* **[Лабораторная работа №7. Honeypot, Nmap.](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html)**
  + [**Основные теоретические сведения**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#id1)
    - [**Настройка сети в VirtualBox**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#virtualbox)
    - [**Nmap**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#nmap)
    - [**Honeypot**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#honeypot)
    - [**Honeyd**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#honeyd)
  + [**Задания к лабораторной работе**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#id5)
  + [**Вопросы к лабораторной работе**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr7.html#id6)

**Лабораторная работа №7. Honeypot, Nmap.**

**Основные теоретические сведения**

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

**IP-адрес** - уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети.

**Примечание**

**IPv4**. В 4-й версии IP-адрес представляет собой 32-битовое число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел значением от 0 до 255, разделённых точками, например, 192.168.0.3.

**IPv6**. В 6-й версии IP-адрес (IPv6) является 128-битовым. Внутри адреса разделителем является двоеточие (напр. 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Ведущие нули допускается в записи опускать. Нулевые группы, идущие подряд, могут быть опущены, вместо них ставится двойное двоеточие (fe80:0:0:0:0:0:0:1 можно записать как fe80::1). Более одного такого пропуска в адресе не допускается.

**MAC-адрес** (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя фрейма, и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать MAC-адрес.

**Маска сети** - битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети (при этом, в отличие от IP-адреса, маска подсети не является частью IP-пакета). Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0 с длиной префикса 24 бита. В случае адресации IPv6 адрес 2001:0DB8:1:0:6C1F:A78A:3CB5:1ADD с длиной префикса 32 бита (/32) находится в сети 2001:0DB8::/32.

Другой вариант определения — это определение подсети IP-адресов. Например, с помощью маски подсети можно сказать, что один диапазон IP-адресов будет в одной подсети, а другой диапазон соответственно в другой подсети.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И).

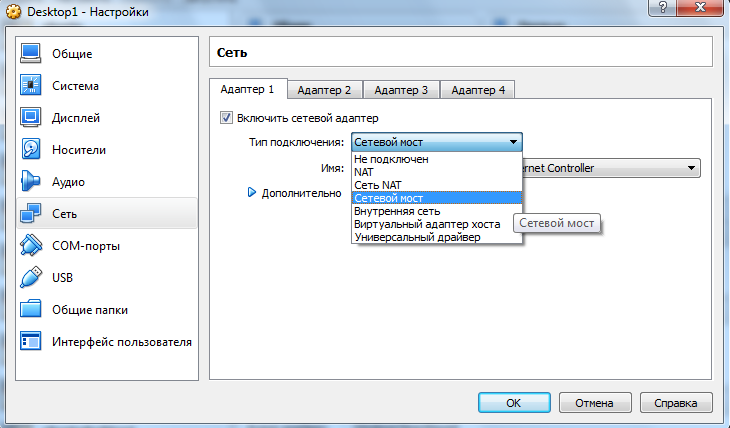
IP-адрес называют **статическим** (постоянным, неизменяемым), если он назначается пользователем в настройках устройства, либо если назначается автоматически при подключении устройства к сети и не может быть присвоен другому устройству.

IP-адрес называют **динамическим** (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, указанного в сервисе назначавшего IP-адрес (DHCP).

**DHCP** - сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

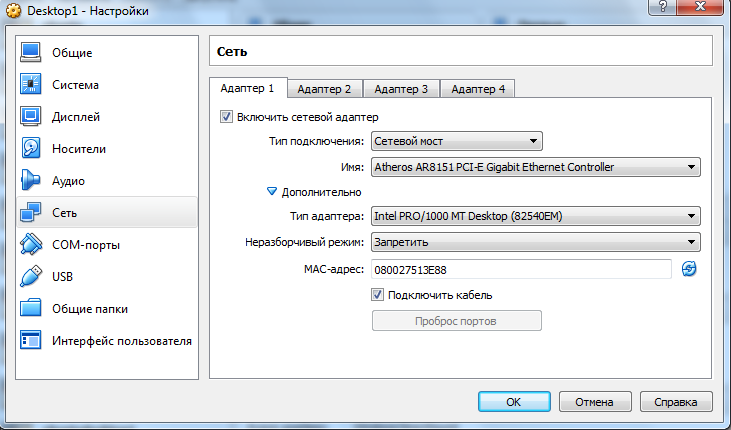
**Настройка сети в VirtualBox**

Чтобы изменить настройки сети для виртуальной машины в VirtualBox, выберите машину, нажмите **Настройки** и перейдите на вкладку сеть.



Существуют следующие варианты настройки сети в VirtualBox:

* NAT
* Сеть NAT
* Сетевой мост
* Внутренняя сеть
* Виртуальный адаптер хоста
* Универсальный драйвер



**Предупреждение**

Здесь стоит обратить внимание на MAC-адрес (Может понадобится для выполнения лабораторных работ). Если вы **«клонировали»** машину, здесь нужно изменить MAC-адрес на новый.

Можно подключить к виртуальной машине еще 3 виртуальных адаптера. Настройки для них, выглядят так же, как и для «Адаптера 1».

Кроме этих настроек, есть еще настройки для сети NAT и Виртуального адаптера хоста. Чтобы получить к ним доступ, нажмите *Файл/Настройки* и перейдите на вкладку сеть.

**Предупреждение**

Для выполнения лабораторной работы рекомендуется выбрать тип подключения **«Сетевой мост»** на обоих машинах.

Подробнее о настройке сети в VirtualBox можно прочитать [на сайте VirtualBox](https://www.virtualbox.org/manual/ch06.html).

**Nmap**

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

**Ping-сканирование**

Самым распространенным и простым способом сканирования является простое ping-сканирование, которое заключается в отправке ICMP пакетов на разные хосты. Хост, который активен, ответит на эти пакеты. Форма подачи запроса:

ping 192.168.58.103

Если хост активен, то будет периодически выводиться строка вида:

64 bytes from 192.168.58.103: icmp\_seq=1 ttl=64 time=0,284mc

**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



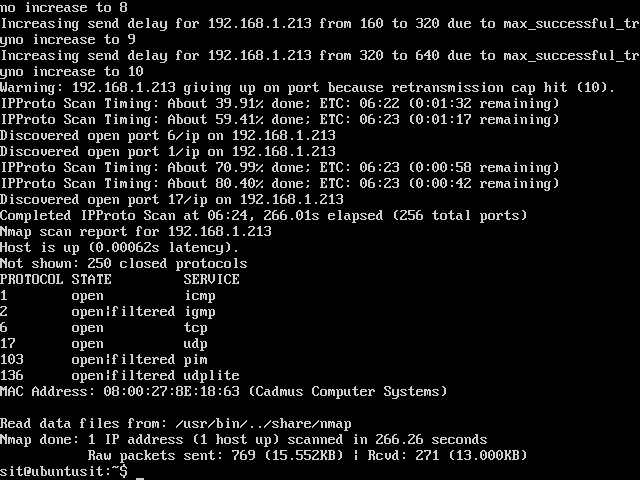
nmap –sN 192.168.58.103



**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.

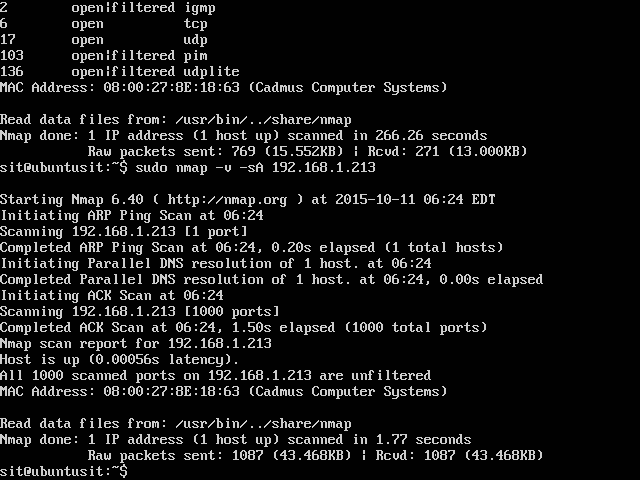
nmap –sO 192.168.58.103



**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».

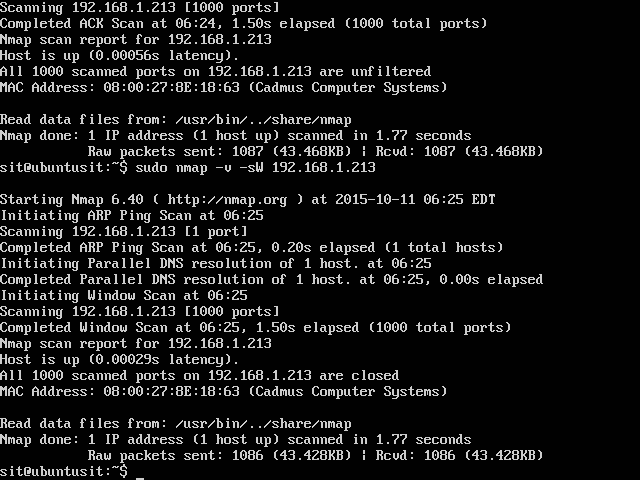
nmap –sA 192.168.58.103



**TCP Window**

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

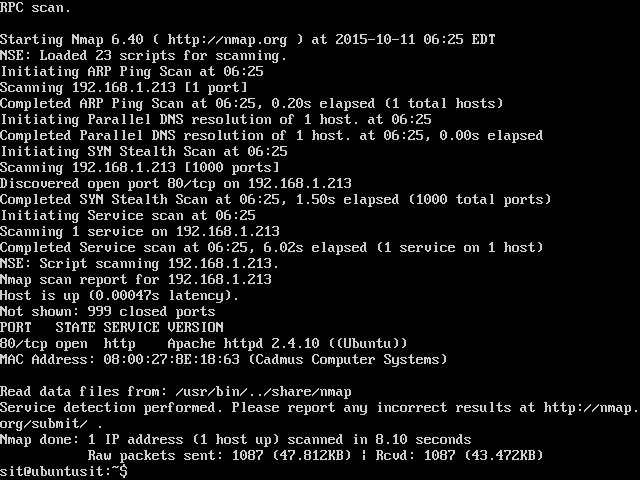
nmap –sW 192.168.58.103



**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.

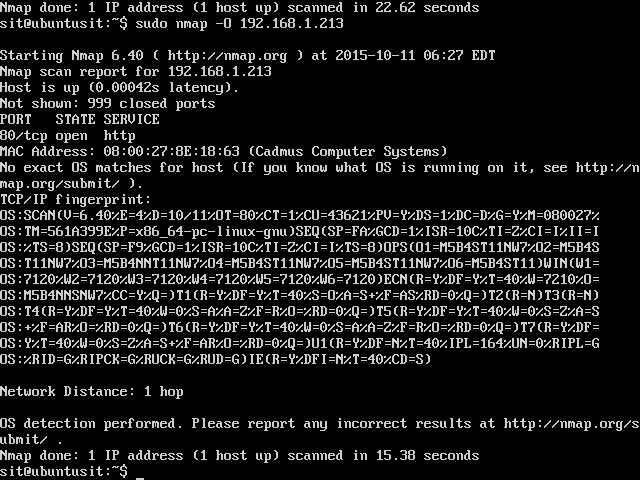
nmap –sR 192.168.58.103



**Сканирование ОС**

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

nmap –O 192.168.58.103



На этом cкриншоте Nmap не удалось определить ОС. Так что просканируем другую систему.



Существует еще несколько методов сканирования Nmap, однако в условиях проведения данной лабораторной работы осуществить их не получится.

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

**Предупреждение**

Однако на некоторых машинах при сканировании может появиться проблема: ни одна из ловушек не видна ни хостовой операционной системе, ни хакеру, ни самому серверу. В этом случае на помощь приходит команда **arp**, выполняемая с терминала хостовой машины. Синтаксис:

arp -s [ip-адрес ловушки] [mac-адрес адаптера]

Mac-адрес можно легко узнать либо в настройках VirtualBox, либо с помощью команды ifconfig. То же самое необходимо сделать и с машиной хакера.

**Honeyd**

**Установка**

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

**Предупреждение**

Если honeyd отсутствует в репозиториях, его можно скачать ([\*.deb](http://archive.ubuntu.com/ubuntu/pool/universe/h/honeyd/honeyd_1.5c-8ubuntu1_amd64.deb) пакет) и установить. Так же, можно скачать исходные коды honeyd с [официального сайта](http://www.honeyd.org/release.php) и их скомпилировать.

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

Эта конфигурация с одной ловушкой. При сканировании будет выведен MAC-адрес, указанный в honeyd.conf, а процесс, запущенный на машине с Honeypot укажет, что был выведен этот адрес.

[Здесь](http://www.honeyd.org/configuration.php) можно найти конфигурационный файл с подробным описанием. Он поможет настроить собственную конфигурацию при необходимости.

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.

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

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

**Предупреждение**

Если у вас есть ошибки в настройке конфигурационного файла «honeyd.conf», honeyd не запуститься. В терминале будет выводиться информация о работе Honeypot.

**Задания к лабораторной работе**

* Настройте сеть, состоящую из двух компьютеров.
* На одну из виртуальных машин устаните web-сервер <sudo apt-get install apache2>.
* На другую установите – Nmap <sudo apt-get install nmap>.
* Определите IP адрес виртуальной машины где установлен web-сервер apache.
* Произведите сканирование web-сервера всеми описанными методами (Изучение средств сканирования Nmap).
* Установите Honeyd.
* Ознакомьтесь с информацией по настройке Honeyd и стандартным содержимым файла /etc/honeypot/honeyd.conf.
* Настройте Honeypot изменив содержание файла /etc/honeypot/honeyd.conf .
* Запустите <farpd -d> .
* Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf>
* Произведите сканирование сети с honeypot.
* Измените настройки Honeypot. Усложните конфигурационный файл. Добавьте несколько ловушек, измените информацию об ОC, информацию о роутере, об открытых портах и.т.д..
* Запустите honeyd. <honeyd -d -f /etc/honeypot/honeyd.conf>
* Произведите сканирование.

**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. Какое наказание предусмотрено в РФ за взлом?
7. Как выявлять Honeypot?
8. Что такое DHCP?
9. Для чего используется RPC-сканирование?
10. Перечислите основные методы сканирования Nmap.