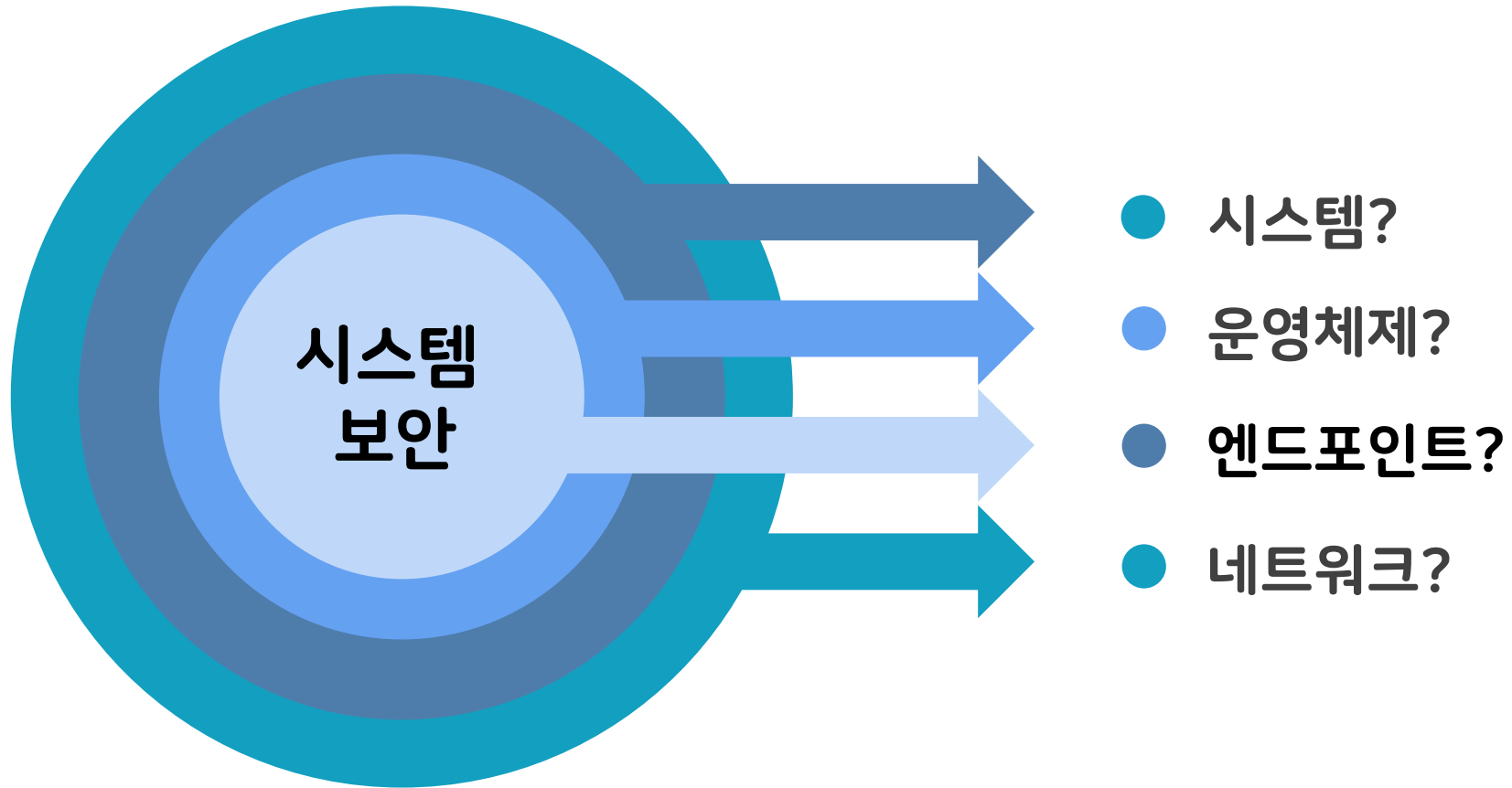


시스템 보안

#1 개요



시스템 보안이란?



시스템 보안이란?

- 시스템 (운영체제) \approx 엔드포인트, 각각의 시스템은 네트워크를 통해서 연결



엔드포인트는 여러가지로 정의할 수 있지만 간단하게 정의하면

1. 네트워크의 말단에서 사용자와 연결되는 장치

- PC, 노트북, 스마트폰, IoT 장치 또는 웹 서버 처럼 사용자와 연결되는 서버도 엔드포인트 범위에 포함

2. 네트워크에 연결하고 네트워크를 통해 통신하는 모든 장치

- 다른 컴퓨팅 디바이스를 네트워크에 연결하는 스위치와 라우터도 엔드포인트 범위에 포함

❖ 시스템 보안이 더 큰 개념이지만, 일반적으로 보안 솔루션 관점에서는 엔드포인트 보안과 같은 의미로 사용

수업 방법



학습 (세모클래스)

시스템보안 관련
기반 지식 학습



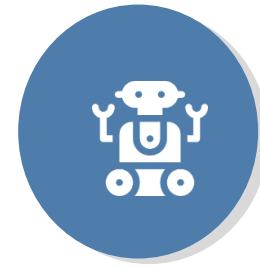
실습

실습 과정에서
관련 내용을 구현해
보면서 이해



사례

최신 보안 이슈 소개



팀프로젝트 (기업연계 프로젝트)

팀별 프로젝트 진행

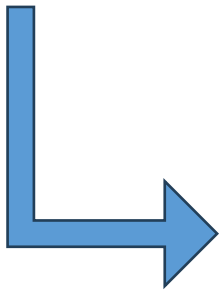
수업 방법

● 세모 클래스(SEMO Class) 수업 방식



사전 학습

- LMS에 업로드된 수업자료 및 동영상 시청
- 오프라인으로 진행되는 본 수업 이후 그 다음 주 수업 자료가 업로드 됨
업로드 되는 주차별 강의 자료 확인(1주차 수업 후 2주차 폴더에 업로드 됨)
- 동영상 시청 기간은 1주일이면 이 기간 내에 시청하지 않으면 출석 점수 감점



본 수업

- 사전 수업 내용 또는 팀프로젝트 보고서에 대한 발표 후 피드백 (3주차 이후)
발표는 팀프로젝트 조별로 진행 (매주 팀별로 한명 씩 자체적으로 선정, 5분 발표)
- 사전 학습에서 이해가 안된 부분에 대한 질의 및 피드백
- 수업 자료에 대한 핵심 부분 요약 설명

수업 방법

● 팀 구성

- 수강인원을 5개 조로 구성하며, 팀프로젝트 발표 및 사전 수업 내용에 대한 본 수업 시간 발표 진행
각 조는 랜덤으로 배정됨
- 팀프로젝트 각 단계별 발표자는 한명으로 지정해도 되지만 (가능하면 다르게 진행해 보는 걸 추천),
본 수업 시간에 진행되는 사전 수업 내용 발표자는 모두 다르게 지정해야 함
(본 수업 발표 시에 실습 내용이 포함된 학습 내용에 대해서는 실습한 결과도 같이 설명해야 함)
- 발표는 경험이 많을 수록 잘 할 수 있기 때문에 편하게 발표해 볼 수 있는 수업 시간에 해보는 걸 추천
꼭 많은 청중이 있는 장소에서 발표해야 발표 역량이 향상되는 게 아니며, 발표 경험(횟수)가 더 중요

평가

출석 및 참여도 (10점)



- 사전학습 영상 시청 및 본 수업 출석

팀프로젝트 (30점)



- 기업 연계형 프로젝트 수행
하나의 프로젝트 주제

중간시험 (30점)



- 객관식과 단답형 문제와 함께
문제를 이해하고 해결 방안을
기술하도록 하는 서술형 문항
포함

기말시험 (30점)

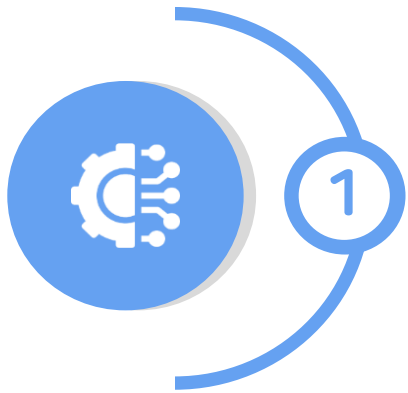


- 객관식과 단답형 문제와 함께
문제를 이해하고 해결 방안을
기술하도록 하는 서술형 문항
포함

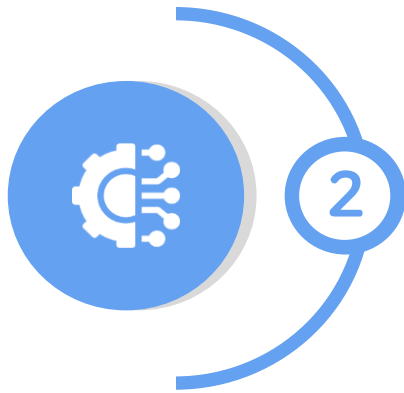


100점

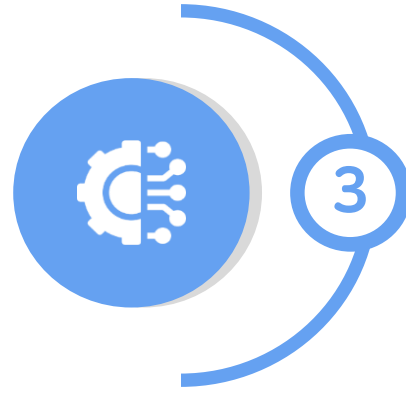
주요 수업 내용



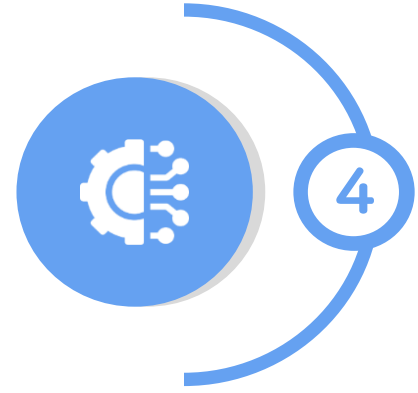
운영체제



어셈블리어



시스템 해킹

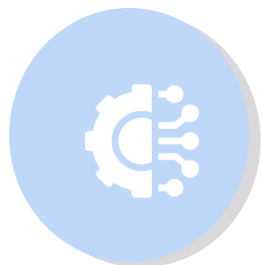
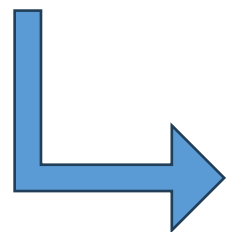


리버싱

주요 수업 내용



어셈블리어
학습 필요성



- 시스템 해킹에는 다양한 좋은 도구들이 사용되고 리버싱도 디컴파일을 통해서 C언어 스타일의 코드를 보면 되는데, 어셈블리어를 왜 알아야 하나?


- 함수의 내부 구조와 동작원리, 호출 방식, 레지스터·메모리 접근을 근본부터 이해하려면 어셈블리어가 필수
- 디컴파일·도구가 보여주지 못하는 실제 제어흐름과 데이터 이동을 '있는 그대로' 보여주는 유일한 원문이 어셈블리어
- 현업에서도 리버싱, 취약점 분석 뿐만 아니라 프로그램이나 커널의 크래시 분석 등을 할 때 어셈블리어 레벨에서의 분석이 필요

수업 및 과제 수행 시 사용하게 될 도구

● 사용 언어

- Python, C++, Assembly

● 사용 도구

- Jupyter Notebook with Google Colab 
- PyCharm Community Edition 
- Visual Studio Community Edition 
- SASM 
- IDA Freeware 
- 기존에 주로 사용하는 툴이 있으면 그 툴을 사용해도 됨



팀프로젝트

● 기업 연계형 팀프로젝트 목표

- 기업에서 실무적으로 필요한 프로젝트 주제를 선정하고 이를 수행해 봄으로써 실무에서 진행되는 업무를 간접 경험
모든 팀이 공통된 하나의 주제에 대하여 프로젝트를 수행함으로써 선의의 경쟁 유도

● 사용 언어

- Python으로 웹 인터페이스를 구현할 수 있는 다양한 프레임워크 중 하나를 선정하여 구현
복잡한 프레임워크보다는 가벼운 프레임워크를 선정하는 걸 추천
- 데이터 수집을 위한 도구, LLM 에이전트 등은 독립적인 프로그램으로 작성해서 구동해도 됨
백그라운드에서 독립적으로 작동하더라도 웹 인터페이스를 통해서 제어가 가능하도록 구성 해야 함

● 과제 결과물

- 과제 기획서부터 소스코드 및 설명서, 최종 결과물 실행 화면까지 전체 프로젝트 보고서를 작성하여 제출
- Github을 이용한 프로젝트 소스코드 관리 및 커뮤니케이션을 위한 다양한 툴을 사용해서 진행
- 💡 Github에 업로드 되어 있는 프로젝트 결과물은 향후 취업 시 포트폴리오로 활용 가능

팀프로젝트

- 팀프로젝트 주제

- 공급망 사이버 보안 위험 평가 AI 에이전트 개발

- 현재의 소프트웨어 공급망 보안 평가는 CVSS 점수 기반으로 이루어지고 있으나, 이는 정적 메타 정보에 불과하여 실제 위협 우선순위를 결정하는 데 한계가 있음

- * CVSS(Common Vulnerability Scoring System) :

- 취약점의 기술적 심각도를 공격 난이도·영향 등을 평가해 0-10 점(등급)으로 정량화 하는 공개 표준

- 따라서 EPSS(실제 공격 확률) 및 공격 사례 정보(Threat Intelligence)를 자동 수집하고, 이를 직관적으로 제공하는 시스템을 개발하는 것을 목표로 함

- * EPSS(Exploit Prediction Scoring System) :

- 공개된 CVE가 향후 30일 이내 실제로 악용될 확률을 0~1 점(0 ~ 100%)으로 예측해 대응 우선순위를 정하는 지표

팀프로젝트

● 주요 개발 요소

1. CVE별 EPSS 수집 기능

- EPSS 공식 API 또는 데이터셋으로부터 최신 점수를 주기적으로 수집
- EPSS 점수는 확률 기반(0~1)으로 제공되며, CVE-ID를 기준으로 정규화

2. CVE-EPSS 매핑 데이터베이스 구축

- CVE ID를 키로, EPSS 포함한 메타정보를 통합

3. LLM 기반 공격 사례 자동 수집 Agent 개발

- Prompt 템플릿 또는 Retrieval 기반 Agent가 다음 작업 수행
- CVE에 대해 실제 악용된 사례 검색 (뉴스, 블로그, 연구 보고서)
- 결과는 JSON 형태로 저장

4. 통합 웹 인터페이스 개발

- CVE ID 또는 제품명으로 검색 → EPSS + 공격 사례 + 대응 권고 종합 제공

팀프로젝트

- 점수는 팀원 모두 동일하게 부여됩니다.

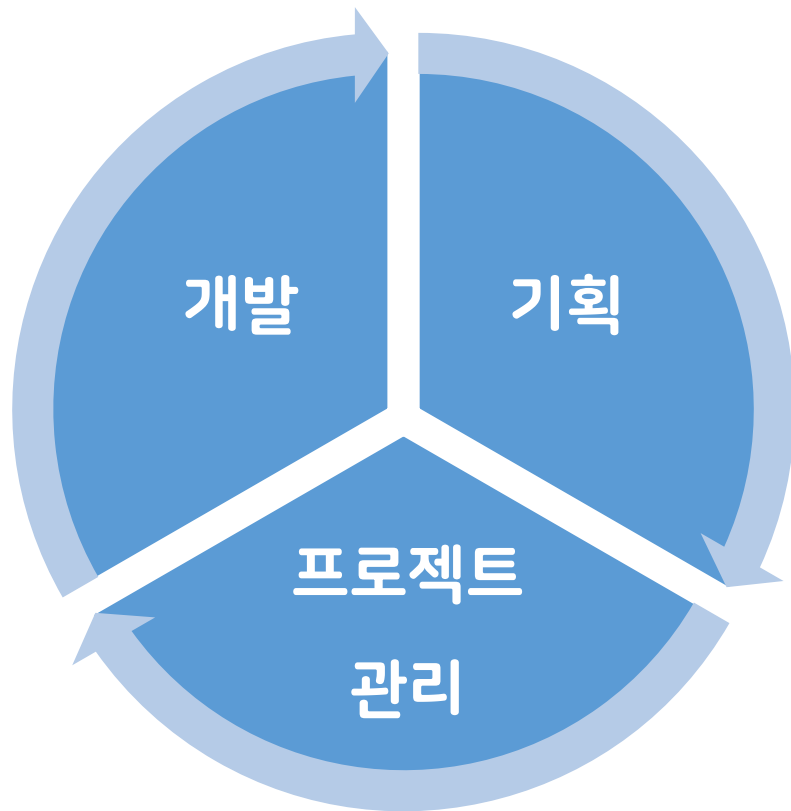
- 단지 학점을 받기 위해 상호 경쟁을 하는 관점이 아닌, 프로젝트를 완성하기 위해서 팀으로써 협업을 하는 것이 중요합니다.
또한, 팀으로 프로젝트를 진행하면서 얻는 다양한 경험들은 여러분들이 향후 사회에서 실무를 할 때에도 도움이 됩니다.
향후 면접 등에서 활용할 수 있는 포트폴리오를 준비한다는 생각으로 진행하기 바랍니다.
- 각 단계별 보고서에 대한 평가는 프로젝트 주제를 선정한 기업에서 진행합니다.
- 기여도가 현저히 낮은 팀원은 패널티 부과 (0점 처리 또는 감점)

팀프로젝트

- 평가는 기획, 프로젝트 완성도와 함께 보고서 내용 구성에 대한 부분을 종합적으로 판단합니다.
- 실제 회사에서 팀으로 업무를 진행할 때에도 형식은 조금씩 다르지만 각 영역의 능력이 모두 필요합니다.
- 개인이 혼자 할 수 있는 범위와 팀으로써 서로를 보완하며 할 수 있는 범위가 얼마나 다른 지에 대해서도 생각해 보기 바랍니다.
- 팀으로 일을 할 때 의사 소통을 잘할 수 있는 방법이 무엇인지,
팀원들 간에 발생하는 다양한 문제를 어떻게 해결해야 하는 지에 대해서도 생각해 보기 바랍니다.
- 코드를 잘 작성하거나 어려운 문제를 해결하는 것도 중요하지만,
사용자 관점에서 어떤 도움을 줄 수 있는 지 잘 기획하고 설계하는 것과 프로젝트에서 해결하려고 했던 문제가 무엇인지,
어떻게 문제를 잘 해결 했는지 장점과 특징 등은 무엇인지를 잘 설명 할 수 있어야 합니다.
- 보고서를 어떻게 하면 잘 작성하는 것인지(형식이나 구성, 디자인 등), 잘 작성된 좋은 코드는 무엇인지 생각해 보기 바랍니다.

팀프로젝트

● 팀 내 역할 분담



각 팀은 팀장 및 각 역할별로 파트장을 선임해야 하며,
구성원들은 기본적으로 세 가지 역할 중 하나를 맡아야 합니다.
각 역할 별 최소 인원은 2명

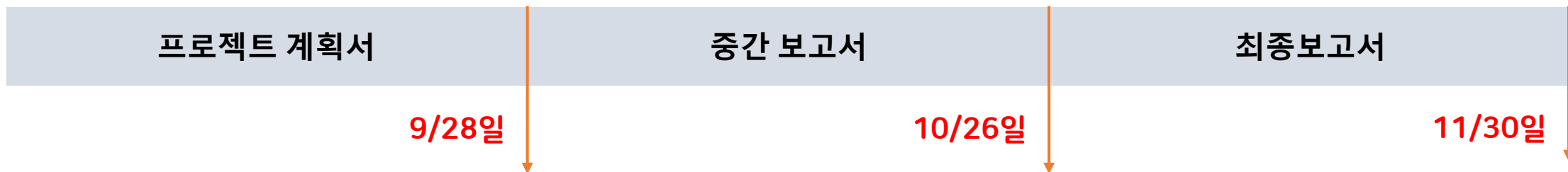
- 개발 : 코드 설계 및 구현
- 기획 : 프로그램 기능 및 UI 명세 작성
- 프로젝트 관리 :
프로젝트 진행 상황 관리 및 보고서 작성 주도
프로젝트 진행 중 커뮤니케이션 주도

공통 : 문제 정의 및 프로젝트 방향 설정,
프로젝트 진행 중 발견된 문제 해결 등의 과정에서는 모두 참여

팀프로젝트

● 팀프로젝트 진행 일정

- **9/28일**까지 프로젝트 계획서 제출, **9/29일** 수업 시간에 발표 진행
프로젝트 기획 의도, 사전 조사 내용, 프로젝트 기획 내용, 팀 구성원의 역할, 프로젝트 수행 일정 등을 포함
- **10/26일**까지 중간 보고서 제출, **10/27일** 수업 시간에 발표 진행
프로젝트 설계 의도 및 자료 조사 내용, 팀 구성원들이 어떤 일을 수행했는지 명확하게 드러나야 함
- **11/30일**까지 최종 보고서 제출, **12/1일** 수업 시간에 발표 진행
프로젝트 설계 및 기획 내용, 결과물 구동 화면 등을 적절히 사용해서 다른 사람들이 쉽게 이해할 수 있도록 구성



팀프로젝트

● 최종 보고서에 필수적으로 포함해야 할 내용

- 프로젝트 진행 과정에서의 활동 사진 포함 (필수)
- 문제 정의 및 기획 의도, 기획 내용, 코드 설계 및 구성, 실행 화면, 프로젝트의 특징점
- 프로젝트 기획 및 개발 단계에서의 관련 자료 조사 내용, 프로젝트 진행 과정에서의 문제(어려움 등) 및 해결 과정 설명
- 프로젝트에서의 각 팀원들의 역할 및 수행 내용
- 추가적인 내용은 자유롭게 포함시켜 작성

● 과제 제출 형식

- 파워포인트를 이용하여 보고서 작성 후 PDF로 변환하여 제출

● 과제 제출 방법

- 팀별 제출이며, 제출 파일명은 팀명_(프로젝트계획서 or 중간보고서 or 최종보고서).pdf
- jsclass90@gmail.com 계정으로 제출 (팀장이 제출)

참고 사항



온라인으로 제공되는 사전 학습 동영상은 필수 시청



LMS 게시판에 올라오는 공지 내용 확인



교재는 있으면 학습에 도움이 되겠지만, 꼭 필요한 것은 아니기 때문에 초반 2~3주 정도 수업을 들어 보고 구매 여부는 각자 선택하면 됨



평가는 공정하게 진행하겠지만, 절대 평가가 아닌 상대평가이기 때문에 정성 평가 요소가 반영되어 평가가 진행됨

QA

