WCNA certification for Wireshark Eğitimi

Süre: **5 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Wireshark, ağ trafiğini ayrıntılı biçimde incelemek için kullanılan ücretsiz bir network protocol analyzer aracıdır. Bu uygulamalı eğitim, Wireshark kullanarak ağ sorunlarını analiz etmeye ve gidermeye yönelik kapsamlı bir çalışma sunar. Eğitim içeriği aynı zamanda katılımcıların WCNA sınavına hazırlanırken ihtiyaç duyacağı temel ve ileri seviye konulara odaklanır.

Program, RFC'lerde tanımlanan protokol ayrıntılarını ele alan **yoğun ve ileri seviye bir TCP/IP eğitimi** niteliğindedir. Özellikle TCP davranışı ve ağ performansı üzerinde durulur. Bu nedenle eğitim, TCP/IP konusunda başlangıç seviyesinde olan katılımcılardan çok, protokollerin temel çalışma mantığını ve adresleme yapılarını zaten bilen kişiler için uygundur.

Uygulamalı oturumlarda Wireshark kullanılarak gerçek veya örnek network traffic üzerinde protocol analysis gerçekleştirilir. Katılımcılar paket yakalama, filtreleme, zamanlama analizi, performans ölçümü, uygulama protokollerinin incelenmesi, kablosuz ağ trafiği, VoIP ve network forensics gibi alanlarda pratik deneyim kazanır.

Önkoşullar

Bu eğitim için zorunlu bir ön koşul eğitimi bulunmamaktadır. Ancak katılımcıların IP'nin nasıl çalıştığı konusunda iyi seviyede bilgi sahibi olması beklenir.

TCP/IP konusunda temel bilgilerini geliştirmek isteyen katılımcılar için TCP/IP foundation seviyesinde bir eğitim faydalı olabilir.

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Paketleri ve protokolleri ayrıntılı biçimde analiz edebilir.
- Wireshark kullanarak network sorunlarını tespit edip giderebilir.
- Ağ performansı problemlerini Wireshark ile belirleyebilir.
- Network forensics çalışmalarında Wireshark'tan yararlanabilir.

Eğitim İçeriği

Wireshark Nedir?

- Network analysis
- Troubleshooting
- Network traffic flows

Uygulama

- Wireshark'ın indirilmesi ve kurulması

WCNA certification for Wireshark Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Wireshark'a Giriş

- Packet capturing
- libpcap, winpcap ve airpcap
- Dissectors ve plugins
- Menüler
- Sağ tık seçenekleri

Uygulama

- Wireshark'ın temel kullanımı

Trafik Yakalama

- Wireshark ile switch ve router ortamlarında çalışma
- Remote traffic capture

Uygulama

- Paket yakalama

Capture Filters

- Capture filter uygulama
- Identifiers ve qualifiers
- Protocol, address ve byte value filtreleri
- File sets ve ring buffers

Uygulama

- Capture filter oluşturma ve kullanma

Preferences

- Configuration folders
- Global ve personal configurations
- Capture preferences
- Name resolution
- Protocol settings
- Traffic colouring
- Profiles

Uygulama

- Wireshark arayüzünü ve tercihlerini özelleştirme

Zaman Analizi

- Packet time
- Timestamps
- Packet arrival times
- Delays
- Traffic rates
- Packet sizes

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Overall bytes

Uygulama

- Yüksek latency ölçümü

Trace File Statistics

- Protocols ve applications
- Conversations
- Packet lengths
- Destinations
- Protocol usage
- Streams
- Flows

Uygulama

- Wireshark statistics araçlarının kullanımı

Display Filters

- Filtre uygulama ve temizleme
- Filter expressions
- Sağ tık ile filtre oluşturma
- Conversations ve endpoints
- Protocol filtreleri
- Filtre kombinasyonları
- Belirli byte'ların filtrelenmesi
- Regex filters

Uygulama

- Görüntülenen trafiğin filtrelenmesi

Streams

- Traffic reassembly
- UDP ve TCP conversations
- SSL traffic

Uygulama

- Stream'lerin yeniden oluşturulması

Saving ve Export

- Filtered packets
- Marked packets
- Packet ranges

Uygulama

- Paket ve trace verilerinin export edilmesi

WCNA certification for Wireshark Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

TCP/IP Analysis

- Wireshark Expert System
- DNS
- ARP
- IPv4
- IPv6
- ICMP
- UDP
- TCP

Uygulama

- Network traffic analizi

IO Rates ve Trends

- Basic graphs
- Advanced IO graphs
- Round Trip Time
- Throughput rates

Uygulama

- Grafiklerle trafik ve performans analizi

Application Analysis

- DHCP
- HTTP
- FTP
- SMTP

Uygulama

- Application traffic analizi

WiFi Analizi

- Signal strength ve interference
- Monitor mode ve promiscuous mode
- Data frames
- Management frames
- Control frames

Uygulama

- WLAN traffic analizi

VoIP Analizi

- Call flows
- Jitter
- Packet loss

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- RTP
- SIP

Uygulama

- Çağrı trafiğinin incelenmesi ve playback

Performance Problems

- Baselining
- High latency
- Arrival times
- Delta times

Uygulama

- Düşük network performansının belirlenmesi

Network Forensics

- Host forensics ve network forensics farkları
- Olağan dışı trafik modelleri
- Scan ve sweep tespiti
- Şüpheli trafik analizi

Uygulama

- Trafik signature'larının incelenmesi

Command Line Tools

- Tshark
- capinfos
- editcap
- mergecap
- text2pcap
- dumpcap

Uygulama

- Wireshark command-line araçlarının kullanımı