Curso On Line Iptables e Squid

A preocupação de preservar a informação aumenta frequentemente na medida em que o número de vítimas de ataques por hackers cresce. Assim, diante deste desafio devem-se criar ações de segurança, notadamente empregar as tecnologias referentes à segurança da informação para obter um nível de segurança aceitável adotando os elementos básicos, cuja fundamentação é:

“Confidencialidade:

Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas as pessoas para quem elas são destinadas;

Integridade:

Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais;

Disponibilidade:

Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.”

A seguir vão algumas definições:

Firewall

O Firewall é um programa que tem como objetivo proteger a máquina contra acessos e tráfegos indesejáveis, proteger serviços que esteja rodando e bloquear a passagem de pacotes que não se queiram receber.

Iptables

É um firewall em nível de pacote e funciona baseado no endereço/porta de origem/destino do pacote. Funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar.

Características:

- Trabalha com a especificação de portas/endereços de origem/destino;
- Suporte a protocolos TCP/UDP/ICMP;
- Suporte a interfaces de origem/destino;
- Manipula serviços de proxy na rede;
- Tratamento de tráfego divido em chains;
- Muito rápido, estável e seguro;
- Permite enviar alertas personalizados ao syslog;

- Suporte a SNAT e DNAT
- Permite especificar prioridade para determinados tipos de pacotes.

Squid

O Squid é um servidor proxy que suporta HTTP, HTTPS, FTP e outros. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache de requisições frequentes de páginas web numa rede de computadores. Ele pode também ser usado como um proxy reverso, sendo que foi escrito originalmente para rodar em sistema operacional tipo Unix, mas ele também funciona em sistemas Windows desde sua versão2.6.STABLE4.2

Com o Squid você pode instalar um servidor Linux com acesso à Internet, e fazer com que outras máquinas clientes (usando Linux, Windows ou outro sistema operacional) acessem páginas web e sites ftp através do servidor Linux, mesmo que estas máquinas clientes não tenham conexão direta com a internet - tudo que elas precisam é o acesso ao próprio servidor onde está rodando o Squid.

Fonte:Wikipedia

Objetivos

Prover conhecimento em desenvolvimento de sistemas de proteção para redes independente do porte da mesma.

Público alvo

Administradores de Sistemas, Estudantes, Analistas de Rede e interessados em geral que desejam aprender como trabalhar com Firewall e Proxy no Linux.

Benefícios

Ao concluir esta formação:

Será possível identificar e proteger o ambiente contra os principais vírus e ataques realizados por hackers, eliminando a vulnerabilidade por falta de proteção e vedando acesso a sites perigosos. Tudo isso se utilizando de computadores e ferramentas de baixo custo.

Em estudar à distância:

- Aula ao vivo gravada e disponibilizada no ambiente à distância. Ela ficará disponível em até 30 (trinta) dias após o término do curso, para o aluno assistir o quanto quiser, tendo duas opções de estudo, online e off-line. O aluno adapta seu tempo de estudo de acordo com sua disponibilidade;

- Fórum de discussão, onde os alunos poderão postar suas dúvidas e ideias. O professor irá respondê-lo em até 5 (cinco) dias após o término do curso;
- O material didático estará disponível na plataforma, para que o aluno faça o download;
- Turma com no máximo 20 alunos, para a melhor didática.

Metodologia de ensino

Ação educacional com forte conteúdo prático.

Pré-requisitos

Conhecimentos básicos de Linux e redes.

Material Didático

Apostila ou livro disponibilizado em ambiente EAD

Conteúdo Programático

Principais tópicos:

- Firewall Filtro de Pacotes
- Firewall NAT
- Firewall Hibrido
- Fluxo do Kernel vs. Netfilter
- A Tabela Filter
- A Tabela Nat
- A Tabela Mangle
- Firewall Iptables
- Conceitos
- Lógica
- Detalhando NAT
- Detalhando a Mangle
- Módulos
- Regras para Firewall Iptables
- Instalando o Squid
- Proxy Transparente
- Bloqueando Sites indesejados
- Bloqueio de Banners
- Protegendo usuários com antivírus
- Controle de Banda

- ACLs
- Gerando relatórios
- Examinando o Squid.conf
- Criando um arquivo de configuração automática
- Trabalhando com Hierarquias
- Configuração de proxy reverso