Using Wireshark to Analyze and Troubleshoot TCP/IP Networks Eğitimi

Süre: **5 Gün**

BİLGİNÇ
IT Academy

info@bilginc.com
bilginc.com

Using Wireshark to Analyze and Troubleshoot TCP/IP Networks, ağ trafiği analizi ve sorun giderme alanında uzmanlaşmak isteyen BT profesyonelleri için tasarlanmış uygulamalı bir eğitim programıdır. Eğitim boyunca katılımcılar, dünyanın en yaygın **Network Protocol Analyzer** araçlarından biri olan **Wireshark** kullanarak ağ paketlerini yakalama, filtreleme, analiz etme ve yorumlama becerileri kazanırlar.

Gerçek dünya senaryoları üzerinden ilerleyen eğitimde, performans sorunları, güvenlik tehditleri, ağ anomalileri ve protokol davranışları detaylı şekilde incelenir. Katılımcılar hem kablolu hem de kablosuz ağlarda trafik analizleri gerçekleştirerek karmaşık ağ problemlerini çözmek için gerekli teknik uzmanlığı geliştirirler.

Program ayrıca **Network Forensics**, **TCP/IP Analysis**, **Packet Analysis**, **Network Security Monitoring** ve gelişmiş sorun giderme tekniklerini kapsayarak katılımcıların profesyonel seviyede ağ analizi yapabilmesini sağlar. Eğitim içeriği aynı zamanda **Wireshark Certified Analyst (WCA)** sınav hedefleriyle uyumlu olacak şekilde yapılandırılmıştır.

Önkoşullar

Bu eğitimden maksimum fayda sağlamak için aşağıdaki bilgi ve deneyimlerin bulunması tavsiye edilir:

- Temel **Networking Fundamentals** bilgisi
- **TCP/IP Protocol Suite** hakkında bilgi
- Ağ güvenliği prensiplerine aşinalık
- Temel ağ analiz araçlarıyla çalışma deneyimi
- Paket analizi ve sorun giderme konusunda başlangıç seviyesinde deneyim (önerilir)

Kimler Katılmalı

Bu eğitim aşağıdaki profesyoneller için uygundur:

- **Network Engineer**
- **Network Administrator**
- **System Administrator**
- **Cyber Security Specialist**
- **SOC Analyst**
- Ağ altyapı yöneticileri
- BT operasyon ekipleri
- Yazılım geliştiriciler
- Ağ performansı ve güvenliğiyle ilgilenen teknik uzmanlar

Using Wireshark to Analyze and Troubleshoot TCP/IP Networks Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitim sonunda katılımcılar:

- **Network Analysis** süreçlerinin temel amaçlarını açıklayabilir.
- **Wireshark** kurulumunu ve yapılandırmasını gerçekleştirebilir.
- Kablolu ve kablosuz ağlarda trafik yakalayabilir.
- **Capture Filter** ve **Display Filter** yapılarını etkin şekilde kullanabilir.
- **TCP/IP**, **DNS**, **ARP**, **ICMP**, **IPv4**, **IPv6**, **UDP** ve **TCP** trafiğini analiz edebilir.
- Ağ performans problemlerini teşhis edebilir.
- Şüpheli trafik ve güvenlik olaylarını tespit edebilir.
- **Network Forensics** süreçlerinde Wireshark kullanabilir.
- Ağ performansını grafikler ve istatistikler yardımıyla değerlendirebilir.
- Komut satırı araçlarıyla gelişmiş analizler gerçekleştirebilir.

Eğitim İçeriği

Ağ Analizi ve Wireshark Temelleri

- **Network Analysis** kavramları
- Wireshark mimarisi ve kullanım alanları
- TCP/IP iletişim analizi
- Yaygın performans problemleri
- Wireshark kurulumu ve güncellenmesi
- Ağ trafiği yakalama teknikleri
- **Network Forensics** giriş

Trafik Yakalama ve Filtreleme

- Paket yakalama yöntemleri
- **Capture Filters**
- Anahtarlamalı ağlarda trafik analizi
- **Network TAP** kullanımı
- Kablosuz ağ analizleri
- Trafik filtreleme teknikleri
- Tarama ve keşif aktivitelerinin tespiti

Özelleştirme ve Gelişmiş Navigasyon

- **Custom Wireshark Profiles**
- Sorun giderme profilleri oluşturma
- Kullanıcı arayüzü özelleştirme
- Özel sütunlar ekleme
- Tercih ve görünüm ayarları
- Renk kuralları oluşturma
- Gelişmiş gezinme teknikleri

Şüpheli Trafik ve Güvenlik Analizi

- Şüpheli ağ aktivitelerinin belirlenmesi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Zararlı trafik analizi
- Güvenlik olaylarının incelenmesi
- Paket içeriklerinin değerlendirilmesi
- Trafik davranışlarının yorumlanması

Zaman Analizi ve İstatistikler

- Delta zaman analizi
- Zaman referansları
- TCP oturum zamanlamaları
- Paket zaman damgalarının incelenmesi
- Temel ve gelişmiş ağ istatistikleri

Komut Satırı ile Ağ Analizi

- Wireshark komut satırı araçları
- Trafik işleme süreçleri
- Otomatik analiz teknikleri
- Ağ tanılama işlemleri

Protokol Bazlı Trafik Analizi

- **Display Filters**
- Paket bazlı filtreleme
- Endpoint ve konuşma analizleri
- TCP/IP iletişim süreçleri
- DNS çözümleme trafiği
- ARP işlemleri
- ICMP mesajları
- UDP ve TCP analizleri

Ağ Performansı ve Sorun Giderme

- **TCP Stream Analysis**
- IO grafiklerinin oluşturulması
- TCP trend analizi
- Performans darboğazlarının belirlenmesi
- Paket kayıplarının incelenmesi
- Ağ gecikmesi ve bağlantı problemleri
- Uzman sistem (Expert System) kullanımı

Güvenlik ve Adli Ağ Analizi

- Tarama aktivitelerinin tespiti
- Keşif süreçlerinin analizi
- Şüpheli payload incelemeleri
- **Network Security Monitoring**
- Güvenlik olaylarının araştırılması
- Adli ağ analizi teknikleri