Network Traffic Analysis for Monitoring & Cyber Security

Tecnologias de Informação - Segurança

- **Nível:** Intermédio
- **Duração:** 21h

Sobre o curso

Sob o lema "**Packets never lie!**", os formandos irão, neste curso de **forte componente prática**, construir um laboratório e, com recurso às soluções da Colasoft – Capsa Enterprise e nChronos – terão a oportunidade de analisar diversos cenários reais de tráfego de rede, por forma a detetar atividades maliciosas.

A crescente complexidade e diversidade de sistemas, aplicações e tecnologias de comunicação acarreta dificuldades acrescidas para as organizações, de modo a que os respetivos profissionais possam ter uma adequada **visibilidade** e **controlo** sobre o tráfego de rede existente.

Frequentemente, encontram-se camuflados problemas de **performance** ou **anomalias** em diversos elementos existentes nas infraestruturas comunicações, resultantes de falhas no seu funcionamento ou na sua configuração.

O domínio da **segurança** é, igualmente, um fator de extrema importância, em consequência de ataques cada vez mais sofisticados, explorando vulnerabilidades diversas, a que acresce ainda a real impreparação da grande maioria dos utilizadores.

Objetivos

Dotar os formados com os conhecimentos necessários e heurísticos para poderem proceder à análise do tráfego de rede nas suas organizações – ou noutras em que efetuem auditorias – de modo a detetarem anomalias, aferir níveis de performance ou situações que coloquem em causa a segurança.

Assim, no final do mesmo, os formandos estarão aptos a:

- Identificar os principais protocolos de rede, bem como familiarizados com os modelos OSI, TCP/IP e serviços associados
- Definir formas de captura de tráfego, consoante os cenários com os quais sejam confrontados

- Proceder à captura, análise e monitorização do tráfego de rede;
- Identificar situações anómalas ou potencialmente problemáticas;
- Realizar análise aplicacional e de transações TCP
- Elaborar procedimentos de alarmística e de filtragem;
- Definir e gerar relatórios relativos ao tráfego de rede;
- Identificar os principais componentes ao nível da descodificação de pacotes;
- Analisar processos locais (Capsa);
- Realizar análise retrospetiva/forense (nChronos).

Destinatários

- Técnicos envolvidos na monitorização, administração e segurança de redes e sistemas, ou na sua auditoria;
- Técnicos em início de atividade ou que desejem aprofundar os seus conhecimentos na análise de tráfego via captura de pacotes.

Pré-requisitos

Aconselham-se conhecimentos base de redes de comunicações, protocolo TCP/IP, sendo aconselhável a compreensão de manuais na língua inglesa e respetivos termos técnicos associados ao âmbito desta formação.

Programa

- OSI & TCP/IP Models
- Network Analysis and Methods
- Capsa & nChronos description
- Preliminary real cases discussion
- Lab environment explanation and its installation
- Exploring Capsa definitions and features
- Practical exercises using Capsa captures
- Exploring nChronos definitions and features
- Practical exercises using nChronos captures
- Fully based on real packet captures, practical exercises

- OSI & TCP/IP Models
- Network Analysis and Methods

- Capsa & nChronos description
- Preliminary real cases discussion
- Lab environment explanation and its installation
- Exploring Capsa definitions and features
- Practical exercises using Capsa captures
- Exploring nChronos definitions and features
- Practical exercises using nChronos captures
- Fully based on real packet captures, practical exercises aim to:
  - Obtain real-time traffic, monitoring, network bandwidth utilization and other related information
  - Identify captured protocols and perform break-down analysis
  - Select and decode packets
  - Determine performance issues
  - Identify abnormal/suspected traffic or content
  - Perceive instructor’s generated network attacks
  - Define alerts and reports
  - Interpret statistics
  - Analyze applications
  - Identify local processes and network behavior (Capsa)
  - Perform retrospective analysis (nChronos)
  - Perform self-practice