

**Disciplina:** Sistemas Operacionais Linux

**Turma:** ADS5

**Professor:** Roitier Campos Gonçalves

**Aluno (a):**

**Data:** 14/11/2018

**Valor:** 25 Pontos

**Resultado:**

## INSTRUÇÕES

- Use caneta azul ou preta, sendo que na prova e/ou questão escrita, entregue a lápis, o aluno perderá o direito de reclamar na vista de prova.
- Não é permitido: consulta a quaisquer materiais, colegas de classe e/ou troca de materiais dentro da sala de aula durante a realização da avaliação.
- Os alunos que cometerem quaisquer atos no intuito de fraudar a avaliação serão punidos e poderão obter nota zero.
- Não será tolerado qualquer tipo de rasura nas questões objetivas.
- Esta prova contém **3** questões. Verifique se o seu exemplar está completo.

## Orientação sobre a resolução das questões de 01 a 03

Pressupondo você foi contratado para Administrar uma rede, em substituição a um Administrador recém demitido. Assuma que neste momento você está administrando um servidor com sistema operacional GnU/Linux Debian 9 e transcreva todos os comandos necessários para realizar as seguintes ações. Mas atente-se, pois não necessariamente as regras se complementem. Sendo assim, quando isso acontecer, transcreva a regra que solucionar a questão, sem se ater a respostas anteriores.

**Cenário:** (Para uso em todas as questões)

A rede conta com 100 Host, todos conectados à Internet através de um único Servidor. O Servidor conta com duas interfaces de rede, uma conectada à LAN e outra conectada à WAN. Neste caso, desconsidere-se especificidade de equipamentos de interconexão de rede e assume que o servidor está diretamente conectado à LAN e WAN.

### Dados da rede:

- LAN: 192.168.0.0/24
- WAN: 177.29.28.1/24
- Gateway do Servidor: 177.29.28.254
- Servidor Proxy Squid
- Filtro de Pacotes Netfilter(Iptables)

### Questão 01: (5,0 pt)

#### Bloqueando o envio de mensagem ICMP echo.

- Verifique as regras instaladas no iptables.
- Supondo que no comando anterior foram encontradas inúmeras regras, remova todas.
- Caso ainda não estejam, mude a política default de todas as chain para ACCEPT
- Crie uma regra Descartando os Pacotes ICMP, de forma que este servidor não possa enviar ou receber requisições de PING na rede. Crie uma regra Rejeitando os Pacotes ICMP, de forma que este servidor não possa enviar ou receber requisições de PING na rede, contudo, quando receber uma requisição, informe o emissor quanto a Rejeição do Pacote.

### Questão 02: (13,0 pt)

#### Elabore um "script shell" que atenda às seguintes necessidades:

- Adicione regras que para criar uma variável chamada "DNS-1" e atribuir um DNS funcional para sua configuração.
- Adicione regras que para criar uma variável chamada REDE-01 e atribuir o endereço da LAN
- Adicione regras que para criar uma variável chamada REDE-02 e atribuir o endereço da WAN
- Adicione regras que Habilite o encaminhamento(FORWARD) de pacotes entre interfaces do Servidor.
- Adicione regras que permita o Squid funcionar no modo Transparente.
- Adicione regras que libere Limpe/Apague todas regras que possam já estar em funcionamento no sistema, inclusive as regras das possíveis Chain outrora criadas pelo Administrador da Rede.
- Defina a Política Padrão de todas as Chain como DROP.
- Adicione regras que libere o acesso ao servidor através da interface de Loopback, exclusivamente.
- Adicione regras que libere consultas a servidores DNS-1.

- j) Adicione regras permitindo que qualquer computador da rede façam, com sucesso, requisições HTTP e HTTPS na internet.
- k) Adicione regras permitindo que qualquer computador da rede envie e receba e-mail utilizando Softwares de Gerenciamento de Email, como Outlook e Thunderbird.
- l) Configure o Script de modo que este seja um executável em ambientes linux.
- m) Adicione regras que libere acesso SSH a um host da rede, mantendo o servidor inacessível a esse tipo de conexão.

**Questão 03: (7,0 pt)**

Configure um Servidor Proxy Squid que atenda às seguintes necessidade:

- a) Funcione em modo Transparente.
- b) Funcione na Porta Padrão.
- c) Permita navegação a apenas computadores presentes na rede local.
- d) Contenha uma blacklist.
- e) Tenha um controle de acesso por horário, o qual apenas os 5 primeiros IPs da rede LAN estejam bloqueados entre 10:00 e 11:00.

*Fim.*

*RESPOSTA A PARTIR DAQUI:*