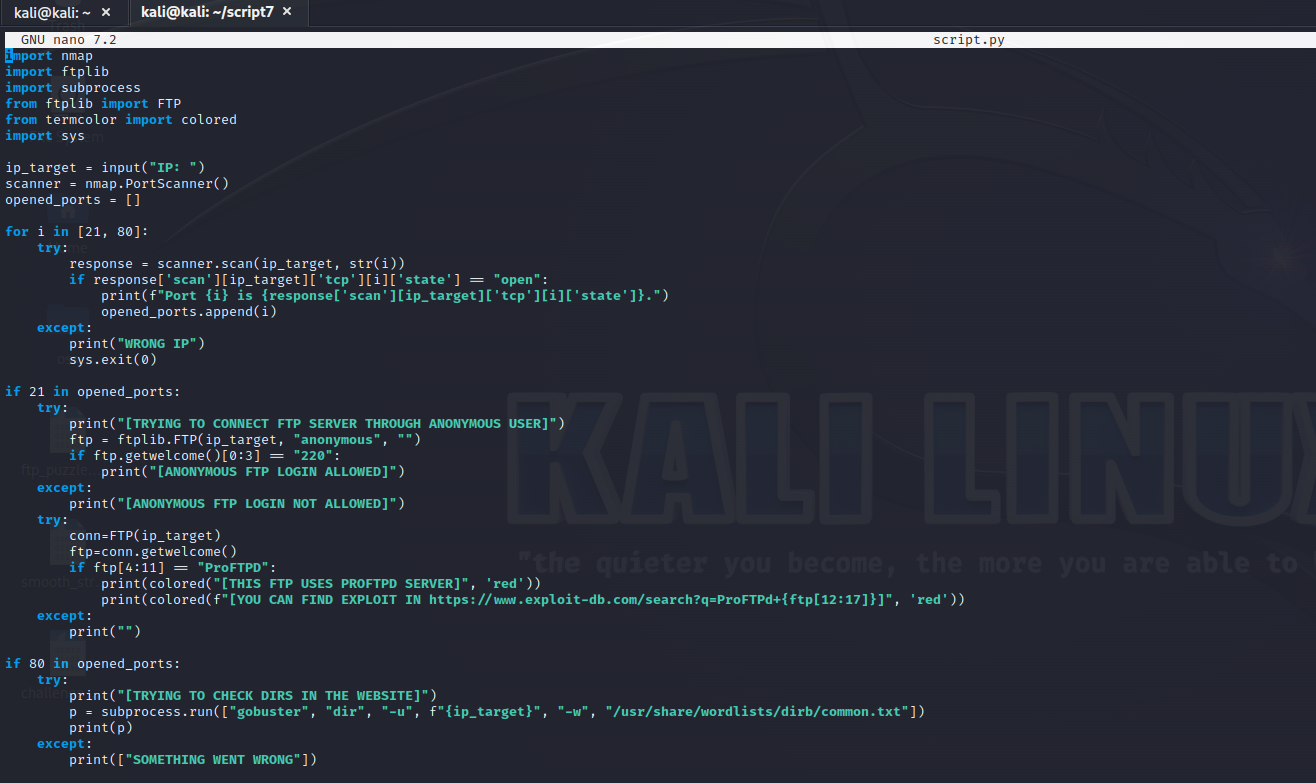
OSS practice 7

Tungatov Almat

Kamyshnik Artem

Shyngys Elemesov



Сперва импортируем все необходимые либы

Затем просим от юзера ввести IP

Далее создаем объект сканнера

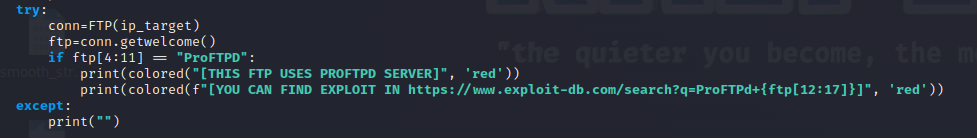
И массив для хранения открытых портов

Цикл в котором проверяются два порта 21(ftp) 80(http)

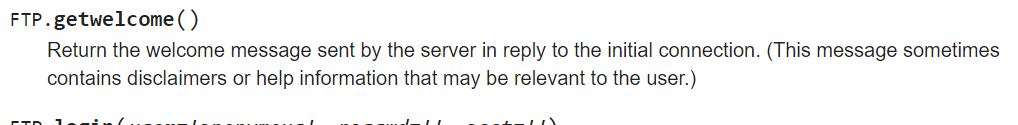
С помощью нмапа сканируем порты и если порт открыт то добавляем его в массив

Далее следует if statement в котором мы пытаемся получить инфу с 21 порта

Для начала пробуем зайти как анонимный юзер, если не получается то пробуем узнать какой сервер используется(мы написали только для FTPD)



Getwelcome() возвращает для нас именно какой сервер используется



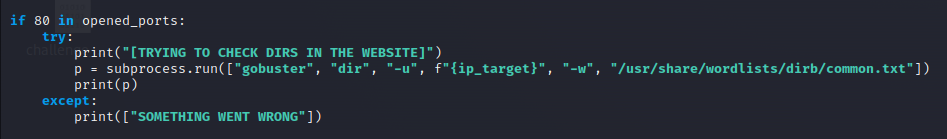
Затем через срез [4:11] который возьмет название ProFTPD сверяем



И далее если все верно то генерируем ссылку нашему юзеру используя срез [12:17] для версий чтобы он нашел експлойт если таков есть



И как видите с задачей хорошо справляется

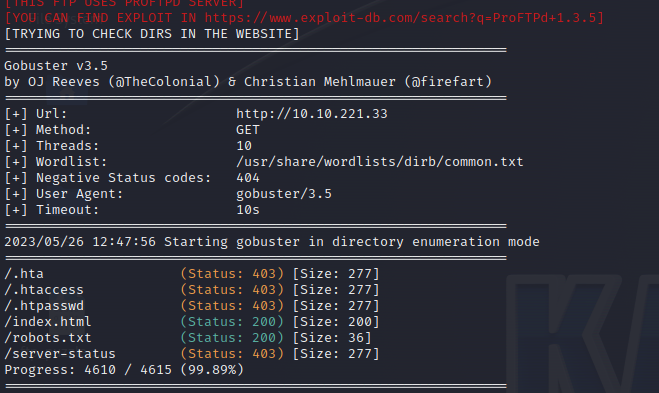


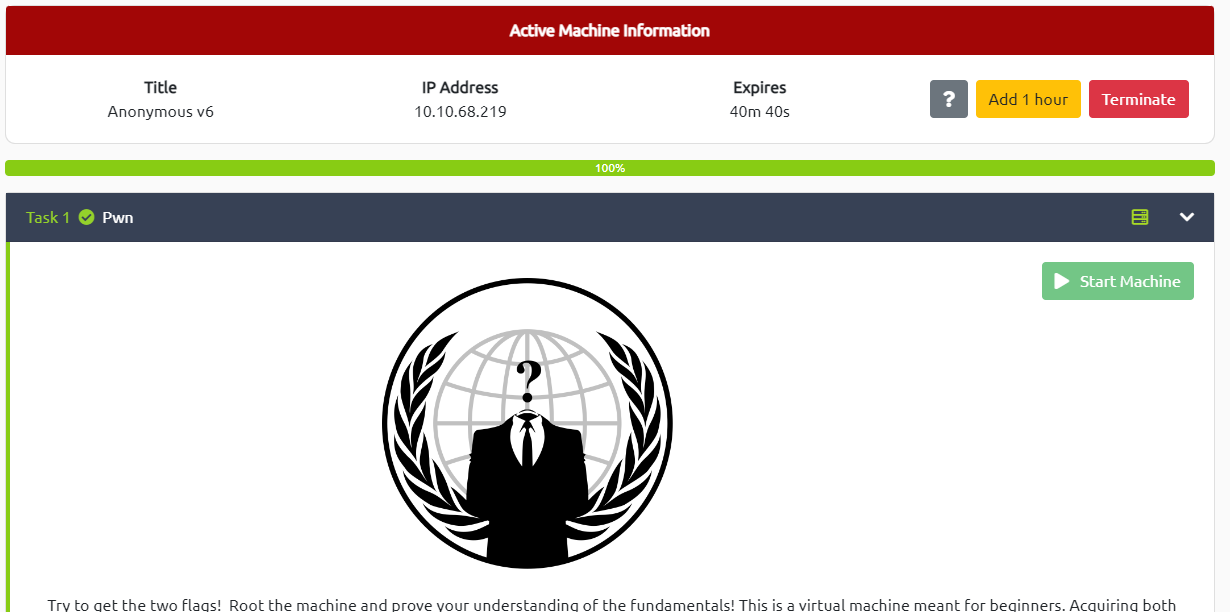
Далее начинаем работу с 80 портом а именно сканируем директорий которые есть на веб сервере

Тут все легко мы просто используем gobuster

Но для этого мы также используем subprocess либу для того чтобы использовать терминал и запустить команду

Далее он сканирует и выводит юзеру папки которые есть





Для того чтобы тестировать правильность работы мы запустили трайхакми сервер и начали тестить наш код

