컴퓨터 보안_01

실습 1주차

동국대학교 CSDC Lab.
실습조교 김선규
2022.03.08 (Wed.)

Index

실습 강좌 소개

➢ 실습 진행 방법

- 간단한 이론 복습 및 해당주차 실습문제 설명
- 실습 후 보고서를 작성하여 다음주 화요일 자정(23:59) 까지 E-Class에 제출(이메일 제출 불가, 반드시 E-Class를 통해 제출)
- 실습 과제 제출 기한 엄수 **(제출기한 이후로는 0점 처리)**

➢ 실습 보고서 [1/2]

- 문제분석
  - 실습 문제에 대한 요구 사항 파악, 해결 방법 등 기술
- 프로그램 설계 / 알고리즘
  - 해결 방법에 따라 프로그램 설계 및 알고리즘 등 기술
  - 문제 해결 과정 및 핵심 알고리즘 기술
- 결과 / 결과 분석
  - 결과 화면을 캡쳐 하여 첨부, 해당 결과가 도출된 이유와 타당성 분석
- 소감
  - 실습 문제를 통해 습득할 수 있었던 지식, 느낀 점 등을 기술

실습 강좌 소개

➢ 실습 보고서 [2/2]

- 제출 방법
  - 보고서를 작성하여 E-Class “과제” 메뉴를 통해 제출
    - **“이름_학번_실습주차.zip” 형태로 제출 (e.g. : 홍길동_2022123456_실습1주차.zip)**
    - 파일명에 공백, 특수 문자 등 사용 금지
- 유의사항
  - 보고서의 표지에는 학과, 학번, 이름, 담당 교수님, 제출일자 반드시 작성
  - 정해진 기한 내 제출
    - **기한을 넘길 시 0점 처리**
    - E-Class가 과제 제출 마지막 날 오류로 동작하지 않을 수 있으므로, 최소 1~2일 전에 제출
    - 당일 E-Class 오류로 인한 미제출은 불인정
  - 보고서를 자신이 작성하지 않은 경우 실습 전체 점수 0점 처리
- 문의
  - code@dgu.ac.kr (실습조교 김선규)

패스워드 크래킹 (Password cracking)

dongguk UNIVERSITY

➢ 패스워드 크래킹?

- 패스워드 크래킹(password cracking)은 컴퓨터 시스템에 저장된 데이터 혹은 네트워크 상에서 전송되는 데이터를 이용하여 암호(password)를 복원하는 기술이다.

- 패스워드 크래킹의 목적 3가지
  - 암호를 잊어버린 사용자를 위해 암호를 복구하는 것
  - 시스템에 허가되지 않은(unauthorized) 접속을 하는 것
  - 관리자가 자신이 설정한 암호가 풀기 쉬운지 체크하는 것

- 암호를 푸는데 걸리는 시간은 암호 강도(password strength)와 관련이 있다.
- 대부분의 패스워드 크래킹 기법은 다수의 후보 암호를 생성하여 크래킹 한다.

패스워드 크래킹 종류 (Password cracking)

dongguk UNIVERSITY

- **Brute-force cracking**
  - 가장 기본적인 방법으로 모든 가능한 후보 암호들(candidate passwords)을 생성하여 성공할 때까지 시도하는 방법이다.

- **Dictionary attacks**
  - 사전에 있는 단어를 입력하여 암호를 알아내거나 해독하는 공격 방법이다.

- **Pattern checking**
  - 데이터를 검색할 때 특정 패턴이 출현하는지, 또한 어디에 출현하는지 등을 특정하는 방법의 일종이다.
  - 대량의 데이터를 다룰 때 효율적으로 쓰일 수 있다.

…

패스워드 크래킹 도구 (Password cracking)

dongguk UNIVERSITY

- Cain and Abel
  - 네트워크 패킷 스니핑, 사전 공격, 무차별 대입 및 암호 분석 공격과 같은 방법을 사용하여 다양한 암호 해시 크래킹과 같은 방법을 사용하여 다양한 종류의 암호를 복구 할 수 있다.

- John the Ripper
  - 존더리퍼는 패스워드의 강도를 테스트하는 윤리적 해커에게 아주 유용한 도구이다.

- Hydra
  - 네트워크 로그인/패스워드 크래킹 툴이며 수많은 프로토콜을 지원하고 병렬 연산을 매우 빠르게 크래킹한다.

- ElcomSoft
  - 1990년 설립된 회사로 암호 및 시스템 복구 소프트웨어에 중점을 둔 컴퓨터 보안 프로그램 개발 회사이다.

실습 환경 : WSL2 소개 및 설치

dongguk UNIVERSITY

- **WSL2(Windows Subsystem for Linux)**
  - Windows에서 ELF64 Linux 이진 파일을 실행할 수 있게 해주는 서브시스템(Subsystem)이다.

- **WSL 사용**
  - 윈도우 시작 버튼 → Powershell 검색 → 마우스 오른쪽 버튼(클릭) → Powershell(관리자) 실행

- **Virtual Machine 사용(Powershell 에 명령어 입력)**
  - dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
  - dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart

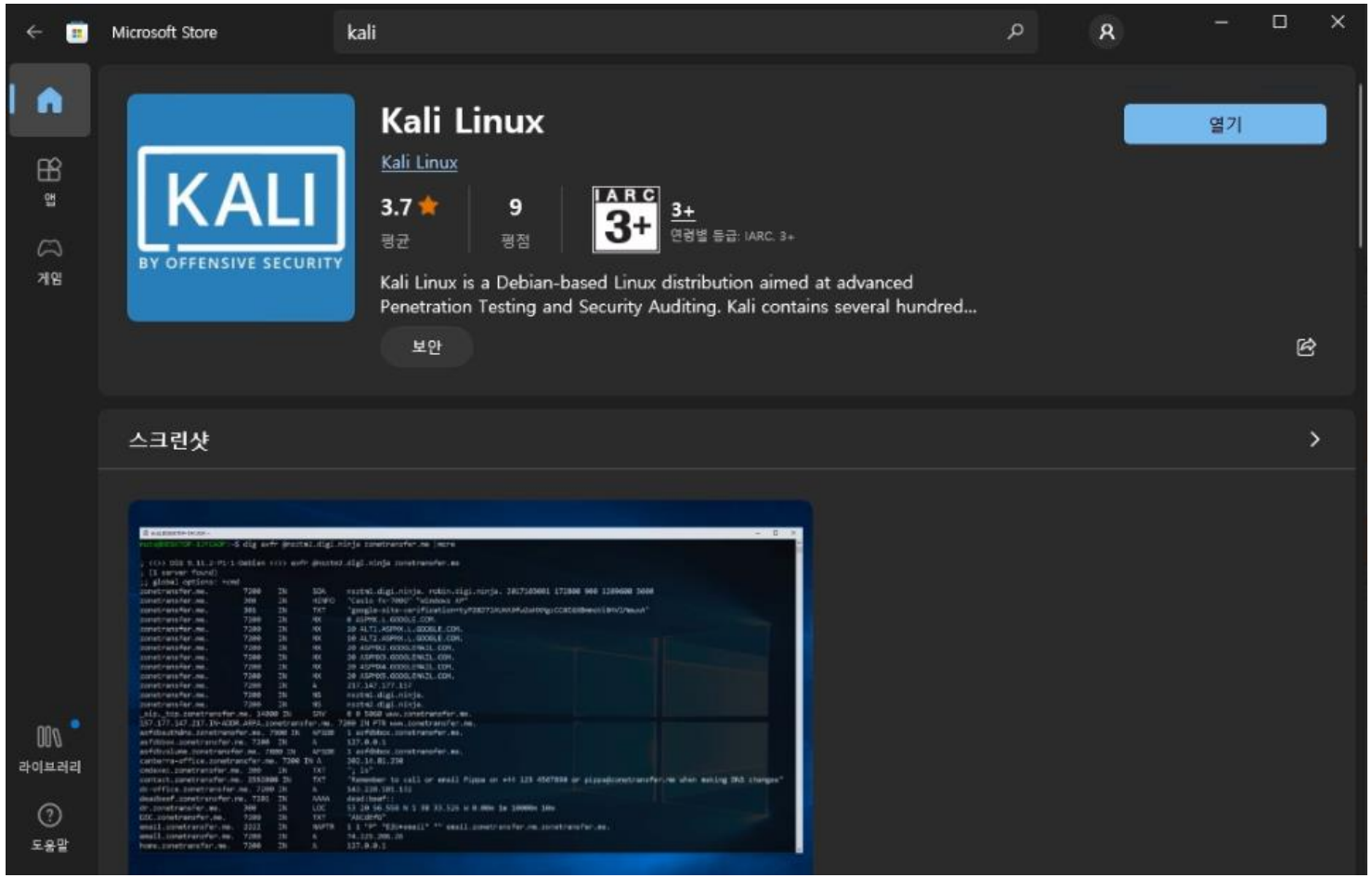
- **WSL2 커널 업데이트**
  - wsl --set-default-version 2

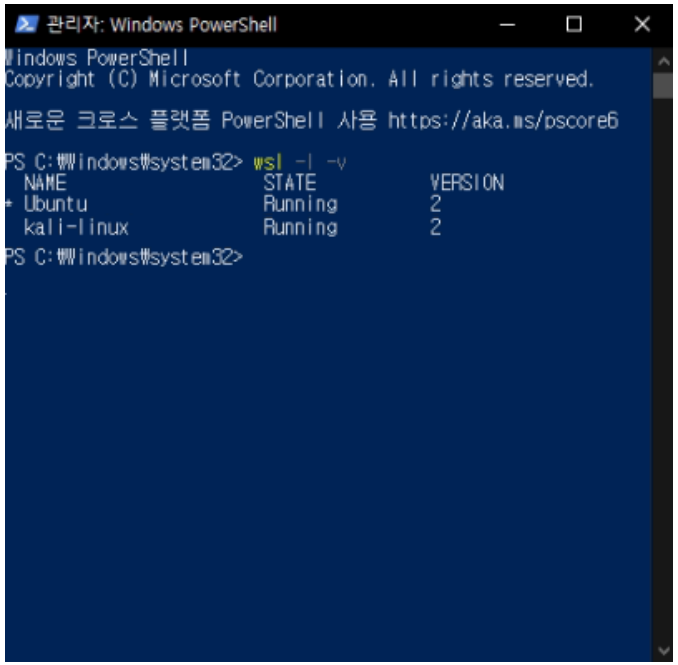
실습 환경 : Kali Linux on WSL2

dongguk UNIVERSITY

➢ Kali Linux on WSL2 설치

- Microsoft Store 접속 → kali 검색 → Kali Linux → 설치





실습 환경 : Kali Linux GUI 세팅

dongguk UNIVERSITY

- Kali Linux 실행 → 터미널 접속 → username & password 설정

- Kali Linux 업데이트
  - sudo apt update && sudo apt upgrade -y

- GUI 환경 Xfce 설치
  - sudo apt install kali-desktop-xfce

- Kali Linux 기본 tool 설치
  - sudo apt install kali-linux-default

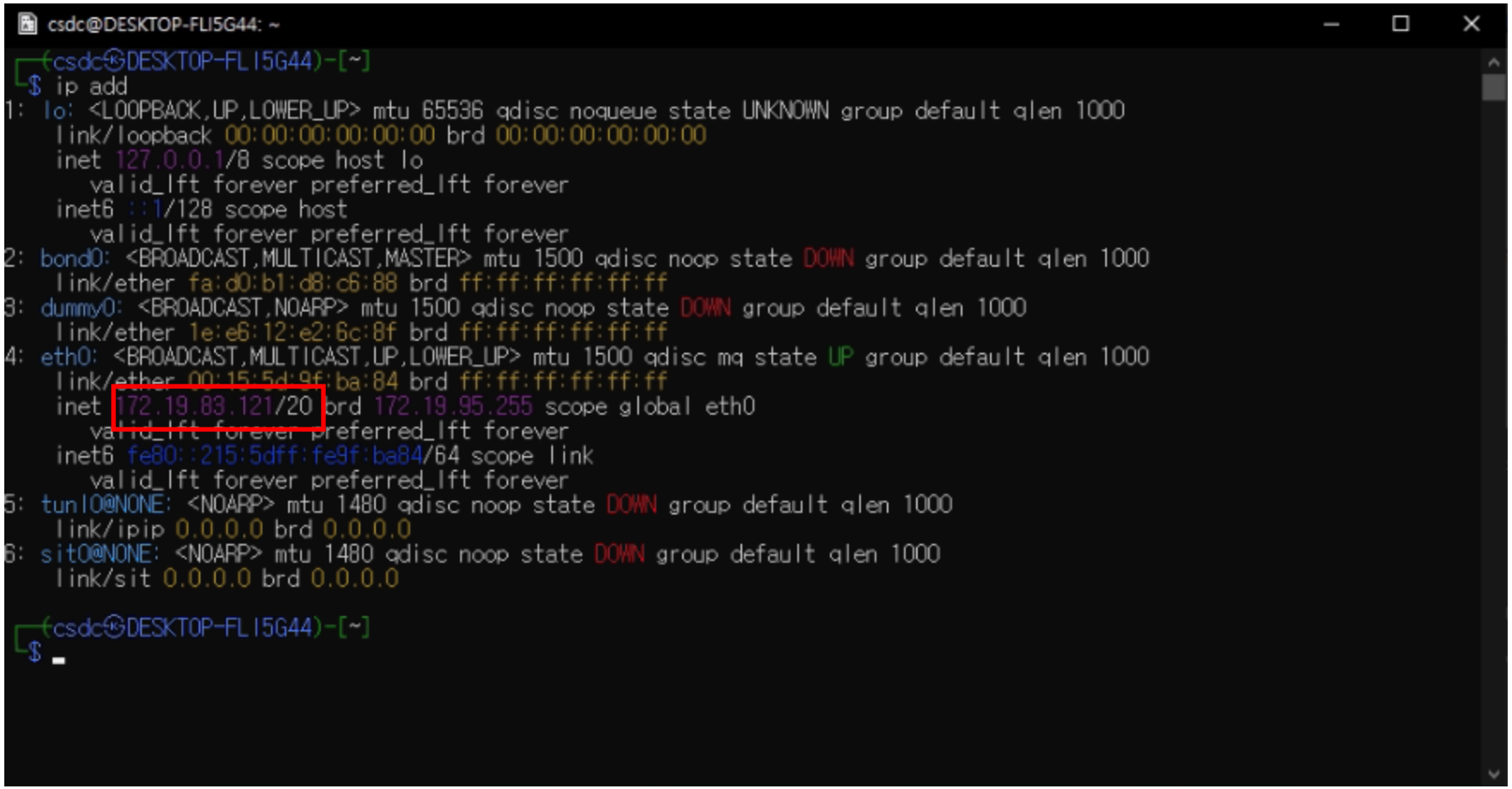
- Xrdp 설치 및 서비스 실행
  - sudo apt install xrdp -y
  - sudo service xrdp start

실습 환경 : Kali Linux GUI 접속을 위한 ip 확인

dongguk UNIVERSITY

➢ Kali Linux GUI 실행

- 시작 버튼 → Kali Linux 검색 → Kali Linux 실행 → $ ip add → ip 확인

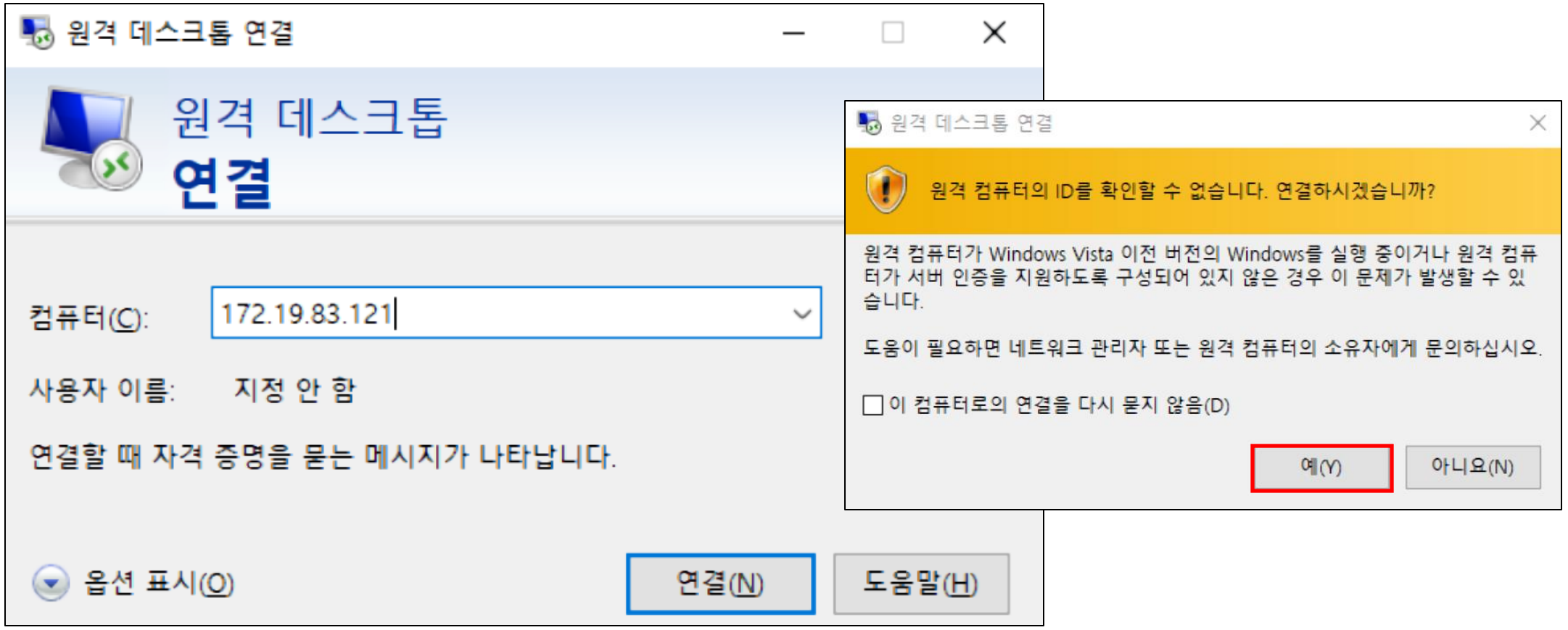


실습 환경 : Kali Linux GUI 원격 데스크톱 연결

dongguk UNIVERSITY

➢ Kali Linux GUI 실행

- 시작 버튼 → “원격 데스크톱 연결” 검색 → ip 입력 → 연결(N) → 예(Y)

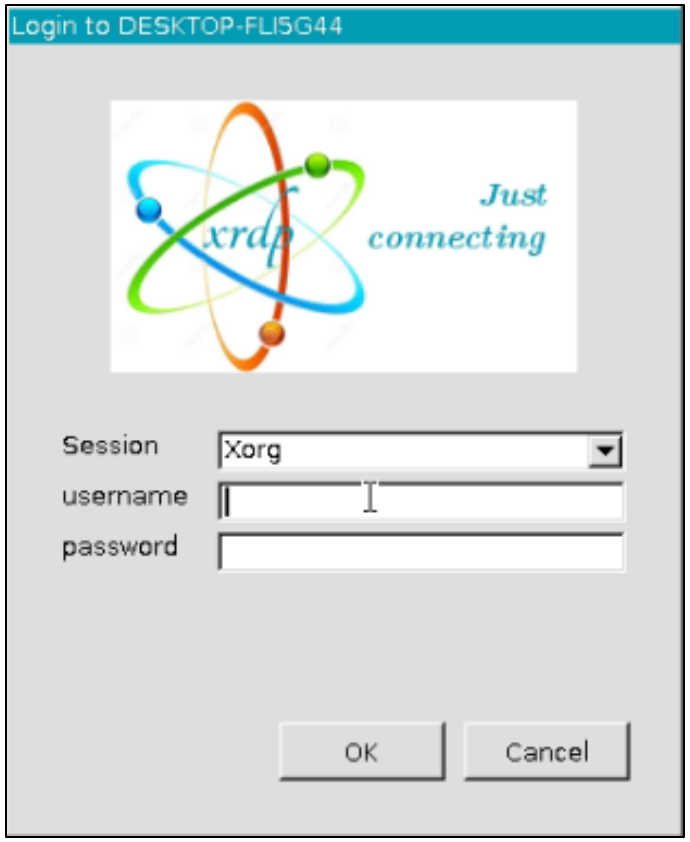


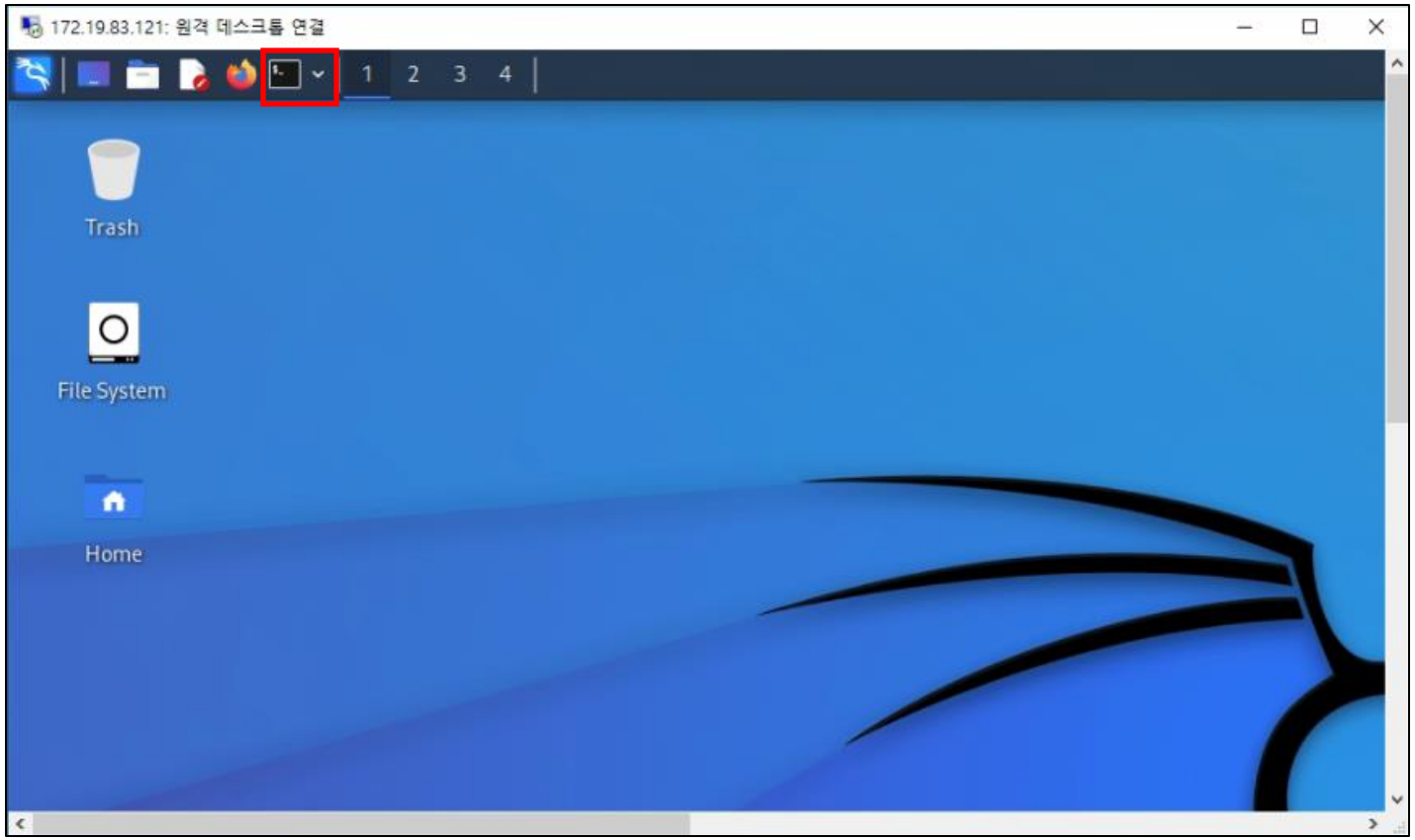
실습 환경 : Kali Linux GUI 원격 데스크톱 연결

dongguk UNIVERSITY

➢ Kali Linux GUI 로그인

- 초기 입력한 username & password 입력 후 Kali Linux GUI 원격 연결





실습 과제 1 : John the Ripper

dongguk UNIVERSITY

➢ Linux Password Cracking

- Kali linux에 내장되어 있는 JTR(John the Ripper) 사용
- JTR(John the Ripper)이 내장되어 있지 않다면 공식 홈페이지 (http://www.openwall.com/john) 접속 후 설치 (ver 1.9.0)

1. 터미널 창을 열어 sudo su 명령을 통해 관리자 권한을 획득, JTR을 설치 및 압축 해제 후 해당 폴더의 src폴더에서 컴파일을 진행 후 run 디렉토리로 이동한다.

2. 기존의 패스워드를 크래킹하기 전에, 몇 개의 사용자를 더 추가하여 패스워드가 얼마나 빨리 크래킹되는지 확인한다. adduser 명령을 통해서 사용자를 추가한다. 3개의 사용자를 user1, user2, user3로 명명하고, 각 사용자의 패스워드를 apple, b4n4n4, P@ssw0rD로 세팅한다.

3. 3개의 사용자를 추가한 후에 명령라인에서 ./john -format=crypt /etc/shadow를 입력하여 존더리퍼를 실행한다.

4. 각 패스워드를 크래킹하는데 얼마나 소요되는지 살펴보자. 패스워드를 크래킹하는데 소요되는 시간과 패스워드의 복잡성은 서로 연관이 있다. 더 복잡한 패스워드를 찾기 위해서는 시간이 더 오래 걸린다.

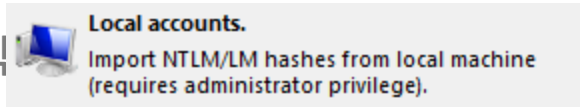
실습 과제 2 : Hash Suite

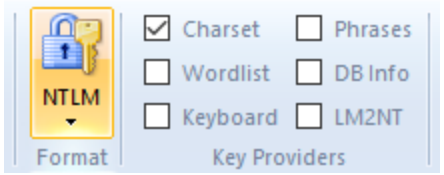
➢ Windows Password Cracking

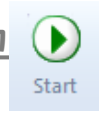
- Hash Suite의 공식 홈페이지 (https://hashsuite.openwall.net/download)

1. Windows 전용 Hash Suite 무료 버전을 설치한다.

2. 기존의 패스워드를 크래킹하기 전에, 몇 개의 윈도우 사용자를 더 추가하여 패스워드가 얼마나 빨리 크래킹되는지 확인한다. 윈도우의 '계정 관리'에서 사용자를 추가한다. 3개의 사용자를 user1, user2, user3로 명명하고, 각 사용자의 패스워드를 apple, b4n4n4, P@ssw0rD로 세팅한다.

3. Hash_Suite_64.exe 실행 후,좌측 상단의  클릭 후 Import → local accounts 클릭 

4. Main 탭에서 

Charset 체크하고 

크래킹을 시작한다.

실습 후 보고서 내용 정리 항목

dongguk UNIVERSITY

➢ **주요 작성 항목**

1. 실습 환경 (가상 환경 종류 및 실습 컴퓨터 사양)

2. 실습을 진행하며 진행 내용 정리

- 진행 내용
- 어려웠던 점
- 유의사항

3. 실습을 진행하며 새로 알게 된 내용 기술

Q & A

Thank you