Gabarito da Prova Prática IFSULDEMINAS

Atividade 1 – Configurações de Rede (Total 25 pontos)

Obs: (1) Para este gabarito foi utilizado a primeira subrede (192.168.10.0), porém conforme o enunciado da questão, poderá ser utilizada qualquer outra sub-rede configurada com a mesma máscara 255.255.255.248. (2) As configurações de endereçamento (address, netmask, network, broadcast e gateway) não precisam estar na sequência apresentada no gabarito.

a) Arquivo(s) de configuração de rede alterado(s): **(peso 5,0)**

```
/etc/network/interfaces
```

b) Alteração(ões) realizada(s) na configuração de rede da máquina virtual Servidor: **(peso 5,0)**

Alterar a linha:
```
iface enp0s3 inet manual
```

para:
```
iface enp0s3 inet dhcp
```

Alterar a linha:
```
iface enp0s8 inet manual
```

para:
```
iface enp0s8 inet static
```

E adicionar as seguintes linhas abaixo da configuração acima:
```
address 192.168.10.1
netmask 255.255.255.248
network 192.168.10.0
broadcast 192.168.10.7
```

c) Alteração(ões) feitas na configuração da rede da máquina virtual Cliente1: **(peso 5,0)**

Alterar a linha:

```
iface enp0s3 inet manual
```

para:
```
iface enp0s3 inet static
```

E adicionar as seguintes linhas abaixo da configuração acima:

```
address 192.168.10.2
netmask 255.255.255.248
network 192.168.10.0
```

```
broadcast 192.168.10.7
gateway 192.168.10.1
```

d) Alteração(ões) feitas na configuração de rede da máquina virtual Cliente2: **(peso 5,0)**

Alterar a linha:

```
iface enp0s3 inet manual
```

para:

```
iface enp0s3 inet static
```

E adicionar as seguintes linhas abaixo da configuração acima:

```
address 192.168.10.3
netmask 255.255.255.248
network 192.168.10.0
broadcast 192.168.10.7
gateway 192.168.10.1
```

e) Alteração(ões) feitas no arquivo “hosts” das máquinas virtuais (se os arquivos ficarem iguais, informe apenas uma vez – desconsidere a configuração de IPv6): **(peso 5,0)**

Adicionar as seguintes linhas no arquivo /etc/hosts das máquinas virtuais Servidor, Cliente1 e Cliente2:

```
192.168.10.1 servidor.ifsuldeminas.edu.br servidor
192.168.10.2 cliente1.ifsuldeminas.edu.br cliente1
192.168.10.3 cliente2.ifsuldeminas.edu.br cliente2
```

ou

```
192.168.10.1 servidor.ifsuldeminas.edu.br
192.168.10.2 cliente1.ifsuldeminas.edu.br
192.168.10.3 cliente2.ifsuldeminas.edu.br
```

Atividade 2 – Configuração de um Servidor Web (Total 27 pontos)

a) Altere o arquivo de configuração do virtual host “padrão” para que o diretório raiz (diretório “root” do serviço) aponte para o diretório “/padrao”, altere o e-mail do administrador do servidor para webmaster@ifsuldeminas.edu.br e altere o nome do servidor para www.ifsuldeminas.edu.br**: (peso 5,0)**

No arquivo /etc/apache2/sites-available/padrao.conf ou no seu link simbólico /etc/apache2/sites-enabled/padrao.conf:

O DocumentRoot deve ser modificado para
`DocumentRoot /padrao`

A diretiva `ServerName` deve ser modificada para
ServerName www.ifsuldeminas.edu.br

A diretiva `ServerAdmin` deve ser modificada para
`ServerAdmin webmaster@ifsuldeminas.edu.br`

b) Altere o arquivo de configuração do virtual host “padrão” para que, ao se realizar um acesso pelo navegador a uma página no site configurado, não se tenha o erro “Forbidden. You don't have permission to access / on this server” (ou seja, acesso negado ao diretório raiz do servidor): **(peso 6,0)**

adicionar a seguinte diretiva no arquivo /etc/apache2/sites-available/padrao.conf ou no seu link simbólico /etc/apache2/sites-enabled/padrao.conf:

```
<Directory /padrao/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

c) Desative o virtual host “siteantigo” de forma que ele possa ser ativado novamente no futuro. Não exclua o(s) arquivo(s) de configuração do virtual host: **(peso 5,0)**

`a2dissite siteantigo`

ou

Remover link simbólico `siteantigo.conf` em /etc/apache2/sites-enabled/ com o comando rm /etc/apache2/sites-enabled/`siteantigo.conf`

d) Altere a configuração do virtual host “sitenovo” para que o diretório raiz aponte para o diretório “/sitenovo” e para que o virtual host funcione utilizando a porta 84. Adicione também configurações para que, ao se realizar um acesso pelo navegador a uma página no site configurado, não se tenha o erro “Forbidden. You don't have permission to access / on this server” (ou seja, acesso negado ao diretório raiz do servidor). Após as configurações, ative o virtual host: **(peso 6,0)**

No arquivo /etc/apache2/sites-available/sitenovo.conf

Adicionar a linha: `Listen 84`

Alterar a diretiva `<VirtualHost *:80>` para `<VirtualHost *:84>`

Alterar a diretiva `DocumentRoot` para
`DocumentRoot /sitenovo`

Adicionar a seguinte diretiva:

```
<Directory /sitenovo/>
     Options Indexes FollowSymLinks
     AllowOverride None
     Require all granted
</Directory>
```

Ativar o virtual host “sitenovo” através do comandos:

```
a2ensite sitenovo
```

ou através da criação de um link simbólico:

```
ln -s /etc/apache2/sites-available/sitenovo.conf /etc/apache2/sites-enabled/sitenovo.conf
```

e) ~~Através de um navegador do computador hospedeiro, acesse o site configurado pelo virtual host “sitenovo” e transcreva aqui o conteúdo exato mostrado na tela do navegador:~~ ~~**(peso 5,0)**~~

~~<edital 72-2019> prova prática - área: "infraestrutura"~~

A PRÁTICA “E” DA ATIVIDADE 2 FOI ANULADA. TODOS RECEBEM OS REFERIDOS PONTOS.

Atividade 3 – Gerenciamento de Servidores (Total 26 pontos)

a) No Servidor: Informe o caminho absoluto do arquivo que deve ser editado para modificar as configurações do servidor OpenSSH: **(peso 5,0)**

```
/etc/ssh/sshd_config
```

b) No Servidor: Altere as diretivas do arquivo de configuração do servidor OpenSSH para que o serviço utilize ("escute") a porta 3333: **(peso 5,0)**

Inserir a linha:
```
Port 3333
```

ou

Descomentar a linha:
```
#Port 22
```
e alterar o número 22 para 3333, ficando:
```
Port 3333
```

c) No Servidor: Altere as diretivas do arquivo de configuração do servidor OpenSSH para que o serviço permita o login do usuário "root": **(peso 5,0)**

Inserir a linha:
```
PermitRootLogin yes
```

ou

Descomentar a linha:

```
#PermitRootLogin prohibit-password
```
e alterar o valor "prohibit-password" para "yes", ficando:
```
PermitRootLogin yes
```

d) No Cliente2: Envie, através do comando de cópia segura de arquivos (que utiliza o protocolo SSH), o arquivo "/root/teste-cliente1.sh" para o diretório "/root" da máquina virtual Servidor. Não utilize o comando SFTP e considere a porta 3333 já alterada no Servidor anteriormente. Obs: (1) Se lhe for apresentada a seguinte mensagem: "Are you sure you want to continue connecting (yes/no)?", responda "yes". (2) Utilize a credencial de acesso já informada: **(peso 6,0)**

```
scp -P 3333 /root/teste-cliente1.sh root@192.168.10.1:/root
```

ou

```
scp -P 3333 /root/teste-cliente1.sh root@servidor.ifsuldeminas.edu.br:/root
```

ou

```
scp -P 3333 /root/teste-cliente1.sh root@servidor:/root
```

Obs: (1) qualquer variação do comando SCP que, depois de testado pela banca, produza o mesmo efeito do comando acima, será aceito. (2) o IP do servidor “192.168.10.1” pode ser outro de acordo com a rede e o IP selecionado na atividade 1. Também poderá ser utilizado o nome do servidor de acordo com a configuração efetuada no arquivo hosts na atividade 1.

e) No Servidor: Execute o script “/root/teste-cliente1.sh” no terminal. Transcreva aqui a saída da execução do script na tela. Obs: (1) Caso o script não execute por falta de permissão, digite no prompt do terminal o comando: “chmod a+x /root/teste-cliente1.sh” e execute o script novamente. (2) Se lhe for apresentada a seguinte mensagem: “Are you sure you want to continue connecting (yes/no)?”, responda “yes”. (3) Utilize a credencial de acesso já informada: **(peso 5,0)**

```
<edital 72-2019> prova prática - área: "infraestrutura" - script teste
cliente1
```

Atividade 4 – Firewall (Total 22 pontos)

a) No Servidor: Execute comandos do IPTABLES para que as conexões ao serviço SSH (OpenSSH) do servidor na porta 3333, vindas da máquina virtual Cliente1, sejam bloqueadas: **(peso 6,0)**

Serão aceitas as seguintes respostas e serão consideradas as outras nomenclaturas das opções de acordo com o manual do IPTABLES:

- `iptables -A INPUT -s 192.168.10.2 -p tcp --dport 3333 -j DROP`
- `iptables -A INPUT -s 192.168.10.2 -p tcp --dport 3333 -j REJECT`
- `iptables -I INPUT -s 192.168.10.2 -p tcp --dport 3333 -j DROP`
- `iptables -I INPUT -s 192.168.10.2 -p tcp --dport 3333 -j REJECT`

Obs: o IP do cliente1 “192.168.10.2” pode ser outro de acordo com a rede e o IP selecionado na atividade 1

b) No Servidor: Execute comandos do IPTABLES para que as conexões ao serviço Web (Apache) do servidor na porta 80, vindas da máquina virtual Cliente2, sejam bloqueadas: **(peso 6,0)**

Serão aceitas as seguintes respostas e serão consideradas as outras nomenclaturas das opções de acordo com o manual do IPTABLES:

- `iptables -A INPUT -s 192.168.10.3 -p tcp --dport 80 -j DROP`
- `iptables -A INPUT -s 192.168.10.3 -p tcp --dport 80 -j REJECT`
- `iptables -I INPUT -s 192.168.10.3 -p tcp --dport 80 -j DROP`
- `iptables -I INPUT -s 192.168.10.3 -p tcp --dport 80 -j REJECT`

Obs: o IP do cliente2 “192.168.10.3” pode ser outro de acordo com a rede e o IP selecionado na atividade 1

c) No Cliente1: Execute o comando NMAP com o parâmetro “-p 0-4000 -open” e verifique as portas dos serviços em funcionamento na máquina virtual Servidor. Transcreva abaixo a saída do comando na tela informando todos os serviços abertos encontrados e suas respectivas portas (apenas as portas encontradas e os respectivos serviços). Obs: Serão consideradas as portas abertas ou fechadas nas atividades 2, 3 e 4 e as já abertas/fechadas na máquina virtual Servidor: **(peso 5,0)**

Comando:

```
nmap 192.168.10.1 -p 0-4000 -open
```

Saída do comando (transcrito somente as portas e o nome dos serviços):

```
PORT      SERVICE
80/tcp    http
84/tcp    ctf
631/tcp   ipp
```

Obs: o IP do servidor “192.168.10.1” pode ser outro de acordo com a rede e o IP selecionado na atividade 1

d) No Cliente2: Execute o comando NMAP com o parâmetro “-p 0-4000 -open” e verifique as portas dos serviços em funcionamento na máquina virtual Servidor. Transcreva abaixo a saída do comando na tela informando todos os serviços abertos encontrados e suas respectivas portas (apenas as portas encontradas e os respectivos serviços). Obs: Serão consideradas as portas abertas ou fechadas nas atividades 2, 3 e 4 e as já abertas/fechadas na máquina virtual Servidor: **(peso 5,0)**

Comando:

```
nmap 192.168.10.1 -p 0-4000 -open
```

Saída do comando (transcrito somente as portas e o nome dos serviços):

```
PORT      SERVICE
84/tcp    ctf
631/tcp   ipp
3333/tcp  dec-notes
```

Obs: o IP do servidor “192.168.10.1” pode ser outro de acordo com a rede e o IP selecionado na atividade 1