Pspy - Любопытный инструмент или инструмент для лыбопытных

Взято: из интернетов, автора установить не получилось.

На недавнем ZN, играя в CTF'чик, зайдя на хост, увидел любопытный инструмент - pspy64. Раньше такого не встречал.

Запустив, понял что этот инструмент находясь в *user space* показывает все запущенные процессы системы с их cmdline и т.д. (В том числе рутовые процессы и процессы других пользователей системы).

Понял что тут примешено чутка хакерской магии, т.к. просто дампнуть процессы пользователя root мы конечно же не можем. Я понимал, что можно спарсить /proc, но это не настолько подробно и мне казалось что это весьма долго.

Так вот, я решил почитать о нем и также захотелось рассказать вам. Опишу идею кратко, а вы если захотите разберетесь глубже.

Встречайте: https://github.com/DominicBreuker/pspy

pspy - unprivileged Linux process snooping

pspy - это инструмент командной строки, предназначенный для наблюдения за процессами без необходимости получения прав root. Он позволяет просматривать команды, запущенные другими пользователями, задания cron и т.д. по мере их выполнения. Отлично подходит для исследования систем Linux в CTF. Также отлично подходит для демонстрации коллегам, почему передача секретов в качестве аргументов в командной строке - плохая идея.

Как это работает

Существуют инструменты, позволяющие перечислить все процессы, выполняемые в системах Linux, включая те, которые завершились. Например, существует forkstat. Он получает уведомления от ядра о событиях, связанных с процессами, таких как fork и exec.

Эти инструменты требуют привилегий root, но это не должно вызывать у вас ложного чувства безопасности. Ничто не мешает вам подглядывать за процессами, запущенными в системе Linux. Много информации видно в procfs до тех пор, пока процесс запущен. Единственная проблема заключается в том, что вам нужно поймать недолговечные процессы за очень короткий промежуток времени, в течение которого они живы. Сканирование каталога /proc в поисках новых PID в бесконечном цикле делает этот трюк, но потребляет много CPU.

Более скрытный способ - использовать следующий трюк. Процессы обычно обращаются к таким файлам, как библиотеки в /usr, временные файлы в /tmp, файлы журналов в /var, … Используя API inotify, вы можете получать уведомления всякий раз, когда эти файлы создаются, изменяются, удаляются, к ним обращаются и т.д. Linux не требует прав привилегированных пользователей для работы с этим API, поскольку он необходим для многих невинных приложений (например, текстовых редакторов, показывающих актуальный проводник файлов). Таким образом, хотя пользователи без права root не могут напрямую следить за процессами, они могут следить за влиянием процессов на файловую систему.

Мы можем использовать события файловой системы как триггер для сканирования /proc, надеясь, что мы сможем сделать это достаточно быстро, чтобы поймать процессы. Именно это и делает pspy. Нет гарантии, что вы не пропустите ни одного процесса, но в моих экспериментах шансы кажутся высокими. В общем, чем дольше идут процессы, тем больше шансов их поймать.

Что сказать? Гениально!