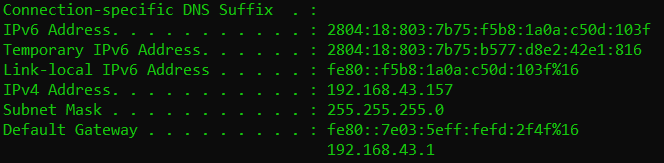
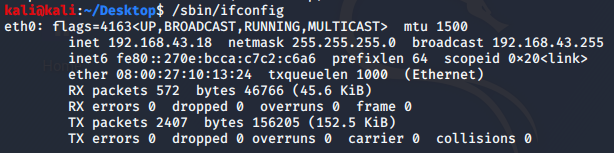
**Setup:**

Windows como hospedeiro, rodando uma VM do kali, com rede conectada a placa em modo bridge.



*Ipconfig* no windows

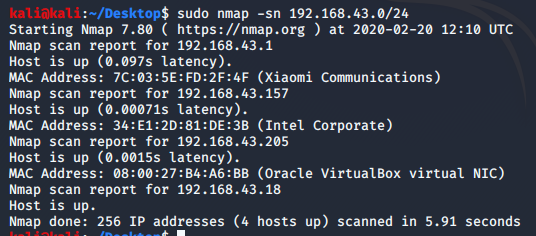


*/sbin/ifconfig* no kali

Com o comando */sbin/ifconfig*, foi possível descobrir o ip da rede e o submask, que são necessários para o primeiro exercício.

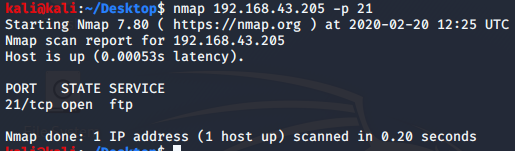
**Exercício 1.1.a: Descubra qual ip do seu alvo**

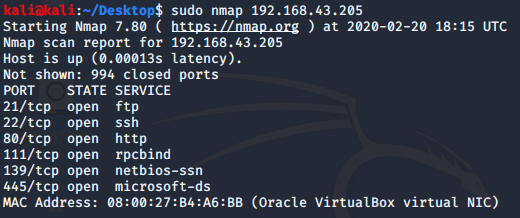
Comando utilizado: *sudo nmap -sn 192.168.43.0/24* . Com esse comando foi possível listar todos os IPs sendo utilizados na redes e todos os MAC address dos respectivos IPs. Por exclusão (192.168.43.1 é o roteador; 192.168.43.157 é o hospedeiro; 192.168.43.18 é o próprio), o IP do alvo é 192.168.43.205, e seu MAC address é 08:00:27:B4:A6:BB.

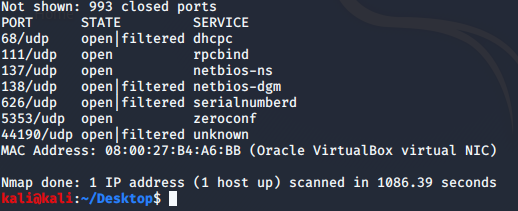


**Exercício 1.1.b: reconhecendo serviços e portas abertas do alvo.**

Comando utilizado: *nmap 192.168.43.205 -p 21* . A porta 21 do alvo está aberta e rodando o serviço *ftp*.

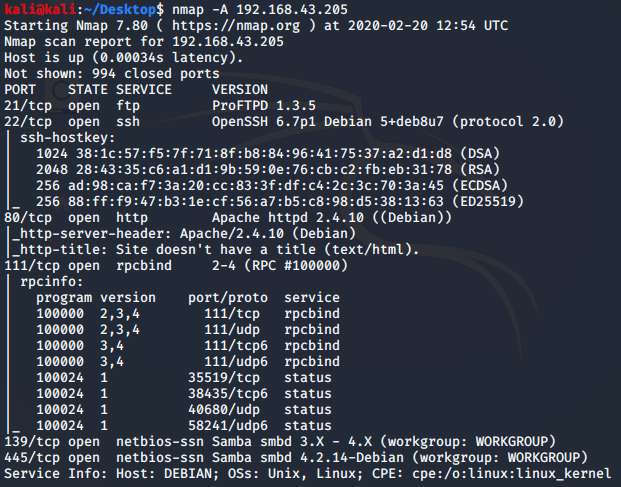


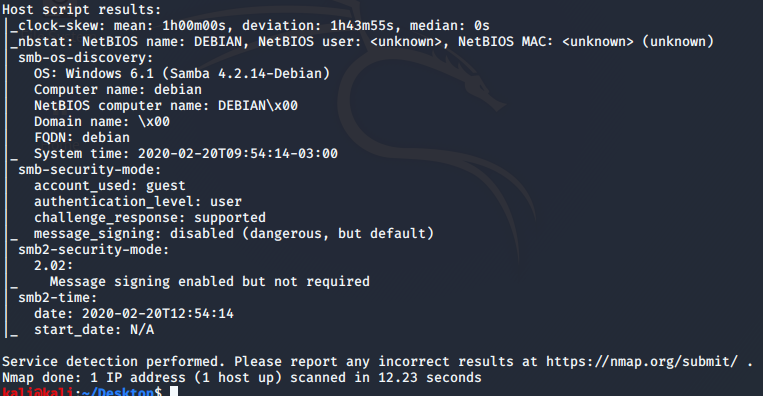




**Exercício 1.1.c: fingerprint.**

Comando utilizado: *nmap -A 192.168.43.205*. Esse comando deu um monte de informação.

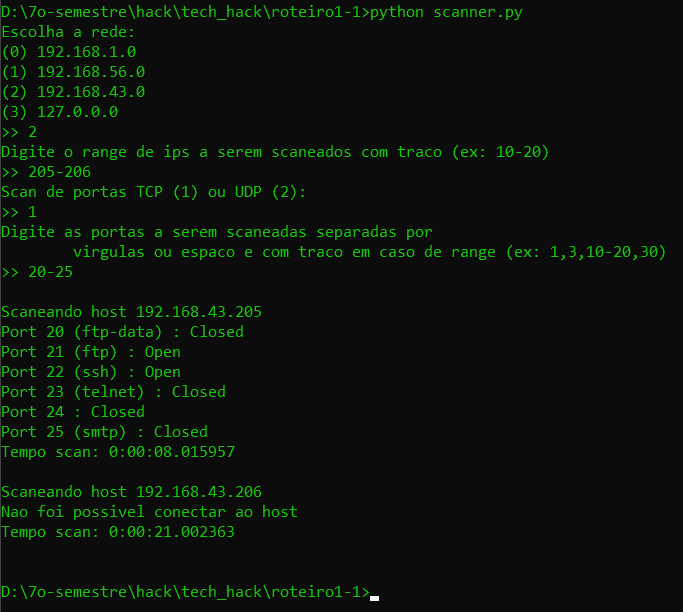




**Exercício 1.1.d: criação de Escaneamento de Portas com Python.**

Url do git: <https://github.com/LiuSeeker/tech_hack>

**Exercício 1.1.e: utilização do Escaneador de Portas.**



Ao scanear o alvo apenas nas portas 20 a 25 como exemplo, o ersultado foi como esperado, tendo apenas as portas 21 e 22 abertas.

Ao tentar scanear um host não existente, tenta-se fazer uma conexão com o host, porém há um timeout.