alura | Para Empresas

Sugestão de Ementa

Linux Avançado

MINFIN - Angola

v2

Objetivo

Capacitar os participantes a administrarem redes e sistemas complexos utilizando Linux, implementando e gerenciando políticas de segurança para proteger redes e dados corporativos. Ao final do curso, os alunos estarão aptos a:

- Configurar e gerenciar redes Linux de maneira avançada
- Administrar sistemas Linux com eficiência
- Implementar medidas de segurança robustas para proteger a infraestrutura de TI

Público Alvo

Profissionais que já possuem nível intermediário de conhecimentos em Linux e desejam aprofundar suas habilidades em administração de redes, administração de sistemas e segurança de redes utilizando o sistema operacional Linux.

Carga Horária

- 60 Horas
    - 24 Horas de Teoria
    - 36 Horas de Prática

Ponto de Partida

- Conhecimentos intermediários e experiência prática em ambientes Linux
- Fundamentos de redes de computadores
- Conceitos básicos de segurança da informação

Ponto de Chegada

- Administração de Sistemas com Linux
- Administração de Redes com Linux
- Segurança de Redes com Linux
- Observabilidade no Linux com ELK Stack

Conteúdo Programático

| Módulo 1: Fundamentos de Linux (Nivelamento)

- Introdução ao Linux
  - História e evolução do Linux
  - Distribuições Linux (Debian, CentOS, Ubuntu, etc.)
- Estrutura de Diretórios do Linux
  - Sistema de arquivos Linux
  - Navegação no sistema de arquivos
- Comandos Básicos do Linux
  - Manipulação de arquivos e diretórios (ls, cp, mv, rm, mkdir, rmdir)
  - Visualização e edição de arquivos (cat, less, nano, vim)
  - Permissões de arquivos e diretórios (chmod, chown, chgrp)
- Gestão de Usuários e Grupos
  - Criação e gerenciamento de usuários
  - Configuração de grupos e permissões associadas
- Processos e Serviços
  - Gerenciamento de processos (ps, top, kill)
  - Introdução ao systemd (inicialização de serviços, logs)

|> Prática Módulo 1

| Módulo 2: Fundamentos de Redes e Segurança da Informação (Nivelamento)

- Conceitos Básicos de Redes
  - Modelos de referência OSI e TCP/IP
  - Endereçamento IP e Subnetting
  - Máscara de sub-rede e cálculo de sub-redes
  - Roteamento básico
- Conceitos Básicos de Segurança da Informação
  - Princípios de confidencialidade, integridade e disponibilidade
  - Introdução a políticas de segurança
  - Revisão de permissões de arquivos e diretórios
  - Revisão de controle de acesso baseado em usuário e grupo

|> Prática Módulo 2

| Módulo 3: Administração de Redes com Linux

- Configuração de Rede Avançada
  - Configuração de interfaces de rede
  - Endereçamento IP, subnetting e supernetting
  - Configuração de VLANs
- Ferramentas de Rede
  - Diagnóstico de rede (ping, traceroute)
  - Análise de conectividade (netstat, nmap, ifconfig/ip)
  - Transferência de arquivos (scp, sftp)
  - Monitoramento básico de rede (iftop, nload)
- Servidores de Rede
  - Configuração e administração de servidores DNS (BIND)
  - Resolução de nomes (hosts, resolv.conf)
  - Configuração e administração de servidores DHCP
  - Administração de servidores web (Apache, Nginx)
  - Servidores de e-mail (Postfix, Dovecot)
  - Compartilhamento de arquivos (Samba, NFS)
- Serviços de Rede e Protocolos
  - Configuração de serviços de diretório (LDAP)
  - Gerenciamento de usuários e grupos via rede
  - Configuração de serviços de tempo (NTP)
  - Monitoramento de rede e sistemas (Nagios, Zabbix)

|> Prática Módulo 3

| Módulo 4: Administração de Sistemas com Linux

- Gerenciamento de Pacotes e Atualizações
  - Sistemas de gerenciamento de pacotes (APT, YUM, DNF)
  - Atualizações automáticas e manuais
- Automação de Tarefas e Scripting
  - Introdução ao Bash scripting
  - Automação de tarefas administrativas com cron e systemd timers
  - Ferramentas de automação (Ansible)
- Gerenciamento de Serviços e Processos

    - Iniciação e controle de serviços com systemd
    - Monitoramento e gerenciamento de processos
    - Logs do sistema e análise de logs (rsyslog, journalctl)
- Virtualização e Contêineres
    - Introdução à virtualização com KVM e QEMU
    - Administração de contêineres com Docker
    - Orquestração de contêineres com Kubernetes

|> Prática Módulo 4

| Módulo 5: Segurança de Redes com Linux

- Ferramentas Básicas de Segurança
    - Configuração e uso de SSH
    - Backup e restauração de dados para recuperação de desastres (rsync, tar)
- Configuração de Firewalls
    - Introdução ao firewall básico (ufw)
    - Configuração e administração de iptables e nftables
    - Firewalls avançados (pfSense, Firewalld)
- Hardening de Sistemas
    - Técnicas de hardening para servidores Linux
    - Configuração de SELinux e AppArmor
    - Controle de acesso baseado em políticas
- Monitoramento e Resposta a Incidentes
    - Monitoramento de segurança e detecção de intrusões (Snort, Suricata)
    - Ferramentas de análise forense (Autopsy, Sleuth Kit)
    - Plano de resposta a incidentes e recuperação de desastres

|> Prática Módulo 5

| Módulo 6: Observabilidade no Linux

- Introdução à Observabilidade
    - Conceitos de observabilidade

    - Importância da observabilidade em ambientes de TI modernos
    - Três pilares da observabilidade: Logs, Métricas e Traces
- Elasticsearch
    - Introdução ao Elasticsearch
    - Instalação e configuração básica
    - Indexação e consulta de dados
    - Mapeamento de índices e tipos de dados
    - Gerenciamento de índices
- Logstash
    - Introdução ao Logstash
    - Instalação e configuração básica
    - Pipelines de Logstash (entrada, filtros e saída)
    - Integração com Elasticsearch
- Kibana
    - Introdução ao Kibana
    - Instalação e configuração básica
    - Navegando na interface do Kibana
    - Criação de dashboards
    - Visualização e análise de dados
    - Alertas e relatórios
- Integração do ELK Stack
    - Configuração completa do ELK Stack
    - Exemplos de coleta, análise e visualização de logs
    - Melhores práticas para escalabilidade e desempenho
- Ferramentas Complementares de Observabilidade
    - Introdução ao Prometheus e Grafana
    - Integração de métricas com Prometheus
    - Criação de dashboards no Grafana
    - Análise de logs em conjunto com métricas e traces

|> Prática Módulo 6