АВТОМАТИЗАЦИЯ ИНСТРУМЕНТА NMAP ДЛЯ СКАНИРОВАНИЯ КОРПОРАТИВНОЙ СЕТИ С МЕЖСЕТЕВЫМ ЭКРАНОМ PFSENSE

Н.А. Рощупкин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

pfSense – это бесплатный межсетевой экран с открытым исходным кодом, основанный на операционной системе FreeBSD [1]. Он включает в себя пакеты с открытым исходным кодом для расширенных возможностей. Выбор межсетевого экрана pfSense обусловлен тем, что он является одним из самых популярных и свободно распространяемых межсетевых экранов. Это дает возможность детально изучать его исходный код, а также использовать его для построения обучающих стендов без необходимости приобретения лицензии.

Цель работы данной работы заключается в демонстрации применения инструмента Nmap для сканирования и тестирования безопасности корпоративной сети, а также в разработке автоматизированного скрипта для контроля сетевого периметра с использованием Nmap.

В результате достижения поставленной цели также был разработан образовательный стенд с возможностью активного мониторинга и моделирования атак на инфраструктуру корпоративной сети. Образовательный стенд состоит из зон DMZ и LAN. Эти зоны разделены межсетевым экраном pfSense, включающим в себя плагин Suricata [2], способный обнаруживать все попытки несанкционированного сканирования периметра (T1595 MITRE ATT&CK) [3] и отправлять журналы в систему SIEM, построенную на базе Opensearch Stack (Opensearch, Opensearch Dashboards, Logstash) [4]. Стенд развернут на базе платформы виртуализации VirtualBox. В зоне DMZ находится веб-сервер, работающий на основе дистрибутива Debian 4.19.181-1. В зоне LAN расположен хост с операционной системой Windows 10. Обе виртуальные машины демонстрируют базовые уязвимости, такие как Script Privilege Esalation, Remote File Inclusion, EthernalBlue, Weak Password, SQL Injection и другие, с целью дальнейшего использования стенда в образовательных целях.

Таким образом, внедрение разработанного образовательного стенда в учебный процесс на кафедре защиты информации будет способствовать развитию следующих навыков у учащихся:

1 Конфигурация межсетевого экрана pfSense с выделение демилитаризованной зоны.

2 Работа с системами мониторинга и журналирования событий информационной системы.

3 Тестирования и определение уязвимостей информационной системы с помощью автоматизированного инструмента Nmap на базе межсетевого экрана pfSense.

4 Устранение выявленных уязвимостей в информационной системе.

Список литературы

1. Межсетевой экран pfsense [Электронный ресурс]. – Режим доступа: https://www.pfsense.org/. – Дата доступа: 07.05.2024.

2. Система обнаружения и предотвращения вторжений Suricata [Электронный ресурс]. – Режим доступа: https://suricata.io/. – Дата доступа: 07.05.2024.

3. Техника активного сканирования матрица MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/techniques/T1595/. – Дата доступа: 07.05.2024.

4. Визулизатор логов Opensearch [Электронный ресурс]. – Режим доступа: https://opensearch.org/. – Дата доступа: 07.05.2024.