Лабораторная работа. Honeypot, Nmap

Оглавление

[Основные теоретические сведения 1](#_Toc58317412)

[Nmap 1](#_Toc58317413)

[Honeypot 3](#_Toc58317414)

[Honeyd 4](#_Toc58317415)

[**Описание выполнения лабораторной работы** 6](#_Toc58317416)

[Часть 1 6](#_Toc58317417)

[Часть 2 6](#_Toc58317418)

[Вопросы к лабораторной работе 7](#_Toc58317419)

[Содержание отчета по лабораторной работе 7](#_Toc58317420)

[Варианты работ 7](#_Toc58317421)

# Основные теоретические сведения

Цель: Получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети

## Nmap

Существует несколько средств сканирования Nmap, широко применяемых в настоящее время. Рассмотрим некоторые из них.

**TCP Connect()**

Второй доступный метод сканирования - TCP Connect. Он заключается в том, что сканирующая машина пытается установить соединение со сканируемой. Успешный результат говорит о том, что порт открыт, неудачный — о том, что он закрыт или фильтруется. Это сканирование легко обнаруживается по огромному количеству записей в log-файле неудачных попыток установления соединения и ошибок исполнения этой операции. Понятно, что средства защиты с максимальным быстродействием заблокируют адрес, вызывающий ошибки.

nmap –sT 192.168.58.103

-v: Увеличить уровень вербальности (задать дважды или более для увеличения эффекта)

**TCP-SYN**

Более совершенным методом сканирования является TCP SYN — так называемое «полуоткрытое сканирование». При вызове Nmap посылает SYN-пакет, как бы ради того, чтобы установить новое соединение. Если в ответе присутствуют флаги SYN или ACK, считается, что порт открыт. Флаг RST говорит об обратном. Если пришел ответ, говорящий о том, что порт открыт, nmap незамедлительно отправляет RST-пакет для сброса еще не установленного соединения. Сканирование осуществляется только при наличии прав суперпользователя (root).

nmap –sS 192.168.58.103

**Сканирования FIN, Xmas Tree и NULL**

Тем не менее, межсетевой экран или другие защитные средства могут ожидать приходящие SYN-пакеты. Из-за этого зачастую такой метод сканирования не дает результата. Поэтому существует еще целая группа возможных способов сканирования, альтернативных TCP SYN. Это FIN, Xmas Tree и NULL-сканирования. Большинство операционных систем по умолчанию, согласно рекомендациям, должны ответить на такие пакеты, прибывшие на закрытые порты флагом RST. Важная деталь: ни одна операционная система семейства Windows никогда не ответит RST пакетом на пришедший FIN, XmasTree или NULL пакет. Используя этот факт даже при подобных, в общем-то, не особо детальных сканированиях можно предположить, как минимум семейство операционных систем.

nmap –sF 192.168.58.103

nmap –sX 192.168.58.103

nmap –sN 192.168.58.103

**Сканирование протоколов IP**

Метод заключается в том, что хосту передаются IP пакеты без заголовков для каждого протокола сканируемого хоста. Если получено сообщение, говорящее о недоступности протокола, то этот протокол не поддерживается хостом. В противном случае — поддерживается.

nmap –sO 192.168.58.103

**ACK-сканирование**

ACK сканирование заключается в передаче ACK пакетов на сканируемый порт. Если в ответ приходит RST пакет, порт классифицируется как не фильтруемый. Если нет ответа или пришел ответ в форме ICMP-сообщения о недоступности порта, порт считается фильтруемым. Этот метод никогда не покажет состояние порта «открыт».

nmap –sA 192.168.58.103

**TCP Window**

TCP Window — похоже на ACK сканирование, однако по значениям поля Initial Window TCP-пакета пришедшего в ответ, можно определить открытые порты.

nmap –sW 192.168.58.103

**RPC-сканирование**

RPC-сканирование используется для определения программы, обслуживающей порт и её версии, и заключается в «затоплении» NULL- пакетами оболочки SunRPC открытых TCP или UDP портов хоста.

nmap –sR 192.168.58.103

**Сканирование ОС**

И, наконец, последнее — сканирование, используемое для определения ОС на сканируемом хосте.

nmap –O 192.168.58.103

## Honeypot

Honeypot («Ловушка») - ресурс, представляющий собой приманку для злоумышленников.

Фактически основная задача Honeypot — подвергнуться атаке или несанкционированному сканированию с целью изучения стратегии и методов сканирования и определения перечня средств, необходимых для предотвращения будущих атак. Суть работы Honeypot заключается в создании ловушек — образов систем, которые извне воспринимаются как полноценные машины с установленными на них операционными системами, а, следовательно, поддающиеся сканированию.

Использование Honeypot имеет практический и исследовательский смысл. Во-первых, если на сервере установлена хорошая система защиты, долгое время можно не замечать постоянных попыток сканирования — Honeypot укажет на их наличие. Во-вторых, серьезной проблемой специалистов по информационной безопасности является нехватка информации о методах и средствах, используемых злоумышленниками. Единственное, что позволяет получить информацию об этих средствах — испытание их действия на себе. И Honeypot является чуть ли не идеальным способом для этого, ведь в настоящее время этом точно известно: грамотно настроенный Honeypot практически невозможно распознать.

Следует отметить, что в условиях, в которых проводится лабораторная работа, придется отойти от реальной ситуации, когда хакеру неизвестно ничего о том, что из себя представляет сервер и не являются ли подключенные к нему машины всего лишь ловушками. Иными словами, нам будут известны ip-адреса сканируемых ловушек.

Для начала необходимо создать локальную сеть из двух машин. Рекомендуется использовать машины с установленными на них операционными системами Ubuntu Server. Далее необходимо разобраться непосредственно с ловушками.



На виртуальную машину «Hacker» необходимо установить Nmap (либо в случае с операционной системой с графической оболочкой - Zenmap) . На виртуальную машину «Server» установить и настроить Honeyd.

**Для выполнения данной работы на виртуальных машинах уже установлен весь необходимый софт.**

## Honeyd

**Установка**

Установка Honeyd. <sudo apt-get install honeyd>.

Установка Farpd. <sudo apt-get install farpd>.

Так же для Honeyd необходимо установить следующие пакеты:

libevent - event notification

libdnet - packet creation

libpcap - packet sniffing

**Настройка**

Настройка Honeyd осуществляется путем изменения конфигурационного файла **honeyd.conf**.

После установки Honeyd появится файл /etc/honeypot/honeyd.conf со стандартными настройками. Вы можете изменить настройки в этом файле на свои. Или же, создать свой конфигурационный файл с настройками и при запуске указывать его.

Пример настройки:

create default

set default default tcp action block

set default default udp action block

set default default icmp action block

create windows

set windows personality "Microsoft Windows XP Professional SP1"

set windows default tcp action reset

add windows tcp port 135 open

add windows tcp port 139 open

add windows tcp port 445 open

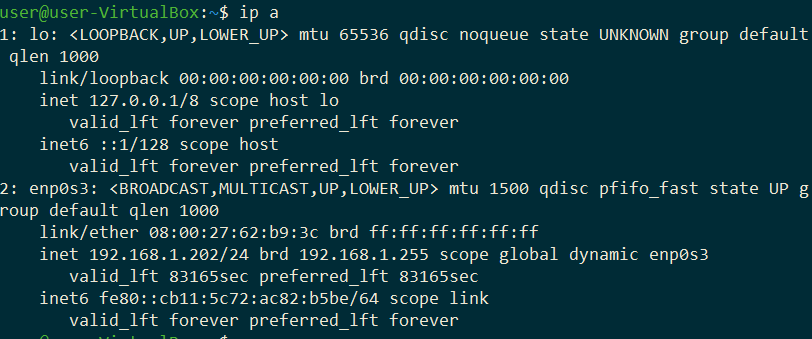
set windows ethernet "00:00:24:ab:8c:12"

bind 192.168.1.117 windows

В виртуальной машине уже есть готовый файл с настройками и желательно его внимательно изучить перед изменением.

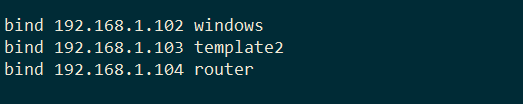
Для выполнения лабораторной работы необходимо внести правки в ip-адреса виртуальных ловушек. Для этого необходимо узнать ip-адрес на вашей виртуальной машине.

Выполним команду «ip a»



Здесь можно увидеть, что у виртуальной машины адрес 192.168.1.202/24

В конце файла настроек «/etc/honeypot/honeyd.conf» необходимо настроить ip адреса виртуальных точек в том же диапазоне, что и ip адрес виртуальной машины. Например, как на картинке ниже:



После этого на сервере необходимо запустить Honeypot ( можно с записью информации о работе в log-файл, либо без неё (см. ниже)). При этом будет осуществляться сканирование ip-адресов (либо отдельных, либо интервала) с помощью средств Nmap.

sudo honeyd -d -f [путь к файлу honeypot.conf]

или

sudo honeyd -d -f [путь к файлу honeypot.conf] -l [путь к log-файлу]

# **Описание выполнения лабораторной работы**

## Часть 1

1. Лабораторная работа выполняется на готовой виртуальной машине “Linux-honey”.
2. Создать копию виртуальной машины “Linux-honey”
3. Обе машины можно запустить: **логин – user, пароль - 1234567**
4. Создать изолированную сеть согласно индивидуальному заданию.
5. Обе виртуальные машины подключить к “Nat” сети
6. Определите IP адреса виртуальных машин и внести в отчет.
7. Произведите изучение средств сканирования Nmap
8. Установите Honeyd (Не требуется для выполнения на готовых ВМ).
9. Ознакомьтесь с информацией по настройке Honeyd и стандартным содержимым файла /etc/honeypot/honeyd.conf.
10. Настройте Honeypot изменив содержание файла /etc/honeypot/honeyd.conf (настройки виртуальных узлов должны быть в подсети согласно индивидульному заданию .
11. Запустите на первой виртуальной машине в новом терминале <sudo farpd -d>.
12. Запустите на первой виртуальной машине honeyd. <sudo honeyd -d -f /etc/honeypot/honeyd.conf>
13. Произведите сканирование вашей сети с honeypot со второй виртуальной машине утилитой nmap всеми типами сканирования. Прокомментируйте результат сканирования в отчете.
14. Измените настройки Honeypot. Усложните конфигурационный файл. Добавьте 2 дополнительные ловушки, измените информацию об ОC, информацию о роутере, об открытых портах и.т.д..
15. Запустите honeyd с новыми настройками. <honeyd -d -f /etc/honeypot/honeyd.conf>
16. Произведите сканирование nmap. Убедитесь, что ваши изменения конфигурации honeyd вошли в новое сканирование.
17. Прокомментируйте результаты всех сканирований в отчете.

## Часть 2

Данную часть можно выполнять из одной из виртуальных машин или на вашем персональном компьютере. Для выполнения на персональном компьютере необходимо дополнительно установить утилиты wireshark и nmap

1. Убедитесь, что у вас есть доступ в интернет.
2. Запустите анализатор трафика wireshark
3. Проведите сканирование ip адреса 195.208.245.253

nmap -T4 -A -v 195.208.245.253

1. Отфильтруйте пакеты, связанные с протоколом FTP
2. Проанализируйте пакеты и прокомментируйте в отчете
3. Какой логин и пароль были использованы для сканирования FTP – сервера?

# Вопросы к лабораторной работе

1. Что такое статический и динамический IP-адреса? В чём разница?
2. В чём заключается метод сканирование протоколов IP?
3. На какие пакеты большинство ОС должны ответить флагом RST?
4. Назначение, цели, описание Honeypot.
5. Какие цели может преследовать злоумышленник, взламывая сервера?
6. Как выявлять Honeypot?
7. Перечислите основные методы сканирования Nmap.

# Содержание отчета по лабораторной работе

1. **За копирование отчета другого студента (вами или вашего отчета) автоматом 0 балов без возможности пересдачи**

1. Название (титульная страница) и цель работы.
2. Номер вашего варианта с параметрами подсетей.

2. Поэтапное описание процесса работы со скринами и комментариями

3. Выводы по выполненной работе.

# Варианты работ

1. Сеть NAT 192.168.10.0/27

Gateway 192.168.10.10

DNS 192.168.10.10

DHCP – работает

1. Сеть NAT 10.10.10.0/27

Gateway 10.10.10.10

DNS 10.10.10.10

DHCP – работает

1. Сеть NAT 10.10.10.0/26

Gateway 10.10.10.10

DNS 10.10.10.10

DHCP – работает

1. Сеть NAT 10.11.10.0/25

Gateway 10.11.10.10

DNS 10.11.10.10

DHCP – работает

1. Сеть NAT 10.12.10.0/24

Gateway 10.12.10.10

DNS 10.12.10.10

DHCP – работает

1. Сеть NAT 10.13.10.0/24

Gateway 10.13.10.10

DNS 10.13.10.10

DHCP – работает

1. Сеть NAT 10.13.10.0/24

Gateway 10.13.10.10

DNS 10.13.10.10

DHCP – работает

1. Сеть NAT 10.14.10.0/25

Gateway 10.14.10.10

DNS 10.14.10.10

DHCP – работает

1. Сеть NAT 10.15.10.0/26

Gateway 10.15.10.10

DNS 10.15.10.10

DHCP – работает

1. Сеть NAT 10.16.10.0/27

Gateway 10.16.10.10

DNS 10.16.10.10

DHCP – работает

1. Сеть NAT 10.17.10.0/28

Gateway 10.17.10.10

DNS 10.17.10.10

DHCP – работает

1. Сеть NAT 10.18.10.0/27

Gateway 10.18.10.10

DNS 10.18.10.10

DHCP – работает