Индивидуальный проект этап 5

Использование Burp Suite

Неустроева Ирина Николаевна

Содержание

Список иллюстраций

Список таблиц

1 Теоретическое введение

Перед тем как атаковать любой сайт, хакер или пентестер сначала составляет список целей. После того, как он проведет хорошую разведку и найдет слабые места для «наведения прицела», ему понадобится инструмент сканирования веб-сервера, такой как Nikto, который поможет найти уязвимости – потенциальные вектора атаки.

Nikto – это простой открытый сканер веб-серверов, который проверяет вебсайт и сообщает о найденных уязвимостях, которые могут быть использованы для эксплойта или взлома. Кроме того, это один из наиболее широко используемых инструментов сканирования веб-сайтов на уязвимости во всей отрасли, а во многих кругах он считается отраслевым стандартом.

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.

Как правильно использовать Nikto

Если вы просто запустите Nikto на целевом веб-сайте, вы, возможно, не поймете, что делать с информацией, полученной после сканирования. Nikto на самом деле больше похож на лазерную указку, которая влечет за собой выстрел, и через некоторое время вы увидите, как это работает.

Для начала давайте поговорим о целях (target). Целью может оказаться почти любое место, куда может нанести свой удар хакер, например, сетевые принтеры или веб-сервер. Когда мы чуть позже перейдем к использованию Nikto, нам

нужно будет предоставить ему один из трех видов информации: IP-адрес для локальной службы, веб-домен для атаки или веб-сайт SSL/HTTPS.

Прежде чем начинать сканирование с помощью Nikto, лучше предварительно провести разведку с помощью такого открытого инструмента как Maltego. Такие инструменты могут оказаться полезными при создании профиля и формировании более конкретного списка целей, на которых стоит сосредоточиться. Как только вы это сделаете, можно будет воспользоваться Nikto для поиска потенциальных уязвимостей в целях из вашего списка.

Если повезет, уязвимость с известным эксплойтом будет найдена, а значит, что уже существует инструмент, который поможет воспользоваться этим слабым местом. С помощью соответствующего инструмента, который автоматически эксплуатирует уязвимость, хакер может получить доступ к цели для выполнения любого количества скрытых атак, таких как, например, добавление вредоносного кода.

2 Цель работы

Приобретение практических навыков по использованию инструмаента Nikto для сканирования веб-сайтов и поиска уязвимости в нем

3 Задание

1. Вызвать справку по nikto
2. Просканировать сайт
3. Просканировать сайт с ssl
4. Выяснить свой ip-адрес

4 Выполнение

1. Перед сканированием веб-серверов использовали параметр -Help, чтобы увидеть, что можно делать с этим инструментом

Рис. 4.1: Знакомство с Nikto

2. Затем используем базовый синтексис nikto -h для классического сканирования сайта. Таким образом мы просканировали сайт rudn.ru

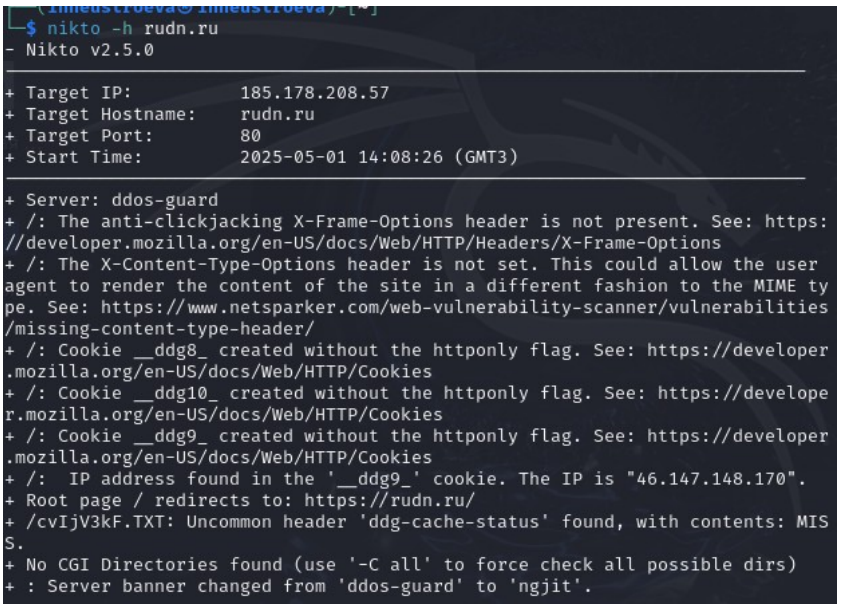

Рис. 4.2: Базовое сканирование сайта

3. Далее сканирую сайт pbs.org с SSL “nikto -h -ssl”

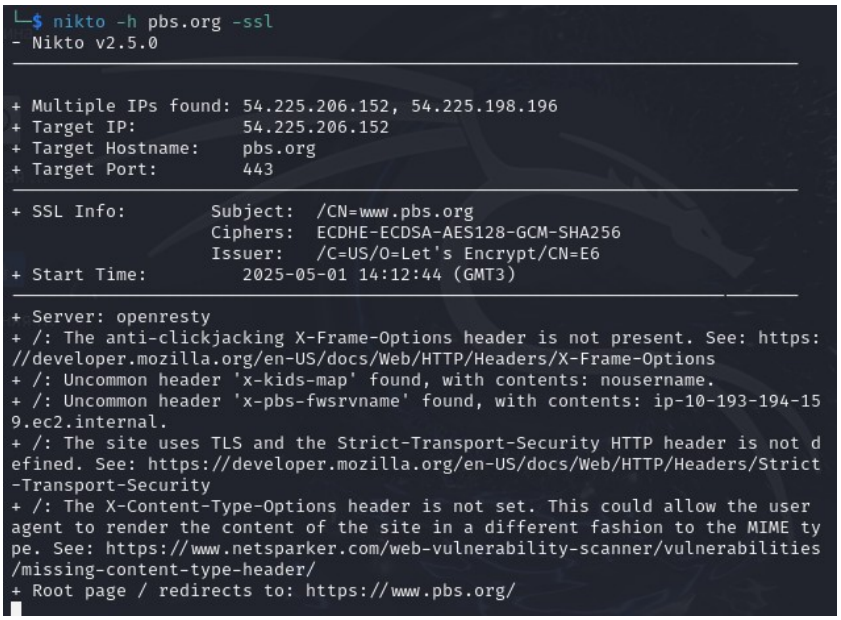

Рис. 4.3: Сканирование сайта pbc.org

4. Теперь, когда мы провели быстрое сканирование веб-сайта, можно 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 сервис без веб-сайта, Чтобы узнать IP-адрес, я буду использовать ifconfig

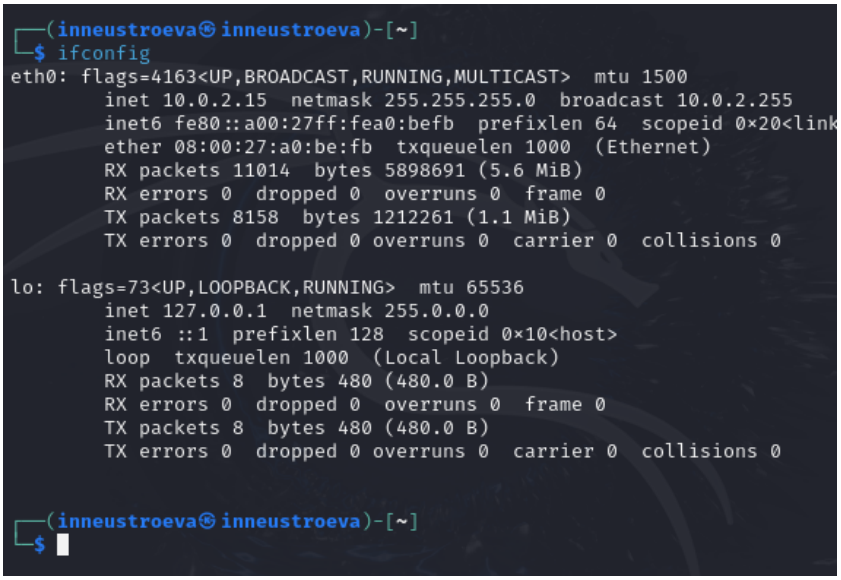

Рис. 4.4: Сканирование IP-адреса с помощью ifconfig

5. IP-адрес, который нам нужен относиться к inet.На нем мы можем использовать ipcal Диапазон будет стоять после Network, в нашем случае это 10.0.2.255

Использование IpCalc для IP-адреса

Рис. 4.5: Использование IpCalc для IP-адреса

5 Выводы

В ходе нашей работы, приобрела практические навыки по использованию инструмаента Nikto для сканирования веб-сайтов и поиска уязвимости в нем.