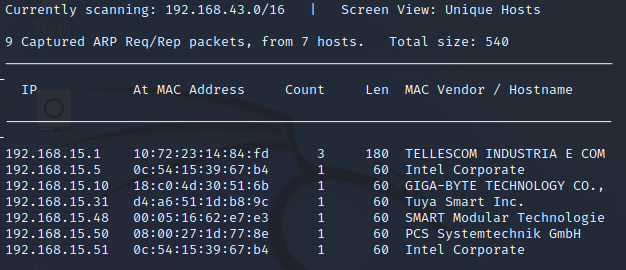
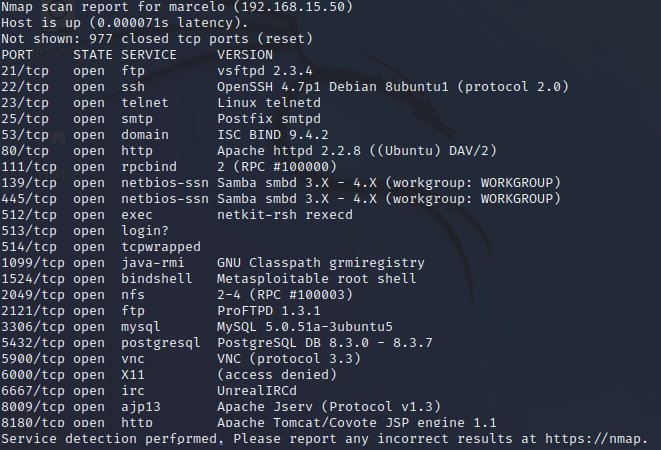
**Roteiro 2 - Segurança em Sistemas Operacionais**

**Marcelo Cesário Miguel**

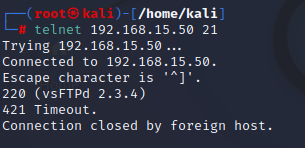
1. **Reconhecimento o alvo**
   1. **Descubra qual ip do seu alvo.**

Primeiro, realizei um netdiscover para ver os ips conectados na rede

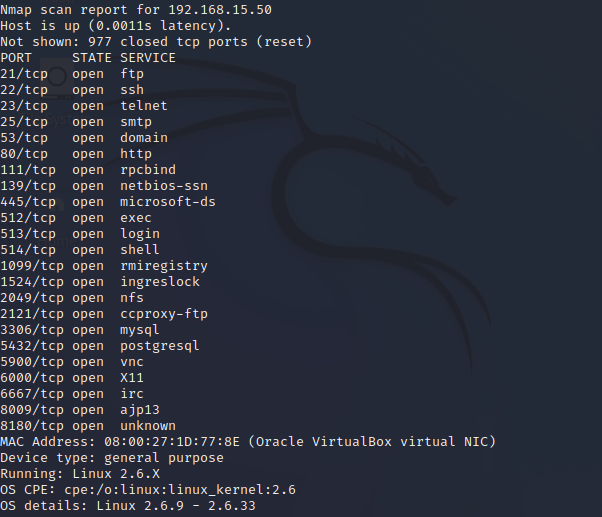


Depois, realizei nmap no range de 192.168.15.1-254 com a flag -sV para identificar meu o metasploit

* 1. **reconhecendo serviços e portas abertas do alvo.**

****

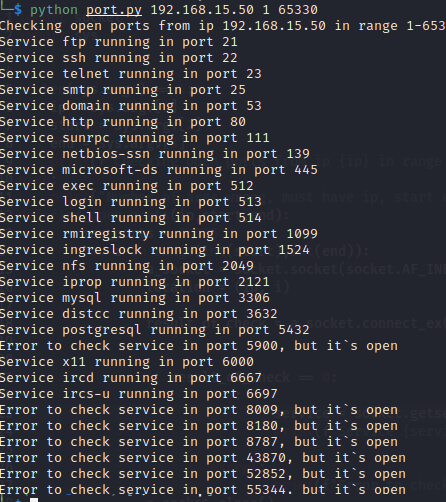
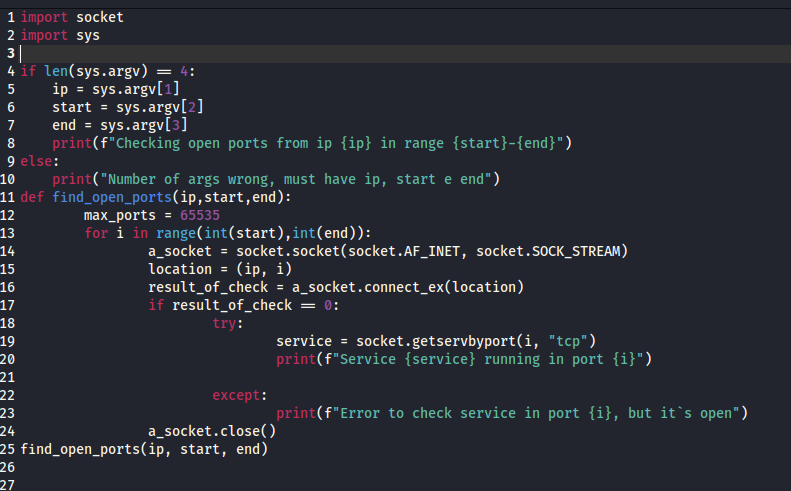
* 1. **Fingerprint**

Para descobrir o sistema operacional, realizei um nmap com a flag -O, tendo o mesmo resultado que o exercício anterior, porém com os dados do sistema operacional de cada ip.

* 1. **Criação de Escaneamento de Portas com Python.**

Criei uma aplicação port.py que recebe como argumento o ip alvo, start port e end port, sendo as duas últimas o intervalo de portas tcp a serem analisadas.

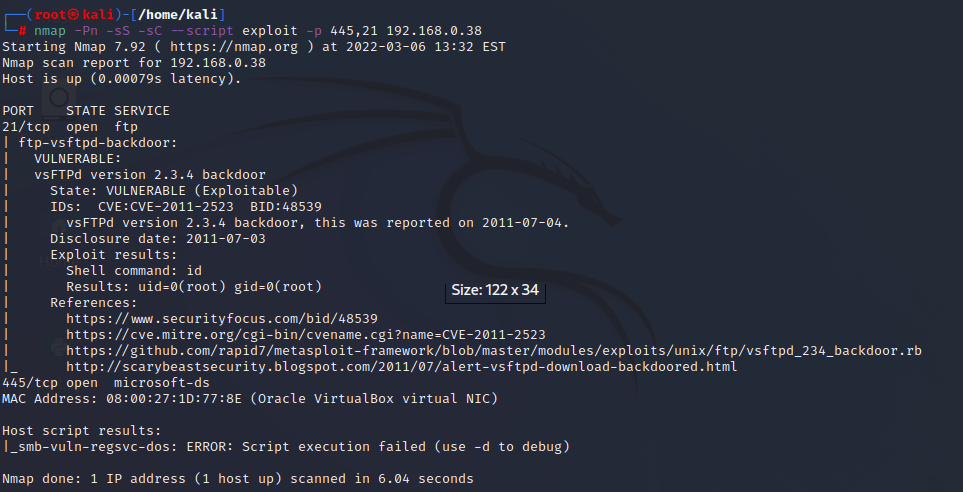
**O arquivo pode ser encontrado aqui: https://github.com/MarceloCMiguel/tec-hack/blob/master/h2/port.py**



* 1. **Listar as vulnerabilidades das portas 21 e 445**

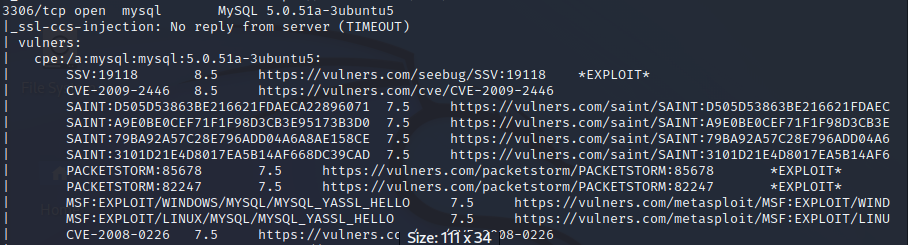
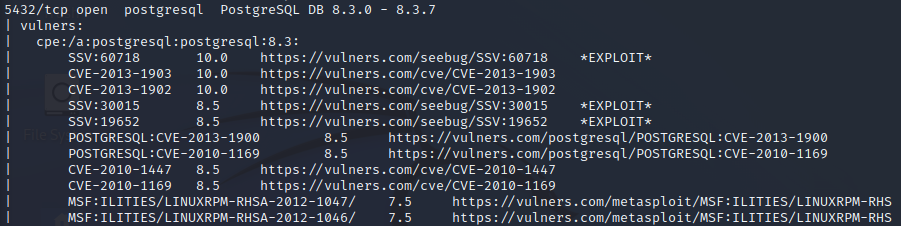
nmap -sV --script vuln -p 21,445 192.168.15.50

* 1. **encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior.**

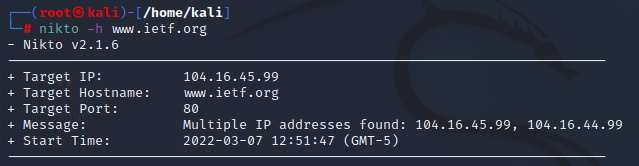
nmap -Pn -sS -sC --script exploit -p 445,21 192.168.0.38

* 1. **Encontrar uma CVE classificada como alta para os serviços das portas 3306 e 5432.**

Sendo um CVE de nivel alto um valor entre 7-8.9.

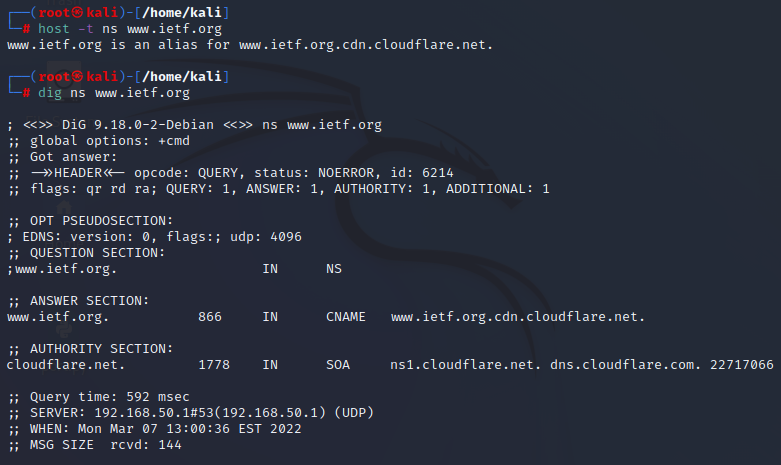
Para a porta 3306:Para a porta 5432

* 1. **Realize uma consulta ao nome www.ietf.org, e responda:**
     1. **Qual é o endereço IP associado?**

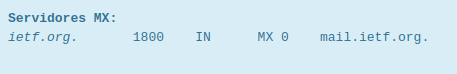


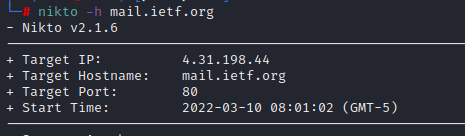
IP: 104.16.45.99

* + 1. **Quais são seus servidores DNS?**



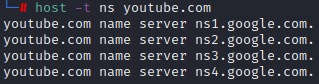
[www.ietf.org.cdn.cloudflare.net](http://www.ietf.org.cdn.cloudflare.net).

* + 1. **Existe algum servidor de e-mail associado ao domínio ietf.org? Qual o seu nome e IP?**

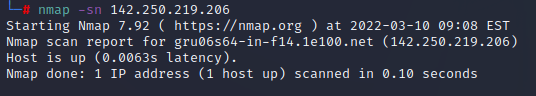
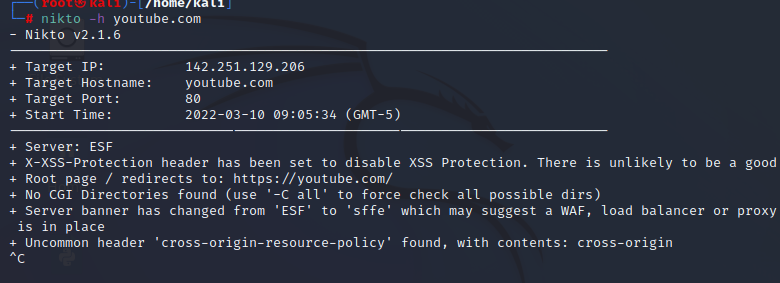
mail.ietf.org

IP = 4.31.198.44

* 1. **Escolha um site na Internet e responda as seguintes perguntas:**
     1. **Quais servidores DNS são responsáveis por este domínio? (print a sua consulta)**

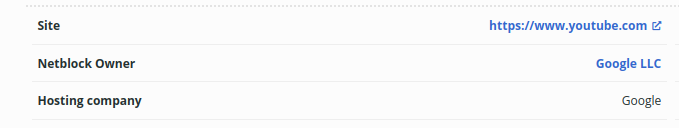


* + 1. **Existem outros domínios ou serviços hospedados no mesmo host (IP)? Quais são?**

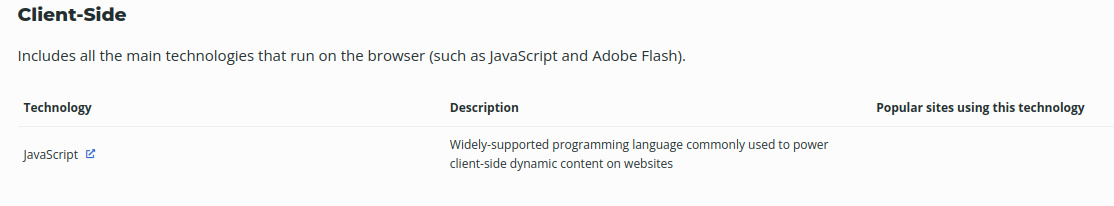
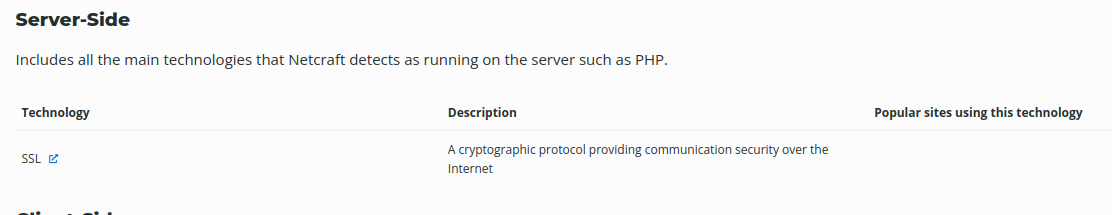


* + 1. **Qual o Servidor WEB e Sistema Operacional que hospedam este site? Quais foram as últimas alterações?**

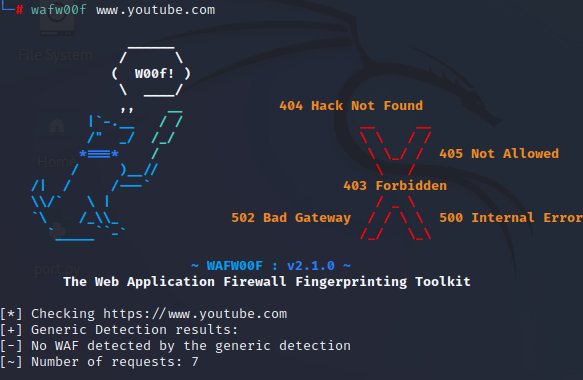




* + 1. **Quais tecnologias (jquery, utilizadas por este site)?**

****

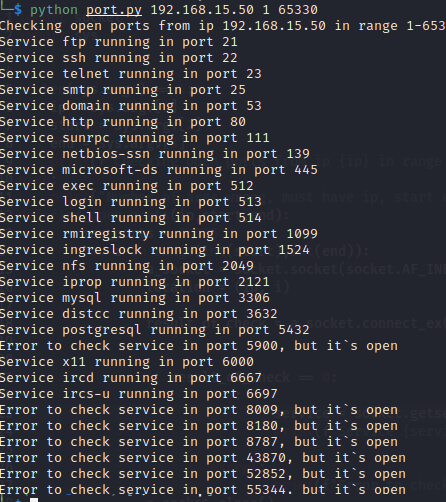
* + 1. **Existe algum WAF protegendo este site? (Print a saída do comando)**

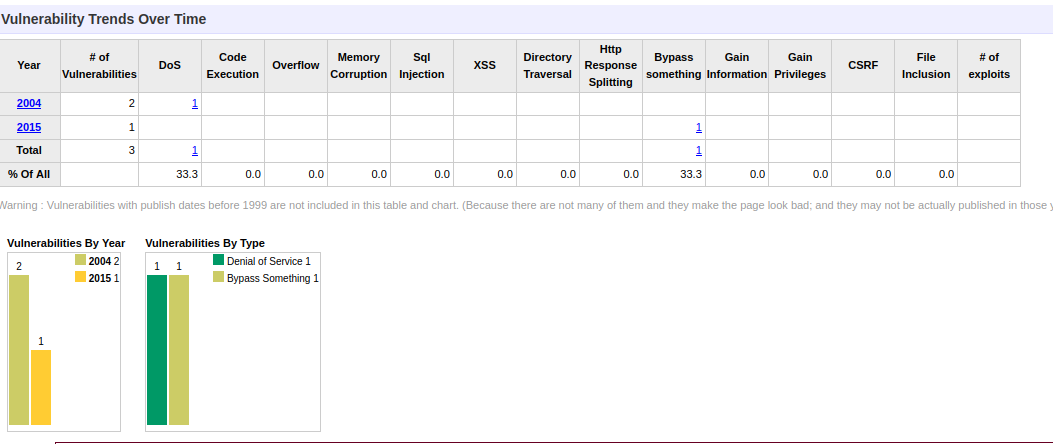
****

* + 1. **O Domínio possuí um servidor de e-mail configurado? Qual (is) Ip (s)?**

****

* 1. **portas TCP e UDP do alvo**





Denial of Service 1

Bypass Something 1