### Обнаружение атак исследования сетевой топологии

Выполним обнаружение двух атак, относящихся к классу ис- следовательских – ICMP-сканирование узла и SYN-сканирование портов. ICMP-сканирование выполним с помощью штатной утили- ты ping, для сканирования портов будет использован сканер nmap.

## ВЫПОЛНИТЬ!

1. В основной ОС выполнить ICMP-сканирование узла-«жертвы» (настроенной, например, на IP-адрес 10.10.10.50). Результатом будет получение четырех ICMP-пакетов типа Есhо Reply (рис. 4.18).

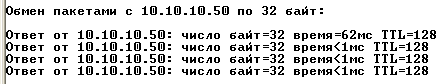


Рис. 4.18. Атакующее воздействие – ICMP-запросы и ответы на них

1. В разделе Monitoring (рис. 4.19) выбрать пункт Events. Установить фильтр отображения предупреждений, сформированных за определенный интервал времени (в примере – 1 минута) и нажать кнопку View.

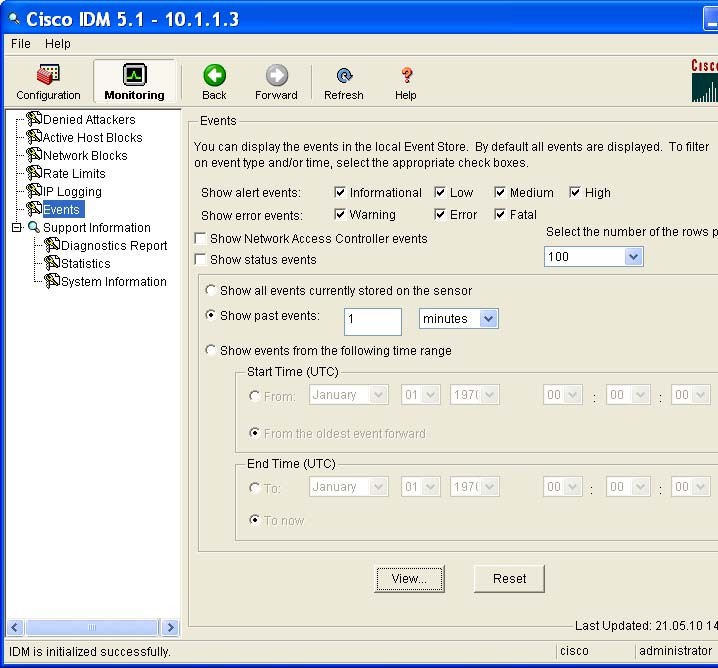


Рис. 4.19. Установка фильтра отображаемых событий

В полученной таблице (рис. 4.20) должны присутствовать предупреждения уровня опасности – информационные (столбец Type), указывающие на зафиксированное атакующее воздействие.

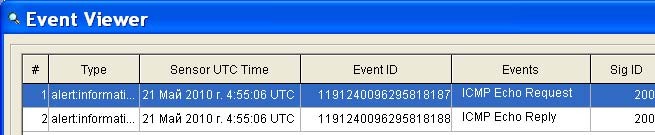


Рис. 4.20. Просмотр списка событий

1. Открыть одно из событий (рис. 4.21). Обратить внимание на уровень сообщения (severity), описание сигнатуры события, его серию и номер, уровень риска (riskRatingValue). В отчете описать обнаруженную атаку. Указать адрес источника атакующего воздействия. Привести снимок окна с детализацией события.

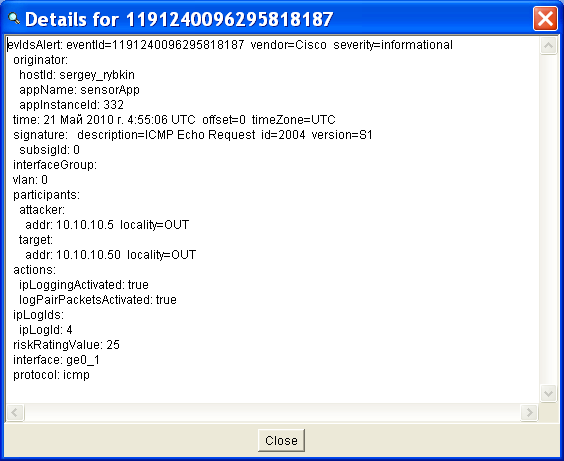


Рис. 4.21. Детализированное представление события

1. В основной ОС выполнить сканирование портов узла-

«жертвы» с помощью сканера nmap в оболочке Zenmap (рис. 4.22).

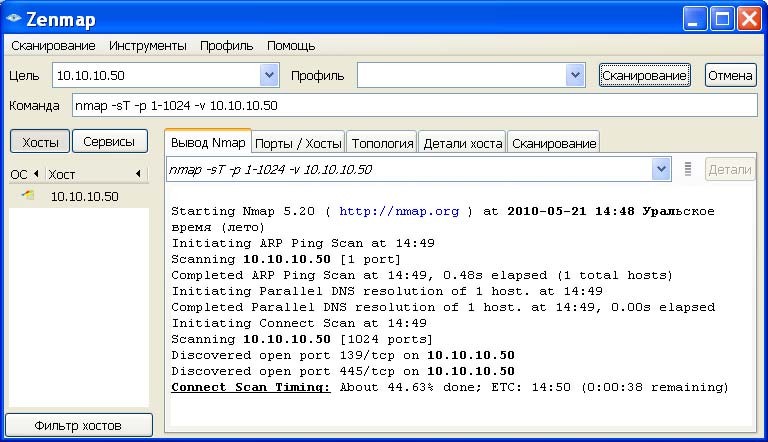


Рис. 4.22. Атакующее воздействие – сканирование портов

1. Просмотреть события, зафиксированные СОА (рис. 4.23). Обратить внимание на иной уровень опасности данного атакующего воздействия – низкий.

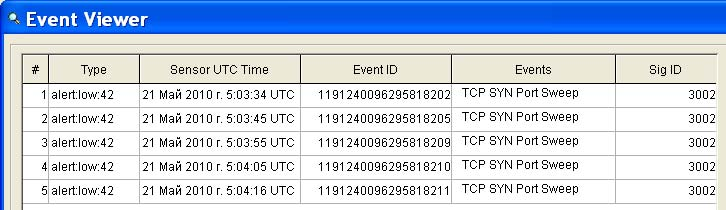


Рис. 4.23. Предупреждения об атакующем воздействии

1. Открыть одно из событий для его детального анализа (рис. 4.24). Обратить внимание на уровень сообщения, описание сигнатуры события, его серию и номер, уровень риска, а также на перечень портов, перебор которых был зафиксирован СОА. В отчете описать обнаруженную атаку. Указать адрес источника атакующего воздействия. Привести снимок окна с детализацией события.



Рис. 4.24. Детализация события – сканирование портов

1. В основной ОС повторно выполнить сканирование портов узла-«жертвы» с целью определения типа и версии операционной системы также с помощью оболочки Zenmap (рис. 4.25).
2. Получить список обнаруженных атак (рис. 4.26). Найти и описать в отчете атаки со средним и высоким уровнем опасности. Привести уровень сообщения, описание сигнатуры события, его серию и номер, уровень риска, а также источник атакующего воздействия. Привести снимки окон с детализацией событий.

Таким образом, в результате выполнения практического зада- ния отработана технология обнаружения атак на основе методов сигнатурного анализа. В процессе работы выполнена настройка об- раза ОС Linux с установленным ПО СОА Cisco IDS Sensor. Настро- ено подключение для управления СОА в режиме web-интерфейса.

В отчете должны быть представлены результаты обнаружения трех атак: ICMP-сканирования, сканирования портов и сбора ин- формации о типе ОС узла-«жертвы».

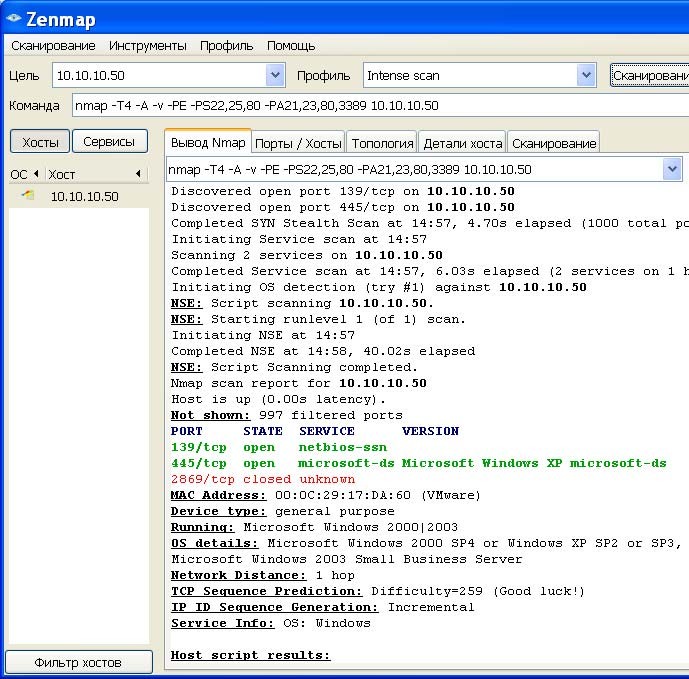


Рис. 4.25. Атакующее воздействие – сбор информации

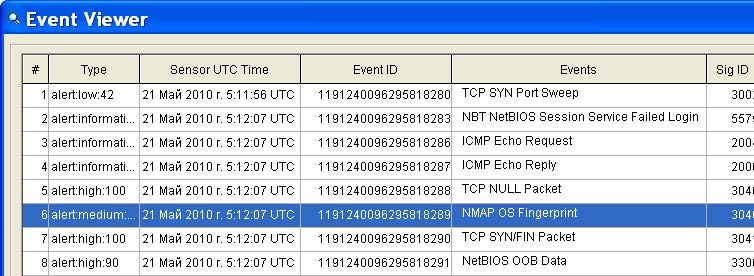


Рис. 4.26. Обнаружение атаки по сбору информации об узле

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Какие задачи решаются с помощью СОА?
2. Для чего предназначен компонент СОА – сенсорная подсис- тема?
3. Какую функцию выполняют интегрированные в сенсор технологии Cisco Threat Response, Threat Risk Rating и Meta Event Generator?
4. Перечислите элементы сети, где согласно рекомендациям производителя следует размещать сенсор.
5. Опишите структуру сигнатуры.
6. Назовите существующие в сенсоре классы сигнатур.