# Безопасное затирание удаленных файлов

## Описание:

Команда производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. path: string - Путь до папки, которую необходимо затереть. Путь должен разделяться "\" или "/". Если переменная не указана явно, то принимает значение "C:/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 cipher\_folder: bool - Возвращает статус выполенения.  
 cipher\_folder\_info: string - Подробная информация о затирании информации.  
}

# Включение (отключение) автозагрузки на всех устройствах Windows

## Описание:

Скрипт disable\_autorun отключает автозапуск вообще всех дисков. Скрипт enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию). Требуется настроенная служба winrm https. Входы и выходы актуальны для обоих скриптов \_\_\_ ## Input: { ❗ ip\_address or hostname : string - Адрес целевой машины }

## Secrets:

{  
 ❗ login : string - Имя пользователя, под которым заходим на машину  
 ❗ password : string - Пароль от пользователя  
 ❗ domain : string - Домен, в котором расположена машина  
}

## Output:

{  
 red\_edit\_result : bool - Возвращает статус выполенения  
 red\_edit\_result\_info : string - Подробная информация о включении (отключении) автозагрузки  
}

# Включение USB-носителей win

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_info: string - Подробная информация о включении usb.  
}

# Включение автообновления win

## Описание

Команда производит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_autoupdate: bool - Возвращает статус выполенения.  
 turn\_on\_autoupdate\_info: string - Подробная информация о включении автообновлений.  
}

# Включение брандмауэра

## Описание

Включает брандмауэр. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_firewall: bool - Возвращает статус выполенения.  
 turn\_on\_firewall\_info: string - Подробная информация о включении фаервола.  
}

# Включение службы Windows

## Описание

Включает службу, имя которой было передано. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ service: string - Имя службы, которую надо включить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_service: bool - Возвращает статус выполенения.  
 turn\_on\_service\_info: string - Подробная информация о включении службы.  
}

# Выключение машины Windows

## Описание

Завершает работу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении. \_\_\_ ## Input: { ❗ ip\_address or *hostname*: string - Адрес целевой машины. sd\_time: int - Время до выключения машины (по умолчанию 60 секунд). message: string - Сообщение, которое увидят пользователи (по умолчанию "Ваш компьютер будет выключен через {sd\_time} секунд(-у, -ы). Сохраните открытые файлы."). }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 win\_shutdown: bool - Возвращает статус выполенения.  
 win\_shutdown\_info: string - Подробная информация о выключении машины.  
}

# Отключение USB-носителей Windows

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее: - будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов; - ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено). \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_info: string - Подробная информация о включении usb.  
}

# Блокировка доменного пользователя

## Описание:

Отключает учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка локального пользователя Windows

## Описание:

Отключает учётную запись пользователя.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка пользователя Linux

## Описание

Блокирует указанного пользователя на указанном хосте. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Принудительное завершение процесса Linux

## Описание

Команда kill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ process\_name: string - Имя процесса, который нужно отключить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о завершении процесса.  
}

# Завершить все RDP соединения на сервере Win.

## Описание

Отключает все RDP сессии на сервере. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_rdp\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_rdp\_sessions\_info: string - Подробная информация об отключении активных RDP сессий.  
}

# Завершить сеансы всех пользователей Windows

## Описание

Завершает ВСЕ активные сессии на указанной машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_sessions\_info: string - Подробная информация об отключении.  
}

# Включение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_write\_info: string - Подробная информация о включении запрета записи usb.  
}

# Изменение политики паролей в домене AD

## Описание:

Скрипт изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!!

Условные обозначения для формата:

D = Дни (от 0 до 10675199)

H = Часы (от 0 до 23)

M = Минуты (от 0 до 59)

S = Секунды (от 0 до 59)

F = Доли секунды (от 0 до 9999999)

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес машины, на которой будет выполняться скрипт (лучше всего подойдёт контроллер домена).  
 ❗ ComplexityEnabled: bool - Указывает, включена ли сложность пароля для политики паролей.  
 ❗ LockoutDuration: string - Требуемый формат: "D.H:M:S.F". Указывает период времени, в течение которого учетная запись блокируется после того, как количество неудачных попыток входа в систему превышает порог блокировки. Вы не можете войти в заблокированную учетную запись, пока не истечет период времени блокировки. Этот параметр задает свойство lockoutDuration объекта политики паролей.  
 ❗ LockoutObservationWindow: string - Требуемый формат: "D:H:M:S.F". Указывает максимальный интервал времени между двумя неудачными попытками входа в систему, по истечении которого количество неудачных попыток входа сбрасывается до 0. Учетная запись блокируется, когда количество неудачных попыток входа превышает порог блокировки политики паролей. Этот параметр задает свойство lockoutObservationWindow объекта политики паролей  
 ❗ LockoutThreshold: int - Указывает допустимое количество неудачных попыток входа, прежде чем учетная запись будет заблокирована. Это число увеличивается, когда время между неудачными попытками входа в систему меньше, чем время, указанное для окна времени наблюдения за блокировкой. Этот параметр задает свойство LockoutThreshold политики паролей.  
 ❗ MaxPasswordAge: string - Требуемый формат: "D.H:M:S.F". Определяет максимальное время, в течение которого вы можете иметь один и тот же пароль. По истечении этого периода срок действия пароля истекает, и вы должны создать новый.  
 ❗ MinPasswordAge: string - Требуемый формат: "D.H:M:S.F". Указывает минимальное время, по истечении которого вы сможете изменить пароль.  
 ❗ MinPasswordLength: int - Указывает минимальное количество символов, которое должен содержать пароль. Этот параметр задает свойство MinPasswordLength политики паролей.  
 ❗ PasswordHistoryCount: int [Указывает количество предыдущих паролей для сохранения. Пользователь не может повторно использовать пароль из списка сохраненных паролей. Этот параметр задает свойство PasswordHistoryCount для политики паролей.  
 ❗ ReversibleEncryptionEnabled: bool - Указывает, должен ли каталог хранить пароли с использованием обратимого шифрования. Этот параметр задает свойство ReversibleEncryption для политики паролей.  
 ❗ identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 change\_password\_policy: bool - Возвращает статус выполенения.  
 change\_password\_policy\_info: string - Подробная информация о изменении парольной политики.  
}

# Получение имени УЗ по SID

## Описание:

Возвращает имя учётной записи по её SID.

## Input:

{  
 ❗ sid: string - SID пользователя, имя УЗ которого надо узнать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_account: bool - Возвращает статус выполенения.  
 get\_account\_info: string - Имя учётной записи пользователя, в случае успеха, или сообщение об ошибке.  
}

# Получение списка интерфейсов и информации о них

## Описание:

Скрипт подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_settings: bool - Возвращает статус выполенения.  
 linux\_settings\_info: list -> string | string - Массив строк, которые содержат название инфтерфейсов и информацию о них, в случае успеха или строка, информация об ошибке.  
}

# Обновление пакетов

## Описание:

Обновляет установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper. Local версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления) Remote версия обновляет на удаленной linux машине. \_\_\_ Local-версия ## Input: {

}

## Secrets:

{  
  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

Remote-версия ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

# Определяет местоположение по ip

## Описание:

Первая версия использует библиотеку ipwhois. Вторая использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).

ipwhois-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

ipinfo-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
 ❗ ipinfo\_token: string - Токен, предоставляемый сервисом.  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение ssh соодинений

## Описание:

Скрипт производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_ssh: bool - Возвращает статус выполенения.  
 turn\_off\_ssh\_info: string - Подробная информация об отключении ssh соединений.  
}

# Отключение активных сессий Liunx

## Описание:

Отключает все активные сессии. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_session: bool - Возвращает статус выполенения.  
 turn\_off\_session\_info: string - Подробная информация об отключенных пользователях.  
}

# Отклюлчение всех сетевых интерфейсов

# Описание:

Отключает все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 disabled: bool - Возвращает статус выполенения.  
 disabled\_info: string - Подробная информация об отключенных интерфейсах.  
}

# Отключение службы Win

## Описание:

Отключает указанный сервис.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ service\_name: string - Имя сервиса, который необходимо отключить.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_service\_result: bool - Возвращает статус выполенения.  
 disable\_service\_result\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение узла Linux

## Описание:

Отключает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. time\_out: int - Время, через которое компьютер выключится. message: string - Сообщение, которое будет выводиться пользователям. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_node: bool - Возвращает статус выполенения.  
 turn\_off\_node\_info: string - Подробная информация о выключении компьютера.  
}

# Включение запрета на cd dvd

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_cddvd: bool - Возвращает статус выполенения.  
 turn\_off\_cddvd\_info: string - Подробная информация о включении запрета записи cd dvd.  
}

# Отключает все сетевые интерфейсы

## Описание:

Отключает сетевые интерфейсы. После отключения невозможно удаленно зайти на машину. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_net\_int\_win: bool - Возвращает статус выполенения.  
 disable\_net\_int\_win\_info: string - Подробная информация об отключении интерфейсов.  
}

# Отправить сообщение авторизованным по ssh пользователям Linux

## Описание:

При использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер. Невозможно достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 send\_message: bool - Возвращает статус выполенения.  
 send\_message\_info: string - Подробная информация об отправленном сообщении.  
}

# Отправить сообщение пользователю Win

## Описание:

Отправляет сообщение на указанный хост.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 message\_result: bool - Возвращает статус выполенения.  
 message\_result\_info: string - Подробная информация об отправленном сообщении.  
}

# Перезагрузить компьютер Windows

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 message: string - Сообщение, отображаемое пользователям.  
 timeout: string - Время до перезагрузки.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reboot\_win: bool - Возвращает статус выполенения.  
 reboot\_win\_info: string - Подробная информация о перезагрузке.  
}

# Перезагрузка узла Linux

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. message: string - Сообщение, отображаемое пользователям. timeout: int - Время до перезагрузки. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 reboot\_node: bool - Возвращает статус выполенения.  
 reboot\_node\_info: string - Подробная информация о блокировке пользователя.  
}

# Получение времени и даты

## Описание:

Возвращает текущее время на Linux-машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_time: bool - Возвращает статус выполенения.  
 linux\_time\_info: string - Подробная информация о времени на устройстве.  
}

# Получение политики паролей в домене AD

## Описание:

Скрипт возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_password\_policy: bool - Возвращает статус выполенения.  
 get\_password\_policy\_info: list - Массив, содержащий политики и их значения.  
 get\_password\_policy\_info.[].name: string - Название политики.  
 get\_password\_policy\_info.[].value: string - Установленное значение политики.  
}

# Получить список запущенных процессов

## Описание:

Позволяет получить список процессов, запущенных на машине и их pid-ы. get\_win\_proc - получает информацию из виндовых машин get\_linux\_proс - пполучает информацию из линуксовой машин

Windows-версия

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

Linux-версия \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

# Завершить процесс Windows

## Описание:

Завершает процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗ \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. user: string - Имя учётной записи пользователя, процессы которого нуобходимо завершить. process: string or int - Имя процесса или его pid. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о блокировке пользователя.  
}

# Проверить целостность системных файлов Windows

## Описание:

Выполняет сканирование системных файлов, результат выводится строкой. Может занять очень много времени.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 check\_win: bool - Возвращает статус выполенения.  
 check\_win\_info: string - Подробная информация о результатах сканирования.  
}

# Проверка в Virus Total

## Описание:

Проверяет заданный url или ip адрес в Virus Total.

## Input:

{  
 ❗ ip: string - ip или url, который неоьбходимо проверить.  
}

## Secrets:

{  
 ❗ vt\_api\_key: string - Api-key для сервиса Virus Total.  
}

## Output:

{  
 result: string - Возвращает строку, содержащую результат проверки.  
}

# Проверка доступности хоста утилитой ping

## Описание:

Работает как на linux, так и на windows Отсылает только один пакет Доступность проверяется с того же хоста, где установлен SOAR \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
   
}

## Output:

{  
 ping: bool - Возвращает статус выполенения.  
 ping\_info: string - Подробная информация о доступности хоста.  
}

# Отключение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_write\_info: string - Подробная информация о выполнении операции.  
}

# Сброс пароля локального пользователя

## Описание:

Сбрасывает (устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https. \_\_\_

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, ккоторому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля пользователя.  
}

# Сброс пароля доменного пользователя

## Описание:

Сбрасывает пароль выбранного пользователя (устанавливает смену пароля при следующем логине).

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля.  
}

# Получение списка подключенных USB устройств

## Описание:

Возвращает список всех usb-устройств, подключенных к компьютеру в данный момент \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_usb: bool - Возвращает статус выполенения.  
 connected\_usb\_info: list -> string - Массив, содержащий названия usb-устройств.  
}

# Получение списка подключенных пользователей

## Описание:

Возвращает список всех подключенных пользователей, а также информацию о них.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_users: bool - Возвращает статус выполенения.  
 connected\_users\_info: list -> string - Подробная информация о подключенных пользователях.  
}

# Список контроля доступа

## Описание:

Скрипт возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке и её подпапкам.  
}

# Список контроля доступа

## Описание

Скрипт возвращает список контроля доступа (ACL) для папки узла Windows. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\" или "/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке.  
}

# Получение списка правил Iptables

## Описание:

Скрипт возвращает правила из Iptables

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list - Массив, содержащий правила из Iptables или информация об ошибке.  
 firewall\_rules\_info.[].chain\_name: string - Название цепочки.  
 firewall\_rules\_info.[].values: list - Массив, содержащий информацию о правилах.  
 firewall\_rules\_info.[].values.[].target: string - Eсли пакет отвечает правилу, заголовок target указывает, что с ним нужно сделать.  
 firewall\_rules\_info.[].values.[].prot: string - Протокол  
 firewall\_rules\_info.[].values.[].opt: string - Данный параметр используется редко и отображает опции IP  
 firewall\_rules\_info.[].values.[].source: string - Исходный IP-адрес или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].destination: string - IP-адрес назначения или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].info: string - Любая часть правила, которая не указана предыдущими столбцами  
}

# Список правил Windows Firewall

## Описание:

Скрипт возвращает список всех правил Windows Firewall.

**Работает только с >= win 10!** \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list -> string - Список всех правил на Firewall.  
}

# Список открытых сессий

## Описание:

Скрипт возвращает все активные активные сессии.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 active\_sessions: bool - Возвращает статус выполенения.  
 active\_sessions\_info: list - Подробная информация об установленных подключениях.  
 active\_sessions\_info.[].username: string - Имя пользователя  
 active\_sessions\_info.[].sessionname: string - Имя сессии  
 active\_sessions\_info.[].id: string - id сессии  
 active\_sessions\_info.[].state: string - Состояние сессии  
 active\_sessions\_info.[].idle\_time: string - Время простоя  
 active\_sessions\_info.[].logon\_time: string - Время входа  
}

# Список установленных сетевых соединений

## Описание:

Скрипт возвращает все активные соединения хоста в виде списка. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 estabilish\_conn\_result: bool - Возвращает статус выполенения.  
 estabilish\_conn\_result\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilish\_conn\_result\_info.[].RemoteAddress: string - Удаленный адрес  
 estabilish\_conn\_result\_info.[].LocalAddress: string - Локальный адерес  
}

# Получение списка установленных соединений

## Описание:

Возвращает массив установленных хостом подключений. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 estabilished\_connetctions: bool - Возвращает статус выполенения.  
 estabilished\_connetctions\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilished\_connetctions\_info.[].local\_address: string - Локальный адерес  
 estabilished\_connetctions\_info.[].foreign\_address: string - Удаленный адрес  
}

# Удаление из локальной группы

## Описание:

Удаляет пользователя из указанной локальной группы. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя учётной записи пользователя, которого необходимо удалить из группы. ❗ group: string - Имя группы, из которой необходимо удалить пользователя. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 del\_user\_from\_group\_result: bool - Возвращает статус выполенения.  
 del\_user\_from\_group\_result\_info: string - Подробная информация об удалении пользователя из группы.  
}

# Удаление папки и её содержимого

## Описание:

Удаляет переданную папку и всё её содержимое. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь до папки, которую необходимо удалить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Удаляет папку win

## Описание:

Производит удаление папки

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Полный путь до папки. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

''.join(document)

# Безопасное затирание удаленных файлов

## Описание:

Команда производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. path: string - Путь до папки, которую необходимо затереть. Путь должен разделяться "\" или "/". Если переменная не указана явно, то принимает значение "C:/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 cipher\_folder: bool - Возвращает статус выполенения.  
 cipher\_folder\_info: string - Подробная информация о затирании информации.  
}

# Включение (отключение) автозагрузки на всех устройствах Windows

## Описание:

Скрипт disable\_autorun отключает автозапуск вообще всех дисков. Скрипт enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию). Требуется настроенная служба winrm https. Входы и выходы актуальны для обоих скриптов \_\_\_ ## Input: { ❗ ip\_address or hostname : string - Адрес целевой машины }

## Secrets:

{  
 ❗ login : string - Имя пользователя, под которым заходим на машину  
 ❗ password : string - Пароль от пользователя  
 ❗ domain : string - Домен, в котором расположена машина  
}

## Output:

{  
 red\_edit\_result : bool - Возвращает статус выполенения  
 red\_edit\_result\_info : string - Подробная информация о включении (отключении) автозагрузки  
}

# Включение USB-носителей win

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_info: string - Подробная информация о включении usb.  
}

# Включение автообновления win

## Описание

Команда производит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_autoupdate: bool - Возвращает статус выполенения.  
 turn\_on\_autoupdate\_info: string - Подробная информация о включении автообновлений.  
}

# Включение брандмауэра

## Описание

Включает брандмауэр. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_firewall: bool - Возвращает статус выполенения.  
 turn\_on\_firewall\_info: string - Подробная информация о включении фаервола.  
}

# Включение службы Windows

## Описание

Включает службу, имя которой было передано. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ service: string - Имя службы, которую надо включить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_service: bool - Возвращает статус выполенения.  
 turn\_on\_service\_info: string - Подробная информация о включении службы.  
}

# Выключение машины Windows

## Описание

Завершает работу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении. \_\_\_ ## Input: { ❗ ip\_address or *hostname*: string - Адрес целевой машины. sd\_time: int - Время до выключения машины (по умолчанию 60 секунд). message: string - Сообщение, которое увидят пользователи (по умолчанию "Ваш компьютер будет выключен через {sd\_time} секунд(-у, -ы). Сохраните открытые файлы."). }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 win\_shutdown: bool - Возвращает статус выполенения.  
 win\_shutdown\_info: string - Подробная информация о выключении машины.  
}

# Отключение USB-носителей Windows

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее: - будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов; - ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено). \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_info: string - Подробная информация о включении usb.  
}

# Блокировка доменного пользователя

## Описание:

Отключает учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка локального пользователя Windows

## Описание:

Отключает учётную запись пользователя.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка пользователя Linux

## Описание

Блокирует указанного пользователя на указанном хосте. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Принудительное завершение процесса Linux

## Описание

Команда kill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ process\_name: string - Имя процесса, который нужно отключить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о завершении процесса.  
}

# Завершить все RDP соединения на сервере Win.

## Описание

Отключает все RDP сессии на сервере. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_rdp\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_rdp\_sessions\_info: string - Подробная информация об отключении активных RDP сессий.  
}

# Завершить сеансы всех пользователей Windows

## Описание

Завершает ВСЕ активные сессии на указанной машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_sessions\_info: string - Подробная информация об отключении.  
}

# Включение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_write\_info: string - Подробная информация о включении запрета записи usb.  
}

# Изменение политики паролей в домене AD

## Описание:

Скрипт изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!!

Условные обозначения для формата:

D = Дни (от 0 до 10675199)

H = Часы (от 0 до 23)

M = Минуты (от 0 до 59)

S = Секунды (от 0 до 59)

F = Доли секунды (от 0 до 9999999)

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес машины, на которой будет выполняться скрипт (лучше всего подойдёт контроллер домена).  
 ❗ ComplexityEnabled: bool - Указывает, включена ли сложность пароля для политики паролей.  
 ❗ LockoutDuration: string - Требуемый формат: "D.H:M:S.F". Указывает период времени, в течение которого учетная запись блокируется после того, как количество неудачных попыток входа в систему превышает порог блокировки. Вы не можете войти в заблокированную учетную запись, пока не истечет период времени блокировки. Этот параметр задает свойство lockoutDuration объекта политики паролей.  
 ❗ LockoutObservationWindow: string - Требуемый формат: "D:H:M:S.F". Указывает максимальный интервал времени между двумя неудачными попытками входа в систему, по истечении которого количество неудачных попыток входа сбрасывается до 0. Учетная запись блокируется, когда количество неудачных попыток входа превышает порог блокировки политики паролей. Этот параметр задает свойство lockoutObservationWindow объекта политики паролей  
 ❗ LockoutThreshold: int - Указывает допустимое количество неудачных попыток входа, прежде чем учетная запись будет заблокирована. Это число увеличивается, когда время между неудачными попытками входа в систему меньше, чем время, указанное для окна времени наблюдения за блокировкой. Этот параметр задает свойство LockoutThreshold политики паролей.  
 ❗ MaxPasswordAge: string - Требуемый формат: "D.H:M:S.F". Определяет максимальное время, в течение которого вы можете иметь один и тот же пароль. По истечении этого периода срок действия пароля истекает, и вы должны создать новый.  
 ❗ MinPasswordAge: string - Требуемый формат: "D.H:M:S.F". Указывает минимальное время, по истечении которого вы сможете изменить пароль.  
 ❗ MinPasswordLength: int - Указывает минимальное количество символов, которое должен содержать пароль. Этот параметр задает свойство MinPasswordLength политики паролей.  
 ❗ PasswordHistoryCount: int [Указывает количество предыдущих паролей для сохранения. Пользователь не может повторно использовать пароль из списка сохраненных паролей. Этот параметр задает свойство PasswordHistoryCount для политики паролей.  
 ❗ ReversibleEncryptionEnabled: bool - Указывает, должен ли каталог хранить пароли с использованием обратимого шифрования. Этот параметр задает свойство ReversibleEncryption для политики паролей.  
 ❗ identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 change\_password\_policy: bool - Возвращает статус выполенения.  
 change\_password\_policy\_info: string - Подробная информация о изменении парольной политики.  
}

# Получение имени УЗ по SID

## Описание:

Возвращает имя учётной записи по её SID.

## Input:

{  
 ❗ sid: string - SID пользователя, имя УЗ которого надо узнать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_account: bool - Возвращает статус выполенения.  
 get\_account\_info: string - Имя учётной записи пользователя, в случае успеха, или сообщение об ошибке.  
}

# Получение списка интерфейсов и информации о них

## Описание:

Скрипт подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_settings: bool - Возвращает статус выполенения.  
 linux\_settings\_info: list -> string | string - Массив строк, которые содержат название инфтерфейсов и информацию о них, в случае успеха или строка, информация об ошибке.  
}

# Обновление пакетов

## Описание:

Обновляет установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper. Local версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления) Remote версия обновляет на удаленной linux машине. \_\_\_ Local-версия ## Input: {

}

## Secrets:

{  
  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

Remote-версия ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

# Определяет местоположение по ip

## Описание:

Первая версия использует библиотеку ipwhois. Вторая использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).

ipwhois-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

ipinfo-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
 ❗ ipinfo\_token: string - Токен, предоставляемый сервисом.  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение ssh соодинений

## Описание:

Скрипт производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_ssh: bool - Возвращает статус выполенения.  
 turn\_off\_ssh\_info: string - Подробная информация об отключении ssh соединений.  
}

# Отключение активных сессий Liunx

## Описание:

Отключает все активные сессии. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_session: bool - Возвращает статус выполенения.  
 turn\_off\_session\_info: string - Подробная информация об отключенных пользователях.  
}

# Отклюлчение всех сетевых интерфейсов

# Описание:

Отключает все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 disabled: bool - Возвращает статус выполенения.  
 disabled\_info: string - Подробная информация об отключенных интерфейсах.  
}

# Отключение службы Win

## Описание:

Отключает указанный сервис.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ service\_name: string - Имя сервиса, который необходимо отключить.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_service\_result: bool - Возвращает статус выполенения.  
 disable\_service\_result\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение узла Linux

## Описание:

Отключает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. time\_out: int - Время, через которое компьютер выключится. message: string - Сообщение, которое будет выводиться пользователям. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_node: bool - Возвращает статус выполенения.  
 turn\_off\_node\_info: string - Подробная информация о выключении компьютера.  
}

# Включение запрета на cd dvd

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_cddvd: bool - Возвращает статус выполенения.  
 turn\_off\_cddvd\_info: string - Подробная информация о включении запрета записи cd dvd.  
}

# Отключает все сетевые интерфейсы

## Описание:

Отключает сетевые интерфейсы. После отключения невозможно удаленно зайти на машину. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_net\_int\_win: bool - Возвращает статус выполенения.  
 disable\_net\_int\_win\_info: string - Подробная информация об отключении интерфейсов.  
}

# Отправить сообщение авторизованным по ssh пользователям Linux

## Описание:

При использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер. Невозможно достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 send\_message: bool - Возвращает статус выполенения.  
 send\_message\_info: string - Подробная информация об отправленном сообщении.  
}

# Отправить сообщение пользователю Win

## Описание:

Отправляет сообщение на указанный хост.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 message\_result: bool - Возвращает статус выполенения.  
 message\_result\_info: string - Подробная информация об отправленном сообщении.  
}

# Перезагрузить компьютер Windows

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 message: string - Сообщение, отображаемое пользователям.  
 timeout: string - Время до перезагрузки.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reboot\_win: bool - Возвращает статус выполенения.  
 reboot\_win\_info: string - Подробная информация о перезагрузке.  
}

# Перезагрузка узла Linux

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. message: string - Сообщение, отображаемое пользователям. timeout: int - Время до перезагрузки. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 reboot\_node: bool - Возвращает статус выполенения.  
 reboot\_node\_info: string - Подробная информация о блокировке пользователя.  
}

# Получение времени и даты

## Описание:

Возвращает текущее время на Linux-машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_time: bool - Возвращает статус выполенения.  
 linux\_time\_info: string - Подробная информация о времени на устройстве.  
}

# Получение политики паролей в домене AD

## Описание:

Скрипт возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_password\_policy: bool - Возвращает статус выполенения.  
 get\_password\_policy\_info: list - Массив, содержащий политики и их значения.  
 get\_password\_policy\_info.[].name: string - Название политики.  
 get\_password\_policy\_info.[].value: string - Установленное значение политики.  
}

# Получить список запущенных процессов

## Описание:

Позволяет получить список процессов, запущенных на машине и их pid-ы. get\_win\_proc - получает информацию из виндовых машин get\_linux\_proс - пполучает информацию из линуксовой машин

Windows-версия

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

Linux-версия \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

# Завершить процесс Windows

## Описание:

Завершает процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗ \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. user: string - Имя учётной записи пользователя, процессы которого нуобходимо завершить. process: string or int - Имя процесса или его pid. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о блокировке пользователя.  
}

# Проверить целостность системных файлов Windows

## Описание:

Выполняет сканирование системных файлов, результат выводится строкой. Может занять очень много времени.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 check\_win: bool - Возвращает статус выполенения.  
 check\_win\_info: string - Подробная информация о результатах сканирования.  
}

# Проверка в Virus Total

## Описание:

Проверяет заданный url или ip адрес в Virus Total.

## Input:

{  
 ❗ ip: string - ip или url, который неоьбходимо проверить.  
}

## Secrets:

{  
 ❗ vt\_api\_key: string - Api-key для сервиса Virus Total.  
}

## Output:

{  
 result: string - Возвращает строку, содержащую результат проверки.  
}

# Проверка доступности хоста утилитой ping

## Описание:

Работает как на linux, так и на windows Отсылает только один пакет Доступность проверяется с того же хоста, где установлен SOAR \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
   
}

## Output:

{  
 ping: bool - Возвращает статус выполенения.  
 ping\_info: string - Подробная информация о доступности хоста.  
}

# Отключение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_write\_info: string - Подробная информация о выполнении операции.  
}

# Сброс пароля локального пользователя

## Описание:

Сбрасывает (устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https. \_\_\_

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, ккоторому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля пользователя.  
}

# Сброс пароля доменного пользователя

## Описание:

Сбрасывает пароль выбранного пользователя (устанавливает смену пароля при следующем логине).

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля.  
}

# Получение списка подключенных USB устройств

## Описание:

Возвращает список всех usb-устройств, подключенных к компьютеру в данный момент \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_usb: bool - Возвращает статус выполенения.  
 connected\_usb\_info: list -> string - Массив, содержащий названия usb-устройств.  
}

# Получение списка подключенных пользователей

## Описание:

Возвращает список всех подключенных пользователей, а также информацию о них.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_users: bool - Возвращает статус выполенения.  
 connected\_users\_info: list -> string - Подробная информация о подключенных пользователях.  
}

# Список контроля доступа

## Описание:

Скрипт возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке и её подпапкам.  
}

# Список контроля доступа

## Описание

Скрипт возвращает список контроля доступа (ACL) для папки узла Windows. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\" или "/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке.  
}

# Получение списка правил Iptables

## Описание:

Скрипт возвращает правила из Iptables

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list - Массив, содержащий правила из Iptables или информация об ошибке.  
 firewall\_rules\_info.[].chain\_name: string - Название цепочки.  
 firewall\_rules\_info.[].values: list - Массив, содержащий информацию о правилах.  
 firewall\_rules\_info.[].values.[].target: string - Eсли пакет отвечает правилу, заголовок target указывает, что с ним нужно сделать.  
 firewall\_rules\_info.[].values.[].prot: string - Протокол  
 firewall\_rules\_info.[].values.[].opt: string - Данный параметр используется редко и отображает опции IP  
 firewall\_rules\_info.[].values.[].source: string - Исходный IP-адрес или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].destination: string - IP-адрес назначения или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].info: string - Любая часть правила, которая не указана предыдущими столбцами  
}

# Список правил Windows Firewall

## Описание:

Скрипт возвращает список всех правил Windows Firewall.

**Работает только с >= win 10!** \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list -> string - Список всех правил на Firewall.  
}

# Список открытых сессий

## Описание:

Скрипт возвращает все активные активные сессии.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 active\_sessions: bool - Возвращает статус выполенения.  
 active\_sessions\_info: list - Подробная информация об установленных подключениях.  
 active\_sessions\_info.[].username: string - Имя пользователя  
 active\_sessions\_info.[].sessionname: string - Имя сессии  
 active\_sessions\_info.[].id: string - id сессии  
 active\_sessions\_info.[].state: string - Состояние сессии  
 active\_sessions\_info.[].idle\_time: string - Время простоя  
 active\_sessions\_info.[].logon\_time: string - Время входа  
}

# Список установленных сетевых соединений

## Описание:

Скрипт возвращает все активные соединения хоста в виде списка. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 estabilish\_conn\_result: bool - Возвращает статус выполенения.  
 estabilish\_conn\_result\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilish\_conn\_result\_info.[].RemoteAddress: string - Удаленный адрес  
 estabilish\_conn\_result\_info.[].LocalAddress: string - Локальный адерес  
}

# Получение списка установленных соединений

## Описание:

Возвращает массив установленных хостом подключений. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 estabilished\_connetctions: bool - Возвращает статус выполенения.  
 estabilished\_connetctions\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilished\_connetctions\_info.[].local\_address: string - Локальный адерес  
 estabilished\_connetctions\_info.[].foreign\_address: string - Удаленный адрес  
}

# Удаление из локальной группы

## Описание:

Удаляет пользователя из указанной локальной группы. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя учётной записи пользователя, которого необходимо удалить из группы. ❗ group: string - Имя группы, из которой необходимо удалить пользователя. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 del\_user\_from\_group\_result: bool - Возвращает статус выполенения.  
 del\_user\_from\_group\_result\_info: string - Подробная информация об удалении пользователя из группы.  
}

# Удаление папки и её содержимого

## Описание:

Удаляет переданную папку и всё её содержимое. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь до папки, которую необходимо удалить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Удаляет папку win

## Описание:

Производит удаление папки

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Полный путь до папки. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

['# Безопасное затирание удаленных файлов## Описание:производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени.***## Input:## Secrets:## Output:', '# Включение (отключение) автозагрузки на всех устройствах Windows## Описание:disable\_autorun отключает автозапуск вообще всех дисков.enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию).настроенная служба winrm https. и выходы актуальны для обоих скриптов***## Input:## Secrets:## Output:', '# Включение USB-носителей win## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится.***## Input:## Secrets:## Output:', '# Включение автообновления win## Описаниепроизводит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки.***## Input:## Secrets:## Output:', '# Включение брандмауэра## Описаниебрандмауэр.***## Input:## Secrets:## Output:', '# Включение службы Windows## Описаниеслужбу, имя которой было передано.***## Input:## Secrets:## Output:', '# Выключение машины Windows## Описаниеработу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении.***## Input:## Secrets:## Output:', '# Отключение USB-носителей Windows## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее:- будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов;- ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено).***## Input:## Secrets:## Output:', '# Блокировка доменного пользователя## Описание:учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.***## Input:## Secrets:## Output:', '# Блокировка локального пользователя Windows## Описание:учётную запись пользователя.***## Input:## Secrets:## Output:', '# Блокировка пользователя Linux## Описаниеуказанного пользователя на указанном хосте.***## Input:## Secrets:## Output:', '# Принудительное завершение процесса Linux## Описаниеkill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным.***## Input:## Secrets:## Output:', '# Завершить все RDP соединения на сервере Win.## Описаниевсе RDP сессии на сервере.***## Input:## Secrets:## Output:', '# Завершить сеансы всех пользователей Windows## ОписаниеВСЕ активные сессии на указанной машине.***## Input:## Secrets:## Output:', '# Включение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется.***## Input:## Secrets:## Output:', '# Изменение политики паролей в домене AD## Описание:изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!! обозначения для формата:= Дни (от 0 до 10675199)= Часы (от 0 до 23)= Минуты (от 0 до 59)= Секунды (от 0 до 59)= Доли секунды (от 0 до 9999999)модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:', '# Получение имени УЗ по SID## Описание:имя учётной записи по её SID.***## Input:## Secrets:## Output:', '# Получение списка интерфейсов и информации о них## Описание:подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools.***## Input:## Secrets:## Output:', '# Обновление пакетов## Описание:установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper.версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления)версия обновляет на удаленной linux машине.***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:', '# Определяет местоположение по ip## Описание:версия использует библиотеку ipwhois.использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:', '# Отключение ssh соодинений## Описание:производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.***## Input:## Secrets:## Output:', '# Отключение активных сессий Liunx## Описание:все активные сессии.***## Input:## Secrets:## Output:', '# Отклюлчение всех сетевых интерфейсов# Описание:все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗***## Input:## Secrets:## Output:', '# Отключение службы Win## Описание:указанный сервис.***## Input:## Secrets:## Output:', '# Отключение узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:', '# Включение запрета на cd dvd## Описание:производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.***## Input:## Secrets:## Output:', '# Отключает все сетевые интерфейсы## Описание:сетевые интерфейсы. После отключения невозможно удаленно зайти на машину.***## Input:## Secrets:## Output:', '# Отправить сообщение авторизованным по ssh пользователям Linux## Описание:использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер.достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.***## Input:## Secrets:## Output:', '# Отправить сообщение пользователю Win## Описание:сообщение на указанный хост.***## Input:## Secrets:## Output:', '# Перезагрузить компьютер Windows## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:', '# Перезагрузка узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:', '# Получение времени и даты## Описание:текущее время на Linux-машине.***## Input:## Secrets:## Output:', '# Получение политики паролей в домене AD## Описание:возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:', '# Получить список запущенных процессов## Описание:получить список процессов, запущенных на машине и их pid-ы.win\_proc - получает информацию из виндовых машин linux\_proс - пполучает информацию из линуксовой машин -версия## Input:## Secrets:## Output:***-версия***## Input:## Secrets:## Output:', '# Завершить процесс Windows## Описание:процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗***## Input:## Secrets:## Output:', '# Проверить целостность системных файлов Windows## Описание:сканирование системных файлов, результат выводится строкой. занять очень много времени.***## Input:## Secrets:## Output:', '# Проверка в Virus Total## Описание:заданный url или ip адрес в Virus Total.***## Input:## Secrets:## Output:', '# Проверка доступности хоста утилитой ping## Описание:как на linux, так и на windows только один пакет проверяется с того же хоста, где установлен SOAR***## Input:## Secrets:## Output:', '# Отключение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется.***## Input:## Secrets:## Output:', '# Сброс пароля локального пользователя## Описание:(устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https. ***## Input:## Secrets:## Output:', '# Сброс пароля доменного пользователя## Описание:пароль выбранного пользователя (устанавливает смену пароля при следующем логине).***## Input:## Secrets:## Output:', '# Получение списка подключенных USB устройств## Описание:список всех usb-устройств, подключенных к компьютеру в данный момент***## Input:## Secrets:## Output:', '# Получение списка подключенных пользователей## Описание:список всех подключенных пользователей, а также информацию о них.***## Input:## Secrets:## Output:', '# Список контроля доступа## Описание:возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.***## Input:## Secrets:## Output:', '# Список контроля доступа## Описаниевозвращает список контроля доступа (ACL) для папки узла Windows.***## Input:## Secrets:## Output:', '# Получение списка правил Iptables## Описание:возвращает правила из Iptables\_\_\_## Input:## Secrets:## Output:', '# Список правил Windows Firewall## Описание:возвращает список всех правил Windows Firewall.\*Работает только с >= win 10!\*\****## Input:## Secrets:## Output:', '# Список открытых сессий## Описание:возвращает все активные активные сессии.***## Input:## Secrets:## Output:', '# Список установленных сетевых соединений## Описание:возвращает все активные соединения хоста в виде списка. ***## Input:## Secrets:## Output:', '# Получение списка установленных соединений## Описание:массив установленных хостом подключений.***## Input:## Secrets:## Output:', '# Удаление из локальной группы## Описание:пользователя из указанной локальной группы.***## Input:## Secrets:## Output:', '# Удаление папки и её содержимого## Описание:переданную папку и всё её содержимое.***## Input:## Secrets:## Output:', '# Удаляет папку win## Описание:удаление папки***## Input:## Secrets:## Output:', '# Безопасное затирание удаленных файлов## Описание:производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени.***## Input:## Secrets:## Output:# Включение (отключение) автозагрузки на всех устройствах Windows## Описание:disable\_autorun отключает автозапуск вообще всех дисков.enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию).настроенная служба winrm https. и выходы актуальны для обоих скриптов***## Input:## Secrets:## Output:# Включение USB-носителей win## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится.***## Input:## Secrets:## Output:# Включение автообновления win## Описаниепроизводит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки.***## Input:## Secrets:## Output:# Включение брандмауэра## Описаниебрандмауэр.***## Input:## Secrets:## Output:# Включение службы Windows## Описаниеслужбу, имя которой было передано.***## Input:## Secrets:## Output:# Выключение машины Windows## Описаниеработу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении.***## Input:## Secrets:## Output:# Отключение USB-носителей Windows## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее:- будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов;- ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено).***## Input:## Secrets:## Output:# Блокировка доменного пользователя## Описание:учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.***## Input:## Secrets:## Output:# Блокировка локального пользователя Windows## Описание:учётную запись пользователя.***## Input:## Secrets:## Output:# Блокировка пользователя Linux## Описаниеуказанного пользователя на указанном хосте.***## Input:## Secrets:## Output:# Принудительное завершение процесса Linux## Описаниеkill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным.***## Input:## Secrets:## Output:# Завершить все RDP соединения на сервере Win.## Описаниевсе RDP сессии на сервере.***## Input:## Secrets:## Output:# Завершить сеансы всех пользователей Windows## ОписаниеВСЕ активные сессии на указанной машине.***## Input:## Secrets:## Output:# Включение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется.***## Input:## Secrets:## Output:# Изменение политики паролей в домене AD## Описание:изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!! обозначения для формата:= Дни (от 0 до 10675199)= Часы (от 0 до 23)= Минуты (от 0 до 59)= Секунды (от 0 до 59)= Доли секунды (от 0 до 9999999)модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получение имени УЗ по SID## Описание:имя учётной записи по её SID.***## Input:## Secrets:## Output:# Получение списка интерфейсов и информации о них## Описание:подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools.***## Input:## Secrets:## Output:# Обновление пакетов## Описание:установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper.версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления)версия обновляет на удаленной linux машине.***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Определяет местоположение по ip## Описание:версия использует библиотеку ipwhois.использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Отключение ssh соодинений## Описание:производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.***## Input:## Secrets:## Output:# Отключение активных сессий Liunx## Описание:все активные сессии.***## Input:## Secrets:## Output:# Отклюлчение всех сетевых интерфейсов# Описание:все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗***## Input:## Secrets:## Output:# Отключение службы Win## Описание:указанный сервис.***## Input:## Secrets:## Output:# Отключение узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Включение запрета на cd dvd## Описание:производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.***## Input:## Secrets:## Output:# Отключает все сетевые интерфейсы## Описание:сетевые интерфейсы. После отключения невозможно удаленно зайти на машину.***## Input:## Secrets:## Output:# Отправить сообщение авторизованным по ssh пользователям Linux## Описание:использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер.достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.***## Input:## Secrets:## Output:# Отправить сообщение пользователю Win## Описание:сообщение на указанный хост.***## Input:## Secrets:## Output:# Перезагрузить компьютер Windows## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Перезагрузка узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Получение времени и даты## Описание:текущее время на Linux-машине.***## Input:## Secrets:## Output:# Получение политики паролей в домене AD## Описание:возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получить список запущенных процессов## Описание:получить список процессов, запущенных на машине и их pid-ы.*win\_proc - получает информацию из виндовых машин linux\_proс - пполучает информацию из линуксовой машин* ***-версия***## Input:## Secrets:## Output:***-версия***## Input:## Secrets:## Output:# Завершить процесс Windows## Описание:процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗***## Input:## Secrets:## Output:# Проверить целостность системных файлов Windows## Описание:сканирование системных файлов, результат выводится строкой. занять очень много времени.***## Input:## Secrets:## Output:# Проверка в Virus Total## Описание:заданный url или ip адрес в Virus Total.***## Input:## Secrets:## Output:# Проверка доступности хоста утилитой ping## Описание:как на linux, так и на windows только один пакет проверяется с того же хоста, где установлен SOAR***## Input:## Secrets:## Output:# Отключение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется.***## Input:## Secrets:## Output:# Сброс пароля локального пользователя## Описание:(устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https.*** ## Input:## Secrets:## Output:# Сброс пароля доменного пользователя## Описание:пароль выбранного пользователя (устанавливает смену пароля при следующем логине).***## Input:## Secrets:## Output:# Получение списка подключенных USB устройств## Описание:список всех usb-устройств, подключенных к компьютеру в данный момент***## Input:## Secrets:## Output:# Получение списка подключенных пользователей## Описание:список всех подключенных пользователей, а также информацию о них.***## Input:## Secrets:## Output:# Список контроля доступа## Описание:возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.***## Input:## Secrets:## Output:# Список контроля доступа## Описаниевозвращает список контроля доступа (ACL) для папки узла Windows.***## Input:## Secrets:## Output:# Получение списка правил Iptables## Описание:возвращает правила из Iptables***## Input:## Secrets:## Output:# Список правил Windows Firewall## Описание:возвращает список всех правил Windows Firewall.\*Работает только с >= win 10!\*\****## Input:## Secrets:## Output:# Список открытых сессий## Описание:возвращает все активные активные сессии.***## Input:## Secrets:## Output:# Список установленных сетевых соединений## Описание:возвращает все активные соединения хоста в виде списка. ***## Input:## Secrets:## Output:# Получение списка установленных соединений## Описание:массив установленных хостом подключений.***## Input:## Secrets:## Output:# Удаление из локальной группы## Описание:пользователя из указанной локальной группы.***## Input:## Secrets:## Output:# Удаление папки и её содержимого## Описание:переданную папку и всё её содержимое.***## Input:## Secrets:## Output:# Удаляет папку win## Описание:удаление папки***## Input:## Secrets:## Output:# Безопасное затирание удаленных файлов## Описание:производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени.***## Input:## Secrets:## Output:# Включение (отключение) автозагрузки на всех устройствах Windows## Описание:disable\_autorun отключает автозапуск вообще всех дисков.enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию).настроенная служба winrm https. и выходы актуальны для обоих скриптов***## Input:## Secrets:## Output:# Включение USB-носителей win## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится.***## Input:## Secrets:## Output:# Включение автообновления win## Описаниепроизводит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки.***## Input:## Secrets:## Output:# Включение брандмауэра## Описаниебрандмауэр.***## Input:## Secrets:## Output:# Включение службы Windows## Описаниеслужбу, имя которой было передано.***## Input:## Secrets:## Output:# Выключение машины Windows## Описаниеработу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении.***## Input:## Secrets:## Output:# Отключение USB-носителей Windows## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее:- будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов;- ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено).***## Input:## Secrets:## Output:# Блокировка доменного пользователя## Описание:учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.***## Input:## Secrets:## Output:# Блокировка локального пользователя Windows## Описание:учётную запись пользователя.***## Input:## Secrets:## Output:# Блокировка пользователя Linux## Описаниеуказанного пользователя на указанном хосте.***## Input:## Secrets:## Output:# Принудительное завершение процесса Linux## Описаниеkill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным.***## Input:## Secrets:## Output:# Завершить все RDP соединения на сервере Win.## Описаниевсе RDP сессии на сервере.***## Input:## Secrets:## Output:# Завершить сеансы всех пользователей Windows## ОписаниеВСЕ активные сессии на указанной машине.***## Input:## Secrets:## Output:# Включение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется.***## Input:## Secrets:## Output:# Изменение политики паролей в домене AD## Описание:изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!! обозначения для формата:= Дни (от 0 до 10675199)= Часы (от 0 до 23)= Минуты (от 0 до 59)= Секунды (от 0 до 59)= Доли секунды (от 0 до 9999999)модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получение имени УЗ по SID## Описание:имя учётной записи по её SID.***## Input:## Secrets:## Output:# Получение списка интерфейсов и информации о них## Описание:подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools.***## Input:## Secrets:## Output:# Обновление пакетов## Описание:установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper.версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления)версия обновляет на удаленной linux машине.***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Определяет местоположение по ip## Описание:версия использует библиотеку ipwhois.использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Отключение ssh соодинений## Описание:производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.***## Input:## Secrets:## Output:# Отключение активных сессий Liunx## Описание:все активные сессии.***## Input:## Secrets:## Output:# Отклюлчение всех сетевых интерфейсов# Описание:все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗***## Input:## Secrets:## Output:# Отключение службы Win## Описание:указанный сервис.***## Input:## Secrets:## Output:# Отключение узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Включение запрета на cd dvd## Описание:производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.***## Input:## Secrets:## Output:# Отключает все сетевые интерфейсы## Описание:сетевые интерфейсы. После отключения невозможно удаленно зайти на машину.***## Input:## Secrets:## Output:# Отправить сообщение авторизованным по ssh пользователям Linux## Описание:использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер.достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.***## Input:## Secrets:## Output:# Отправить сообщение пользователю Win## Описание:сообщение на указанный хост.***## Input:## Secrets:## Output:# Перезагрузить компьютер Windows## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Перезагрузка узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Получение времени и даты## Описание:текущее время на Linux-машине.***## Input:## Secrets:## Output:# Получение политики паролей в домене AD## Описание:возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получить список запущенных процессов## Описание:получить список процессов, запущенных на машине и их pid-ы.*win\_proc - получает информацию из виндовых машин linux\_proс - пполучает информацию из линуксовой машин* ***-версия***## Input:## Secrets:## Output:***-версия***## Input:## Secrets:## Output:# Завершить процесс Windows## Описание:процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗***## Input:## Secrets:## Output:# Проверить целостность системных файлов Windows## Описание:сканирование системных файлов, результат выводится строкой. занять очень много времени.***## Input:## Secrets:## Output:# Проверка в Virus Total## Описание:заданный url или ip адрес в Virus Total.***## Input:## Secrets:## Output:# Проверка доступности хоста утилитой ping## Описание:как на linux, так и на windows только один пакет проверяется с того же хоста, где установлен SOAR***## Input:## Secrets:## Output:# Отключение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется.***## Input:## Secrets:## Output:# Сброс пароля локального пользователя## Описание:(устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https.*** ## Input:## Secrets:## Output:# Сброс пароля доменного пользователя## Описание:пароль выбранного пользователя (устанавливает смену пароля при следующем логине).***## Input:## Secrets:## Output:# Получение списка подключенных USB устройств## Описание:список всех usb-устройств, подключенных к компьютеру в данный момент***## Input:## Secrets:## Output:# Получение списка подключенных пользователей## Описание:список всех подключенных пользователей, а также информацию о них.***## Input:## Secrets:## Output:# Список контроля доступа## Описание:возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.***## Input:## Secrets:## Output:# Список контроля доступа## Описаниевозвращает список контроля доступа (ACL) для папки узла Windows.***## Input:## Secrets:## Output:# Получение списка правил Iptables## Описание:возвращает правила из Iptables***## Input:## Secrets:## Output:# Список правил Windows Firewall## Описание:возвращает список всех правил Windows Firewall.\*Работает только с >= win 10!\*\****## Input:## Secrets:## Output:# Список открытых сессий## Описание:возвращает все активные активные сессии.***## Input:## Secrets:## Output:# Список установленных сетевых соединений## Описание:возвращает все активные соединения хоста в виде списка. ***## Input:## Secrets:## Output:# Получение списка установленных соединений## Описание:массив установленных хостом подключений.***## Input:## Secrets:## Output:# Удаление из локальной группы## Описание:пользователя из указанной локальной группы.***## Input:## Secrets:## Output:# Удаление папки и её содержимого## Описание:переданную папку и всё её содержимое.***## Input:## Secrets:## Output:# Удаляет папку win## Описание:удаление папки***## Input:## Secrets:## Output:# Безопасное затирание удаленных файлов## Описание:производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени.***## Input:## Secrets:## Output:# Включение (отключение) автозагрузки на всех устройствах Windows## Описание:disable\_autorun отключает автозапуск вообще всех дисков.enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию).настроенная служба winrm https. и выходы актуальны для обоих скриптов***## Input:## Secrets:## Output:# Включение USB-носителей win## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится.***## Input:## Secrets:## Output:# Включение автообновления win## Описаниепроизводит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки.***## Input:## Secrets:## Output:# Включение брандмауэра## Описаниебрандмауэр.***## Input:## Secrets:## Output:# Включение службы Windows## Описаниеслужбу, имя которой было передано.***## Input:## Secrets:## Output:# Выключение машины Windows## Описаниеработу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении.***## Input:## Secrets:## Output:# Отключение USB-носителей Windows## Описаниепроизводит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее:- будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов;- ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено).***## Input:## Secrets:## Output:# Блокировка доменного пользователя## Описание:учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.***## Input:## Secrets:## Output:# Блокировка локального пользователя Windows## Описание:учётную запись пользователя.***## Input:## Secrets:## Output:# Блокировка пользователя Linux## Описаниеуказанного пользователя на указанном хосте.***## Input:## Secrets:## Output:# Принудительное завершение процесса Linux## Описаниеkill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным.***## Input:## Secrets:## Output:# Завершить все RDP соединения на сервере Win.## Описаниевсе RDP сессии на сервере.***## Input:## Secrets:## Output:# Завершить сеансы всех пользователей Windows## ОписаниеВСЕ активные сессии на указанной машине.***## Input:## Secrets:## Output:# Включение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется.***## Input:## Secrets:## Output:# Изменение политики паролей в домене AD## Описание:изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!! обозначения для формата:= Дни (от 0 до 10675199)= Часы (от 0 до 23)= Минуты (от 0 до 59)= Секунды (от 0 до 59)= Доли секунды (от 0 до 9999999)модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получение имени УЗ по SID## Описание:имя учётной записи по её SID.***## Input:## Secrets:## Output:# Получение списка интерфейсов и информации о них## Описание:подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools.***## Input:## Secrets:## Output:# Обновление пакетов## Описание:установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper.версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления)версия обновляет на удаленной linux машине.***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Определяет местоположение по ip## Описание:версия использует библиотеку ipwhois.использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).***-версия## Input:## Secrets:## Output:***-версия## Input:## Secrets:## Output:# Отключение ssh соодинений## Описание:производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.***## Input:## Secrets:## Output:# Отключение активных сессий Liunx## Описание:все активные сессии.***## Input:## Secrets:## Output:# Отклюлчение всех сетевых интерфейсов# Описание:все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗***## Input:## Secrets:## Output:# Отключение службы Win## Описание:указанный сервис.***## Input:## Secrets:## Output:# Отключение узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Включение запрета на cd dvd## Описание:производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.***## Input:## Secrets:## Output:# Отключает все сетевые интерфейсы## Описание:сетевые интерфейсы. После отключения невозможно удаленно зайти на машину.***## Input:## Secrets:## Output:# Отправить сообщение авторизованным по ssh пользователям Linux## Описание:использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер.достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.***## Input:## Secrets:## Output:# Отправить сообщение пользователю Win## Описание:сообщение на указанный хост.***## Input:## Secrets:## Output:# Перезагрузить компьютер Windows## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Перезагрузка узла Linux## Описание:компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".***## Input:## Secrets:## Output:# Получение времени и даты## Описание:текущее время на Linux-машине.***## Input:## Secrets:## Output:# Получение политики паролей в домене AD## Описание:возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.***## Input:## Secrets:## Output:# Получить список запущенных процессов## Описание:получить список процессов, запущенных на машине и их pid-ы.*win\_proc - получает информацию из виндовых машин linux\_proс - пполучает информацию из линуксовой машин* ***-версия***## Input:## Secrets:## Output:***-версия***## Input:## Secrets:## Output:# Завершить процесс Windows## Описание:процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗***## Input:## Secrets:## Output:# Проверить целостность системных файлов Windows## Описание:сканирование системных файлов, результат выводится строкой. занять очень много времени.***## Input:## Secrets:## Output:# Проверка в Virus Total## Описание:заданный url или ip адрес в Virus Total.***## Input:## Secrets:## Output:# Проверка доступности хоста утилитой ping## Описание:как на linux, так и на windows только один пакет проверяется с того же хоста, где установлен SOAR***## Input:## Secrets:## Output:# Отключение запрета записи на USB## Описание:производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется.***## Input:## Secrets:## Output:# Сброс пароля локального пользователя## Описание:(устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https.*** ## Input:## Secrets:## Output:# Сброс пароля доменного пользователя## Описание:пароль выбранного пользователя (устанавливает смену пароля при следующем логине).***## Input:## Secrets:## Output:# Получение списка подключенных USB устройств## Описание:список всех usb-устройств, подключенных к компьютеру в данный момент***## Input:## Secrets:## Output:# Получение списка подключенных пользователей## Описание:список всех подключенных пользователей, а также информацию о них.***## Input:## Secrets:## Output:# Список контроля доступа## Описание:возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.***## Input:## Secrets:## Output:# Список контроля доступа## Описаниевозвращает список контроля доступа (ACL) для папки узла Windows.***## Input:## Secrets:## Output:# Получение списка правил Iptables## Описание:возвращает правила из Iptables***## Input:## Secrets:## Output:# Список правил Windows Firewall## Описание:возвращает список всех правил Windows Firewall.\*Работает только с >= win 10!\*\****## Input:## Secrets:## Output:# Список открытых сессий## Описание:возвращает все активные активные сессии.***## Input:## Secrets:## Output:# Список установленных сетевых соединений## Описание:возвращает все активные соединения хоста в виде списка. ***## Input:## Secrets:## Output:# Получение списка установленных соединений## Описание:массив установленных хостом подключений.***## Input:## Secrets:## Output:# Удаление из локальной группы## Описание:пользователя из указанной локальной группы.***## Input:## Secrets:## Output:# Удаление папки и её содержимого## Описание:переданную папку и всё её содержимое.***## Input:## Secrets:## Output:# Удаляет папку win## Описание:удаление папки***## Input:## Secrets:## Output:# Удаление файла## Описание:файл, путь до которого передаётся.***## Input:## Secrets:## Output:# Удаление файла## Описание:файл, путь до которого передаётся.***## Input:## Secrets:## Output:# Удаление файла## Описание:файл, путь до которого передаётся.***## Input:## Secrets:## Output:', '# Удаление файла## Описание:файл, путь до которого передаётся.\_\_\_## Input:## Secrets:## Output:']

# Удаление файла

## Описание:

Удаляет файл, путь до которого передаётся. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Полный путь до удаляемого файла. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_file: bool - Возвращает статус выполенения.  
 remove\_file\_info: string - Подробная информация об удалении файла.  
}

# Безопасное затирание удаленных файлов

## Описание:

Команда производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. path: string - Путь до папки, которую необходимо затереть. Путь должен разделяться "\" или "/". Если переменная не указана явно, то принимает значение "C:/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 cipher\_folder: bool - Возвращает статус выполенения.  
 cipher\_folder\_info: string - Подробная информация о затирании информации.  
}

# Включение (отключение) автозагрузки на всех устройствах Windows

## Описание:

Скрипт disable\_autorun отключает автозапуск вообще всех дисков. Скрипт enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию). Требуется настроенная служба winrm https. Входы и выходы актуальны для обоих скриптов \_\_\_ ## Input: { ❗ ip\_address or hostname : string - Адрес целевой машины }

## Secrets:

{  
 ❗ login : string - Имя пользователя, под которым заходим на машину  
 ❗ password : string - Пароль от пользователя  
 ❗ domain : string - Домен, в котором расположена машина  
}

## Output:

{  
 red\_edit\_result : bool - Возвращает статус выполенения  
 red\_edit\_result\_info : string - Подробная информация о включении (отключении) автозагрузки  
}

# Включение USB-носителей win

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_info: string - Подробная информация о включении usb.  
}

# Включение автообновления win

## Описание

Команда производит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_autoupdate: bool - Возвращает статус выполенения.  
 turn\_on\_autoupdate\_info: string - Подробная информация о включении автообновлений.  
}

# Включение брандмауэра

## Описание

Включает брандмауэр. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_firewall: bool - Возвращает статус выполенения.  
 turn\_on\_firewall\_info: string - Подробная информация о включении фаервола.  
}

# Включение службы Windows

## Описание

Включает службу, имя которой было передано. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ service: string - Имя службы, которую надо включить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_service: bool - Возвращает статус выполенения.  
 turn\_on\_service\_info: string - Подробная информация о включении службы.  
}

# Выключение машины Windows

## Описание

Завершает работу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении. \_\_\_ ## Input: { ❗ ip\_address or *hostname*: string - Адрес целевой машины. sd\_time: int - Время до выключения машины (по умолчанию 60 секунд). message: string - Сообщение, которое увидят пользователи (по умолчанию "Ваш компьютер будет выключен через {sd\_time} секунд(-у, -ы). Сохраните открытые файлы."). }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 win\_shutdown: bool - Возвращает статус выполенения.  
 win\_shutdown\_info: string - Подробная информация о выключении машины.  
}

# Отключение USB-носителей Windows

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее: - будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов; - ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено). \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_info: string - Подробная информация о включении usb.  
}

# Блокировка доменного пользователя

## Описание:

Отключает учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка локального пользователя Windows

## Описание:

Отключает учётную запись пользователя.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка пользователя Linux

## Описание

Блокирует указанного пользователя на указанном хосте. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Принудительное завершение процесса Linux

## Описание

Команда kill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ process\_name: string - Имя процесса, который нужно отключить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о завершении процесса.  
}

# Завершить все RDP соединения на сервере Win.

## Описание

Отключает все RDP сессии на сервере. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_rdp\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_rdp\_sessions\_info: string - Подробная информация об отключении активных RDP сессий.  
}

# Завершить сеансы всех пользователей Windows

## Описание

Завершает ВСЕ активные сессии на указанной машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_sessions\_info: string - Подробная информация об отключении.  
}

# Включение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_write\_info: string - Подробная информация о включении запрета записи usb.  
}

# Изменение политики паролей в домене AD

## Описание:

Скрипт изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!!

Условные обозначения для формата:

D = Дни (от 0 до 10675199)

H = Часы (от 0 до 23)

M = Минуты (от 0 до 59)

S = Секунды (от 0 до 59)

F = Доли секунды (от 0 до 9999999)

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес машины, на которой будет выполняться скрипт (лучше всего подойдёт контроллер домена).  
 ❗ ComplexityEnabled: bool - Указывает, включена ли сложность пароля для политики паролей.  
 ❗ LockoutDuration: string - Требуемый формат: "D.H:M:S.F". Указывает период времени, в течение которого учетная запись блокируется после того, как количество неудачных попыток входа в систему превышает порог блокировки. Вы не можете войти в заблокированную учетную запись, пока не истечет период времени блокировки. Этот параметр задает свойство lockoutDuration объекта политики паролей.  
 ❗ LockoutObservationWindow: string - Требуемый формат: "D:H:M:S.F". Указывает максимальный интервал времени между двумя неудачными попытками входа в систему, по истечении которого количество неудачных попыток входа сбрасывается до 0. Учетная запись блокируется, когда количество неудачных попыток входа превышает порог блокировки политики паролей. Этот параметр задает свойство lockoutObservationWindow объекта политики паролей  
 ❗ LockoutThreshold: int - Указывает допустимое количество неудачных попыток входа, прежде чем учетная запись будет заблокирована. Это число увеличивается, когда время между неудачными попытками входа в систему меньше, чем время, указанное для окна времени наблюдения за блокировкой. Этот параметр задает свойство LockoutThreshold политики паролей.  
 ❗ MaxPasswordAge: string - Требуемый формат: "D.H:M:S.F". Определяет максимальное время, в течение которого вы можете иметь один и тот же пароль. По истечении этого периода срок действия пароля истекает, и вы должны создать новый.  
 ❗ MinPasswordAge: string - Требуемый формат: "D.H:M:S.F". Указывает минимальное время, по истечении которого вы сможете изменить пароль.  
 ❗ MinPasswordLength: int - Указывает минимальное количество символов, которое должен содержать пароль. Этот параметр задает свойство MinPasswordLength политики паролей.  
 ❗ PasswordHistoryCount: int [Указывает количество предыдущих паролей для сохранения. Пользователь не может повторно использовать пароль из списка сохраненных паролей. Этот параметр задает свойство PasswordHistoryCount для политики паролей.  
 ❗ ReversibleEncryptionEnabled: bool - Указывает, должен ли каталог хранить пароли с использованием обратимого шифрования. Этот параметр задает свойство ReversibleEncryption для политики паролей.  
 ❗ identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 change\_password\_policy: bool - Возвращает статус выполенения.  
 change\_password\_policy\_info: string - Подробная информация о изменении парольной политики.  
}

# Получение имени УЗ по SID

## Описание:

Возвращает имя учётной записи по её SID.

## Input:

{  
 ❗ sid: string - SID пользователя, имя УЗ которого надо узнать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_account: bool - Возвращает статус выполенения.  
 get\_account\_info: string - Имя учётной записи пользователя, в случае успеха, или сообщение об ошибке.  
}

# Получение списка интерфейсов и информации о них

## Описание:

Скрипт подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_settings: bool - Возвращает статус выполенения.  
 linux\_settings\_info: list -> string | string - Массив строк, которые содержат название инфтерфейсов и информацию о них, в случае успеха или строка, информация об ошибке.  
}

# Обновление пакетов

## Описание:

Обновляет установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper. Local версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления) Remote версия обновляет на удаленной linux машине. \_\_\_ Local-версия ## Input: {

}

## Secrets:

{  
  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

Remote-версия ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

# Определяет местоположение по ip

## Описание:

Первая версия использует библиотеку ipwhois. Вторая использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).

ipwhois-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

ipinfo-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
 ❗ ipinfo\_token: string - Токен, предоставляемый сервисом.  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение ssh соодинений

## Описание:

Скрипт производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_ssh: bool - Возвращает статус выполенения.  
 turn\_off\_ssh\_info: string - Подробная информация об отключении ssh соединений.  
}

# Отключение активных сессий Liunx

## Описание:

Отключает все активные сессии. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_session: bool - Возвращает статус выполенения.  
 turn\_off\_session\_info: string - Подробная информация об отключенных пользователях.  
}

# Отклюлчение всех сетевых интерфейсов

# Описание:

Отключает все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 disabled: bool - Возвращает статус выполенения.  
 disabled\_info: string - Подробная информация об отключенных интерфейсах.  
}

# Отключение службы Win

## Описание:

Отключает указанный сервис.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ service\_name: string - Имя сервиса, который необходимо отключить.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_service\_result: bool - Возвращает статус выполенения.  
 disable\_service\_result\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение узла Linux

## Описание:

Отключает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. time\_out: int - Время, через которое компьютер выключится. message: string - Сообщение, которое будет выводиться пользователям. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_node: bool - Возвращает статус выполенения.  
 turn\_off\_node\_info: string - Подробная информация о выключении компьютера.  
}

# Включение запрета на cd dvd

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_cddvd: bool - Возвращает статус выполенения.  
 turn\_off\_cddvd\_info: string - Подробная информация о включении запрета записи cd dvd.  
}

# Отключает все сетевые интерфейсы

## Описание:

Отключает сетевые интерфейсы. После отключения невозможно удаленно зайти на машину. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_net\_int\_win: bool - Возвращает статус выполенения.  
 disable\_net\_int\_win\_info: string - Подробная информация об отключении интерфейсов.  
}

# Отправить сообщение авторизованным по ssh пользователям Linux

## Описание:

При использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер. Невозможно достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 send\_message: bool - Возвращает статус выполенения.  
 send\_message\_info: string - Подробная информация об отправленном сообщении.  
}

# Отправить сообщение пользователю Win

## Описание:

Отправляет сообщение на указанный хост.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 message\_result: bool - Возвращает статус выполенения.  
 message\_result\_info: string - Подробная информация об отправленном сообщении.  
}

# Перезагрузить компьютер Windows

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 message: string - Сообщение, отображаемое пользователям.  
 timeout: string - Время до перезагрузки.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reboot\_win: bool - Возвращает статус выполенения.  
 reboot\_win\_info: string - Подробная информация о перезагрузке.  
}

# Перезагрузка узла Linux

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. message: string - Сообщение, отображаемое пользователям. timeout: int - Время до перезагрузки. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 reboot\_node: bool - Возвращает статус выполенения.  
 reboot\_node\_info: string - Подробная информация о блокировке пользователя.  
}

# Получение времени и даты

## Описание:

Возвращает текущее время на Linux-машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_time: bool - Возвращает статус выполенения.  
 linux\_time\_info: string - Подробная информация о времени на устройстве.  
}

# Получение политики паролей в домене AD

## Описание:

Скрипт возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_password\_policy: bool - Возвращает статус выполенения.  
 get\_password\_policy\_info: list - Массив, содержащий политики и их значения.  
 get\_password\_policy\_info.[].name: string - Название политики.  
 get\_password\_policy\_info.[].value: string - Установленное значение политики.  
}

# Получить список запущенных процессов

## Описание:

Позволяет получить список процессов, запущенных на машине и их pid-ы. get\_win\_proc - получает информацию из виндовых машин get\_linux\_proс - пполучает информацию из линуксовой машин

Windows-версия

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

Linux-версия \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

# Завершить процесс Windows

## Описание:

Завершает процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗ \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. user: string - Имя учётной записи пользователя, процессы которого нуобходимо завершить. process: string or int - Имя процесса или его pid. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о блокировке пользователя.  
}

# Проверить целостность системных файлов Windows

## Описание:

Выполняет сканирование системных файлов, результат выводится строкой. Может занять очень много времени.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 check\_win: bool - Возвращает статус выполенения.  
 check\_win\_info: string - Подробная информация о результатах сканирования.  
}

# Проверка в Virus Total

## Описание:

Проверяет заданный url или ip адрес в Virus Total.

## Input:

{  
 ❗ ip: string - ip или url, который неоьбходимо проверить.  
}

## Secrets:

{  
 ❗ vt\_api\_key: string - Api-key для сервиса Virus Total.  
}

## Output:

{  
 result: string - Возвращает строку, содержащую результат проверки.  
}

# Проверка доступности хоста утилитой ping

## Описание:

Работает как на linux, так и на windows Отсылает только один пакет Доступность проверяется с того же хоста, где установлен SOAR \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
   
}

## Output:

{  
 ping: bool - Возвращает статус выполенения.  
 ping\_info: string - Подробная информация о доступности хоста.  
}

# Отключение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_write\_info: string - Подробная информация о выполнении операции.  
}

# Сброс пароля локального пользователя

## Описание:

Сбрасывает (устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https. \_\_\_

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, ккоторому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля пользователя.  
}

# Сброс пароля доменного пользователя

## Описание:

Сбрасывает пароль выбранного пользователя (устанавливает смену пароля при следующем логине).

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля.  
}

# Получение списка подключенных USB устройств

## Описание:

Возвращает список всех usb-устройств, подключенных к компьютеру в данный момент \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_usb: bool - Возвращает статус выполенения.  
 connected\_usb\_info: list -> string - Массив, содержащий названия usb-устройств.  
}

# Получение списка подключенных пользователей

## Описание:

Возвращает список всех подключенных пользователей, а также информацию о них.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_users: bool - Возвращает статус выполенения.  
 connected\_users\_info: list -> string - Подробная информация о подключенных пользователях.  
}

# Список контроля доступа

## Описание:

Скрипт возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке и её подпапкам.  
}

# Список контроля доступа

## Описание

Скрипт возвращает список контроля доступа (ACL) для папки узла Windows. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\" или "/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке.  
}

# Получение списка правил Iptables

## Описание:

Скрипт возвращает правила из Iptables

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list - Массив, содержащий правила из Iptables или информация об ошибке.  
 firewall\_rules\_info.[].chain\_name: string - Название цепочки.  
 firewall\_rules\_info.[].values: list - Массив, содержащий информацию о правилах.  
 firewall\_rules\_info.[].values.[].target: string - Eсли пакет отвечает правилу, заголовок target указывает, что с ним нужно сделать.  
 firewall\_rules\_info.[].values.[].prot: string - Протокол  
 firewall\_rules\_info.[].values.[].opt: string - Данный параметр используется редко и отображает опции IP  
 firewall\_rules\_info.[].values.[].source: string - Исходный IP-адрес или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].destination: string - IP-адрес назначения или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].info: string - Любая часть правила, которая не указана предыдущими столбцами  
}

# Список правил Windows Firewall

## Описание:

Скрипт возвращает список всех правил Windows Firewall.

**Работает только с >= win 10!** \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list -> string - Список всех правил на Firewall.  
}

# Список открытых сессий

## Описание:

Скрипт возвращает все активные активные сессии.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 active\_sessions: bool - Возвращает статус выполенения.  
 active\_sessions\_info: list - Подробная информация об установленных подключениях.  
 active\_sessions\_info.[].username: string - Имя пользователя  
 active\_sessions\_info.[].sessionname: string - Имя сессии  
 active\_sessions\_info.[].id: string - id сессии  
 active\_sessions\_info.[].state: string - Состояние сессии  
 active\_sessions\_info.[].idle\_time: string - Время простоя  
 active\_sessions\_info.[].logon\_time: string - Время входа  
}

# Список установленных сетевых соединений

## Описание:

Скрипт возвращает все активные соединения хоста в виде списка. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 estabilish\_conn\_result: bool - Возвращает статус выполенения.  
 estabilish\_conn\_result\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilish\_conn\_result\_info.[].RemoteAddress: string - Удаленный адрес  
 estabilish\_conn\_result\_info.[].LocalAddress: string - Локальный адерес  
}

# Получение списка установленных соединений

## Описание:

Возвращает массив установленных хостом подключений. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 estabilished\_connetctions: bool - Возвращает статус выполенения.  
 estabilished\_connetctions\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilished\_connetctions\_info.[].local\_address: string - Локальный адерес  
 estabilished\_connetctions\_info.[].foreign\_address: string - Удаленный адрес  
}

# Удаление из локальной группы

## Описание:

Удаляет пользователя из указанной локальной группы. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя учётной записи пользователя, которого необходимо удалить из группы. ❗ group: string - Имя группы, из которой необходимо удалить пользователя. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 del\_user\_from\_group\_result: bool - Возвращает статус выполенения.  
 del\_user\_from\_group\_result\_info: string - Подробная информация об удалении пользователя из группы.  
}

# Удаление папки и её содержимого

## Описание:

Удаляет переданную папку и всё её содержимое. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь до папки, которую необходимо удалить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Удаляет папку win

## Описание:

Производит удаление папки

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Полный путь до папки. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Безопасное затирание удаленных файлов

## Описание:

Команда производит полное затирание (без возможности восстановления) удаленных файлов с диска C: (по умолчанию) узла Windows. Cвободное место на диске перезаписывается за 3 прохода: сначала нулями, затем единицами, в финале - случайными значениями. Возможно указание конкретной папки на диске. Перед запуском рекомендуется отчистить корзину и закрыть все активные программы. Затирание занимает длительный промежуток времени. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. path: string - Путь до папки, которую необходимо затереть. Путь должен разделяться "\" или "/". Если переменная не указана явно, то принимает значение "C:/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 cipher\_folder: bool - Возвращает статус выполенения.  
 cipher\_folder\_info: string - Подробная информация о затирании информации.  
}

# Включение (отключение) автозагрузки на всех устройствах Windows

## Описание:

Скрипт disable\_autorun отключает автозапуск вообще всех дисков. Скрипт enable\_autorun разрешает автозапуск только неизвестных и сетевых дисков (по идее это значение по умолчанию). Требуется настроенная служба winrm https. Входы и выходы актуальны для обоих скриптов \_\_\_ ## Input: { ❗ ip\_address or hostname : string - Адрес целевой машины }

## Secrets:

{  
 ❗ login : string - Имя пользователя, под которым заходим на машину  
 ❗ password : string - Пароль от пользователя  
 ❗ domain : string - Домен, в котором расположена машина  
}

## Output:

{  
 red\_edit\_result : bool - Возвращает статус выполенения  
 red\_edit\_result\_info : string - Подробная информация о включении (отключении) автозагрузки  
}

# Включение USB-носителей win

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства хранения данных, будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то доступ к нему не предоставится. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_info: string - Подробная информация о включении usb.  
}

# Включение автообновления win

## Описание

Команда производит запись ключа реестра Windows, который отвечает за настройки автоматического обновления Windows. Значения параметра "AUOptions" = 3 означает, что обновления будут скачаны автоматически и пользователь получит уведомление о возможности их установки. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_autoupdate: bool - Возвращает статус выполенения.  
 turn\_on\_autoupdate\_info: string - Подробная информация о включении автообновлений.  
}

# Включение брандмауэра

## Описание

Включает брандмауэр. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_firewall: bool - Возвращает статус выполенения.  
 turn\_on\_firewall\_info: string - Подробная информация о включении фаервола.  
}

# Включение службы Windows

## Описание

Включает службу, имя которой было передано. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ service: string - Имя службы, которую надо включить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_service: bool - Возвращает статус выполенения.  
 turn\_on\_service\_info: string - Подробная информация о включении службы.  
}

# Выключение машины Windows

## Описание

Завершает работу указанной машины. Перед завершением работы пользователю будет показано предупреждение о завершении. \_\_\_ ## Input: { ❗ ip\_address or *hostname*: string - Адрес целевой машины. sd\_time: int - Время до выключения машины (по умолчанию 60 секунд). message: string - Сообщение, которое увидят пользователи (по умолчанию "Ваш компьютер будет выключен через {sd\_time} секунд(-у, -ы). Сохраните открытые файлы."). }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 win\_shutdown: bool - Возвращает статус выполенения.  
 win\_shutdown\_info: string - Подробная информация о выключении машины.  
}

# Отключение USB-носителей Windows

## Описание

Скрипт производит запись ключа реестра Windows, который отвечает за работу USB устройств хранения данных. В результате ее выполнения все, заново подключенные USB устройства, не будут отображаться в интерфейсе ОС. При этом, если на момент изменения ключа реестра, USB устройство хранения данных будет уже использоваться, то доступ к нему не прервется. Если взять USB устройство хранения данных, на которое ОС еще не установила драйвер, то произойдет следующее: - будет использован файл usbstor.pnf (при его отсутствии usbstor.inf) и будет определен набор драйверов; - ОС от имени учетной записи SYSTEM установит эти драйвера и исправит значение параметра Start для USBSTOR на значение 3 (разрешено). \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_info: string - Подробная информация о включении usb.  
}

# Блокировка доменного пользователя

## Описание:

Отключает учётную запись доменного пользователя, путём замены значения в атрибуте "userAccountControl" на 2.

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка локального пользователя Windows

## Описание:

Отключает учётную запись пользователя.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, которого необходимо заблокировать.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Блокировка пользователя Linux

## Описание

Блокирует указанного пользователя на указанном хосте. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 block\_user: bool - Возвращает статус выполенения.  
 block\_user\_info: string - Подробная информация о блокировке пользователя.  
}

# Принудительное завершение процесса Linux

## Описание

Команда kill не возвращает статус выполнения, поэтому результат выполнения скрипта не является достоверным. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ process\_name: string - Имя процесса, который нужно отключить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о завершении процесса.  
}

# Завершить все RDP соединения на сервере Win.

## Описание

Отключает все RDP сессии на сервере. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_rdp\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_rdp\_sessions\_info: string - Подробная информация об отключении активных RDP сессий.  
}

# Завершить сеансы всех пользователей Windows

## Описание

Завершает ВСЕ активные сессии на указанной машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_sessions: bool - Возвращает статус выполенения.  
 turn\_off\_sessions\_info: string - Подробная информация об отключении.  
}

# Включение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате его выполнения, на все заново подключенные USB устройства хранения данных, будет запрещено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то запрет на запись к нему не применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_off\_usb\_write\_info: string - Подробная информация о включении запрета записи usb.  
}

# Изменение политики паролей в домене AD

## Описание:

Скрипт изменяет текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается при подключении. все поля должны быть обязательно заполнены!!!

Условные обозначения для формата:

D = Дни (от 0 до 10675199)

H = Часы (от 0 до 23)

M = Минуты (от 0 до 59)

S = Секунды (от 0 до 59)

F = Доли секунды (от 0 до 9999999)

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес машины, на которой будет выполняться скрипт (лучше всего подойдёт контроллер домена).  
 ❗ ComplexityEnabled: bool - Указывает, включена ли сложность пароля для политики паролей.  
 ❗ LockoutDuration: string - Требуемый формат: "D.H:M:S.F". Указывает период времени, в течение которого учетная запись блокируется после того, как количество неудачных попыток входа в систему превышает порог блокировки. Вы не можете войти в заблокированную учетную запись, пока не истечет период времени блокировки. Этот параметр задает свойство lockoutDuration объекта политики паролей.  
 ❗ LockoutObservationWindow: string - Требуемый формат: "D:H:M:S.F". Указывает максимальный интервал времени между двумя неудачными попытками входа в систему, по истечении которого количество неудачных попыток входа сбрасывается до 0. Учетная запись блокируется, когда количество неудачных попыток входа превышает порог блокировки политики паролей. Этот параметр задает свойство lockoutObservationWindow объекта политики паролей  
 ❗ LockoutThreshold: int - Указывает допустимое количество неудачных попыток входа, прежде чем учетная запись будет заблокирована. Это число увеличивается, когда время между неудачными попытками входа в систему меньше, чем время, указанное для окна времени наблюдения за блокировкой. Этот параметр задает свойство LockoutThreshold политики паролей.  
 ❗ MaxPasswordAge: string - Требуемый формат: "D.H:M:S.F". Определяет максимальное время, в течение которого вы можете иметь один и тот же пароль. По истечении этого периода срок действия пароля истекает, и вы должны создать новый.  
 ❗ MinPasswordAge: string - Требуемый формат: "D.H:M:S.F". Указывает минимальное время, по истечении которого вы сможете изменить пароль.  
 ❗ MinPasswordLength: int - Указывает минимальное количество символов, которое должен содержать пароль. Этот параметр задает свойство MinPasswordLength политики паролей.  
 ❗ PasswordHistoryCount: int [Указывает количество предыдущих паролей для сохранения. Пользователь не может повторно использовать пароль из списка сохраненных паролей. Этот параметр задает свойство PasswordHistoryCount для политики паролей.  
 ❗ ReversibleEncryptionEnabled: bool - Указывает, должен ли каталог хранить пароли с использованием обратимого шифрования. Этот параметр задает свойство ReversibleEncryption для политики паролей.  
 ❗ identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 change\_password\_policy: bool - Возвращает статус выполенения.  
 change\_password\_policy\_info: string - Подробная информация о изменении парольной политики.  
}

# Получение имени УЗ по SID

## Описание:

Возвращает имя учётной записи по её SID.

## Input:

{  
 ❗ sid: string - SID пользователя, имя УЗ которого надо узнать.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_account: bool - Возвращает статус выполенения.  
 get\_account\_info: string - Имя учётной записи пользователя, в случае успеха, или сообщение об ошибке.  
}

# Получение списка интерфейсов и информации о них

## Описание:

Скрипт подключается к удаленной машине и возвращает массив строк, которые содержат название инфтерфейсов и информацию о них. На целевой машине необходим установленный пакет net-tools. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_settings: bool - Возвращает статус выполенения.  
 linux\_settings\_info: list -> string | string - Массив строк, которые содержат название инфтерфейсов и информацию о них, в случае успеха или строка, информация об ошибке.  
}

# Обновление пакетов

## Описание:

Обновляет установленные пакеты. Работает с пакетными менеджерами apt, apt-get, yum, dnf, pacman, zypper. Local версия обновляет на текущей машине linux (необходимо что лямбда была запущена с правами, достаточными для обновления) Remote версия обновляет на удаленной linux машине. \_\_\_ Local-версия ## Input: {

}

## Secrets:

{  
  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

Remote-версия ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя пользователя, которого нужно заблокировать. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 updated: bool - Возвращает статус выполенения.  
 updated\_info: string - Подробная информация об обновлении.  
}

# Определяет местоположение по ip

## Описание:

Первая версия использует библиотеку ipwhois. Вторая использует сторонний сервис http://ipinfo.io/. На бесплатном аккаунте лимит запросов 50к/месяц (на момент 28.03.2022).

ipwhois-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

ipinfo-версия ## Input: { ❗ ip: string - IP-адрес, который необходимо проверить. }

## Secrets:

{  
 ❗ ipinfo\_token: string - Токен, предоставляемый сервисом.  
}

## Output:

{  
 geo: bool - Возвращает статус выполенения.  
 geo\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение ssh соодинений

## Описание:

Скрипт производит отключение всех активных ssh соединений. После этого скрипты не могут подключиться к целевой машине до перезапуска сервиса sshd.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_ssh: bool - Возвращает статус выполенения.  
 turn\_off\_ssh\_info: string - Подробная информация об отключении ssh соединений.  
}

# Отключение активных сессий Liunx

## Описание:

Отключает все активные сессии. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_session: bool - Возвращает статус выполенения.  
 turn\_off\_session\_info: string - Подробная информация об отключенных пользователях.  
}

# Отклюлчение всех сетевых интерфейсов

# Описание:

Отключает все сетевые интерфейсы, которые сможет найти. ❗После того как интерфейсы будут отключены - зайти на машину удаленно будет невозможно❗

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 disabled: bool - Возвращает статус выполенения.  
 disabled\_info: string - Подробная информация об отключенных интерфейсах.  
}

# Отключение службы Win

## Описание:

Отключает указанный сервис.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ service\_name: string - Имя сервиса, который необходимо отключить.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_service\_result: bool - Возвращает статус выполенения.  
 disable\_service\_result\_info: string - Подробная информация о блокировке пользователя.  
}

# Отключение узла Linux

## Описание:

Отключает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. time\_out: int - Время, через которое компьютер выключится. message: string - Сообщение, которое будет выводиться пользователям. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 turn\_off\_node: bool - Возвращает статус выполенения.  
 turn\_off\_node\_info: string - Подробная информация о выключении компьютера.  
}

# Включение запрета на cd dvd

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за отключение CD DVD-Rom устройств. После выполнения данной команды изменения вступят в силу только после перезагрузки ОС.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_off\_cddvd: bool - Возвращает статус выполенения.  
 turn\_off\_cddvd\_info: string - Подробная информация о включении запрета записи cd dvd.  
}

# Отключает все сетевые интерфейсы

## Описание:

Отключает сетевые интерфейсы. После отключения невозможно удаленно зайти на машину. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 disable\_net\_int\_win: bool - Возвращает статус выполенения.  
 disable\_net\_int\_win\_info: string - Подробная информация об отключении интерфейсов.  
}

# Отправить сообщение авторизованным по ssh пользователям Linux

## Описание:

При использовании sudo сообщение приходило не всегда, поэтому все сообщения отправляются от пользователя, под которым заходим на сервер. Невозможно достоверно сказать, когда команда выполняется удачно. Результат выполнения предположительный.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 send\_message: bool - Возвращает статус выполенения.  
 send\_message\_info: string - Подробная информация об отправленном сообщении.  
}

# Отправить сообщение пользователю Win

## Описание:

Отправляет сообщение на указанный хост.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ message: string - Сообщение, которое отправляется на хост.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 message\_result: bool - Возвращает статус выполенения.  
 message\_result\_info: string - Подробная информация об отправленном сообщении.  
}

# Перезагрузить компьютер Windows

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 60 секунд. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.".

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 message: string - Сообщение, отображаемое пользователям.  
 timeout: string - Время до перезагрузки.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reboot\_win: bool - Возвращает статус выполенения.  
 reboot\_win\_info: string - Подробная информация о перезагрузке.  
}

# Перезагрузка узла Linux

## Описание:

Перезагружает компьютер через указанный промежуток времени. Если промежуток не указан, то компьютер будет выключен через 1 минуту. Так же выводит сообщение всем пользователям, работающим на устройстве, по умолчанию "The computer will shutdown, please save all work.". \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. message: string - Сообщение, отображаемое пользователям. timeout: int - Время до перезагрузки. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 reboot\_node: bool - Возвращает статус выполенения.  
 reboot\_node\_info: string - Подробная информация о блокировке пользователя.  
}

# Получение времени и даты

## Описание:

Возвращает текущее время на Linux-машине. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 linux\_time: bool - Возвращает статус выполенения.  
 linux\_time\_info: string - Подробная информация о времени на устройстве.  
}

# Получение политики паролей в домене AD

## Описание:

Скрипт возвращает текущую политику паролей в указанном домене. Если домен не указан, то берётся тот домен, который указывается в secrets.domain.

Командлеты модуля PowerShell AD, которые используются в скрипте, можно запускать в Windows Server 2003, 2008 и выше, а также в Windows 7 и выше, но должен быть хотя бы один контроллер домена Windows Server 2008 R2 и выше. Если используется машина под управлением не серверной ОС, то обязательно должно быть установлено расширение Active Directory for PowerShell.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 identity: string - Домен, политики которого необходимо проверить. По умолчанию используется тот, что указан в secrets.domain.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 get\_password\_policy: bool - Возвращает статус выполенения.  
 get\_password\_policy\_info: list - Массив, содержащий политики и их значения.  
 get\_password\_policy\_info.[].name: string - Название политики.  
 get\_password\_policy\_info.[].value: string - Установленное значение политики.  
}

# Получить список запущенных процессов

## Описание:

Позволяет получить список процессов, запущенных на машине и их pid-ы. get\_win\_proc - получает информацию из виндовых машин get\_linux\_proс - пполучает информацию из линуксовой машин

Windows-версия

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

Linux-версия \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 tasks\_list: bool - Возвращает статус выполенения.  
 tasks\_list\_info: list - Массив, содержащий названия процессов и их pid-ы.  
 tasks\_list\_info.[].name: string - Название процесса.  
 tasks\_list\_info.[].pids: list -> int - Массив, pid-ы процессов.  
}

# Завершить процесс Windows

## Описание:

Завершает процесс в Windows системе. Если в переменной process находится число, то оно рассматривается как PID, а если строка, то как название процесса. Также есть возможность завершить все процессы конкретного пользователя. ❗ В скрипт обязательно должно придти одна из переменных: user или process. ❗ \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. user: string - Имя учётной записи пользователя, процессы которого нуобходимо завершить. process: string or int - Имя процесса или его pid. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 kill\_process: bool - Возвращает статус выполенения.  
 kill\_process\_info: string - Подробная информация о блокировке пользователя.  
}

# Проверить целостность системных файлов Windows

## Описание:

Выполняет сканирование системных файлов, результат выводится строкой. Может занять очень много времени.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 check\_win: bool - Возвращает статус выполенения.  
 check\_win\_info: string - Подробная информация о результатах сканирования.  
}

# Проверка в Virus Total

## Описание:

Проверяет заданный url или ip адрес в Virus Total.

## Input:

{  
 ❗ ip: string - ip или url, который неоьбходимо проверить.  
}

## Secrets:

{  
 ❗ vt\_api\_key: string - Api-key для сервиса Virus Total.  
}

## Output:

{  
 result: string - Возвращает строку, содержащую результат проверки.  
}

# Проверка доступности хоста утилитой ping

## Описание:

Работает как на linux, так и на windows Отсылает только один пакет Доступность проверяется с того же хоста, где установлен SOAR \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
   
}

## Output:

{  
 ping: bool - Возвращает статус выполенения.  
 ping\_info: string - Подробная информация о доступности хоста.  
}

# Отключение запрета записи на USB

## Описание:

Скрипт производит запись ключа реестра Windows, который отвечает за возможность записи на USB устройства хранения данных. В результате ее выполнения, на все заново подключенные USB устройства хранения данных, будет разрешено произвоить запись файлов. При этом, если на момент изменения ключа реестра, USB устройство хранения данных уже использовалось, то разрешение все-равно применяется. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 turn\_on\_usb\_write: bool - Возвращает статус выполенения.  
 turn\_on\_usb\_write\_info: string - Подробная информация о выполнении операции.  
}

# Сброс пароля локального пользователя

## Описание:

Сбрасывает (устанавливает смену пароля при следующем логине) пароль локального пользователя на указанной машине. Требуется настроенная служба winrm https. \_\_\_

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ user: string - Имя учётной записи пользователя, ккоторому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля пользователя.  
}

# Сброс пароля доменного пользователя

## Описание:

Сбрасывает пароль выбранного пользователя (устанавливает смену пароля при следующем логине).

## Input:

{  
 ❗ user: string - Имя учётной записи пользователя, которому необходимо сбросить пароль.  
}

## Secrets:

{  
 ❗ ldap\_server: string - Адрес LDAP сервера.  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 reset\_user\_password\_result: bool - Возвращает статус выполенения.  
 reset\_user\_password\_result\_info: string - Подробная информация о сбросе пароля.  
}

# Получение списка подключенных USB устройств

## Описание:

Возвращает список всех usb-устройств, подключенных к компьютеру в данный момент \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_usb: bool - Возвращает статус выполенения.  
 connected\_usb\_info: list -> string - Массив, содержащий названия usb-устройств.  
}

# Получение списка подключенных пользователей

## Описание:

Возвращает список всех подключенных пользователей, а также информацию о них.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 connected\_users: bool - Возвращает статус выполенения.  
 connected\_users\_info: list -> string - Подробная информация о подключенных пользователях.  
}

# Список контроля доступа

## Описание:

Скрипт возвращает список контроля доступа (ACL) для папки и ее подпапок узла Windows.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке и её подпапкам.  
}

# Список контроля доступа

## Описание

Скрипт возвращает список контроля доступа (ACL) для папки узла Windows. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь к папке, права доступа которой необходимо проверить. Путь должен разделяться "\" или "/". }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 folder\_acl: bool - Возвращает статус выполенения.  
 folder\_acl\_info: list -> string - Массив, содержащий подробную информация о правах доступа к папке.  
}

# Получение списка правил Iptables

## Описание:

Скрипт возвращает правила из Iptables

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list - Массив, содержащий правила из Iptables или информация об ошибке.  
 firewall\_rules\_info.[].chain\_name: string - Название цепочки.  
 firewall\_rules\_info.[].values: list - Массив, содержащий информацию о правилах.  
 firewall\_rules\_info.[].values.[].target: string - Eсли пакет отвечает правилу, заголовок target указывает, что с ним нужно сделать.  
 firewall\_rules\_info.[].values.[].prot: string - Протокол  
 firewall\_rules\_info.[].values.[].opt: string - Данный параметр используется редко и отображает опции IP  
 firewall\_rules\_info.[].values.[].source: string - Исходный IP-адрес или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].destination: string - IP-адрес назначения или подсеть трафика, либо anywhere  
 firewall\_rules\_info.[].values.[].info: string - Любая часть правила, которая не указана предыдущими столбцами  
}

# Список правил Windows Firewall

## Описание:

Скрипт возвращает список всех правил Windows Firewall.

**Работает только с >= win 10!** \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 firewall\_rules: bool - Возвращает статус выполенения.  
 firewall\_rules\_info: list -> string - Список всех правил на Firewall.  
}

# Список открытых сессий

## Описание:

Скрипт возвращает все активные активные сессии.

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 active\_sessions: bool - Возвращает статус выполенения.  
 active\_sessions\_info: list - Подробная информация об установленных подключениях.  
 active\_sessions\_info.[].username: string - Имя пользователя  
 active\_sessions\_info.[].sessionname: string - Имя сессии  
 active\_sessions\_info.[].id: string - id сессии  
 active\_sessions\_info.[].state: string - Состояние сессии  
 active\_sessions\_info.[].idle\_time: string - Время простоя  
 active\_sessions\_info.[].logon\_time: string - Время входа  
}

# Список установленных сетевых соединений

## Описание:

Скрипт возвращает все активные соединения хоста в виде списка. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 estabilish\_conn\_result: bool - Возвращает статус выполенения.  
 estabilish\_conn\_result\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilish\_conn\_result\_info.[].RemoteAddress: string - Удаленный адрес  
 estabilish\_conn\_result\_info.[].LocalAddress: string - Локальный адерес  
}

# Получение списка установленных соединений

## Описание:

Возвращает массив установленных хостом подключений. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 estabilished\_connetctions: bool - Возвращает статус выполенения.  
 estabilished\_connetctions\_info: list - Массив, содержащий подробную информацию об установленных подключениях.  
 estabilished\_connetctions\_info.[].local\_address: string - Локальный адерес  
 estabilished\_connetctions\_info.[].foreign\_address: string - Удаленный адрес  
}

# Удаление из локальной группы

## Описание:

Удаляет пользователя из указанной локальной группы. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ user: string - Имя учётной записи пользователя, которого необходимо удалить из группы. ❗ group: string - Имя группы, из которой необходимо удалить пользователя. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 del\_user\_from\_group\_result: bool - Возвращает статус выполенения.  
 del\_user\_from\_group\_result\_info: string - Подробная информация об удалении пользователя из группы.  
}

# Удаление папки и её содержимого

## Описание:

Удаляет переданную папку и всё её содержимое. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Путь до папки, которую необходимо удалить. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Удаляет папку win

## Описание:

Производит удаление папки

## Input:

{  
 ❗ ip\_address or hostname: string - Адрес целевой машины.  
 ❗ path: string - Полный путь до папки. Путь должен разделяться "\\" или "/".  
}

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.  
 ❗ domain: string - Домен, в котором расположена машина.  
}

## Output:

{  
 remove\_folder: bool - Возвращает статус выполенения.  
 remove\_folder\_info: string - Подробная информация об удалении папки.  
}

# Удаление файла

## Описание:

Удаляет файл, путь до которого передаётся. \_\_\_ ## Input: { ❗ ip\_address or hostname: string - Адрес целевой машины. ❗ path: string - Полный путь до удаляемого файла. }

## Secrets:

{  
 ❗ login: string - Имя пользователя, под которым заходим на машину.  
 ❗ password: string - Пароль от пользователя.   
 OR pem\_file: string - Закрытый ключ.  
 root\_password: string - Пароль от sudo, если у переданного пользователя недостаточно прав для выполнения команды.  
}

## Output:

{  
 remove\_file: bool - Возвращает статус выполенения.  
 remove\_file\_info: string - Подробная информация об удалении файла.  
}