Для проверки работоспособности bash-сценария необходимо провести эксперимент по подмене произвольного исполняемого файла.

Атака, направленная на подмену файлов подразумевает внедрение сторонних команд или данных в работающую систему и осуществляется злоумышленниками при помощи вредоносного ПО.

Вредоносное ПО - любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда, ущерба владельцу информации, или владельцу ЭВМ, путем копирования, искажения, удаления или подмены информации.

Распространяется подобное ПО как обычный вирус и заражение происходит при запуске исполняемого файла. В дальнейшем изменение исполняемых файлов системы может быть использовано для нарушения работы системы или получения несанкционированного доступа к данным.

В нашем случае для воссоздания вторжения в систему и изменения исполняемых файлов мы сделаем резервную копию произвольного исполняемого файла, а на его место переместим другой файл с идентичным названием, но содержанием, отличным от оригинала.

В результате мы воссоздали ситуацию, где при атаке на систему был подменен конфигурационный файл и теперь можем приступать к bash-сценарию, который уведомит администратора об изменении файлов.