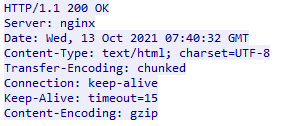
Анализ уязвимостей веб-сайта [guewaz.narod.ru](http://guewaz.narod.ru/) (193.109.247.248)

1. Wireshark, анализ TCP-трафика:



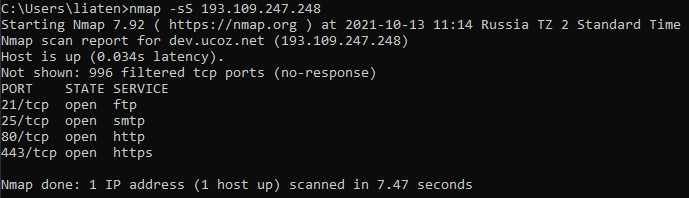


По анализу TCP-трафика можно судить, что сервер – nginx (защищенный сервер, к которому сложно будет получить доступ)

Кодирование – gzip.

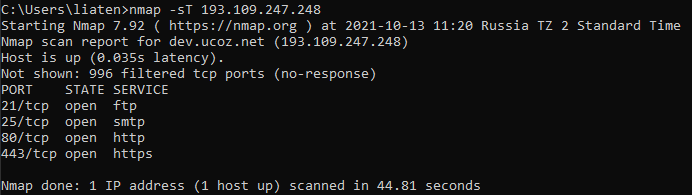
Версия HTTP – 1.1.

1. **nmap -sS 193.109.247.248:** скрытое TCP-сканирование (без соединения)



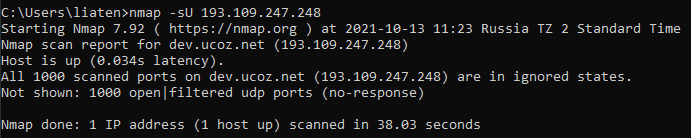
Делаем результат, что открыты порты: 21, 25, 80, 443

1. **nmap -sT 193.109.247.248:** TCP-сканирование с соединением



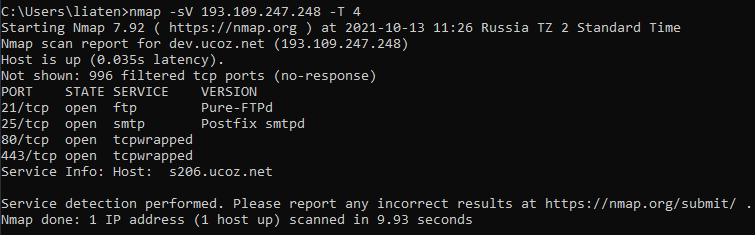
Новых портов не обнаружено

1. UDP-сканирование:



Портов не обнаружено.

1. **nmap -sV 193.109.247.248 -T 4** – сканирование служб (Т - тайминг)

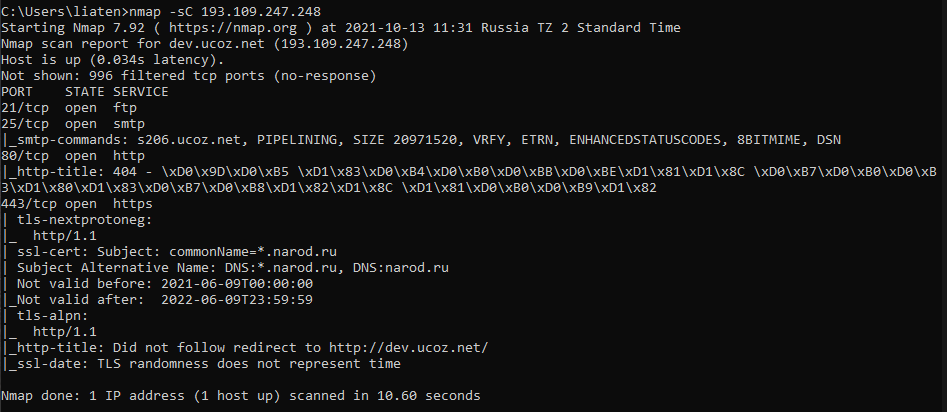
****

Найдены службы на портах:

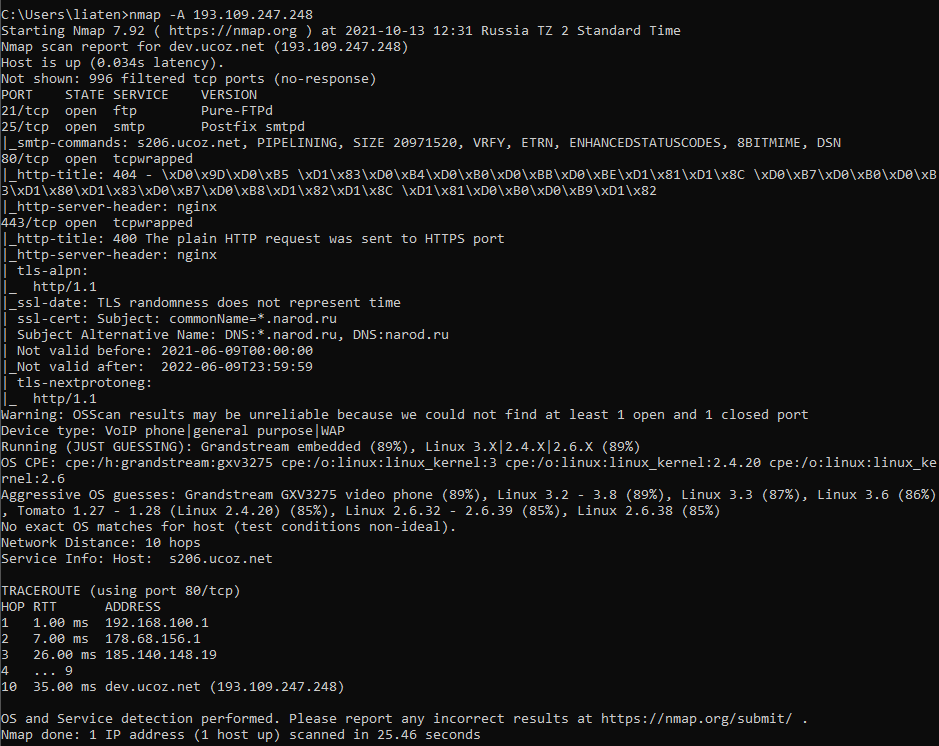
21 – Pure-FTPd

25 – Postfix smtpd

1. **nmap -sC 193.109.247.248** – скриптовый движок nmap



1. **nmap -A 193.109.247.248 –** определение всех версий ПО



Обнаружились аргументы SMTP-COMMANDS для 25 порта:



Определена система:

