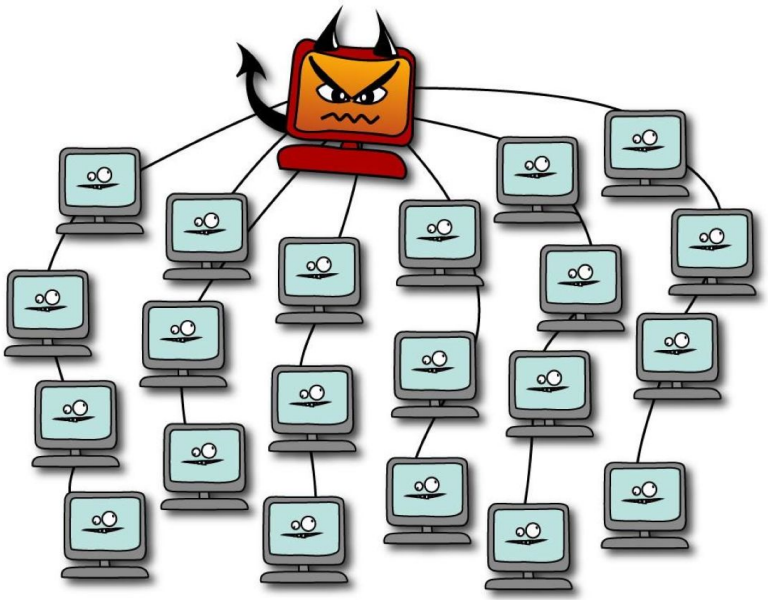
Сетевой бот для автоматизации пентеста



Данная программа является смесью двух популярных программ:

- Masscan
- И программ для автоматического тестирования, а именно: брутфорс, эксплойты, веб уязвимости

Консольное меню настройка программы

Первым делом программа запрашивает допустимый ip диапазон для сканирования адресов. На выбранном диапазоне(вместе с подсетями для уменьшения количества итераций проверок) Программа будет проверять определенные порты, есть ли там интересеющий нас сервис, и отвечает ли он, которые характерные для разных сервисов, что бы передать валидные адреса дальше по стеку, исходя из того какую функцию выбрал пользователь при настройке.

Из функций можно выделить исходя из предыдущего скриншота:

[1] - full

[2] - lfi

[3] - brute ssh

[4] - xss

[5] - rce

[6] - ip cam

[7] - brute site admin

[8] - brute bd

[9] - react2shell

Описывать каждый думаю нет смысла, но думаю нужно сразу подчеркнуть, что программа написана с использованием основных принципов ООП, что делает ее гибкой к расширению функционала и изменению существующего. А так же реализована многопоточность через чаны, для более быстрого сканирования как диапазонов адресов, так и для дальнейших их проверок.

Все найденные результаты, а именно с подтвержденными уязвимостями, записываются в текстовый фаил, в корневой директории вашей ОС, с названием файла MihBot.txt. Запись происходит в многопоточном режиме с соблюдение очереди.

Исходный код можно скомпилировать в .jar фаил и запустить на любой ОС(mac/win/linux) где стоит JVM от 11+ версии.