conhost.exe-powershell.exe как на скриншоте выше правым кликом мыши на процесс Kill process

Выход из и вход в учетную запись Log off / Log in

Скрипт запускается через механизм Startup исполняемый при входе в учетную запись аккаунта, и так же проконтролировать, что приходят ли письма принимающему адресу и терминировать (удалить) процесс powershell.exe и потом conhost.exe в ветке cmd.exe-conhost.exe-powershell.exe как на скриншоте выше правым кликом мыши на процесс Kill process

Перезагрузка системы или выключение\включение

Механизм проверки аналогичен “Выход из и вход в учетную запись Log off / Log in”

Возможные ошибки и их решение

Не запускается любой из файлов

(bat, ps1, ярлык) - проверить правильность пути к скрипту ss.ps1

Нет писем в течении 1-2 минут

у принимающего адреса - возможна задержка в работе между серверами около 10 минут, что требует ожидания.

Нет писем после ожидания более чем 10 минут

- проверить подключение в интернет.

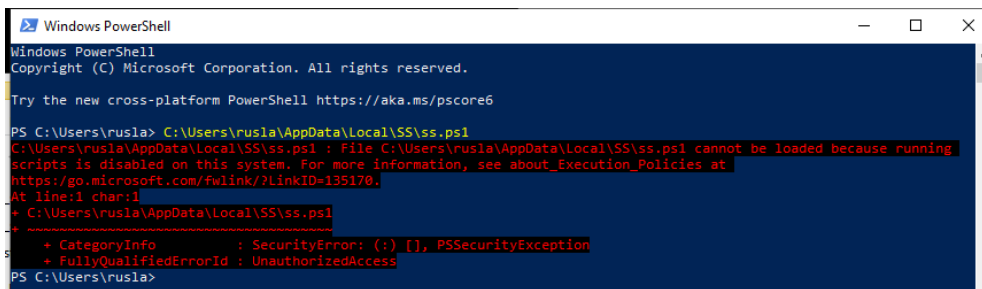
Антивирус или встроенные Defender блокирует скрипт

и предупредил нотификацией, что скрипт будет заблокирован и помещен в карантин, тогда необходимо зайти в Антивирус и/или Defender и разрешить исполнение или выставить указание игнорировать этот скрипт.

Необходимость проверить ss.ps1 в powershell консоли

Эту проверку нет необходимости выполнять для запуска в работу или если нет цели модернизировать скрипт.

При запуске скрипта C:\Users\rusla\AppData\Local\SS\ss.ps1 в powershell консоли есть ошибка



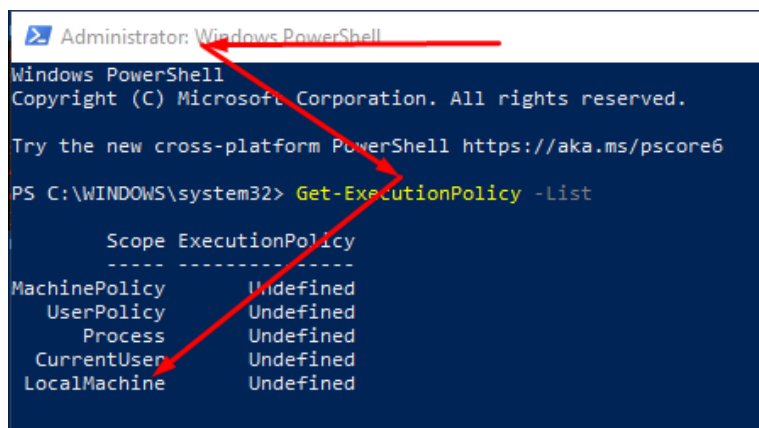
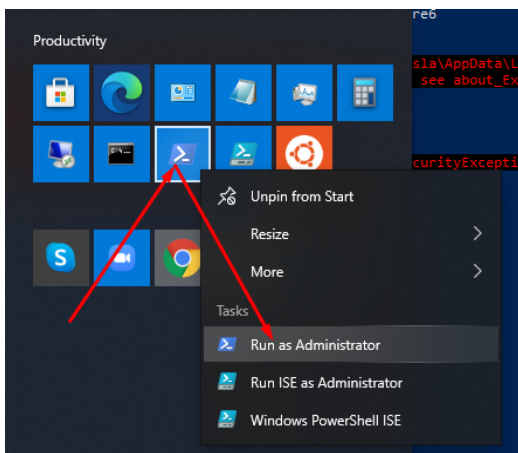
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\rusla> C:\Users\rusla\AppData\Local\SS\ss.ps1
C:\Users\rusla\AppData\Local\SS\ss.ps1 : File C:\Users\rusla\AppData\Local\SS\ss.ps1 cannot be loaded because running
scripts is disabled on this system. For more information, see about_Execution_Policies at
https://go.microsoft.com/fwlink/?LinkID=135170.
at line:1 char:1
+ C:\Users\rusla\AppData\Local\SS\ss.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\Users\rusla>
```

Это не является критичным, что решаемо если запустить консоль powershell от Администратора и внести правки в настройки Execution_Policies и проверить разрешения **Get-ExecutionPolicy -List**:



```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Get-ExecutionPolicy -List

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine Undefined
```

И включить разрешение для LocalMachine:

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\WINDOWS\system32> Get-ExecutionPolicy -List

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine RemoteSigned

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\rusla> C:\Users\rusla\AppData\Local\SS\ss.ps1
C:\Users\rusla\AppData\Local\SS\ss.ps1 : File C:\Users\rusla\AppData\Local\SS\ss.ps1 cannot be loaded because running
scripts is disabled on this system. For more information, see about_Execution_Policies at
https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ C:\Users\rusla\AppData\Local\SS\ss.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\Users\rusla> C:\Users\rusla\AppData\Local\SS\ss.ps1
C:\Users\rusla\screenshot.png
The screenshot has gotten
Mail Sent
Screen removed
The 10 seconds period has done
The screenshot has gotten
PS C:\Users\rusla> ^C
```

Ruslan Dzhusmaiev (Dzhusmaiev.com)