<목차>

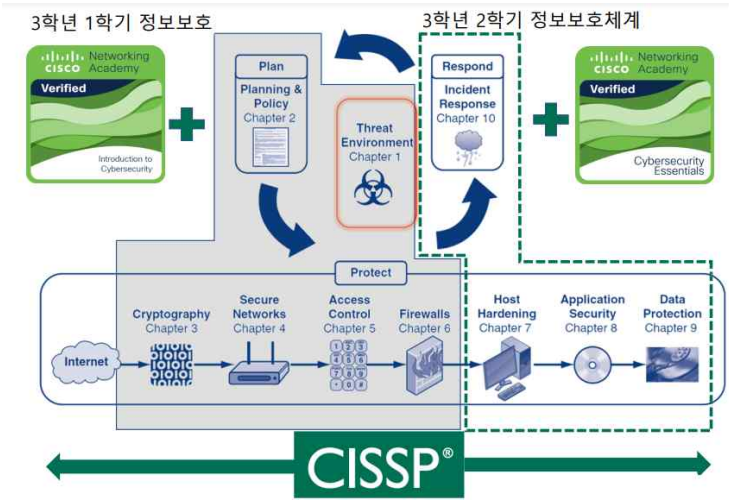
1) 2023-1학기, 이민우 교수님의 '정보보호'강의를 수강하다.

나는 CISSP 자격증을 취득하기 위해 준비하고 있다. CISSP은 국제공인 정보시스템 보안전문가 자격증으로, 정보보안 업계에서 국제적으로 가장 널리 인정받는 자격증이다. 1년 후 공군 정보통신장교로 임관하여 SW(정보통신) 업무를 수행하는 것을 희망하고 있는데, F-35 전투기와 같은 첨단 무기체계의 SW 시스템을 관리하기 위해서는 CISSP 자격증이 필요하여 이와 연관된 정보보호 과목 수강 필요성을 느꼈다.

2023년 1월, 3학년으로 올라가는 겨울방학 중 어느 날, CISSP 취득과 관련해서 정보보호 담당 교수님인 이민우 교수님과 면담을 진행했다. 이민우 교수님은'정보보호'과목과 관련 고급과목인'정보보호체계'과목을 수강하면 CISSP의 70% 정도를 다룰 수 있다고 말씀해주셨다. 그래서 나는 3-1학기에 이민우 교수님의 '정보보호'과목을 수강하게 되었다.

2) 이민우 교수님의 '정보보호'진행방식 + 장점

CISSP에서 다루는 내용은 아래 그림과 같이 총 10개의 Chapter로 구성되어 있다. OT에서 이 중 1~6번 Chapter까지를 다루고 나머지 7~10번 Chapter는 '정보보호체계' 과목에서 다룬다고 하셨다.



'정보보호'수업은 주로 강의 노트를 통해 진행되었다. 이 수업은 강의 노트만으로도 충분히 학습을 잘 정리할 수 있다는 편리함이 있다.

▼ 강의노트 예시

학습 목표

- 접근 제어와 관련된 기본적인 용어를 정의할 수 있다.
- 건물과 컴퓨터의 물리적 보안에 대해 설명할 수 있다.
- 재사용 가능한 패스워드에 대해 설명할 수 있다.
- 액세스 카드와 토큰이 어떻게 작동하는지 설명할 수 있다.
- 검증 및 신원 확인을 포함하여, 생체인증에 대해 설명할 수 있다.
- 권한부여에 대해 설명할 수 있다.
- 감사에 대해 설명할 수 있다.
- 중앙 인증 서버, 디렉토리 서버를 설명할 수 있다.
- 완벽한 ID 관리를 정의할 수 있다.

해킹의 흐름

- Spoofing
  - 공격자(attacker)가 마치 공격 대상자(희생자, victim)로 가장하는 것
  - 예) 공격자는 수신자로 가장하여 송신자로부터의 메시지를 강탈
  - 예) 송신자로 가장하여 수신자에게 거짓 메시지를 전송

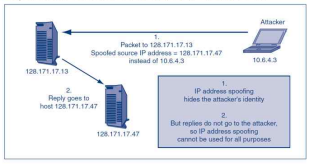


FIGURE 1-12 Source IP Address Spoofing

또한 각 Chapter가 끝나면, Cisco Networking Academy라는 사이트에서 해당 Chapter에 대한 퀴즈를 풀고, Bb 토론글에 해당 Chapter를 이수한 소감을 작성해야 했다. 이 과제를 하면서 다른 학우들의 소감도 보며 새로운 관점을 얻을 수도 있었고 내가 생각하지 못한 점들을 학우들의 소감을 통해 깨닫게 되기도 했다.

▼ Bb 토론글에 게시한 나의 토론글	▼ 나의 토론글에 대한 학우의 댓글과 교수님의 대댓글(피드백)
	

위와 같이 토론글을 작성하면 학우들이 자신의 관점을 나누기도 하고, 교수님께서는 대댓글로 피드백을 주셨다.

무엇보다 이 수업의 가장 큰 장점은 교과서에는 다루지 않지만, CISSP 시험에 자주 출제되는 핵심 주제들에 대해 참고자료를 제공해 준다는 것이다. 그래서 저는 이 강의를 통해 CISSP 시험 준비에 필요한 중요 주제들을 배울 수 있었다. 아래 그림과 같이, [참고]라고 되어 있는 부분은 교재에는 없지만 CISSP 준비에 필수적인 내용들을 포함하고 있어 CISSP 준비에 큰 도움이 되었다.

▼ [참고] → CISSP 핵심 주제 학습

참고: 리눅스/유닉스의 권한 상승

- 시스템에서 해킹을 하는 주요 목적은 권한 상승
  - 합법적인 권한 상승 방법 : SetUID
  - 이것을 악용하는 것이 시스템 해킹의 목적
- SetUID

```
srlshfree@ubuntu:/$ ls -al /usr/bin/passwd
-rwsr-xr-x 1 root root 54224 Aug 20  2017 /usr/bin/passwd
```

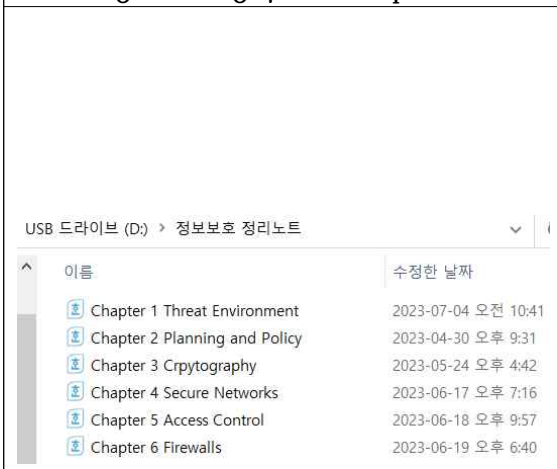
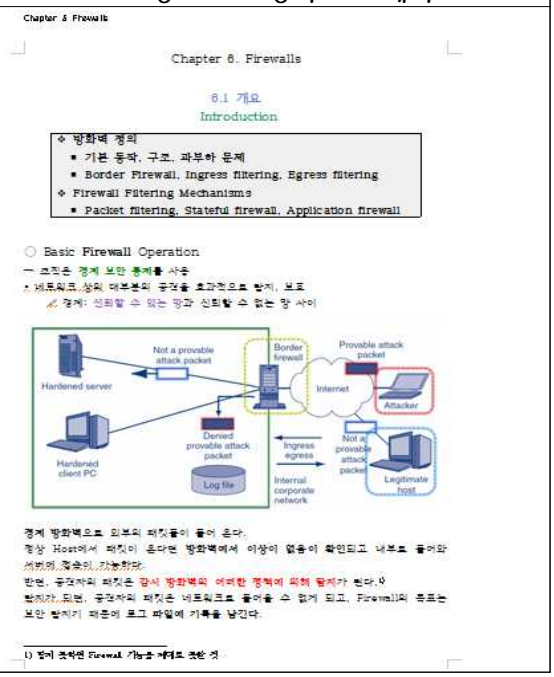
  - 유닉스 시스템의 첫 번째 특허
  - 시스템 권한 획득에 사용
    - 백도어, 버퍼 오버플로, 포맷 스트링 취약점 공격에 이용
  - 시스템 운영에 필수
  - "지속적 관리 대상"
    - SetUID가 설정된 root 소유의 파일 검색법

```
find / -user root -perm /4000
```

3) 나만의 학습 노하우

3-1) 수업 정리

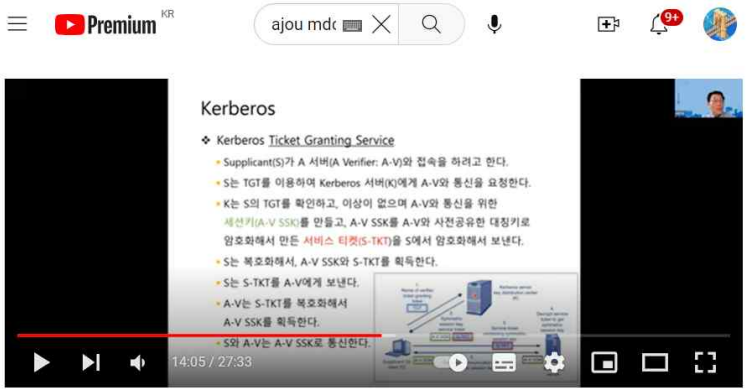
나는 태블릿을 가지고 있지 않아 수업시간에 중요하다고 생각되는 부분은 간략히 노트에 적었다. 수업 시간 이후에는 한글 파일로 정리하였고 시험기간 직전에는 한글파일로 정리한 내용을 프린트하여 공부하였다. 아래는 정보보호 수업을 정리한 내용 예시이다.

▼ 정보보호 정리노트 Chapter 1~6	▼ 정보보호 정리노트 예시
	

3-2) 유튜브 강의 활용

다른 강의와의 가장 큰 차이점이라고 할 수 있는데, 이민우 교수님은 강의를 유튜브에 올리시

기 때문에 복습할 때 효과적이었다. 수업시간에 잘 이해가 안 가는 부분이 있으면 체크했다가 나중에'정보보호'강의가 올라온 유튜브를 검색하면 되어서 편리하게 부족한 부분을 채울 수 있었다.



(정보보호-2022년) 5. Access Control 9. Central Authentication Servers ~ 10. Directory Severs

예시) Kerberos Server에 대해 이해가 가지 않아 유튜브를 활용

3-3) 메일 적극 활용0

이해 가지 않는 부분이 있으면 나는 일단 유튜브 강의를 참고하였다. 그러나 유튜브 강의로도 이해가 안 된다면, 메일을 통하여 질문하고 해결하는 방법을 선택했다. 일방향 소통인 유튜브 강의와 달리, 교수님과 직접적으로 메일을 주고받음으로써 의문점을 효과적으로 해소할 수 있었다.

▼ 메일을 통한 질문	▼ 질문에 대한 교수님의 답
[정보보호 질문] 국방디지털융합학과 박준상  받는 사람: 이민우 안녕하세요, 정보보호를 수강하고 있는 국방디지털융합학과 입니다. 다름이 아니라, Chapter 4.2 Secure Network-DoS Attack를 공부하던 중 모르는 점이 있어 메일을 보내게 되었습니다. DDoS 공격은 Direct Attack과 Indirect 공격으로 나뉘어지는데, 강의노트를 보면 Direct Attack은 공격자가 희생자를 직접 공격하는 것이고, 그 예시로 TCP Syn Flooding-> Land Attack), ICMP Flooding (->Smurf), UDP Flooding(Fraggle)이 있습니다. 제가 궁금한 것은 다음과 같습니다. 1. Land Attack은 TCP SYN Attack의 일종이라고 할 수 있나요? 마찬가지로, Smurf 공격도 ICMP Flooding 공격의 일종인지 궁금합니다 Land Attack은 IP 패킷 헤더의 송신지 IP 주소와 목적지 IP 주소를 같게 설정하고 공격하면 수신자는 SYN/ACK 패킷을 자신에게 보내는 공격방법으로 알고 있습니다. Smurf 공격도 broadcasting을 이용하여 victim에게 증폭된 트래픽을 줘 리소스를 고갈시키는것으로 알고 있는데, 각각 TCP SYN Attack, ICMP Flooding에 속하는지 알고 싶습니다. 2. TCP SYN Attack은 Transport 계층, 즉 4계층 공격이라면 Landattack은 몇계층 공격이라고 할 수 있나요? 3. Land Attack 공격과 Smurf 공격은 Direct 공격인지, Indirect 공격에 해당하는지 궁금합니다. 또 이러한 공격을 나누는 기준을 잘 모르겠습니다. 학생과 토론을 해보았는데, 둘 다 잘 모르겠어서 이렇게 메일로 질문드려봅니다. 감사합니다.	이민우 <iminu@ajou.ac.kr> 2023-06-16 오후 11:10 받는 사람: h ; 수고 많다. 각 용어의 분류 기준이 명확하지 않아 이해하는데 어려웠겠다. 질문해줘서 고맙다. 이렇게 정리하면 좋겠다. 1. Direct vs. Indirect o 공격자가 희생자의 취약점을 이용하여 직접 공격하는 경우: Direct o 공격자가 리플렉터(reflector)를 사용하는 경우: Indirect 2. Land vs. Smurf o 출발지와 도착지 주소를 같게하는 경우: Land o 브로드캐스팅으로 여러 출발지에서 하나의 도착지로 집중하는 경우: Smurf 3. TCP SYN Flooding vs. ICMP Flooding o TCP 악용해서 DoS 공격: TCP SYN Flooding o ICMP 악용해서 DDoS 공격: ICMP Flooding 수고^^

이러한 방법들을 이용해 공부하여 정보보호 과목에 대한 이해도를 높일 뿐만 아니라 학점까지 챙길 수 있었다.

F109	1	정보보호	3	A+	4.5	이민우

4) 소융대 IT 해외연수 경험

나는 3학년 1학기를 마치고, 6월 26일부터 30일까지 일본 도쿄에서 '소융대 IT 해외연수' 프로그램에 참여했다. 이 프로그램은 소융대의 이민우 교수님이 지도하셨다. 나는 교수님과 함께 전용 버스를 타고 도쿄 시내를 둘러보며, 다양한 주제에 대해 대화를 나눌 수 있는 기회를 가졌다. 특히, 제 진로와 다가올 2학기 '정보보호체계' 과목에 대한 교수님의 생각을 듣는 것이 매우 유익했다. 호텔에서의 조식 시간에도 교수님과 많은 대화를 나누며 좋은 추억을 만들었다.

5) 방학 중 정보보호체계 수강 신청 및 교수님의 사임

여름방학이 끝나고 3-2 학기를 준비하면서 정보보호와 연계된 교육과정인 '정보보호체계'를 듣기로 나는 했다. 그런데 3-2학기 '정보보호체계'를 포함한 예비수강신청을 하루 앞두고, 이민우 교수님께서 다른 대학으로 이직하신다는 소식을 들었다. 교수님이 떠나신다는 소식을 듣고, 교수님께 배울 수 있는 남은 기간이 없어진 것에 대한 큰 아쉬움이 생겼다. 이러한 아쉬움을 바탕으

로 '함께하고 싶은 교수님 공모전'에 참여하기로 결정했다. 이민우 교수님과의 교육적 관계가 제 학문적 성장에 큰 영향을 미쳤기 때문에,이 공모전을 통해 교수님과의 소중한 기억을 되새기고, 남은 기간 동안 함께하지 못한 아쉬움을 표현하고자 한다.