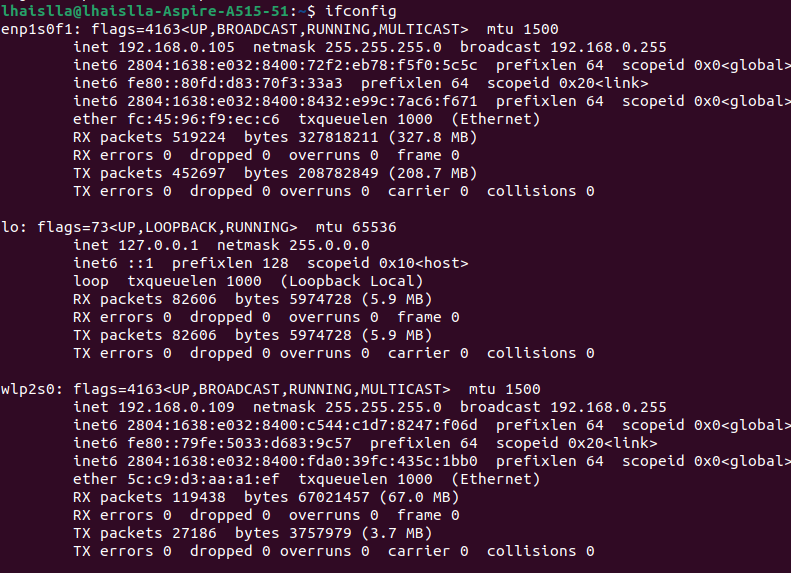
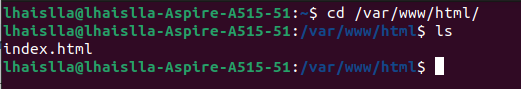
## Universidade Federal Rural de Pernambuco Sistemas de Informação Segurança e Auditoria de Sistemas Lhaíslla Eduarda Cavalcanti Rodrigues da Silva RECIFE-PE

2023

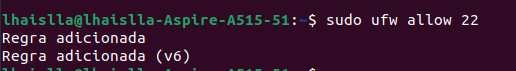
**Configurações de segurança**

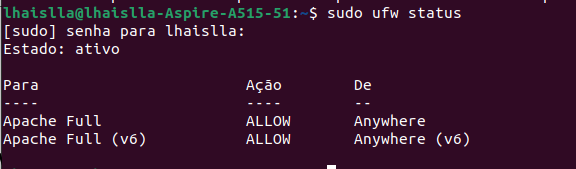
1. **Instalar o apache2:** sudo apt-get install apache2  
   verificar se a instalação está ok:  
     
   
2. **Instalar php:** sudo apt-get install php  
   para o servidor web interpretar códigos php
3. **verificar o ip da máquina:  
   Obs:** Tenha o pacote net-tools instalado na máquina  
     
   no caso desta máquina o Ip é: 192.168.0.105
4. **Colar o Ip da máquina no navegador:** 192.168.0.105
5. **Acessar o servidor web:** Entrar no diretório padrão onde ficam as aplicações web  
   
6. **Criar nova pasta**   
   
7. **Acessar pasta web e executando a página PHP**   
   Colocar o arquivo .html dentro da pasta seg  
   ir ao navegador digitar: http://192.168.0.105/seg/seg.html

**Medidas de segurança**

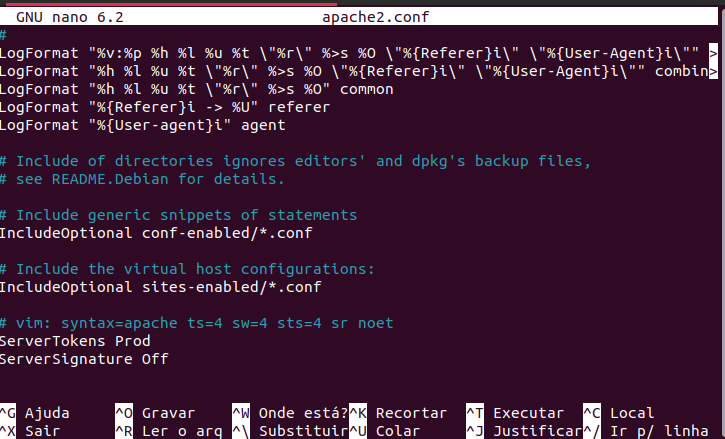
1. **Ativar firewall:** Os firewalls são utilizados como ferramenta de impedimento a acesso das portas de rede de fontes não autorizadas, apresentando recursos para det detecção de tentativas de invasão.



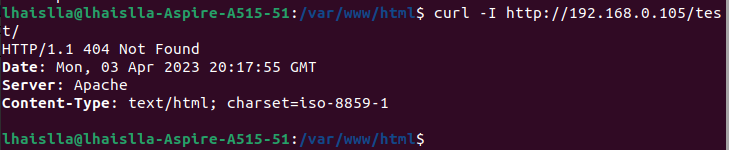
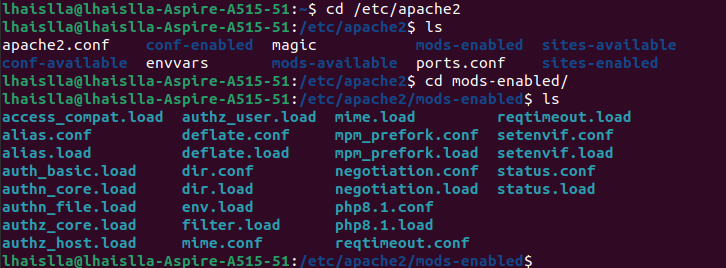
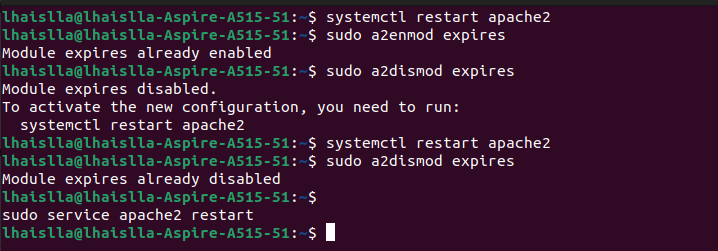
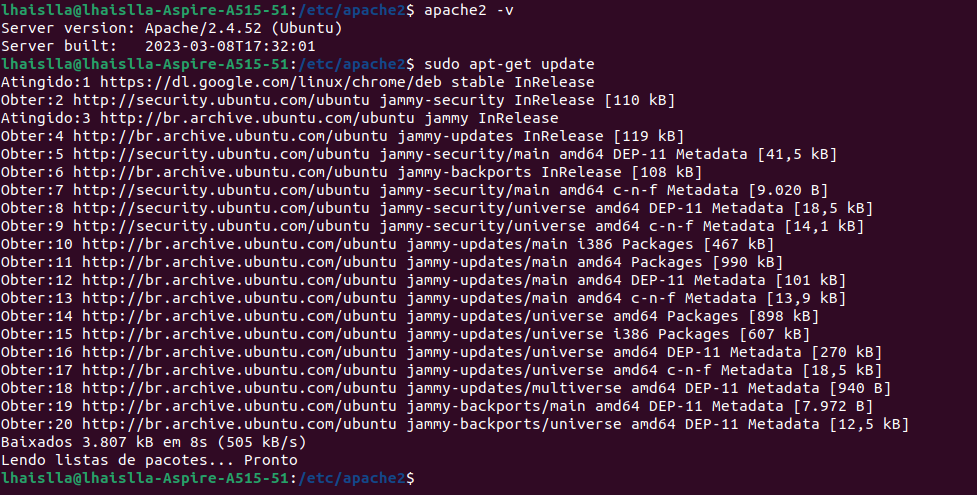


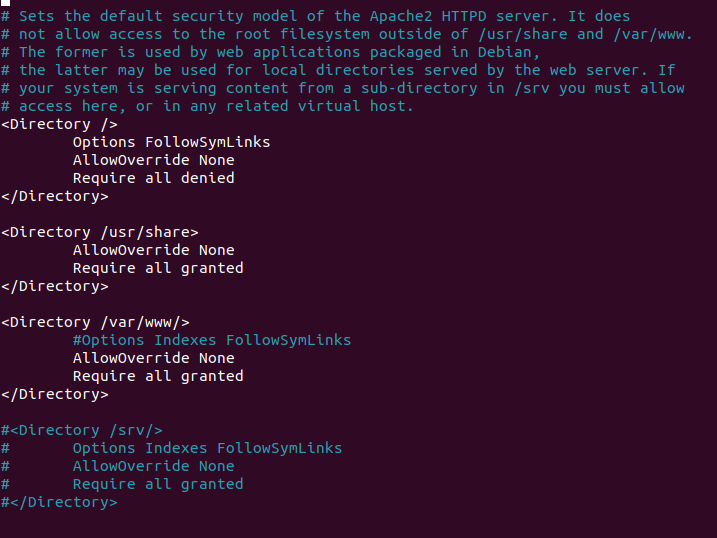
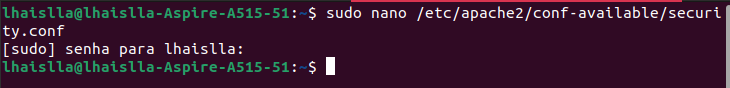
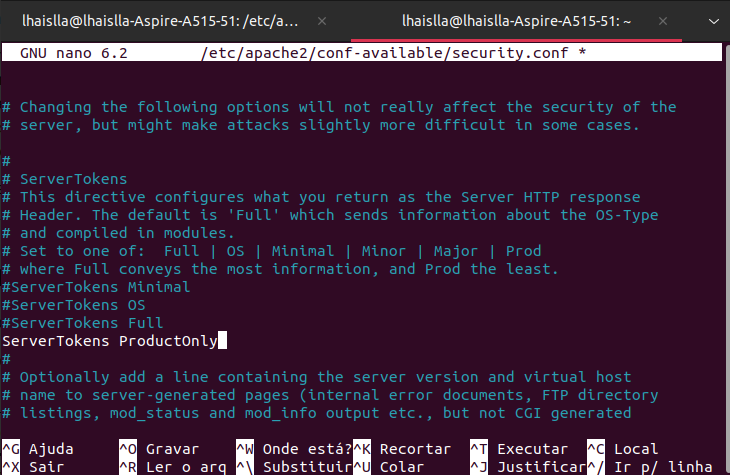
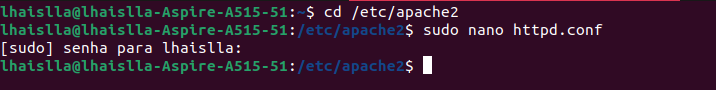


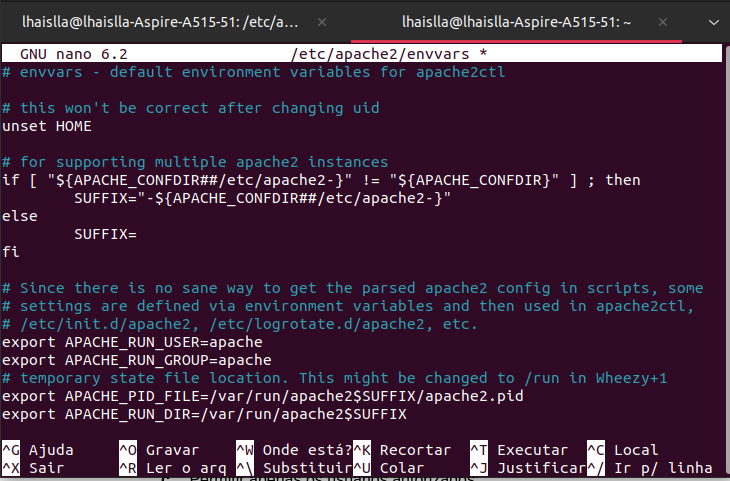
1. **Ocultar a versão do apache no servidor:** A inibição do “excesso” de informações a pessoas estranhas, ninguém precisa saber qual a versão do apache está sendo executada, saber que módulos estão rodando e quais as vulnerabilidades(baseado na versão do servidor web em execução). o procedimento não protege contra vulnerabilidades existentes,mas dificulta a vida de quem deseja obter informações sobre o seu sistema. ****

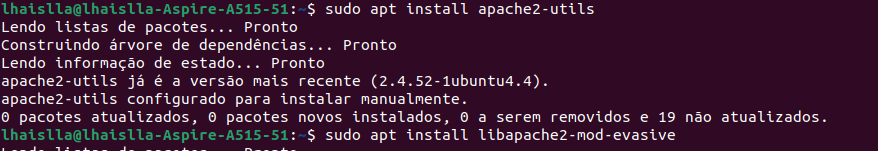
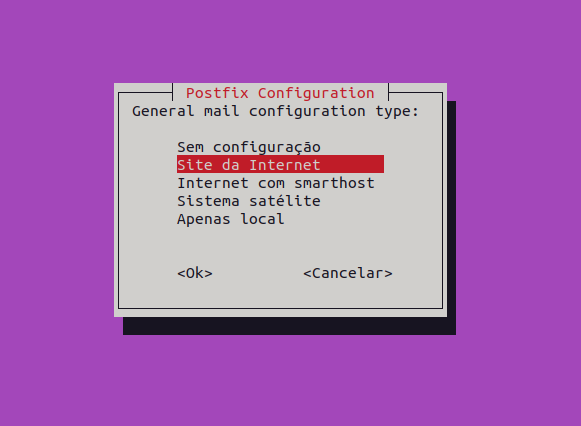
****

****

1. **Desabilitar a listagem de diretórios:**A listagem de diretórios é um recurso que permite ao visitante, visualizar todo o conteúdo de um determinado diretório do servidor WEB através do browser, se este não conter um arquivo de índice. Este recurso é bom por um lado, porém automaticamente abre brechas, pois acaba expondo todos os arquivos de um determinado diretório para qualquer visitante que chegar ao seu site. **  
     
     
   **
2. **Desabilitar módulos desnecessários:**Por padrão, o Apache vem com uma série de módulos pré-instalados e ativados. No entanto, isso cria uma vulnerabilidade de segurança adicional. A fim de reduzir suas chances de se tornar uma vítima de um ataque web, é melhor para desativar os módulos que não estão sendo usados ​​atualmente. A exemplo o módulo expires esta sendo desabilitados, mas outra forma de desabilitar módulos desnecessários é através do arquivo httpd.conf, adicionando um caractere # na frente da linha LoadModule.   
    ****
3. **Atualizar o Apache:** Ao instalar o apache é necessário que se mantenha atualizado, evitando que brechas no servidor web gerem invasões e possibilitando a corrigidas de uma versão para outra ao atualizar.   
   

1. **Limitar o acesso ao sistema operacional:** comentar a linha options Indexes FollowSymLinks para que algum invasor não possa navegar pelos diretórios do Apache, é que links simbólicos não permita o acesso ao /, ou seja, ao sistema operacional. **  
   **
2. **SeverTokens**  
   É recomendável acordo com as especificações HTTP que os servidores web sejam identificados por meio do cabeçalho, que inclui em informações de versão, paar que não haja a divulgação e execução indesejável em ambiente sensíveis, é indicado que se remova a versão do cabeçalho.   
    **  
     
   **
3. **Bloquear acesso ao diretório:**O bloqueio dos diretórios, permite ao servidor web identificar o que esta sendo acessado do diretório. 
   1. Para bloquear o diretório completamente:
      1. Require all denied
   2. Permitir o acesso ao diretório para determinadas pastas:
      1. Require all granted
   3. Permitir apenas os usuários autorizados:
      1. Require all granted
   4. Ocultar o diretório raiz dos usuários:
      1. Options -Indexes
4. **Desabilitar o rastreamento HTTP**A ativação do traceEnable, pode facilitar o acesso das informações por parte de hackers mediante cookies e causar problemas de rastreamento dos sites. Desta forma é imprescindível que HTTP Trace na configuração do apache seja modificado ou adicionado para evitar vulnerabilidades ao servidor web.   
     
   

1. **Controle de grupos:** Os servidores apache, como pacote de sistemas operacional, permitem o uso de um nome de grupo como data ou nobody. ****
2. **Ativar mod\_evasive:** O mod\_evasive atua na proteção do servidor web contra Sistibuted Denial of Service(DDoS) e ataques de força bruta, bloqueando as tentativas de login simultâneo e com falhas, além de monitorar IPs mal-intencionados.

Referências:

<https://youtu.be/zE5CJQRdcJw>

<https://www.twaino.com/pt/blogue/criacao-do-site/servidor-apache-um-guia-completo-para-iniciantes/>

<https://www.vivaolinux.com.br/artigo/13-dicas-de-seguranca-para-o-Apache>   
  
<https://help.umbler.com/hc/pt-br/articles/9660495371405-Melhorando-a-seguran%C3%A7a-do-Apache>

<https://youtu.be/9LYJctk3gWQ>

<https://www.ppgia.pucpr.br/pt/arquivos/techdocs/linux/foca-avancado/ch-s-apache.html>

<https://youtu.be/tkGXvGGiGpo>