### Назначение СОА Cisco IDS Sensor

Система обнаружения атак (англ. Intrusion Detection System) – это программный или программно-аппаратный комплекс, предна- значенный для выявления и по возможности предупреждения дей- ствий, угрожающих безопасности информационной системы [1].

Основными задачами, решаемыми с помощью систем обнару- жения атак (СОА), являются:

* + - * обнаружение атак (вторжений);
      * прогнозирование возможных сценариев развития комплекс- ных атак на основе выявления признаков начальных этапов атаку- ющего воздействия;
      * фиксация информации об источниках компьютерного напа- дения;
      * получение информации об уязвимостях, использованных для компьютерного нападения.

В большинстве случаев СОА состоит из следующих компо- нентов:

* + - * сенсорной подсистемы, предназначенной для сбора событий, связанных с безопасностью защищаемой сети или системы;
      * подсистемы анализа, служащей для выявления комплексных компьютерных атак;
      * информационного хранилища (базы данных), в котором накапливаются первичные события и результаты анализа;
      * консоли управления, позволяющей конфигурировать СОА и просматривать выявленные подсистемой анализа инциденты.

В настоящее время существует ряд сетевых СОА фирмы Cisco Systems линейки 4200, предназначенных для сетей, работающих на технологии Fast Ethernet (рис. 4.1). Эти системы обладают общим программным обеспечением и различаются главным образом по производительности – пропускной способности:

* + - * Cisco IDS 4210 – 45 Мб/с;
      * Cisco IDS 4215 – 80 Мб/с;
      * Cisco IDS 4230 – 100 Мб/с;
      * Cisco IDS 4235 – 250 Мб/с;
      * Cisco IDS 4250 – 500 Мб/с;
      * Cisco IDS 4250 XL – 1000 Мб/с.



Рис. 4.1. Устройства линейки Cisco IDS 4200

На практическом занятии рассматривается модель Cisco IDS 4215 Sensor. Характеристики модели IDS-4215, обеспечивающие пропускную способность до 80 Мб/с: возможность сбора трафика с пяти сетевых интерфейсов, поддержка до 800 новых TCP-соединений в секунду, до 800 HTTP-соединений в секунду, средний размер пакета 445 байт.

Особенностями комплексов линейки 4200 являются:

* + - * точность обнаружения атак, обусловленная применением сигнатурных алгоритмов;
      * интеллектуальный анализ, основанный на применении ана- литических алгоритмов обнаружения;
      * простота и удобство администрирования при наличии трех интерфейсов администрирования;
      * гибкость развертывания.

Наряду с традиционными сигнатурными алгоритмами в Cisco IDS используются и алгоритмы, отслеживающие аномалии в сете- вом трафике и отклонения от нормального поведения сетевых при- ложений, что позволяет обнаруживать как известные, так и неиз- вестные атаки. С целью снижения числа ложных срабатываний, неизбежно возникающих при использовании аналитических алго- ритмов, в комплексы интегрированы технологии корреляции собы- тий безопасности: Cisco Threat Response, Threat Risk Rating и Meta Event Generator. Указанные технологии позволяют концентриро- вать внимание администраторов на наиболее критичных атаках.

Cisco IDS может также работать в режиме предотвращения атак, завершая сеанс атаки путем отключения соединений с опас-

ных IP-адресов, динамически изменяя списки доступа (Access Control Lists) на сетевом оборудовании.

Существуют три интерфейса администрирования Cisco IDS Sensor:

* + - * интерфейс командной строки (CLI интерфейс) операционной системы устройства;
      * графический интерфейс Cisco IDS Event Viewer (IEV), раз- работанный на языке Java для применения в ОС семейства Windows;
      * графический интерфейс Cisco IDS Device Manager (IDM),

основывающийся на использовании браузера.

Для защищенного обмена данными между администратором сети и сенсором применяется протокол Remote Data Exchange Pro- tocol (RDEP) (начиная с версии 4.0). Протокол RDEP является раз- новидностью протокола HTTP и основывается на XML-конфигурации (TCP-порт 443). Безопасность передаваемых данных обеспечивается за счет использования протокола SSL (Secure Socket Layer). Для управления сенсором администратор должен за- дать имя устройства Cisco IDS Sensor и номер порта.

В сети СОА может располагаться как перед, так и после меж- сетевого экрана. Установка СОА перед межсетевым экраном поз- воляет обнаруживать все атаки, идущие на систему извне. Однако при этом не обнаруживается активность внутреннего нарушителя. Расположение СОА за межсетевым экраном позволяет контролиро- вать весь трафик, однако не будут фиксироваться те атаки, которые были отражены самим межсетевым экраном. Дополнительным пре- имуществом расположения СОА за межсетевым экраном является уменьшение срабатываний СОА.

Согласно рекомендациям производителя сенсор следует раз- мещать в одном из следующих элементов сети (или в нескольких):

* + - * на границе локальной сети и сети «Интернет», что позволит анализировать и контролировать весь трафик обмена внутренней сети с внешней;
      * около шлюзов сторонних организации, к которым нет пол- ного доверия;
      * на границе между отдельными сегментами сети;
      * около точек, используемых для модемной связи и связи с помощью технологий VPN и Wi-Fi.

### Аппаратная часть СОА Cisco IDS 4215 Sensor

СОА Cisco IDS 4215 Sensor является аппаратным устройством, предназначенным для размещения в серверной стойке (рис. 4.2).

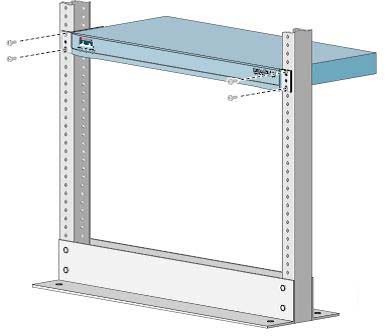


Рис. 4.2. Схема установки Cisco IDS 4215 Sensor в серверной стойке

На лицевой панели устройства (рис. 4.3) расположены три ин- дикатора: POWER (наличие питания), ACT (индикатор режима ра- ботоспособности устройства) и NETWORK (индикатор наличия се- тевого трафика в канале).



Рис. 4.3. Лицевая панель Cisco IDS 4215 Sensor

На задней панели устройства (рис. 4.4) расположен ряд ин- терфейсов (рис. 4.5):

* + - * консольный порт для подключения к последовательному порту персонального компьютера с использованием коннектора RJ-45 и управления устройством в режиме командной строки;
      * интерфейс FastEthernet0/1 для подключения устройства к анализируемому каналу передачи данных (интерфейс сенсора);
      * интерфейс FastEthernet0/0 для управления устройством в ре- жиме web-интерфейса;
      * четыре дополнительных интерфейса типа FastEthernet для подключения анализируемых каналов передачи данных (функцио- нируют в случае наличия дополнительно установленной карты типа 4FE) .



Рис. 4.4. Задняя панель Cisco IDS 4215 Sensor

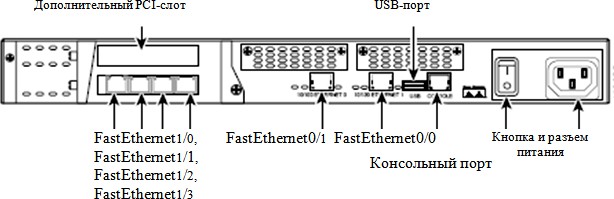


Рис. 4.5. Интерфейсы Cisco IDS 4215 Sensor

Интерфейс сенсора FastEthernet0/1находится в режиме захвата пакетов (promiscuous mode), не имеет IP-адреса и не обнаруживает- ся в сегменте сети.

Управляющий интерфейс FastEthernet0/0 должен иметь IP-адрес, быть видимым в сегменте сети. Для защиты управляюще- го канала связи применяется шифрование средствами службы SSH (при работе в режиме командной строки) и протокола SSL (в режи- ме web-интерфейса).

Внутри устройство представляет собой компьютер, оборудо- ванный жестким магнитным диском с операционной системой Linux и специализированным программным обеспечением (рис. 4.6), а также оборудованный flash-картой памяти.

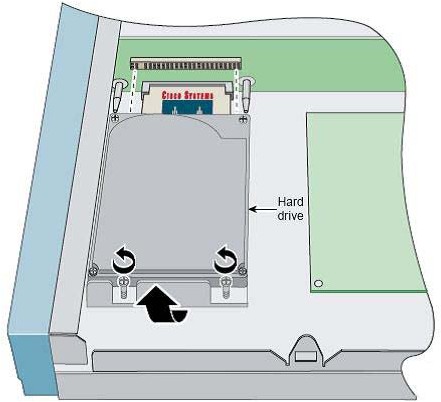


Рис. 4.6. Вид Cisco IDS 4215 Sensor со снятым кожухом

### Предварительная настройка СОА Cisco IDS Sensor

***в режиме командной строки***

Рассмотрим некоторую организацию, в сети которой внедре- но аппаратное устройство Cisco IDS Sensor с целью обнаружения компьютерных атак. Для имитации указанной сети развернем стенд на базе технологии виртуальных машин.

Основная ОС (рис. 4.7) будет имитировать работу админи- стратора для конфигурирования Cisco IDS Sensor, она же будет ис- пользована для имитации атакующего воздействия. Оборудование Cisco IDS Sensor в учебных целях представлено виртуальным обра- зом. Сетевое соединение выполняется с помощью виртуальной подсети VWNet1 (тип соединения – Host-only). Для имитации узла-

«жертвы» может быть использована любая виртуальная система, подключенная к сети VWNet1.

В связи с тем что в основе Cisco IDS Sensor лежит операци- онная система Linux, для работы необходимы минимальные знания в области администрирования данной ОС. Для выполнения работы потребуется система VMware Player, образ Cisco IDS Sensor (предо- ставляется преподавателем в архиве cisco\_ids.rar), сканер портов nmap (или его аналог), анализатор трафика Wireshark (или его ана- лог). Для имитации узла-«жертвы» может быть использована лю-

бая виртуальная система (например, ОС Windows 2003 Server), под- ключенная к сети VWNet1.

Также может потребоваться система Java (TM) 2 Platform (файл с дистрибутивом – j2re-1\_4\_2\_07-windows-i586-p.exe).



Основная ОС

VMNet1

Виртуальная ОС

4215

Sensor

eth0 10.1.1.3

Рис. 4.7. Схема сетевого соединения Cisco IDS 4215 Sensor и основной ОС

Прежде чем работать с образом Cisco IDS Sensor, необходимо правильно настроить конфигурационный файл образа.

## ВЫПОЛНИТЬ!

1. Запустить VMWare Player, открыть имеющийся образ Cisco IDS 4215 Sensor.
2. Настроить виртуальный сетевой адаптер на тип соединения

Host-only.

1. В каталоге с образом найти файл с расширением .vmx (конфигурационный файл). Открыть его любым текстовым редактором.
2. Найти в файле строку bios440.filename= «...» и модифицировать ее в вид bios440.filename=«/Путь к каталогу с образом / CISCO\_IDS4215\_440. BIOS.ROM».
3. Проверьте наличие строк: ethernet0.virtualDev = «e1000» ethernet1.virtualDev = «e1000» ethernet2.virtualDev = «e1000»
4. Сохранить конфигурационный файл.

Следующий этап работы состоит в настройке операционной системы Linux. Предполагается, что в устройстве должны быть три сетевых интерфейса: один для управления и два для анализа трафика.

## ВЫПОЛНИТЬ!

1. Запустить виртуальную машину (Power on this Virtual Machine).
2. После загрузки системы и появления окна выбора способа загрузки выбрать Cisco IPS и нажать клавишу [e]. Далее выбрать вторую строку с надписью kernel и снова нажать [e].
3. Прокрутить строку влево, пока на экране не появится надпись init=loadrc.
4. Заменить значение loadrc на 1 (чтобы получилось init=1) (рис. 4.8).

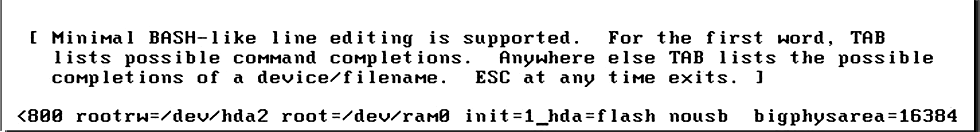


Рис. 4.8. Корректировка загрузки ОС Cisco IDS Sensor

1. Нажать [Enter] и затем клавишу [b] для начала загрузки.
2. Нажать [Enter] для перехода в режим правки.
3. Cменить раскладку клавиатуры на английскую. Ввести:

/loadrc

/etc/init.d/rc.init

touch /usr/share/zoneinfo/cidsZoneInfo.

1. Теперь необходимо выяснить значение быстродействия процессора, для чего ввести следующую команду: **cat /proc/cpuinfo**.
2. Найти строку cpu MHz путем прокрутки списка вниз. Записать или запомнить значение (только целую часть, рис. 4.9).
3. Теперь нужно изменить функциональный файл аппаратного устройства (ids\_functions). Для начала необходимо сделать резервную копию функционального файла аппаратного устройства на случай ошибочной настройки. Ввести:

cd /etc/init.d

cp ids\_functions ids\_functions.orig vi ids\_functions.

1. Прокрутить список вниз до строки 4215, что соответствует линии #252. Найти надпись:

elif [[ ‘isCPU 845’ –eq $TRUE && ... MODEL=$IDS4215

1. Вместо значения 845 ввести ранее записанное значение быстродействия процессора (в примере – 1958, рис. 4.10).

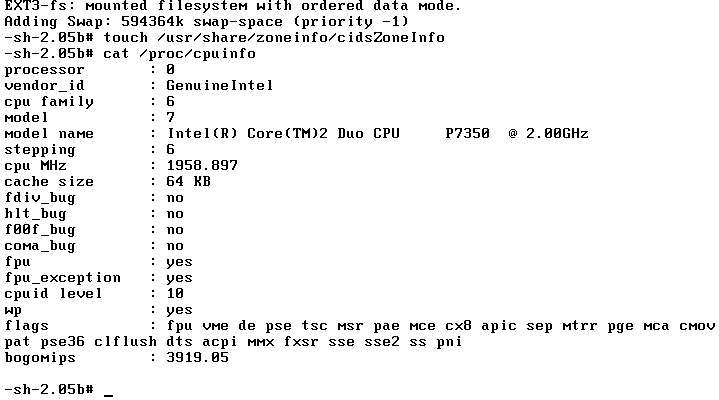


Рис. 4.9. Значение тактовой частоты процессора – 1958 МГц

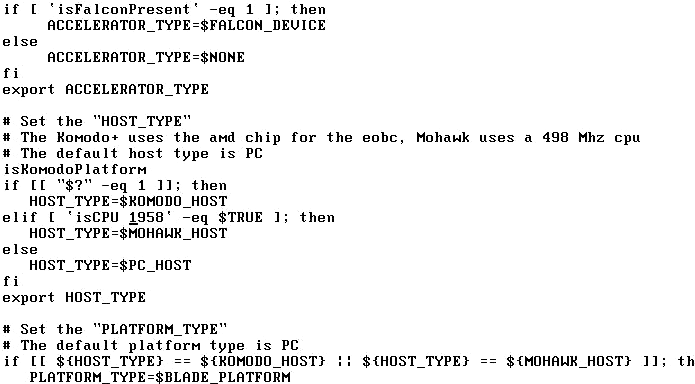


Рис. 4.10. Изменение частоты процессора в ОС Cisco IDS Sensor

1. Найти две строки чуть ниже с надписями DEFAULT\_MGT\_OS и DEFAULT\_MGT\_CIDS. Изменить их следующим способом (рис. 4.11): DEFAULT\_MGT\_OS=”ma0\_0”

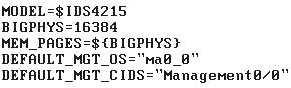
DEFAULT\_MGT\_CIDS=”Management0/0”.

Рис. 4.11. Настройки интерфейса управления ОС Cisco IDS Sensor

1. Сохранить и выйти из режима редактирования.
2. Теперь необходимо изменить конфигурационный файл сетевых интерфейсов. Для этого ввести следующие строки: cd /usr/cids/idsRoot/etc

cp interface.conf interface.conf.orig vi interface.conf

1. Прокрутить список вниз, пока на экране не появится второй раздел IDS-4215. Изменить строки следующим образом:

[models/IDS-4215/slots/1] # lower slot

pci- bus=0 pci-device=17

[models/IDS-4215/slots/2 # upper slot

pci-bus=0

pci-device=19

1. Прокрутить список еще ниже и изменить блок первого интерфейса [models/IDS-4215/interfaces/1] следующим образом: [models/IDS-4215/interfaces/1]

# built-in 10/100 TX mgmt interface, Intel 82559ER # was eth1 (int1) in 4.x

# rightmost connector on front panel # labeled “Ethernet 1” on panel name-template=Management0/0

pci-bus=0

pci-device= 17 pci-function=0 vendor-id=0x8086 device-id=0x100f type=ge

mgmt-capable=yes

1. Изменить теперь второй интерфейс: [models/IDS-4215/interfaces/2]

# built-in 10/100 TX mgmt interface, Intel 82559ER # was eth0 (int0) in 4.x

# leftmost connector labeled “Ethernet 0” name-template= GigabitEthernet0/1

pci-bus=0

pci-device= 18 pci-function=0 vendor-id=0x8086 device-id= 0x100f type=ge

sensing-capable=yes tcp-reset-capable=yes

1. Создать третий интерфейс путем копирования второго и замены значений в строках, как показано ниже:

[models/IDS-4215/interfaces/3] name-template=GigabitEthernet0/2 pci-bus=0

pci-device= 19 pci-function=0 vendor-id=0x8086 device-id=0x100f type=ge

sensing-capable=yes tcp-reset-capable=yes

1. Сохранить настройки, выйти из режима редактирования и перезагрузить ОС командой **reboot**.
2. На данном этапе необходимо изменить пароль учетным записям root, service и cisco при помощи команды **passwd**

# <username>.

1. В случае необходимости можно удалить имеющиеся пароли учетных записей cisco и service командой vi

/etc/passwd. Удалить в учетной записи cisco «крестик» для ее загрузки без пароля. Аналогично сделать с учетной записью service, которую необходимо также разблокировать командой: **passwd -u service**.

1. Сохранить настройки, выйти из режима редактирования и перезапустить устройство командой **reboot**.
2. Выбрать первый способ загрузки (Cisco IPS), и после того как система загрузится и попросит ввести регистрационные данные (sensor login), ввести cisco, а на запрос ввода пароля (password) – пароль, например pbdrc001A.
3. Задать пароль для режима service. Для этого ввести:

**conf t**

**username service pass <password> privy service**

**exit.**

1. Теперь войти в систему с учетной записью service (пароль был установлен на предыдущем шаге). Для перехода в режим администратора (root) ввести **su -**.
2. Теперь открыть файл /usr/share/zoneinfo/cidsZoneInfo. Если не удается открыть, то ввести touch /usr/share/zoneinfo/

/cidsZoneInfo. Без этого файла интерфейс командной строки CLI не будет доступен.

1. Завершить сеанс работы учетной записи service и войдите в систему, используя учетную запись cisco.

Следующий этап работы состоит в первоначальной настройке Cisco IDS 4215 Sensor, а именно в указании IP-адреса (10.1.1.3/24), при обращении к которому можно будет выполнять дальнейшие настройки из web-интерфейса.

## ВЫПОЛНИТЬ!

1. Ввести команду **setup** для перехода в режим системной конфигурации.
2. Нажать клавишу Пробел для перехода к вопросу Continue with configuration dialog? [yes]:. Ввести yes для продолжения.
3. При появлении строки Enter host name[sensor] ввести имя сенсора. По умолчанию имя сенсора – sensor. Можно

задать любое имя длиной до 256 символов без пробела и знака дефис. Нажать [Enter].

1. При появлении запроса Enter IP address[10.1.9.201] ввести

10.1.1.3/24 10.1.1.1. Где 10.1.1.3 – адрес IDS, /24 – маска

255.255.255.0, 10.1.1.1 – адрес шлюза.

1. При появлении запроса Enter telnet-server status [disabled] ввести enable. Ввести команду exit дважды до появления строки Use this configuration?[yes]. Ввести yes.
2. Перезагрузить с помощью команды **reset** и войти, используя учетную запись cisco.
3. Ввести команду **configure terminal** для перехода в режим конфигурирования терминала.
4. Последовательно ввести следующие команды (после ввода команды не забывайте нажимать [Enter]):

**service host** (для перехода в режим конфигурации), **network-settings** (для перехода в режим конфигури- рования сетевых параметров),

**show settings** (для вывода настроек на экран).

1. Для добавления нужной сети (10.1.1.1/24) в список доступа (ACL) необходимо сначала удалить из него адрес ненужной сети, а затем ввести адрес требуемой сети. Для этого ввести следующие команды:

# no access-list 1 access-list 10.1.1.1/24 exit.

1. Затем необходимо вводить команду **exit** до тех пор, пока на экране не появится запрос на применение изменений Apply Changes:?[yes]. Ввести yes.
2. При появлении запроса Continue with reboot?:[yes] ввести

no.

1. Выйти из режима sensor(config)#, используя команду **exit**.
2. Установить дату и время. Для этого ввести:

**clock set hh:mm month day year** (например clock set 15:36 Jan 20 2010).

1. Для перезагрузки системы ввести команду **reset**.
2. Для проверки результатов (а именно того, что теперь возможна настройка Cisco IDS 4215 Sensor с помощью web-интерфейса) в адресной строке браузера основной ОС

ввести https://10.1.1.3/. Обратить внимание, что обмен осуществляется по защищенному каналу SSL (рис. 4.12).

1. При необходимости в системе VMware для сетевых интерфейсов сенсора произвести операцию Disconnect, затем Connect.



Рис. 4.12. Окно Web-интерфейса конфигурирования