개정일 : `23. 12. 19.

직 종 설 명 서

▣ 직종명 : 사이버보안 (Cyber Security)

순 서

1 직종정의

○ 사이버 보안은 정보보안 업무를 주로 수행하는 직업군 또는 그 기술을 총칭하는 용어로 조직의 컴퓨터 시스템과 연결된 네트워크를 보호하고 민감한 정보 및 데이터에 액세스하거나 도용하는 것을 방지하는 직업 또는 작업을 말함

2 작업범위

○ 조직의 컴퓨터 및 네트워크 시스템을 방어하기 위해 시스템 내부의 민감한 데이터에 대한 해킹을 모니터링하고 이를 방어할 수 있어야 한다.

○ 방어작업을 위해 기본적으로 방화벽을 설치하고 구성된 프로파일을 설정할 수 있어야 한다.

○ 데이터를 해킹으로부터 방어하기 위해 암호화 소프트웨어를 통해 비밀성 및 무결성을 적용할 수 있어야 한다.

○ 해킹과 같은 외부 침입이 발생하였을 때 이를 감지하고 모니터링하여 분석할 수 있어야 한다.

○ 주어진 환경에 모의침투 테스트를 진행하고 해당 네트워크에 존재하는 취약점을 찾아내고 보완할 수 있어야 한다.

○ 조직의 재해복구 수행 계획을 설계할 수 있어야 한다.

○ 공격이나 재해 상황 이후에 적절한 절차에 의해 복원 절차를 수행할 수 있어야 한다.

○ 사이버 공격에 대비하기 위해 항상 새로운 지식과 기술을 습득해야 하며 이를 통해 위협에 대응할 수 있는 계획을 수립할 수 있어야 한다.

3 과제내용 및 시간

○ 지방기능경기대회

순번	과 제 명	주 요 작 업 내 용	과제시간 (단위:시간)
1	이론시험 (2024년까지)	시스템보안, 네트워크 보안, 어플리케이션 보안, 정보보안 일반에 대한 이론시험	2
2	취약점 분석 및 모의침투 테스트 (2025년부터)	구성된 시스템의 취약점을 분석하기 위해 모의침투 테스트를 수행하고 이에 대한 취약점을 분석하는 과제(전국기능경기대회 보다 범위 축소) • 시스템 취약점 • 서비스 취약점	4
3	네트워크 보안 장비 설정	요구하는 시스템 구성에 따라 네트워크 및 인증에 해당하는 기능을 보안장비에 설정 • 구성에 따른 네트워크 보안 장비 설정 • 보안 이벤트 모니터링 (단, 패킷트레이서 시뮬레이터를 활용한 네트워크 보안 설정)	4
4	인프라 환경 설정 및 보안 강화	시스템 및 네트워크 구성을 계획한 후 이에 대한 보안을 강화하기 위한 환경설정 및 보안강화 • 서버 인프라 보안 강화 • 서비스 보안 강화	4
계			10(2025년부터 12)

○ 전국기능경기대회

순번	과 제 명	주 요 작 업 내 용	과제시간 (단위:시간)
1	인프라 환경 설정 및 보안 강화	시스템 및 네트워크 구성을 계획한 후 이에 대한 보안을 강화하기 위한 환경설정 및 보안강화 • 서버 인프라 보안 강화 • 서비스 보안 강화	4
2	네트워크 보안 장비 설정	요구하는 시스템 구성에 따라 네트워크 및 인증에 해당하는 기능을 보안장비에 설정 • 구성에 따른 네트워크 보안 장비 설정 • 보안 이벤트 모니터링 • SNORT 적용	4
3	취약점 분석 및 모의침투 테스트	구성된 시스템의 취약점을 분석하기 위해 모의 침투 테스트를 수행하고 이에 대한 취약점을 분석하는 과제 • 시스템 취약점 • 네트워크 취약점 • 서비스 취약점	4
계			12

구분	(1~2주전)	(토)	(일)	대회기간				
				1일차(월)	2일차(화)	3일차(수)		별도 일정
지방대회			경기장 점검	사전 준비	경기진행(3일간)		채점완료 결과발표	
전국대회	기술위원회의/ 본부요원교육		경기장 점검 및 사전준비	경기진행(3일간)			채점완료 결과발표 자체 시상식	폐회식

4 과제 작업내용

1) 인프라 환경 설정 및 보안 강화(지방/전국 공통)

항목	세부내용
기본 사항	- IT 위험 관리 표준, 정책, 요구사항 및 절차 숙지 - 사이버 방어 및 취약점 평가 도구의 세부 기능 - 컴퓨터 언어, 프로그래밍, 테스트, 디버깅 및 개념 - 프로그램 개발에 적용되는 사이버 보안(시큐어 코딩) 및 개인정보보호 원칙
개인 준수 원칙	- 전반적인 프로그램 테스트 및 평가 절차를 설계하고 문서화 할 때 사이버 보안 및 개인정보보호 원칙을 준수하고 이를 조직의 요구사항에 적용(기밀성, 무결성, 가용성, 인증, 부인 방지 등의 보안 원칙 준수)
운영 / 유지관리	- SQL (구조적 쿼리 언어) 및 데이터베이스 시스템과 같은 쿼리 언어 활용 - 데이터 백업 및 복구, 관리 및 데이터 표준화 정책 - TCP / IP, 동적 호스트 구성, DNS (Domain Name System) 및 디렉토리 서비스와 같은 네트워크 프로토콜 - 방화벽 개념 및 기능에 대한 메시지 검색, 데이터 손실 보호 검색, 가속화 된 암호화 작업, IPSec 및 SSL 등의 보안 프로토콜, 구성 요소 및 원칙 활용 - IT 사용자 보안 정책 (예 : 계정 생성, 비밀번호 규칙, 액세스 제어) - IT 보안 원칙 및 방법 (예 : 방화벽, 완충 영역, 암호화 등) - 인증, 권한 부여 및 액세스 제어 방법 등
시스템 설치 및 관리감독	- 서버 구성 (하드웨어 및 소프트웨어)을 설치, 구성, 문제 해결 및 유지 관리하여 기밀성, 무결성 및 가용성을 보장 - 계정, 방화벽 및 패치 관리 - 액세스, 비밀번호 및 계정 생성 및 관리 제어

보호 및 방어	- 파일 시스템 구현 (예 : NTFS (New Technology File System), 파일 할당 테이블 (FAT), 파일 확장자 [EXT]) 등 - 시스템 파일 (예 : 로그 파일, 레지스트리 파일, 구성 파일)에 관련 정보와 해당 시스템 파일을 찾을 수 있는 위치를 포함 - 인증, 권한 부여 및 액세스 방식 (예 : 역할 기반 액세스 제어, 필수 액세스 제어 및 임의 액세스 제어). - 다양한 출처에서 수집 한 방어 조치 및 정보를 사용하여 정보, 정보 시스템 및 네트워크를 위협으로부터 보호하기 위해 네트워크 내에서 발생하거나 발생할 수 있는 이벤트를 식별, 분석 및 보고 - 효과적으로 인프라의 하드웨어 및 소프트웨어를 테스트, 구현, 배포, 유지관리 및 검토 - 승인되지 않은 활동을 적극적으로 개선하기 위해 네트워크를 모니터링 - 즉각적이고 잠재적인 위협을 완화하기 위해 위기 또는 긴급 상황에 대응 - 위협 및 취약성 평가 수행
분석 기능	- 사이버 위협 행위자 및 공격 방법 - 다양한 해킹 활동을 탐지하는 데 사용되는 방법과 기술 - 사이버 인텔리전스 / 정보 수집 기능 및 리포지토리 - 사이버 위협 및 취약점 - 네트워크 보안 기본 사항 (예 : 암호화, 방화벽, 인증, 허니팟, 경계 보호) - 취약성 정보 보급 출처 (예 : 경고, 권고, 게시판) - 수집된 정보를 분석하여 취약점과 악용 가능성을 식별

수집 및 운영	- 수집 전략, 기술 및 도구 - 사이버 인텔리전스 / 정보 수집 기능 및 리포지토리 - 정보 요구 및 수집 요구 사항을 번역 및 추적 - 사이버 운영 전략, 리소스 및 도구 - 통합 정보 및 사이버 공간 운영을 위한 전체 운영 범위에서 전략 및 운영 수준 계획 설정
조사	- 위협 조사, 보고, 조사 도구 및 관련 법률 / 규정 - 악성 코드 분석 개념 및 방법론 - 전자 증거를 수집, 포장, 운송 및 저장하는 프로세스 - 영구 데이터의 유형 및 수집 - 디지털 포렌식 데이터 처리의 개념과 실습 - 디지털 포렌식 데이터의 유형 및 인식 방법 - 운영 체제 구조 및 운영에 대한 사이버 보안 침해의 특정 운영 영향

2) 네트워크 보안 장비 설정

가. 지방대회

항목	세부내용
구성에 따른 네트워크 보안 장비 설정	- 패킷트레이서 최신버전에서 제공하는 CCNA R&S(200-301) 보안 수준
보안 이벤트 모니터링	

나. 전국대회

항목	세부내용
방화벽 등의 보안 장비 설치	- 방화벽 등의 보안장비 설치, 구성, 테스트, 운영, 유지 관리, 및 관리

	- 인터페이스 설정 및 Ingress, Egress 구성 및 기본 보안 정책 관리 - 접속 제어, 패스워드, 계정 생성 및 관리 책임 등을 포함한 사용자 계정, 인증 등의 관리 - 기밀유지, 무결성, 가용성을 확보하기 위해 필요한 보안 구성 요소들(하드웨어와 소프트웨어)을 설치, 구성, 문제해결, 유지 관리 - 내/외부망을 분리하기 위한 5-Tuple 기반의 보안 정책 설정 - 침입차단시스템 구동을 위한 환경 설정 및 보안 정책 설정 - 분산서비스거부공격 대응을 위한 환경 설정 및 보안 정책 설정 - IPSec 또는 SSL 보안장비의 암호화 설정 및 동작 구성
보안 장비 모니터링	- 보안장비 운용에 따른 보안 이벤트 모니터링 - 보안 이벤트 내용 분석 및 재발방지 조치 설정 - 모니터링 툴을 활용한 보안 로그 분석 및 보안 이벤트 분석

3) 취약점 분석 및 모의침투 테스트(전국)

항목	세부내용
모의침투 테스트	- 토폴로지, 프로토콜, 구성 요소 및 원칙을 포함한 네트워크 보안 아키텍처 개념 - 취약점을 식별하기 위한 표준 및 조직적으로 인정된 분석 원칙, 방법 및 도구 활용 - 위협 조사, 보고, 조사 도구, 법률 및 규정 - 사이버 방어 및 취약성 평가 도구 및 해당 기능 - 공격 도구 (예 : 스니퍼, 키로거) 및 기술 (예 : 백도어 액세스, 데이터 수집 / 노출, 다른 시스템에 대한 취약성 분석 수행)의 구조, 접근 및 전략
취약점 분석	- 취약성 정보 보급 출처 (예 : 경고, 권고, 게시판) - 수집된 정보를 분석하여 취약점과 악용 가능성을 식별 - 다양한 출처에서 수집 한 방어 조치 및 정보를 사용하여 정보, 정보 시스템 및 네트워크를 위협으로부터 보호하기 위해 네트워크 내에서 발생하거나 발생할 수 있는 이벤트를 식별, 분석 및 보고

4) 이론 시험(지방-2024년까지)

항목	세부내용
시스템보안	- 클라이언트 보안 관리 - 서버 보안 관리
네트워크 보안	- 네트워크 개념 이해 - 네트워크의 활용 - 서비스 거부(DoS) 공격 - 분산 서비스 거부(DDoS) 공격 - 스캐닝 - 스푸핑 공격 - 스니핑 공격 - 원격접속 공격 - 보안 프로토콜 이해 - 보안 솔루션 이해
어플리케이션 보안	- FTP 보안 - 메일 보안 - 웹 보안 - DNS 보안 - DB 보안 - 전자상거래 보안 기술

정보보안 일반	- 인증 - 접근통제 - 키 분배 프로토콜 - 전자서명 - 암호 알고리즘 - 해시함수 - 정보보호 및 개인정보보호특성 이해 - 정보보호 및 개인정보보호법 체계

5 과제출제 및 공개에 관한 사항

1) 과제출제범위

순번	과제명	출제기준	비고
1	인프라 환경 설정 및 보안 강화	과제 작업범위 내에서 문제출제 (별첨 3 예시문제 참조)	• 모든 과제는 정해진 경기시간 내에 해결할 수 있는 수준 및 분량이어야 한다.
2	네트워크 보안 장비 설정		
3	취약점 분석 및 모의침투 테스트		
4	이론 시험 (2024년 지난기능경기대회까지만 유지 - 2025년부터 취약점 분석 및 모의침투 테스트로 대체)	시스템보안, 네트워크 보안, 어플리케이션 보안, 정보보안 일반 (별첨 2 예시문제 참조)	• 이론시험은 객관식 4지선다형식으로 40문제(분야별 10문제) 출제

2) 과제출제 방법

- 지방기능경기대회와 전국기능경기대회 과제는 한국산업인력공단 기술자격출제실에서 출제하는 것을 원칙으로 한다.

  - 단, 문제의 난이도나 객관성이 부족할 경우 추가적인 문제를 각 시도에서 추가 제출할 수 있다.

- 전국기능경기대회 1과제와 2과제는 독립된 과제로 출제한다.

3) 과제공개에 관한 사항

- 공개시기 : 전국 및 지방대회 30일 전 과제 공개
- 공개방법 : 마이스터넷을 통해 공개
- 공개범위

  - 지방기능경기대회 : 이론시험(1과제)는 출제범위 공개, 네크워크 보안장비 설

정(2과제) 과제 및 채점 기준 공개, 인프라 환경 설정 및 보안강화(3과제) 채점 기준 공개**(문제를 해결하기 위한 서버 이미지를 함께 공개하되 대회 당일 공개되어야만 하는 부분은 제외하고 공개 가능)**

- 전국기능경기대회 : 과제 / 채점기준 공개를 원칙으로 하되 취약점 분석 및 모의침투 테스트(3과제)는 도면(구체적)만 공개**(문제를 해결하기 위한 서버 이미지를 함께 공개하되 대회 당일 공개되어야만 하는 부분은 제외하고 공개 가능)**

• 최종과제는 경기 시작 전 과제 및 채점기준표를 함께 공개. 단, 채점기준표 공개로 답이 공개될 수 있는 과제는 과제 및 주제만 공개

4) 과제수정에 관한 사항

• 대회 당일에 공개된 과제는 기능경기대회관리규칙에 따라 수정할 수 있다.

6 경기진행 절차

1) 기본방침

(1) 기능경기대회관리규칙, 사이버보안 직종설명서, 시행자료, 경기과제, 채점기준표, 마이스터넷 홈페이지 등 사전 관련 근거에 의해 경기를 운영하여야 하며, 이를 위반하여 경기를 진행할 수 없다.

- 심사위원과 선수 및 지도교사는 경기시작 전 위 관련 규칙 및 근거 문서를 열람해야 하며, 모두 숙지한 것으로 간주한다.
- 그럼에도 불구하고, 위 관련 근거에서 규정하지 않은 사항 또는 원활한 경기 운영을 위해 수정이 필요할 시 심사위원의 협의에 의해 결정한다.
- 심사위원의 협의 사항이 있을 시 심사위원 전원 동의로 결정하고, 전원 동의가 어렵거나 심사위원 부재 등 협의 및 합의가 어려울 시 심사장이 분과장과 협의하여 결정한다.

(2) 심사장은 원활한 경기진행을 위하여 각 심사위원에게 별도의 직책을 정하여 적절한 임무를 부여할 수 있다.

(3) 선수, 심사위원, 대회 관계자 모두는 투명하고 깨끗한 경기가 될 수 있도록 노력하며 안전이 우리의 최종 목표라는 생각으로 경기장 안전에 최선을 다한다.

2) 선수 등번호부여 및 장비점검

(1) 선수 등번호 부여 및 장비점검 시간에 선수들은 경기장에 입실하여 심사장 및 심사위원의 지시에 따라 선수지참 장비에 점검을 받도록 한다.

(2) 선수 등번호는 추첨을 통하여 결정하며 등번호가 선수 자리 배정 번호로 사용된다.

(3) 선수는 등번호 추첨에 따른 자리 배정이 창측 또는 복도측 등 개인적으로 불편한 자리가 배정될 수 있음을 인지하고 추첨결과에 이의를 제기할 수 없다.

(4) 선수지참 장비

- 선수는 사이버보안 직종설명서와 시행 자료에서 정한 규격의 장비와 수량만 경기장에 반입할 수 있다.
- 선수는 데이터 저장기능이 없는 본인의 키보드와 마우스를 지참하여 심사위원의 승인 후 사용할 수 있다.
- 선수는 어떤 경우에도 데이터 저장기능 또는 촬영 기능이 포함된 기기나 장비를 휴대하거나 사용할 수 없다(예, USB 볼펜, 구글글래스, 스마트워치 등).
- 선수는 블루투스 기능이 없는 이어폰/헤드폰을 반입하여 음악을 들을 수 있다.

(5) 선수지참 장비는 시행자료를 토대로 점검을 마친 후 봉인한다.

(6) 모든 장비점검을 마친 후 경기장에서 제공되는 장비(컴퓨터) 및 소프트웨어(운영체제)를 통하여 장비의 이상 유무를 확인 후 지급된 장비 및 소프트웨어가 있을 때 즉시 교체 받을 수 있도록 한다.

(7) 지급, 지참재료 및 공구 확인(검사) 시간에 선수는 반드시 본인의 지급, 지참재료와 공구의 이상 유무를 확인해야 하며, 본인의 확인 잘못으로 인한 오작동 및 작동 불능이 생길 경우 모든 책임은 선수에게 있다.

(8) 경기에 필요한 모든 소프트웨어는 대회 본부에서 제공한다.

3) 과제선정 및 수정

(1) 최종 경기과제는 각 과제별 경기 당일에 공개된다.

(2) 과제 진행 및 채점 중 오류가 발견된 경우, 해당 문항은 만점처리 한다.

4) 경기진행

(1) 모든 심사위원은 휴대전화, 인터넷 등 사용가능하나 과제파일 및 채점결과 등에 대해서는 접근할 수 없다.

(2) 심사위원은 경기 중 특정 선수에게 불필요한 질문이나 행동을 삼가도록 한다.

(3) 선수가 손을 들어 질문을 하거나 협조를 요청할 때 선수가 소속된 시·도 심사위원을 제외한 2명 이상의 심사위원이 동행해야 하며, 질의/응답 기록지를 통하여 그 내용을 기록으로 남겨 추후 누구나 열람할 수 있도록 한다. 아울러 질문 내용이 모든 선수에게 알려야 할 사항이라면 심사장에게 보고 후 모든 선수에게 공지할 수 있도록 한다.

(4) 선수는 이해 못하는 어떠한 질문도 할 수 있으며, 심사위원(장)은 대답할 의무가 있다. (단, 질문 내용이 문제에 대한 답을 요구할 경우는 심사위원 협의 후 답변 여부를 결정할 수 있다.)

(5) 심사위원은 경기장 내에서 사진 촬영이 가능하다. 단 촬영된 사진이 채점의 감점 요인으로 작용할 수 없으며 촬영된 사진은 직종홈페이지 및 SNS를 통하여 공개할 수 있다.

(6) 선수가 안전 불이행으로 3차례 이상 경고를 받고도 계속 시정이 되지 않을 경우 선수는 안전교육을 받은 후 경기를 치를 수 있다. 안전교육 시간은 10분 이내로 하며 경기시간에 포함된다.

(7) 심사위원은 심사위원간 합의된 사항에 대하여 심사장이 발표 이전에 밖에 있는 지도교사 등에서 미리 알리거나 본인의 의견이 관철되지 않는다고 해서 욕설 또는 폭력을 행사 하는 등 심사위원의 품위를 해 하는 행동을 할 경우 분과장 및 기술위원장에게 보고 후 심사 채점에서 제외시킨다.

(8) 경기진행과 관련한 지도교사의 개인적인 의견은 심사의원 또는 심사장에게 직접 제안할 수 없으며 지도교사협의회의 회장을 통하여 제안할 수 있다.

(9) 경기 중, 경기 후 선수, 지도교사, 심사위원의 명백한 부정행위가 발각되면 대회 규정에 따라 엄격히 처리한다.

(10) 경기장은 경기에 지장을 초래하지 않는 범위 내에서 최대한 개방한다.

단, 참관자가 경기 중인 선수 근처에 접근하는 것은 금지한다. 만약 선수 근처에 접근할 필요성이 발생할 경우 2명 이상의 심사위원이 동행하여야 한다.

(11) 선수는 경기 시작 10분 전에 경기장에 도착해야 하며, 경기시작부터 종료시간까지 자신의 등번호와 일치하는 작업대에 앉아 과제를 수행한다.

(12) 선수는 경기장 입장 시 관리위원에게 모든 저장 장치 및 휴대폰을 전원 OFF 상태로 보관 후 경기장에 입장할 수 있다. (적발 시 부정행위로 간주한다.)

(13) 과제가 종료된 선수는 먼저 경기장에서 퇴실할 수 있다.

(14) 선수가 경기 중 화장실 출입이 필요한 경우 심사위원에게 요청하여야 하며, 심사위원은 선수를 화장실까지 안내하여 부정행위 또는 사고가 발생하지 않도록 감독하여야 한다. 화장실 출입에 소요되는 시간은 선수의 경기시간에 포함되며 별도의 추가시간을 제공하지 않는다.

(15) 경기 중 장비에 문제가 발생한 경우 즉시 심사위원에게 알려야 하며, 장비의 결함이 확인되면 대체장비로 교체 받아 경기를 계속할 수 있다. 이때 소요되는 시간은 경기시간에 포함되지 않으며 추가시간을 제공한다.

(16) 선수는 경기 중 돌발 상황(정전)에 대비하여 항상 작업내용을 수시로 저장하여야 한다. 본인의 실수로 인하여 설정 파일이 손상된 경우 선수 본인의 책임이며 추가시간 또한 제공되지 않는다.

(17) 경기시간이 점심시간을 경과하여 진행되는 만큼 지도교사는 선수에게 간식을 제공할 수 있다. 단, 지도교사가 직접 선수에게 전달할 수 없으며 2명 이상의 심사위원이 내용물을 확인한 후 전달하여야 한다.

(18) 심사장은 위 모든 사항을 경기장 이탈 없이 감독하며 심사위원의 업무 수행이 적절히 이루어지고 있는지 관리하며 관리위원과 기능경기팀의 활발한 업무

공유가 이루어질 수 있도록 한다.

(19) 채점순서는 경기 종료 후 추첨을 통해 선정하도록 한다.

(20) 부정행위 처리기준

- 부정행위에 관련된 사항은 기능경기대회관리규칙을 따른다.

7 경기장 구성 및 시설목록

1) 경기장 구성

○ 1인당 소요면적 : 6.6㎡ (2 평 이상)

2) 경기장 시설목록

순번	품목	규 격	수량		비고
			지방	전국	
1	작업대	1800×600×720㎜	선수수x 1	선수수x 1	
2	의자	사무용 의자	선수수x 1	선수수x 1	
3	전원	6구 멀티 콘센트 (전원 안전덮개 있는 모델) * 전원용량 =선수 수 x 1.0 KW	선수수x 1	선수수x 1	
4	보안장비 (소규모용)	HardWare 타입 통합보안장비 - Intel Celeron J1900 2.0GHz(4Core) 이상 - 방화벽 기능, L3 라우팅 기능, NAT 기능 - VPN 기능, IPS/IDS 기능, NIC 4Port 이상 - HA(High Availability) 기능		4대	예비용 4대
5	컴퓨터(PC)	CPU : 64bit 4Core 8Thread (3.0 GHz) 이상 RAM : 64GB 이상 SSD : 512GB 이상 OS : Windows 10 이상 NIC : 1Gbps이상 x 1 Port(전국대회) GPU : 1개 이상의 HDMI Port가 있는 GPU USB 3.1 이상 2포트	선수수x1 예비2	선수수x2 예비8	'심사용 4대 예비용 4대
6	모니터	해상도 1920 x 1080 이상 HDMI 포트 1개 이상	선수수x1 예비2	선수수x 2 추가8대	심사용 4대 예비용 4대
7	L2 Switch	1Gbps 8Port이상		선수수x 2	예비용 4대
8	LAN Cable	UTP LAN Cable(CAT.6) 2M		선수수x6	예비용 4개
9	OS	취약점 분석용 : Kali Linux - "과제출제 기준" 의 최신버전		선수수x 1	
		시스템 구축용 : Ubuntu Linux - "과제출제 기준" 의 최신버전 Windows server : Windows server 2019 Windows PC - Windows 10 pro 20H2 이상	선수수x 1	선수수x 1	
10	Software	VMWare : VMWare Workstation Pro - "과제출제 기준" 의 최신버전 VirtualBox : VirtualBox - "과제출제 기준" 의 최신버전	선수수x 1	선수수x 1	심사용 2대
11	Software	PuTTY : Windows Installer - "과제출제 기준" 의 최신버전	선수수x 1	선수수x 1	
12	Software	WireShark : Windows Installer - "과제출제 기준" 의 최신버전		선수수x 1	
13	Software	패킷트레이서 : windows - "과제출제 기준" 의 최신버전	선수수x 1		
14	인터넷 회선	인터넷이 가능한 IP Address	4	4	심사용
15	프린터	Color Laser A4 인쇄 복합기	2	2	심사용
16	프로젝터	해상도 : 풀HD 이상 밝기 : 2,000안시 이상 명암비 : 15,000:1 이상		1	심사용
17	스크린	150인치 이상 스크린		1	심사용

3) 선수지참 목록

순번	품목	규 격	수량		비고
			지방	전국	
1	보안장비 (소규모용)	HardWare 타입 통합보안장비 - Intel Celeron J1900 2.0GHz(4Core) 이상 - 방화벽 기능, L3 라우팅 기능, NAT 기능 - VPN 기능, IPS/IDS 기능, NIC 4Port 이상 - HA(High Availability) 기능		선수수x 2	선수 지참

※ 하드웨어 및 소프트웨어는 매년 Upgrade를 한다.

※ 모든 경기용 소프트웨어는 대회장에서 제공함.

※ 가상화 소프트웨어는 문제출제 시 사용하는 프로그램명과 버전을 제공함.

4) 탄소중립을 위한 우리의 노력

❍ 경기장(개인공간 포함) 크기 축소를 위한 노력

❍ 사용 공구 목록 및 재료목록 최소화를 위한 노력

❍ 과제축소를 위한 노력(난이도를 낮추지 않는 범위에서 지속적으로 노력)

❍ 경기 시간 단축을 위한 노력

❍ 탄소중립에 필요한 직종 세부 계획

① 경기시간 단축으로 탄소량 줄이기

② 공구사용을 줄여 경기용 화물무게 줄이기

③ 전기 사용량 줄이기(전등, 컴퓨터, 공구 등 불필요한 전기 소모 줄이기)

④ 실내 에어컨 사용량 줄이기(28℃ 이상 유지)

⑤ 발전기 사용을 안 하거나 사용 시간을 줄이기

⑥ 물 사용량 줄이기(절수 장치 부착 등)

⑦ 가스 사용량 줄이기(부탄가스, LPG, 아세칠렌, 에어컨 냉매, 스프레이 등)

⑧ 친환경 재료 사용하기(페인트, 시너, 시멘트, 오일 등)

⑨ 경기용 재료를 줄이고 재사용하기

⑩ 쓰레기 배출량 줄이기(본인이 발생시킨 쓰레기 전량 수거해가기)

8 지급재료목록

1) 지급재료목록

순번	품목	규 격	수량	비고
1	이동저장장치	USB 3.1이상 128GB 이상	선수 수	과제수거용

9 채점에 관한 사항

1) 과제별 배점기준

지방대회(2024년까지)			전국대회		
순번	과 제 명	배 점	순번	과 제 명	배 점
1	이론 시험	20	1	인프라 환경 설정 및 보안 강화	30
2	네트워크 보안 장비 설정	40	2	네트워크 보안 장비 설정	30
3	인프라 환경 설정 및 보안 강화	40	3	취약점 분석 및 모의침투 테스트	40
계		100	계		100

지방대회(2025년부터)			전국대회		
순번	과 제 명	배 점	순번	과 제 명	배 점
1	취약점 분석 및 모의침투 테스트	40	1	인프라 환경 설정 및 보안 강화	30
2	네트워크 보안 장비 설정	30	2	네트워크 보안 장비 설정	30
3	인프라 환경 설정 및 보안 강화	30	3	취약점 분석 및 모의침투 테스트	40
계		100	계		100

※ 과제별 배점은 난이도에 따라 조정할 수 있다.

2) 배점등급

• 채점항목별 부분점수가 가능할 경우 부분점수에 대한 명시가 되어야 한다.

3) 심사채점방법

(1) 경기 전 심사위원 간 합의되지 않은 사항은 채점 시 어떠한 영향력도 미칠 수 없다.

(2) 경기 종료 후 채점은 조별로 나누어 심사장이 부여한 조별 채점항목을 채점하며, 각 시·도 소속의 심사위원의 자신의 시·도 선수의 채점 시 채점 조에 편성되

지 않은 예비 심사위원이 그 역할을 대신할 수 있도록 한다.

(3) 각 심사위원은 본인이 부여받은 그룹 및 해당 선수들의 경기결과를 채점을 한다. 채점 중 다른 그룹으로 이동할 수 없으며, 자리를 비울 경우는 심사장에게 보고 후 다른 심사위원에게 채점을 부탁하고 비워야 한다. 심사장의 허가 없이 다른 채점그룹으로 이동할 경우 부정행위로 간주하여 채점 심사에서 제외시킨다.

(4) 부정행위로 탈락한 선수를 제외한 모든 선수의 채점은 작업한 부분까지 채점이 이루어져야 한다.

(5) 채점은 심사장이 제공한 보조채점표에 직접 채점해야 하며, 개인적으로 메모한 채점은 인정되지 않는다.

(6) 대표로 나온 시·도 또는 경쟁 시·도 선수의 작업물을 편파적으로 채점하지 않으며 객관적이고 공정한 채점을 해야 한다. 이를 어길 시 심사채점에서 제외된다.

(7) 선수 및 선수의 지도교사는 자신의 과제에 대한 채점을 참관할 수 있지만, 채점 진행 과정에 개입 또는 심사의원에게 이의를 제기할 수 없다. 채점의 공정성에 문제가 있다고 생각되면 심사장에게 이의를 제기하고 이의제기 내용이 타당하면 심사장은 심사위원에게 재채점을 지시할 수 있다.

(8) 모든 채점이 끝나면 선수 본인과 심사위원은 채점표에 확인(서명)하고 이의가 있으면 바로 해결한다. 서명이 완료된 후 이의 제기는 수용하지 않는다.

(9) 모든 채점은 공정하게 이루어져야 하며 채점기준표를 준수하여 채점하도록 한다. 심사위원의 개인적인 지식 또는 경험을 바탕으로 채점하여서는 안 된다. 기타 의문점이나 문제점이 발생하면 심사장에게 알리고 심사장은 출제자에게 질의 후 해결한다.

(10) 선수가 채점기준에 제시되지 않은 솔루션을 사용하여 과제를 해결했을 경우, 심사장에게 알리고 심사장은 출제자에게 질의 후 해결한다.

(11) 심사위원은 채점결과를 외부에 유출 시키지 말아야 하는 의무를 지닌다.

(12) 모든 선수 및 지도교사는 타 시·도 선수의 채점결과에 이의를 제기할 수 없다.

10 적용시기

1) 시행일시 : 2024년 전국기능경기대회부터

2) 기타사항

○ 본 직종설명서의 내용은 과제출제 및 경기진행, 심사채점 과정 등에서 일부 변경될 수 있음

○ 본 직종설명서에 정의되어 있지 않거나 문구 의미가 해석자에 따라 혼동의 여지가 있는 사항의 경우에는 심사장 및 심사위원 합의하에 결정함.

○ 직종설명서의 내용보다 경기과제, 채점기준표, 시행자료(시행 시 유의사항, 경기장시설 목록, 선수지참재료 목록, 선수지참공구 목록) 등이 우선함.

[별첨1] 대회별 경기일정 (예시)

1) 지방대회

일정	시 간	내 용	비고
1일차	08:30~09:30	○ 선수 입실 및 신분 확인 ○ 등번호 추첨/ 부여	경기장
	09:00~09:30	○ 선수 자리 배정 및 과제 설명	
	09:30~11:30	○ 제1과제	
	13:00~	○ 장비 점검	
2일차	08:30~09:00	○ 선수 입실 및 과제 설명	경기장
	09:00~12:00	○ 제 2과제 경기	
	12:00~	○ 제 2과제 채점 및 공지	
3일차	08:00~08:30	○ 선수 입실 및 과제 설명	경기장
	08:30~13:30	○ 제 3과제 경기	
	13:30~	○ 제 3과제 채점	
	과제 종료 후	○ 채점 통계/ 전산 입력/ 강평	
	강평 종료 후	○ 채점결과 발표	

2) 전국대회

일정	시 간	내 용	비고
사전준비	12:30~14:00	○ 경기장 사전준비 ○ 심사위원 소개 및 등번호 추첨	경기장
	14:00~15:00	○ 자리 점검	
	15:00~18:00	○ 장비 및 소프트웨어 점검	
1일차	08:00~09:00	○ 선수 입실 및 과제 설명	경기장
	09:00~13:00	○ 제 1과제 경기	
	13:00~	○ 제 1과제 채점	
2일차	08:00~09:00	○ 선수 입실 및 과제 설명	경기장
	09:00~13:00	○ 제 2과제 경기	
	13:00~	○ 제 2과제 채점	
3일차	08:00~09:00	○ 선수 입실 및 과제 설명	경기장
	09:00~13:00	○ 제 3과제 경기	
	13:00~13:30	○ 강평	
	13:30~	○ 제 3과제 채점	
	16:30~	○ 채점결과 발표	

[별첨2] 이론시험 예시

1. 다음에서 설명하는 공격용 소프트웨어는 무엇인가?

· 안티바이러스 프로그램에 의해 탐지된다.
· 특정 문자열을 타이핑한 후 파일의 내용에서 타이핑한 문자열이 검색된다.
· 지정된 시간에 로그파일을 설정된 공격자 메일로 자동 전송기능을 포함한다.
· 소프트웨어로 winhawk가 있다.

① Root Kit ② Key Logger software
③ Port Scanning ④ Nessassin

정답 : ②

2. 다음 중에서 데이터링크 계층에 대한 설명으로 옳지 않은 것은?

① 데이터링크 계층(Datalink Layer)은 에러처리(Error Control)를 수행한다.
② Flag와 패턴이 데이터에 나타날 경우에 대비하여 네트워크 계층에서 이를 처리하기 위한 메커니즘을 가지고 있다.
③ MAC(Media Access Control) 주소 제어와 데이터링크 제어를 한다.
④ 에러제어 및 흐름제어 역할을 한다.

정답 : ②

[별첨3] 실기과제 예시

[1과제] 인프라 환경 설정 및 보안 강화

1. 과제 소개

가. 과제 개요

당신은 gaia 시스템의 보안 엔지니어로 회사에서 기본적으로 운영되고 있는 웹서비스 구축과 외부로부터의 사이버 위협에 대응하기 위한 보안시스템을 구축하고자 합니다. 이를 위해 내부에 웹서버를 구축하고 웹서버 관리를 위해 SSH 통신이 이루어지도록 시스템을 구축하여야 합니다.

나. 배포자료

- 서버 시스템
- 운영체제 이미지 또는 ISO
  - Windows 10 Pro 2004
  - Server.ova (Ubuntu 16.04 + Apache2 + SSH Server)
  - Client.ova (Ubuntu 16.04)
- 윈도우용 가상화 툴(VirtualBox-6.1.12-139181-Win.exe)
- 가상화 툴 확장팩(Oracle_VM_VirtualBox_Extension_Pack-6.1.12.vbox-extpack)
- 패킷분석툴 (Wireshark-win64-3.2.5.exe)
- putty-64bit-0.73-installer.msi

다. 주의 사항

○ 작업시 대소문자를 구별하여 과제를 수행해야 합니다.

○ 채점 시 서비스 및 운영체제 재시작은 총 3회까지만 가능합니다.

○ 과제 제시되지 않은 password 는 "gaia_user!@#"으로 설정합니다.

○ 시스템을 재부팅 시에도 각 서버의 서비스들이 원활히 동작해야 합니다.

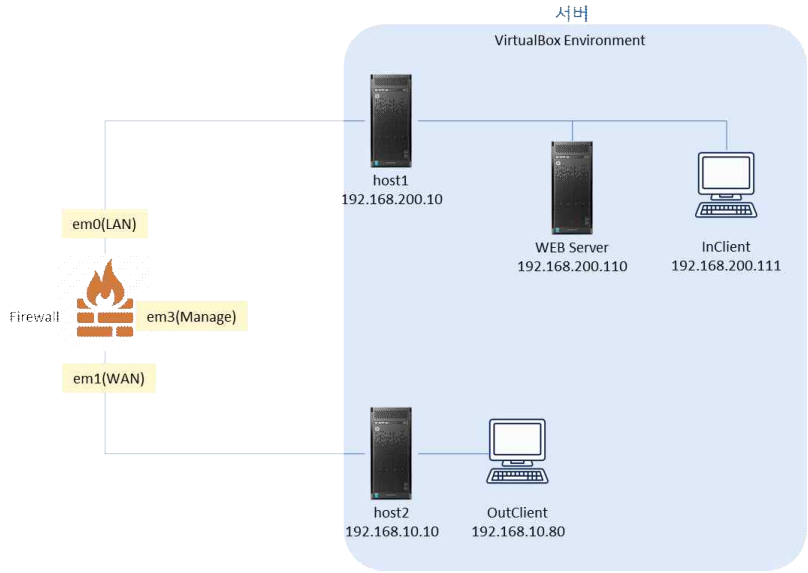
○ 대회장에서 제공되지 않은 소프트웨어 설치는 부정행위로 간주됩니다.

○ 선수는 모든 전자기기 및 저장장치 휴대를 금합니다.

○ 서버 및 클라이언트 방화벽 정책을 임의로 수정하면 감점 또는 “0”점 처리될 수 있습니다

2. 과제 내용

가. 운영체제 설치 및 네트워크 구성



1) 운영체제의 구성 및 설치

Guest OS의 설치 위치는 “D:₩VMs₩컴퓨터이름”폴더로 합니다. 문제에서 제시되지 않은 암호는 “gaia_ubuntu!@#”로 설정합니다. 제시되지 않은 설정 중 반드시 필요한 설정에 한하여 선수가 임의로 지정할 수 있습니다. 또한, 불필요한 설정은 채점에서 불이익을 받을 수 있습니다.

- 네트워크 구성도 및 정보를 참고하여 서버의 HOST1 및 HOST2의 네트워크 환경을 구성하도록 합니다. (사용자 포함)
- Guest OS는 Bridge Mode로 동작하도록 설치 합니다.
- Guest OS의 root 계정을 활성화 하도록 합니다.
- Guest OS의 기본 사용자는 gaia_ubuntu입니다.

○ 서버 정보

- OS : Windows 10 Pro 2004
- User ID : gaia_admin / gaia_Admin!@#
- WireShark 설치
- HOST1
  - IP : 192.168.200.10 / 24 / 192.168.200.1
  - IPv6 프로토콜 제거

- WEB Server
  - Name : WEBServer
  - Guest OS : Ubuntu Linux
  - IP : 192.168.200.110 / 24 / 192.168.200.1
  - User ID : root / gaia_Admin!@#
  - User ID : gaia_ubuntu / gaia_ubuntu!@#
  - User ID : gaia_client / gaia_client!@#
  - IPv6 프로토콜 제거
  - Apach 웹서버 & SSH 설치 확인

- InClient
  - Name : InClient
  - Guest OS : Ubuntu Linux
  - IP : 192.168.100.111 / 24 / 192.168.200.1
  - IPv6 프로토콜 제거
  - User ID : root / gaia_Admin!@#
  - User ID : gaia_ubuntu / gaia_ubuntu!@#
  - User ID : gaia_client / gaia_client!@#

- HOST2
  - IP : 192.168.10.10 / 24
  - IPv6 프로토콜 제거

- OutClient
  - Name : OutClient
  - Guest OS : Ubuntu Linux
  - IP : 192.168.10.80 / 24
  - User ID : root / gaia_Admin!@#
  - User ID : gaia_ubuntu / gaia_ubuntu!@#
  - User ID : gaia_client / gaia_client!@#
  - IPv6 프로토콜 제거

2) 리눅스 운영체제 설정

○ 모든 OS들의 경우 Screen Save 기능을 제거하도록 합니다.

○ 네트워크 인터페이스 설정
  - Guest OS는 인터페이스 이름이 enp0s3 로 표시되어야 합니다.
  - Guest OS의 네트워크 인터페이스는 enp0s3, lo(loopback)만 존재해야 한다.
  - Guest OS IP 주소와 HOST OS IP주소 상호간의 ICMP 통신이 이루어져야 합니다.

○ SSH 설정
  - InClient에서만 WEBServer에 SSH를 통한 접속이 가능해야 합니다.
  - SSH 접속은 root로 로그인이 불가능해야 하며, 접속 포트는 2200을 사용하여 gaia_ubuntu 사용자로만 접속이 가능해야 합니다.

나. WEB Server 시스템 보안

- WEB Server 운영체제에만 적용한다.

1) 세션관리

- SSH 로 접속한 사용자가 1분 동안 아무런 작업을 하지 않으면 로그아웃되도록 설정하시오.

2) root 사용자 보안

- root 사용자는 터미널/원격 등 모든 경로에서 직접 로그인이 불가능하도록 설정하시오.

3) 계정 보안

- 패스워드는 반드시 영문, 숫자, 특수문자를 포함하여 최소 8자리 이상을 만족해야 합니다.
- 패스워드는 마지막 변경일로부터 최소 1일간 사용되어야 하며, 90일 마다 변경 되도록합니다. 또한 만료 30일전에는 경고메시지가 출력되어야 합니다.
- 암호 변경 시 이전 암호를 5개까지 기억하여, 사용했던 암호의 재사용을 방지합니다.
- 모든 사용자(root 포함)는 로그인 3회 실패 시 해당 계정이 잠기도록 하며, 5분 이후 잠금이 해제되도록 설정하시오.
- su 명령어의 사용을 gaia_ubuntu 계정만 가능하도록 하며, su 사용 시 /var/log/sulog에 로그가 남도록 합니다.

[2과제-지방경기대회] 인프라 환경 설정 및 보안 강화

1. 과제 소개

가. 과제 개요

당신은 Nox 시스템의 보안 엔지니어로 회사에서 기본적으로 운영되고 있는 웹서비스 구축과 외부로부터의 사이버 위협에 대응하기 위한 보안시스템을 구축하고자 합니다. 이를 위해 내부에 웹서버를 구축하고 웹서버를 보호하기 위해 보안장비를 설치하도록 합니다. 또한, 지점에서 인터넷으로의 모든 통신은 VPN 장비를 이용하여 본점의 보안장비에 의해 보호 받을 수 있도록 보안 네트워크를 구성하여야 합니다.

나. 배포자료

- 서버 시스템
- 운영체제 이미지 또는 ISO
  - Windows 10 Enterprise editions 2004
- 패킷트래이서 7.3.1 (PacketTracer-7.3.1-win64-setup.exe)

다. 주의 사항

○ 작업시 대소문자를 구별하여 과제를 수행해야 합니다.

○ 채점 시 서비스 및 운영체제 재시작은 총 3회까지만 가능합니다.

○ 과제 제시되지 않은 password 는 "nox_user!@#"으로 설정합니다.

○ 대회장에서 제공되지 않은 소프트웨어 설치는 부정행위로 간주됩니다.

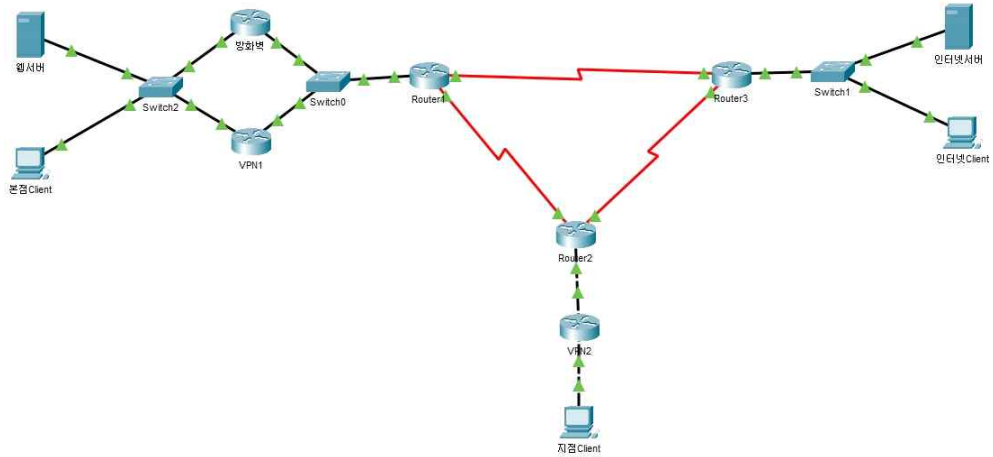
○ 선수는 모든 전자기기 및 저장장치 휴대를 금합니다.

2. 과제 내용

가. 보안 네트워크 구성도

1) 구성도

- 제공되는 패킷트레이서를 이용하여 시스템 정보를 기반으로 위의 보안네트워크를 구성하도록 합니다.
- 각 Router들간의 연결은 Serial로 통신하도록 구성합니다.
- 지점에서 인터넷으로 통신을 하기 위해서는 VPN연결을 이용하여 반드시 본점을 통해 인터넷으로 연결되어야 합니다.



2) 시스템 정보

○ 지점

- Network
  - VPN 외부 : 203.230.18.0 / 24
  - VPN 내부 : 192.168.2.0 / 24
- Router
  - 종류 : Cisco 2901 + HWIC-2T
  - Name : R3
  - IP 주소
    - □ Ethernet : 203.230.18.1 / 24
    - □ S0 : 10.10.1.254 / 24
    - □ S1 : 10.10.3.254 / 24
- VPN
  - 종류 : Cisco 2901
  - Name : RVPN
  - IP 주소
    - □ Ethernet0 : 203.230.18.254 / 24
    - □ Ethernet1 : 192.168.2.1 / 24
- 지점 Client

◆ 종류 : PC-PT

◆ **Name : PC3**

◆ IP 주소 : 192.168.2.101 / 24

○ 본점

- Network

◆ 방화벽 외부 : 203.230.7.0 / 24

◆ 방화벽 내부 : 192.168.1.0 / 24

- Router

◆ 종류 : Cisco 2901 + HWIC-2T

◆ Name : R1

◆ IP 주소

☐ Ethernet0 : 203.230.7.1 / 24

☐ S0 : 10.10.1.1 / 24

☐ S1 : 10.10.2.1 / 24

- VPN

◆ 종류 : Cisco 2901

◆ Name : VPN

◆ IP 주소

☐ Ethernet0 : 203.230.7.101 / 24

☐ Ethernet1 : 192.168.1.254 / 24

- 방화벽

◆ 종류 : Cisco 2901

◆ Name : Firewall

◆ IP 주소

☐ Ethernet0 : 203.230.7.254 / 24

☐ Ethernet1 : 192.168.1.1 / 24

- 본점 Client

◆ 종류 : PC-PT

◆ Name : PC1

◆ IP 주소 : 192.168.1.101 / 24

- 웹서버

◆ 종류 : Server-PT

◆ Name : Server1

◆ IP 주소 : 192.168.1.10 / 24

○ 인터넷

- Network : 203.230.17.0 / 24

- Router

◆ 종류 : Cisco 2901 + HWIC-2T

◆ Name : R2

◆ IP 주소

☐ Ethernet0 : 203.230.17.1 / 24

☐ S0 : 10.10.2.254 / 24

☐ S1 : 10.10.3.1 / 24

- 인터넷 Client

◆ 종류 : PC-PT

◆ Name : PC2

◆ IP 주소 : 203.230.17.101 / 24

- 인터넷 서버

◆ 종류 : Server-PT

◆ Name : Server2

◆ IP 주소 : 203.230.17.10 / 24

나. 보안네트워크 설정 및 정책 구현

1) 보안네트워크 환경 설정

○ 라우터 통신 설정

- 라우터간 연결은 시리얼 통신을 하도록 설정합니다.
- 모든 Router의 시리얼 clock rate는 128000으로 설정합니다.
- 라우터간 라우팅 프로토콜은 OSPF를 사용하도록 설정합니다.

○ 방화벽 설정

- 동적 NAT, PAT를 설정하도록 합니다.
- 정책 요구사항 이외의 모든 통신은 deny 되도록 설정합니다.

○ Firewall, VPN, RVPN 장비의 경우 보안 모듈 활성화를 위해 security 관련 모듈을 설치하여야 합니다.

○ 서버 설정

- 모든 서버는 HTTP, SSH 서버스만 동작되도록 설정합니다.

2) 정책 요구사항

○ 결과물 제출

- 결과물은 아래의 모든 정책이 적용된 패킷트레이서 파일을 '비번호_Exma2.pkt' 파일로 제출하도록 합니다.
- 제출 파일에는 각 요구사항에 대한 시뮬레이션을 진행하고 정상적으로 동작이 되는지 반드시 확인하도록 합니다.
- 패킷트레이서의 각 시스템의 이름은 제시된 이름의 변경하도록 합니다.

○ 본점 및 지점간 통신

- 본점과 지점간의 모든 시스템은 VPN과 RVPN 장비들간의 GRE 터널링을 이용한 IPSec VPN 을 이용하여 암호화 통신을 하도록 설정합니다.
- 본점에서는 각 시스템들의 Default gateway는 방화벽의 내부 IP를 사용하도록 설정합니다.
- 본점과 지점간의 VPN통신을 위한 GRE 터널링에 필요한 IP주소는 임의로 사용하여 설정하도록 합니다.

○ IPsec VPN은 아래의 조건을 만족시켜야 합니다.

- ISAKMP 정책
  - Authentication : pre-share
  - key : Nox_AES_256
  - Encryption : aes 256
  - Hash : sha
  - Lifetime : 36000초
- IPSec 정책
  - Encryption : esp-3des
  - Hash : esp-md5-hmac
  - transnform-set name : Nox_Enc
  - map name : Nox_Vpn

○ 본/지점과 인터넷간 통신

- 본/지점에서 Server2로 통신하는 경우 Firewall IP 주소로 동적 NAT가 이루어지도록 설정합니다.
- PC2에서 Server1으로 통신하는 경우 Firewall IP주소의 TCP/80 포트를 Server1 TCP/80 포트로 PAT를 적용하여 통신이 이루어지도록 설정합니다.

[2과제-전국경기대회] 네트워크 보안 장비 설정

1. 과제 소개

가. 과제 개요

당신은 gaia 시스템의 보안 엔지니어로 회사에서 기본적으로 운영되고 있는 웹서비스 구축과 외부로부터의 사이버 위협에 대응하기 위한 보안시스템을 구축하고자 합니다. 이를 위해 내부에 웹서버를 구축하고 웹서버를 보호하기 위해 보안장비를 설치하도록 합니다. 내부의 웹서버의 보호와 문제발생 시 긴급 복구를 위해 외부에서 원격 접속이 가능하도록 보안장비의 정책을 설정하여야 합니다.

나. 배포자료

- 서버 시스템
- 운영체제 이미지 또는 ISO
  - Windows 10 Enterprise editions
  - Server.ova (Ubuntu 16.04 + Apache2 + SSH Server)
- 윈도우용 가상화 툴(VirtualBox-6.1.12-139181-Win.exe)
- 가상화 툴 확장팩(Oracle_VM_VirtualBox_Extension_Pack-6.1.12.vbox-extpack)
- 패킷분석툴 (Wireshark-win64-3.2.5.exe)

다. 주의 사항

○ 작업시 대소문자를 구별하여 과제를 수행해야 합니다.

○ 채점 시 서비스 및 운영체제 재시작은 총 3회까지만 가능합니다.

○ 과제 제시되지 않은 password 는 "gaia_user!@#"으로 설정합니다.

○ 시스템을 재부팅 시에도 각 서버의 서비스들이 원활히 동작해야 합니다.

○ 대회장에서 제공되지 않은 소프트웨어 설치는 부정행위로 간주됩니다.

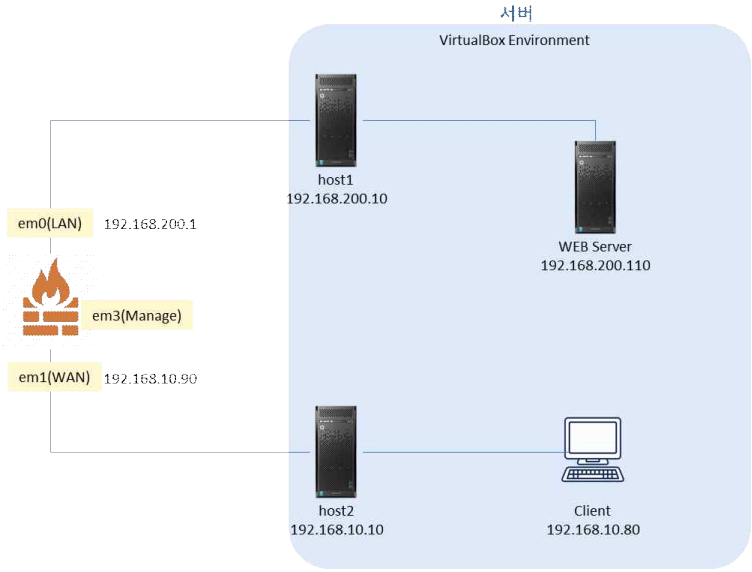
○ 선수는 모든 전자기기 및 저장장치 휴대를 금합니다.

○ 서버 및 클라이언트 방화벽 정책을 임의로 수정하면 감점 또는 "0"점 처리될 수 있습니다

※ WEB Server의 경우 과제 1에서 사용하였던 WEB Server를 사용하여도 무방합니다.

2. 과제 내용

가. 네트워크 보안 장비 설치 및 네트워크 구성



1) 구성도

- 네트워크 구성도 및 정보를 참고하여 서버 및 개인용 PC를 보안장비와 연결하도록 합니다.
- Guest OS는 Server.ova 단일 이미지를 사용하며, Bridge Mode로 동작하도록 설치 합니다.

2) 시스템 정보

○ 보안장비

- 관리자 ID : root
- 관리자 패스워드 : PassWord
- LAN(em0) : IP : 192.168.200.1 / 24
- WAN(em2) : IP : 192.168.10.90 / 24 / 192.168.10.1

○ 서버 정보

- OS : Windows 10 Pro 2004
- User ID : gaia_admin / gaia_Admin!@#
- HOST1
  - IP : 192.168.200.10 / 24 / 192.168.200.1

  - IPv6 프로토콜 제거

- WEB Server
  - Name : WEBServer
  - Guest OS : Ubuntu Linux
  - IP : 192.168.200.110 / 24 / 192.168.200.1
  - User ID : gaia_ubuntu / gaia_ubuntu!@#
  - IPv6 프로토콜 제거
  - Apach 웹서버 & SSH 설치 확인

- HOST2
  - IP : 192.168.10.10 / 24
  - IPv6 프로토콜 제거

- Client
  - Name : Client
  - Guest OS : Ubuntu Linux
  - IP : 192.168.10.80 / 24 / 192.168.10.1
  - User ID : gaia_ubuntu / gaia_ubuntu!@#
  - IPv6 프로토콜 제거

3) 리눅스 운영체제 설정

○ 모든 OS들의 경우 Screen Save 기능을 제거하도록 합니다.

○ 네트워크 인터페이스 설정

- Guest OS는 인터페이스 이름이 enp0s3 로 표시되어야 합니다.
- Guest OS의 네트워크 인터페이스는 enp0s3, lo(loopback)만 존재해야 한다.
- Guest OS IP 주소와 HOST OS IP주소 상호간의 ICMP 통신이 이루어져야 합니다.

○ SSH 설정

- WEBServer와 Client에 SSH 서버가 정상적으로 동작되도록 하여야 합니다.
- SSH 접속은 root로 로그인이 불가능해야 하며, 접속 포트는 22을 사용하여 gaia_ubuntu 사용자로만 접속이 가능해야 합니다.

나. 보안장비 설정 및 정책 구현

1) 보안장비 환경 설정

○ 보안장비 접속

- 개인 PC 컴퓨터를 이용하여 보안장비의 LAN1 콘솔포트에 접속하여 구성도와 같이 각 포트들의 IP를 설정하도록 합니다.
- 접속 LAN1 IP : https://192.168.1.1
- 접속 ID / 패스워드 : root / PassWord

○ 정책 구성

- 내부의 모든 시스템들간의 통신 서비스는 모든 서비스가 가능하도록 설정 합니다.
- 내부의 모든 시스템은 외부로의 통신을 하는 경우 보안장비의 WAN Port의 IP를 이용하여 Source NAT가 이루어 지도록 설정 합니다.
- 단, 내부에서 외부로의 통신은 다음의 포트들만 가능하도록 설정 합니다.
  - TCP : 80, 443, 22, 21
  - UDP : 53
  - ICMP
- 외부에서 내부의 웹서버의 웹으로 Port NAT를 이용하여 접속이 가능하도록 설정 합니다.
  - 접속 Port : TCP / 80
  - 내부 전달 : TCP / 80
- 외부에서 내부의 웹서버로 SSH로 Port NAT를 이용하여 접속이 가능하도록 설정 합니다.
  - 접속 Port : TCP / 1030
  - 내부 전달 : TCP / 22
- 위에서 정의하지 않은 모든 통신은 Deny가 되도록 설정 합니다.

2) 보안장비 정책 테스트

○ 결과물 제출 방법

- 서버와 개인 PC에서 WireSahrk를 실행시키고 각 단계별 패킷 및 화면을 캡쳐 및 저장하여 제출하도록 합니다.
- 저장하는 패킷의 이름은 'Test_비번호_테스트명_위치' 로 저장합니다.
  - 예) Test_B1203201_통신_서버.pkt, Test_B1203201_통신_PC.pkt
  - Test_B1203201_통신_서버.png, Test_B1203201_통신_PC.png

○ 테스트 내용

- SourceNAT 테스트

  - WEBServer에서 Client으로 PING 5회 요청
  - WEBServer에서 Client으로 HTTP 2회 접속
  - WEBServer에서 Client으로 Telnet 2회 접속
  - WEBServer에서 Client으로 SSH 접속 후 hostname 및 ip 주소 확인
- PortNAT 테스트
  - Client에서 WEBServer으로 PING 5회 요청
  - Client에서 WEBServer으로 HTTP 2회 접속
  - Client에서 WEBServer으로 Telnet 2회 접속
  - Client에서 WEBServer으로 SSH 접속(Port 번호 TCP/1030) 후 hostname 및 ip 주소 확인
  - WEBServer로의 통신은 보안장비의 WAN 인터페이스의 IP로 통신함을 의미한다.

[3과제] 취약점 분석 및 모의침투 테스트

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security mis-configurations
- Cross Site Scripting (XSS)
- Insecure De-serialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring