

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА-Российский технологический университет»**

**Институт:** Институт кибербезопасности и цифровых технологий **Специальность(направление): 09**.03.02 «Информационные системы и технологии»

**Кафедра:** КБ-14 «Цифровые технологии обработки данных» **Дисциплина:** Методы и средства защиты информации

**ОТЧЕТ ПО**

**ПРАКТИЧЕСКОЙ РАБОТЕ №3**

Honeypot

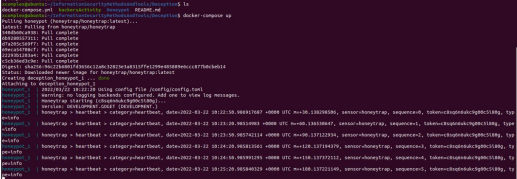
Выполнил студент группы

БСБО-06-20

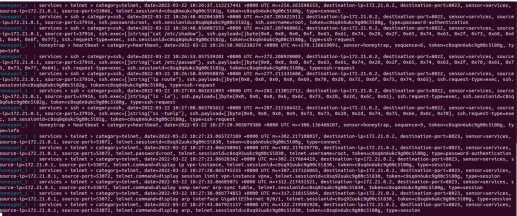
*Ибрахим.Х.К*

**Москва 2022г.**

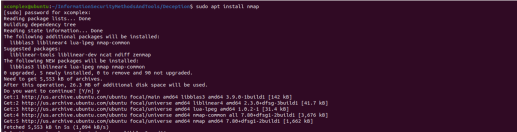
Первый раз с ошибкой, во второй нормально

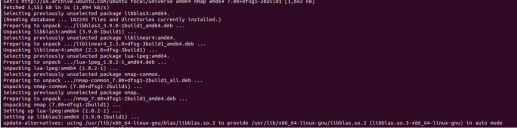


Запуск симулятора злоумшленика и Логи

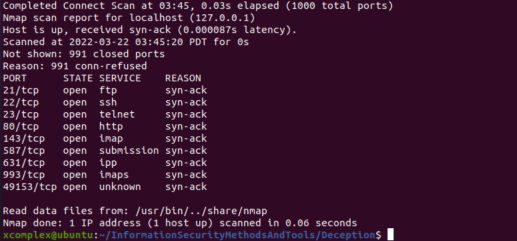
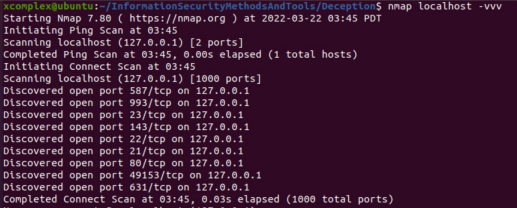


Подключение утилиты nmap

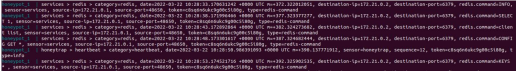




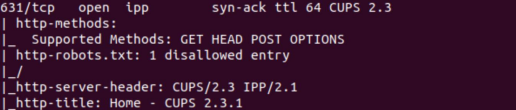
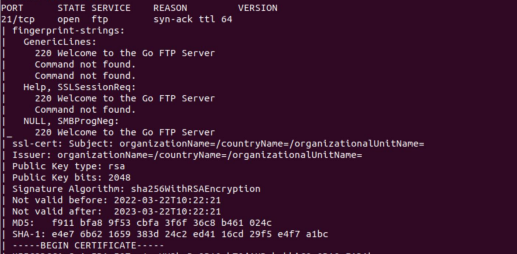
Honeypot



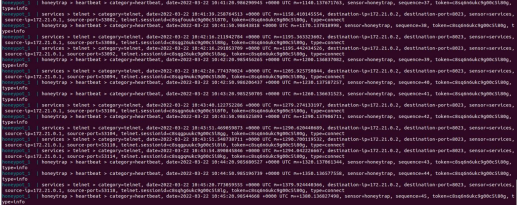
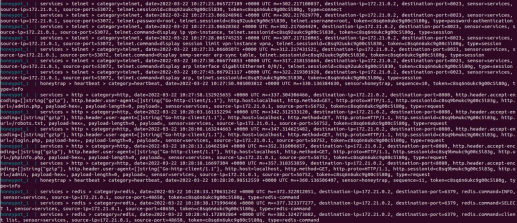
Данный список не отражает только honeypot redis



Подробная информация



Действия hackersActivity



.connect – подключение

.password-authentication – аутентификация





redis

-redis.command=INFO

-redis.command=SELECT 1

-redis.command=client list

-redis.command=CONFIG GET \*

-redis.command=KEYS

ftp

-ftp.command=USER anonymous -ftp.command=PASS anonymous -ftp.command=FEAT

-ftp.command=LIST -l

-ftp.command=STOR /etc/passwd -ftp.command=PWD

-ftp.command=HELP

-ftp.command=APPE /exploit.sh