

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

CSS

Сканер уязвимостей OpenVAS

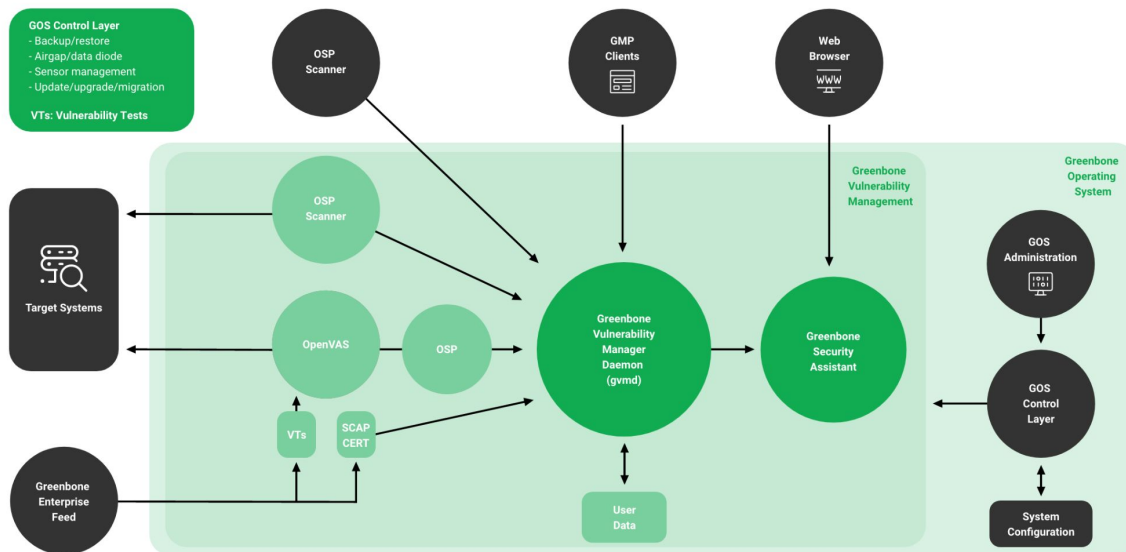
OpenVAS — форк коммерческого сканера Nessus, появившийся после того как разработчики Nessus закрыли исходный код.

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



Архитектура GVM

Greenbone OS 20.08 and 21.04 Architecture



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:



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

Запуск сканирования:



Greenbone Security Assistant

Report: Wed, Mar 30, 2022 10:53 AM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificate

(66 of 541) (1 of 1) (19 of 23) (14 of 14) (1 of 1) (27 of 27) (0 of 0) (2 of 2)

1 - 66 of 66

Vulnerability	Severity	QoD	Host		Location	Created
			IP	Name		
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (high)	99 %	192.168.56.101		8787/tcp	Wed, Mar 30, 2022 11:17 AM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (high)	80 %	192.168.56.101		80/tcp	Wed, Mar 30, 2022 11:14 AM UTC
rlogin Passwordless Login	10.0 (high)	80 %	192.168.56.101		513/tcp	Wed, Mar 30, 2022 11:08 AM UTC
OS End Of Life Detection	10.0 (high)	80 %	192.168.56.101		general/tcp	Wed, Mar 30, 2022 11:13 AM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (high)	95 %	192.168.56.101		1099/tcp	Wed, Mar 30, 2022 11:18 AM UTC
The rexec service is running	10.0 (high)	80 %	192.168.56.101		512/tcp	Wed, Mar 30, 2022 11:13 AM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. www.greenbone.net

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 — 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/>