Индивидуальный проект

Этап 4. Использование nikto

Хватов Максим Григорьевич

Содержание

# 1 Цель работы

Научиться использовать nikto для сканирования сайтов на уязвимости

# 2 Теоритическое введение

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Несмотря на то, что этот инструмент чрезвычайно эффективен, он не действует скрытно. Любой сайт с системой обнаружения вторжений или иными мерами безопасности поймет, что его сканируют. Nikto был разработан для тестирования безопасности и о скрытности его работы никто не задумывался.

# 3 Выполнение этапа проекта

Сначала проверяю установку nikto командой nikto -HELP и получаю справку всех имеющихся команд, что говорит о наличии nikto на машине.

# 4 Сканирование сайта с SSl

Я пробую сканировать сайт pbs.org. Использую команду nikto -h pbs.org -ssl Получаю резултат:

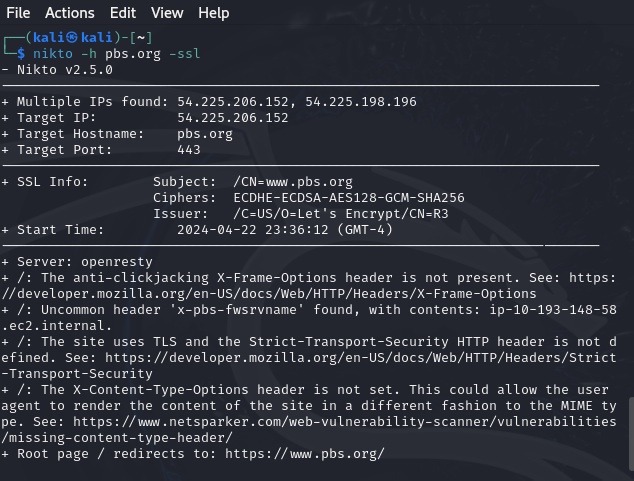


Рис. 1

# 5 Cканирование IP-адреса

Теперь, когда мы провели быстрое сканирование веб-сайта, мы можем попробовать использовать Nikto в локальной сети, чтобы найти embedded-сервера, такие как страница логина роутера или HTTP-сервис на другой машине, который представляет из себя просто сервер без веб-сайта. Чтобы узнать IP-адрес мы будем использовать ifconfig.

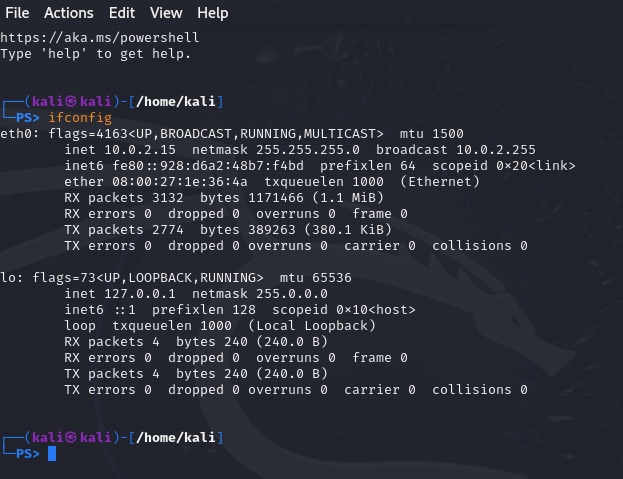


Рис. 2

Cоздаю файл targetIP.txt командой touch и просматриваю его содержиимое через cat



Рис. 3

Начинаю сканировать список IP-адресов с помощью команды nikto -h targetIP.txt Результатов никаких не получено почему-то. Скорее всего из-за того, что не использовад ipcalc, а его устновить нельзя.

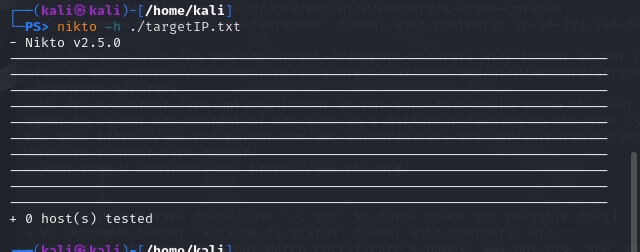


Рис. 4

# 6 Сканирование HTTP-сайта

До этого мы сканировали защищенный сайт, а теперь просканиуем незащищенны, который работает на 80-м порту. Используем команду nikto -h www.afl.com.au. И через какое-то время получаем результат.

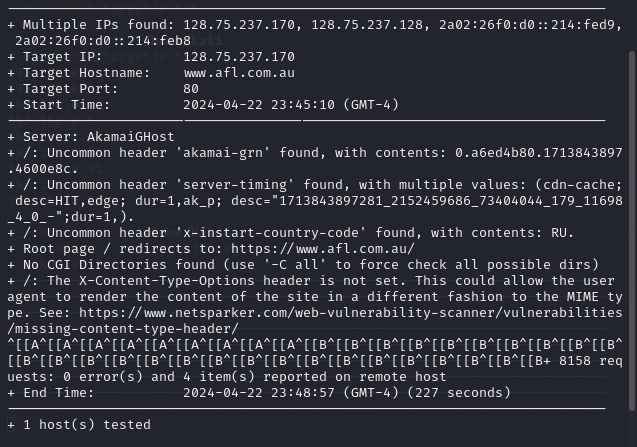


Рис. 5

# 7 Вывод

Я научился использовать nikto для сканирования защищенных и незащищенных сайтов на уязвимости, и научился также получать дополнительную информацию из nikto.