Universidade Federal do Ceará

Curso: Redes de Computadores
Disciplina: Segurança da Informação
Professor: Marcos Dantas Ortiz

Exercícios – Iptables e Squid

1) Explicar o que as seguintes regras fazem:

a) iptables -t filter -A INPUT -s 192.168.0.0/24-i eth1 -j ACCEPT

b) iptables -A INPUT -j LOG --log-prefix "FW INPUT"

c) iptables -I FORWARD -s 192.168.0.0/24 -d www.facebook.com -j DROP

d) iptables -A OUTPUT -o lo -j ACCEPT

e) iptables -D FORWARD -s 192.168.13.0/24 -d www.google.com -j REJECT

f) iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

2) Criar regras necessárias para implantar as seguintes políticas de segurança no Firewall, utilizando cenário de rede virtualizado (virtaulbox):
Obs.: adicione nas respostas as regras e os prints dos tráfegos

a) Por padrão, o Firewall deve descartar todos os pacotes.

b) Habilitar a realização de pings destinados ao Firewall, provenientes apenas da rede externa.

c) Habilitar a realização de pings de máquinas da rede interna, para máquinas da rede externa.

d) Habilitar a o acesso à Internet para as máquinas da rede interna, bloqueando as requisições HTTP provenientes da rede externa.

e) Permitir o acesso remoto via SSH, no host do Firewall, apenas para as máquinas da rede interna.

3) Utilizando o Squid e Iptables, configure um Proxy Transparente. Crie acls que implementem os seguintes controles:
Obs.: adicione nas respostas as regras e os prints dos tráfegos

- Não permitam acessos a sites listados em um arquivo (lista negra)
- Permitam acesso a sites listados em um arquivo (lista branca)
- Não permitam acessos a sites que contenham a palavra “porn” na url de origem
- Não permitam acessos das 12h até as 13h.