Conheça as melhores ferramentas de segurança e aprenda a instalar e configurar sistemas Windows e Unix de forma segura Modalidade.

Segurança de Redes e Sistemas (EaD)

O aluno aprenderá sobre perímetros de segurança, através da implementação de uma solução completa de proteção de redes, utilizando técnicas como firewall, IDS, IPS e VPN.

O amplo escopo de conceitos abordados permitirá a aplicação das técnicas aprendidas de autenticação e autorização segura, auditorias de segurança e os requisitos de configuração segura de servidores Linux e Windows.

Após o curso, o aluno será capaz de montar um perímetro seguro, aumentar a segurança dos servidores da rede, realizar auditorias de segurança e implantar sistemas de autenticação seguros.

Características

- Curso com 5 (cinco) semanas de duração, com 2 (dois) encontros online por semana (total de 10 encontros);
- Os encontros serão ao vivo com tutor e terão 2 (duas) horas de duração;
- Para o auto estudo, o material de apoio será disponibilizado no AVA: livro do curso, materiais extras, indicação de leituras, atividades;
- Sugerimos que antes de iniciar os estudos, o aluno verifique o seu acesso à internet;
- Para acompanhamento do curso, sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox;
- **Para conclusão do curso é necessário que o aluno responda aos questionários e realize 75% das atividades propostas dentro dos prazos estabelecidos.**

Escola Superior de Redes RNP

esr.rnp.br

RNP

Competências desenvolvidas

Ao final do curso o aluno será capaz de:

- Propor novas soluções para perímetros seguros de rede.
- Avaliar aspectos relacionados à segurança de servidores Linux e Windows.
- Empregar soluções de proteção como IDS, IPS e realizar auditorias de segurança.

Conhecimentos prévios

- Conceitos e ações básicas na área de segurança física e lógica de redes e sistemas, como criptografia, assinatura, certificado digital e questões de segurança da informação, edição de textos em Linux ou o curso Introdução à Segurança de Redes;
- Conhecimentos básicos sobre arquitetura TCP/IP.

Investimento

- R$ 960,00

Programa do curso

Sessão 1: Fundamentos de segurança

1) Da divisão de grupos

2) Topologia geral de rede

3) Configuração do Virtualbox

4) Detalhamento das configurações de rede

5) Configuração da máquinas virtuais

6) Configuração de firewall e NAT

7) Teste de conectividade das VMs

8) Instalação do Virtualbox Guest Additions nas VMs Windows

9) Instalação do Virtualbox Guest Additions nas VMs Linux

10) Exercitando os fundamentos de segurança

11) Normas e políticas de segurança

Sessão 2: Explorando vulnerabilidades em redes

1) Transferindo arquivos da máquina física para as VMs

2) Sniffers para captura de dados

3) Ataque SYN flood

4) Ataque Smurf

5) Levantamento de serviços usando o nmap

Escola Superior de Redes RNP

esr.rnp.br

RNP

6) Realizando um ataque com o Metasploit em ambiente Windows

7) Realizando um ataque com o Metasploit em ambiente Linux

8) Realizando um ataque de dicionário com o medusa

Sessão 3: Firewall

1) Trabalhando com chains no iptables

2) Firewall stateful

3) Configurando o firewall FWGW1-G: tabela filter

4) Configurando o firewall FWGW1-G: tabela nat

6) Revisão final da configuração do firewall FWGW1-G

Sessão 4: Serviços básicos de segurança

1) Configuração do servidor de log remoto

2) Configuração do servidor de hora

3) Monitoramento de serviços

Sessão 5: Sistema de detecção/prevenção de intrusos

1) Instalação do Snort

2) Configuração inicial do Snort

3) Configurando atualizações de regras de forma automática com o PulledPork

4) Processando arquivos de log do Snort com o Barnyard2

5) Visualizando eventos com o Snorby

6) Integração dos serviços com o sistema

7) Gerando alertas para o IDS

8) Referências

Sessão 6: Autenticação, autorização e certificação digital

1) Uso de criptografia simétrica em arquivos

2) Uso de criptografia assimétrica em arquivos

3) Uso de criptografia assimétrica em e-mails

Escola Superior de Redes RNP

esr.rnp.br

RNP

4) Criptografia de partições e volumes

5) Autenticação usando sistema OTP

Sessão 7: Redes privadas virtuais e inspeção de tráfego

1) Interceptação ofensiva de tráfego HTTPS com o mitmproxy

2) Inspeção corporativa de tráfego HTTPS usando o Squid

3) VPN SSL usando o OpenVPN

Sessão 8: Auditoria de segurança da informação

1) Instalação do Nessus

2) Realizando um scan em SO Linux

3) Realizando um scan em SO Windows

4) Efeitos do firewall em um scan

5) Auditoria de servidores web

Sessão 9: Configuração segura de servidores Windows

1) Uso do Microsoft Security Compliance Toolkit

2) Configuração do controlador de domínio Active Directory

3) Configuração do firewall para o Active Directory

4) Adição de clientes ao Active Directory

5) Adição de usuários ao Active Directory

6) Distribuição de configurações via GPOs

7) Instalação e configuração do WSUS

8) Configuração de clientes no WSUS

Sessão 10: Configuração segura de servidores Linux

1) Análise de rootkits

2) Inserção de senha no bootloader

3) Remoção de serviços desnecessários

4) Controle granular de acesso a comandos

Escola Superior de Redes RNP

esr.rnp.br

RNP

5) Controle de uso do binário su

6) Controle de acesso à console do sistema

7) Exigência de parâmetros mínimos de senha

8) Controle de logoff automático

9) Desabilitando a combinação de teclas CTRL + ALT + DEL

Escola Superior de Redes RNP

esr.rnp.br

RNP