Практическая работа

Тема: Установка и настройка системы обнаружения вторжений ViPNet IDS NS

Цель: Получить опыт установки и настройки системы обнаружения вторжений уровня сети.

Теоретические сведения

ViPNet IDS NS – это сетевой сенсор обнаружения сетевых атак и вредоносного программного обеспечения в файлах, передаваемых в сетевом трафике, и предназначенный для интеграции в компьютерные сети с целью повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

ViPNet IDS NS может использоваться как самостоятельный продукт, а также в составе решений ViPNet Threat Detection and Response (TDR) и совместно с решением ViPNet Channel Protection.

ViPNet IDS NS представлен следующими исполнениями:

- ViPNet IDS NS100;
- ViPNet IDS NS1000;
- ViPNet IDS NS2000;
- ViPNet IDS NS10000;
- Виртуальное устройство ViPNet IDS NS VA.

Может быть использован как для небольших офисов, так и для ЦОДов.

Практическая часть

1. Развернуть и настроить виртуальный стенд для IDS.

Для стенда нужны 3 виртуальные машины: Kali Linux, Windows 10 (или Metasploitable) и VipNet IDS.

- Kali Linux – виртуальная машина (установленная ОС) находится на HDD вашего ПК или на сервере.
- Windows 10 (или Metasploitable) можно также найти на ПК или сервере, не забыть откатиться к раннему снимку состояния.
- ViPNet IDS – образ для развёртывания виртуальной машины имеется также на HDD вашего ПК или на сервере.

Данные для аутентификации

Kali Linux: логин – Kali, пароль – Kali.

ViPNet IDS: первичный вход - idsuser/vipnet, вход в консоль управления – admin/vipnet.

Настройки сети: ViPNet IDS – настраиваются 2 сетевых адаптера, один для управления с хостовой машины (можно Bridge или NAT), другой адаптер для внутренней сети (VMnet или сегмент). Windows (Metasploitable) и Kali по 1 сетевому адаптеру во внутреннюю сеть.

2. Установка ViPNet IDS

- Установить ViPNet IDS
- Активировать лицензию
- Настроить нового администратора системы с полным доступом (officer).
- Настроить сетевые интерфейсы управления и перехвата

3. Базовая работа с правилами ViPNet IDS VA

- Создать и применить пользовательское правило ViPNet IDS VA обнаружения попыток доступа к сетевым папкам виртуальной машины (win). Проверить выполнение с помощью виртуальной машины.
- Провести детектирование трафика согласно указанным правилам с помощью IDS

  Зафиксировать выполнение задания (правила и обнаруженные события в IDS) скриншотами.

4. Проверка системы на выявление известной атаки

- Самостоятельно, с помощью утилит Kali Linux или аналогичных имитировать атаку (НСД, DoS) на уязвимую виртуальную машину. Конкретный вектор атаки определяет участник.
- Зафиксировать детектирование атаки с помощью IDS-VA: вкладка События