**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ**

**КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Поволжский государственный университет телекоммуникаций и информатики»**

КОЛЛЕДЖ СВЯЗИ

Технологическая карта №2

по

УП.09 Обеспечение безопасности Веб-приложений

Выполнили:

Студентыbгруппы 3ИСПВ-2к

Петров Даниил

Проверил:

Преподаватель КС ПГУТИ Ахмедова К.Р

Самара 2024

|  |  |
| --- | --- |
| Утилита или ПО | Назначение/Функции |
| Nessus | Популярный сканер уязвимостей, используемый для выявления проблем безопасности в сетях и системах. Он предоставляет подробные отчеты о уязвимостях и неправильных настройках. |
| OpenVAS | Открытый сканер уязвимостей, который также ищет слабые места в сетях и хостах. Он аналогичен Nessus, но бесплатен. |
| Lynis | Инструмент для аудита безопасности, который анализирует конфигурации, настройки и потенциальные уязвимости системы. |
| OWASP Zed | Сканер безопасности веб-приложений и инструмент для тестирования на проникновение. Он помогает выявить уязвимости в веб-приложениях. |
| SPARTA | Инструмент для тестирования на проникновение инфраструктуры сети, который автоматизирует сбор информации, сканирование и перечисление. |
| Metasploit | Мощный фреймворк для разработки, тестирования и выполнения эксплойтов против удаленных целей. Широко используется для тестирования на проникновение. |
| fping | Утилита Fping предназначена для быстрого сканирования доступности хостов в сети. Она позволяет проверить, отвечает ли хост на ICMP-запросы (пинг). |
| Network MapperNmap | Универсальный инструмент для сканирования сети, который обнаруживает хосты, службы и открытые порты. |
| HTTrack | Инструмент для зеркалирования веб-сайтов, который позволяет загружать целые веб-сайты для офлайн-просмотра. |
| Fierce | Инструмент для DNS-реконнесанса, который помогает обнаруживать поддомены, связанные с целевым доменом. |
| Maltego | Графический инструмент анализа связей, используемый для открытого сбора информации (OSINT) и сбора данных. |
| Dig | Утилита Dig (Domain Information Groper) используется для выполнения DNS-запросов. Она позволяет получить информацию о доменных именах, IP-адресах, записях MX и других DNS-данных. |
| Wireshark | Анализатор протоколов сети, который захватывает и анализирует сетевой трафик. Полезен для устранения неполадок и анализа безопасности. |
| Bettercap | Фреймворк для атак на сеть, выполняющий атаки типа “человек посередине”, манипуляцию пакетами и другие действия. |
| Nikto | Сканер веб-серверов, который выявляет общие уязвимости и неправильные настройки в веб-приложениях. |
| Wapiti | Еще один сканер уязвимостей в веб-приложениях, который проверяет наличие уязвимостей. |
| Skipfish | Сканер безопасности веб-приложений, который обходит и анализирует веб-страницы на предмет уязвимостей. |
| WPScan | WPScan - это бесплатный инструмент для сканирования уязвимостей в WordPress. Он предназначен для тестирования безопасности веб-сайтов, использующих эту популярную платформу для управления контентом. |
| WhatWeb | WhatWeb - это инструмент для “отпечатков” веб-сайтов. Он анализирует технологии, используемые на сайте, и помогает определить, какие CMS, фреймворки и другие компоненты используются. |
| Burp Suite | Комплексный инструмент для тестирования безопасности веб-приложений, включающий прокси, сканер и другие функции. |
| sqlmap | Инструмент для обнаружения и эксплуатации уязвимостей SQL-инъекций в веб-приложениях. |
| John The Ripper | Инструмент для восстановления паролей, который может атаковать хеши паролей различных форматов. |
| THC Hydra | Быстрый и гибкий инструмент для брутфорса паролей, поддерживающий множество протоколов. |
| Hashcat | Мощный инструмент для восстановления паролей, поддерживающий различные алгоритмы хеширования. |
| Aircrack-ng | Набор инструментов для оценки безопасности Wi-Fi, включая взлом WEP и WPA/WPA2. |
| App-Ray | Сканер безопасности мобильных приложений, который выявляет уязвимости в Android и iOS-приложениях. |
| Wifite2 | Автоматизированный инструмент для взлома Wi-Fi, который взламывает ключи WEP, WPA и WPS. |
| mitmproxy | Прокси-сервер для перехвата и модификации HTTP/HTTPS-трафика. |
| Autopsy | Платформа для цифровой судебной экспертизы, предназначенная для анализа образов дисков и файловых систем. |
| Social-Engineer Toolkit | Фреймворк для атак социальной инженерии, включая фишинг и сбор учетных данных. |
| Reaver | Инструмент для брутфорса WPS-PIN для взлома паролей Wi-Fi WPA/WPA2. |
| pwnat | Инструмент для обхода NAT и проксирования, полезный для обхода брандмауэров. |
| smali | Дизассемблер/ассемблер для формата байт-кода DEX в Android. |
| Yersinia | Инструмент для анализа и атак на протоколы сетевого уровня, такие как STP, CDP, HSRP и другие. |
| Kismet Wireless | Обнаружение беспроводных сетей, сниффинг трафика и система обнаружения вторжений. |
| Snort | Открытая система обнаружения и предотвращения вторжений (IDS/IPS). |
| weevely | Веб-оболочка для выполнения команд на удаленных серверах через HTTP/HTTPS. |
| mimikatz | Инструмент для извлечения паролей, ключей и другой информации из памяти Windows. Часто используется для анализа безопасности и тестирования на проникновение. |
| spiderfoot | Инструмент для сбора информации об уязвимостях, учетных записях, доменах и других аспектах целевой системы. |

**Ссылки:**

1. **<https://www.kali.org/tools/>**
2. **<https://www.educba.com/kali-linux-tools-list/>**
3. **<https://www.kali.org/docs/general-use/metapackages/>**
4. **<https://en.kali.tools/all/?category>**
5. **<https://www.geeksforgeeks.org/kali-linux-tools/>**
6. **<https://ru.wikipedia.org/wiki/Kali_Linux>**
7. **<https://github.com/topics/kali-tools>**
8. **<https://www.kali.org/tools/all-tools/>**
9. **<http://http.kali.org/kali>**
10. **<https://web.whatsapp.com/>**
11. **<https://www.hackers-arise.com/post/2019/05/14/Web-App-Hacking-Part-13-Web-site-Fingerprinting-and-Vulnerability-Scan>**
12. **[https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/](https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/https:/www.kali.org/docs/general-use/kali-linux-sources-list-repositories/)**
13. **<https://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/>**

**Контрольные вопросы:**

**1.**Существует три основных категории (класса) уязвимостей:

-*уязвимости при разработке* — обнаруживаются из-за недостатков в технических

требованиях к программному обеспечению;

-*уязвимости реализации* — технические ошибки безопасности, найденные в коде системы;

*-эксплуатационные уязвимости* — уязвимости, которые могут возникнуть из-за

неправильной настройки и разворачивания системы в целевой среде.

1. Локальная уязвимость - получение доступа злоумышленником, при выполнении кода, получая больше прав и получения неограниченного доступа к компьютеру.
2. Удаленная уязвимость — это состояние, при котором злоумышленник еще не имеет доступа,

но может его получить, запустив вредоносную часть кода через сеть.