Практическое задание № 6

Опубликована **07.11.2023**

Дедлайн **21.11.2023**

Задача 1:

1. Загрузить на машину с Metasploitable 2 и распаковать в папку /var/www следующий архив: lab01_nslookup.zip.

   После этого должна открываться ссылка: `http://xx.xx.xx.xx/nslookup.php`, где xx.xx.xx.xx — IP-адрес виртуальной машины с Metasploitable 2.

   Указание: для загрузки можно воспользоваться scp.

2. Выполнить свой код (полезную нагрузку) на целевой системе двумя способами. Получить удалённый доступ к машине двумя способами:

   (a) используя инъекцию команд OS

   (b) используя уязвимость Shellshock

3. Полезная нагрузка у студентов должна быть разной.

   Примеры: различные вариации бэкдоров, php-shell, загрузка и запуск инструментов по типу nmap/sqlmap/strike-back-backdoor/hydra/др.

4. Найти флаг для задания (логин/пароль для доступа - в Discord):
   `http://tasks.crypto-kantiana.com:10777/`

Замечания: в пункте 2.a вместо Metasploitable 2 можно использовать Windows или любой дистрибутив Linux с установленным и настроенным веб-сервером и PHP. Для пункта 2.b требуется дистрибутив Linux со старой версией bash.