Министерство образования Республики Беларусь

Учреждение образования

"Белорусский государственный университет информатики и радиоэлектроники"

Кафедра защиты информации

Лабораторная работа №7-8

«СОЗДАНИЕ И НАСТРОЙКА ВИРТУАЛЬНЫХ МАШИН В ORACLE VM VIRTUALBOX

УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА MHN И РАЗВЕРТЫВАНИЕ HONEYPOTS НА ВИРТУАЛЬНЫХ МАШИНАХ»

|  |  |
| --- | --- |
| Выполнили:  ст.гр.961401  Савченко Е.А.  Савич О.А. | Проверил:  Лобунов В.В. |

Минск 2022

**Цель:** Ознакомиться с программой для создания виртуальных машин Oracle VM VirtualBox. Изучить устройство виртуальной машины. Ознакомиться с операционной системой Linux. Установить дистрибутив Ubuntu 18.04 на виртуальную машину. Ознакомиться с «ловушками»-honeypot и программным комплексом MHN. Установить и настроить MHN и honeypots на виртуальных машинах. Для проверки результатов работы honeypots ознакомиться и установить необходимое программное обеспечение на атакующую виртуальную машину.

Рисунок 1 – Тест honeypot Cowrie с помощью программы medusa

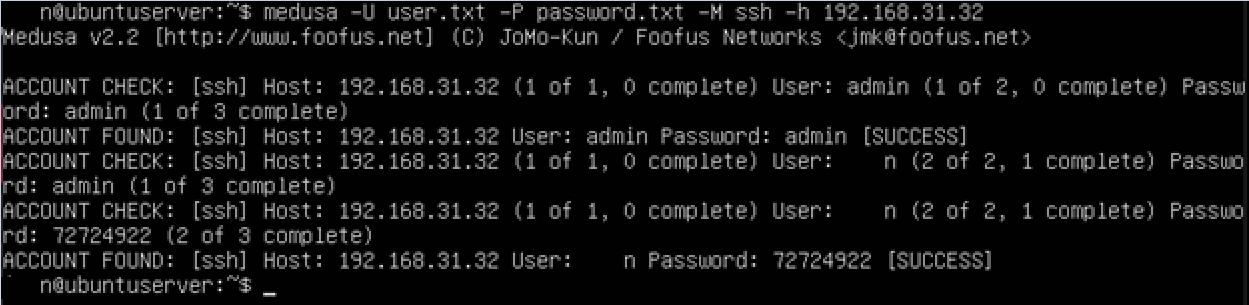


Рисунок 2 – Получение доступа к Cowrie по ssh с помощью данных аутентификации, полученных при брутфорс-атаке:



Рисунок 3 – Результаты атаки в Web приложении MHN сервере, логи на сервере Cowrie, описывающие действия нарущителя:

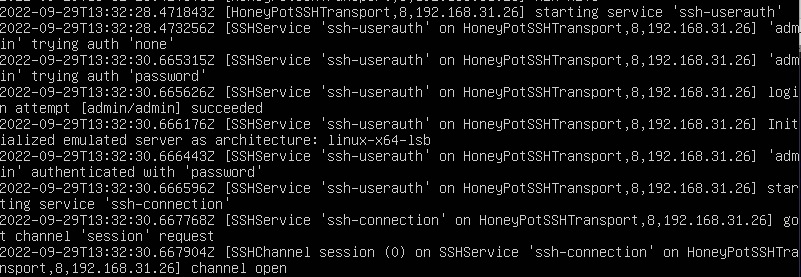


Рисунок 4 –Результаты сетевого сканирования honeypot Dionaea посредством nmap:

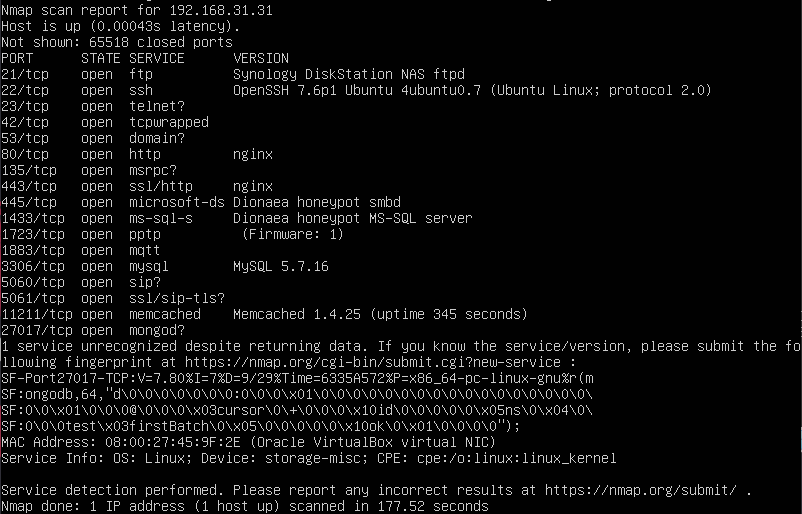


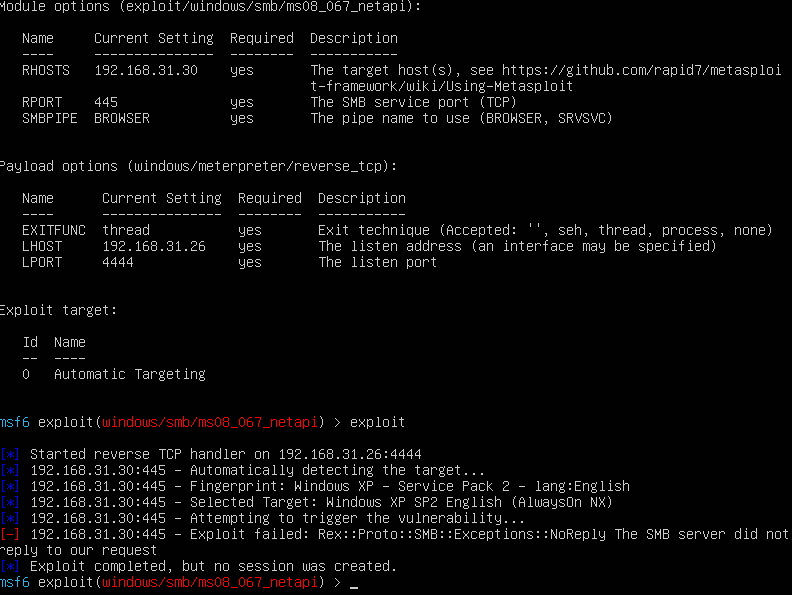
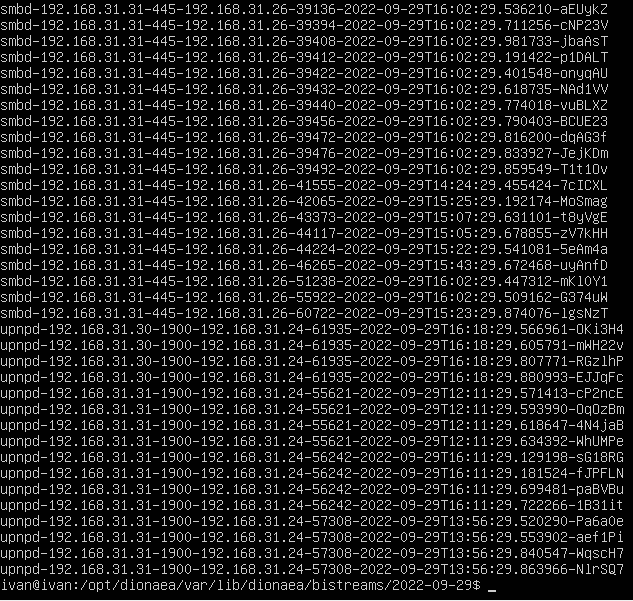
Рисунок 5 – Попытка воспользоваться уязвимостью протокола SMB(Samba) на 445 порте через программу доставки Metasploit:

Рисунок 6 – Файлы с перехваченными от атакующего данными в бинарном виде:



**` Вывод:** по итогу выполнения лабораторной работы были созданы и настроены виртуальные машины на базе OC Ubuntu Linux, на которые были установленные различные системы типа honeypot, а также продемонстрирован их функционал и главные задачи.

Контрольные вопросы:

1. Технология Honeypot - ресурс безопасности, назначение которого состоит в том, чтобы стать исследованным или подвергшимся нападению. Как правило, honeypot может быть имитируемым сервисом либо полноценной операционной системой. Honeypots можно классифицировать на основе их развертывания и исходя из уровня использования. Основываясь на развертывании, honeypot можно классифицировать как: • производственные; • исследовательские.

Основываясь на критериях проектирования, honeypots можно классифицировать как: • простые honeypots; • высокопоточные honeypots; • honeypots с низким взаимодействие.

MHN – это проект с отрытым исходным кодом, который упрощает развертывание сенсоров honeypot и сбор статистических данных в любом масштабе для создания сети honeynet.

1. Nmap – эта программа является одной из наиболее распространенных в среде пользователей Linux и отличается мощным инструментарием и высокой скоростью работы. Nmap может определять большинство основных параметров сетевого адаптера: MAC-адрес, имя компьютера в домене, открытые порты, порты, закрытые брандмауэром, компанию — производителя чипсета сетевого адаптера исследуемого компьютера, версии ОС и служб.

Medusa — это быстрый, параллельный и модульный брут-форсер входа. Цель заключается в поддержке такого количество служб, на которых возможна удалённая аутентификация.

1. Metasploit – это платформа для тестирования на проникновение, с которой вы можете находить, эксплуатировать и подтверждать уязвимости. Metasploit позволяет имитировать сетевую атаку и выявлять уязвимости системы, проверить эффективность работы IDS/IPS, или разрабатывать новые эксплоиты (код с помощью которого злоумышленник может взломать систему, программу и т.п., у которой есть уязвимость) с созданием подробного отчета.
2. Эксплоиты – код с помощью которого злоумышленник может взломать систему, программу и т.п., у которой есть уязвимость. Брутфорс – техника взлома систем защиты с возможностью аутентификации заключающаяся в прямолинейном и последовательном переборе возможных наборов данных аутентификации.
3. Полезная нагрузка это исполняемый файл, который может предоставить доступ злоумышленнику, а также расширить его привелегии внутри системы или открыть уязвимости для загрузки более весомых эксплойтов.
4. Dionaea представляет доступ к сетевым сервисам и позволяет перехватить и сохранить любой файл, отправленный на эти сервисы злоумышленником.
5. **SSH**  — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов).