Внешний аудит безопасности корпоративных сетей

Лекция 13
Сканеры уязвимостей

Семён Новосёлов

2022

Введение

Сканеры уязвимостей предназначены для автоматизированного поиска известных проблем безопасности в системах.

Виды сканеров:

- Сетевые сканеры
- Локальные сканеры
- Специализированные сканеры под конкретные приложения / протоколы

Локальное сканирование

- Представляет собой поиск ошибок конфигурации и сканирование установленных программ на уязвимости.
- Для такого сканирования сканеру необходимо указывать данные для входа в систему (например, логин/пароль к ssh).

Принцип работы сетевых сканеров

Сканирование версий сервисов

NVD

Автоматический поиск по базам уязвимостей

CVE®

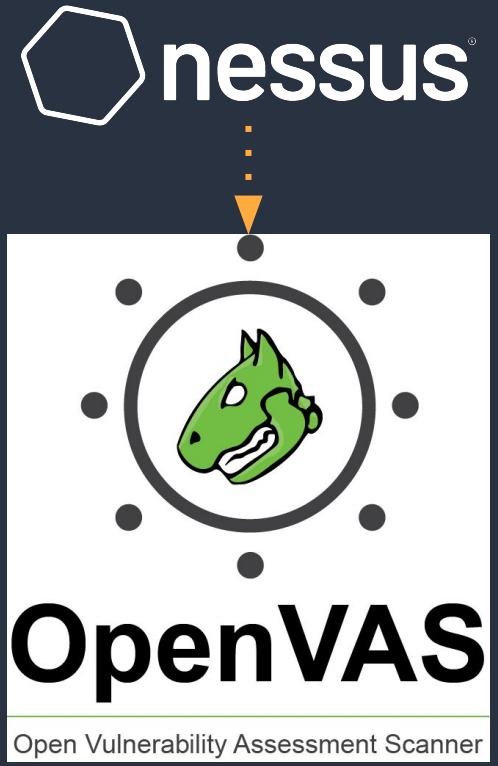
Оценка опасности уязвимостей / рекомендации по устранению

CVSS

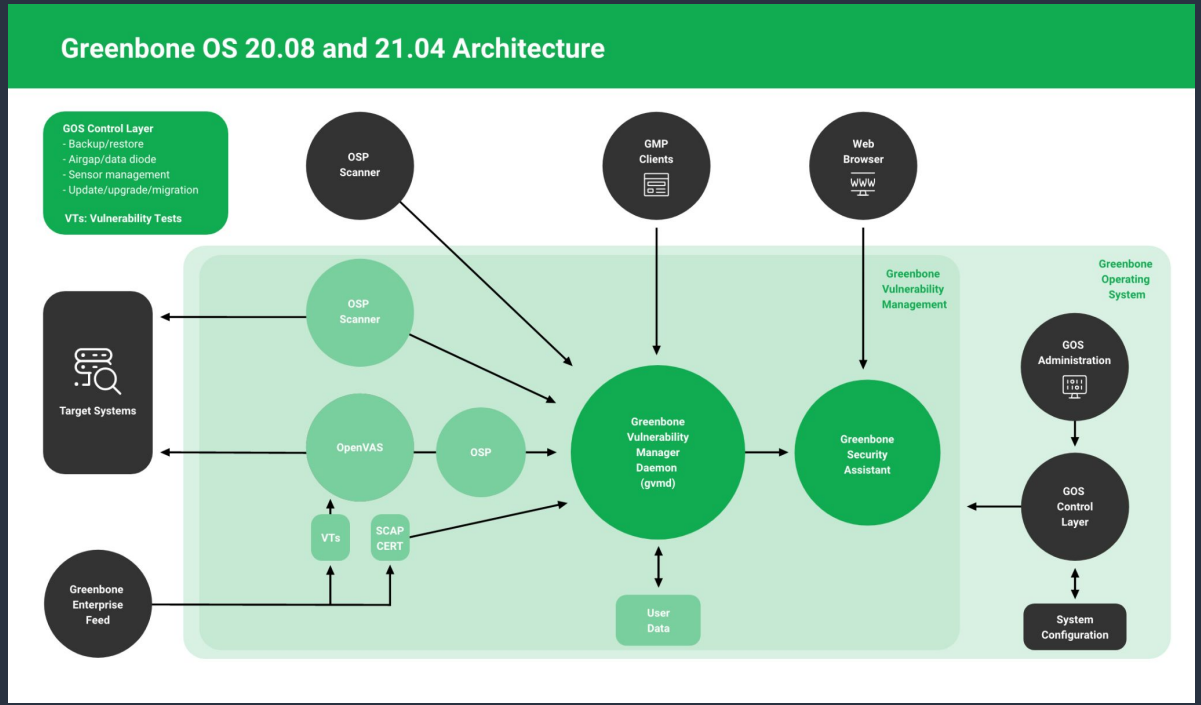
Сканер уязвимостей OpenVAS

OpenVAS — форк коммерческого сканера Nessus, появившийся после того как разработчики Nessus закрыли исходный код.

- В настоящее время сканер является частью Greenbone Vulnerability Management (GVM)



Архитектура GVM



https://docs.greenbone.net/GSM-Manual/

Установка и настройка GVM

На примере Kali Linux.

1. Установить Greenbone Vulnerability Management:
   sudo apt install gvm
2. Запустить скрипт первоначальной настройки:
   sudo gvm-setup
   - будут в том числе загружены версии скриптов, базы уязвимостей CVE/NVD

   Важно: записать пароль для входа после завершения установки

3. Проверить корректность установки:
   sudo gvm-check-setup
4. Запустить GVM (sudo gvm-start) и открыть ссылку: http://127.0.0.1:9392

Запуск сканирования

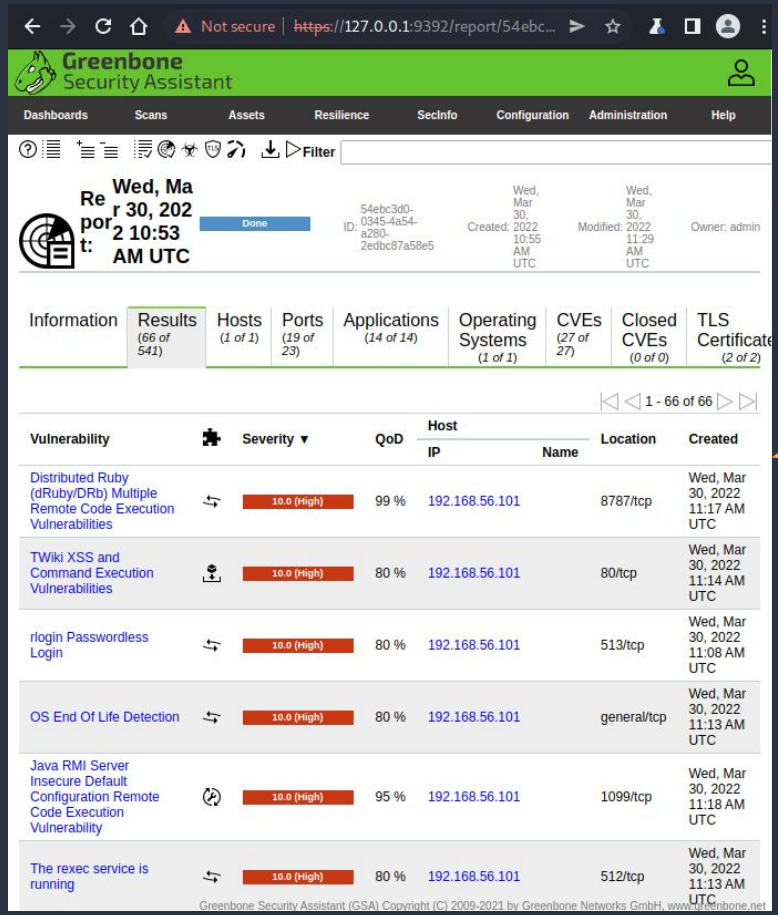
Задание цели:

Configuration ⇨ Targets ⇨ New Target

Для локального сканирования необходимо также указать данные для входа (например, логин/пароль к ssh).

Запуск сканирования:

Scans ⇨ Tasks ⇨ New Task ⇨ Start Task



Результат сканирования Metasploitable 2 с помощью GVM/OpenVAS

Специализированные сканеры

Nikto — сканер веб серверов на проблемы безопасности: устаревшие версии, ошибки конфигурации, …
https://cirt.net/Nikto2

WPScan

WPScan — сканер уязвимостей в Wordpress
https://github.com/wpscanteam/wpscan

Wapiti — сканер уязвимостей веб-приложений, включая SQLi, XSS, shellshock. Работает на основе фаззинга.
https://wapiti-scanner.github.io/