와이어샤크 *(Wireshark)*를 활용한 패킷분석 및 트러블슈팅

▣ 교육과정

2단계 : 와이어샤크를 활용한 패킷분석 및 트러블슈팅 (네트워크 초중급, 60시간 교육)

실무에 많이 사용하는 네트워크 트래픽을 캡처하고 분석하는 방법을 이해 할 수 있다.
각종 프로토콜 구조와 원리, 헤더 및 통신 방법에 대한 내용과 장애 발생 포인트 및 패킷 분석을
통한 문제 해결 방법과 실무에 직접 적용이 가능한 필터 기법과 비정상적인 패킷을 찾는 방법을 이해 할 수 있다.
패킷 분석을 성공적으로 마치기 위한 TCP/IP, DNS, ARP, IPv4/IPv6, ICMPv4/ICMPv6, UDP,
TCP,DHCP, HTTP, FTP, POP, SMTP, 802.11 WLAN,SIP, RTP 와 관련하여 이 프로토콜들에 대한 사례별 디스플레이 필터를 이해 할 수 있다.
성능문제나 네트워크 증거수집, 공격 감지 및 의심 트래픽 분석 기법 등 각 프로토콜의 보안 사고를 이해하고 응용할 수 있다.

▣ 학습목표

실제 네트웍안에서 이루어지는 패킷의 구조와 구성요소를 이용한 문제해결과 어플리케이션 응답 속도 검사 및 시각화를 사용한 어플리케이션의 Winsock 사용 방법 등에 대하여 숙지하고 이용할수 있도록 학습합니다.

▣ 교육진행

- 최소의 필수 이론을 습득 후 실습을 최대한 진행,
- 실습방식 : 실제 환경에서 발생할수 있는 문제를 통한 원인 및 해결방안 도출

▣ 과정강점

본 과정은 네트워크의 관련 기반 지식을 통하여, 전 세계적으로 가장 많이 사용되는 강력한 네트워크 분석 도구인 WireShark (와이어샤크) 의 안정화 Version(버젼) 및 기술화 버젼을 이용하여, 기초부터 메뉴 사용 방법 및 지원 기능을 학습하여 고급 필터링 / 네트워크 포렌식 및 스캐닝 탐지, 네트워크 분석 및 관리 업무에 필요한 트래픽을 수집, 처리하는 지식 습득을 목표로 합니다

▣ 교육대상 및 전망

- 기본 적인 Wireshark 사용자 또는 통신에 대한 기초적인 이론을 숙지하고 있으신 분
- Traffic에 대한 동작 원리를 파악하거나, 프로토콜에 대한 깊은 이해가 필요하신 분, 통신에 대한 깊은 이해를 원하시는 분
- Wireshark에 대한 추가적인 기능을 필요로 하는 분
- 네트워크 관리 및 컴퓨터 관리 분야의 관심 있는 분 및 현재 재직자
- 네트워크엔지니어 / 정보보안 / 보안관제 / 정보통신공사업체 / IT시스템관리자 / 서버엔지니어
- 각종 네트워크 헤더에 대한 구조와 인터넷 통신에 대한 깊은 지식이 필요하신 분
- 네트워크 장애 발생을 근본적으로 해결 하고 싶으신 분
- 높은 경로 지연 시간으로 인한 취약한 네트워크 성능을 파악하고 싶으신 분
- 패킷 누락을 시키는 네트워크 장비를 추적하고 싶으신 분
- 네트워크 호스트의 최적화된 설정을 검증하고 싶으신 분

▣ 강의시간표

평일 교육시간(월~금)	주말 교육시간(토, 일)
19:30 ~ 22:30 (3H)	토 : 11:30~19:30 [8H] (점심 X) 일 : 11:30~18:30 [7H] (점심 X)

* 상기 교육시간은 상황에 따라 변동이 가능합니다.
* 와이어샤크 과정 주말반 개강 예정입니다.

▣ 수강료

단계	수강료 (교재비 포함)	사업주환급 (교육수료후 환급률)		재직자 내일배움카드 본인부담금(근로자카드)	
		중소기업	대기업	중소기업	대기업
CCNA	280,000	x	x	x	
와이어샤크	395,280(30,000)	70~80%환급	대략 50~60%환급	118,590원	
CCNP(R/S)	650,000(30,000)	x	x	x	x
CCIE	2,000,000 (이론+실습 통합)	개강예정			

* 재직자 국비지원은 근로자카드(재직자 내일배움카드) 발급자 대상입니다.
* 정규과정 등록시 온라인 동영상 강의 지원 : www.studydesk.co.kr

▣ 세부진도표

[와이어샤크를 활용한 패킷분석 및 트러블슈팅]

교 육 내 용				
순서	과목명	모듈	세부과정	시간
1	와이어샤크 (Wireshark)를 활용한 패킷분석 및 트러블슈팅	Wireshark 기능	1.1 트래픽 수집 1.2 캡처 필터 생성과 적용? 1.3 전역및 개인 환경 설정 1.4 트래픽 컬러링? 1.5 시간 값 지정과 요약 해석 1.6 기본 추적 파일 통계 해석 1.7 디스플레이 필터 생성과 적용? 1.8 네트워크 기본 파일 추적 파일 통계 1.9 네트워크 Stream 분석과 데이터 조립	15
		Wireshark Packet 분석	2.1 TCP/IP 분석 개요 2.2 DNS 트래픽 분석? 2.3 ARP 트래픽 분석 2.4 IPv4/IPv6 트래픽 분석 2.5 ICMPv4/ICMPv6 트래픽 분석? 2.6 UDP 트래픽 분석 2.7 TCP 트래픽 분석? 2.9 DHCP 트래픽 분석? 2.10 HTTP 트래픽 분석? 2.11 FTP 트래픽 분석? 2.12 POP3/SMTP 트래픽 분석 2.13 802.11(WLAN) 분석 개요?	20
		Wireshark를 이용한 분석	3.1 정상 트래픽 패턴 베이스라인? 3.2 성능 문제의 가장 큰 원인 찾기? 3.3 스캐닝 탐지와 발견 처리? 3.4 의심스런 트래픽 분석? 3.5 커맨드라인 도구의 효과적인 사용	15
		Wireshark Network 분석 시나리오 연습	4.1 웹 컨텐츠 누락 분석 시나리오 4.2 네트워크 통신 불가 분석 시나리오 4.3 일관성이 없는 Application 분석 시나리오 4.4 지사간 통신 불가에 대한 분석 시나리오 4.5 소프트웨어 데이터 손상 분석 시나리오	10
합계				60