Факультет компьютерных технологий и прикладной математики

Кафедра вычислительных технологий

02.03.02

Информационная безопасность

Лабораторная работа № 6

Тема: Honeypot, Nmap.

Цель работы

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

Указания к работе

Вначале студенты изучают теоретическую часть. Далее каждый студент должен выполнить задания, а также ответить на вопросы к лабораторной работе. За проделанную работу студент может получить оценку от «неудовлетворительно» до «отлично». Для получения оценки «удовлетворительно» студент должен выполнить ВСЕ задания к лабораторной работе. Оценка «хорошо» ставится, если студент ответил на ВСЕ вопросы к лабораторной работе. Оценку «отлично» студент получает, если подготовлен отчёт по лабораторной работе.

ОЦЕНКУ ЗА ПРОДЕЛАННУЮ РАБОТУ МОЖНО ПОВЫСИТЬ ДО СДАЧИ СЛЕДУЮЩЕЙ ЛАБОРАТОРНОЙ РАБОТЫ.

Теоретическая часть

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.

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).

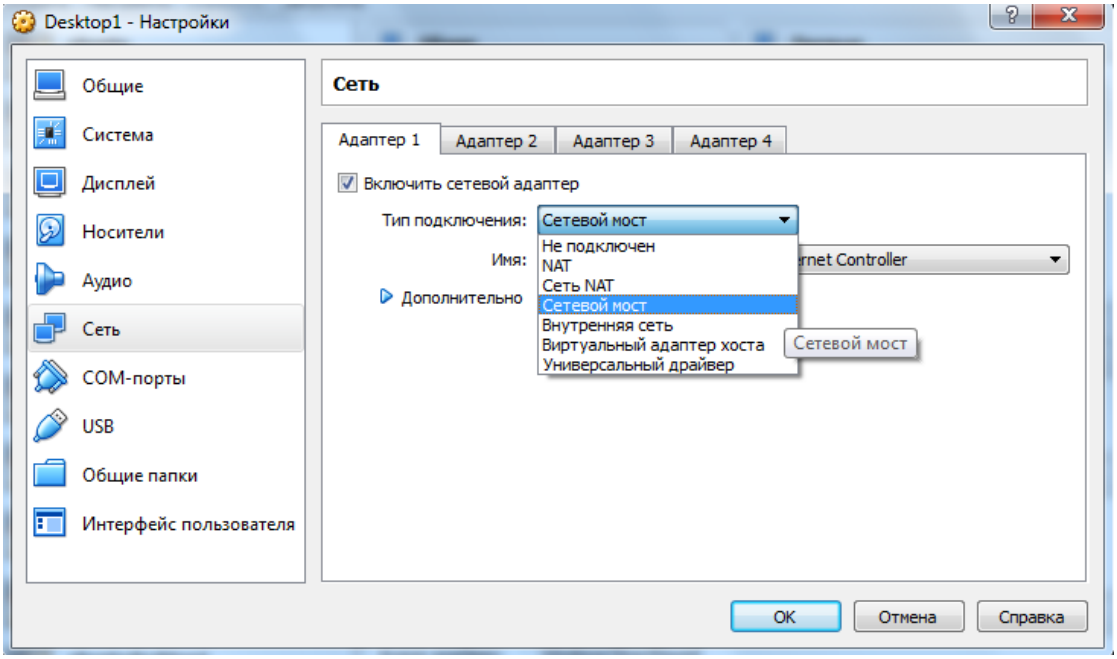
IP-адрес называют **статическим** (постоянным, неизменяемым), если он назначается пользователем в настройках устройства, либо если назначается автоматически при подключении устройства к сети и не может быть присвоен другому устройству.

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.

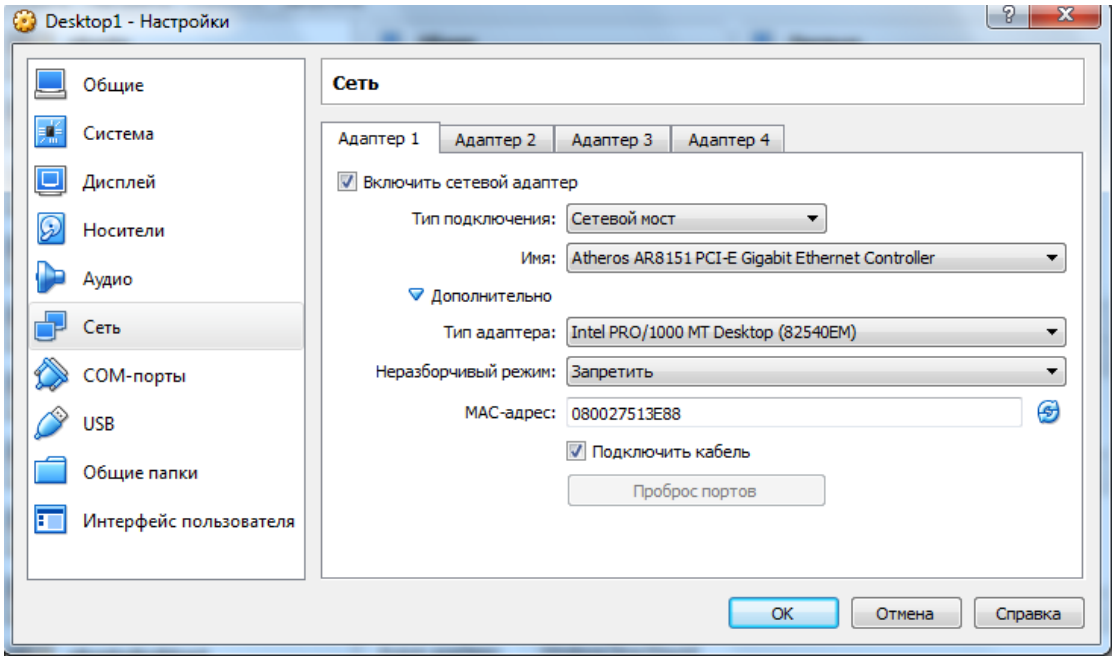
Настройка сети в VirtualBox

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.



Здесь стоит обратить внимание на MAC-адрес (может понадобиться 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.

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

Подробнее о настройке сети в VirtualBox можно прочитать на сайте VirtualBox.

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).

Стоит отметить, что мы можем заставить Nmap работать без привилегий root и в то же время поддерживать все расширенные функции и методы сканирования портов.

Все, что нам нужно сделать, это использовать возможности процесса Linux и назначить эти 3 возможности двоичному файлу Nmap:

- CAP_NET_RAW
- CAP_NET_ADMIN

• CAP_NET_BIND_SERVICE

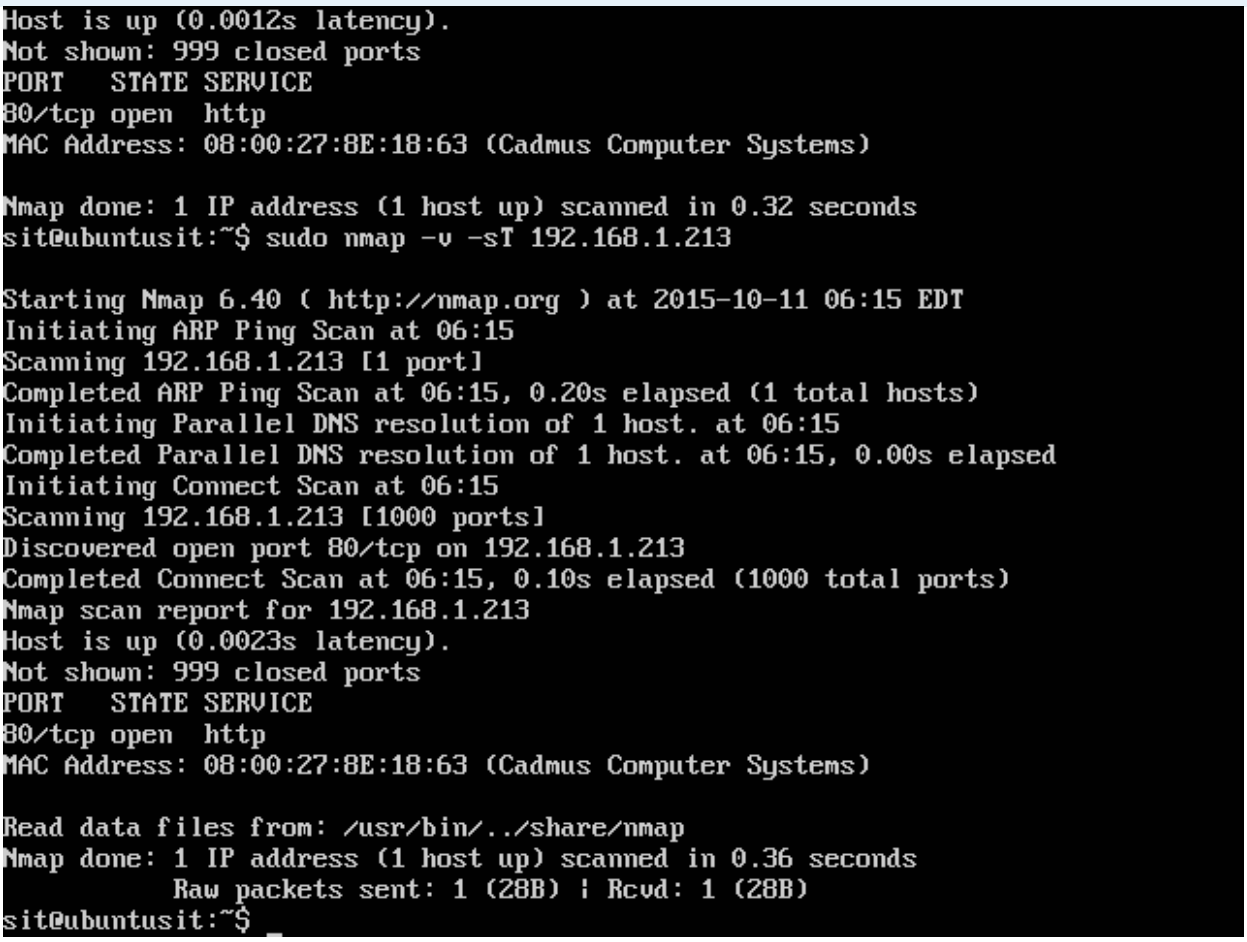
Вот как это сделать:

sudo setcap cap_net_raw,cap_net_admin,cap_net_bind_service+eip /usr/bin/nmap

С этого момента мы можем запускать Nmap как обычный непривилегированный пользователь следующим образом:

nmap --privileged -sT 192.168.0.1

Обратите внимание, что мы должны сообщить Nmap через --privileged флаг, что у него есть все необходимые возможности, даже если мы не root.

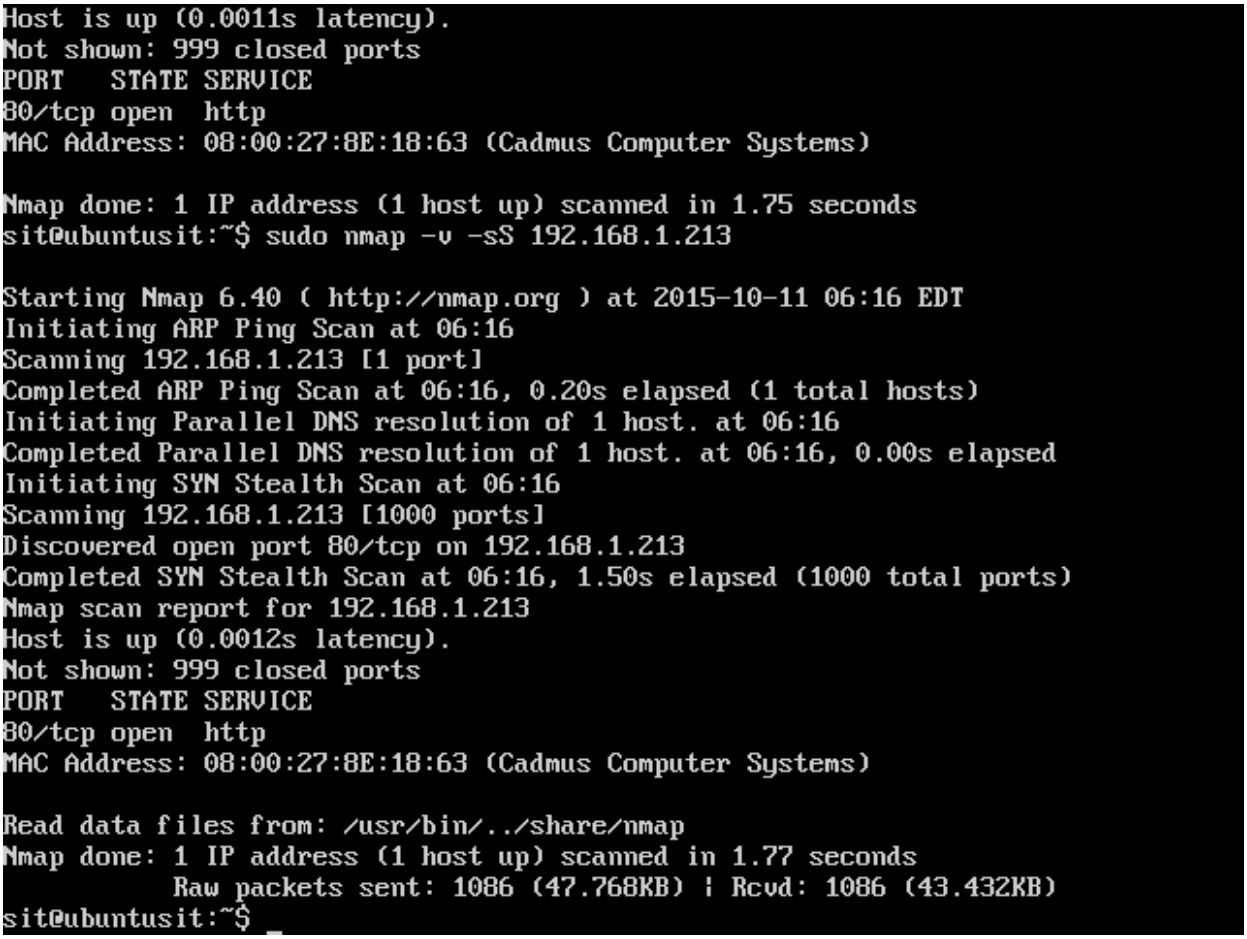


TCP-SYN

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

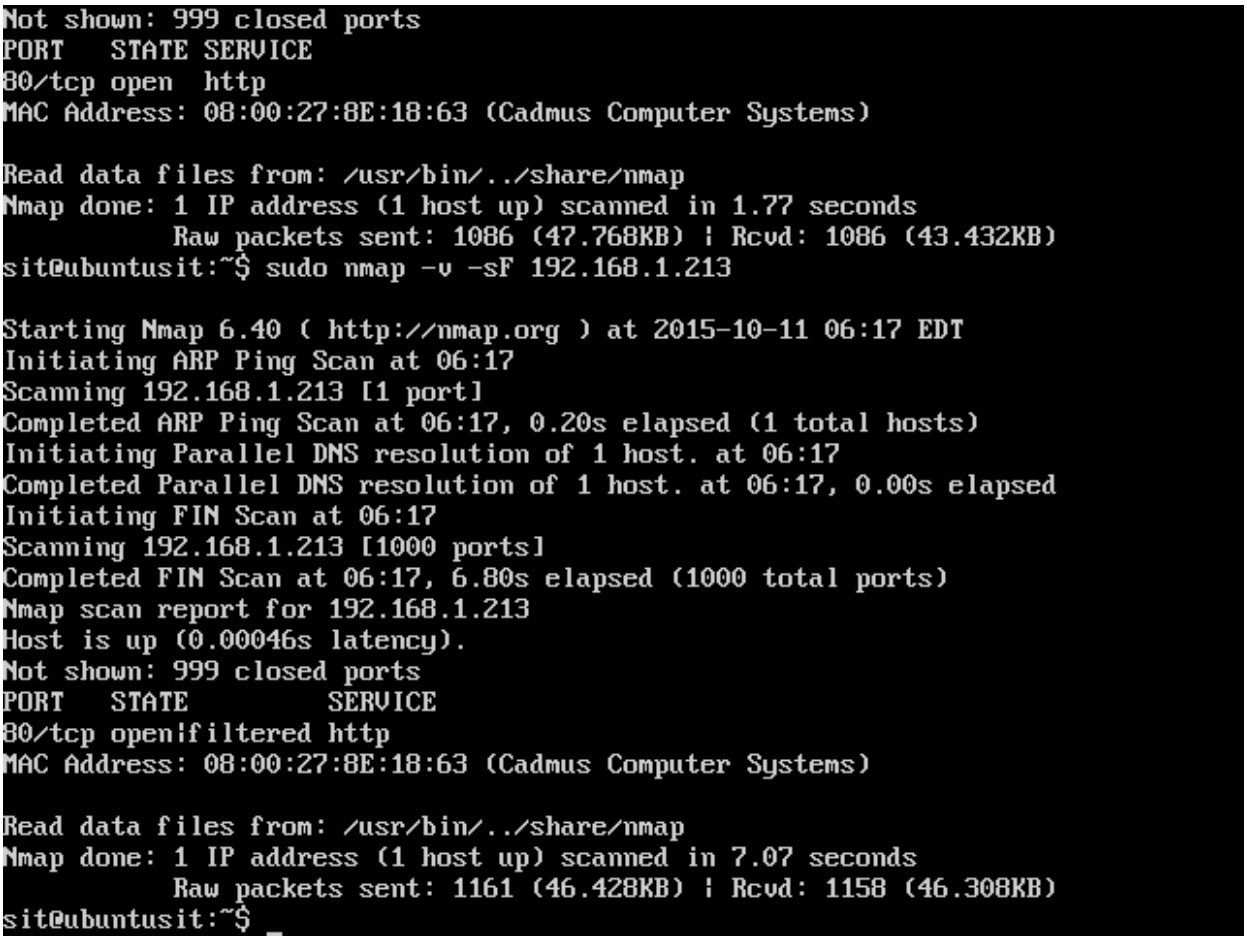


Сканирования FIN, Xmas Tree и NULL

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

```
Initiating ARP Ping Scan at 06:17
Scanning 192.168.1.213 [1 port]
Completed ARP Ping Scan at 06:17, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:17
Completed Parallel DNS resolution of 1 host. at 06:17, 0.00s elapsed
Initiating XMAS Scan at 06:17
Scanning 192.168.1.213 [1000 ports]
Increasing send delay for 192.168.1.213 from 0 to 5 due to 15 out of 49 dropped
probes since last increase.
Increasing send delay for 192.168.1.213 from 5 to 10 due to 21 out of 68 dropped
 probes since last increase.
Increasing send delay for 192.168.1.213 from 10 to 20 due to 11 out of 25 droppe
d probes since last increase.
Increasing send delay for 192.168.1.213 from 20 to 40 due to 11 out of 26 droppe
d probes since last increase.
Increasing send delay for 192.168.1.213 from 40 to 80 due to 11 out of 31 droppe
d probes since last increase.
XMAS Scan Timing: About 41.73% done; ETC: 06:19 (0:00:43 remaining)
Completed XMAS Scan at 06:19, 94.20s elapsed (1000 total ports)
Nmap scan report for 192.168.1.213
Host is up (0.00048s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 94.48 seconds
           Raw packets sent: 1306 (52.228KB) | Rcvd: 1302 (52.068KB)
sit@ubuntusit:~$
```

nmap -sN 192.168.58.103

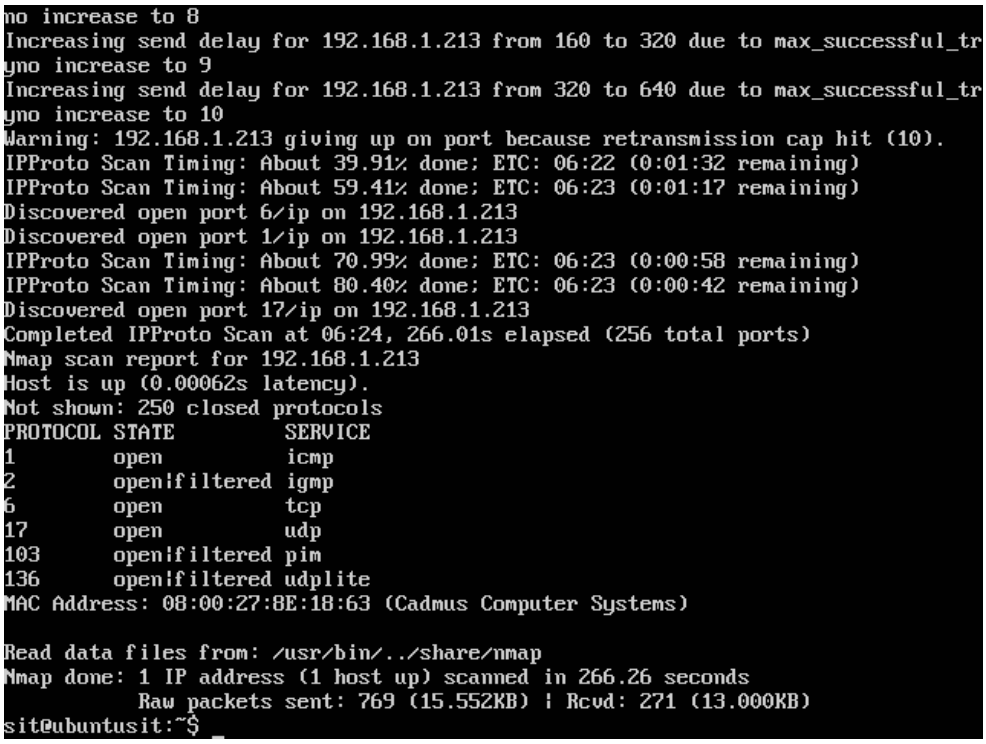
```
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 94.48 seconds
           Raw packets sent: 1306 (52.228KB) | Rcvd: 1302 (52.068KB)
sit@ubuntusit:~$ sudo nmap -v -sN 192.168.1.213

Starting Nmap 6.40 ( http://nmap.org ) at 2015-10-11 06:19 EDT
Initiating ARP Ping Scan at 06:19
Scanning 192.168.1.213 [1 port]
Completed ARP Ping Scan at 06:19, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:19
Completed Parallel DNS resolution of 1 host. at 06:19, 0.00s elapsed
Initiating NULL Scan at 06:19
Scanning 192.168.1.213 [1000 ports]
Completed NULL Scan at 06:19, 2.90s elapsed (1000 total ports)
Nmap scan report for 192.168.1.213
Host is up (0.00044s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
           Raw packets sent: 1131 (45.228KB) | Rcvd: 1128 (45.108KB)
sit@ubuntusit:~$
```

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.

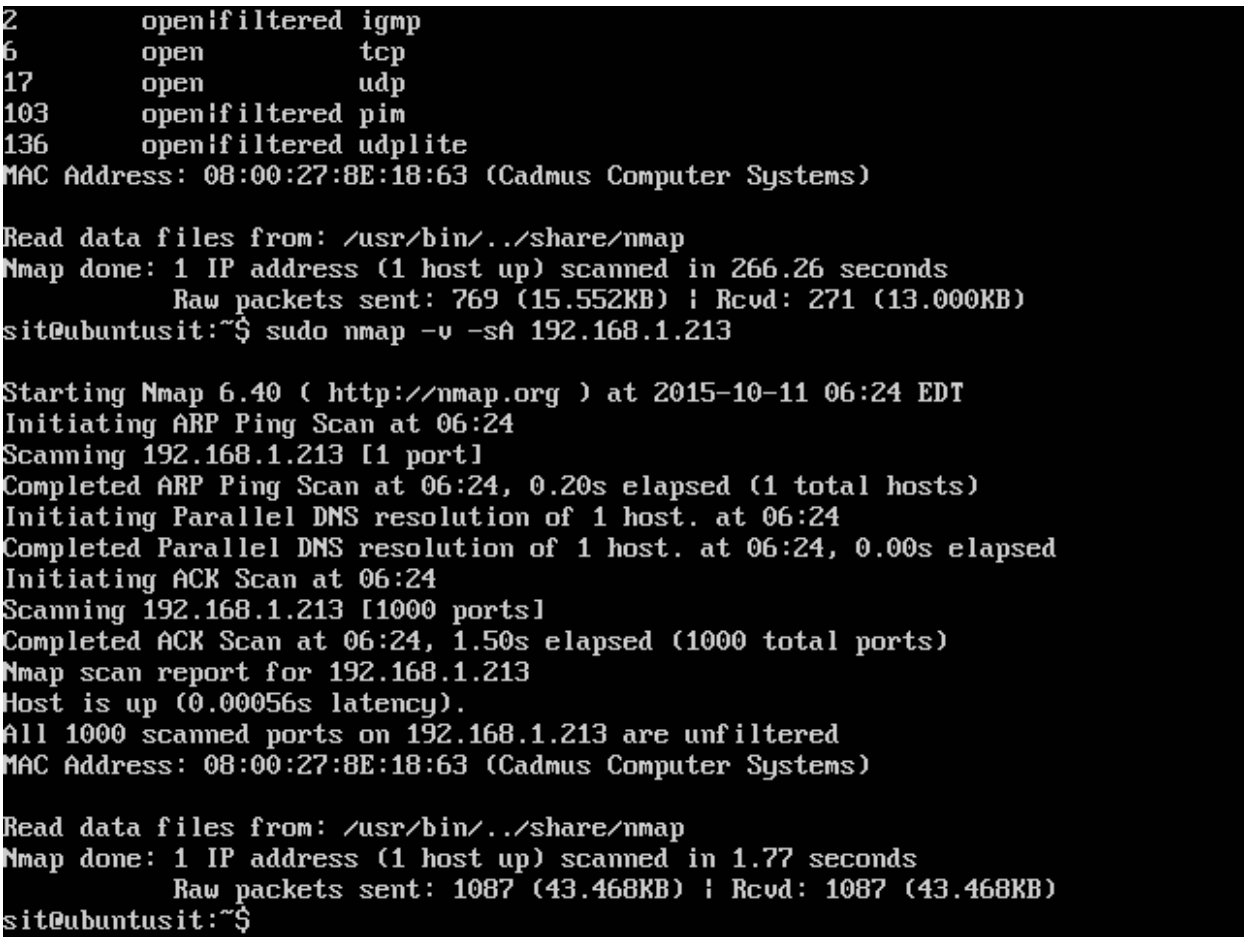
nmap -sO 192.168.58.103



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

```
Scanning 192.168.1.213 [1000 ports]
Completed ACK Scan at 06:24, 1.50s elapsed (1000 total ports)
Nmap scan report for 192.168.1.213
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.1.213 are unfiltered
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
           Raw packets sent: 1087 (43.468KB) | Rcvd: 1087 (43.468KB)
sit@ubuntusit:~$ sudo nmap -v -sW 192.168.1.213

Starting Nmap 6.40 ( http://nmap.org ) at 2015-10-11 06:25 EDT
Initiating ARP Ping Scan at 06:25
Scanning 192.168.1.213 [1 port]
Completed ARP Ping Scan at 06:25, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:25
Completed Parallel DNS resolution of 1 host. at 06:25, 0.00s elapsed
Initiating Window Scan at 06:25
Scanning 192.168.1.213 [1000 ports]
Completed Window Scan at 06:25, 1.50s elapsed (1000 total ports)
Nmap scan report for 192.168.1.213
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.1.213 are closed
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
           Raw packets sent: 1086 (43.428KB) | Rcvd: 1086 (43.428KB)
sit@ubuntusit:~$
```

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

```
RPC scan.

Starting Nmap 6.40 ( http://nmap.org ) at 2015-10-11 06:25 EDT
NSE: Loaded 23 scripts for scanning.
Initiating ARP Ping Scan at 06:25
Scanning 192.168.1.213 [1 port]
Completed ARP Ping Scan at 06:25, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:25
Completed Parallel DNS resolution of 1 host. at 06:25, 0.00s elapsed
Initiating SYN Stealth Scan at 06:25
Scanning 192.168.1.213 [1000 ports]
Discovered open port 80/tcp on 192.168.1.213
Completed SYN Stealth Scan at 06:25, 1.50s elapsed (1000 total ports)
Initiating Service scan at 06:25
Scanning 1 service on 192.168.1.213
Completed Service scan at 06:25, 6.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.213.
Nmap scan report for 192.168.1.213
Host is up (0.00047s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.10 seconds
           Raw packets sent: 1087 (47.812KB) | Rcvd: 1087 (43.472KB)
sit@ubuntusit:~$
```

Сканирование ОС

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

nmap -O 192.168.58.103

```
Nmap done: 1 IP address (1 host up) scanned in 22.62 seconds
sit@ubuntusit:~$ sudo nmap -O 192.168.1.213

Starting Nmap 6.40 ( http://nmap.org ) at 2015-10-11 06:27 EDT
Nmap scan report for 192.168.1.213
Host is up (0.00042s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:8E:18:63 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=10/11%OT=80%CT=1%CU=43621%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=561A399E%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=1%ISR=10C%TI=Z%CI=I%II=I
OS:%TS=8)SEQ(SP=F9%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4S
OS:T11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=
OS:7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=
OS:M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds
sit@ubuntusit:~$
```

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

```
 System information as of Sun Oct 11 07:01:30 EDT 2015

 System load:  0.08              Processes:           86
 Usage of /:   7.8% of 14.88GB   Users logged in:     0
 Memory usage: 7%                IP address for eth0: 192.168.1.124
 Swap usage:   0%                IP address for eth1: 192.168.56.122

 Graph this data and manage this system at:
   https://landscape.canonical.com/

sit@ubuntusit:~$ sudo nmap -O 192.168.1.116
[sudo] password for sit:

Starting Nmap 6.40 ( http://nmap.org ) at 2015-10-11 07:02 EDT
Nmap scan report for 192.168.1.116
Host is up (0.00041s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:97:DF:41 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.84 seconds
sit@ubuntusit:~$
```

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.

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>.

Если honeyd отсутствует в репозиториях, его можно скачать (*.deb пакет) и установить. Так же, можно скачать исходные коды honeyd с официального сайта 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 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. далее)). 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]

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

Часть 1

1. Настройте сеть, состоящую из двух компьютеров.

2. На одну из виртуальных машин установите web-сервер <sudo apt-get install apache2>.

3. На другую установите – Nmap <sudo apt-get install nmap>.

4. Определите IP адрес виртуальной машины где установлен web-сервер apache.

5. Произведите сканирование web-сервера всеми описанными методами (изучение средств сканирования Nmap).

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.