Universidade Federal do Ceará

Disciplina: Segurança

Professor: Marcos Dantas Ortiz

Exercícios – Iptables

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

2) Criar regras necessárias para implantar as seguintes políticas de segurança no Firewall, utilizando cenário de rede virtualizado (virtualbox):

   Obs.: adicione nas respostas as regras e os prints dos tráfegos (quando possível)

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

   b) Permitir o tráfego loopback no host do firewall.

   Testar com ping (ICMP) para o próprio host - 127.0.01

   c) Permitir o acesso remoto via SSH, no host do Firewall.

   -------- Configurar o firewall através de outra máquina por ssh --------

   ssh user@ip_do_firewall

   d) Habilitar a realização de pings destinados ao Firewall.

   e) Permitir que o host do firewall faça requisições DNS.

   Testar com nslookup

   f) Permitir que o host do firewall faça requisições HTTP.

   Testar com wget

   g) Permitir que o host do firewall faça requisições HTTPS.

Testar com wget

h) Rejeite o envio de e-mails a partir do host do firewall.

i) Bloqueie conexões vindas do IP: 200.129.23.54

j) Refaça os itens e),f) e g) usando o controle de estados.