Аудит защищенности сети сканером Nmap

Предназначение

Свободная утилита **Nmap** предназначена для разнообразного настраиваемого сканирования IP-сетей с любым количеством хостов (объектов), определения состояния объектов сканируемой сети (портов и соответствующих им сервисов).

Nmap использует множество различных методов сканирования, таких как UDP, TCP (connect), TCP SYN (полуоткрытое), ftp-proxy (прорыв через ftp), ICMP (ping), FIN, ACK, SYN- и NULL-сканирование и др. Nmap также поддерживает большой набор дополнительных возможностей: определение типа операционной системы удалённого хоста с использованием отпечатков стека TCP/IP, "невидимое" сканирование, динамическое вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, определение неактивных хостов методом параллельного ping-опроса, сканирование с использованием ложных хостов, определение наличия пакетных фильтров, RPC-сканирование, сканирование с использованием IP-фрагментации, быстрый поиск уязвимостей SQL Injection, а также произвольное указание IP-адресов и номеров портов сканируемых сетей.

В последних версиях добавлена возможность написания произвольных сценариев на скриптовом языке программирования Lua - Nmap Scripting Engine (NSE).

Для лабораторных работ:

Организуйте с помощью утилиты Nmap сканирование сегмента сети. Используйте всевозможные режимы сканирования для получения как можно более подробной информации о сегменте сети и о хостах, применяя различные опции, направляя вывод на консоль или в файл (с последующей фильтрацией), применяя временные параметры (расписания сканирования) и т.д.

https://compress.ru/article.aspx?id=17371#%D0%A1%D0%BA%D0%B0%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%BE%D0%BC%20Maimon

https://www.youtube.com/watch?v=iUZ6nTMO8K0&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO

https://www.youtube.com/watch?v=TyUtnOb-kS0&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO&index=4

https://www.youtube.com/watch?v=YjrZF5v_o-&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO&index=9

https://www.youtube.com/watch?v=Qxa7QyiQvPE&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO&index=13

https://www.youtube.com/watch?v=lXK5j2nRuv8&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO&index=7

https://www.youtube.com/watch?v=9JCR81W3-Z4&list=PLW5y1tjAOzI0ZLv7YfQtToQmc0yVDfkKO&index=6

Сравните возможности сетевого сканера **Nmap** с другими известными средствами аудита сети (**Netcat, ping** и др.)

ТРЕБОВАНИЯ К ОТЧЕТАМ

По результатам выполнения лабораторных работ необходимо составлять отчет. Рекомендуется составлять отчет параллельно с выполнением заданий лабораторных работ, не оставляя этот процесс на потом. Отчет должен быть оформлен с титульным листом с названием университета, института и высшей школы. На титульном листе указывается ф.и.о. студента исполнителя работы, номер студенческой группы и ф.и.о. преподавателя.

В отчете приводится информация, удостоверяющая выполнение студентом заданий лабораторных работ: скриншоты с результатами исполнения сценариев, команд и программ, командных файлов, дампы памяти и пакетов, составленные вами скрипты (*BASH* или др.), ответы на поставленные в заданиях вопросы и т.д.

Результаты выполнения каждого из заданий должны предваряться в отчете фрагментом текста, формулирующим само задание (фрагменты копируются прямо из текста заданий).

Защита лабораторных работ происходит по предъявлению оформленного отчета и сопровождается демонстрацией исполнения программ и командных файлов, а также ответами на вопросы преподавателя.

Отчет можно создавать под *ОС Linux*, например, с помощью приложения *LibreOffice Writer* , сохраняя в *Home* каталоге вашего рабочего компьютера. Либо можете использовать офисные средства от MS Windows или MacOS.