

Objetivos

O objetivo deste curso é capacitar aos alunos o entendimento filosófico sobre segurança, baseando-se na cultura popular de que: “O conhecimento é a chave do sucesso”.

O curso não se preocupa com o ensinamento de comandos do firewall ou contra-ataques aos intrusos.

A preocupação maior está relacionada aos fundamentos sobre segurança e aplicação de políticas de segurança, de forma que o aluno após o curso esteja apto a identificar as vulnerabilidades e o emprego de regras de segurança em seu site, assim como configurar firewall e ferramentas IDS. A seguir apresentamos os tópicos básicos do curso.

Módulo de Firewall

- Tipos de Firewall: Filtro de pacotes, Proxy Server e Stateful
- Atuação do Firewall nas camadas de protocolo
- Vantagens e desvantagens de cada tipo de Firewall
- Topologia do Firewall

Módulo de Serviços da Internet

Serviços a nível de camada de aplicação e as vulnerabilidades
Configuração de cada serviço nos tipos de Firewall

- | | |
|----------------------|----------------|
| • E-mail: SMTP e POP | • FTP |
| • Telnet | • WWW:HTTP |
| • NFS | • DNS |
| • Finger | • Whois |
| • X11 | • Comandos “R” |
| • UUCP | • ICMP |
| • Serviços ARP | |

Módulo de Autenticação e Criptografia

- Kerberos implementações e Vulnerabilidades
- Criptografia: Chaves simétricas, assimétricas e certificação de chave pública
- PGP
- HTTPS

Módulo de Vírus

- Vírus: Boot Record, FAT, Diretório Root, Floppy Boot Record, MBR, Sistema de Serviços, de Macro e Arquivos de Programas
- Tipos: Polifórmicos, Invisíveis e Multipartite
- Medidas de Prevenção
- Vírus no ambiente Windows NT
- Vírus na Internet

Módulo de IDS

- | | |
|---------------------------------|------------------|
| • Tipos de IDS: Hosts e Network | • Assinaturas |
| • Fases de um ataque | • IDS + Firewall |
| • Implementação de IDS | |