



시스템 해킹이란 무엇인가?

System Hacking Tutorial

Kali Linux를 이용한 Reverse Engineering의 이해

[BOSS] 손 우 규

<https://github.com/swk3169/system-hacking>

목차

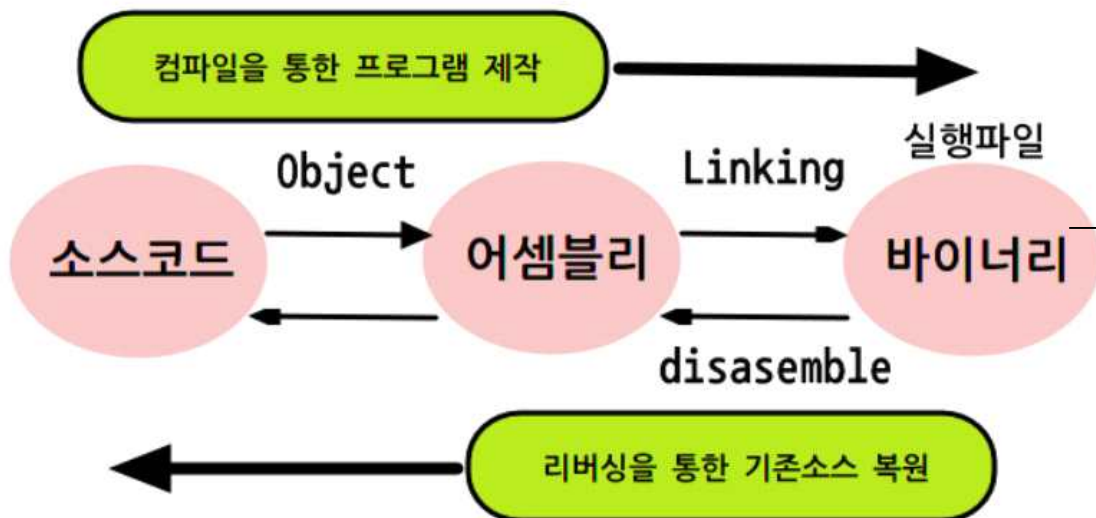
1. Reverse Engineering	1
1.1 정의	
1.2 위험성	
1.3 공격법	
1.4 방어법	
2. 실습	6
2.1 Assembly "Hello World"	
3. 참조	11

1. Reverse Engineering

1.1 정의

리버스 엔지니어링(Reverse Engineering)은 인조물로 부터 청사진을 얻는 것에서 유래되었다. 이진 코드로 되어 있는 실행 파일을 분석하려는 일련의 행위이다. 소프트웨어를 분석하고 동작을 해명해나가는 것을 리버스 엔지니어링이라 부른다. 이것은 멀웨어에 한정하지 않고 일반적인 소프트웨어를 분석하는 것을 말하기 때문에, 컴퓨터 보안과 관계가 없는 곳에서도 사용된다.

1.2 위험성



윈도우 보안 패치나 인터넷에 돌아다니는 바이러스 확인방법도 리버싱의 산물이다. 예로 워너크라이 랜섬웨어가 전파되었을 때 파일 공유 설정을 해제하게 시킨 것도 랜섬웨어의 작동 방식을 분석했기 때문이다.

DOC은 사실상 표준 문서 포맷이었지만 구조가 비공개되어 오랜 기간 마이크로소프트가 사실상 독점하고 있었다. 그러나 썬 마이크로시스템즈와 오픈오피스 재단이 리버스 엔지니어링을 시행하였고, 이후 포맷 구조를 공개했다.

KOF 시리즈를 늘 괴롭혀 온 치트로 해금하는 캐릭터나 플레이 불가 보스 캐릭터를 처음부터 고를수 있게 연락하고 파워 게이지 무한등의 개조가 가해진 개조 롬도 소프트웨어 리버스 엔지니어링의 산물이다.

1.3 공격법

- 키젠



리버싱 해킹의 가장 일반적인 예로, 키젠과 크랙을 들 수 있다. 소프트웨어를 설치할 때 보통 시리얼 넘버를 요구하는 경우가 많은데, 리버싱 과정을 통해, 시리얼 넘버의 알고리즘을 분석해 키젠을 만들어 소프트웨어를 불법으로 사용하는 경우가 많이 있다.

- 크랙



크랙의 경우 특히 게임을 해킹하는 사례가 많으며, 위의 사이트는 게임 해킹과 불법 복제로 유명한 skidrow(스키드로우) 해커 그룹의 홈페이지이다.

1.4 방어법

클라이언트 컴퓨터에서 실행되는 프로그램의 리버싱을 막을 방법은 없다. CPU로 로드될 시점에는 반드시 기계어로 번역돼야 하기 때문에 기계어 코드를 직접 메모리에서 덤프해서 리버싱하면 그만이기 때문이다.

- 정보 은닉

클라이언트에서 중요한 코드를 실행하지 않으면 된다. 서버에 중요 로직을 보관하고 API만 오픈한 경우에는 해킹 말고는 코드를 리버싱할 방법이 없다. 그래서 요즘에는 중요한 코드를 서버에 두고, 소비자에게는 API만을 노출시켜 사용하게 하는 방법으로 리버싱을 방어하고 있다. 단점은 사용자가 항상 온라인 상태여야 한다는 것, 사용자가 늘어나면 서버 부하가 커진다는 등이다.

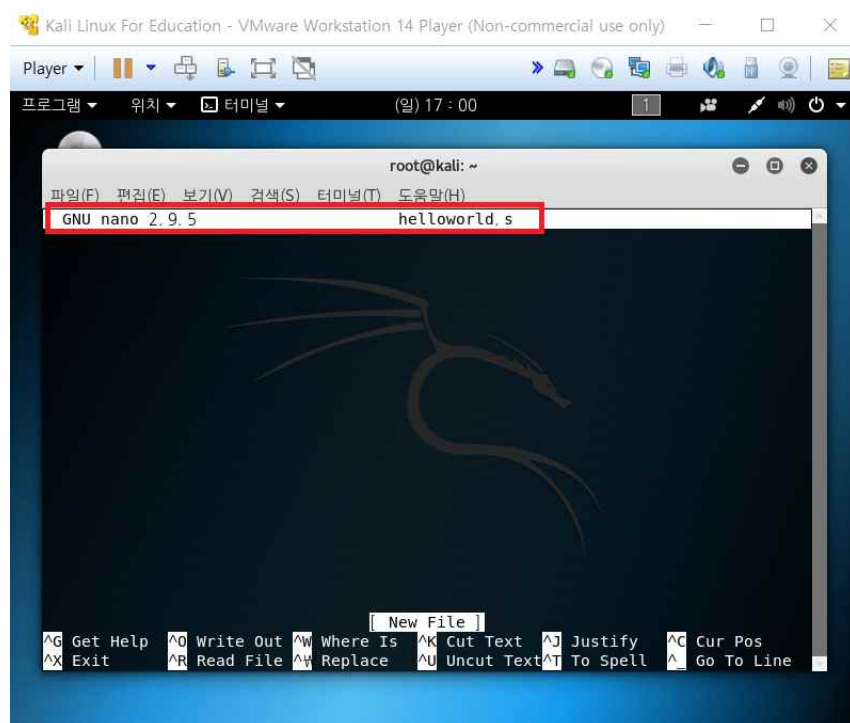
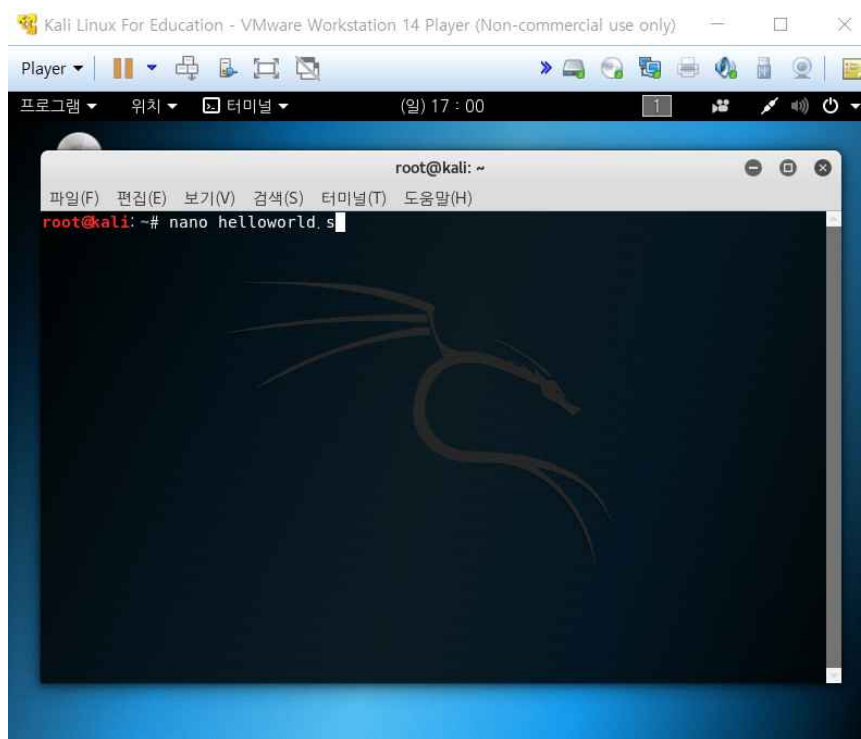
- 암호화 및 난독화

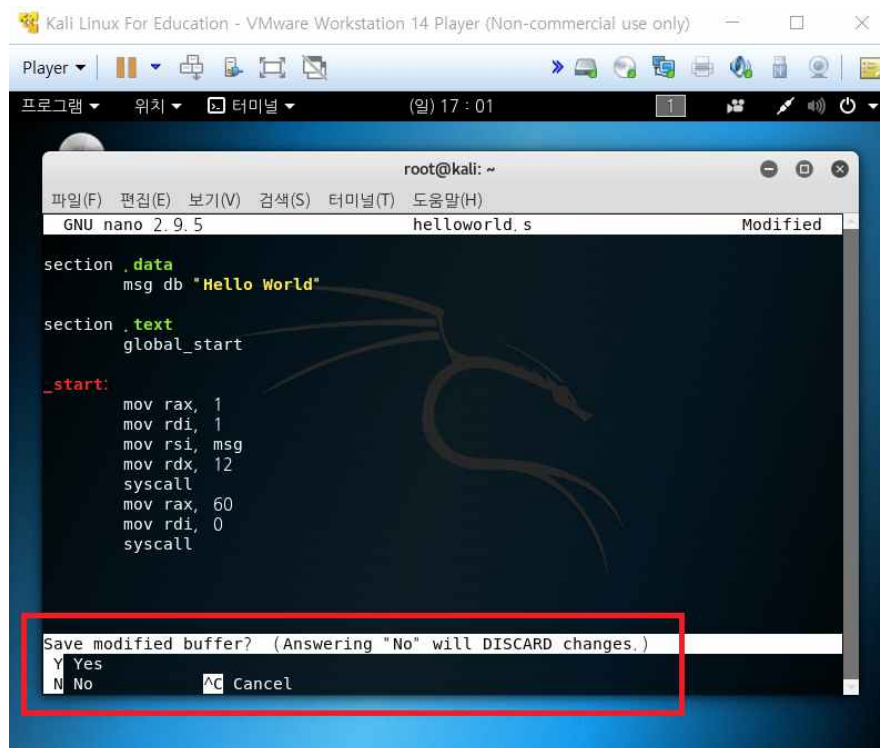
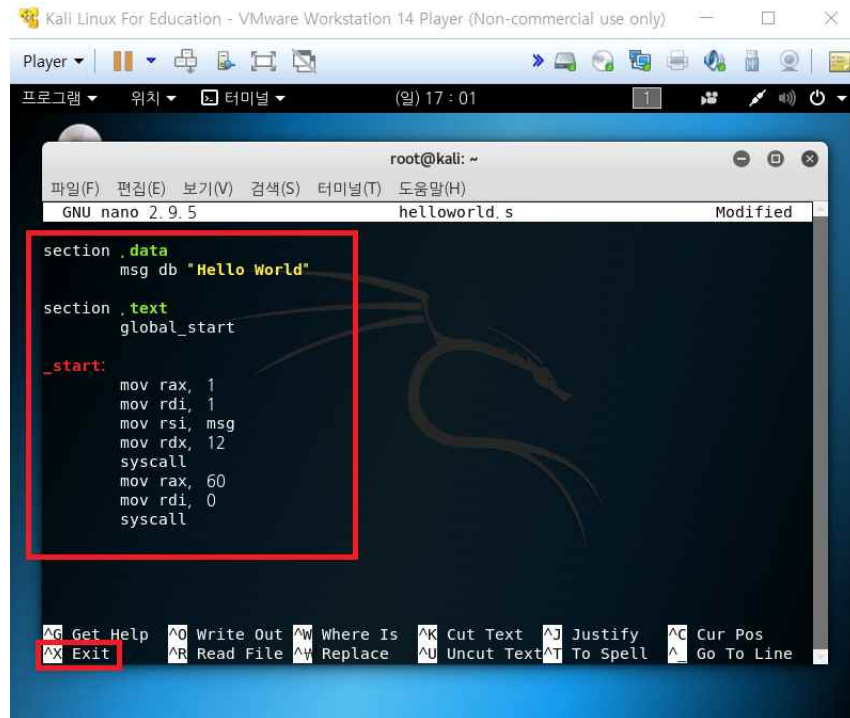
온라인상태를 기대할 수 없는 애플리케이션은 여전히 암호화 기술을 사용한다. 암호화 및 난독화 기술로 리버싱을 방해해서 지연시킨다. 실행 바이너리에 더미 데이터를 집어넣어 분석을 어렵게 만들고, 같은 기능을 하는 여러 함수를 일부러 중복 작성하거나 변수나 함수명을 읽기 힘들게 바꾸는 식으로 분석 난이도를 높이는 방법도 있다.

그러나 인공지능 리버싱 도구도 같이 발전해서 난독화된 코드의 패턴을 분석해 중복 작성된 함수의 중복을 제거하고 변수명을 추정하여 명명해 주고 바이너리 데이터를 이미 소스 코드가 알려진 다른 프로그램과 매칭시켜 손상된(난독화된) 코드를 상당한 수준으로 복원해내고 있기 때문에 들이는 노력에 비해 난이도는 별로 올라가지 않는다. 특히 현대의 프로그램은 오픈 소스 라이브러리에 크게 의존하기 때문에 그만큼 복원률도 높은 편이다.

2. 실습

2.1 Assembly "Hello World"





Kali Linux For Education - VMware Workstation 14 Player (Non-commercial use only)

Player | (일) 17:02

```
root@kali: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
GNU nano 2.9.5 helloworld.s Modified

section .data
msg db "Hello World"

section .text
global _start

_start:
mov rax, 1
mov rdi, 1
mov rsi, msg
mov rdx, 12
syscall
mov rax, 60
mov rdi, 0
syscall

File Name to Write: helloworld.s
^G Get Help      M-D DOS Format   M-A Append      M-B Backup File
^C Cancel        M-M Mac Format   M-P Prepend     ^T To Files
```

Kali Linux For Education - VMware Workstation 14 Player (Non-commercial use only)

Player | (일) 17:02

```
root@kali: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

root@kali:~# nano helloworld.s
root@kali:~# cat helloworld.s
section .data
msg db "Hello World"

section .text
global _start

_start:
mov rax, 1
mov rdi, 1
mov rsi, msg
mov rdx, 12
syscall
mov rax, 60
mov rdi, 0
syscall

root@kali:~#
```


Kali Linux For Education - VMware Workstation 14 Player (Non-commercial use only)

Player | 위치 | 터미널 | (일) 17:02

```
root@kali: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@kali:~# nano helloworld.s
root@kali:~# cat helloworld.s
section .data
    msg db "Hello World"

section .text
    global _start

_start:
    mov rax, 1
    mov rdi, 1
    mov rsi, msg
    mov rdx, 12
    syscall
    mov rax, 60
    mov rdi, 0
    syscall

root@kali:~# nasm -f elf64 -o helloworld.o helloworld.s
helloworld.s:5: warning: label alone on a line without a colon might be in error [-w+orphan-labels]
root@kali:~#
```

Kali Linux For Education - VMware Workstation 14 Player (Non-commercial use only)

Player | 위치 | 터미널 | (일) 17:02

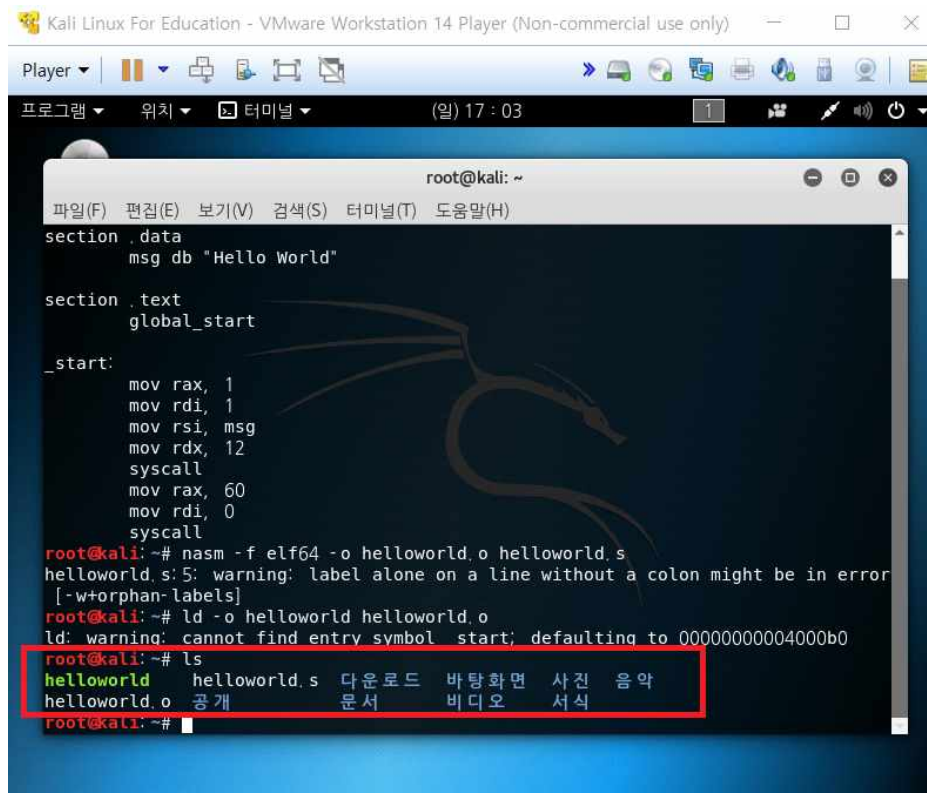
```
root@kali: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@kali:~# nano helloworld.s
root@kali:~# cat helloworld.s
section .data
    msg db "Hello World"

section .text
    global _start

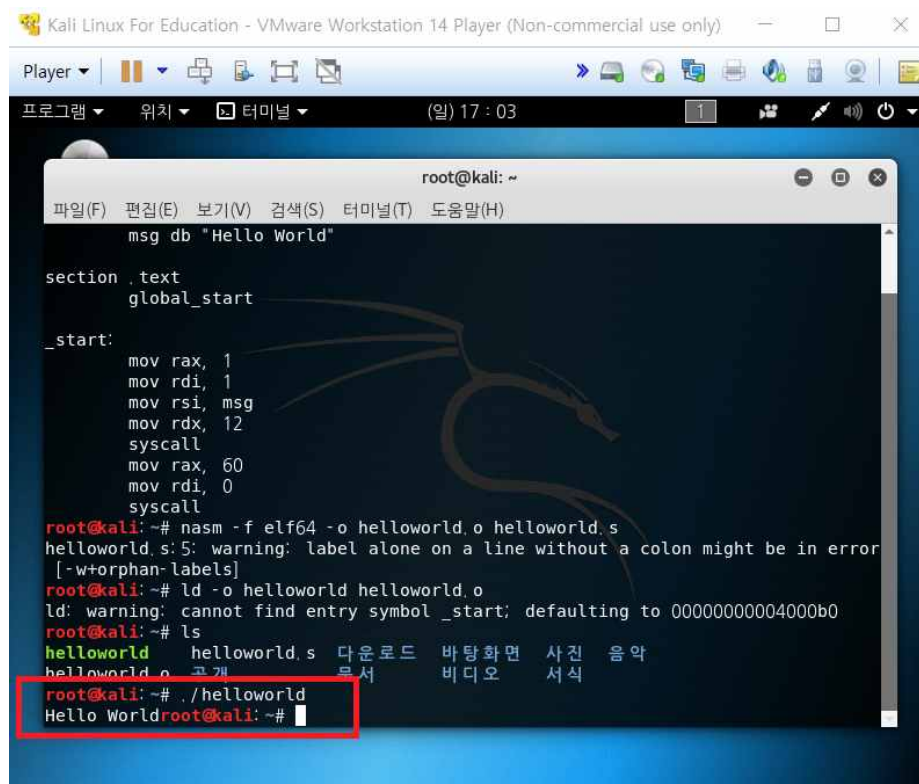
_start:
    mov rax, 1
    mov rdi, 1
    mov rsi, msg
    mov rdx, 12
    syscall
    mov rax, 60
    mov rdi, 0
    syscall

root@kali:~# nasm -f elf64 -o helloworld.o helloworld.s
helloworld.s:5: warning: label alone on a line without a colon might be in error [-w+orphan-labels]
root@kali:~# ld -o helloworld helloworld.o
ld: warning: cannot find entry symbol _start; defaulting to 00000000004000b0
root@kali:~#
```

SECURITY REPORT



```
root@kali: ~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
section .data  
    msg db "Hello World"  
  
section .text  
    global _start  
  
_start:  
    mov rax, 1  
    mov rdi, 1  
    mov rsi, msg  
    mov rdx, 12  
    syscall  
    mov rax, 60  
    mov rdi, 0  
    syscall  
root@kali:~# nasm -f elf64 -o helloworld.o helloworld.s  
helloworld.s:5: warning: label alone on a line without a colon might be in error  
[-w+orphan-labels]  
root@kali:~# ld -o helloworld helloworld.o  
ld: warning: cannot find entry symbol _start; defaulting to 00000000004000b0  
root@kali:~# ls  
helloworld  helloworld.s  다운로드  바탕화면  사진  음악  
helloworld.o  공개  문서  비디오  서식  
root@kali:~#
```



```
root@kali: ~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
msg db "Hello World"  
  
section .text  
    global _start  
  
_start:  
    mov rax, 1  
    mov rdi, 1  
    mov rsi, msg  
    mov rdx, 12  
    syscall  
    mov rax, 60  
    mov rdi, 0  
    syscall  
root@kali:~# nasm -f elf64 -o helloworld.o helloworld.s  
helloworld.s:5: warning: label alone on a line without a colon might be in error  
[-w+orphan-labels]  
root@kali:~# ld -o helloworld helloworld.o  
ld: warning: cannot find entry symbol _start; defaulting to 00000000004000b0  
root@kali:~# ls  
helloworld  helloworld.s  다운로드  바탕화면  사진  음악  
helloworld.o  공개  문서  비디오  서식  
root@kali:~# ./helloworld  
Hello Worldroot@kali:~#
```

3. 참조

- <https://namu.wiki/w/%EB%A6%AC%EB%B2%84%EC%8A%A4%20%EC%97%94%EC%A7%80%EB%8B%88%EC%96%B4%EB%A7%81>