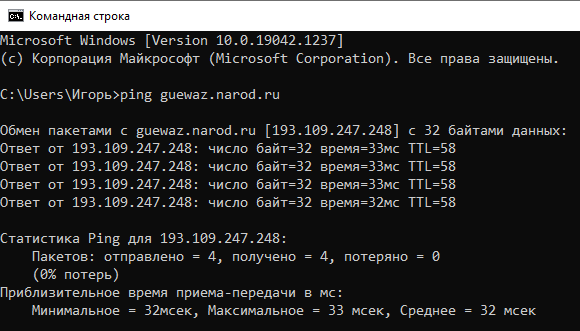
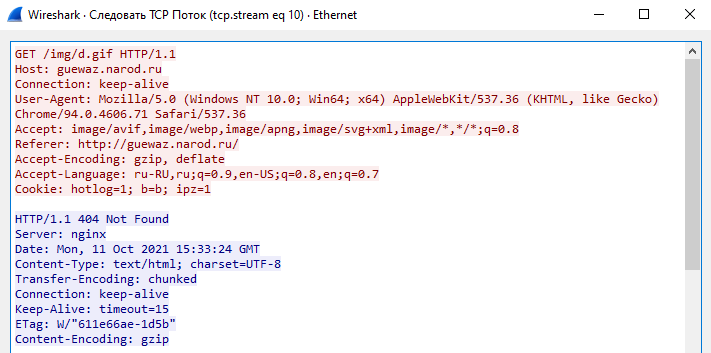
Анализ уязвимостей веб-сайта [guewaz.narod.ru](http://guewaz.narod.ru/)

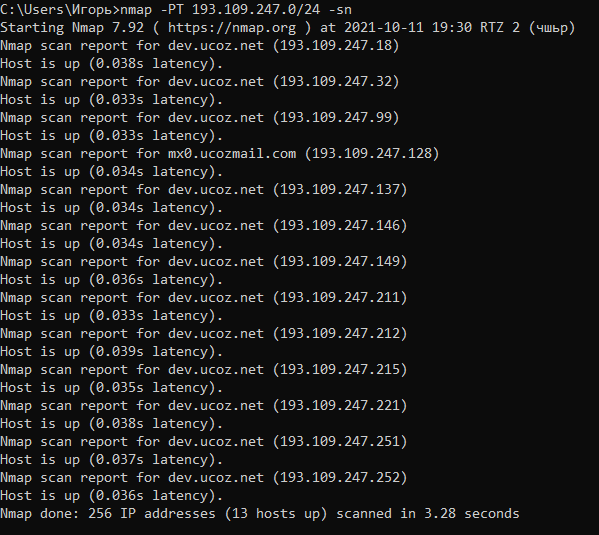
Узнаем ip адрес сайта: 193.109.247.248



В Wireshark мы видим сервер, на котором работает веб-сайт – **nginx**, но не видим его версию, что усложняет поиск уязвимостей для этого сайта.

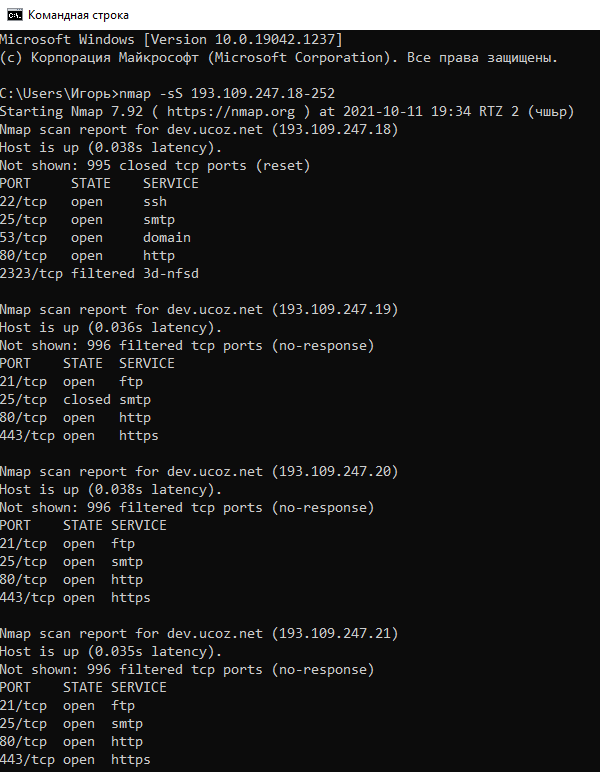


Осуществим интрузивный целевой поиск с помощью команды **nmap - PT**:



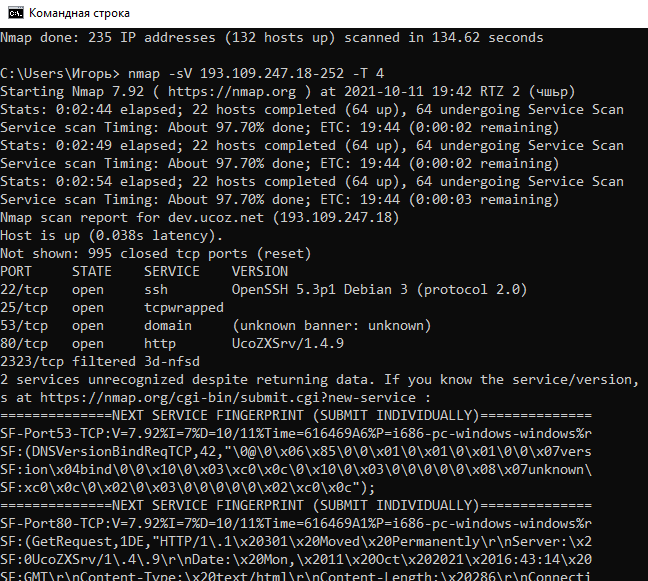
По результатам TCP сканирования было найдено 13 хостов в сети.

Проведем скрытое TCP сканирование портов: **nmap -sS 193.109.247.18-252**

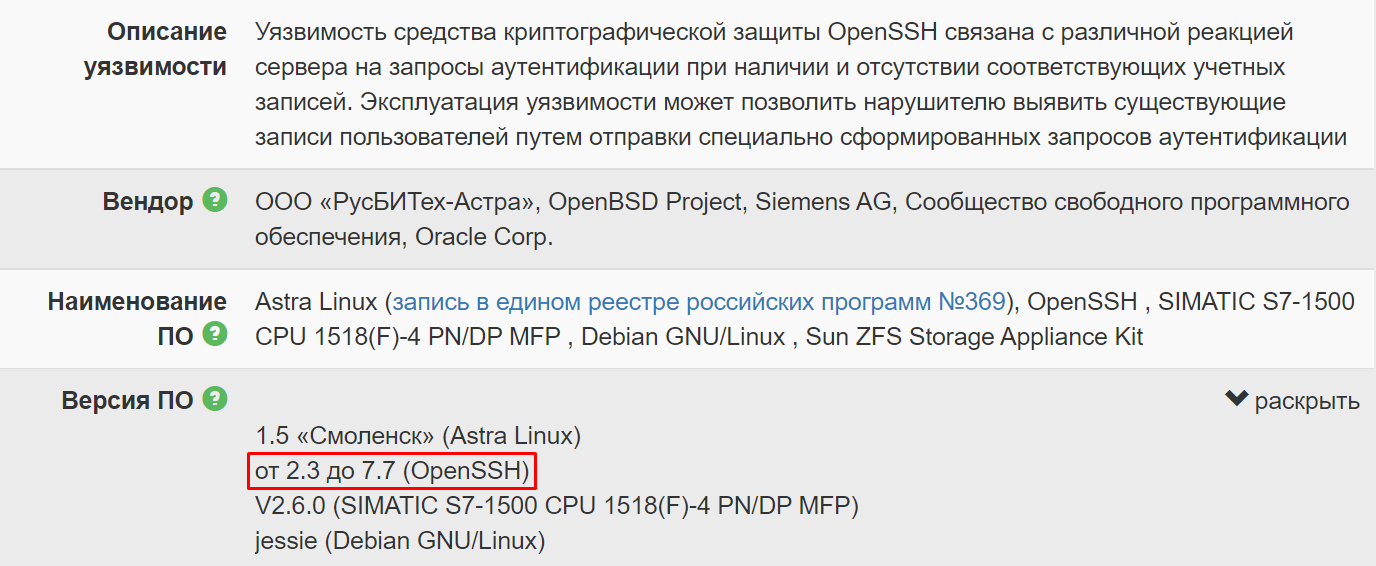


Получаем список и статус портов.

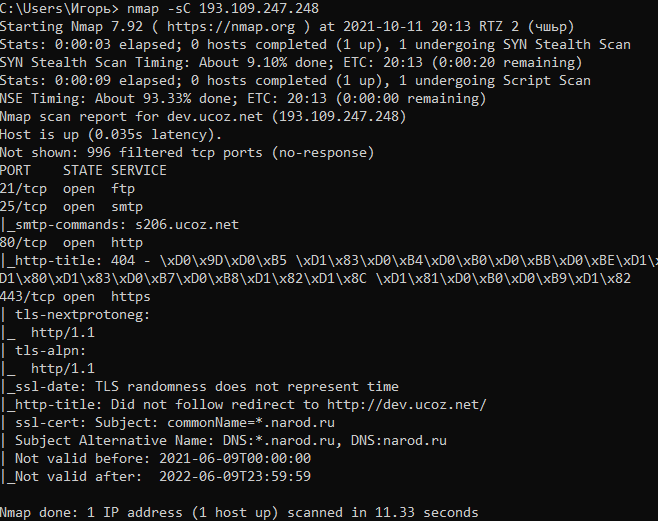
Запустим сканирование служб, командой **nmap –sV 193.109.247.18-252**



Мы нашли OpenSSH 5.3. В Банке данных угроз безопасности информации видим:

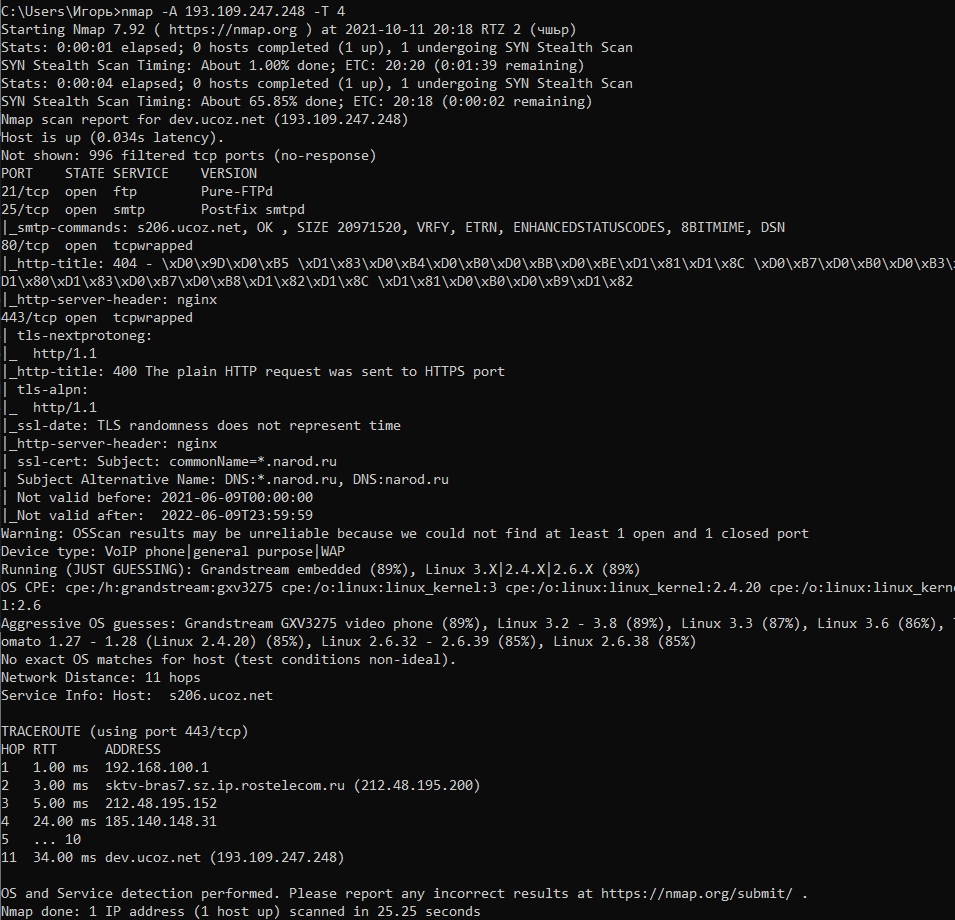


Введем команду **nmap -sC 193.109.247.248**

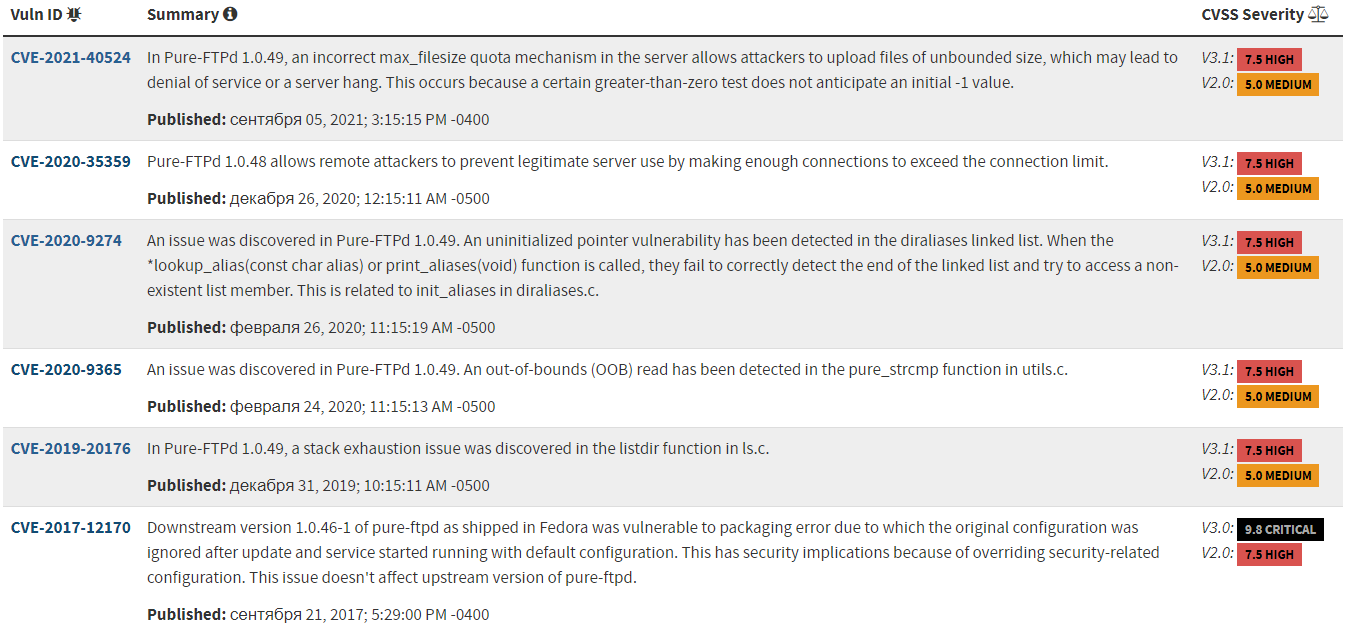


Видим версию HTTP 1.1. Эта версия подвержена уязвимости при обходе каталогов, поскольку ему не удается в достаточной степени очистить вводимые пользователем данные. Использование этой проблемы позволит злоумышленнику просматривать произвольные локальные файлы и каталоги в контексте веб-сервера. Собранная информация может помочь в проведении дальнейших атак.

Введя команду **nmap -A 193.109.247.248 -T 4** увидим следующее:



Есть версия Pure-FTPd, имеющая много уязвимостей:



Видим ОС, на которых работает сайт и их примерные версии:



Видим таблицу Traceroute:

