Segurança de Redes
Prática – Firewall – Netfilter/iptables

Entregar um relatório contendo as regras configuradas no laboratório e explicação de todas elas. Descrever como foram feitos os testes para verificação do funcionamento das regras, indicando o correto funcionamento (ou não) das mesmas.

Crie regras usando *iptables* e teste seu funcionamento. Utilize os slides da aula de firewall, a ajuda do Linux e sites da Internet como referência. Cada exercício é independente, não se esqueça de apagar as regras anteriores se necessário.

1) Definir as regras da política padrão dos *chains* das tabelas filter.
2) Criar regra(s) para "esconder" seu computador na rede (bloquear tentativas de ping).
3) Criar uma *blacklist* de IPs bloqueados e definir regra(s) para bloquear estes endereços IP.
4) Criar regra(s) para bloquear ping originado do seu computador.
5) Armazenar em log os pacotes descartados nos itens 3 e 4 (o *syslog* do sistema geralmente está em *var/log*).
6) Aceitar todo o tráfego vindo da interface de rede Ethernet e bloquear o tráfego de loopback.
7) Definir uma política (aceitar/bloquear) para os protocolos SMTP, POP e acesso a web (HTTP e HTTPS). Criar regras que implementem a política definida.
8) Pesquise e crie regras para tentar evitar atividades maliciosas na rede, como DoS, scanner de portas, *ip spoofing*, etc.
9) Crie um *chain* na tabela filter onde será tratado todo o tráfego de um IP específico. Este computador deve ter acesso a todos os serviços, exceto FTP.
10) Suponha que você seja o administrador de redes de uma empresa. Considere que a empresa possui três departamentos: recursos humanos, engenharia e tecnologia da informação (cada departamento usa uma sub-rede específica). Cada departamento tem necessidades diferentes de acesso à rede. Considere ainda que gerentes possuem privilégios maiores de acesso que outros usuários. Crie políticas de acesso à rede para os usuários e crie as regras correspondentes usando Netfilter/iptables.