



Aprenda a mitigar risco e executar atividades corretivas na sua infraestrutura baseada no sistema operacional Linux com objetivo de torná-la preparada para enfrentar tentativas de ataque internas ou externas.

Hardening em Linux (Presencial)

Este curso tem como objetivo auxiliar administradores Linux interessados em proteger suas redes, mitigar riscos e executar atividades corretivas preparando sua infraestrutura de servidores Linux para resistir a determinadas tentativas de ataques ou violação na segurança da informação.

Características

- ▲ O curso está dividido em dez sessões, totalizando 40 horas;
- ▲ O curso oferece atividades práticas em laboratório. Cada aluno tem sua própria estação de trabalho;
- ▲ A Escola Superior de Redes oferece material didático exclusivo.

Competências desenvolvidas

Ao final do curso o aluno estará apto a:

- ▲ Realizar aplicações de baseline de segurança, com foco em Hardening do sistema operacional linux;
- ▲ Colocar um servidor Linux em produção, utilizando boas práticas de segurança que também possibilitará conformidade com vários itens destacados na NBR ISO/IEC 27002;
- ▲ Implantar serviços de log centralizado, resolução de nomes, atualização de horário e autenticação para garantir a padronização e segurança de servidores Linux;
- ▲ Implementar um ecossistema com o objetivo de implantar, automatizar e gerir a configuração segura de máquinas Linux utilizando o Ansible.

Conhecimentos prévios

Para aproveitamento ideal do conteúdo é necessário ter conhecimento de administração de sistemas Linux e de segurança de redes ou feito os cursos de [Administração de Sistemas Linux](#) e [Segurança de Redes e Sistemas](#).

Investimento

▲ R\$ 1.920,00

Programa do curso

Sessão 1: Instalação e configurações iniciais

- 1) Criação de máquina virtual no Virtualbox
- 2) Instalação do Debian Linux
- 3) Ajustes pós-instalação
- 4) Configuração do LVM
- 5) Inserção de senha no bootloader
- 6) Clonando máquinas virtuais
- 7) Operações avançadas com LVM
- 8) Criptografia de partições

Sessão 2: Firewall e DNS

- 1) Topologia desta sessão
- 2) Criação da VM de firewall e DNS primário
- 3) Configuração inicial do firewall
- 4) Configuração do servidor DNS primário
- 5) Configuração do DNSSEC
- 6) Automatizando assinatura DNSSEC após alterações
- 7) Reconfiguração da VM debian-template
- 8) Criação da VM de DNS secundário
- 9) Configuração do DNS secundário

Sessão 3: Autenticação centralizada



esr.rnp.br



- 1) Topologia desta sessão
- 2) Configuração do servidor LDAP
- 3) Habilitando logs do LDAP
- 4) Edição de índices e permissões no LDAP
- 5) Adição de grupos e usuários no LDAP
- 6) Integração e teste do sistema de autenticação com LDAP
- 7) Configurando uma autoridade certificadora (CA) para o SSH
- 8) Configurando a SSH-CA no servidor LDAP
- 9) Automatizando a assinatura de chaves SSH de usuários
- 10) Configurando o template para funcionar com LDAP/SSH-CA
- 11) Ajuste das regras de firewall
- 12) Configurando um cliente Linux
- 13) Configurando o firewall para funcionar com LDAP/SSH-CA
- 14) Restringindo login por grupos e usuários
- 15) Restringindo logins SSH apenas via chaves assimétricas
- 16) Bloqueando tentativas de brute force contra o SSH

Sessão 4: Controles de segurança

- 1) Topologia desta sessão
- 2) Requisitos de senha na base LDAP
- 3) Busca de senhas fracas
- 4) Criação da VM do servidor de arquivos NFS
- 5) Ajuste das regras de firewall
- 6) Configuração do servidor de arquivos NFS e quotas de disco
- 7) Uso de ACLs localmente
- 8) Uso de ACLs via NFS
- 9) Controle granular de permissões via sudo

Sessão 5: Gestão de configuração

- 1) Topologia desta sessão
- 2) Instalação e configuração inicial do Ansible
- 3) Execução de comandos simples
- 4) Uso de roles no Ansible
- 5) Testando os controles do sudo
- 6) Controle da senha do usuário root
- 6) Versionamento de configuração com git

Sessão 6: Registro e correlacionamento de eventos

- 1) Topologia desta sessão
- 2) Criação da VM de gestão de logs
- 3) Ajuste das regras de firewall para o NTP
- 4) Configuração do NTP
- 5) Registro de comandos digitados com SnoopyLog
- 6) Instalação e configuração inicial do Graylog
- 7) Ajuste das regras de firewall para o Graylog
- 8) Visualizando logs de máquinas no Graylog
- 9) Autenticação centralizada via LDAP no Graylog
- 10) Configurando inputs customizados no Graylog

Sessão 7: Hardening de sistemas web

- 1) Topologia desta sessão
- 2) Configuração do servidor de banco de dados
- 4) Configuração do servidor web www1
- 5) Configuração automática do servidor web www2
- 6) Configuração do balanceador de carga

Sessão 8: Isolamento de processos e containerização



esr.rnp.br



- 1) Topologia desta sessão
- 2) Criação da VM docker1 e instalação
- 3) Criação da VM docker2
- 4) Trabalhando com containers
- 5) Distribuindo containers para um registry externo
- 6) Construindo serviços com o Docker
- 7) Operando com múltiplos membros no cluster
- 8) Adicionando novos serviços ao cluster
- 9) Configurando a persistência dos dados

Sessão 9: Criação de sistemas Linux customizados

- 1) Topologia desta sessão
- 2) Criação da VM de build
- 3) Construindo uma distribuição mínima
- 4) Utilizando um repositório local de pacotes
- 5) Construindo uma imagem mais... divertida?

Sessão 10: Módulos de segurança do kernel e auditoria

- 1) Topologia desta sessão
- 2) Criação do ambiente de segurança
- 3) Instalação do AppArmor
- 4) Criação de um perfil AppArmor para o servidor web Nginx
- 5) Auditoria automatizada de sistemas usando o OpenSCAP



esr.rnp.br

