МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** «Инженерно-экономический институт»

                                                  (название факультета/института)

**Кафедра** «Безопасности и информационных технологий»

            (название кафедры)

**ПРАКТИЧЕСКАЯ РАБОТА № 2**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема:** Hack the Box. Прохождение модуля «Fawn»

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | | 3 | | | курса | | |
| очной формы обучения | | | | | | |  |  |
| Группа №: | ИЭ-41-20 | | | | | | |  |
| ФИО: | [Ахтямов В.И.](https://app.hackthebox.com/users/80291) | | | | | | |  |
| Проверил |  | | | | | | |  |
| ФИО: | Шарафутдинов Р.Ф. | | | | | | |  |
| дата проверки: | « |  | | » |  | | 2023г. |  |
| Оценка: |  | | | | | | |  |

Москва, 2023

1. : Какое расшифровывается сокращение VM? Ответ: Виртуальная машина.
2. : Какой инструмент мы используем для взаимодействия с операционной системой, чтобы выполнять команды через командную строку, например, для запуска нашего VPN-соединения? Он также известен как консоль или оболочка. Ответ: Терминал.
3. : Какой сервис мы используем для установления VPN-соединения в лаборатории HTB? Ответ: OpenVPN.
4. : Какое сокращение используется для 'tunnel interface' в выводе запуска VPN-соединения? Ответ: tun.
5. : Какой инструмент мы используем для проверки соединения с целевой машиной с помощью запроса ICMP echo? Ответ: ping.
6. : Какое название у наиболее распространенного инструмента для нахождения открытых портов на целевой машине? Ответ: nmap.
7. : Какой сервис мы определяем на порту 23/tcp во время наших сканирований? Ответ: telnet.
8. : Какое имя пользователя может войти на целевую машину по протоколу telnet с пустым паролем? Ответ: root.

FTP открывает свою сессию для команд серверу, и возвращает номер ответа, после каждого запроса – например 230 – успешная авторизация

0) проверил работает ли машина ping 10.30.211.112

1)проверил открытые порты и подробную информацию о них – какая версия ftp + какая ОС на машине Nmap -sV 10.30.211.112

3)ftp 10.30.211.112

4) ввел логин не авторизованного пользователя ftp – anonymous, далее хоть и пароль запрашивался просто прожал enter

5) внутри был файл flag.txt, скачал его себе с помощью команды **get** flag.txt

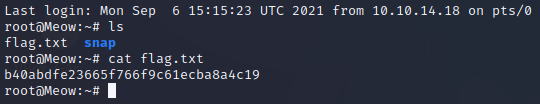


Рисунок 2 - Флаг