

SNIFFING - TRACING - PROTOCOL ANALYSIS (WSSTPA)

Eđitim Hakkında

Bu eđitim, Wireshark® ve TCP/IP iletiřim analizi konusunda derinlemesine bilgi ve uygulamalı deneyim sunar. Katılımcılar, Wireshark'ın kullanımını öğrenerek TCP/IP iletiřimlerdeki en yaygın performans sorunlarının nedenlerini belirleme becerisi kazanır. Eđitim, ađ trafiđi yakalama teknikleri, analizör yerleřtirme, filtreleme, profil oluřturma, renk kuralları, grafik oluřturma, protokol alanlarının yorumlanması ve temel TCP/IP iletiřimlerinin iřlevselliđi gibi konuları kapsar. ARP, DNS, IP, TCP, UDP, ICMP, HTTP/HTTPS protokollerinin normal davranıřları ile gecikme sorunları, bađlantı kurulum endiřeleri, hizmet reddi ve gúvenlik ihlali belirtilerinin nasıl tespit edileceđi öğretilir.

Ön Kořullar

Herhangi bir ön kořul olmamakla birlikte, TCP/IP ađ temelleri, ađ cihazları ve temel ađ protokolleri hakkında bilgi sahibi olmak faydalıdır.

Eđitim Süresi

- **Eđitmen liderliđinde eđitim:** 5 gün (uygulamalı laboratuvar çalıřmalarıyla)
 - **Sanal eđitmen liderliđinde eđitim:** 5 gün (web tabanlı dersler ve uygulamalı laboratuvar çalıřmalarıyla)
-

Kimler Katılmalı?

Ađ trafiđini analiz etmek ve TCP/IP ađlarını optimize ederek sorunları gidermek isteyen herkes için uygundur.

Özellikle:

- Ađ mühendisleri
 - Bilgi teknolojileri uzmanları
 - Gúvenlik analistleri
-

Eđitim İçeriđi

Bölüm 1: Ađ Analizi Dünyasına Giriř

- Ađ analizi ve temel kavramlar

Bölüm 2: Wireshark'a Giriř

- Wireshark arayüzü ve temel özellikler

Bölüm 3: Trafik Yakalama

- Yakalama teknikleri ve analizör yerleştirme

Bölüm 4: Yakalama Filtreleri Oluşturma ve Uygulama

Bölüm 5: Global ve Kişisel Tercihleri Tanımlama

Bölüm 6: Trafiği Renklendirme

- Renk kuralları ve özelleştirme

Bölüm 7: Zaman Değerlerini Tanımlama ve Özetleri Yorumlama

Bölüm 8: Temel İz Dosyası İstatistiklerini Yorumlama

Bölüm 9: Görüntü Filtreleri Oluşturma ve Uygulama

Bölüm 10: Akışları Takip Etme ve Veriyi Yeniden Oluşturma

Bölüm 11: Wireshark Profillerini Özelleştirme

Bölüm 12: Paketleri Not Alma, Kaydetme, Dışa Aktarma ve Yazdırma

Bölüm 13: Wireshark Uzman Sistemini Kullanma

Bölüm 14: TCP/IP Analizine Genel Bakış

Bölüm 15-24: Protokol Analizi

- DNS, ARP, IPv4/IPv6, ICMP, UDP, TCP, DHCP, HTTP, FTP ve E-posta trafiği analizi

Bölüm 25: 802.11 (WLAN) Analizine Giriş

Bölüm 26: Sesli İletişim Üzerinden IP (VoIP) Analizine Giriş

Bölüm 27: Normal Trafik Modellerini Belirleme

Bölüm 28: Performans Sorunlarının Temel Nedenlerini Bulma

Bölüm 29: Ağ Adli Tıbbına Genel Bakış

Bölüm 30: Tarama ve Keşif Süreçlerini Tespit Etme

Bölüm 31: Şüpheli Trafiği Analiz Etme

Eğitim Sonunda Kazanacaklarınız

Bu eğitimi tamamlayan katılımcılar:

- **Wireshark**'ı etkin bir şekilde kullanarak ağ performansı sorunlarını tespit edebilir.
- Protokol analizi yaparak trafik davranışlarını yorumlayabilir.

- Ađ sorunlarını teŖhis ederek özüm önerileri geliŖtirebilir.
- Ađ güvenliđi ve performans analizi konularında uzmanlaŖabilir.