МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**Исследование сетевых атак на VPN, VNC, RDP**

отчёт по лабораторной работе №8

по курсу «Системы обнаружения вторжений»

Выполнили: студенты гр. 230781 \_\_\_\_\_\_\_\_\_ Глейм С.М.

(подпись)

\_\_\_\_\_\_\_\_\_ Ивлев А.Р.

(подпись)

Проверил: асс. каф. ИБ \_\_\_\_\_\_\_\_\_ Чаговец С.Н.

(подпись)

Тула, 2022 г.

**Цель работы**

Изучение и исследование особенностей сетевых и локальных атак на службы VPN, VNC, RDP. Способы идентификации и противодействия атакам данного вида.

**Задание на работу**

1. Скачать из Internet программу VNC-сервер и клиент (например, UltraVNC), установить и настроить серверную и клиентские части на тестовые ПК, рекомендуется использовать виртуальные машины.
2. С помощью программы снифера (WireShark) прослушать трафик VNC. сохранить передаваемый хеш пароля с клиентской станции на сервер VNC. Используя программу VNC Crack из дистрибутива Kali Linux попытаться установить пароль VNC.
3. Использовать программу VNC Crack для установления пароля VNC, сохранённого в конфигурационном файле.
4. На виртуальной машине создать учётную запись с привилегиями для работы с удалёнными рабочими столами и паролем из словаря, поставляемого с дистрибутивом kali Linux. используя пакет crowbar из дистрибутива Kali Linux попытаться выполнить брутфорс-атаку по словарю на уязвимый RDP сервис.

**Ход работы**

С помощью программы-сниффера в смоделированной виртуальной локальной сети были перехвачены необходимые пакеты.

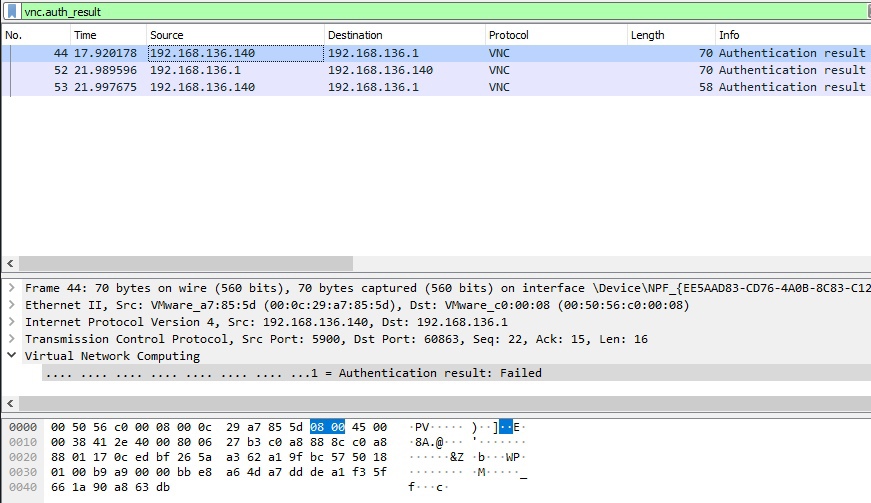


Рисунок 1 - Перехваченные пакеты

Перехваченные хеш-значения (последние 16 байт последних двух перехваченных пакетов на рисунке 1):

bbe8a64da7dddea1f35f661a90a863db – хеш-значение вызова

622c782f7c8ae78e873bedb4df8f89b7 – хеш-значение ответа

Затем с помощью программы vncrack\_s, перхваченных хеш-значений и словаря паролей rockyou.txt был получен пароль на подключение к vnc-серверу

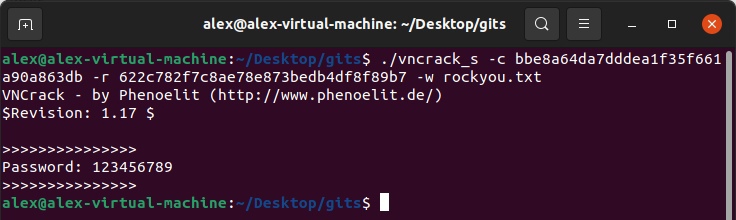


Рисунок 2 – Подбор пароля к vnc-серверу с помощью vncrack\_s

После на отдельной виртуальной машине был установлен vnc-сервер tightvncserver. С помощью программы vncrack\_s был раскрыт пароль, находящийся в файле ~/.vnc/passwd.



Рисунок 3 – Пример использования программы vncrack

Для атаки на rdp было организовано rdp-соединение между атакующей и атакуемой машинами. С помощью программы crowbar и словаря rockyou.txt был подобран пароль для пользователя rdp.



Рисунок 4 - Пример использования программы crowbar

**Вывод**

Были изучены и исследованы особенности сетевых и локальных атак на службы VNC, RDP. Атаки на данные службы основаны на подборе пароля доступа к атакуемому хосту. Для проведения успешной атаки на данные службы достаточно найти хороший список паролей.