Для удобства работы создаем расшаренную папку и запрещаем в ней выполнение любых файлов (будет использоваться для хранения семплов и их сканирования без пересылки на виртуалку).

Антивирус Касперского:

1. Прописать папку с антивирусом в PATH
2. Команда: avp.com SCAN
3. Флаги:
   1. /i0 – выдать только репорт
   2. /RA:<report\_file> - сохранить все события в репорт
   3. /R:<report\_file> - сохранить только критические события

Можно добавить разные функции: скан памяти (/MEMORY), автозагрузка (/STARTUP) и т.д. типа на выбор.

Пример команды: avp.com SCAN "E:\Programs\ubuntu-16.04.7-desktop-amd64.iso" /i0 /RA:brokendick.txt

ESET:

1. Добавляем в PATH
2. Команда: ecls [опции] “имя\_файла”
3. Используем опции:
   1. /log\_file=LOGPATH(задает пользователь в настройках скрипта)
   2. /no\_quarantine – не пихаем в карантин
   3. /adv-heur – расширенная эвристика (разницы не заметил)

Windows Defender:

1. Будем обращаться не из Path, а напрямую через команду “%ProgramFiles%\Windows Defender\MpCmdRun.exe” -Scan -ScanType 3 -DisableRemediation -File “ПУТЬ К ФАЙЛУ”

По всей видимости, придется файл из шары копировать. Антивирусы не горят желанием сканировать проги из нее. Более того, надо запускать все команды от имени администратора.

Как мы запускаем кукушку:

- Из-под рута пишем: /home/cuckoo/cuckoo/bin/cuckoo rooter –sudo –group cuckoo

- Из-под куку-пользователя пишем: . ~/cuckoo/bin/activate и cuckoo –debug

VMCloak.

Чистый образ – finalone

Клон с надстройками – win7cuckoo