Лабораторная работа №3

БАЗОВЫЕ МЕТОДЫ АКТИВНОГО СБОРА ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ОБЪЕКТА ЗАЩИТЫ

1. Цель и задачи работы

Ознакомится с основными методами сканирования сети защищаемых или анализируемых объектов с использованием, специализированных средств.

2. Теоретические положения

Использование методов активного сбора информации являются одним из основных этапов проведения аудита и проверки уровня защищённости автоматизированных систем.

В качестве базовых средств активного сбора информации наиболее часто используются следующие.

1.NMap – средство сканирования портов и служб с консольным интерфейсом и открытым исходным кодом.

2.ZenMap – одна из версий NMap для ОС Windows, имеет улучшенный интерфейс и GUI, но по формату команд полностью совместим с NMap.

Предложенные средства позволяет искать следующую информацию.

1. Информацию об открытых портах сервера цели. По умолчанию выдаёт данные по первой 1000 портов.
2. Информацию о версиях сетевых служб, отрытые порты которых были обнаружены.
3. Информация о версии операционной системы, установленной на сервере – цели.
4. Информацию об IP адресах и всех открытых портах компьютеров анализируемой АС.
5. Отправка ошибочных пакетов, имитирующих разрыв соединения.
6. Сканирование сети с автоматической проверкой на наличие стандартных уязвимостях.
7. Получение топологии сети. В случае использования утилиты ZenMap, возможно получение топологии в графическом виде.
8. Управлять производительностью сканирования. Режимы T1 –T5.
9. Подмена адреса с которого производится сканирование.
10. Использование прокси серверов для сокрытия запросов.
11. Использование скриптов при сканировании сетей. NMap Script Engine

3. Оборудование

Персональный компьютер с количеством процессорных ядер не менее 2, работающих на частоте не менее 2 GHz, работающий под управлением операционной системы Kali Linux, Ubuntu Linux с пакетом дополнений Forensic Tools и NMap, Windows 7, или более новая. Видеокарта с поддержкой технологий CUDA или Open CL. Не менее 4 GB оперативной памяти. Не менее 20GB свободного места на HDD.

4. Задание на работу

4.1 Установить NMap, или ZenMap.

4.2 Изучить документацию по базовым опциям NMap https://nmap.org/man/ru/man-briefoptions.html опциями иммитации разрыва соединения https://nmap.org/book/scan-methods-null-fin-xmas-scan.html https://habr.com/ru/articles/131433/ https://nmap.org/man/ru/man-briefoptions.html . Полная документация https://nmap.org/man/ru/index.html

4.3 Просканировать сайт scanme.org с использованием различных опций NMap.

4.4 Поискать уязвимости на сайте scanme.org с использованием скриптового движка NMap и базы данных https://www.exploit-db.com/, например, с использованием следующих опций https://geekflare.com/nmap-vulnerability-scan/

4.5 Найти субдомены сайта scanme.org с использованием скрипта dns-brute.

4.6 При наличии такой возможности, постараться использовать опции подмены адреса и опции управления пакетами данных, встроенные в среду NMap.

5. Порядок выполнения работы

5.1 Установить NMap и ознакомится с документацией на данное средство сбора информации.

5.2 Выполнить задания на работу в предложенном порядке.

5.3 Предоставить скриншот каждого этапа выполнения задания.

5.4 Сделать выводы о проделанной работе.

6. Оформление отчета

Отчет оформляется в тетради или листах формата А4 и должен содержать:

- название курса, название и номер лабораторной работы;
- цель работы и задание на исследование;
- скриншоты окон приложения NMap, или содержимое текстового файла, полученные в результате выполнения команд;
- справочные данные об открытых портах, версиях и назначении служб, установленных на сканируемой цели;
- краткие выводы о проделанной работе.

7. Контрольные вопросы

7.1 Каково назначение приложения средства сбора информации NMap?

7.2 Каким образом можно получить информацию об открытых портах и версии служб при помощи NMap и какие ограничения имеются при сканировании по - умолчанию?

7.3Каким образом возможно применение опций изменения размера пакетов и средств подмены адреса для обхода средств защиты, установленных на АС?

7.4 Какие опции таймингов существуют в системе NMap?
7.5 Каким образом и в каких форматах возможно сохранить результат сканирования NMap?
7.6 Каким образом возможно использование скриптовых движков NMap?
7.7 Перечислите основные виды ответственности за использование средств NMap и скриптовых средств сканирования NMap?
7.8 Почему в качестве цели был выбран общедоступный и обще используемый для сканирования ресурс, а не сайт https://tulsu.ru/?
7.9 Какая юридическая ответственность наступит, или может наступить в случае сканирования сайта https://tulsu.ru/? !!!Внимание!!! Сканировать сайт https://tulsu.ru/ в рамках выполнения данной работы категорически запрещается!