05.11.2023

Курс:

Практическая работа к уроку № Lesson_3

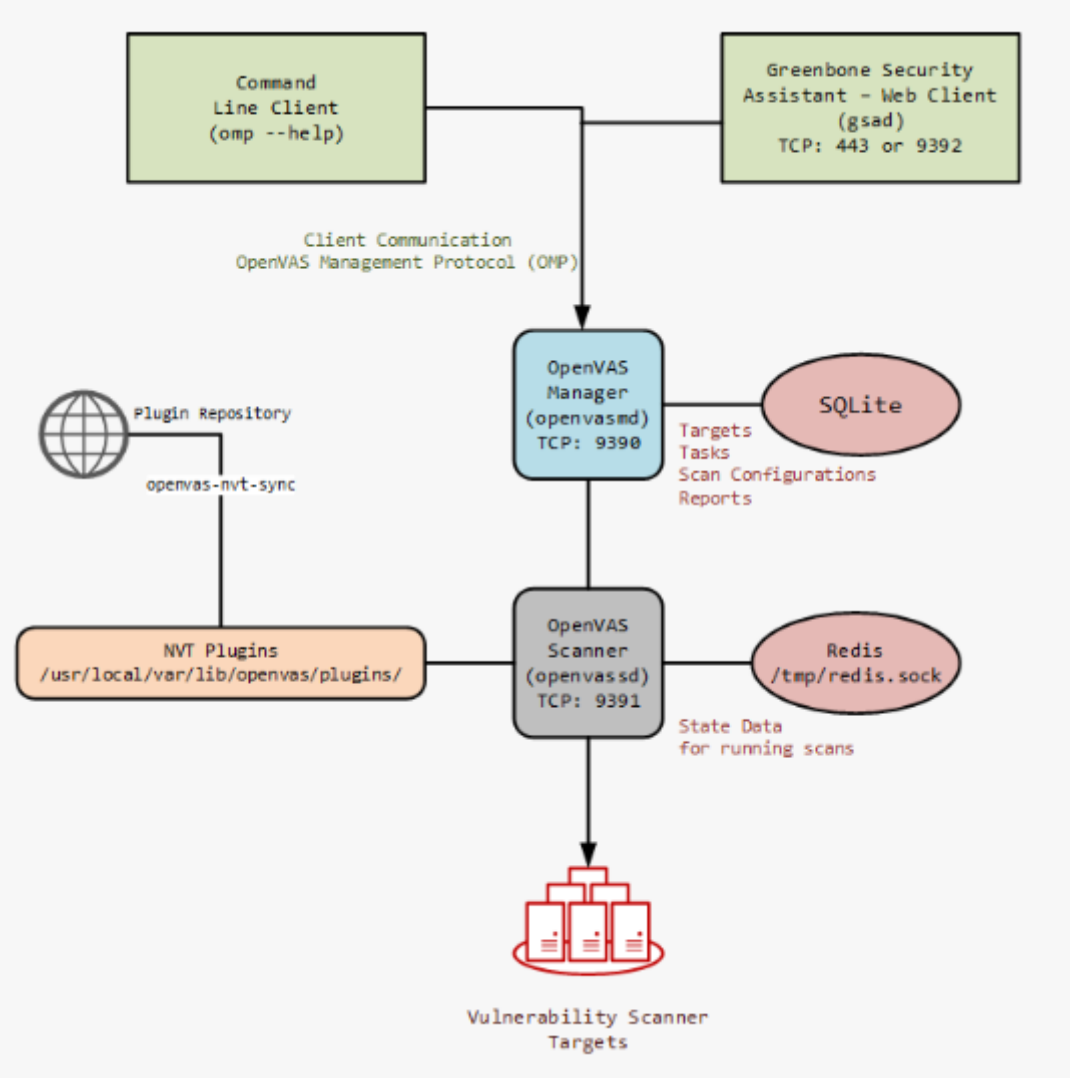
--
Активные сетевые атаки

Задание_1:

Установить OpenVAS в Kali Linux.

OpenVAS — это набор решений для комплексного сканирования сетевых ресурсов на уязвимости и управления найденными.

```
sudo su
apt install openvas
ps -aux|grep openvas
ps -aux|grep gsad
netstat -antp
```



- Updating NVT — обновление базы NVT;
- Updating SCAP data — обновление базы SCAP, которая содержит БД автоматизированного управления уязвимостями OpenSCAP (Security Content Automation Protocol);
- Updating CERT data — обновление сертификатов.

Задание_2:

Установить систему DVL Linux в качестве виртуальной машины, настроить сетевой доступ к ней со стороны Kali Linux и просканировать систему DVL Linux на наличие уязвимостей.

Установить систему DVL Linux в качестве виртуальной машины (ссылка для скачивания https://sourceforge.net/projects/virtualhacking/files/os/dvl/DVL_1.5_Infectious_Disease.iso/download, можно просто загрузиться с iso образа), настроить сетевой доступ к ней со стороны Kali Linux и просканировать систему DVL Linux на наличие уязвимостей.

Задание_3:

(*) Установить виртуальную машину на базе Windows 7 (8, 8.1 или 10), активировать сетевой доступ к общим папкам. Просканировать ВМ при помощи OpenVAS с использованием данных

протокола SMB.

Выводы:

Сканер можно применять шире:

- установить OpenVAS в ОС Linux, отличную от Kali Linux, и использовать его как отдельное решение для сканирования сетевых ресурсов;
- планирования с помощью OpenVAS стратегию внедрения политики безопасности и приоритизации рисков;
- использовать OpenVAS в сочетании с metasploit, если требуется единая платформа для анализа защищенности сети

Ссылки / дополнительные материалы

1. https://ru.wikipedia.org/wiki/Переполнение_буфера.
2. https://www.veracode.com/security/buffer-overflow.
3. https://habr.com/company/1cloud/blog/252991/.
4. https://habr.com/post/136046/.
5. https://nmap.org/nsedoc/categories/vuln.html.
6. https://linoxide.com/linux-how-to/install-security-updates-ubuntu/.
7. https://vulners.com/help.
8. https://www.ptsecurity.com/ru-ru/products/xspider/.
9. http://www.openvas.org/software.html.
10. https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/.
11. http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/openvasmd.
12. http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/openvassd.
13. http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/gsad.
14. https://habr.com/company/pentestit/blog/323568/.

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- https://gb.ru

Выполнил: AndreiM