

정보보호론 실습

브루트 포스 (존 더 리퍼)

브루트 포스(brute-force attack)

- **brute**는 "짐승같은, 난폭한"이라는 뜻이고, **brute-force**는 "난폭한 힘, 폭력"이라는 뜻이며, 암호학 용어로는 **brute-force attack** 또는 **exhaustive key search** 불림
- 조합 가능한 모든 문자열을 하나씩 대입해 보는 방식으로 문제를 푸는 방식으로 무식한 방법이지만 가장 무서운 기술

브루트 포스(brute-force attack)

- 실습 후 제출
 - 실습 화면 캡처
 - 분석 : 공격을 통해 파악할 수 있는 정보 (캡처x)
 - Ex) ooo 명령을 통해 패스워드, 고객주소, 핸드폰 번호등을 알 수 있었음
 - Ex2) ooooo 소스코드를 통해 ooo에 취약함
 - Ex3) ooo 명령을 방어할 수 있는 방안
- 제출 메일주소 : nykim@seoultech.ac.kr

브루트 포스(brute-force attack)

- 존 더 리퍼 설치 방법

- <http://www.openwall.com/john/> 설치
- [John the Ripper 1.7.9 \(Windows - binaries, ZIP, 2029 KB\)](#) and its [signature](#) 를 다운

John the Ripper is free and Open Source software, distributed primarily in source code form. If you would rather use a commercial product tailored for your specific operating system, please consider *John the Ripper Pro*, which is distributed primarily in the form of "native" packages for the target operating systems and in general is meant to be easier to install and use while delivering optimal performance.

Proceed to *John the Ripper Pro* homepage for your OS:

- John the Ripper *Pro* for Linux
- John the Ripper *Pro* for Mac OS X
- On Windows, consider [Hash Suite](#) (developed by a contributor to John the Ripper)

Download one of the latest *official free versions* (release notes):

- John the Ripper 1.7.9 (Unix - sources, tar.gz, 848 KB) and its signature
- John the Ripper 1.7.9 (Unix - sources, tar.bz2, 701 KB) and its signature
- [John the Ripper 1.7.9 \(Windows - binaries, ZIP, 2029 KB\) and its signature](#)

Download the latest *community-enhanced* version (release notes):

- John the Ripper 1.7.9-jumbo-6 (Unix - sources, tar.gz, 1892 KB) and its signature
- John the Ripper 1.7.9-jumbo-6 (Unix - sources, tar.bz2, 1564 KB) and its signature
- [John the Ripper 1.7.9-jumbo-5 \(Windows - binaries, ZIP, 3845 KB\) and its signature](#)



브루트 포스(brute-force attack)

- 존 더 리퍼 설치 방법
 - <http://www.openwall.com/john/> 설치
 - [John the Ripper 1.7.9 \(Windows - binaries, ZIP, 2029 KB\)](#) and its [signature](#) 를 다운
 - 다운 후에 경로를 그림과 같이 설정(ex=C:\PC\john179w2\john179\run)

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\KimNamYong>cd
```

```
C:\>cd C:\Documents and Settings\KimNamYong\바탕 화면\john179w2\john179\run
```

브루트 포스(brute-force attack)

- 존 더 리퍼 사용 방법
 - <http://twodragon.tistory.com/179> 에서 pass.txt 파일 다운로드
 - 암호화된 pass.txt 를 패스워드 공격 실행하여 해독 패스워드를 알려줌

```
C:\Documents and Settings\KimNamYong\바탕 화면\john179w2\john179\run>john.exe pass.txt
Loaded 36 password hashes with no different salts (FreeBSD MD5 [32/32])
No password hashes left to crack (see FAQ)
```

```
C:\Documents and Settings\KimNamYong\바탕 화면\john179w2\john179\run>john.exe pass.txt
Loaded 36 password hashes with no different salts (FreeBSD MD5 [32/32])
```

Q & A