Relatório - Trabalho Prático de Instalação - Redes de Computadores

Integrantes:
Breno Carvalho Pedroso - 10A
Caio Henrique Noronha - 10A
Lucas Malachias Furtado - 10A
Thiago Pereira Freire - 10A

VMS Utilizadas:
As máquinas virtuais utilizadas pelo grupo foram: 192.168.1.9, que foi utilizada para hospedar o servidor web e o servidor NTP; e 192.168.1.10.

Configurações gerais:

Após termos configurado o VPN, logamos nas duas VMs e utilizamos o comando “passwd” para atualizar as senhas do usuário “aluno”.

Serviço de sincronização de hora:

Para sincronizar o horário da primeira VM (192.168.1.9) com o servidor NTP.br foi utilizado o timesyncd. Primeiramente foi modificado o arquivo de configuração /etc/systemd/timesyncd.conf. Nele foram adicionados os servidores para serem feitas as requisições. O arquivo ficou da seguinte forma:

```
Unset
        [Time]
        NTP=a.st1.ntp.br b.st1.ntp.br c.st1.ntp.br d.st1.ntp.br gps.ntp.br
a.ntp.br b.ntp.br c.ntp.br
```

Após isso, para verificar o funcionamento do serviço de sincronização de hora, foi utilizado o comando “timedatectl” como mostrado a seguir:

```
[21:19:37] DEBIAN: aluno@vm09 [~]$ timedatectl status
               Local time: sáb 2023-06-17 21:19:48 -03
           Universal time: dom 2023-06-18 00:19:48 UTC
                 RTC time: dom 2023-06-18 00:19:48
                Time zone: America/Sao_Paulo (-03, -0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

```
[21:20:09] DEBIAN: aluno@vm09 [~]$ timedatectl show-timesync
SystemNTPServers=a.st1.ntp.br b.st1.ntp.br c.st1.ntp.br d.st1.ntp.br gps.ntp.br a.ntp.br b.ntp.br c.ntp.br
FallbackNTPServers=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
ServerName=a.st1.ntp.br
ServerAddress=200.160.7.186
RootDistanceMaxUSec=5s
PollIntervalMinUSec=32s
PollIntervalMaxUSec=34min 8s
PollIntervalUSec=34min 8s
NTPMessage={ Leap=0, Version=4, Mode=4, Stratum=1, Precision=-22, RootDelay=0, RootDispersion=991us, Reference=ONBR, OriginateTimestamp=Sat 2023-06-17 20:51
:51 -03, ReceiveTimestamp=Sat 2023-06-17 20:51:51 -03, TransmitTimestamp=Sat 2023-06-17 20:51:51 -03, DestinationTimestamp=Sat 2023-06-17 20:51:51 -03, Igno
red=yes PacketCount=6, Jitter=2.108ms }
Frequency=1722286
```

Além disso, nessa VM também foi colocado um servidor NTP para servir a segunda VM (192.168.1.10). Para isso foi utilizado o próprio programa NTP. Para fazer ele apontar para o horário da própria foi o arquivo em /etc/ntp.conf foi modificado com as seguintes configurações de ip:

server 127.127.1.0

fudge 127.127.1.0 stratum 10

Após isso, o ntp foi reiniciado e o servidor começou a funcionar.

Por fim, foi feito o mesmo procedimento de configuração de cliente NTP na segunda VM. A única diferença foi que o arquivo /etc/systemd/timesyncd.conf ficou da seguinte forma para requisitar da primeira VM:

```
[Time]
NTP=192.168.1.9
```

O método de verificação foi o mesmo da primeira VM.

Problemas encontrados:

Para a sincronização de hora, encontramos problemas durante a utilização do Chrony. Portanto, decidimos que poderíamos tentar como alternativa a utilização de outro serviço e, dessa forma, conseguimos configurar o servidor corretamente utilizando o timesyncd, que não apresentou os problemas anteriores do Chrony.

Configuração do Servidor Web com Nginx e HTTPS:

A configuração do servidor web foi feita utilizando o servidor Nginx, incluindo a geração de um certificado auto-assinado e a configuração do HTTPS. Os detalhes da configuração são fornecidos a seguir.

1. Geração do Certificado Auto-assinado: Para habilitar a comunicação segura HTTPS, foi gerado um certificado auto-assinado juntamente com uma chave privada usando o comando OpenSSL. A seguinte linha de comando foi executada para gerar o certificado e a chave:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout /etc/nginx/ssl/chave_privada.key -out
/etc/nginx/ssl/certificado.crt
```

Esse comando gerou um certificado válido por 365 dias e uma chave privada RSA de 2048 bits. Os arquivos de certificado foram salvos em "/etc/nginx/ssl/certificado.crt" e a chave privada em "/etc/nginx/ssl/chave_privada.key".

2. Configuração do Nginx para HTTPS: No arquivo de configuração principal do Nginx, em "/etc/nginx/nginx.conf", foi adicionado o seguinte bloco de configuração para habilitar o suporte HTTPS:
   nginx

```
server {
    listen 443 ssl;
    server_name 192.168.1.9;

    ssl_certificate /etc/nginx/ssl/certificado.crt;
    ssl_certificate_key /etc/nginx/ssl/chave_privada.key;
}
```

   Nessa configuração, o Nginx é configurado para escutar na porta 443, que é o padrão para HTTPS. O certificado e a chave privada gerados anteriormente são especificados nos parâmetros `ssl_certificate` e `ssl_certificate_key`, respectivamente.

Para averiguar o funcionamento do servidor web foi utilizado um navegador. No browser, ao digitar o endereço do servidor web 192.168.1.9 foi possível ver que a página estava funcionando. Além disso, por meio da opção do navegador “Informações da Página“ foi possível certificar que a configuração do HTTPs estava correta.

Problemas encontrados:
Para configurar Nginx para HTTPS, era necessário um certificado. Como solução, adicionamos um certificado auto-assinado. Porém, ao entrar na página web, o navegador identifica o site como não seguro.