ПР3 5 Threat Hunting

Threat Hunting - это процесс активного поиска и обнаружения угроз безопасности. Это практическое занятие по Threat Hunting состоит из 10 заданий, которые могут быть выполнены с использованием операционной системы Linux.

1) Создайте внутреннюю сеть виртуальных машин (VM) или контейнеров: Создайте среду с несколькими виртуальными машинами или контейнерами, чтобы имитировать потенциальные уязвимости и атаки(одна из виртуальных машин будет служить сервером для атаки). https://www.virtualbox.org/wiki/Downloads https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-12.1.0-amd64-netinst.iso
2) Установите и настройте систему мониторинга: Для этого можно использовать инструменты, такие как Wazuh (https://wazuh.com/) или DSIEM (https://github.com/defenxor/dsiem). Выберите источники данных для мониторинга и разверните их для дальнейшего выявления угроз с использованием базы правил https://github.com/archanchoudhury/Detection-Rule-Dump.
3) Разверните уязвимые сервисы/сборки ОС в составе стенда.
4) Создайте профили источников данных: Определите, какие источники данных будут использоваться для мониторинга сети. Некоторые примеры: логи сетевых устройств(journalctl -u NetworkManager.service), логи операционной системы(ls -l /var/log/), события IDS/IPS и т. д.
5) Создайте правила обнаружения: Настройте правила обнаружения для каждого источника данных, чтобы автоматически обнаруживать потенциальные угрозы безопасности. Примеры инструментов для создания правил обнаружения: Snort (https://www.snort.org/), Suricata (https://suricata-ids.org/).
6) Настройте инструменты для мониторинга и обнаружения угроз безопасности, а также анализа данных. Примеры таких инструментов: Zeek (https://zeek.org/), YARA (https://virustotal.github.io/yara/).
7) Запустите сканеры уязвимостей: Используйте инструменты, такие как OpenVAS (https://www.openvas.org/) или Nessus (https://www.tenable.com/products/nessus), чтобы сканировать виртуальную среду на наличие уязвимостей.
8) Создайте «локальные» угрозы безопасности: Искусственно создайте угрозы безопасности, например, с помощью инструментов Metasploit

(https://www.metasploit.com/) или Burp Suite (https://portswigger.net/burp).

9) Анализируйте потенциальные угрозы: Используйте логи и инструменты мониторинга для выявления потенциальных угроз безопасности.
10) Подготовьте отчеты о найденных угрозах и уязвимостях с указанием их критичности и предложениями по их устранению.

По результатам выполнения задания Вы должны:

1. Собрать стенд по заданию

2. Развернуть СЗИ (на выбор) по одному из каждого класса: SIEM (Wazuh/DSIEM),

IDS/IPS (Snort/Suricata),

Scanner (OpenVAS/Nessus),

ThreatHuntingTools (Zeek/YARA).

3. Подготовить отчет со скриншотами о проделанной работе и выявленных инцидентах каждым из классов защиты.

4. Отчет предоставить в срок до 13.12.23.

Задание является обязательным для допуска к зачету.