Check Point Troubleshooting Administrator R82 (CCTA)

Check Point

- **Nível:**
- **Duração:** 14h

Sobre o curso

O curso Certified Troubleshooting Administrator (CCTA) proporciona as competências fundamentais necessárias para diagnosticar e resolver eficazmente problemas em Quantum Security Management Servers e Security Gateways executados no sistema operativo Gaia.

Após uma introdução ao troubleshooting, são abordados os fundamentos da monitorização de tráfego e da captura de pacotes, seguindo-se a análise de capturas de pacotes através da CLI e do Wireshark.

O curso aborda ainda o troubleshooting de processos, SmartConsole, recolha de logs, Identity Awareness, Application Control e URL Filtering.

Destinatários

- Administradores de Segurança
- Engenheiros de Segurança
- Analistas de Segurança
- Consultores de Segurança
- Arquitetos de Segurança

Objetivos

- Aplicar uma metodologia estruturada de troubleshooting para identificar e isolar a causa de problemas.
- Utilizar o modelo OSI como referência no diagnóstico de problemas de comunicação e de rede.
- Analisar recursos, desempenho e informações de sistema em Security Management Servers e Security Gateways com Gaia.
- Utilizar ferramentas como CPStat, CPView e CPInfo na recolha e análise de dados de diagnóstico.
- Monitorizar o tráfego de rede e interpretar logs durante processos de troubleshooting.
- Identificar e resolver problemas relacionados com políticas de segurança, routing e NAT.
- Realizar capturas de pacotes com FW Monitor, tcpdump e Check Point PCAP.

- Analisar capturas de pacotes através da CLI e do Wireshark.
- Diagnosticar problemas relacionados com processos Check Point e respetiva conectividade.
- Investigar e resolver problemas no SmartConsole.
- Diagnosticar falhas na recolha de logs e interrupções de comunicação.
- Utilizar comandos e ferramentas adequados para resolver problemas de Identity Awareness.
- Investigar e resolver problemas relacionados com Application Control e URL Filtering.
- Restaurar o ambiente após a execução de tarefas práticas de troubleshooting.

Condições

Após a formação, é possível adquirir, o exame de certificação do parceiro oficial com 10% de desconto. Oferta válida até 6 meses após a conclusão do curso.

Pré-requisitos

Conhecimentos fundamentais de:

- Sistemas operativos Unix-like e/ou Windows
- Fundamentos da Internet
- Fundamentos de redes
- Segurança de redes
- Administração de sistemas
- Redes TCP/IP
- Editores de texto em sistemas operativos Unix-like

Programa

- I
- ntrodução ao Troubleshooting
- Fundamentos da Monitorização de Tráfego
- Fundamentos da Captura de Pacotes
- Análise de Capturas de Pacotes através da CLI
- Análise de Capturas de Pacotes através do Wireshark
- Troubleshooting de Processos Check Point
- Troubleshooting do SmartConsole
- Troubleshooting da Recolha de Logs
- Troubleshooting do Identity Awareness
- Troubleshooting do Application Control e URL Filtering

Introdução ao Troubleshooting

- Identificar os princípios da metodologia de troubleshooting.
- Compreender como utilizar o modelo OSI — Open Systems Interconnection — para isolar a causa de um problema.
- Identificar os recursos disponíveis para diagnosticar e resolver problemas em Check Point Security Gateways e Security Management Servers executados no sistema operativo Gaia.

Labs:

- Analisar recursos e desempenho.
- Analisar informações do sistema com o CPStat.
- Analisar dados estatísticos com o CPView.
- Recolher o output do CPInfo no Security Management Server.
- Recolher o output do CPInfo no Security Gateway.
- Analisar o output do CPInfo.

Fundamentos da Monitorização de Tráfego

- Descrever as funções das capturas de pacotes.
- Descrever como os logs e a monitorização são utilizados no troubleshooting.
- Investigar e resolver potenciais problemas relacionados com o fluxo de tráfego.
- Monitorizar a atividade e o desempenho da rede.

Labs:

- Analisar logs.
- Rastrear regras e criar uma política.
- Testar regras de política e NAT.
- Examinar o encaminhamento e os logs de estado.

Fundamentos da Captura de Pacotes

- Compreender o impacto e as limitações das capturas de pacotes.
- Compreender a utilização e as limitações de quatro ferramentas que podem ser utilizadas na captura de pacotes.
- Investigar e resolver potenciais problemas relacionados com o fluxo de tráfego através de capturas de pacotes.
- Monitorizar a atividade e o desempenho da rede através de capturas de pacotes.

Labs:

- Capturar tráfego com o filtro de expressões do FW Monitor.
- Capturar tráfego com o filtro simples do FW Monitor.
- Capturar tráfego com o utilitário tcpdump.
- Capturar tráfego com o Check Point PCAP.

Análise de Capturas de Pacotes através da CLI

- Identificar os formatos de output da linha de comandos do tcpdump, cppcap, fw monitor -e e fw monitor -F.
- Identificar as flags do cppcap e o respetivo impacto no nível de detalhe do output.
- Compreender como o CPMonitor pode ser utilizado durante a análise de capturas de pacotes.
- Analisar capturas de pacotes através da CLI.

Labs:

- Criar problemas.
- Diagnosticar e resolver problemas fundamentais de tráfego.
- Diagnosticar e resolver problemas de configuração de políticas.
- Diagnosticar e resolver problemas de encaminhamento.
- Diagnosticar e resolver problemas de NAT.
- Restaurar o ambiente.

Análise de Capturas de Pacotes através do Wireshark

- Compreender as regras de cores do Wireshark e as alterações que podem ser efetuadas.
- Identificar a metodologia de gravação de ficheiros para capturas analisadas no Wireshark.
- Analisar capturas de pacotes no Wireshark.

Labs:

- Configurar o Wireshark para utilização com a Check Point.
- Guardar capturas de pacotes.
- Analisar capturas de pacotes do FW Monitor no Wireshark.
- Analisar capturas de pacotes de interfaces no Wireshark.

Troubleshooting de Processos Check Point

- Demonstrar conhecimentos sobre user space, kernel space e os processos do Check Point User Space Firewall.
- Investigar, diagnosticar e resolver problemas relacionados com processos.

Labs:

- Verificar os estados dos processos.
- Analisar a conectividade dos processos.

Troubleshooting do SmartConsole

- Investigar, diagnosticar e resolver problemas relacionados com o Check Point SmartConsole.

Labs:

- Ativar o Bad Actor.
- Diagnosticar e resolver problemas de início de sessão no SmartConsole.

- Restaurar o ambiente.

Troubleshooting da Recolha de Logs

- Diagnosticar e resolver problemas relacionados com a recolha de logs e interrupções nas comunicações.

Labs:

- Ativar o Bad Actor.
- Diagnosticar e resolver problemas de conectividade dos logs do Gateway.
- Diagnosticar e resolver problemas na recolha de logs do Security Management Server.
- Restaurar o ambiente.

Troubleshooting do Identity Awareness

- Identificar e utilizar os comandos e as ferramentas de troubleshooting adequados para resolver problemas avançados de Identity Awareness.

Labs:

- Ativar o Bad Actor.
- Diagnosticar e resolver problemas de Identity Awareness.
- Restaurar o ambiente.

Troubleshooting do Application Control e URL Filtering

- Investigar, diagnosticar e resolver problemas relacionados com Application Control e URL Filtering.

Labs:

- Ativar o Bad Actor.
- Diagnosticar e resolver problemas de URL Filtering.
- Restaurar o ambiente.