hackone

hackone PRO

Soluções de **infraestrutura** em TI em um único **ecossistema**.



hackone

Ensinar pela prática. Viabilizar objetivos. Conquistar resultados. Isso é Hackone PRO.

Na **Hackone PRO**, nosso compromisso é formar especialistas através de treinamentos de infraestrutura **100% online e práticos**, em um **programa completo e 360º**, além de benefícios exclusivos.



hackone

Você busca...

✔ Especialização nas principais áreas da infraestrutura de TI (redes e cibersegurança)?

✔ Acesso ao conhecimento dos melhores profissionais do mercado?

✔ Certificações essenciais dos principais fabricantes, como Fortinet e Cisco?

✔ Suporte total na transição de carreira para infraestrutura de TI?



hackone

O que você tem acesso na Hackone PRO.

Trilhas de Infraestrutura

Nossas trilhas envolvem as principais vertentes do mercado tech – Redes e Cibersegurança.

Descubra em qual delas você quer trilhar o seu caminho até a excelência.

Redes

Cibersegurança



hackone

Como a **Hackone** vai acelerar a sua jornada até o topo do mercado?



hackone

Redes

Aqui, você será preparado para criar uma base sólida em infraestrutura de redes a partir do zero, com o objetivo final de ser aprovado em algumas das certificações mais relevantes do mercado tech, como o CCNA e o CCNP.



Redes

Confira alguns treinamentos dessa trilha

CCNA

Conteúdo completo para a aprovação em uma das certificações mais relevantes do mercado, o CCNA, conhecida como a porta de entrada da Cisco.

ENARSI

Dividido em 4 módulos cobrindo desde troubleshooting em BGP, OSPF, EIGRP, como também soluções para VPN e MPLS, Troubleshooting da Segurança da Infra Estrutura.

MTCNA

Aprenda desde a configuração básica do RouterOS e toda a parte de roteamento até os detalhes sobre Layer 2 e implementação de rotas estáticas, e prepare-se para atuar com os conceitos básicos até os mais avançados.

ENCOR

Prepare-se para o ENCOR com treinamentos dinâmicos e práticos começando com arquitetura de rede, cobrindo diferentes modelos de arquitetura, entre Spine and Leaf, 2 TIER, 3 TIER, além de tecnologias de virtualização e um módulo completo sobre Automação de Redes.

Quer conferir a lista completa?

FALAR COM UM CONSULTOR

hackone

Redes

Confira alguns treinamentos dessa trilha

AWS Zero to Hero

Aqui, você vai começar a compreender a estrutura da Amazon Web Services (AWS), uma plataforma de serviços de computação em nuvem oferecida pela Amazon.

Azure Zero to Hero

Dividido em 4 módulos cobrindo desde troubleshooting em BGP, OSPF, EIGRP, como também soluções para VPN e MPLS, Troubleshooting da Segurança da Infra Estrutura.

MTCRE

Aqui, você terá acesso a um treinamento 100% focado na parte de roteamento, um dos tópicos mais relevantes para profissionais que estão no mercado com MikroTik.

Quer conferir a lista completa?

FALAR COM UM CONSULTOR

hackone

hackone

Cibersegurança

Prepare-se para passar no exame mais aguardado da sua carreira, aumentar ainda mais a sua régua salarial e se tornar um profissional certificado internacionalmente no mercado de cibersegurança.



Cibersegurança

Confira alguns treinamentos dessa trilha

FCP Network Security

Um módulo especial sobre a certificação que valida sua habilidade em proteger redes e aplicativos através do gerenciamento eficiente de produtos de segurança de rede Fortinet.

FCSS Network Security

Prepare-se para uma certificação que valida sua capacidade de projetar, administrar, monitorar e solucionar problemas de segurança de rede Fortinet.

Fortinac

O melhor conteúdo com introdução e configurações iniciais do FortiNAC, para você aprender a alcançar a visibilidade na rede, identificar e classificar Rogues, Logging, e muito mais!

CompTIA Security+

Uma preparação completa para a certificação CompTIA Security+, para você dominar seus conhecimentos em segurança cibernética através de tópicos como gerenciamento de riscos, criptografia, segurança de redes e muito mais!

Quer conferir a lista completa?

FALAR COM UM CONSULTOR

hackone

hackone

Confira os benefícios deste plano

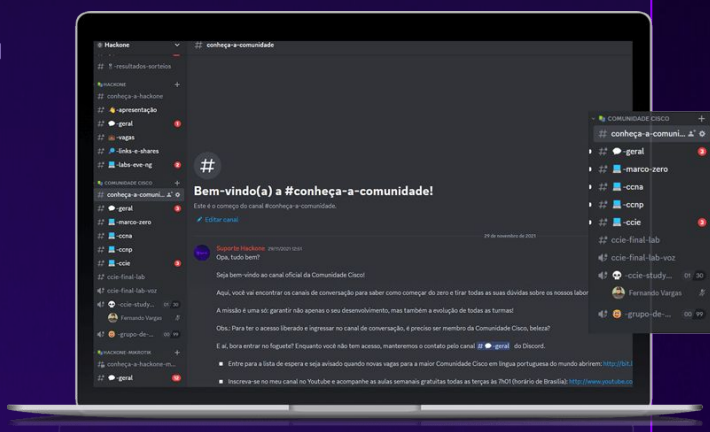
ACESSO A TODAS AS TRILHAS DE ESPECIALIZAÇÃO DA HACKONE

Você terá acesso liberado ao melhor conteúdo de redes e cibersegurança – treinamentos completos que, juntos, dão uma visão 360º para sua jornada no mercado tech.



COMUNIDADE NO DISCORD COM TODOS OS ALUNOS PRO

Networking é um dos alicerces fundamentais para uma carreira de sucesso. Aqui, você terá acesso ao nosso fórum exclusivo para desenvolver sua rede e receber nossos conteúdos e atualizações.

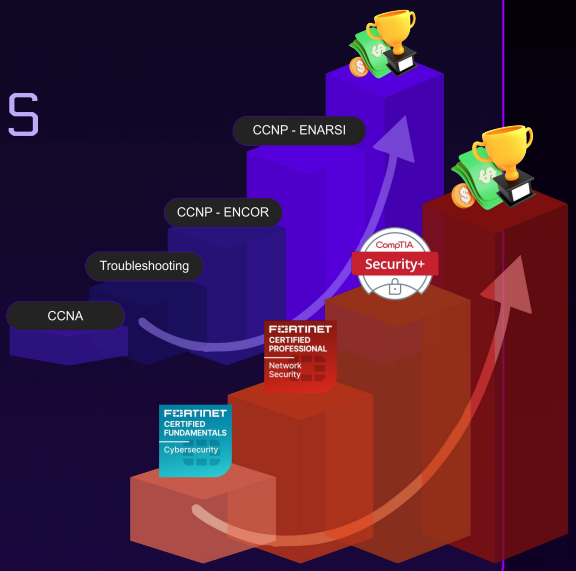


hackone

Benefícios **PRO**

PROGRAMAS DE ESPECIALIZAÇÃO EM REDES E CIBERSEGURANÇA

Você terá acesso a programas estruturados para **evoluir em 12 meses** com aulas que abrangem o que você realmente precisa aprender e colocar em prática em duas das áreas mais relevantes da atualidade.



TUTORIAS E ACOMPANHAMENTOS SEMANAIS AO VIVO

Toda semana realizamos uma masterclass com temas quentes da atualidade do mercado, ministrada por especialistas, além de formações ao vivo às quintas.

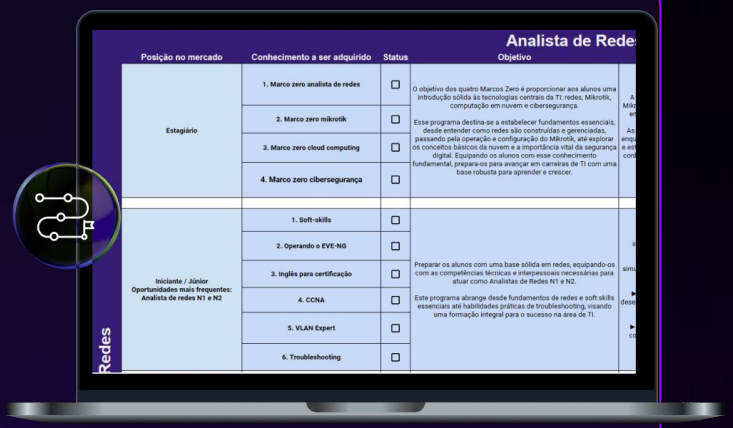


hackone

Benefícios **PRO**

MAPA DE CARREIRAS

Acesso a um plano de estudos especial, feito para guiar a jornada de forma eficiente e projetar a sua carreira para um futuro de excelência.



CERTIFICADO DE CONCLUSÃO

Após concluir cada treinamento, você receberá um certificado atestando que adquiriu novas habilidades.



BOOTCAMP HANDS ON AO VIVO

Participe de bootcamps especiais para assimilar ao máximo o conteúdo dos nossos treinamentos 100% na prática.



hackone

CURSOS

TRILHA REDES DE COMPUTADORES

- SOFT SKILLS
- MARCO ZERO
- INGLÊS PARA CERTIFICAÇÃO
- CCNA [200-301]
- INTELIGÊNCIA ARTIFICIAL PARA INFRA
- ENCOR [350-401]
- ENARSI [300-410]
- SD-WAN
- ACI
- TROUBLESHOOTING
- INTRODUÇÃO AO IS-IS
- THOUSAND EYES
- JUNIPER JNCIA
- DEVOPS - LINUX
- AWS ZERO TO HERO
- AZURE ZERO TO HERO
- BOOTCAMP - CLOUD ADVANCED NETWORKING
- INTRODUÇÃO AO BGP
- INTRODUÇÃO A MPLS E L3VPN
- DOMINANDO SERVICE PROVIDER
- AMBIENTE DE LABORATÓRIO
- IMPLEMENTANDO MULTICAST
- INTRODUÇÃO A QOS
- IMPLEMENTANDO IPV6
- EIGRP
- OSPF
- IMPLEMENTANDO WIFI
- FORMAÇÃO VIRTUALIZAÇÃO EM DATACENTER
- INTRODUÇÃO A WIFI E SITE SURVEY
- ZABBIX E GRAFANA
- BOOTCAMP COMPUTAÇÃO NA NUVEM DO ZERO À PRÁTICA
- EBOOK - 7 PASSOS PARA SER UM ARQUITETO CLOUD

hackone

CURSOS

SOFT SKILLS; MARCO ZERO; INGLÊS PARA CERTIFICAÇÃO

SOFT SKILLS

➡️ Desenvolvendo o jargão técnico e o comportamento correto de analistas de infraestrutura
➡️ Inteligência emocional
➡️ Entrevista de emprego para analista de redes: Como se preparar
➡️ Como conquistar uma promoção em 6 meses

DURAÇÃO: 5 HORAS

MARCO ZERO

➡️ A carreira em redes
➡️ Por onde começar?
➡️ Infraestrutura básica
➡️ Service Provider
➡️ Base de Redes - Plano de estudo
➡️ Prática: Laboratório, Bootcamp e Campo de Batalha.
➡️ Prática: Endereçamento DHCP e STATIC
➡️ Prática: Configurando a interface de um router
➡️ Lab de configuração básica do roteador

DURAÇÃO: 5 HORAS

INGLÊS PARA CERTIFICAÇÃO

➡️ Introdução ao vocabulário preparatório
➡️ Pronoun and Nouns
➡️ Verbs and Nouns
➡️ Adjective, Nouns, Adverb, Verb

DURAÇÃO: 4 HORAS

hackone

CURSO
CCNA [200-301]

MÓDULO 1: FUNDAMENTOS DE REDES
MÓDULO 2: NETWORK ACCESS
MÓDULO 3: CONECTIVIDADE IP
MÓDULO 4: IP SERVICES
MÓDULO 5: SECURITY FUNDAMENTALS
MÓDULO 6: AUTOMATION AND PROGRAMMABILITY
BÔNUS: BOOTCAMP CCNA
DURAÇÃO: 77 HORAS

MÓDULO 1: FUNDAMENTOS DE REDES

- ➡️ Como tudo começou
- ➡️ Componentes de Rede
- ➡️ Impacto nos Componentes de Infra Estrutura
- ➡️ Camada OSI
- ➡️ Topologia de Rede
- ➡️ PoE
- ➡️ Padrões, CSMA-CD e issues identificados na camada física
- ➡️ IPv4, TCP e UDP
- ➡️ Binário & Decimal
- ➡️ Classes de IP e Máscara
- ➡️ Configuração e Verificação
- ➡️ Subnetting em IPv4 - Parte 1
- ➡️ VLSM e CIDR
- ➡️ IPv4 Sumarização
- ➡️ Endereço público, privado e reservado
- ➡️ IPv6 - A história e representação de endereço
- ➡️ IPv4 e IPv6 Comparando cabeçalhos
- ➡️ IPv6 Interface-ID
- ➡️ IPv6 - Tipos de endereço
- ➡️ Tutorial para verificação da configuração de IP no Windows, MAC e Linux
- ➡️ SSID e Criptografia
- ➡️ RF Power e DB
- ➡️ Virtualização
- ➡️ Servidor de laboratório
- ➡️ Conceitos de Switch e Ethernet - Parte 1
- ➡️ Introdução ao IOS - Parte 1
- ➡️ Configurações básicas do Switch

hackone

CURSO
CCNA [200-301]

MÓDULO 2: NETWORK ACCESS

- ➡️ Entendendo e configurando Vlans
- ➡️ Entendendo e configurando Trunk
- ➡️ Vlan Trunk Protocol [VTP] e Vlan Nativa
- ➡️ DTP - Dynamic Trunk Protocol
- ➡️ CDP e LLDP - Discovery Protocols
- ➡️ Layer 2 Etherchannel
- ➡️ Layer 3 Etherchannel
- ➡️ Por que usar Spanning-Tree
- ➡️ Como o protocolo funciona
- ➡️ STP Port States e Cálculo do Root Bridge
- ➡️ Implementando Spanning-Tree
- ➡️ Mecanismos de proteção ao BPDU
- ➡️ Rapid Spanning-Tree Protocol RSTP
- ➡️ Wireless - Tipos de Implementação
- ➡️ Wireless - Tipos de AP e Antenas
- ➡️ WLAN - Interfaces e Portas
- ➡️ Acessando WLC via Service Port
- ➡️ Acessando a WLC via SSH, TELNET, HTTP e HTTPS
- ➡️ Configurando WLAN

MÓDULO 3: CONECTIVIDADE IP

- ➡️ O que é roteamento?
- ➡️ IGP e EGP
- ➡️ Classificando Roteamento Dinâmico
- ➡️ Implementando IPv6
- ➡️ ARP em IPv6
- ➡️ Rota Estática
- ➡️ Rota Estática Floating
- ➡️ Rota Default
- ➡️ Rota Estática em IPv6
- ➡️ Router on Sticky
- ➡️ SVI
- ➡️ Introdução ao OSPF
- ➡️ Tipos de pacotes e adjacência
- ➡️ Eleição de DR/BDR e Router-ID
- ➡️ OSPF Network Types e Tabelas
- ➡️ Métrica do OSPF :: Custo
- ➡️ Implementando OSPF
- ➡️ Implementando OSPFv3 :: Bônus
- ➡️ HSRP

hackone

CURSO
CCNA [200-301]

MÓDULO 4: IP SERVICES

- ➡️ Introdução a NAT
- ➡️ NAT Estático
- ➡️ NAT Dinâmico
- ➡️ PAT - Port Address Translation
- ➡️ NTP - Introdução e Configuração
- ➡️ DHCP
- ➡️ DNS
- ➡️ SNMP
- ➡️ Entendendo Syslog
- ➡️ DHCP Relay
- ➡️ Introdução a QOS
- ➡️ Classificação e Marcação
- ➡️ Congestion Avoidance
- ➡️ Congestion Management
- ➡️ Congestion Avoidance - Pre-Emptive Drops
- ➡️ FTP e TFTP

MÓDULO 5: SECURITY FUNDAMENTALS

- ➡️ Conceitos Importantes de Segurança
- ➡️ Elementos e Programas de Segurança
- ➡️ Segurança Básica da Rede
- ➡️ SSH vs Telnet
- ➡️ Controlando Solicitações SSH e Telnet
- ➡️ Passwords
- ➡️ Introdução à VPN
- ➡️ GRE
- ➡️ DMVPN
- ➡️ Introdução a Access-List
- ➡️ Standard Access-List
- ➡️ Extended Access-List
- ➡️ ACL Nomeada [NAMED]
- ➡️ IPv6 ACL
- ➡️ Introdução a DHCP Snooping
- ➡️ Implementando DHCP Snooping e Dynamic Arp Inspection
- ➡️ Port-Security
- ➡️ AAA
- ➡️ WPA, WPA2 e WPA3
- ➡️ Configurando WLAN usando WPA2 + PSK

hackone

CURSO
CCNA [200-301]

MÓDULO 6: AUTOMATION AND PROGRAMMABILITY

- ➡️ Como a automação impacta a gerência da rede
- ➡️ Traditional Network e Controller Based
- ➡️ Introdução a SDN - Control Plane e Data Plane
- ➡️ Componentes de SDN - North and South Bound API
- ➡️ Underlay, Overlay e Fabric
- ➡️ Comparando DNA Networks com Traditional Networks
- ➡️ Material de apoio e links úteis
- ➡️ Preparando o ambiente de Laboratório
- ➡️ Entendendo esse laboratório
- ➡️ Introdução a Python
- ➡️ Usando Loop For
- ➡️ Usando Loops em Python
- ➡️ Usando Loop e Arquivos externos para configurar múltiplos Switches
- ➡️ Introdução a NetMiko
- ➡️ NetMiko e Loops
- ➡️ Configurando o Switch a partir de um arquivo
- ➡️ WHAT IS AN API
- ➡️ XML e JSON Data Encoding
- ➡️ Chef Puppet Ansible and SaltStack
- ➡️ JSON Encoded Data
- ➡️ Fundamentos de rede
- ➡️ Network Access
- ➡️ Conectividade IP
- ➡️ IP Services
- ➡️ Fundamentos de segurança
- ➡️ Automação de rede

BÔNUS: BOOTCAMP CCNA

- ➡️ Workbook e topologia
- ➡️ Como construir uma rede a partir do zero
- ➡️ Habilitando Roteamento
- ➡️ Resolvendo incidentes na rede
- ➡️ Construindo o ambiente de rede em seu laboratório
- ➡️ O passo a passo para habilitar o roteamento de rede
- ➡️ Configurando sites remotos para acesso à internet
- ➡️ Habilitando segurança na rede e fazendo troubleshooting
- ➡️ Preparando o design da rede e o ambiente de laboratório
- ➡️ Configurações iniciais e acesso remoto
- ➡️ Configuração da lan e roteamento
- ➡️ Habilitando acesso à internet (WAN) e implementando segurança na rede
- ➡️ Troubleshooting avançado

CURSOS

INTELIGÊNCIA ARTIFICIAL PARA INFRAESTRUTURA

INTELIGÊNCIA ARTIFICIAL PARA INFRAESTRUTURA

- ➡️ Overview do treinamento e pré requisitos
- ➡️ IA para Infraestrutura
- ➡️ Introdução a Machine Learning e RL
- ➡️ Q-learning
- ➡️ Aplicando Q-learning em Infraestrutura
- ➡️ Exemplos e uso de caso

DURAÇÃO: 1 HORA

hackone

hackone

CURSO
ENCOR [350-401]

MÓDULO 1: ARCHITECTURE
MÓDULO 2: VIRTUALIZATION
MÓDULO 3: INFRASTRUCTURE
MÓDULO 4: NETWORK ASSURANCE
MÓDULO 5: SECURITY
MÓDULO 6: AUTOMATION
DURAÇÃO: 68 HORAS

MÓDULO 1: ARCHITECTURE

- Introduction, summary and slides
- Enterprise network design
- Tier2 Tier3 and Fabric Capacity Planning
- High availability techniques
- Deployment models
- Location services in a WLAN design
- On-premises and cloud infrastructure deployments
- Principles of cisco SD-WAN solution
- SD-WAN Control and data plane
- WAN vs. SD-WAN solution
- Control plane and data plane elements
- Campus interoperating with SD-ACCESS
- QOS components
- QoS with DNA Center
- PROCESS and CEF
- CAM AND TCAM
- FIB vs. RIB

MÓDULO 2: VIRTUALIZATION

- Hypervisor type 1 and 2
- Virtual switching
- VRF
- Implementing VRF - LAB
- GRE
- MGRE - DMVPN
- Implementing GRE and MGRE - LAB
- IPSEC
- Implementing IPSEC - LAB
- Servidor de laboratório :: Hackone
- Network virtualization
- VXLAN overview
- VXLan Bum traffic
- VXLAN - Data plane and control plane learning
- Implementing VXLAN - LAB
- LISP overview
- LISP variants
- SD-ACCESS integration with virtualization

hackone

CURSO
CCNA [200-301]

MÓDULO 3: INFRASTRUCTURE

- Trunk fundamentals
- Troubleshoot static and dynamic 802.1q trunking protocols
- Etherchannel fundamentals
- Troubleshoot static and dynamic etherchannels
- Introduction to STP
- Configure and verify common spanning tree protocols RSTP AND MST
- Introduction to IGP protocols
- EIGRP - Building the EIGRP topology table
- EIGRP - Building the ip routing table
- EIGRP - Optimizing EIGRP convergence
- EIGRP - Route filtering
- EIGRP Route summarization
- EIGRP - Default routes
- OSPF - OSPF Review
- OSPF - LSAS and the OSPF link-state database
- OSPF - The database exchange process
- OSPF - Choosing the best internal OSPF routes
- OSPF - Route filtering
- OSPF - Route summarization
- OSPF - Default routes and STUB areas
- Compare routing concepts of EIGRP and OSPF
- Border gateway protocol BGP
- Verifying the BGP table
- BGP Path attributes and best-path algorithm
- Managing BGP attributes weight and local preference
- Network time protocol NTP
- NAT AND PAT
- Multicast protocols

hackone

CURSO
CCNA [200-301]

MÓDULO 4: NETWORK ASSURANCE

- ➡ Debugs and conditional debugs
- ➡ Trace route and ping
- ➡ SNMP
- ➡ Configure and verify device monitoring using SYLOG
- ➡ Netflow and flexible netflow
- ➡ SPAN RSPAN and ERSPAN
- ➡ IP SLA
- ➡ DNA Workflows
- ➡ What is an API
- ➡ Data Model - YANG
- ➡ NETCONF
- ➡ RESTCONF

MÓDULO 5: SECURITY

- ➡ Lines and password protection
- ➡ Authentication and authorization using AAA
- ➡ Introduction to ACLS, PORT ACL, VLAN ACL, IP ACL
- ➡ Port ACCESS-LIST
- ➡ VLAN ACCESS-LIST
- ➡ COPP
- ➡ OAuth - RestAPI Security
- ➡ Configure WLAN EAP
- ➡ Configure WLAN PSK and WEBAUTH
- ➡ Threat Defense
- ➡ ENDPOINT Security
- ➡ Next generation Firewall
- ➡ TrustSec MACsec
- ➡ Network access control with 802.1X MAB and WebAuth

MÓDULO 5: SECURITY

- ➡ Preparando o ambiente de Laboratório
- ➡ Entendendo esse laboratório
- ➡ Introdução a Python
- ➡ Usando Loop For
- ➡ Usando Loops em Python
- ➡ Usando Loop e Arquivos externos para configurar múltiplos Switches
- ➡ Introdução a NetMiko
- ➡ NetMiko e Loops
- ➡ Configurando o Switch a partir de um arquivo
- ➡ NETCONF - Get and push config
- ➡ JSON Encoded data
- ➡ YANG
- ➡ APIs for Cisco DNA Center and vManage
- ➡ Rest api response codes and results in payload using Cisco DNA
- ➡ EEM APPLET
- ➡ compare agent vs. agentless orchestration tools such as Chef Puppet Ansible and SaltStack

hackone

CURSO
ENARSI [300-410]

MÓDULO 1: LAYER 3 TECHNOLOGIES
MÓDULO 2: VPN TECHNOLOGIES
MÓDULO 3: INFRASTRUCTURE SECURITY
MÓDULO 4: INFRASTRUCTURE SERVICES
DURAÇÃO: 64 HORAS

MÓDULO 1: LAYER 3 TECHNOLOGIES

- Troubleshoot administrative distance
- Route-map
- TAG - Loop prevention mechanisms
- Split-Horizon Poizon e Poizon Reverse
- Troubleshooting Redistribution
- Troubleshoot manual and auto-summarization
- PBR
- VRF LITE
- Bidirectional Forward Detection BFD
- EIGRP - Address family IPv4 and IPv6
- EIGRP Neighbors Adjacency Troubleshooting
- EIGRP Neighbors Authentication Troubleshooting
- EIGRP Loop Free - Feasible Condition
- Stuck in Active and EIGRP Stub
- EIGRP Load Balance and Metrics
- OSPF Address-family IPv4 and IPv6
- OSPF Neighbor adjacency
- Neighbor OSPFv2 authentication
- Neighbor OSPFv3 authentication
- OSPF Network Types
- OSPF Areas
- Internal Router Backbone Router ASBR and ABR
- OSPF Virtual Link
- OSPF Path Preference

hackone

CURSO
ENARSI [300-410]

MÓDULO 2: VPN TECHNOLOGIES

- ➡️ MPLS
- ➡️ DMVPN - Phase 1
- ➡️ DMVPN - Phase 2 e 3
- ➡️ DMVPN - IPSEC

MÓDULO 3: INFRASTRUCTURE SECURITY

- ➡️ Troubleshoot e configuration AAA
- ➡️ O poder da Access-List
- ➡️ IPv6 Traffic filter
- ➡️ Unicast Reverse Path Forwarding uRPF
- ➡️ CoPP
- ➡️ Describe IPv6 First Hop Security Features

MÓDULO 4: INFRASTRUCTURE SERVICES

- ➡️ Console VTY HTTP HTTPS SCP FTP and TFTP
- ➡️ SNMP v2c e V3
- ➡️ Syslog debug e conditional debug
- ➡️ DHCP em IPv4
- ➡️ DHCPv6
- ➡️ Understanding and Troubleshooting IP SLA
- ➡️ Troubleshoot NetFlow v5 v9 flexible NetFlow
- ➡️ Troubleshooting Basics with DNA

hackone

CURSO
SD-WAN

MÓDULO 1: Laboratório e Bring UP Process
MÓDULO 2: vManage e Configuração via Feature Template
MÓDULO 3: OMP Overlay Management Protocol & TLOC
MÓDULO 4: Viptela Smart Policy
MÓDULO 5: Design Considerations
DURAÇÃO: 25 HORAS

MÓDULO 1: Laboratório e Bring UP Process

- ➡️ Entendendo o Laboratório
- ➡️ Montando o seu ambiente de Laboratório
- ➡️ Control Plane e Data Plane Devices
- ➡️ Bring UP Controllers
- ➡️ Bring UP vEdges
- ➡️ Revisão dos Steps Iniciais

MÓDULO 2: vManage e Configuração via Feature Template

- ➡️ Introdução a Feature e Device Template
- ➡️ Configurando Feature Template
- ➡️ Feature Template - Service VPN
- ➡️ Habilitando BGP como Underlay Transport
- ➡️ Revisão device e feature templates

MÓDULO 3: OMP Overlay Management Protocol & TLOC

- ➡️ OMP e TLOC
- ➡️ OMP - Entendendo o Protocolo
- ➡️ OMP - Routes e verificação
- ➡️ OMP - Tabela de Roteamento e Seleção de Caminhos
- ➡️ OMP - Path Selection
- ➡️ [TLOC EXTENSION] - Conectando sites com 2 Vedges na topologia SD-WAN

hackone

CURSO
SD-WAN

MÓDULO 4: Viptela Smart Policy

➡️ Introdução AAR
➡️ Preparando o vSmart
➡️ Introdução a SD-WAN Policy Template
➡️ Criando Control Policy Lists
➡️ AAR usando Port e Protocol Based
➡️ AAR usando Deep Packet Inspection
➡️ Control Policy - Routing Preference
➡️ Filtro de Rotas Usando Prefix-List

MÓDULO 5: Design Considerations

➡️ Topologia e Design SD-WAN

hackone

CURSO
ACI

MÓDULO 1: Introdução ao ACI
MÓDULO 2: Inicializando uma fabric do ACI
MÓDULO 3: Descrevendo e configurando componentes
MÓDULO 4: Conectividade dentro do ACI
MÓDULO 5: Conectividade externa ao ACI
MÓDULO 6: Conectividade entre DataCenter
MÓDULO 7: Automatizando Rotinas no ACI
MÓDULO 8: Monitorando e operando o ACI
DURAÇÃO: 16 HORAS

MÓDULO 1: Introdução ao ACI

- ➡️ Arquitetura Spine/Leaf
- ➡️ Introdutório a VxLAN
- ➡️ CIMC
- ➡️ APIC
- ➡️ LAB - APIC
- ➡️ Como simular um ambiente ACI

MÓDULO 2: Inicializando uma fabric do ACI

- ➡️ Configuração inicial APIC
- ➡️ Processo de descobrimento da Fabric
- ➡️ Registro dos Spines e Leafs
- ➡️ LAB - Verificando o cluster da APIC

MÓDULO 3: Descrevendo e configurando componentes

- ➡️ Tenant, VRF e Bridge Domain
- ➡️ Application Profile e Endpoint Groups
- ➡️ Contratos e filtros
- ➡️ Fabric Domain e VLAN Pools
- ➡️ Interface Policy Group, Profiles e Policies

MÓDULO 4: Conectividade dentro do ACI

- ➡️ Processo de aprendizagem de Endpoint
- ➡️ Tipos de Endpoints
- ➡️ Analisando a tabela de endpoints
- ➡️ Tabela Coop

hackone

CURSO
ACI

MÓDULO 5: Conectividade externa ao ACI

- ➡️ L3OUT com BGP
- ➡️ L3OUT com OSPF
- ➡️ L2OUT

MÓDULO 6: Conectividade entre DataCenter

- ➡️ Single-pod 7.2 - Multi-pod e IPN
- ➡️ Multi site e ISN

MÓDULO 7: Automatizando Rotinas no ACI

- ➡️ ACI Toolkit
- ➡️ API inspector
- ➡️ Ansible e ACI

MÓDULO 8: Monitorando e operando o ACI

- ➡️ Acesso Out-of-Band (OOB) e In-band
- ➡️ SNMP e Syslog
- ➡️ Login e autenticação
- ➡️ Backup e rollback
- ➡️ ACI Tech-support
- ➡️ Faults, Health Score e Audit

CURSOS

TROUBLESHOOTING; INTRODUÇÃO AO IS-IS

TROUBLESHOOTING

➡️ Instruções para uso do LAB e material de apoio
➡️ Metodologia do CCIE Lucas Palma de Troubleshooting
➡️ Entendendo topologias
➡️ Troubleshooting - Resolvendo incidentes em Layer 3 - OSPF BGP e HRSP
➡️ Resolvendo incidentes - L2 e L3
➡️ Troubleshooting - DHCP DORA e Roteamento
➡️ Resolvendo Incidentes - Routing
➡️ Troubleshooting - Finalizando o work book

DURAÇÃO: 12 HORAS

INTRODUÇÃO AO IS-IS

➡️ Introdução ao protocolo IS-IS
➡️ Configurando IS-IS Single Level
➡️ Configurando IS-IS Multi Level

DURAÇÃO: 3 HORAS

hackone

hackone

CURSO
THOUSAND EYES

MÓDULO 1: Aulas Introdutórias
MÓDULO 2: O que é Thousand Eyes?
MÓDULO 3: Componentes da Solução
MÓDULO 4: Como criar testes no Thousand Eyes
MÓDULO 5: Interpretando os diferentes tipos de teste
MÓDULO 6: Monitoria da WAN e Internet
MÓDULO 7: Dimensionando Thousand Eyes
MÓDULO 8: Melhores práticas para implementação da solução
DURAÇÃO: 13 HORAS

MÓDULO 1: Aulas Introdutórias

➡️ Overview sobre Thousand Eyes (A inteligência da solução)
➡️ Principais desafios relacionados a visibilidade
➡️ Principais aspectos da solução
➡️ Como conseguir acesso ao Thousand Eyes?

MÓDULO 2: O que é Thousand Eyes?

➡️ O que é Thousand Eyes (Cloud Agent, Enterprise & Endpoint Agent)

MÓDULO 3: Componentes da Solução

➡️ Como implementar Enterprise Agents e suas características
➡️ Cloud Agents como eles funcionam?
➡️ Como instalar e começar usar os Endpoint Agents

MÓDULO 4: Como criar testes no Thousand Eyes

➡️ Como criar testes para Enterprise e Cloud Agents
➡️ Como criar testes para Endpoint Agents?
➡️ Quais são as métricas que cada tipo de teste entrega?

hackone

CURSO
THOUSAND EYES

MÓDULO 5: Interpretando os diferentes tipos de teste

➡️ Dragging Interpretando os diferentes tipos de teste
➡️ HTTP Server (Problemas na migração para nuvem) - Empresa William Hill
➡️ Serviços indisponíveis (Problemas na WAN) - Empresa LAS
➡️ Problemas de roteamento (Aplicações indisponíveis) - Azure
➡️ Testes de transações - script O365
➡️ Teste de transações - script com problemas OneDrive
➡️ Problemas com DNS - DNS Trace
➡️ Analisando Overlay e Underlay com problemas - SD-WAN
➡️ Endpoint Agent - Problemas com domínios, Redes e aplicações Office 365 Webex
➡️ Criando Shared Links
➡️ Criação de alertas

MÓDULO 6: Monitoria da WAN e Internet

➡️ Internet Insights (Problemas na Internet)

MÓDULO 7: Dimensionando Thousand Eyes

➡️ Como dimensionar a solução corretamente

MÓDULO 8: Melhores práticas para implementação da solução

➡️ Guia geral das melhores práticas

hackone

CURSO
INTRODUÇÃO AO BGP

MÓDULO 1: Introdução ao BGP e BGP Peering
MÓDULO 2: BGP - Path Vector e Seleção de rotas
MÓDULO 3: Route-Reflector
MÓDULO 4: Troubleshooting
DURAÇÃO: 16 HORAS

MÓDULO 1: Introdução ao BGP e BGP Peering

➡️ Entendendo e Operando o LDP Label Distribution Protocol
➡️ Labels e TTL

MÓDULO 2: BGP - Path Vector e Seleção de rotas

➡️ Monitorando e Troubleshooting MPLS LDP

MÓDULO 3: Route-Reflector

➡️ Introdução a MPLS L3VPN
➡️ BGP VPNv4

MÓDULO 4: Troubleshooting

➡️ MPLS L3VPN - Roteamento entre PE e CE
➡️ Roteamento PE-CE usando OSPF
➡️ Roteamento PE-CE usando eBGP

hackone

CURSO
INTRODUÇÃO A MPLS E L3VPN

MÓDULO 1: LDP e Labels
MÓDULO 2: Troubleshooting
MÓDULO 3: L3VPN
MÓDULO 4: Roteamento PE-CE
DURAÇÃO: 16 HORAS

MÓDULO 1: LDP e Labels

- ➡️ Mensagens, States e Sessão do BGP
- ➡️ BGP Address-Families
- ➡️ BGP Peer-Group
- ➡️ Processando o Next-hop e Tabela do BGP

MÓDULO 2: Troubleshooting

- ➡️ Algoritmo do BGP e Escolha de Caminho - Weight, Local Preference, AS Path, MED
- ➡️ Aplicando filtro de rotas no BGP

MÓDULO 3: L3VPN

- ➡️ Single Route Reflector Topology

MÓDULO 4: Roteamento PE-CE

- ➡️ Melhores práticas de troubleshooting no BGP

hackone

CURSOS

DOMINANDO SERVICE PROVIDER; IMPLEMENTANDO MULTICAST; INTRODUÇÃO A QOS; IMPLEMENTANDO IPV6

DOMINANDO SERVICE PROVIDER

➡️ Implementando os protocolos essenciais de uma operadora de internet e MPLS
➡️ Dominando MPLS e L3VPN na prática
➡️ Preparando a infraestrutura do backbone
➡️ BGP criando uma operadora de internet do absoluto zero
➡️ Configurando acesso à rede 5G e resolvendo incidentes

DURAÇÃO: 6 HORAS

IMPLEMENTANDO MULTICAST

➡️ Introdução ao Protocolo Multicast
➡️ Como Multicast funciona em Layer 2 [IGMP]
➡️ Configurando Multicast em Layer 3 usando o protocolo PIM
➡️ Como usar Multicast em sua empresa

DURAÇÃO: 8 HORAS

INTRODUÇÃO A QOS

➡️ Aprenda QoS a partir do zero
➡️ QoS - Classificando o tráfego
➡️ QoS fim a fim usando Policy e Shaping

DURAÇÃO: 8 HORAS

IMPLEMENTANDO IPV6

➡️ Introdução ao protocolo IPv6
➡️ Rota Estática em IPv6 e RIPng
➡️ Implementando EIGRP em IPv6
➡️ Implementando OSPFv3

DURAÇÃO: 6 HORAS

hackone

CURSOS
EIGRP

EIGRP

- EIGRP Introdução e Configuração
- EIGRP Building the EIGRP topology table
- EIGRP Optimizing EIGRP convergence
- EIGRP Address family IPv4 and IPv6
- Implementando EIGRP em IPv6
- EIGRP Neighbors Adjacency Troubleshooting
- EIGRP Neighbors Authentication Troubleshooting
- EIGRP Loop Free - Feasible Condition
- Stuck in Active and EIGRP Stub
- EIGRP Load Balance and Metrics
- EIGRP Load Balance e Sumarização
- EIGRP Building the IP routing table
- EIGRP Route filtering
- EIGRP Route summarization
- EIGRP Default routes
- Compare routing concepts of EIGRP and OSPF
- EIGRP Optimizing EIGRP convergence
- EIGRP Address family IPv4 and IPv6
- Implementando EIGRP em IPv6
- EIGRP Neighbors Adjacency Troubleshooting
- EIGRP Neighbors Authentication Troubleshooting
- EIGRP Loop Free - Feasible Condition
- Stuck in Active and EIGRP Stub
- EIGRP Load Balance and Metrics
- EIGRP Load Balance e Sumarização
- EIGRP Building the IP routing table
- EIGRP Route filtering
- EIGRP Route summarization
- EIGRP Default routes
- Compare routing concepts of EIGRP and OSPF

DURAÇÃO: 10 HORAS

hackone

CURSOS

OSPF

OSPF

- ➡️ OSPF Path Preference
- ➡️ OSPF - Choosing the best internal OSPF routes
- ➡️ OSPF - The database exchange process
- ➡️ OSPF - Route filtering
- ➡️ OSPF - Route summarization
- ➡️ Implementando OSPFv3
- ➡️ Implementando OSPFv3 :: Bônus
- ➡️ Neighbor OSPFv3 authentication
- ➡️ Configurando OSPF a partir do zero
- ➡️ Configurando OSPF - Tipos de interface e eleição de DR e BDR
- ➡️ Configurando OSPF - Tipos de área
- ➡️ OSPF - LSAs and the OSPF link-state database
- ➡️ OSPF Network Types e Tabelas
- ➡️ Fazendo Troubleshooting no OSPF
- ➡️ OSPF Address-family IPv4 and IPv6
- ➡️ OSPF Neighbor adjacency
- ➡️ Neighbor OSPFv2 authentication
- ➡️ OSPF Virtual Link
- ➡️ Métrica do OSPF :: Custo

DURAÇÃO: 11 HORAS

hackone

CURSO

FORMAÇÃO VIRTUALIZAÇÃO EM DATACENTER

MÓDULO 1: Introdução ao vSphere and the Software-Defined Data Center
MÓDULO 2: vCenter Server
MÓDULO 3: Virtual Network
MÓDULO 4: Virtual Storage
MÓDULO 5: Criação de máquina virtual
MÓDULO 6: Gerenciamento de máquina virtual
MÓDULO 7: Gerenciamento de recursos e monitoramento
MÓDULO 8: vSphere HA
MÓDULO 9: vSphere DRS
MÓDULO 10: vSphere Life Cycle Manager/Update Manager
DURAÇÃO: 14 HORAS

MÓDULO 1: Introdução ao vSphere and the Software-Defined Data Center

- ➡️ Overview Software-Defined Data Center
- ➡️ Overview - ESXi
- ➡️ Preparação do laboratório
- ➡️ Instalar ESXi
- ➡️ Configuração inicial do ESXi

MÓDULO 2: vCenter Server

- ➡️ Arquitetura e função do vCenter
- ➡️ Instalação do vCenter
- ➡️ vSphere Client na visão geral - Inventário, pastas, configurações gerais
- ➡️ Funções e permissões - Autenticação e integração com AD

MÓDULO 3: Virtual Network

- ➡️ Introdução ao vSphere Standard Switches
- ➡️ Introdução ao vSphere Distributed Virtual Switches

hackone

CURSO
FORMAÇÃO VIRTUALIZAÇÃO EM DATACENTER

MÓDULO 4: Virtual Storage

- ➡️ Conceito geral de storage e Fiber Channel
- ➡️ iSCSI Storage
- ➡️ VMFS Datastore - conceito, criação e expansão
- ➡️ NFS Datastore, vSAN e vVOL Datastore

MÓDULO 5: Criação de máquina virtual

- ➡️ Conceito de máquina virtual e composição de arquivos
- ➡️ Criando uma máquina virtual

MÓDULO 6: Gerenciamento de máquina virtual

- ➡️ Templates e Clones - criação, deploy e modificação
- ➡️ Content Libraries
- ➡️ Migração de máquina virtual (vMotion e Storage vMotion)
- ➡️ VM Snapshot

MÓDULO 7: Gerenciamento de recursos e monitoramento

- ➡️ Conceito de Virtual CPU e Memória
- ➡️ Limit, reserva e shares
- ➡️ Resource Pools e vAPP
- ➡️ Monitoramento de uso de recursos
- ➡️ Alarmes

MÓDULO 8: vSphere HA

- ➡️ vSphere HA - Introdução e configuração

hackone

CURSO

FORMAÇÃO VIRTUALIZAÇÃO EM DATACENTER

MÓDULO 9: vSphere DRS

➡️ vSphere DRS - Introdução, configuração e affinity/anti-affinity rules
➡️ vSphere DRS - Introdução e configuração

MÓDULO 10: vSphere Life Cycle Manager / Update Manager

➡️ vSphere Life Cycle Manager / Update Manager - Introdução e configuração
➡️ Backing Up and Restoring vCenter Server Appliance, DVS e ESXi

hackone

CURSO

INTRODUÇÃO A WIFI E SITE SURVEY

MÓDULO 1: Visão Geral do 802.11
MÓDULO 2: Fundamentos da Configuração de WLAN
MÓDULO 3: Princípios de Segurança em WLAN
MÓDULO 4: Etapas de implantação
MÓDULO 5: Solução Wireless Cisco
MÓDULO 6: WLC 3504
MÓDULO 7: WLC 9800
MÓDULO 8: WLC 9800 Cloud
MÓDULO 9: WLCs EVE
MÓDULO 10: Access-point autonomo
MÓDULO 11: Tunning Wifi
MÓDULO 12: Redundância
MÓDULO 13: Introdução Pentest Wifi
DURAÇÃO: 10 HORAS

MÓDULO 1: Visão Geral do 802.11

- ➡️ Conceitos Básicos
- ➡️ Estrutura das Camadas Física e de Enlace
- ➡️ Características Físicas dos Sinais Sem Fio
- ➡️ Características da Camada de Enlace
- ➡️ Frequências de Rádio e Canais Utilizados
- ➡️ Métodos de Modulação de Sinais
- ➡️ Relação entre Taxa de Dados, Intensidade e Força de Sinal
- ➡️ Padrão 802.11b
- ➡️ Padrão 802.11a
- ➡️ Padrão 802.11g
- ➡️ Padrão 802.11n
- ➡️ Tecnologia MIMO no 802.11n
- ➡️ Agregação de Canais no 802.11n
- ➡️ Padrão 802.11ac
- ➡️ Padrão 802.11ax
- ➡️ Padrão 802.11be
- ➡️ Comparativo entre os Padrões 802.11a/b/g/n/ac/ax/be
- ➡️ Relação entre Taxa de Dados, Intensidade e Força de Sinal
- ➡️ Questões de fixação
- ➡️ InSSIDEr

hackone

CURSO
INTRODUÇÃO A WIFI E SITE SURVEY

MÓDULO 2: Fundamentos da Configuração de WLAN

- ➡️ Configuração de Rede Ad Hoc
- ➡️ Configuração em Modo Infraestrutura
- ➡️ Configuração em Modo Bridge
- ➡️ Definição de BSS e BSSID
- ➡️ Definição de ESS e ESSID
- ➡️ Conceitos de WLAN
- ➡️ Diferenças entre WLANs Abertas e Fechadas
- ➡️ Processo de Associação e Autenticação no 802.11
- ➡️ Autenticação por Chave Compartilhada
- ➡️ Autenticação EAP
- ➡️ Questões de fixação
- ➡️ Packet-tracer

MÓDULO 3: Princípios de Segurança em WLAN

- ➡️ Autenticação, Privacidade e Integridade de Dados
- ➡️ Autenticação por MAC (MAC-Auth)
- ➡️ WEP
- ➡️ Desenvolvimento do WPA e WPA2
- ➡️ Opções de Autenticação para WPA e WPA2
- ➡️ WPA/WPA2-PSK
- ➡️ WPA/WPA2 com 802.1X
- ➡️ WPA3
- ➡️ Autenticação Web (Web-Auth)
- ➡️ Resumo das opções de Segurança Sem Fio
- ➡️ Questões de fixação
- ➡️ Laboratório

MÓDULO 4: Etapas de implantação

- ➡️ Site-Survey Físico
- ➡️ Site-Survey Preditivo
- ➡️ Pre deployment
- ➡️ Post deployment
- ➡️ Padronização da implantação
- ➡️ Questões de fixação
- ➡️ VisiWave Site-Survey Pro
- ➡️ Adicionar Mapas/Plantas
- ➡️ Calibrando a Planta
- ➡️ Pontos de Acesso e Antenas
- ➡️ Site-Survey Passivo
- ➡️ Adaptadores Wireless
- ➡️ Captura contínua
- ➡️ Captura fixa
- ➡️ Captura via GPS
- ➡️ Site-Survey Ativo
- ➡️ Report

hackone

CURSO
INTRODUÇÃO A WIFI E SITE SURVEY

MÓDULO 5: Solução Wireless Cisco

- ➡️ Modelos de WLC e Access-points
- ➡️ Modos de implantação da WLC
- ➡️ Modo local
- ➡️ Flex-Connect
- ➡️ Modos de implantação do AP
- ➡️ Autônomo
- ➡️ Lightweight
- ➡️ Laboratório
- ➡️ Resumo
- ➡️ Configurar opção 43 do DHCP
- ➡️ Configuração do switch para o WLC
- ➡️ Configuração do switch para o LAP

MÓDULO 6: WLC 3504

- ➡️ Startup do controlador wireless
- ➡️ Interface do controlador wireless
- ➡️ Upgrade
- ➡️ Banner
- ➡️ Line Vty
- ➡️ NTP
- ➡️ TACACS
- ➡️ Adição de access-point
- ➡️ Troubleshooting

MÓDULO 7: WLC 9800

- ➡️ Startup do controlador wireless
- ➡️ Interface do controlador wireless
- ➡️ Upgrade
- ➡️ Banner
- ➡️ Line Vty
- ➡️ NTP
- ➡️ TACACS
- ➡️ Adição de access-point
- ➡️ Troubleshooting

MÓDULO 8: WLC 9800 Cloud

- ➡️ Startup do controlador wireless

MÓDULO 9: WLCs EVE

- ➡️ Startup do controlador wireless

hackone

CURSO

INTRODUÇÃO A WIFI E SITE SURVEY

MÓDULO 10: Access-point Autônomo

➡️ Preparação e Configuração

MÓDULO 11: Tunning Wifi

➡️ Melhores Práticas de Rede
➡️ Melhores Práticas da WLC
➡️ Tunning SSID
➡️ Tunning RF

MÓDULO 12: Redundância

➡️ Redundância com WLC na Cloud

MÓDULO 13: Introdução Pentest Wifi

➡️ Tipos de ataque
➡️ Setup Wifi Pineapple
➡️ Quebrando Senha com Wifi Pineapple
➡️ Criando EvilPortal com Wifi Pineapple
➡️ Introdução
➡️ PPTP
➡️ IPIP
➡️ EOIP
➡️ GRE
➡️ L2TPv2 e L2TPv3
➡️ SSTP
➡️ OpenVPN

hackone

CURSO
JUNIPER JNCIA

MÓDULO 1: Junos Fundamentals
MÓDULO 2: Junos User Interface
MÓDULO 3: Junos Basic Configuration
MÓDULO 4: Junos Routing Policy and Firewall Filters
MÓDULO 5: Junos Routing Policy and Firewall Filters
MÓDULO 6: Junos Routing Fundamentals
MÓDULO 7: Futher Study and Exam Prep

DURAÇÃO: 16 HORAS

MÓDULO 1: Junos Fundamentals

➡️ RE/PFE & Software Architecture
➡️ Transit vs Local Host Bound Traffic
➡️ Junos Architecture: CLI Demo

MÓDULO 2: Junos User Interface

➡️ Initial Login & CLI Modes
➡️ Candidate Config Files & Commiting Configuration
➡️ CLI Operational Mode

MÓDULO 3: Junos Basic Configuration

➡️ Factory Default Configuration & Login and Initial Configuration
➡️ Junos User Configuration and Authentication
➡️ Junos Interfaces and Terminology
➡️ Configuration Groups
➡️ Loggin Configuration

hackone

CURSO
JUNIPER JNCIA

MÓDULO 4: Junos Routing Policy and Firewall Filters

- ➡️ Monitoring System Operation & System Hardware
- ➡️ Managing System Components (Outside of Configuration Mode)
- ➡️ Monitoring System Interface
- ➡️ Common Ops Tools & Operational and Troubleshooting Commands
- ➡️ Password Recovery

MÓDULO 5: Junos Routing Policy and Firewall Filters

- ➡️ Policy and Link State Protocols
- ➡️ Routing Policy Behaviour and Actions
- ➡️ Default Policy Actions
- ➡️ Matching Address Space: Route-Filters
- ➡️ Policy and Firewall Prefix List
- ➡️ Junos Firewall Filters

MÓDULO 6: Junos Routing Fundamentals

- ➡️ Routing Protocol Preference and Static Routes
- ➡️ Recursive Resolution of Static Next Hops
- ➡️ Preventing Accidental Resdistribution of Static
- ➡️ Routing Instances and Routing Tables
- ➡️ Copy Routing Between Tables (RIB Groups)

MÓDULO 7: Futher Study and Exam Prep

- ➡️ Day one books
- ➡️ Juniper Learning Portal & Exam Voucher

hackone

CURSO
ZABBIX E GRAFANA

MÓDULO 1: Introdução ao Monitoramento e Ferramentas
MÓDULO 2: Configuração Inicial do Zabbix
MÓDULO 3: Monitoramento Avançado no Zabbix
MÓDULO 4: Configuração de Alertas e Notificações
MÓDULO 5: Integração Zabbix e Grafana
MÓDULO 6: Projeto Real de Monitoramento
DURAÇÃO: 16 HORAS

MÓDULO 1: Introdução ao Monitoramento e Ferramentas

➡️ A Importância do Monitoramento de Infraestrutura
➡️ O Papel do Monitoramento na Manutenção de Redes e Infraestruturas
➡️ Introdução ao Zabbix
➡️ Introdução ao Grafana

MÓDULO 2: Configuração Inicial do Zabbix

➡️ Preparação do ambiente de instalação
➡️ Instalação e configuração inicial do Zabbix
➡️ Configuração de Hosts e Templates

MÓDULO 3: Monitoramento Avançado no Zabbix

➡️ Monitoramento Avançado no Zabbix
➡️ Host via SNMP
➡️ Monitoramento Ativo vs. Passivo

MÓDULO 4: Configuração de Alertas e Notificações

➡️ Triggers no Zabbix – Condições para Alertas
➡️Configuração de notificações

MÓDULO 5: Integração Zabbix e Grafana

➡️ Instalando o Grafana
➡️ Criando Dashboard no Grafana

hackone

CURSO
DEVOPS – LINUX

- ➡️ Aula 1: Apresentação do módulo
- ➡️ Aula 2: Porque aprender Linux?
- ➡️ Aula 3: Entendendo a estrutura do S.O
- ➡️ Aula 4: Instalando e entendendo a estrutura do Linux
- ➡️ Aula 5: Estrutura de diretórios
- ➡️ Aula 6: Criação e remoção de arquivos e diretórios
- ➡️ Aula 7: Comandos essenciais no linux
- ➡️ Aula 8 - Permissionamento
- ➡️ Aula 9: Usuários e grupos
- ➡️ Aula 10: Introdução a shell script
- ➡️ Aula 11: Escrevendo códigos com qualidade
- ➡️ Aula 12: Variáveis
- ➡️ Aula 13: Arrays
- ➡️ Aula 14: Funções e Alias
- ➡️ Aula 15 - Criando scripts
- ➡️ Aula 16: Assessment

hackone

CURSO
HUAWEI HCIA

MÓDULO 1: Fundamentos de Comunicação de Dados e Rede
MÓDULO 2: Construção de uma Rede IP com Interconexão e Interoperabilidade
MÓDULO 3: Construção de Rede de Comutação Ethernet
MÓDULO 4: Infraestrutura de Cibersegurança e Acesso à Rede
MÓDULO 5: Serviços e Aplicações de Rede
MÓDULO 6: Fundamentos de WLAN
MÓDULO 7: Noções básicas de WAN
MÓDULO 8: Gestão de rede e O&M
MÓDULO 9: Noções básicas de IPv6
MÓDULO 10: Noções básicas de SDN e automação
DURAÇÃO: 16 HORAS

MÓDULO 1: Fundamentos de Comunicação de Dados e Rede

- O que é roteamento?
- Introdução a Roteamento
- Conceitos básicos de rede - Como tudo começou
- Conceitos básicos de rede - Componentes de Rede
- Conceitos básicos de rede - Impacto nos Componentes de Infra Estrutura
- Camada OSI
- Princípios do ARP
- IPv4, TCP e UDP
- Princípios básicos e operações do VRP (Plataforma de Roteamento Versátil da Huawei)

MÓDULO 2: Construção de uma Rede IP com Interconexão e Interoperabilidade

- Fundamentos do IPv4 - Classes de IP e Máscara
- Fundamentos do IPv4 - Subnetting em IPv4
- Fundamentos do IPv4 - VLSM e CIDR
- Fundamentos do IPv4 - IPv4 Sumarização
- Fundamentos de roteamento IP e princípios de encaminhamento de dispositivos de Camada 3
- Fundamentos de roteamento estático e implementação no VRP
- Protocolo OSPF e implementação no VRP - Parte 1

hackone

CURSO
HUAWEI HCIA

MÓDULO 3: Construção de Rede de Comutação Ethernet

➡️ Conceitos de Switch e Ethernet
➡️ VLAN Principles and Configuration
➡️ STP Principles and Configuration
➡️ Inter-VLAN Communication
➡️ Eth-Trunk iStack and CSS

MÓDULO 4: Infraestrutura de Cibersegurança e Acesso à Rede

➡️ Princípios básicos e métodos de configuração de ACLs (Listas de Controle de Acesso)
➡️ Princípios de AAA (Autenticação, Autorização e Contabilidade) e cenários de aplicação
➡️ Princípios básicos do NAT (Tradução de Endereço de Rede)
➡️ Cenários de aplicação e métodos de configuração de NAT

MÓDULO 5: Serviços e Aplicações de Rede

➡️ Princípios básicos de FTP
➡️ Princípios básicos de TFTP
➡️ Princípios básicos de TELNET
➡️ Princípios básicos de DHCP
➡️ Princípios básicos do DNS e HTTP

MÓDULO 6: Fundamentos de WLAN

➡️ Conceitos básicos de WLAN (Família de Protocolos 802.11, Dispositivos Básicos e Configuração Básica de Rede)
➡️ Processo básico de funcionamento da WLAN
➡️ Configuração básica de WLAN

MÓDULO 7: Noções básicas de WAN

➡️ Conceitos básicos de WAN
➡️ Configuração PPP
➡️ Configuração PPPoE
➡️ Conceitos básicos de MPLS e SR

hackone

CURSO
HUAWEI HCIA

MÓDULO 8: Gestão de rede e O&M

➡️ Conceitos básicos de gerenciamento de rede
➡️ Noções básicas das configurações do protocolo SNMP

MÓDULO 9: Noções básicas de IPv6

➡️ Noções básicas de IPv6
➡️ Classificação de endereço IPv6
➡️ Configuração Básica IPv6

MÓDULO 10: Noções básicas de SDN e automação

➡️ Conceitos básicos de SDN e produtos e soluções Huawei
➡️ Introdução ao SDN e produtos e soluções Huawei
➡️ Continuação SDN e produtos e soluções Huawei
➡️ Conceitos básicos de NFV e produtos e soluções da Huawei
➡️ Conceitos básicos de O&M automático
➡️ Noções básicas de Python
➡️ Noções básicas de Python e Netmiko
➡️ Script Python e Lib Netmiko
➡️ Configurações com arquivos externos

hackone

CURSO
AWS ZERO TO HERO

MÓDULO 1: Conceitos sobre Cloud Computing
MÓDULO 2: Arquitetura da Infraestrutura da AWS
MÓDULO 3: O Famoso AWS EC2 - Amazon Elastic Compute Cloud
MÓDULO 4: Gerenciamento do AWS EC2
MÓDULO 5: Amazon Elastic File System - EFS
MÓDULO 6: HA e Resiliência com ELB e Autoscaling
DURAÇÃO: 16 HORAS

MÓDULO 1: Instalação

- ➡️ O que é Cloud Computing Realmente?
- ➡️ Vantagens de adoção de Cloud
- ➡️ Segurança e Compliance com Cloud
- ➡️ Casos de Uso de Cloud no Mercado de TI
- ➡️ Modelos de Cloud Computing (IaaS, PaaS, SaaS)
- ➡️ Tipos de Deploy em Cloud (Cloud Privada, Pública e Híbrida)
- ➡️ Dicionário de Cloud Computing
- ➡️ Resiliência - Resilience
- ➡️ Alta Disponibilidade - High Availability
- ➡️ Escalabilidade - Scalability
- ➡️ Agilidade - Agility
- ➡️ Tolerância a falha - Fault Tolerance
- ➡️ Recuperação de Falhas - Disaster Recovery
- ➡️ CapEx vs OpEx
- ➡️ TCO - Total Cost Ownership
- ➡️ Servidor Stateless

MÓDULO 2: Arquitetura da Infraestrutura da AWS

- ➡️ História da AWS
- ➡️ Regiões e Availability Zones (Zonas de Disponibilidade)
- ➡️ Infraestrutura Global da AWS
- ➡️ Conhecendo a Infraestrutura Global da AWS
- ➡️ Acessando a Console de Gerenciamento da AWS

hackone

CURSO
AWS ZERO TO HERO

MÓDULO 3: O Famoso AWS EC2 - Amazon Elastic Compute Cloud

- ➡️ Download dos Recursos dos Laboratórios do módulo
- ➡️ O Que Realmente é o EC2?
- ➡️ Filosofia de Custos do EC2
- ➡️ Modelo de Preços do EC2
- ➡️ Quando usar o EC2 On-Demand e Reserved Instances?
- ➡️ Tipos de Instâncias EC2
- ➡️ Criando uma Instância EC2 Linux - Parte 1
- ➡️ Criando uma Instância EC2 Linux - Parte 2
- ➡️ Criando uma Instância EC2 Windows Server
- ➡️ O que são Security Groups?
- ➡️ Criando um Security Group
- ➡️ Usando o SSH Terminal Web-based
- ➡️ Usando o SSH do Systems Manager

MÓDULO 4: Gerenciamento do AWS EC2

- ➡️ Discos EBS - Elastic Block Store
- ➡️ Criando Discos EBS
- ➡️ Modificando e Deletando Discos EBS
- ➡️ EBS vs Instance Store
- ➡️ Amazon Machine Image (AMI)
- ➡️ Criando um Snapshot
- ➡️ Criando uma EC2 AMI Customizada
- ➡️ Criptografando Volumes EBS
- ➡️ EC2 com IAM Role
- ➡️ Multi-Tenant vs Host Dedicado
- ➡️ Bootstrap Script
- ➡️ Instance Metadata
- ➡️ EC2 Placement Group
- ➡️ Scaling Up e Scaling Down

hackone

CURSO
AWS ZERO TO HERO

MÓDULO 5: Amazon Elastic File System (EFS)

- ➡️ Download dos recursos do Lab AWS
- ➡️ Amazon EFS - Introdução
- ➡️ Criando o EFS - Parte 1
- ➡️ Preparando o ambiente com EFS - Parte 2
- ➡️ Website dentro do EFS - Parte 3
- ➡️ Outros usos do EFS
- ➡️ Limpeza dos recursos da DEMO

MÓDULO 6: Alta Disponibilidade e Resiliência com ELB e Autoscaling

- ➡️ Download dos recursos da DEMO
- ➡️ Amazon Elastic Load Balancer (ELB)
- ➡️ Dicas de High Availability (HA)
- ➡️ Amazon Auto Scaling
- ➡️ Explicação do Projeto Final
- ➡️ Criando Site ELB - Parte 1
- ➡️ Criando Site ELB - Parte 2
- ➡️ Preparando EC2 AMI de Template (Golden Image)
- ➡️ Configurando o Auto Scaling

hackone

CURSO
AZURE ZERO TO HERO

MÓDULO 1: Conceitos sobre Cloud Computing
MÓDULO 2: Arquitetura do Azure
MÓDULO 3: Azure Virtual Machines
MÓDULO 4: Azure File Storage
MÓDULO 5: HA e Resiliência com o Azure
MÓDULO 6: Azure Web App
MÓDULO 7: Azure AD
DURAÇÃO: 16 HORAS

MÓDULO 1: Conceitos sobre Cloud Computing

- ➡️ O que é Cloud Computing realmente?
- ➡️ Vantagens da adoção de Cloud
- ➡️ Segurança e Compliance com Cloud
- ➡️ Casos de uso de Cloud no mercado de TI
- ➡️ Modelos de Cloud Computing: IaaS, PaaS, SaaS
- ➡️ Tipos de Deploy em Cloud: Privada, Pública e Híbrida
- ➡️ Dicionário de Cloud Computing
- ➡️ Resiliência (Resilience)
- ➡️ Alta Disponibilidade (High Availability)
- ➡️ Escalabilidade (Scalability)
- ➡️ Agilidade (Agility)
- ➡️ Tolerância a falha (Fault Tolerance)
- ➡️ Recuperação de falhas (Disaster Recovery)
- ➡️ CapEx vs OpEx
- ➡️ TCO - Total Cost Ownership
- ➡️ Servidor Stateless

hackone

CURSO
AZURE ZERO TO HERO

MÓDULO 2: Arquitetura do Azure

➡️ O que é o Microsoft Azure
➡️ Como administrar o Azure
➡️ Arquitetura global do Azure
➡️ Azure Resource Manager (ARM) e Resource Group
➡️ ARM Locks e movimentação de recursos
➡️ ARM Locks e movimentação de recursos
➡️ ARM Template
➡️ Hands-on: Criando um Resource Group
➡️ Hands-on: Usando um ARM Template

MÓDULO 3: Azure Virtual Machines

➡️ Download dos recursos do Lab
➡️ O que é o Azure Virtual Machine
➡️ Modelo de preço do Azure VM
➡️ Qual modelo de preço usar?
➡️ Tipos de instâncias e tamanhos de Azure VM
➡️ Criando uma Azure VM Windows – Parte 1 e 2
➡️ Criando uma Azure VM Linux – Parte 1 e 2
➡️ Criando uma VM no Azure Cloud Shell – PowerShell e Bash
➡️ Importância de segmentar Resource Groups
➡️ Clean Up dos recursos do Lab
➡️ Azure Network Security Group (NSG)
➡️ Criando um NSG – Hands-on
➡️ Azure Virtual Machine Disk
➡️ Criando uma VM com múltiplos Data Disks – Hands-on
➡️ Azure Marketplace
➡️ Localização e preços do Azure
➡️ Azure VM Custom Image – Parte 1 e 2
➡️ Azure VM Extensions
➡️ Hands-on: VM Windows e Linux com
➡️ Custom Script (Portal e Cloud Shell)
➡️ Salvando 50% do custo de uma VM – Hands-on
➡️ Tour pelo menu de VM – Parte 1 e 2
➡️ Scaling UP e Scaling Down do Azure
➡️ VM – Hands-on

hackone

CURSO
AZURE ZERO TO HERO

MÓDULO 4: Azure File Storage

➡️ Download dos recursos do Lab
➡️ Azure Storage Account
➡️ Criando uma Storage Account – Portal e Cloud Shell – Hands-on
➡️ Azure File Storage
➡️ Criando Azure File Storage – Parte 1 – Hands-on
➡️ Usando o File Storage com Windows – Parte 2 – Hands-on
➡️ Usando VM Linux com File Storage – Parte 3 – Hands-on
➡️ Azure File Snapshot – Como usar – Hands-on
➡️ Limpando todos os recursos do Lab – Hands-on

MÓDULO 5: HA e Resiliência com o Azure

➡️ Download dos recursos do Lab
➡️ Azure Load Balancer
➡️ Criando um Site HA com Load Balancer – Hands-on
➡️ 3 Fases da Disponibilidade
➡️ Azure Availability Sets
➡️ Azure Update Domains e Fault Domains
➡️ Azure Virtual Machine Scale Set (VMSS)
➡️ Criando Linux Image para VMSS – Parte 1 – Hands-on
➡️ Criando o VMSS – Parte 2 – Hands-on
➡️ Finalizando e validando o VMSS com Load Balancer – Parte 3 – Hands-on
➡️ Manual Scaling com o VMSS – Parte 4 – Hands-on
➡️ Autoscaling em ação com o VMSS – Parte 5 – Hands-on
➡️ VMSS Resiliente e Imutável em ação – Hands-on
➡️ Limpando recursos do VMSS – Hands-on

MÓDULO 6: Azure Web App

➡️ Azure Web App
➡️ Deploy de Web App – Hands-on
➡️ Tipos de Deploy de Web App
➡️ Hands on - Deployment Slots
➡️ Escalabilidade e Disponibilidade do Web App
➡️ Hands on - Escalabilidade no Web App

MÓDULO 7: Azure AD

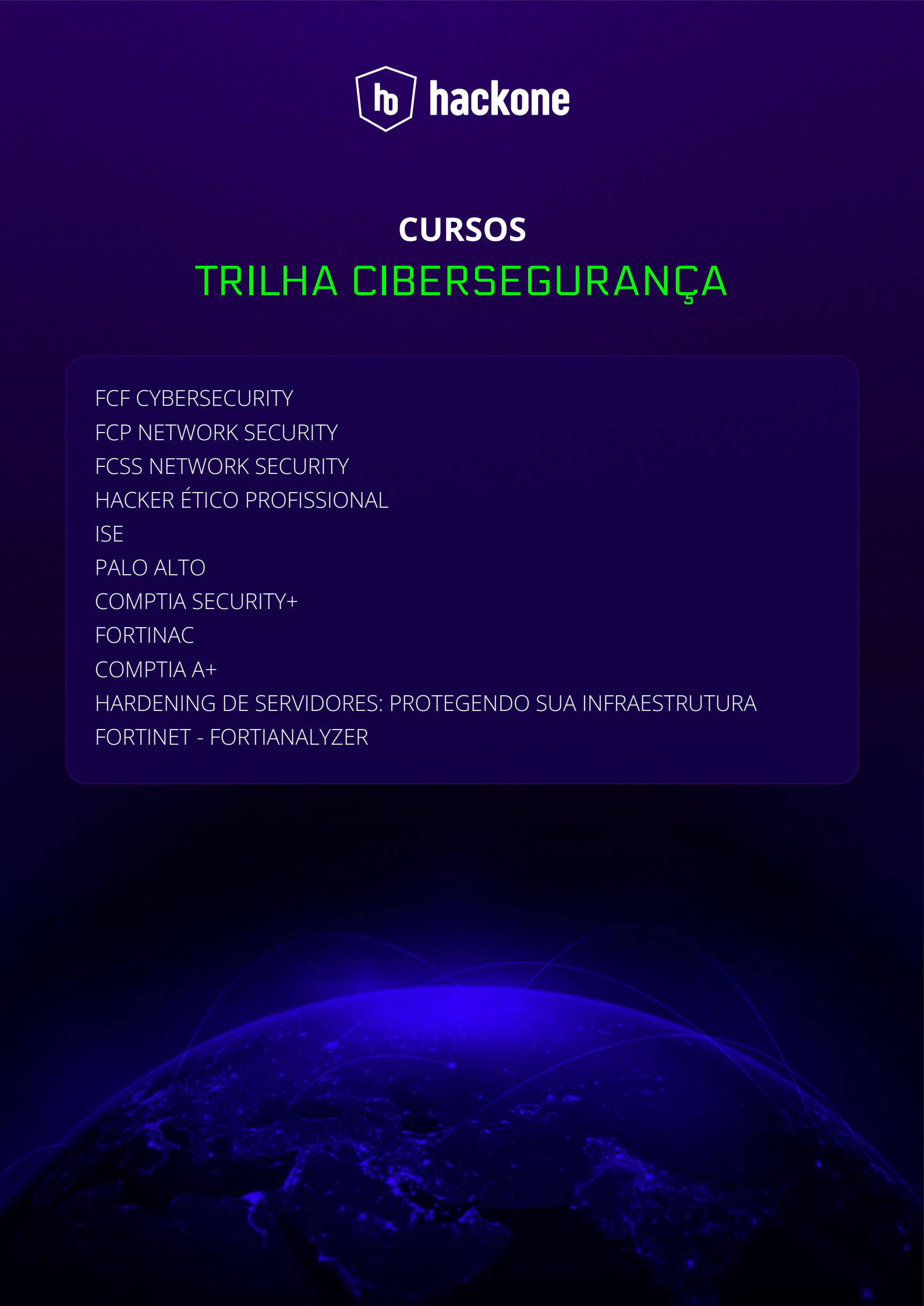
➡️ Azure AD + Lab

hackone

CURSOS

TRILHA CIBERSEGURANÇA

FCF CYBERSECURITY
FCP NETWORK SECURITY
FCSS NETWORK SECURITY
HACKER ÉTICO PROFISSIONAL
ISE
PALO ALTO
COMPTIA SECURITY+
FORTINAC
COMPTIA A+
HARDENING DE SERVIDORES: PROTEGENDO SUA INFRAESTRUTURA
FORTINET - FORTIANALYZER



hackone

CURSO
FCF CYBERSECURITY

MÓDULO 1: Introdução ao Cenário de Ameaças
MÓDULO 2: Introdução à segurança cibernética
MÓDULO 3: Introdução Técnica à Cibersegurança
DURAÇÃO: 6 HORAS

MÓDULO 1: Introdução ao Cenário de Ameaças

- ➡️ Maus atores
- ➡️ Perspectivas de Segurança de Dados
- ➡️ Perspectivas de Senhas
- ➡️ Ameaças de Internet
- ➡️ Ameaças Internas

MÓDULO 2: Introdução à Segurança Cibernética

- ➡️ SASE (Security Access Service Edge)
- ➡️ Cloud Security
- ➡️ SD-WAN
- ➡️ Endpoint Security
- ➡️ Firewall
- ➡️ Wi-Fi
- ➡️ Serviço de Inteligência de Ameaças
- ➡️ SOAR (Security Orchestration, Automation and Response)
- ➡️ Controle de Acesso à Rede
- ➡️ Sandbox
- ➡️ SIEM (Security Information & Event Management)
- ➡️ Web Application Firewall
- ➡️ Secure E-mail Gateway
- ➡️ Web Filter

MÓDULO 3: Introdução Técnica à Cibersegurança

- ➡️ Security-Fabric Overview
- ➡️ Security-Driven Networking
- ➡️ FortiGate
- ➡️ FortiAP
- ➡️ FortiManager
- ➡️ FortiSwitch
- ➡️ Zero Trust Access
- ➡️ FortiAuthenticator
- ➡️ FortiClient
- ➡️ FortiNAC

hackone

CURSO
FCP CYBERSECURITY

MÓDULO 1: FortiGate - Básico
MÓDULO 2: Fortigate - Avançado
DURAÇÃO: 20 HORAS

MÓDULO 1: FortiGate - Básico

- ➡ Introdução e Configurações Iniciais
- ➡ Políticas de Firewall
- ➡ NAT (Network Address Translation)
- ➡ Central NAT
- ➡ Gerenciando Sessões
- ➡ Melhores Práticas & Troubleshooting
- ➡ Métodos de Autenticação
- ➡ Servidores de Autenticação Remota
- ➡ Políticas de Firewall usando Autenticação
- ➡ Autenticação através de Captive Portal
- ➡ Monitoramento e Troubleshooting
- ➡ Log Básico
- ➡ Logging Local e Remoto
- ➡ Log Settings e Log Search
- ➡ Operações de Certificados
- ➡ Inspecionar Dados Criptografados
- ➡ Gerenciar Certificados Digitais
- ➡ Web Filtering
- ➡ Entendendo o Web Filtering
- ➡ Video Filtering
- ➡ DNS e File Filtering
- ➡ Melhores Práticas e Troubleshooting
- ➡ Controle de Aplicação
- ➡ Entendendo o Antivirus
- ➡ Modos de Escaneamento
- ➡ Configuração e Boas Práticas
- ➡ Intrusion Prevention System (IPS)
- ➡ Denial of Service
- ➡ Web Application Firewall
- ➡ Melhores Práticas e Troubleshooting
- ➡ SSL-VPN

MÓDULO 2: FortiGate - Avançado

- ➡ Routing, Routing Monitor e Atributos de Rotas no FortiGate
- ➡ Equal Cost Multipath Routing (ECMP)
- ➡ Diagnósticos de Roteamento
- ➡ SD-WAN (Breakout Local)
- ➡ VDOM (Domínios Virtuais)
- ➡ L2 Switching
- ➡ IPSEC VPN
- ➡ Formas de Implementação
- ➡ FSSO com Windows Active Directory
- ➡ Autenticação NTLM
- ➡ High Availability (HA)
- ➡ Diagnósticos Gerais
- ➡ Debug Flow
- ➡ CPU e Memória
- ➡ Testes de Hardware
- ➡ Security Fabric

hackone

CURSOS

FCSS; HACKER ÉTICO PROFISSIONAL

FCSS NETWORK SECURITY

- FortiAnalyzer - Setup Inicial
- Implementando Security Fabric
- Features - Security Fabric
- Vida de um Pacote
- Arquitetura de Memória
- Comandos Troubleshooting
- Conserve Mode
- Otimização de Memória
- Troubleshooting System Crashes
- Tabela de Sessões
- Sniffer
- Debug Flow
- Conceitos Gerais
- Reverse Path Forwarding
- Retorno do Roteamento do Pacote
- Mudança de Roteamento
- Virtual Routing and Forwarding
- FortiGuard - Setup Inicial FortiManager
- FortiGuard
- FortiManager como um FDS Local
- Alta Disponibilidade (HA)
- Active-Active Load Balancing
- FGCP Virtual Clustering
- Gerenciamento Centralizado
- OSPF
- OSPF Lab
- BGP
- BGP Lab
- Web Filtering
- Sistema de Prevenção de Intrusos (IPS)
- Sistema de Prevenção de Intrusos (IPS) e Lab
- IPSec
- Auto-Discovery VPN
- Topologia ADVPN

DURAÇÃO: 26 HORAS

HACKER ÉTICO PROFISSIONAL

- O que é Ethical Hacking?
- Aspectos Legais
- Certificações e Mercado de Trabalho
- Penetration Test
- Processo de um teste de invasão
- Termos de Responsabilidade e Confidencialidade
- Relatórios
- Instalação do VirtualBox
- Instalação do VMWare Player
- Softwares e VMs que serão utilizados
- Instalação do Kali Linux - Parte 01
- Instalação do Kali Linux - Parte 02
- Configurações iniciais do Kali Linux
- Instalação das Máquinas Windows - XP
- Instalação das Máquinas Windows 7
- Instalação e configuração do Metasploitable
- Instalação do Android na Virtual Machine (VM)
- Instalação do Emulador Genymotion
- VBox Additions no Windows
- VBox Additions no Linux

DURAÇÃO: 6 HORAS

hackone

CURSOS

ISE

ISE

- ➡️ Preparando o Windows Server - Cisco ISE
- ➡️ Cisco FTD/FMC - Configurações Iniciais
- ➡️ Cisco ISE - Certificados
- ➡️ Cisco ISE - Integração com AD
- ➡️ Cisco ISE - Configurando Switch
- ➡️ Cisco ISE - 802.1X
- ➡️ Cisco ISE - 802.1X (Parte 2)
- ➡️ Cisco ISE - 802.1X
- ➡️ Cisco ISE - MAB Estático
- ➡️ Cisco ISE - MAB Dinâmico
- ➡️ Cisco FTD/FMC - Configurando Interfaces
- ➡️ Cisco FMC - Integração com AD
- ➡️ Cisco FMC - Certificados
- ➡️ Cisco FMC - Teste de Navegação

DURAÇÃO: 7 HORAS

hackone

CURSO
PALO ALTO

MÓDULO 1: Instalação
MÓDULO 2: Configurações de Rede e Roteamento
MÓDULO 3: Security Policies NAT
MÓDULO 4: Security Profiles (Content-ID)
MÓDULO 5: Authentication & VPN
MÓDULO 6: Gerenciamento de Dispositivo
DURAÇÃO: 20 HORAS

MÓDULO 1: Instalação

- ➡️ Laboratório
- ➡️ Instalação do Firewall Virtual
- ➡️ Licenciamento

MÓDULO 2: Configurações de Rede e Roteamento

- ➡️ Configurando Zonas de Segurança
- ➡️ Configuração de Interface
- ➡️ Interface Management Profile
- ➡️ Criando uma Subinterface
- ➡️ Configuração do servidor DHCP
- ➡️ Configuração de Relay
- ➡️ Roteamento Estático

MÓDULO 3: Security Policies NAT

- ➡️ Introdução a Políticas de Segurança
- ➡️ Dynamic NAT (PAT)
- ➡️ Static (Source) NAT
- ➡️ Destination NAT (DNAT)
- ➡️ APP-ID e Filters
- ➡️ Utilizando Tags
- ➡️ SSL Decryption - HTTPS Inspection

hackone

CURSO
PALO ALTO

MÓDULO 5: Authentication & VPN

- ➡️ DAP Authentication Profile
- ➡️ Enable User-ID
- ➡️ Authentication Portal
- ➡️ VPN Zone e Tunnel Interface
- ➡️ CA Certificate - SSL VPN
- ➡️ Global Protect Gateway e Configurações de Portal
- ➡️ Global Protect Portal e SSL Client VPN Access
- ➡️ IPsec VPN Site-to-Site

MÓDULO 6: Gerenciamento de Dispositivo

- ➡️ Role Based Administration
- ➡️ PAN-OS Update
- ➡️ High Availability - HA
- ➡️ Gerenciamento dos Arquivos de Configurações

hackone

CURSOS

COMPTIA SECURITY+; FORTINAC

COMPTIA SECURITY+

- ➡️ Comparando Funções de Segurança e Controles de Segurança
- ➡️ Explicando Atores e Inteligência de Ameaças
- ➡️ Realizando Avaliações de Segurança
- ➡️ Identificando Engenharia Social e Malware
- ➡️ Resumindo Conceitos Básicos de Criptografia
- ➡️ Implementando Infraestrutura de Chave Pública
- ➡️ Implementando Controles de Autenticação
- ➡️ Implementando Controles de Gerenciamento de Identidade e Conta
- ➡️ Implementando Projetos de Rede Segura
- ➡️ Implementando Dispositivos de Segurança de Rede
- ➡️ Implementando Protocolos de Rede Seguros
- ➡️ Implementando Soluções de Segurança de Hospedagem
- ➡️ Implementando Soluções de Mobilidade Segura
- ➡️ Resumindo Conceitos de Aplicações Seguras
- ➡️ Implementando Soluções Seguras em Nuvem
- ➡️ Explicando Conceitos de Privacidade e Proteção de Dados
- ➡️ Realizando Resposta a Incidentes
- ➡️ Explicando a Forense Digital
- ➡️ Resumindo Conceitos de Gerenciamento de Riscos
- ➡️ Implementando Resiliência em Cibersegurança
- ➡️ Explicando Controles Físicos

DURAÇÃO: 36 HORAS

FORTINAC

- ➡️ Alcançando Visibilidade na Rede
- ➡️ Identificando e Classificando Rogues
- ➡️ Visibilidade, Troubleshooting e Logging
- ➡️ Logical Networks, Fortinet Security e Fabricance Firewall Tags
- ➡️ State-Based Control
- ➡️ Gerenciamento de Visitantes e Usuários

DURAÇÃO: 6 HORAS

hackone

CURSO
COMPTIA A+

MÓDULO 1: Instalando Motherboards e Conectores
MÓDULO 2: Instalando Dispositivos do Sistema
MÓDULO 3: Troubleshooting PC Hardware
MÓDULO 4: Comparando Hardware de Rede Local
MÓDULO 5: Configurando Endereçamento de Rede e Conexões à Internet
MÓDULO 6: Serviços de Suporte à Rede
MÓDULO 7: Entendendo Conceitos de Virtualização e Cloud
MÓDULO 8: Entendendo Dispositivos Móveis
MÓDULO 9: Entendendo Dispositivos de Impressão
MÓDULO 10: Configurando Windows
MÓDULO 11: Gerenciando Windows
MÓDULO 12: Identificando Tipos de Sistemas Operacionais e suas características
MÓDULO 13: Instalação e solução de problemas dos sistemas operacionais
MÓDULO 14: Gerenciando Redes Windows
MÓDULO 15: Gerenciando Linux e MacOS
MÓDULO 16: Configurando Segurança de Rede SOHO
MÓDULO 17: Gerenciando Configurações de Rede
MÓDULO 18: Suporte para Software Mobile
MÓDULO 19: Usando Ferramentas de Suporte e Scripting
MÓDULO 20: Implementando Procedimentos Operacionais
DURAÇÃO: 20 HORAS

MÓDULO 1: Instalando Motherboards e Conectores

➡️ Explicando Tipos de Cabos e Conectores
➡️ Instalar e Configurar Motherboards
➡️ Explicando Tipos de Cabos Legados

hackone

CURSO
COMPTIA A+

MÓDULO 2: Instalando Dispositivos do Sistema

➡️ Instalar e Configurar Fontes e Cooling
➡️ Selecionar e Instalar Dispositivos de Armazenamento
➡️ Instalar e Configurar Memória do Sistema
➡️ Instalar e Configurar CPU

MÓDULO 3: Troubleshooting PC Hardware

➡️ Aplicando a Metodologia de Troubleshooting
➡️ Configurando a BIOS/UEFI
➡️ Solucionando Problemas de Energia e Disco
➡️ Solucionando Problemas de Sistema e Display

MÓDULO 4: Comparando Hardware de Rede Local

➡️ Comparando Tipos de Redes
➡️ Comparando Hardware de Rede
➡️ Explicando Tipos de Cabo de Rede
➡️ Comparando Tipos de Rede Wireless

MÓDULO 5: Configurando Endereçamento de Rede e Conexões à Internet

➡️ Comparando Tipos de Conexão à Internet
➡️ Conceitos Básicos de TCP/IP
➡️ Comparando Protocolos e Portas

MÓDULO 6: Serviços de Suporte à Rede

➡️ Serviços Fornecidos por Host em Rede
➡️ Comparando Dispositivos Embarcados e Internet
➡️ Troubleshoot Networks

hackone

CURSO
COMPTIA A+

MÓDULO 7: Entendendo Conceitos de Virtualização e Cloud

➡️ Virtualização Client-side
➡️ Entendendo Conceitos de Cloud

MÓDULO 8: Entendendo Dispositivos Móveis

➡️ Dispositivos Móveis e Periféricos
➡️ Apps em Dispositivos Móveis
➡️ Laptop Hardware
➡️ Falhas em Dispositivos Móveis

MÓDULO 9: Entendendo Dispositivos de Impressão

➡️ Implantar Impressoras e Dispositivos
➡️ Solucionar Problemas do Dispositivo de Impressão
➡️ Substituir os Consumíveis dos Dispositivos de Impressão

MÓDULO 10: Configurando Windows

➡️ Configurações de Usuário
➡️ Configurações do Sistema

MÓDULO 11: Gerenciando Windows

➡️ Utilizando Consoles de Gerenciamento
➡️ Ferramentas de Performance e Troubleshooting
➡️ Ferramentas que utilizam Linhas de Comando

MÓDULO 12: Identificando Tipos de Sistemas Operacionais e suas Características

➡️ Tipos de Sistemas Operacionais
➡️ Comparando Edições do Windows

hackone

CURSO
COMPTIA A+

MÓDULO 13: Instalação e Solução de Problemas dos Sistemas Operacionais

➡️ Instalações e Atualizações de Sistema Operacional
➡️ Instalar e Configurar Aplicações
➡️ Solucionando Problemas do Windows

MÓDULO 14: Gerenciando Redes Windows

➡️ Configurando Rede no Windows
➡️ Resolvendo Problemas de Rede no Windows
➡️ Definindo Configurações de Segurança no Windows

MÓDULO 15: Gerenciando Linux e MacOS

➡️ Identificando Recursos do Linux
➡️ Identificando Recursos do MacOS

MÓDULO 16: Configurando Segurança de Rede SOHO

➡️ Ataques, Ameaças e Vulnerabilidades
➡️ Comparando Protocolos de Segurança de Redes Wireless

MÓDULO 17: Gerenciando Configurações de Rede

➡️ Configurando Segurança em uma Workstation
➡️ Configurando Segurança em Browsers
➡️ Solucionando Problemas em Workstations

MÓDULO 18: Suporte para Software Mobile

➡️ Configurando Segurança para Sistemas Operacionais Mobile
➡️ Resolvendo Problemas em Sistemas Operacionais Mobile e Apps

hackone

CURSO
COMPTIA A+

MÓDULO 19: Usando Ferramentas de Suporte e Scripting

➡️ Tecnologias de Acesso Remoto
➡️ Implementando Backup e Recuperação

MÓDULO 20: Implementando Procedimentos Operacionais

➡️ Melhores Práticas de Documentação

hackone

CURSO

HARDENING DE SERVIDORES: PROTEGENDO SUA INFRAESTRUTURA

MÓDULO 1: Introdução à Cibersegurança e Hardening
MÓDULO 2: Fundamentos de Segurança
MÓDULO 3: Sistema Operacional e Configurações de Segurança
MÓDULO 4: Serviços de Rede e Protocolos
MÓDULO 5: Proteção de Dados e Criptografia
MÓDULO 6: Monitoramento e Resposta a Incidentes
MÓDULO 7: Práticas Avançadas de Hardening
MÓDULO 8: Exercícios Práticos e Estudo de Caso
MÓDULO 9: Revisão e Avaliação

DURAÇÃO: 14 HORAS

MÓDULO 1: Introdução à Cibersegurança e Hardening

➡️ Conceitos básicos de cibersegurança
➡️ O que é hardening de servidores e sua importância

MÓDULO 2: Fundamentos de Segurança

➡️ Conceitos básicos de cibersegurança
➡️ O que é hardening de servidores e sua importância

MÓDULO 3: Sistema Operacional e Configurações de Segurança

➡️ Configuração segura do sistema operacional (ex: Windows Server, Linux)
➡️ Gerenciamento de contas de usuário e permissões
➡️ Configuração de firewalls e políticas de segurança

MÓDULO 4: Serviços de Rede e Protocolos

➡️ Análise dos serviços de rede mais comuns
➡️ Configuração segura de serviços (ex: HTTP, SSH, FTP)
➡️ Proteção contra ataques de rede (ex: DDoS, brute force)

hackone

CURSO

HARDENING DE SERVIDORES: PROTEGENDO SUA INFRAESTRUTURA

MÓDULO 5: Proteção de Dados e Criptografia

➡️ Importância da proteção de dados
➡️ Conceitos básicos de criptografia
➡️ Implementação de criptografia em servidores

MÓDULO 6: Monitoramento e Resposta a Incidentes

➡️ Ferramentas e técnicas de monitoramento de segurança
➡️ Identificação e resposta a incidentes de segurança
➡️ Estratégias de recuperação após incidentes

MÓDULO 7: Práticas Avançadas de Hardening

➡️ Tendências e desafios futuros em hardening de servidores
➡️ Hardening específico para ambientes on-premise
➡️ Automação de processos de hardening

MÓDULO 8: Exercícios Práticos e Estudo de Caso

➡️ Aplicação dos conceitos aprendidos em cenários práticos
➡️ Análise de um estudo de caso de uma violação de segurança
➡️ Discussão sobre estratégias para prevenir incidentes semelhantes

MÓDULO 9: Revisão e Avaliação

➡️ Revisão dos principais tópicos abordados no curso
➡️ Avaliação do aprendizado dos participantes
➡️ Feedback e sugestões para futuras melhorias

hackone

CURSO
FORTINET – FORTIANALYZER

MÓDULO 1: Introdução, Modos de Operação e Configuração de Rede
MÓDULO 2: Administração, Segurança e Domínios Administrativos
MÓDULO 3: RAID e HA
MÓDULO 4: Gerenciamento de Dispositivos e Troubleshooting
MÓDULO 5: Logs e Gerenciamento de Reports
MÓDULO 6: Bônus

DURAÇÃO: 14 HORAS

MÓDULO 1: Introdução, Modos de Operação e Configuração de Rede

- ➡️ Introdução ao FortiAnalyzer e Configuração Inicial
- ➡️ Centralização de Logs com Security Fabric
- ➡️ Modos de Operação: Analyzer vs. Collector
- ➡️ Configuração de Interfaces e Rede no FortiAnalyzer

MÓDULO 2: Administração, Segurança e Domínios Administrativos

- ➡️ Gerenciamento de Acessos e Política de Senhas
- ➡️ Perfis de Administrador e Autenticação Externa
- ➡️ Monitoramento de Usuários e Gerenciamento de ADOMs

MÓDULO 3: RAID e HA

- ➡️ O que é RAID e como ele protege dados
- ➡️ Tipos de operação RAID Parte 1
- ➡️ Como configurar RAID e os níveis de RAID
- ➡️ Como visualizar o status, diagnóstico e falhas no RAID
- ➡️ O que é HA (High Availability)
- ➡️ Como configurar e usar HA no FortiAnalyzer
- ➡️ Diferença entre modos Active-Active e Active-Passive em HA
- ➡️ Opções e processos de eleição primária em HA e Sincronização Parte 1
- ➡️ Opções e processos de eleição primária em HA e Sincronização Parte 2
- ➡️ Balanceamento de carga, firmware e monitoramento no FortiAnalyzer

hackone

CURSO
FORTINET – FORTIANALYZER

MÓDULO 4: Gerenciamento de Dispositivos e Troubleshooting

➡️ Registro e Monitoramento de Dispositivos no FortiAnalyzer
➡️ Diagnóstico e Solução de Problemas de Conectividade
➡️ Coleta de Logs dos Dispositivos FortiGate
➡️ Integração com Clusters HA do FortiGate

MÓDULO 5: Logs e Gerenciamento de Reports

➡️ O que é o gerenciamento de logs e relatórios
➡️ Fluxo de trabalho de arquivos de log
➡️ Adicionando device no FortiAnalyzer
➡️ Como configurar o backup de logs no FortiAnalyzer.
➡️ Considerações e melhores práticas para backup de dados de log.
➡️ O que são conectores de armazenamento?
➡️ Como configurar e usar conectores de armazenamento para logs
➡️ Como garantir redundância de logs no FortiAnalyzer
➡️ Alta disponibilidade e segurança dos logs - Server secundário de logs
➡️ Alta disponibilidade e segurança dos logs - Log forwarding Collector
➡️ O que é, e como configurar o encaminhamento de logs
➡️ Como configurar a comunicação de logs encriptada usando OFTPS e seus benefícios
➡️ Como impedir a modificação não autorizada dos logs
➡️ Gerenciamento de limpeza de logs
➡️ Para que servem os relatórios no FortiAnalyzer e ADOM
➡️ Aula Bônus - External Storage Mail e SQL Hard Cache

MÓDULO 6: Bônus

➡️ Automação e Event Monitor
➡️ Relatórios do FortiAnalyzer
➡️ Threat View

hackone

CURSO

FIREWALL AVANÇADO – MIKROTIK

MÓDULO 1: INTRODUÇÃO AO FIREWALL MIKROTIK
MÓDULO 2: FIREWALL FILTER MIKROTIK
MÓDULO 3: COMPREENDENDO O PORTSCAN E COMO SE PROTEGER NO MIKROTIK
MÓDULO 4: COMPREENDENDO CONECTIONS STATES DO MIKROTIK
MÓDULO 5: BLOQUEIO DE PÁGINAS NO FIREWALL MIKROTIK
MÓDULO 6: CERTIFICADO DE CONCLUSÃO

hackone

CURSO
WIREGUARD EXPERT

MÓDULO 1: Introdução ao Wireguard
MÓDULO 2: Conceito Wireguard
MÓDULO 3: Entendendo as chave públicas e privadas
MÓDULO 4: Criando Interface Matriz e Filia
MÓDULO 5: Criando os peers na matriz e filiais
MÓDULO 6: Implementando segurança no Wireguard
MÓDULO 7: Implantando rotas estáticas no Wireguard
MÓDULO 8: Implantando OSPF no Wireguard
MÓDULO 9: Testes de desempenho
MÓDULO 10: Conectando outros clientes no Wireguard

MÓDULO 1: Introdução ao Wireguard

➡️ Introdução ao Wireguard

MÓDULO 2: Conceito Wireguard

➡️ Conceito Wireguard

MÓDULO 3: Entendendo as chave públicas e privadas

➡️ Entendendo as chave públicas e privadas

MÓDULO 4: Criando Interface Matriz e FiliaIS

➡️ Criando Interface Matriz e FiliaIS

MÓDULO 5: Criando os peers na matriz e filiais

➡️ Criando os peers na matriz e filiais

hackone

CURSO
WIREGUARD EXPERT

MÓDULO 6: Implementando segurança no Wireguard

➡️ Implementando segurança no Wireguard

MÓDULO 7: Implantando rotas estáticas no Wireguard

➡️ Implantando rotas estáticas no Wireguard

MÓDULO 8: Implantando OSPF no Wireguard

➡️ Implantando OSPF no Wireguard

MÓDULO 9: Testes de desempenho

➡️ Testes de desempenho

MÓDULO 9: Conectando outros clientes no Wireguard

➡️ Conectando outros clientes no Wireguard
➡️ Conectando um PC Windows no Wireguard
➡️ Conectando um celular Android no Wireguard - Criar túnel do zero
➡️ Conectando um celular Android no Wireguard - Criar túnel com QR Code
➡️ Conectando um celular Android no Wireguard - Criar túnel de um arquivo
➡️ Conectando um IOS no túnel Wireguard

hackone

CURSO
VPN EXPERT V7

MÓDULO 1: Introdução
MÓDULO 2: PPTP
MÓDULO 3: IPIP
MÓDULO 4: EOIP
MÓDULO 5: GRE
MÓDULO 6: L2TPv2 e L2TPv3
MÓDULO 7: SSTP
MÓDULO 8: OpenVPN

MÓDULO 1: Introdução

- ➡️ Introdução
- ➡️ Montando o LAB do Zero
- ➡️ Importando a Base Config
- ➡️ Quais equipamentos usar

MÓDULO 2: PPTP

- ➡️ Sobre o PPTP
- ➡️ Configurando PPTP Server
- ➡️ Conectando Filiais
- ➡️ PPTP com OSPF
- ➡️ PPTP no Windows

MÓDULO 3: IPIP

- ➡️ Introdução IPIP
- ➡️ Confgurando entre Matriz e Filial
- ➡️ IPIP com IPSec

hackone

CURSO
VPN EXPERT V7

MÓDULO 4: EIOP

- ➡️ Introdução ao EOIP
- ➡️ Interligando Matriz e Filial
- ➡️ EOIP com IPSec
- ➡️ EOIP L2

MÓDULO 5: GRE

- ➡️ Introdução ao GRE
- ➡️ Interligando Matriz e Filial
- ➡️ Wireshark e MTU
- ➡️ GRE com IPSec

MÓDULO 6: L2TPv2 e L2TPv3

- ➡️ Introdução ao L2TP v2
- ➡️ Conceito L2TP v3
- ➡️ L2TPv2 Server 2 com OSPF
- ➡️ Configurando L2TP v3 com VLAN
- ➡️ L2TPv3 com UDP Firewall
- ➡️ Configurando Filial Fortaleza
- ➡️ Troubleshooting
- ➡️ Configurando OSPF na Filial
- ➡️ Configurando Filial São Paulo
- ➡️ L2TP com IPSec
- ➡️ VPN Client to Site L2TP com Windows

hackone

CURSO
VPN EXPERT V7

MÓDULO 7: SSTP

- ➡️ Conceito SSTP
- ➡️ Preparando o LAB
- ➡️ Configurando SSTP Server
- ➡️ Configurando SSTP Client
- ➡️ VPN redundante
- ➡️ Gerando Certificado e Export
- ➡️ Importando o Certificado
- ➡️ Utilizando SSTP com Certificado
- ➡️ Revogar um certificado

MÓDULO 8: OpenVPN

- ➡️ Conceito OVPN
- ➡️ Preparando o LAB
- ➡️ Certificado CA Server e Client
- ➡️ OVPN Server
- ➡️ OVPN Client no MikroTik

hackone PRO

Ficou alguma dúvida?

Para mais informações que não estejam detalhadas neste documento ou demais dúvidas, entre em contato com as nosso time de consultores de carreira através do Whatsapp tocando no botão abaixo:

FALAR COM UM CONSULTOR

