ОБРПО. Лекция 4 Безопасность сетей

ТЮРИН КАЙ АНДРЕЕВИЧ

Роль сетевой безопасности

Огромна

Всякая компания имеет компьютеры

Эти компьютеры объединены в сеть

И подключены к Интернету

С чего начинается сетевая безопасность

Если мы откроем любой offensive-мануал по сетевой безопасности, то первое, что мы увидим - … инструменты сканирования

С чего начинается атака?

Определение узлов сети

Определение вида оборудования

Определение операционной системы

Определение открытых портов

Определение наличия IDS/IPS

Определение ПО и версий того, что висит на этих портах

nmap

Впервые опубликован в сентябре 1997 года

Используется для

1. обнаружения узлов в сети
2. сканирования портов

nmap

Сканируем 1000 наиболее часто используемых портов:

```
nmap 12.34.56.78
```

Указываем список портов:

```
nmap -p22,80,100-200 12.34.56.78
```

Сканирование подсети:

```
nmap -p22 52.8.254.0/24
```

Сканирование списка хостов из файла:

```
nmap -p22 -iL iplist.txt
```

nmap

Сканирование методом установки TCP соединения:

```
nmap -p22,80 -sT 12.34.56.78
```

SYN-сканирование:

```
sudo nmap -p22,80 -sS 12.34.56.78
```

Определение версии сервисов:

```
nmap -p22,80,100-200 -sV 12.34.56.78
```

Определение операционной системы:

```
sudo nmap -O 12.34.56.78
```

ARP-сканирование

Не оставляет следов (почти)

arping

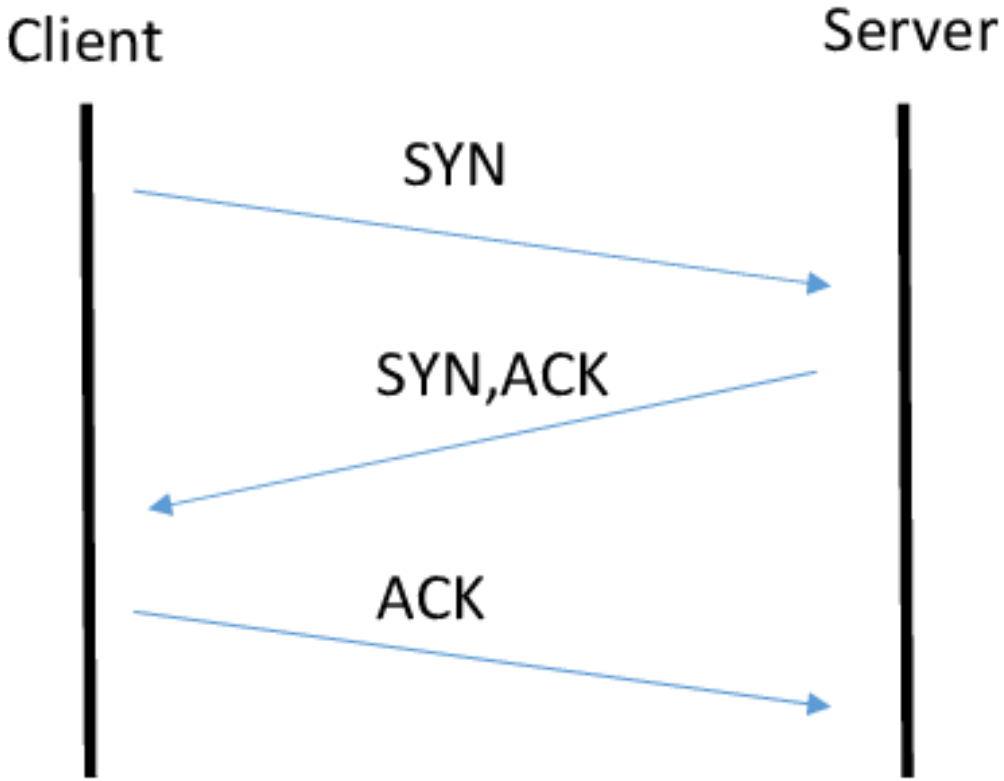
netdiscover

Можно сканировать в

1. активном режиме
2. пассивном режиме

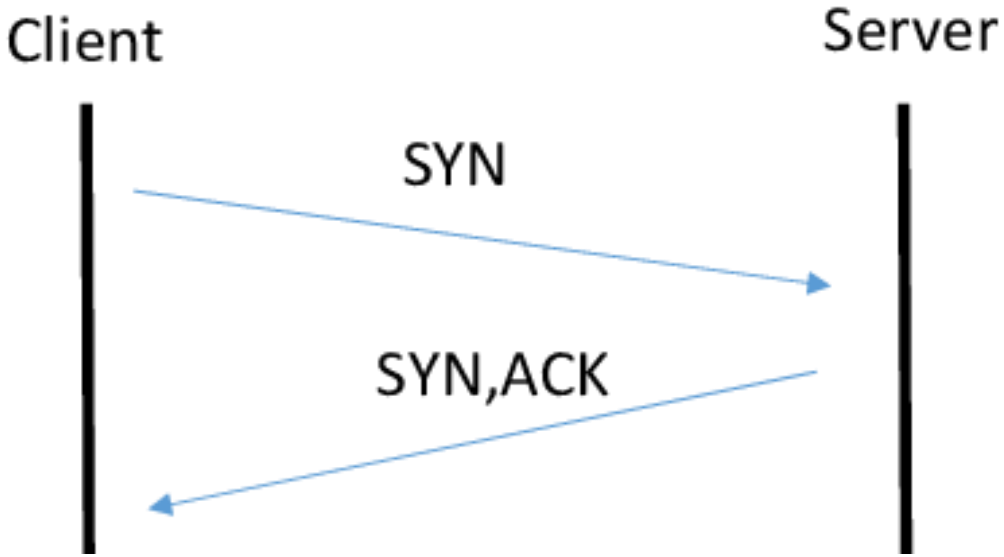
Сканирование полухэндшейком

Обычный TCP-handshake



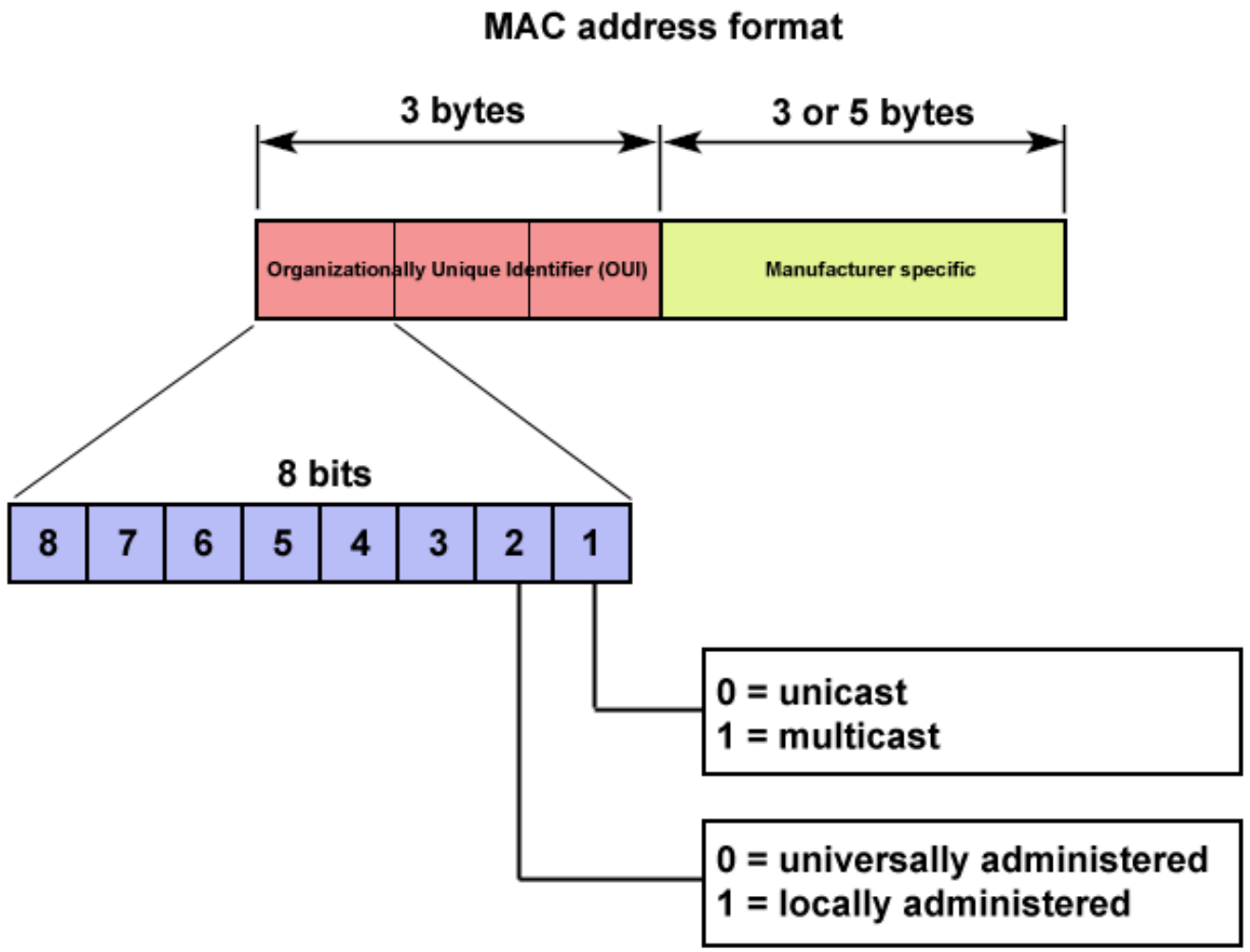
Сканирование полухэндшейком

TCP-handshake, достаточный для того, чтобы понять, что порт открыт (и не оставить информации о коннекте в логах)



Определение вида оборудования

Устройство MAC-адреса



Как спрятаться?

Перенести оборудование на нестандартные порты – (не такая уж) плохая идея!

Security Advisor

Severity: High

Description: SSH port has not been changed from default value.

Details

Changing the SSH port helps prevent unauthorized users from attacking your system via default port number 22.

Recommended Action

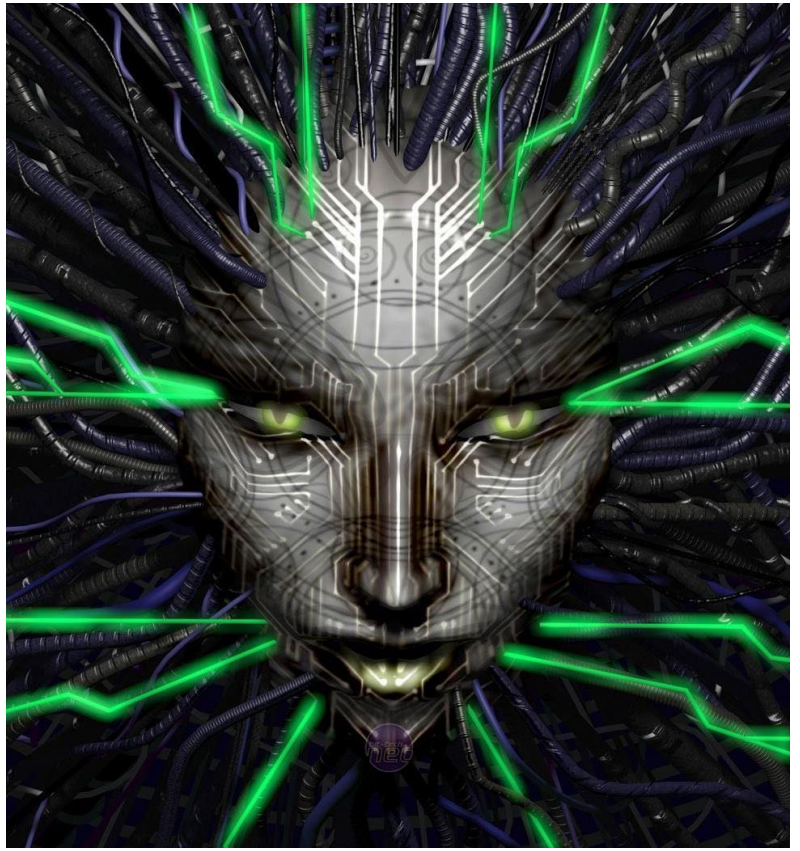
Go to Control Panel > Terminal & SNMP > Terminal and change the SSH port to another value other than the default value 22. Please also change the SSH port settings for SSH clients.

Open **Control Panel** to take recommended actions.

Shodan

Поисковик по устройствам в интернете

Непрерывно сканирует весь интернет на предмет доступных сервисов



SHODAN telnet Explore Developer Pricing

Exploits Maps Images

TOTAL RESULTS

134,036

TOP COUNTRIES

China	57,876
United States	17,149
Korea, Republic of	13,217
Japan	4,329
Turkey	3,678

103.29.133.251

Beijing WangYuanXinHui Technology Co.,Ltd

Added on 2019-03-04 02:11:20 GMT

China

```
Warning: Telnet is not a se

Login authentication

Username:
```

181.10.230.25

host25.181-10-230.telecom.net.ar

Telecom Personal

Added on 2019-03-04 02:12:05 GMT

Argentina, Macia

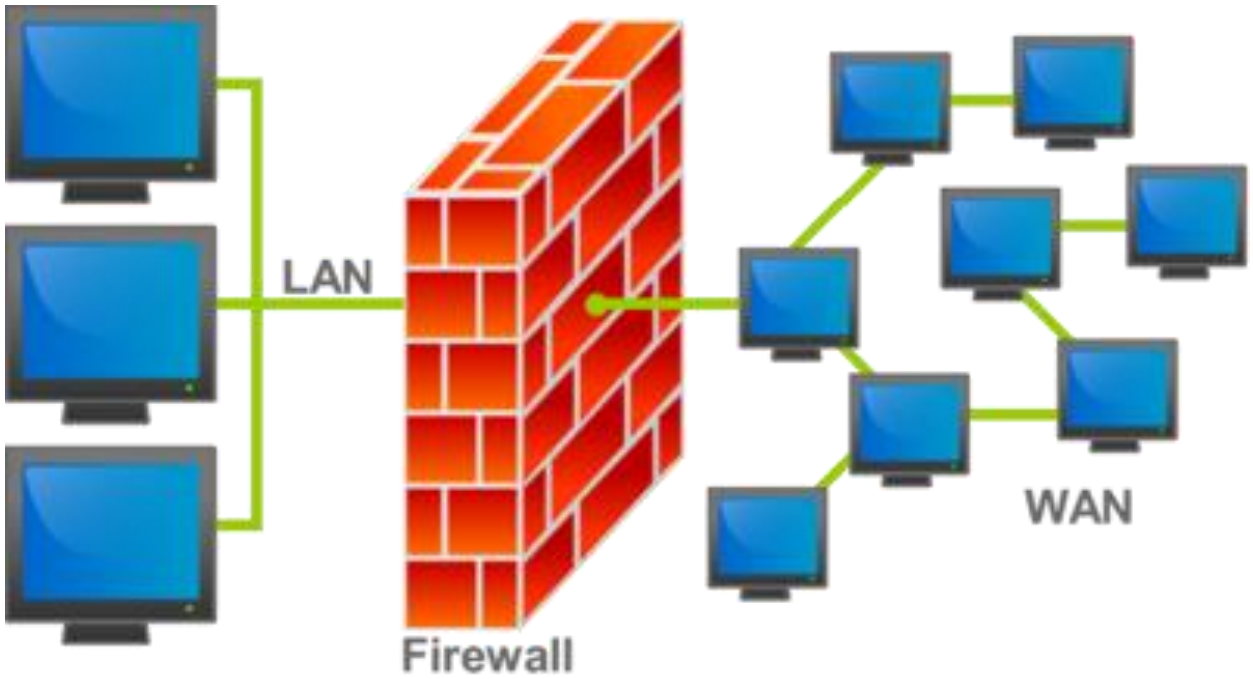
```
Warning: Telnet is not a se

Login authentication
```

И что с этим делать?

Firewall!

(межсетевой экран)

Позволяет контролировать сетевые соединения.



Linux

iptables – НЕ ФАЙРВОЛ!

iptables – консольный интерфейс для файрвола netfilter.

Основные понятия:

Правило — состоит из критерия, действия и счетчика.

Критерий — логическое выражение, анализирующее свойства пакета и/или соединения.

Действие — описание действия, которое нужно проделать с пакетом и/или соединением в том случае.

Основные понятия iptables

Счетчик — компонент правила, обеспечивающий учет количества пакетов.

Цепочка — упорядоченная последовательность правил.

Базовая цепочка — цепочка, создаваемая по умолчанию при инициализации таблицы.

Пользовательская цепочка — цепочка, созданная пользователем.

Таблица — совокупность базовых и пользовательских цепочек, объединенных общим функциональным назначением.

Пример

iptables -F # Очищаем все цепочки таблицы filter

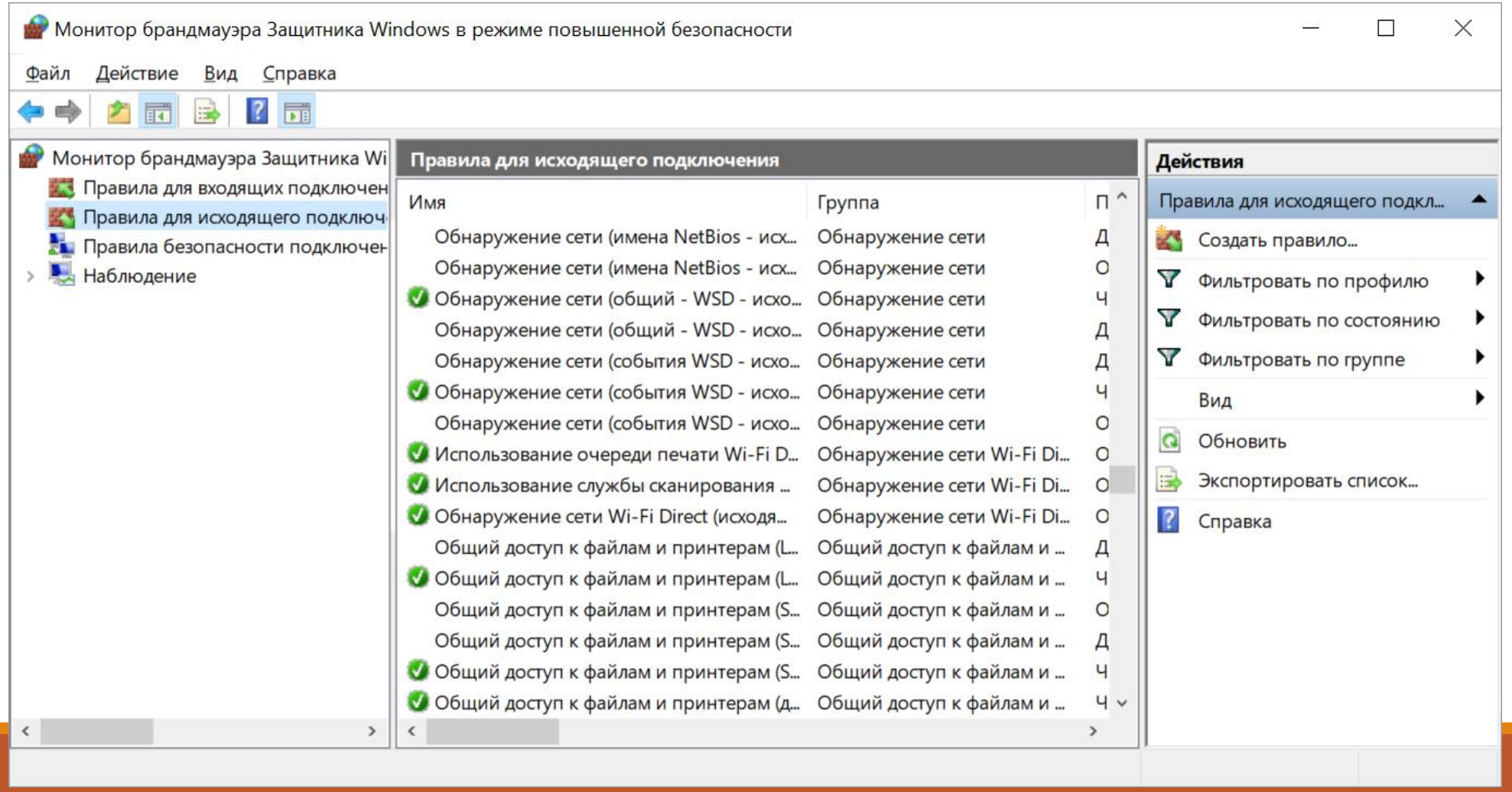
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT # Ко всем пакетам, которые относятся к уже установленным

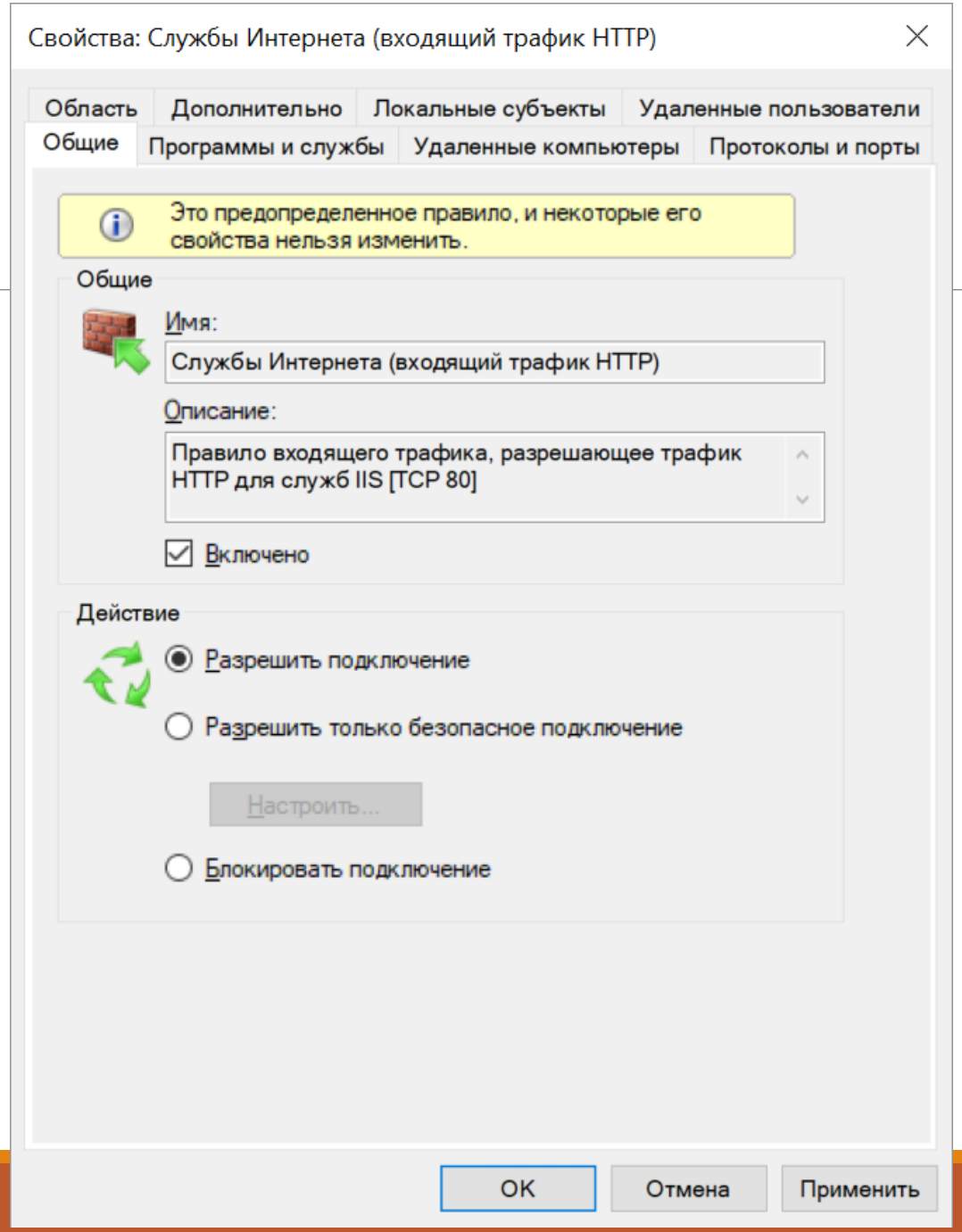
соединениям, применяем терминальное действие ACCEPT — пропустить

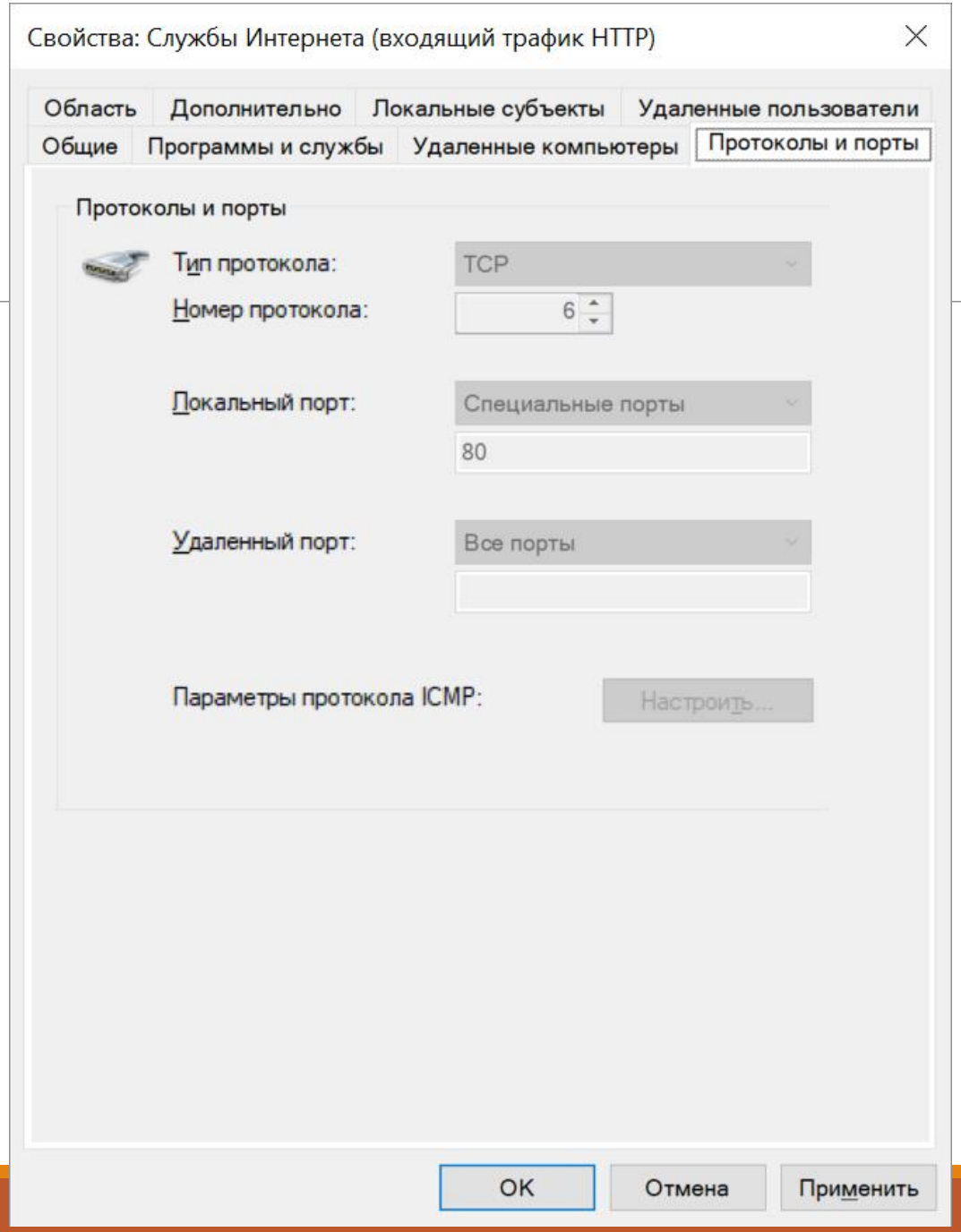
iptables -P INPUT DROP # В качестве действия по умолчанию для входящих пакетов устанавливаем DROP — блокирование пакета

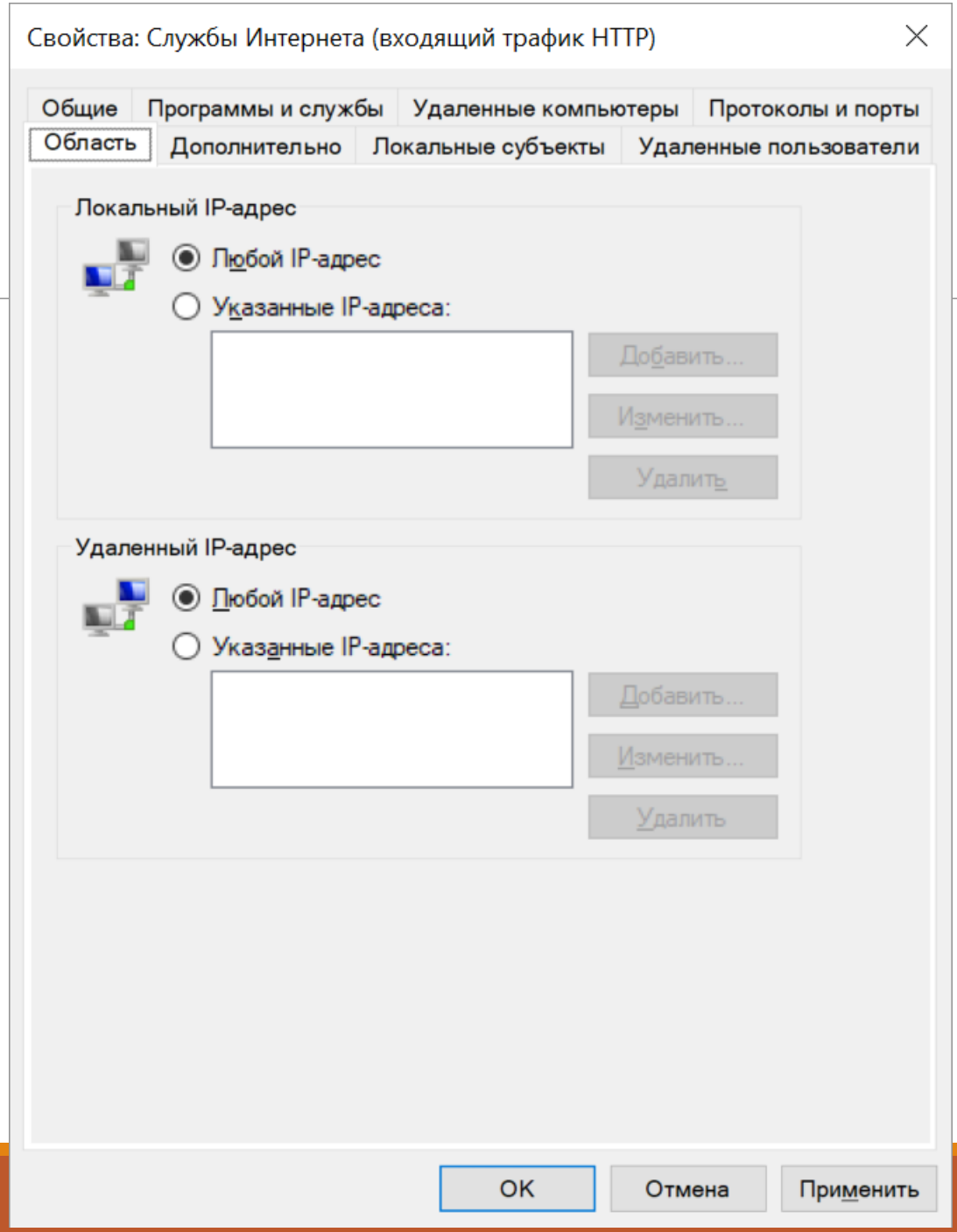
iptables -P OUTPUT ACCEPT # Разрешаем все исходящие пакеты

Windows

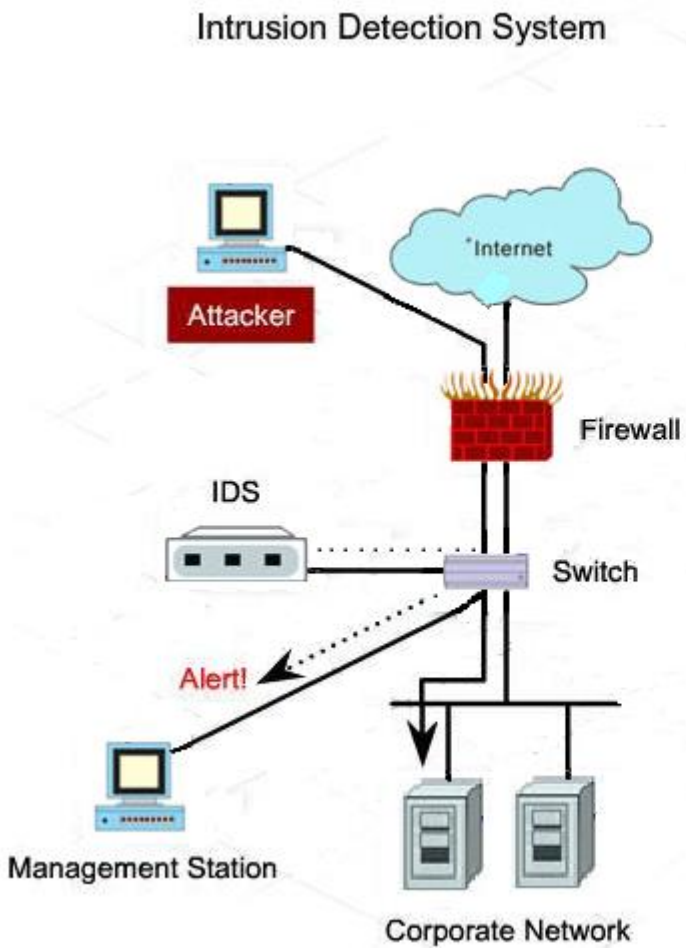

Монитор брандмауэра Защитника Windows в режиме повышенной безопасности
Файл Действие Вид Справка
Монитор брандмауэра Защитника Wi
Правила для входящих подключен
Правила для исходящего подключ
Правила безопасности подключен
Наблюдение
Правила для исходящего подключения
Имя
Группа
П
Обнаружение сети (имена NetBios - исх... Обнаружение сети Д
Обнаружение сети (имена NetBios - исх... Обнаружение сети О
Обнаружение сети (общий - WSD - исхо... Обнаружение сети Ч
Обнаружение сети (общий - WSD - исхо... Обнаружение сети Д
Обнаружение сети (события WSD - исхо... Обнаружение сети Д
Обнаружение сети (события WSD - исхо... Обнаружение сети Ч
Обнаружение сети (события WSD - исхо... Обнаружение сети О
Использование очереди печати Wi-Fi D... Обнаружение сети Wi-Fi Di... О
Использование службы сканирования ... Обнаружение сети Wi-Fi Di... О
Обнаружение сети Wi-Fi Direct (исходя... Обнаружение сети Wi-Fi Di... О
Общий доступ к файлам и принтерам (L... Общий доступ к файлам и ... Д
Общий доступ к файлам и принтерам (L... Общий доступ к файлам и ... Ч
Общий доступ к файлам и принтерам (S... Общий доступ к файлам и ... О
Общий доступ к файлам и принтерам (S... Общий доступ к файлам и ... Д
Общий доступ к файлам и принтерам (S... Общий доступ к файлам и ... Ч
Общий доступ к файлам и принтерам (д... Общий доступ к файлам и ... Ч
Действия
Правила для исходящего подкл...
Создать правило...
Фильтровать по профилю
Фильтровать по состоянию
Фильтровать по группе
Вид
Обновить
Экспортировать список...
Справка

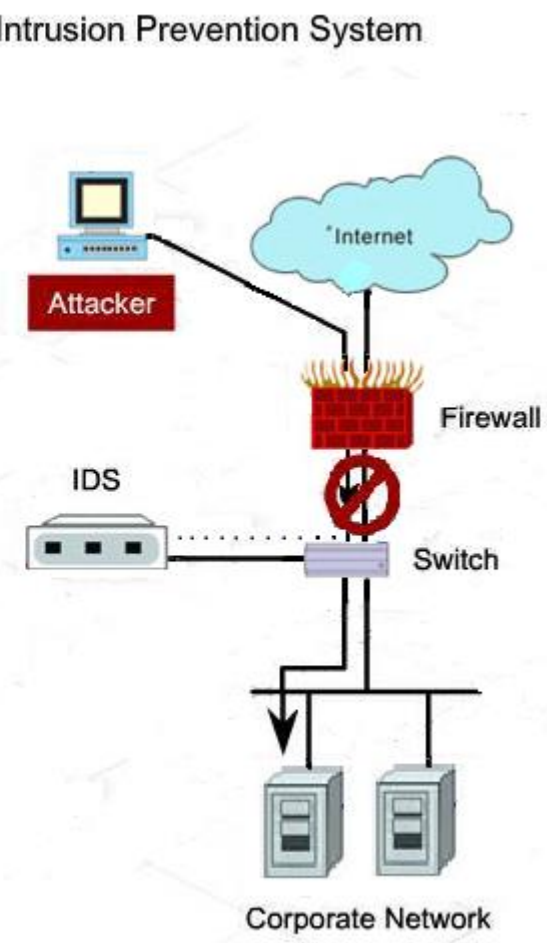

Свойства: Службы Интернета (входящий трафик HTTP)
Область
Дополнительно
Локальные субъекты
Удаленные пользователи
Общие
Программы и службы
Удаленные компьютеры
Протоколы и порты
Это предопределенное правило, и некоторые его свойства нельзя изменить.
Общие
Имя:
Службы Интернета (входящий трафик HTTP)
Описание:
Правило входящего трафика, разрешающее трафик HTTP для служб IIS [TCP 80]
Включено
Действие
Разрешить подключение
Разрешить только безопасное подключение
Настроить...
Блокировать подключение
OK
Отмена
Применить


Свойства: Службы Интернета (входящий трафик HTTP)
Область
Дополнительно
Локальные субъекты
Удаленные пользователи
Общие
Программы и службы
Удаленные компьютеры
Протоколы и порты
Протоколы и порты
Тип протокола:
TCP
Номер протокола:
6
Локальный порт:
Специальные порты
80
Удаленный порт:
Все порты
Параметры протокола ICMP:
Настроить...
OK
Отмена
Применить


Свойства: Службы Интернета (входящий трафик HTTP)
Общие
Программы и службы
Удаленные компьютеры
Протоколы и порты
Область
Дополнительно
Локальные субъекты
Удаленные пользователи
Локальный IP-адрес
Любой IP-адрес
Указанные IP-адреса:
Добавить...
Изменить...
Удалить
Удаленный IP-адрес
Любой IP-адрес
Указанные IP-адреса:
Добавить...
Изменить...
Удалить
OK
Отмена
Применить

IDS/IPS


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network


Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network

Honeypot

«Фейковый» сервер, представляющий приманку для злоумышленника

Существуют различные вариации по степени проработанности

Обращение к honeypot в локальной сети может являться признаком компрометации

NAT с точки зрения безопасности

НЕ ОБЕСПЕЧИВАЕТ БЕЗОПАСНОСТЬ