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 № 3**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | | 3 | | | курса | | |
| очной формы обучения | | | | | | |  |  |
| Группа №: | ИЭ-41-20 | | | | | | |  |
| ФИО: | Ахтямов В.И. | | | | | | |  |
| Проверил |  | | | | | | |  |
| ФИО: | Шарафутдинов Р.Ф. | | | | | | |  |
| дата проверки: | « |  | | » |  | | 2023г. |  |
| Оценка: |  | | | | | | |  |

Москва, 2023

1) What does the 3-letter acronym SMB stand for?

Что означает 3-буквенная аббревиатура SMB?

Ответ: Server Message Block

2) What port does SMB use to operate at?

Какой порт использует SMB для работы?

Ответ: 445

3) What is the service name for port 445 that came up in our Nmap scan?

Какое имя службы для порта 445 появилось при сканировании Nmap?

Ответ: microsoft-ds

4) What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share?

Какой "флаг" или "переключатель" мы можем использовать с помощью инструмента SMB для "перечисления" содержимого общего ресурса?

Ответ: -L

5) How many shares are there on Dancing?

Сколько акций на Dancing?

Ответ: 4

6) What is the name of the share we are able to access in the end with a blank password?

Как называется общий ресурс, к которому мы можем получить доступ в конце с пустым паролем?

Ответ: WorkShares

7) What is the command we can use within the SMB shell to download the files we find?

Какую команду мы можем использовать в оболочке SMB для загрузки найденных файлов?

Ответ: get

1. проверил работает ли машина ping 10.30.211.112
2. проверил открытые порты и подробную информацию о них – как называется порт 445 на машине Nmap -sV 10.30.211.112
3. smbclient 10.30.211.112 -L – показать все ресурсы, один из ресурсов – без доллара в конце – общий без пароля
4. sudo smbclient //10.129.123.210/WorkShares -N – подключился к ресурсы
5. dir или l – директории ресурса
6. в одной из директорий нашел текстовый файл flag.txt – скачал его командой get
7. далее не выходя из smb сессии с сервером ввел !cat flag.txt – чтобы посмотреть содержимое файла

