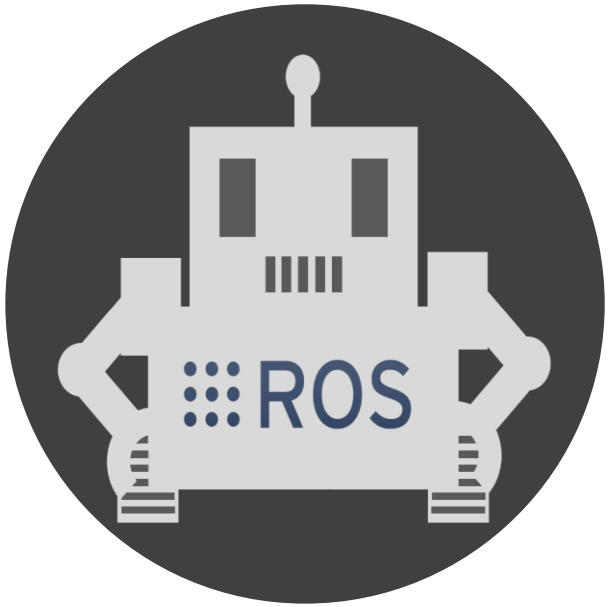
리눅스 해킹&보안

Chapter 6. 악성코드

구선생 로보틱스



Update 20240521

강의 자료 다운로드

리눅스 해킹&보안 강의 노트

https://github.com/DoveSensei/HackingSecurity

1. 악성코드란?
2. 악성코드 감염 사례
3. 악성코드 탐지

악성코드란?

개요

컴퓨터 시스템에 손상을 주거나
원치 않는 행동을 하도록 설계된 소프트웨어

악성코드란?

개요

- 바이러스 : 다른 프로그램이나 파일에 자신을 복제하여 삽입함으로써 퍼지는 악성코드, 감염된 파일이 실행될 때 활성화되며 시스템에 손상을 줄 수 있다.
- 웜 : 네트워크를 통해 스스로 복제하여 퍼지는 악성코드. 독립적으로 작동하며 감염된 시스템의 네트워크 성능을 저하시킬 수 있다
- 트로이 목마 : 유용한 프로그램인 척하며 사용자에게 설치되도록 유도한 후, 백그라운드에서 악성 활동을 수행하는 악성코드. 시스템에 백도어를 열어 해커가 접근할 수 있게 하거나, 데이터를 탈취하는 데 사용될 수 있다.

악성코드란?

개요

- 랜섬웨어 : 사용자의 파일을 암호화하여 접근을 차단하고, 이를 해제하는 대가로 금전을 요구하는 악성코드.
- 스파이웨어 : 사용자의 동의 없이 컴퓨터 활동을 감시하고 정보를 수집하는 악성코드. 주로 개인 정보나 금융 정보를 탈취하는 데 사용.
- 애드웨어 : 사용자의 동의 없이 광고를 표시하는 악성코드.
  광고 수익을 목적으로 하며, 시스템 성능 저하를 초래할 수 있다.

1. 악성코드란?
2. 악성코드 감염 사례
3. 악성코드 탐지

악성코드 감염 사례

웹 취약점을 통한 악성 코드 감염

- 패키지 업데이트

```
$ sudo apt-get update
```

- 패키지 업그레이드

```
$ sudo apt-get upgrade
```

- 아파치 웹 서버 설치

```
$ sudo apt-get install apache2
```

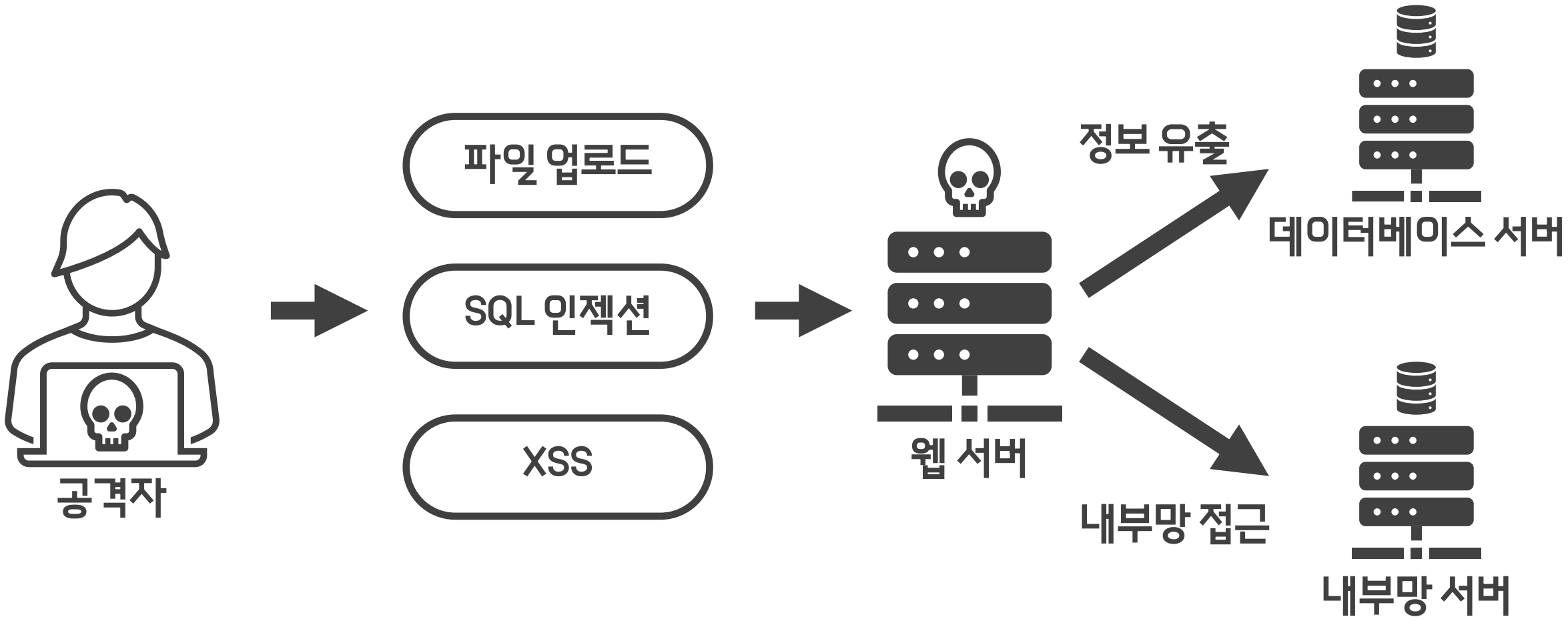
- MariaDB 설치

```
$ sudo apt-get install mariadb-server
```

데이터 베이스는 웹서버와 함께 동작하기 때문에
셋업 방법은 동일하다.

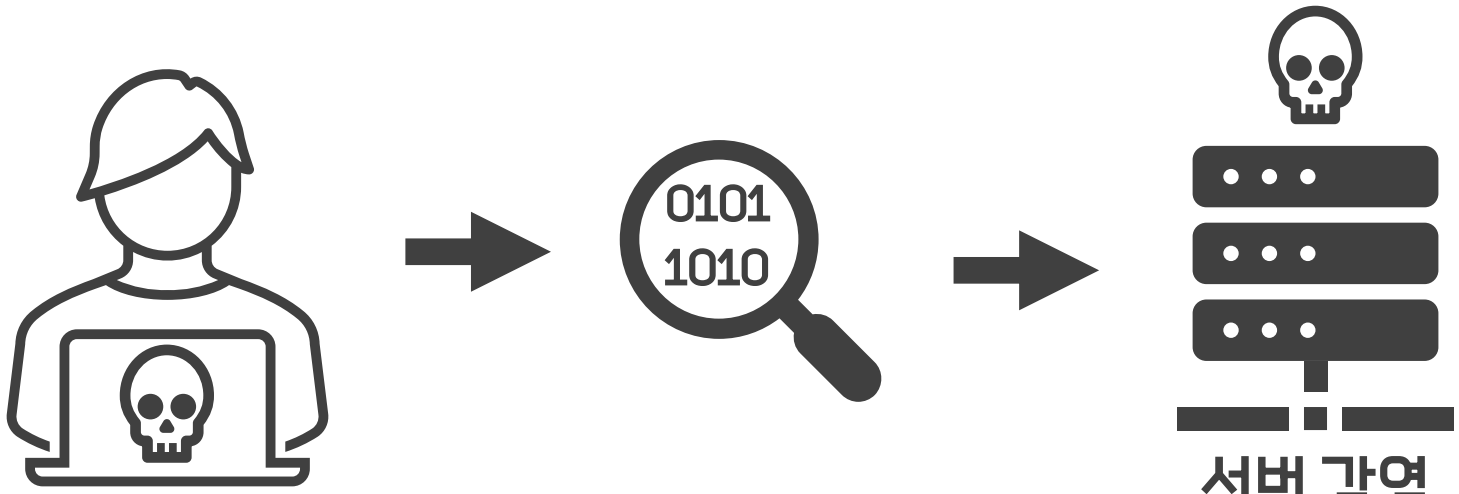
악성코드 감염 사례

웹 취약점을 통한 악성 코드 감염



악성코드 감염 사례

시스템 취약점을 통한 악성 코드 감염



1. 악성코드란?
2. 악성코드 감염 사례
3. **악성코드 탐지**

악성코드 탐지

백신 설치

- 패키지 업데이트

```
$ sudo apt-get update
```

- 패키지 업그레이드

```
$ sudo apt-get upgrade
```

- ClamAV 백신 설치

```
$ sudo apt-get install clamav
```

- ClamAV 업데이트 데몬 실행

```
$ sudo systemctl restart clamav-freshclam.service
```

악성코드 탐지

악성코드 탐지 실행

- ClamAV 백신 악성코드 탐지 명령어

```
$ sudo clamscan -r [검사경로] --move=[감염파일 격리 경로]
```

```
$ sudo clamscan -r /home/ubuntu/ --move=/home/ubuntu/malware
```

```
----------- SCAN SUMMARY -----------
Known viruses: 8693036
Engine version: 0.103.11
Scanned directories: 165
Scanned files: 157
Infected files: 0
Data scanned: 5.23 MB
Data read: 10.30 MB (ratio 0.51:1)
Time: 34.235 sec (0 m 34 s)
Start Date: 2024:05:21 12:05:59
End Date:   2024:05:21 12:06:33
```

감사합니다

구선생 로보틱스