**Лабораторная работа по теме № 15. Настройка удаленного доступа в ОС Windows. Сниффинг.**

**Цель:** освоить навык организации удаленного управления по RDP и сниффинга.

**Задачи:**

1. включение и настройка удаленного управления на установленных ранее виртуальных машинах;
2. знакомство со структурой пакетов HTTP с помощью сниффинга.

**Порядок выполнения работы.**

1. Зайдите в «Панель управления», «Система», «Настройка удаленного доступа» и установите переключатель в положение «Разрешить удаленные подключения к этому компьютеру».
2. Зайдите в редактор реестра, откройте раздел HKEY\_LOCAL\_MACHINE\ System\ CurrentControlSet\ Control\ Terminal Server\ WinStations\ RDP-Tcp\ и установите значение параметра PortNumber равным

10000 + <число рождения> \* 100 + <месяц рождения>

1. В бранмауэре создайте правило для разрешения входящих подключений на указанный для RDP порт.
2. Скопируйте на виртуальную машину с файлового сервера по имени «A246K401» или IP-адресам «172.16.0.38» или «172.16.192.252» из папки «!admin\2» установочный пакет «Wireshark-win64-3.2.1.exe» и установите его. Логин: user, пароль: 777.
3. Переключите сетевые адаптеры созданных ранее виртуальных машин в режим «Виртуальный адаптер хоста».
4. Запустите (перезапустите) виртуальные машины и определите назначенные им IP-адреса.
5. Включите захват пакетов с помощью Wireshark на виртуальной машине.
6. Подключитесь с помощью приложения «Подключение к удаленному рабочему столу» физической машины по IP-адресу и порту к виртуальной машине.
7. Запустите и откройте учебные веб-приложения из лабораторной работы №1, нажмите обе кнопки.
8. Остановите захват пакетов в Wireshark, выполните фильтрацию захваченных пакетов путем ввода «http» в строку фильтрации.
9. Ознакомьтесь со структурой HTTP-пакетов и порядком отправки запросов и получения ответов в веб-приложениях.

**Порядок защиты лабораторной работы.**

1. Зайдите с физической машины на виртуальную по RDP.
2. Продемонстрируйте захватываемые при работе с веб-приложениями из лабораторной работы №1 пакеты в Wireshark.
3. Опишите структуру и виды http-пакетов.