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.

В нашем случае для воссоздания вторжения в систему и изменения исполняемых файлов был написан сценарий на bash следующего содержания:

```
#!/bin/bash
file="test"
fileOrig="/bin/nano"
fileCopy="/bin/nano1"
fileChanged=$fileOrig
sudo mv $fileOrig $fileCopy
echo $file > $fileChanged
```

В результате мы воссоздали ситуацию, где при атаке на систему был подменен конфигурационный файл и теперь можем приступать к bash-сценарию, который покажет нам изменения файла “ ” и уведомит об этом администратора по электронной почте.