- 4차산업 대비 -

사이버보안 전문가 인재양성 과정

커 리 큐 럼

○ 세부교육일정

교육주차	강의기간	강의내용	시간
1	5일	○ 리눅스 기본 - 파일 제어 , 프로세스 제어 , 파일 관리 및 편집기 활용 - 사용자 및 그룹 관리 , 고급 권한 관리 - 디스크 관리 , 파일시스템 및 스왑 메모리 , Systemd - 로그 관리, 네트워크 관리	40
2	5일	○ 네트워크 기본 - OSI 참조 모델, TCP/IP, 서브넷팅 - 라우터와 스위치의 기본 설정 - 정적 경로 설정 - 라우팅 프로토콜: RIPv1과 RIPv2 - EIGRP, OSPF - VLAN과 Inter-VLAN 라우팅 , VTP와 STP	40
3	5일	○ 네트워크 공격 및 보안 솔루션 활용 - 네트워크 취약점 및 공격 - 네트워크 보안 실습을 위한 환경 구축 - 방화벽 구축 , 네트워크 침입 탐지/차단 시스템 - 네트워크 접근 제어 시스템	40
4	5일	○ 네트워크 포렌식 - 증거 수집 - 패킷 분석 - 네트워크 침입 탐지와 분석 - Challenge	40
총 교육시간			160

○ 일차별 교육일정

• (1주차) 네트워크 침해사고 대응 실무 과정 (40h)

	일차	교시	모듈(주제)	교육내용
	1.8 (월)	1-5교시	사용자 및 그룹 관리	- 사용자 및 그룹 정보 파일 - 사용자 및 그룹 관리 - 사용자 전환 - 사용자 패스워드 속성
		6-8교시	고급 권한 관리	- 확장 권한 - 접근 제어 리스트 (Access Control List) 소개 - 접근 제어 리스트(ACL) 설정
	1.9 (화)	1-2교시	작업 스케줄링	- 단일성 작업 예약 - 주기적인 작업 예약
		3-5교시	디스크 관리	- 디스크 기본 구조 - 디스크 이름 및 확인 - 하드디스크 파티셔닝
		6-8교시	파일시스템 및 스왑 메모리	- 리눅스 파일시스템 소개 - 파일시스템 관리 , 스왑 메모리
	1.10 (수)	1-4교시	논리 볼륨(Logical Volume) 관리	- 논리 볼륨 소개 / 생성 - 논리 볼륨요소 확인 - 볼륨 그룹 및 논리 볼륨 관리
		5-6교시	Systemd	- systemd 소개 - systemd 유닛 , systemctl 사용
		7-8교시	로그 관리	- 로그 아키텍처 (Log Architecture) - rsyslogd , systemd-journald
	1.11 (목)	1-3교시	리눅스 부트 프로세스	- 리눅스 시스템 부팅 절차 - systemd 타겟 유닛 (Target Unit) - root 패스워드 복구 , 파일시스템 문제 복구
		7-8교시	소프트웨어 패키지	- RPM(Redhat Package Manager)을 사용하여 패키지 관리 - YUM(을 사용하여 패키지 관리
	1.12 (금)	1-3교시	네트워크 관리	- 네트워크 정보 확인 , 네트워크 관리자 소개 - 네트워크 관리자도구 활용, 호스트이름(hostname) 설정
		4-5교시	OpenSSH(Open Secure Shell)	- OpenSSH 소개 , OpenSSH 설정 파일 - OpenSSH 키 기반 인증 , 원격 파일 전송
		5-6교시	NTP 서버 관리	- NTP 소개 , chrony 서비스 , 수동 시간 설정
		7-8교시	방화벽 관리	- 방화벽 소개, firewall-config 사용법 - firewall-cmd 사용법, 리치 규칙(Rich Rule)

• (2주차) 네트워크 침해사고 대응 실무 과정 (40h)

일차	교시	모듈(주제)	교육내용
1.15 (월)	1-8교시	OSI 참조 모델, TCP/IP, 서브넷팅	- OSI(Open Systems Interconnection) 참조 모델 - TCP/IP(Transmission Control Protocol/Internetwork Protocol) - 서브넷팅(Subnetting)
1.16 (화)	1-8교시	라우터와 스위치의 기본 설정	- 라우터와 스위치의 기본 설정
1.17 (수)	1-2교시	정적 경로 설정	- 디폴트 정적 경로(Default Static Route) 설정 - 경로 요약(Route Summarization) - 디버깅(Debugging) - 시스코 탐색 프로토콜(CDP; Cisco Discovery Protocol)
	3-5교시	라우팅 프로토콜: RIPv1과 RIPv2	- 거리 벡터 라우팅 프로토콜(Distance Vector Routing Protocol) - 링크 상태 라우팅 프로토콜(Link State Routing Protocol) - RIPv1 , RIPv2 - 라우트 포이즈닝(Route Poisoning)과 포이즈닝 리버스(Poisoning Reverse) - 디폴트 경로(Default Route) 설정하기
	6-8교시	EIGRP	- EIGRP 설정 , 자동 경로 요약 - EIGRP 메트릭 값 , EIGRP DUAL - EIGRP의 다른 기능
1.18 (목)	1-4교시	OSPF	- OSPF
	5-8교시	VLAN과 Inter-VLAN 라우팅	- VLAN(Virtual LAN), 트렁크(Trunk) - Native VLAN, DTP(Dynamic Trunking Protocol) - Inter-VLAN , Port-Security 설정
1.19 (금)	1-3교시	VTP와 STP	- VTP(VLAN Trunking Protocol) - STP(Spanning Tree Protocol)
	4-6교시	접근 제어 목록	- 표준 ACL , 확장 ACL , Named 표준 ACL - Named 확장 ACL, TCP Established , ACL 중간 삽입 - 락-앤-키(Lock-and-Key) 인증, RACL(Reflexive ACL) - 시간 기반의(time-based) ACL
	7-8교시	DHCP, NAT, IPv6	- DHCP , NAT(Network Address Translation) - IPv6, RIPng 설정 , OSPFv3 설정 - IPv6를 위한 EIGRP 설정

• (3주차) 네트워크 침해사고 대응 실무 과정 (40h)

일차	교시	모듈(주제)	교육내용
1.22 (월)	1-3교시	네트워크 기본 취약점	- 프로토콜별 취약점
	4-6교시	foot printing	- 네트워크 자원 정보 수집 - 스캐닝, 배너그래빙
	7-8교시	sniffer	- sniffing 의 원리 - sniffing 도구의 활용
1.23 (화)	1-8교시	spoof	- ARP Spoofing, Ip spoofing, DNS spoofing - 은닉채널 , 프록시 , 터널링, - Session Hijacking
1.24 (수)	1-3교시	MITM	- SSHMITM - SSLMITM
	4-6교시	DoS	- Ping of Death , Bonk, Boink, Teardrop - Land , Smurf , SYN Flooding
	7-8교시	DDoS , DrDoS	- DDoS 공격 이해, DrDoS 공격 이해 - Layer 7 DDoS
1.25 (목)	1-4교시	보안솔루션 소개	- 보안솔루션별 특징 - 보안솔루션별 특장점
	5-8교시	방화벽 구축	- 방화벽 설치 및 구성 - 방화벽 운영 기술
	5-8교시	네트워크 / 호스트 기반	- IDS / IPS 구축 - IDS/ IPS 설치 및 구성
1.26 (금)	1-3교시	웹 방화벽 구축	- 웹방화벽 설치 및 구성 - 웹방화벽 운영
	4-8교시	네트워크 접근제어	- 네트워크 접근제어 시스템 구축 - 네트워크 접근제어 운영

• (4주차) 네트워크 침해사고 대응 실무 과정 (40h)

일차	교시	모듈(주제)	교육내용
1.29 (월)	1-2교시	네트워크 포렌식 개론	- 디지털 증거상 개념 - 네트워크 증거에 관한 과제 - 네트워크 포렌식 조사 방법론
	3-8교시	기술적 원리	- 네트워크 기반 증거의 출처 - 인터 네트워킹의 원리 - 인터넷 프로토콜 스위트
1.30 (화)	1-2교시	증거 수집	- 물리적 감청 - 트래픽 수집 소프트웨어 - 액티브 수집
	3-8교시	패킷 분석	- 프로토콜 분석 - 패킷 분석 - 흐름 분석 - 상위 계층 트래픽 분석
1.31 (수)	1-4교시	통계적 플로우 분석	- 프로세스 개요 - 센서 , 플로우 기록 내보내기 프로토콜 - 수집과 통합, 분석
	5-8교시	무선: 플러그가 뽑힌 네트워크 포렌식	- IEEE 2계층 프로토콜 시리즈 ,무선 접근 지점 - 무선 트래픽 캡처와 분석 - 일반적인 공격 , 무선 장비 위치
2.1 (목)	1-4교시	네트워크 침입 탐지와 분석	- NIDS/NIPS를 조사하는 이유 - 일반적인 NIDS/NIPS 기능 - 탐지 모드 , NIDS/NIPS 종류 - NIDS/NIPS 증거 획득 , 종합적인 패킷 로깅
	5-8교시	이벤트 로그 통합과 상관 관계, 분석	- 로그의 종류 - 네트워크 로그 아키텍처 ,증거 수집과 분석
2.2 (금)	1-3교시	스위치와 라우터, 방화벽	- 저장 매체 , 스위치 - 라우터 , 방화벽, 로깅
	4-6교시	웹 프록시	- 웹 프록시 기능 - 증거, 스퀴드 - 웹 프록시 분석, 암호화된 트래픽
	7-8교시	리눅스 침해사고 분석	- Live Reponse - Live Data Collection

※ 상황에 따라 진도 및 커리큘럼이 달라 질수 있습니다.