Лабораторная работа №4 27.11.2024г.

Полещук Илья

Исходный код: <https://github.com/Qwertask/OSInfo>

Задача лабораторной работы:

1. Реализовать приложение/скрипт, которое собирает информацию о системе:

•Состояние антивируса

• Установлен? Включен? Сигнатуры обновлены?

•Состояние сетевой защиты (файрвола)

•Состояние защиты диска (Bitlocker, Filevault, ...)

•Состояние обновлений ОС

•Основная информация о Hardware

• Процессор: количество ядер/загрузка, RAM – количество/загрузка,

диск – общая память/свободная память, Сеть – имя, адрес, тип –проводная/беспроводная

1. GUI
2. Возможность расширения проверок - например, на наличие определенных файлов/их версий

• Список задается в отдельном конфигурационном файле или в аргументах для приложения

• --check-file-ver "c:\program files\office14\winword.exe" ">14.0"

1. Возможность запускать сбор информации покомпонентно

(только обновления, только AV/FW, ...)

1. Возможность выводить результат в формате JSON

Примечания:

1. Приложение проверено и отлажено для Windows. На ОС Linux и Mac данные могут не совпадать с действительностью.
2. На Windows необходимо запускать от имени администратора, так как BitLocker иначе не выдаст ничего кроме «Ошибка: попытка получения доступа к требуемому ресурсу была отклонена. Убедитесь, что учетная запись на этом компьютере имеет права администратора.»
   1. Состояние антивируса:

Получаем результат «powershell Get-MpComputerStatus» и разбираем его. Нас интересуют строки *AMServiceEnabled* и *ProductStatus*. Если есть подстрока *AMServiceEnabled: True*, то антивирус есть и включен, если значение False – то выключен, а если такое подстроки нет – то и антивирусника нет (речь идет про Microsoft Defender Antivirus). Обновление сигнатур определяется через *ProductStatus* (подробнее <https://learn.microsoft.com/en-us/graph/api/resources/intune-devices-windowsdefenderproductstatus?view=graph-rest-1.0> ), если имеется статус 524288, то ошибок нет, антивирус работает в штатном режиме и все сигнатуры обновлены. Так же если статус 1, то сигнатуры нуждаются в обновлении.

Для macOS через «/usr/bin/sweep -v» ищем антивирус Sophos.

Для Linux через «clamdscan --version» ищем антивирус Clamd.

* 1. Состояние сетевой защиты:

netsh advfirewall show allprofiles state > nul 2>&1– для Windows

sudo pfctl -sr > /dev/null 2>&1 – для Mac

ufw status | grep -i active > /dev/null 2>&1– для Linux

* 1. Состояние защиты диска:

manage-bde -status – для Windows. Ищем подстроку «Fully Encrypted»

fdesetup status – для Mac. Ищем подстроку «FileVault is On»

lsblk -o TYPE – для Linux. Ищем подстроку «crypt»

Важно заранее поставить вывод на en\_US(можно и ru\_RU), чтобы проверять можно было на одном языке.

BitLocker очень долго выводит результат из-за огромного количества проверок по диску и тяжеловесной криптографии под капотом.

* 1. Состояние обновления ОС:

wmic qfe list brief /format:table – для Windows. Выводит таблицу доступных обновлений. Остается лишь проверить количество столбцов в ней и если из больше 0, то обновления имеются.

softwareupdate -l - для Mac

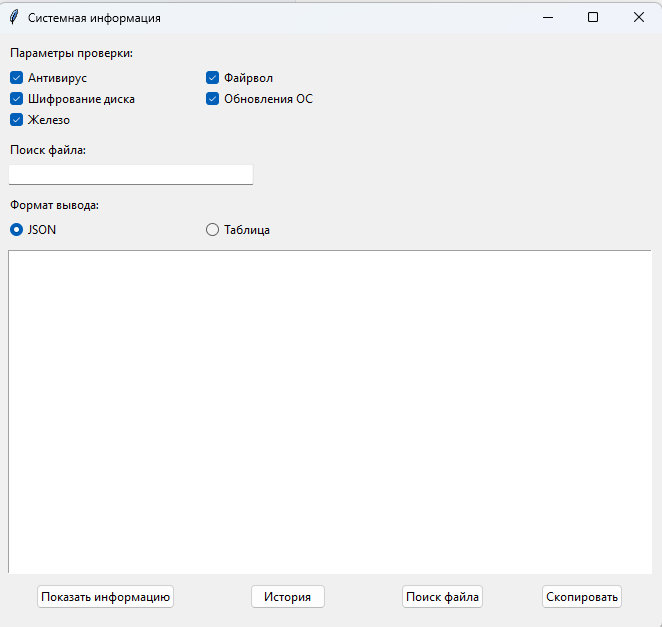
apt list –upgradable для Linux

* 1. Основная информация о hardware и процессор:

Сбор данных при помощи psutil и platform.

1. Файл для поиска необходимо указывать с расширением. В случае с PE будет также найдена их версия из VS\_VERSIONINFO внутри PE по полю ProductVersion, если она указана. Также стоит отметить, что поиск будет происходить по всему диску рекурсивно, так что процесс довольно ЗАТРАТНЫЙ по времени(как вариант можно использовать отдельный поток, чтобы само приложение не зависало, но стоит ли….).
2. GUI:

Собирается при помощи tkinter и имеет следующий вид:



Доступен просмотр истории, выбор необходимых сведений, которые будут выводится, представление как в виде таблицы, так и в виде JSON.