### Настройка СОА Cisco IDS Sensor в режиме

***Web-интерфейса***

На данном этапе работы предполагается выполнить основные настройки СОА в режиме Web-интерфейса для обнаружения атак.

## ВЫПОЛНИТЬ!

1. Перейти по адресу интерфейса управления сенсора

https://10.1.1.3.

1. В графическом интерфейсе Cisco IDS Device Manager зарегистрироваться с учетной записью cisco. Откроется окно Cisco IDM 5.1 (рис. 4.13).



Рис. 4.13. Окно Cisco IDM 5.1

Если графический интерфейс не запускается, то необходимо в основной ОС установить систему Java (TM) 2 Platform (файл j2re-1\_4\_2\_07-windows-i586-p.exe). В случае появления ошибки о нехватке памяти следует открыть панель управления – Control Panel (нажать правой кнопкой мыши на иконке Java (TM) 2 Platform в строке состояния и выбрать пункт Open Control Panel). В открыв- шемся окне на вкладке Advanced в строке Java Runtime Parameters ввести -Xmx256m и нажать Apply (рис. 4.14). После перезапустить интерфейс (закрыть все окна и заново перейти по ссылке https://10.1.1.3).



Рис. 4.14. Увеличение объема оперативной памяти для Java

Выполним настройку сетевых интерфейсов.

1. В разделе Configuration (рис. 4.15) выбрать пункт Interface Configuration → Interfaces. Поменять статус обоих интерфейсов GigabitEthernet0/1 и GigabitEthernet0/2 на Ena- bled (Включенный).



Рис. 4.15. Включение сетевых интерфейсов

1. В разделе Configuration выберите Analysis Engine → Virtual Sensor → Edit. Поменять статус интерфейсов GigabitEthernet0/1 и GigabitEthernet0/2, работающих в режиме захвата пакетов, на Assigned (Назначенный, рис. 4.16).



Рис. 4.16. Настройка интерфейсов сенсора

# Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor

### Сигнатуры компьютерных атак СОА Cisco IDS Sensor

Процесс выявления опасной активности в сети заключается в том, что СОА Cisco IDS 4215 Sensor анализируется трафик сети, который сравнивается с сигнатурами, содержащимися в базе зна- ний. Если при анализе трафика сети находятся совпадения в базе сигнатур, то СОА формируются сигналы тревоги, которые затем могут быть записаны в журнал, переданы аппаратному устройству Cisco MARS и по почте и т. п.

Сигнатуры СОА основываются на информационном наполне- нии (content-based) или на контексте (context-based).

Сигнатуры Content-based предназначены для выявления ата- кующего воздействия, содержащегося в полезной нагрузке пакета, например строки URL-запроса.

Сигнатуры Context-based предназначены для выявления атак по заголовкам пакетов в определенных полях или по определенно- му смещению в пределах пакета.

В рассматриваемой СОА существуют четыре основных класса сигнатур:

* + - * исследовательские (reconnaissance);
			* информационные (informational);
			* сигнатуры доступа (access);
			* отказ в обслуживании (denial of service).

Исследовательские – класс сигнатур, позволяющий обнару- жить начальный этап компьютерной атаки – исследование атакуе- мой сети. К таким атакам относятся DNS-атака, сканирование узлов и портов, и т. п.

Информационные – класс сигнатур, позволяющий обнаружить второй этап атакующего воздействия – получение информации об атакуемой системе (например, определение типа и версии системы, сетевых служб).

Сигнатуры доступа – класс сигнатур, позволяющий опреде- лить факт несанкционированного доступа в компьютерную систему.

Отказ в обслуживании – класс сигнатур, позволяющий обна- ружить типы атак, направленных на нарушение работоспособности устройств в сети.

Структура сигнатуры зависит от количества пакетов, которые должны быть проанализированы. Сигнатуры могут быть атомар- ными или составными. Сигнатура называется атомарной, если при обнаружении анализируется отдельный пакет без учета его взаимо- связи с иными пакетами, и составной, если при обнаружении ана- лизируется множество пакетов. При обнаружении сенсором перво- го пакета, который является потенциальной атакой, он анализирует информацию из следующих пакетов.

Например, в случае SYN-атаки отправляется единственный пакет с установленным SYN-флагом без завершения процедуры установления TCP-соединения. Для анализа требуется единствен- ный SYN-пакет вне последовательности. В случае Windows Locator

атаки для обнаружения требуется больше чем один пакет, СОА опознает первый пакет последовательности, пометит его как подо- зрительный и будет отслеживать дальнейшие совпадения с извест- ными последовательностями, используемыми для данной атаки.

Все сигнатуры делятся на серии от 1000 до 11000. Данное де- ление помогает администратору быстрее определить, чем вызвана произошедшая атака. Ниже приведен список некоторых серий сиг- натур СОА Cisco IDS 4215 Sensor:

* + - * 1000 – охватывает сигнатуры, которые анализируют инфор- мацию IP-заголовков;
			* 2000 – охватывает сигнатуры, анализирующие информацию, передаваемую по протоколу ICMP;
			* 3000 – TCP- порты;
			* 4000 – UDP-порты;
			* 5000 – HTTP-трафик;
			* 6000 – сигнатуры мультипротокола;
			* 7000 – ARP-протокола;
			* 8000 – сигнатуры сопоставления строк и др. Также различают следующие типы сигнатур:
			* General Connection (общего подключения);
			* String (строковые);
			* ACL (списка контроля доступа).

Сигнатуры типа General охватывают следующие серии сигна- тур: 1000, 2000, 5000 и 6000. В зависимости от типа атаки General-сигнатуры ищут отклонения в известном типе трафика. Например, удостоверяется, правильно ли ведет себя определенный протокол, или «полезная» информация в пакетах только выглядит правильной. Пример General-сигнатуры: 1037-TCP FRAG SYN FIN Host Sweep. Эта сигнатура вызывается, когда последовательность TCP-пакетов с SYN- и FIN- набором флагов отправлена множеству узлов с тем же самым портом адресата. Одновременное наличие флагов SYN и FIN является недопустимым.

Сигнатуры типа Connection охватывают 3000 и 4000 серии. Они анализируют трафик UDP-портов и TCP-соединений. Пример Connection-сигнатуры: 3001-TCP Port Sweep. Данная сигнатура дей- ствует тогда, когда последовательность TCP-подключений опреде- лена на аппаратном устройстве ко многим портам. Диапазон портов – меньше чем 1024.

Сигнатуры типа String универсальны и контролируют строки (текст) в пределах пакетов, которые считаются важными. Пример string-сигнатуры: 8000:2303-Telnet-+ + (Telnet сеанс инициализиро- ван, и введена команда «++»).

Сигнатуры ACL применяются для анализа трафика с целью выявления деятельности, связанной с попытками обхода списков контроля доступа на маршрутизаторах. Эти сигнатуры относятся к серии 10000. Пример ACL-сигнатуры: 10000:1001-IP-Spoof Interface 2.

На рис. 4.17 изображен фрагмент окна с сигнатурами серии 2000, выделена сигнатура 2000-ICMP Есhо Reply, которая срабаты- вает на исходящий ICMP эхо-ответ.



Рис. 4.17. Фрагмент окна настройки сигнатур обнаружения

По результатам анализа СОА выдает предупреждения (Alarm), каждому из которых назначен уровень тревоги: низкий (Low, 3), средний (Medium, 4), и высокий (High, 5). Также предупреждения могут быть еще двух уровней – неиспользуемый (None, 1) и ин- формационный (Informational, 2).

Кроме того, используются служебные тревожные сообщения (сигнатуры 900-999). В частности, требует внимания сигнатура 993-Missed Packet Count. Появление данного сигнала тревоги свя- зано с пропуском пакетов при анализе, что свидетельствует о за- груженности СОА.

## ВЫПОЛНИТЬ!

1. Найти следующие сигнатуры обнаружения атак:
	* 2000-ICMP Есhо Reply;
	* 2004-ICMP Есhо Request;
	* 3002-TCP SYN Port Sweep.