Vinicius Augusto de Souza - 1997530
AS36B - Segurança e Auditoria de Sistemas - N16
Atividade 5 - Firewall

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS CORNÉLIO PROCÓPIO

Um Firewall é um dispositivo de segurança de rede que monitora e filtra o tráfego de rede de entrada e saída com base nas políticas de segurança estabelecidas anteriormente por uma organização. Basicamente, um firewall é essencialmente a barreira que fica entre uma rede interna privada e a Internet pública. O objetivo principal de um firewall é permitir a entrada de tráfego não ameaçador e impedir a entrada de tráfego perigoso.

Firewalls são importantes para as redes cabeadas, porém existem algumas opções que também podem ser acatadas para melhorar a segurança, como por exemplo, realizar um mapeamento e auditoria sobre a rede para levantar as possíveis ameaças, utilização de VLANs para separar o tráfego, o que também aumenta a performance , utilizar filtros de endereçamento MAC que vão realizar uma primeira autenticação na rede com fio, uso da autenticação 802.1x que também aplica autenticação e criptografia, utilização de VPNs para também implementar criptografia.

Já para as redes sem fio, é importante que haja também um gerenciamento dos dispositivos conectados, para que não hajam dispositivos maliciosos na rede que sejam capazes de interferir, realizar a segmentação de acesso a rede, para que existam barreiras de acesso a informações, utilizar um sistema de prevenção de intrusões – WIPS, o qual realiza a monitorização das ondas de rádio, procurando e alertando para pontos de acesso não autorizados ou atividades nocivas

Os iptables são firewalls muito potentes, os quais permitem a manipulação e configuração dos pacotes na camada de rede ou transporte. Os pacotes são modificados utilizando o comando `iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE`, o qual troca os IP's internos pelos IP's externos quando os pacotes estão quase sendo enviados para a rede, para que assim o retorno seja efetuado, e realiza a troca novamente quando a resposta é devolvida, fazendo com que se pareça que não existe um servidor intermediando toda esta operação.