리버스엔지니어링 역분석 구조와 원리

오타 수정 정리 v2012.06.12

3p	
수정 전	**수정 후**
박병익 : pbi12@nate.com, http://simples.co.kr 이강석 : certlab@gmail.com, http://certlab.org	박병익 : pbi12@nate.com, **http://simples.kr** 이강석 : **codeengn@gmail.com, http://codeengn.com**

5p 저자약력	
수정 전	**수정 후**
박병익 저자 약력 전체 수정 독자 A/S 사이트 운영중 : http://simples.co.kr 이강석(certlab@gmail.com) 저자 약력 전체 수정 독자 A/S 사이트 운영중 : http://certlab.org	박병익 **(주)에이쓰리시큐리티를 거쳐 현재 (주)엔씨소프트 전산감사팀에서 근무하고 있다. HSD(Hacker'S Dream)그룹에서 활동 중이며, 심플스 커뮤니티(http://simples.kr)를 운영하고 있다. 저서로는 '리버스엔지니어링(역분석 구조와 원리)'과 '리눅스 웹 서버와 실전 웹해킹(그대로 따라하는)'이 있고, 역서로는 'Fedora Linux Toolbox'가 있다.** 독자 A/S 사이트 운영중 : **http://simples.kr** 이강석(**codeengn@gmail.com**) **코드엔진 리버스엔지니어링 컨퍼런스 운영자이며 2007년부터 운영을 하고 있다. 삼성SDS, 한국인터넷진흥원, 학교 등의 여러 세미나에서 해킹, 보안 강의를 했고 (주)에이쓰리시큐리티를 거쳐 현재 금융결제원 금융ISAC에서 일하고 있다. 2007 Defcon 15th CTF 국제해킹대회에서 Song of Freedom 팀의 멤버로 참가하여 본선 6위에 입상하였다.** 독자 A/S 사이트 운영중 : **http://codeengn.com**

9p	
수정 전	**수정 후**
20번째 줄 M/S 취약점	**MS 취약점**

42p	
수정 전	**수정 후**
8. 레지스터와 플래그 값 부분 레지스트리는 특별한 메모리 공간으로써..	**레지스터는 특별한 메모리 공간으로써..**

65p	
수정 전	**수정 후**
테이블 내에 JLE 부분 3번째 컬럼 ZF=1 and OF!=OF	ZF=1 and **SF!=OF**

92p	
수정 전	**수정 후**
4번째줄 그 이유는 스택(stack)에 값을 순서대로 쌓아놓고, 나중에 쌓인 값을 우선으로 해 빼서 사용하기 때문이다.	**그 이유는 스택(stack)에 값을 순서대로 쌓아놓고, 나중에 쌓인 값을 우선으로 빼서 사용하기 때문이다.**

95p	
수정 전	**수정 후**
95쪽 음영소스 1번째줄 ebs를 ebp로 변경 mov dword ptr [ebs - 8], 1 // i변수	mov dword ptr [**ebp** - 8], 1 // i변수

130p	
수정 전	**수정 후**
11번째줄 섹션의 크기는 0x00001000h에서 0x0000F00h까지인 0xF00h만 할당하면 될 것이다 23번째줄 부분에서 숫자 1이 4곳에서 빠져있음 0x00000fffh 0x000004ffh 0x00000500h ~ 0x00000fffh	섹션의 크기는 **0x00001F00h**에서 0x0000F00h까지인 0xF00h만 할당하면 될 것이다 **0x00001fffh** **0x000014ffh** **0x00001500h ~ 0x00001fffh**

155p	
수정 전	**수정 후**
9번째줄 4.9버전 Freeware 공개로 개인 사용자도 쓸 수 있음(기능 제한이 있음) IDA는 http://www.hex-rays.com/idapro에서 받을 수 있다.	**5.0버전** Freeware 공개로 개인 사용자도 쓸 수 있음(**기능 제한이 없음**) IDA는 http://www.hex-rays.com/products/ida/support/download_freeware.shtml 에서 받을 수 있다.

156p	
수정 전	**수정 후**
2~3번째줄 아래 문장이 4~5번째 줄에도 동일한 내용이 중복되어 있음 IDA는 Hex-rays 사이트에서 받을 수 있으며 IDA Pro v5.2 Evaluation version 과 IDA Pro v4.9버전을 다운받을 수 있다. IDA는 Hex-rays 사이트에서 받을 수 있으며 IDA Pro v5.2 Evaluation version과 IDA Pro v4.9 Freeware 버전을 다운 받을 수 있다.	**문구 삭제** IDA는 Hex-rays 사이트에서 받을 수 있으며 IDA **Pro v6.2 Demo version과** IDA Pro **v5.0 Freeware** 버전을 다운 받을 수 있다.

180p	
수정 전	**수정 후**
8번째줄과 11번째 줄 중복.. 8번째 줄 삭제 Ctrl+F2 : Debugging 종료	해당 줄 삭제

193p	
수정 전	**수정 후**
6번째줄 ebp+var_8에 eax의 값은 0을넣는다.	ebp+var_8**에 eax의 값 0을 넣는다.**

197p	
수정 전	**수정 후**
2번째줄 이 부분은 소스에서 int i=0	이 부분은 소스에서 **int i=5**

250p	
수정 전	**수정 후**
250쪽 끝에서 2번째줄 앞에서 소개한 QUnpack은 업데이트가 거의 되지 않고 있지만,	해당 부분 삭제

319p	
수정 전	**수정 후**
요즘에는 인터넷 용어로 "악성 코드"를 줄여서 "악코"라고 부르기도 한다.	**해당 줄 삭제**