

컴퓨터보안 13주차

2023. 05. 30. (Wed)



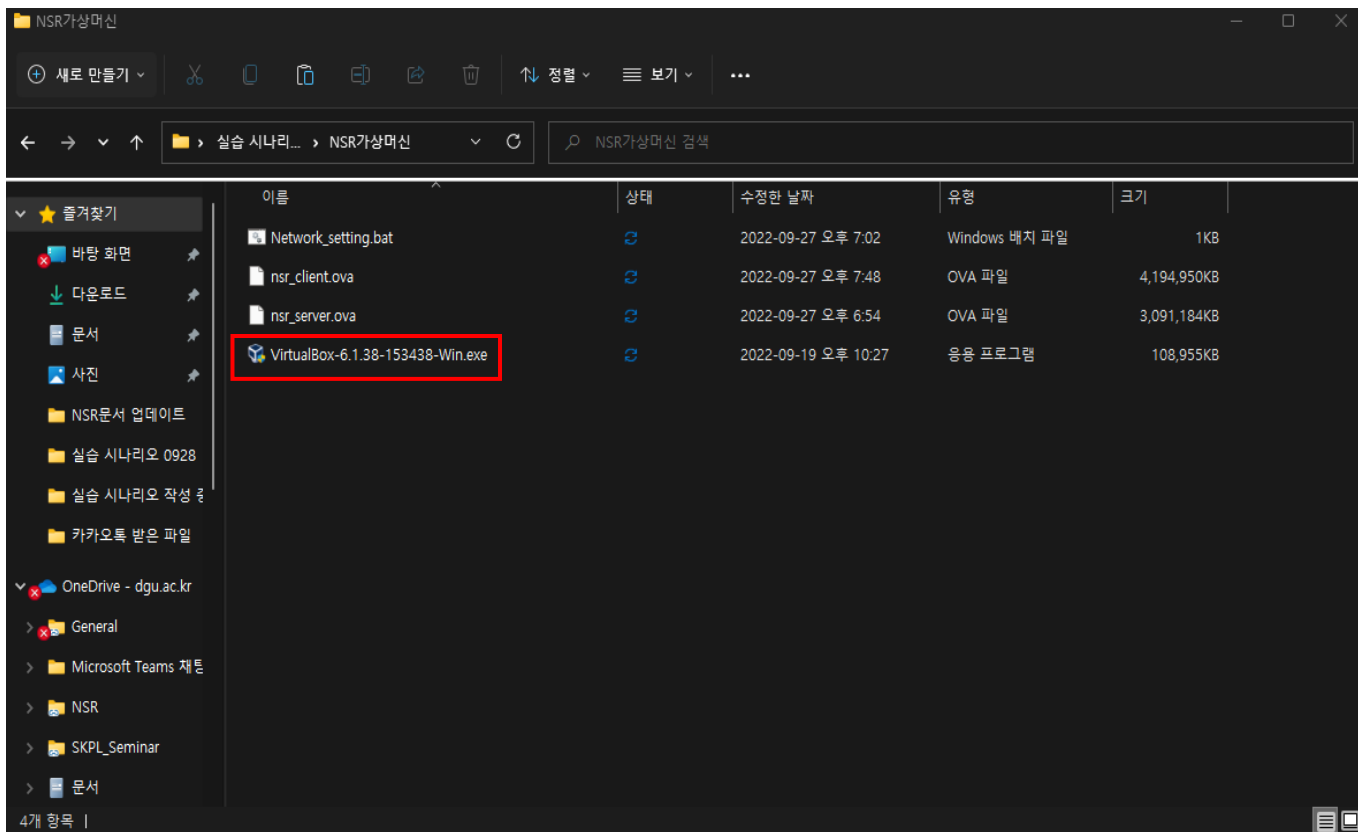
Table of Contents

1. 환경 세팅
2. 실습 과제1: 보물찾기
3. 실습 과제2: 보안약점 시나리오 작성
4. Q&A

1. 환경 세팅

❖ 버추얼 박스 다운로드 [1/3]

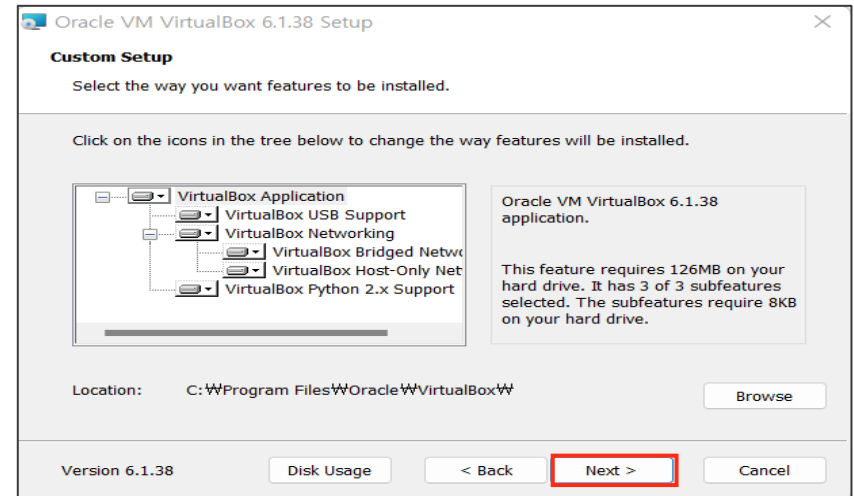
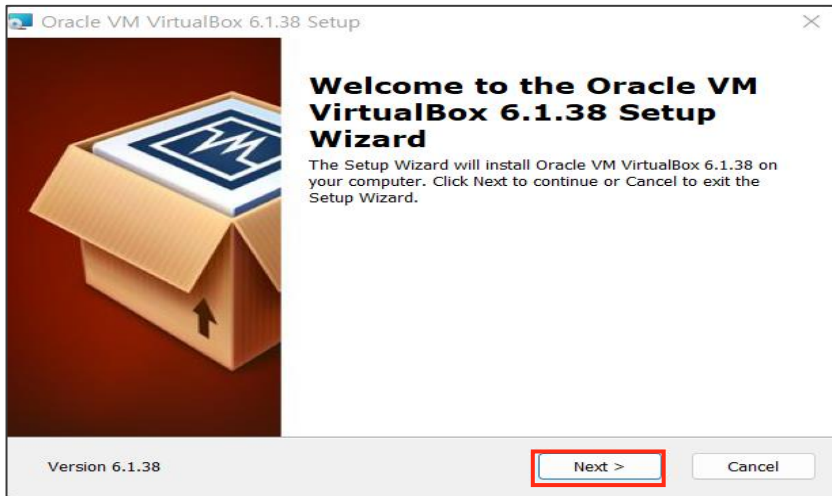
- 버추얼 박스 설치를 위해 표시된 버추얼 박스 설치파일을 실행



1. 환경 세팅

❖ 버추얼 박스 다운로드 [2/3]

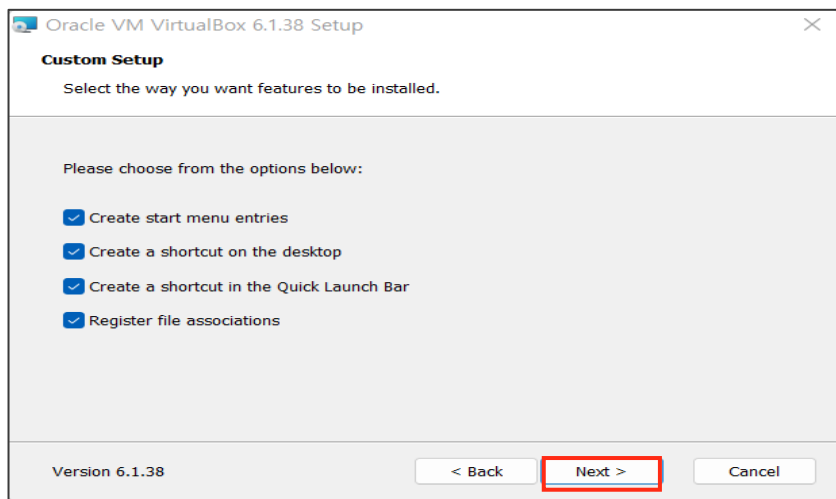
- 설치파일을 실행 시킨 후 모두 Next를 클릭



1. 환경 세팅

❖ 버추얼 박스 다운로드 [3/3]

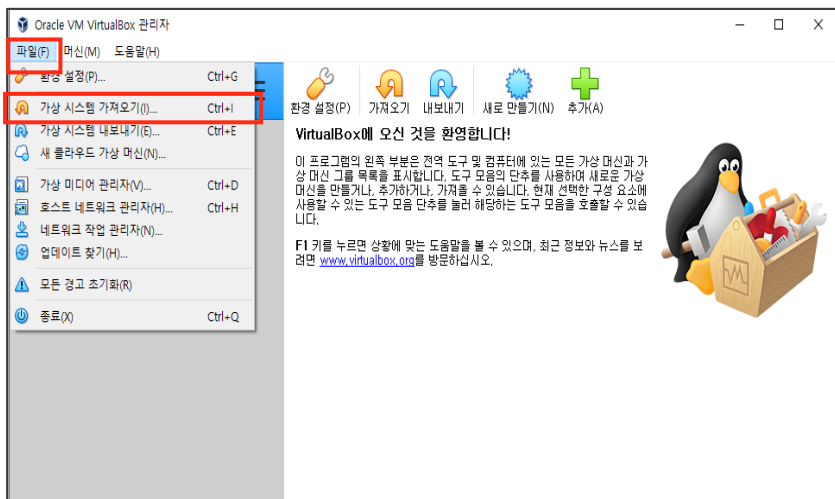
- 설치파일을 실행 시킨 후 모두 Next를 클릭



1. 환경 세팅

❖ 가상머신 설치[1/4]

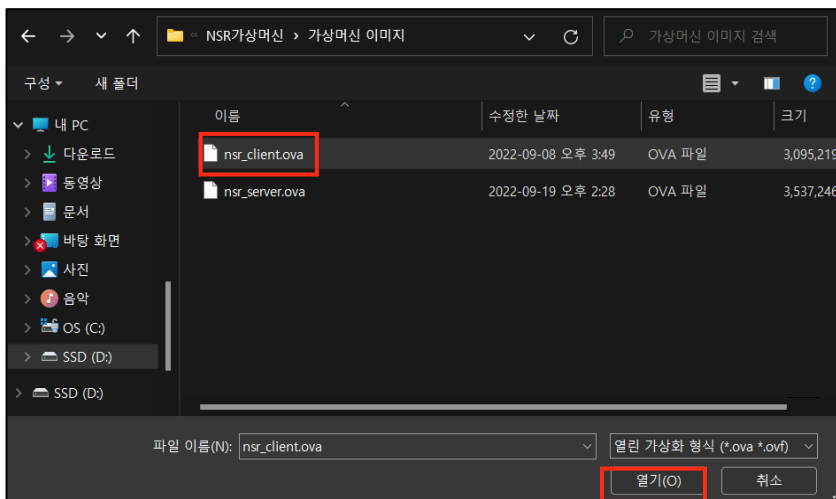
- 가상머신 이미지 파일에서 가상머신을 설치하기 위해 파일 -> 가상 시스템 가져오기 클릭
- 설치한 가상머신을 선택해야 하기 때문에 오른쪽 그림의 표시된 폴더 그림을 클릭



1. 환경 세팅

❖ 가상머신 설치 [2/4]

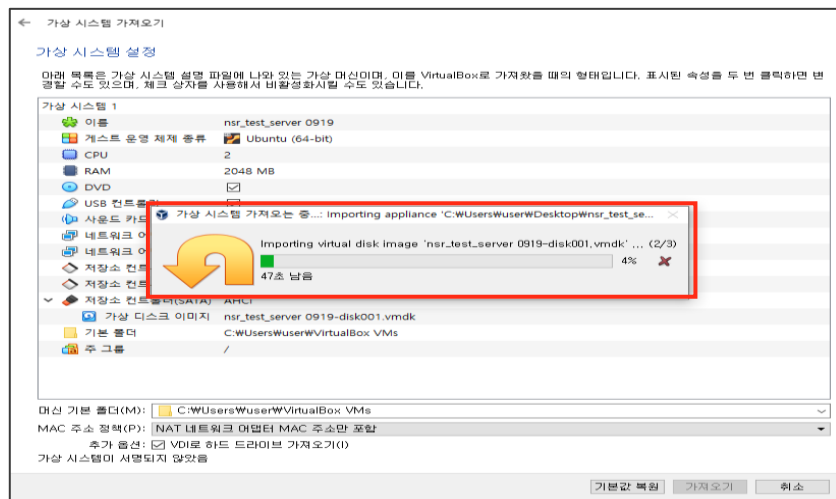
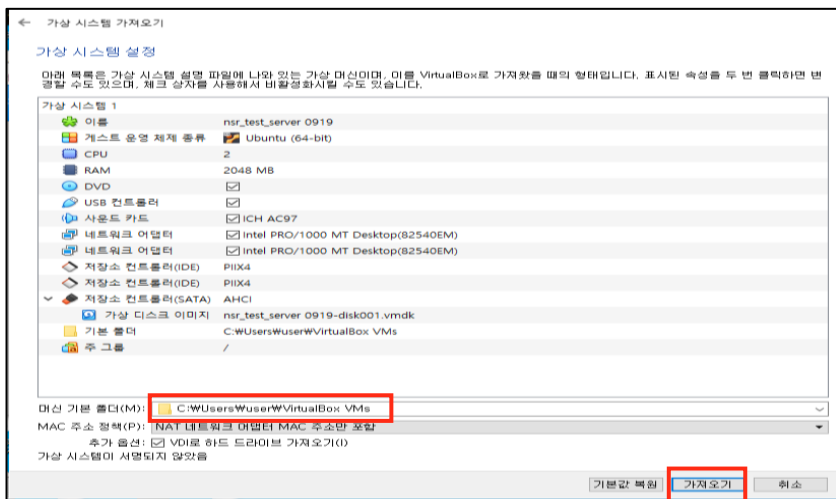
- 가상머신 이미지가 위치한 폴더로 이동하여 설치할 가상머신 이미지를 선택한 후 열기(O)를 클릭
- 오른쪽 그림처럼 가상머신 이미지가 성공적으로 선택된 것을 확인 후 다음(N)을 클릭



1. 환경 세팅

❖ 가상머신 설치[3/4]

- 가상머신을 설치할 폴더 경로를 지정한 후 왼쪽 그림과 같이 가져오기를 클릭
- 가져오기를 클릭하면 오른쪽 그림처럼 로딩을 시작



1. 환경 세팅

❖ 가상머신 설치 [4/4]

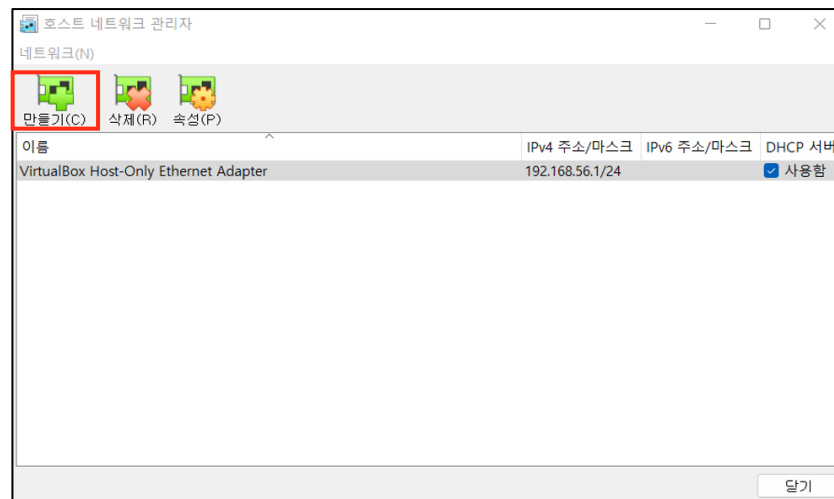
- 로딩이 완료되면 오른쪽 그림과 같이 가상머신 설치가 완료
- 서버 가상머신 또한 (1) ~ (3)의 과정을 진행



1. 환경 세팅

❖ 네트워크 세팅 [1/6]

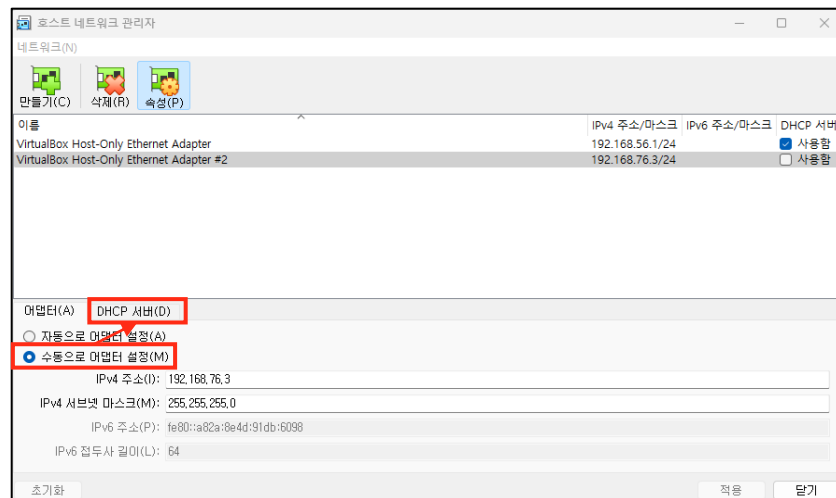
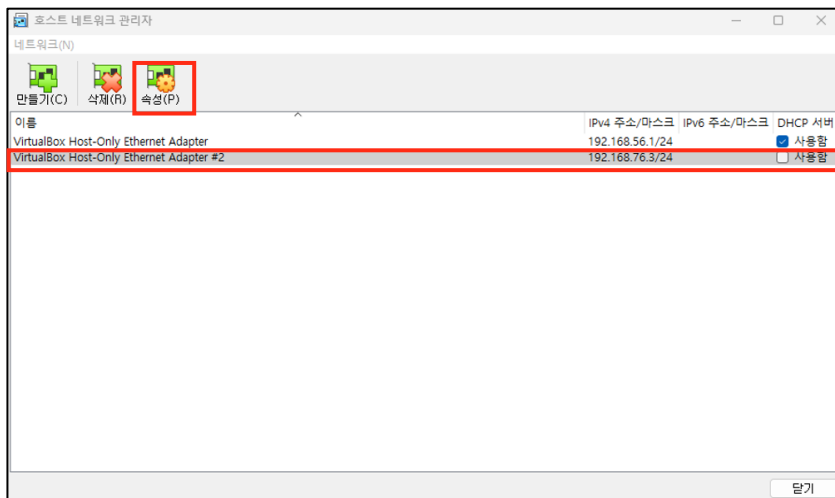
- 오른쪽 그림의 왼쪽 상단에 표시된 만들기(C) 클릭



1. 환경 세팅

❖ 네트워크 세팅 [2/6]

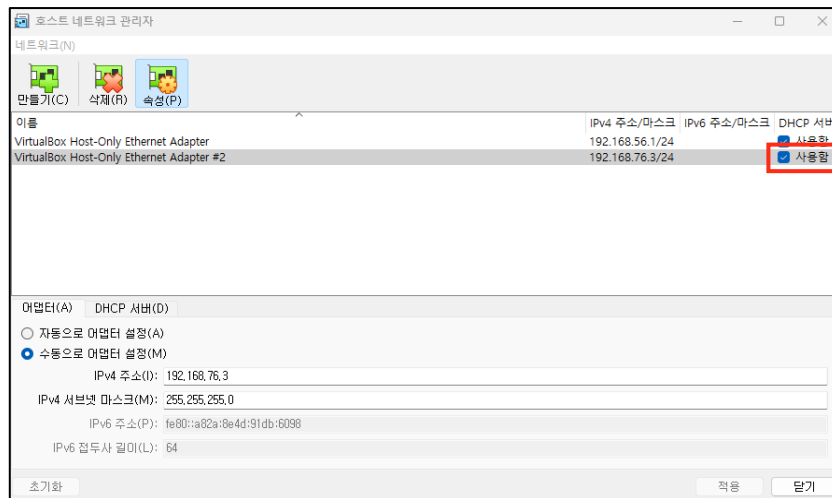
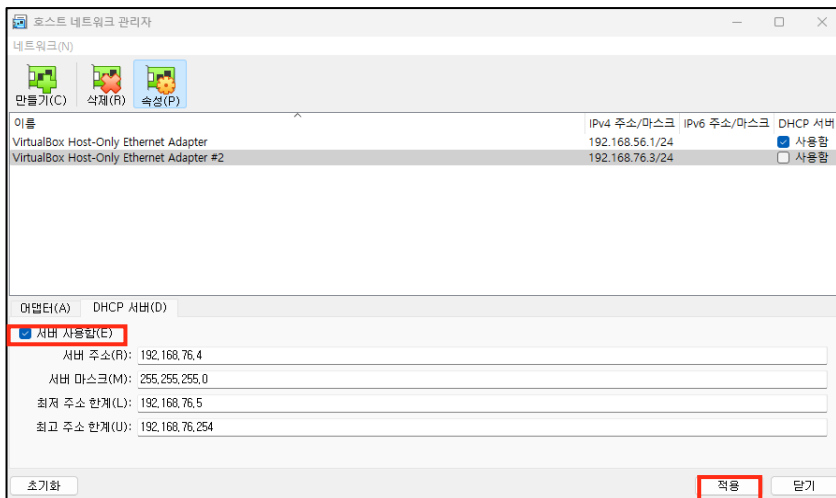
- 새로 생성된 네트워크 관리자 이름을 클릭한 후 표시된 속성을 클릭
- 속성을 클릭하면 오른쪽 그림과 같이 하단에 네트워크 정보가 보이며 표시된 '수동으로 어댑터 설정'을 클릭 후 DHCP 서버를 클릭



1. 환경 세팅

❖ 네트워크 세팅 [3/6]

- DHCP서버 클릭 후 표시된 '서버 사용함'을 클릭하여 오른쪽 하단에 '적용'을 클릭
- 성공적으로 적용이 되었다면 오른쪽 그림과 같이 표시된 '사용함'에 체크 표시를 확인 후 단기를 클릭



1. 환경 세팅

❖ 네트워크 세팅 [4/6]

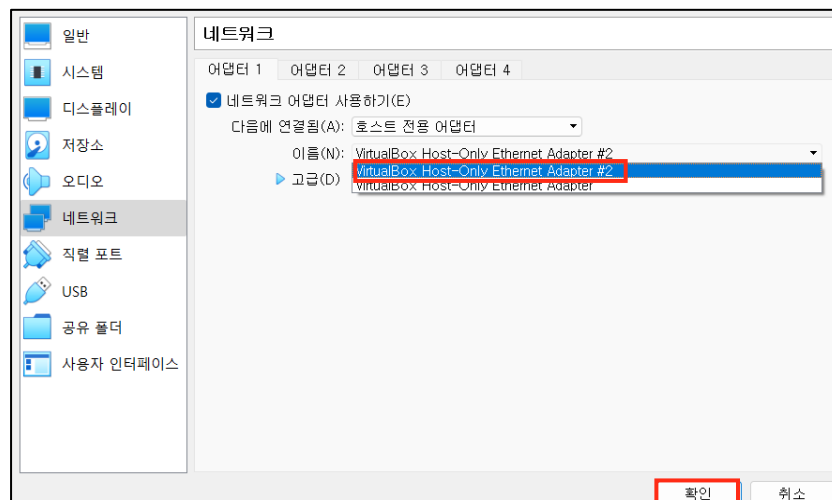
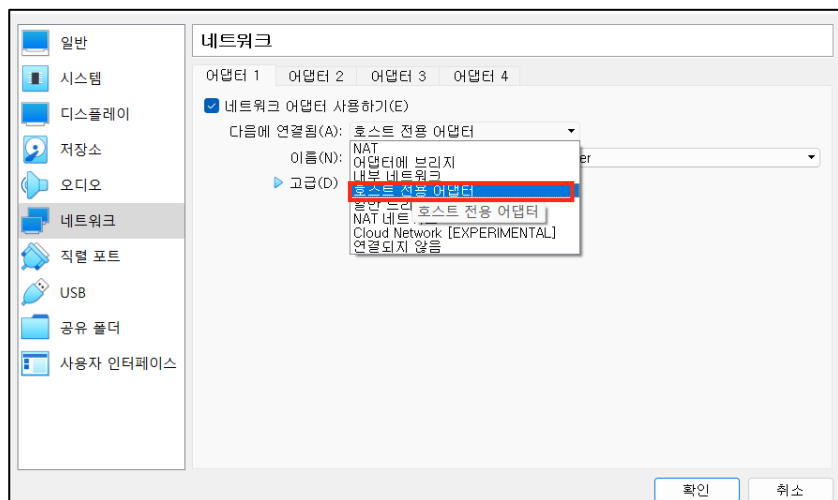
- 호스트 네트워크 관리자 설정 후 nsr_server 가상머신을 클릭 후 왼쪽 그림과 같이 표시된 설정(S)을 클릭
- 오른쪽 그림과 같이 설정화면에서 왼쪽에 표시된 '네트워크'를 클릭



1. 환경 세팅

❖ 네트워크 세팅 [5/6]

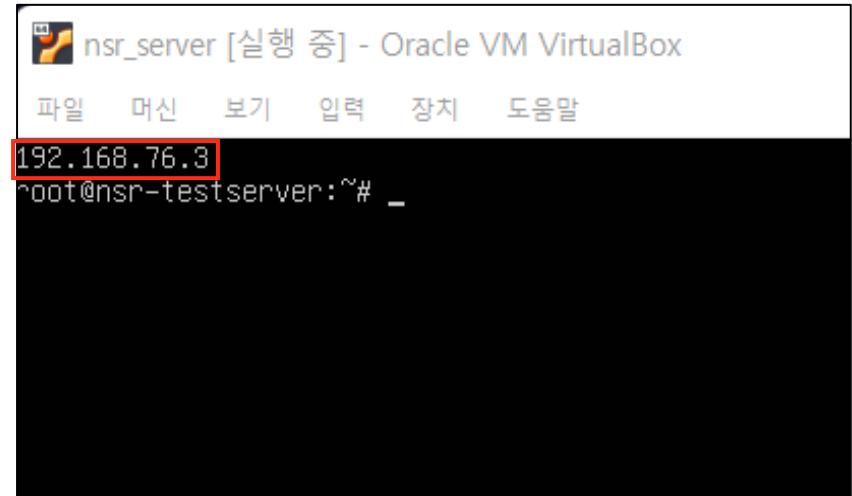
- 네트워크 클릭 후 표시된 '다음에 연결됨'에서 '호스트 전용 어댑터'를 선택
- 호스트 전용 어댑터 선택 후 이름(N) 클릭하여 (1)~(3)에서 설정한 어댑터를 선택 후 확인 버튼 클릭



1. 환경 세팅

❖ 네트워크 세팅 [6/6]

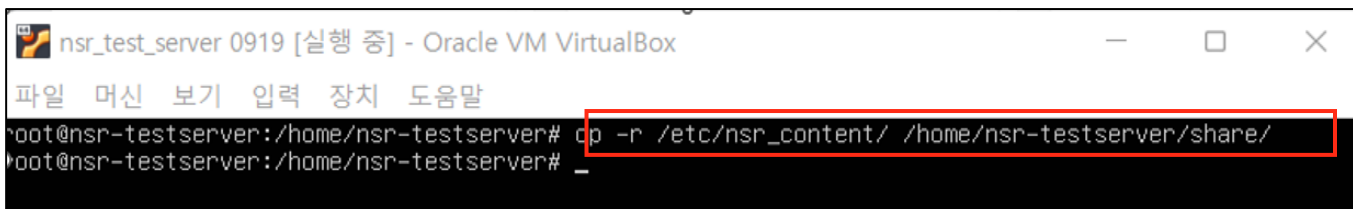
- 네트워크 설정 후 설정이 완료되었는지 확인하기 위해 nsr_server 가상머신 실행
- 성공적으로 IP가 설정된 것을 확인



1. 환경 세팅

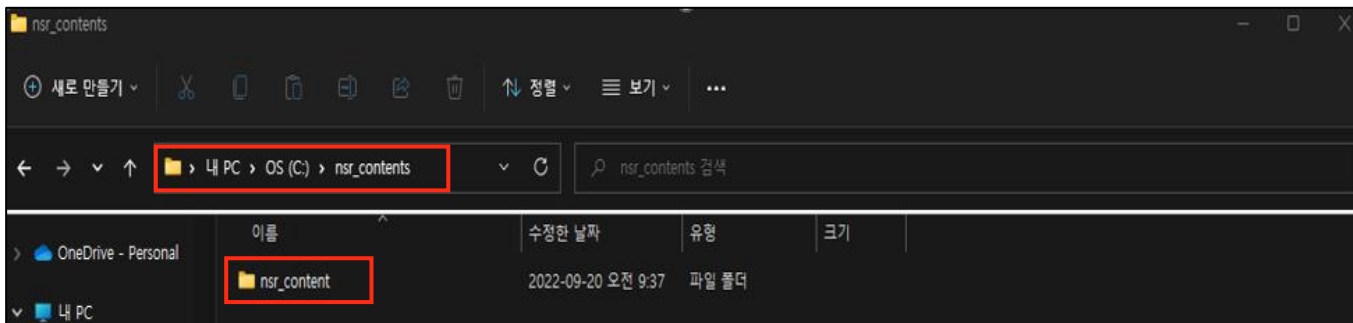
❖ 공유 디렉토리 설정

- 서버 가상머신 처음 부팅 시 초기 설정 명령어 실행(초기 세팅할 때 한번만 사용)
 - `cp -r /etc/nsr_content /home/nsr-testserver/share/`
 - 부팅 시 자동으로 `/home/nsr-testserver/share/` 폴더가 공유 디렉토리에 마운트됨



```
nsr_test_server 0919 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
root@nsr-testserver:/home/nsr-testserver# cp -r /etc/nsr_content /home/nsr-testserver/share/
root@nsr-testserver:/home/nsr-testserver# _
```

- 호스트PC의 C:\nsr_contents 폴더안에 nsr_content 폴더가 있으면 성공
 - 공유폴더인 nsr_contents폴더는 미리 수동으로 호스트의 C:\W 안에 생성해야 함



2. 실습 과제1: 보물찾기

❖ 실습 과제1: 보물찾기

• 소개

- 본 과제에서 보물은 “보안약점”을 의미한다. 조교가 제시하는 웹사이트에는 대표적으로 4가지 보안약점이 내재되어 있다. 대상 보안약점 목록은 다음과 같다.

No.	보안약점명
1	Improper Neutralization of Input During Web Page Generation (크로스사이트 스크립팅)
2	Improper Neutralization of Special Elements used in an SQL Command (SQL 삽입)
3	Improper Limitation of a Pathname to a Restricted Directory (경로순회)
4	Deserialization of Untrusted Data (역직렬화)

- 실습을 위한 웹사이트는 자바(Java) 언어로 작성된 코드이며 JSP * (Java Server Pages)와 JDBC * (Java Database Connectivity)를 사용한다.

* JSP는 HTML 내에 자바 코드를 삽입하여 웹 응용프로그램 서비스를 제공하며 동적으로 웹 페이지를 생성 후 웹 브라우저에 돌려주는 서버 사이드 스크립트 언어

* JDBC는 자바에서 데이터베이스에 접속할 수 있도록 하는 자바 API (Application Programming Interface)

2. 실습 과제1: 보물찾기

❖ 실습 과제1: 보물찾기

• 실습 내용

- 컴퓨터 보안을 수강하는 학생들은 다음 “실습시나리오 예제 구성”을 참고하여 웹사이트에 존재하는 최대한 많은 보물을 찾으시오!!

보안약점	실습시나리오 예제 구성
SQL 삽입	로그인창, 주소창, 검색창
크로스사이트 스크립트	Reflected XSS, Stored XSS, DOM based XSS
경로순회	파일 다운로드, 파일 내용 출력, 파일 삭제
역직렬화	데이터 위조, 원격 명령어 실행, 서비스 거부 공격

• 배점

- 10개 이상 찾을 시 만점
- 10개 미만 시 1개당 1점 감점

3. 실습 과제2: 보안약점 시나리오 작성

❖ 실습 과제2: 보안약점 시나리오 작성

• 소개

- 보물을 찾지 못했다면 직접 구상해보자. 본 실습은 보물찾기에서 내재되어 있는 보안약점 외에 다음 보안약점 4가지를 대상으로 실습 웹사이트에서 해당 보안약점들이 존재한다는 가정하에 직접 시나리오를 상세히 작성해 보는 것이다.

No.	보안약점명
1	Improper Input Validation (보안기능 결정에 사용되는 부적절한 입력값)
2	Unrestricted Upload of File with Dangerous Type (위험한 형식 파일 업로드)
3	Improper Restriction of XML External Entity Reference (부적절한 XML 외부 개체 참조)
4	Improper Control of Generation of Code (코드 삽입)

• 배점

- 보안약점 시나리오 한 개당 **1점** 부여

3. 실습 과제2: 보안약점 시나리오 작성

❖ 실습 과제2: 보안약점 시나리오 작성

• 시나리오 작성 양식 및 예시

➤ 시나리오는 다음의 양식을 만족해야 하며, 필요 시 몇가지 가정이나 항목을 추가하여 설명하여도 좋다.

1) 보안약점명

- ex. 위험한 형식 파일 업로드

2) 주제 및 시나리오

- ex. 시스템 제어 – 웹shell 파일 업로드 및 시스템 명령을 전송을 통한 시스템 제어

3) 보안약점 원인

- ex. 실습 웹사이트에서 게시판에 존재하는 파일 업로드 기능은 MultipartRequest 객체를 이용하고 있으며, 유저가 파일을 업로드 시 별도로 확장자 검사를 시행하지 않는다. 이는 즉, 서버 측에서 실행될 수 있는 스크립트 파일(asp, jsp, php 파일 등)이 업로드가 가능할 것이며 이 파일을 공격자가 웹으로 직접 실행시킬 수 있는 경우, 시스템 내부 명령어를 실행하거나 외부와 연결하여 시스템을 제어로 이어질 수 있다.

4) 공격방법

- 공격 시나리오를 설명할 수 있는 간단한 그림
- 공격을 시행하는 웹페이지 or 폼(form)
- 공격 절차 및 공격에 필요한 요소(코드, 스크립트, 문자열 등)

5) 대응방안

- 시큐어 코딩 적용 방법 및 코드
- 시큐어 코딩 적용 후 기대 효과

4. 실습 과제3: 보안약점 시나리오 구현

❖ 실습 과제3: 보안약점 시나리오 구현

• 소개

- 보물을 찾지 못했다면 직접 만들어보자. 본 실습은 보물찾기에서 내재되어 있는 보안약점 외 **실습 웹사이트에서 다음 보안약점 4가지를 대상으로 직접 작성한 시나리오를 구현**해 보는 것이다.

No.	보안약점명
1	Improper Input Validation (보안기능 결정에 사용되는 부적절한 입력값)
2	Unrestricted Upload of File with Dangerous Type (위험한 형식 파일 업로드)
3	Improper Restriction of XML External Entity Reference (부적절한 XML 외부 개체 참조)
4	Improper Control of Generation of Code (코드 삽입)

• 유의사항

- 실습 과제2를 통해 작성한 내용을 바탕으로 직접 구현하시오.
- 구현 과정과 결과에 대한 분석 내용을 작성하시오.

• 배점

- 보안약점 시나리오 구현당 **3점** 부여

Q&A