9주차_백하연 컴구정리

1. 자기 증식 프로그램은 가능한가?

목적: 주소 100h에서 Hello World 실행되는 프로그램 → 주소 200h로 전송하여 실행

100h : Hello World in 100
200h : Hello World in 200

과정 : Hello World를 200h로 전송->전송된 내용 수정

2. 무한 자기 증식 프로그램

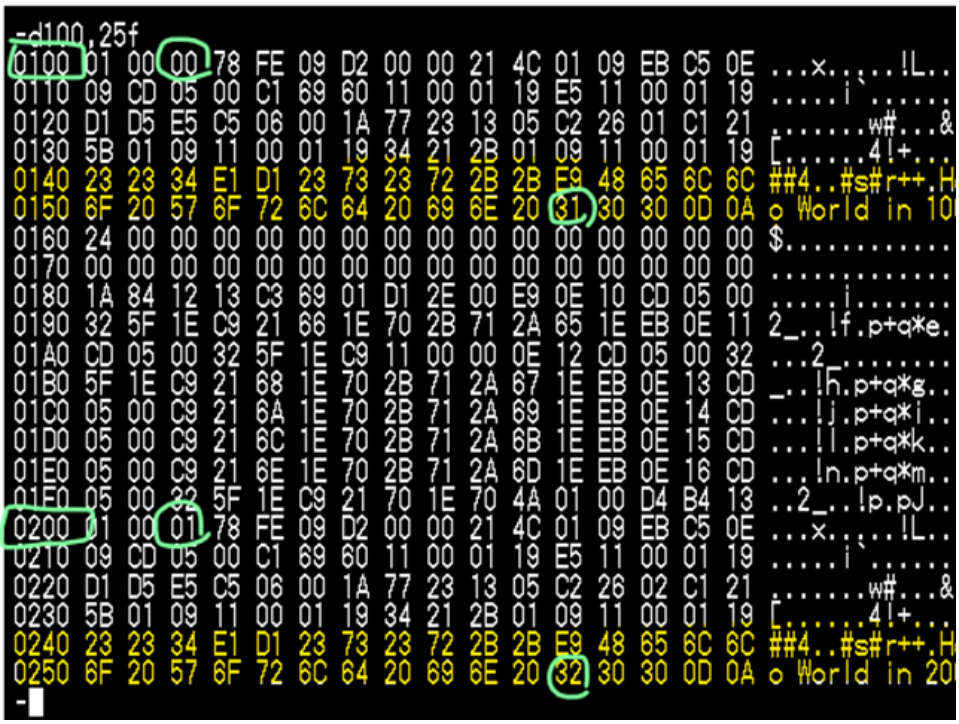
고정 주소로 기록하지 않으면 구현 가능.

→BC 레지스터 페어에 (목적 장소-현 장소) 값 저장 → DAD B
목적 주소의 오프셋 값을 얻기 위해 100h를 더하여 주소를 구함. →BC+100h
복사본 이동 →PCHL

PCHL이 HL레지스터 페어에 있는 처음 주소를 목적 주소로 옮겨 줌.

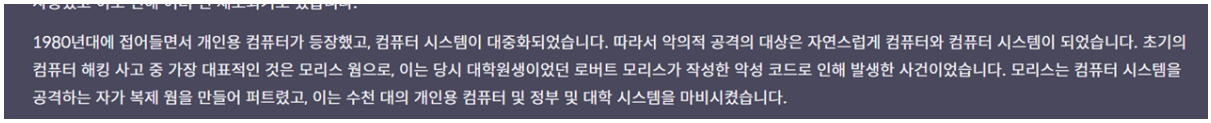
개별 갱신

3번째 바이트에 1을 더하는 것으로 주소 갱신



근데 이건 왜 3번째 말고 노란색 저 부분도 1 더해졌을까

무조건 고정 주소로 기록해야 한다면? 복사->주소 변환



3. 악의를 가진 제삼자가 처리에 끼어들 수 있을까?

특정 키(A)를 누르면 시스템 정지 시키는 프로그램

1. 프로그램 실행
2. 미사용 영역에 프로그램을 전송
3. BIOS의 한 문자 입력을 가로채서 입력된 문자 조사
4. A면 CPU 정지시킴

벡터 탈취라고 함.

쓰는 이유 : 1. 편리한 도구 작성 위해

2. 악성 프로그램 작성 위해

5. CVE-2015-1489
SEPM 12.1, 12.1-RU6-MP1 이전 버전의 관리 콘솔에서 발견된 취약점으로 인증된 사용자가 원격에서 명시되지 않은 벡터를 통해 특권을 탈취할 수 있게 해줍니다.
Copyrighted 2015. UBM-Tech. 117153:0515BC
[국제부 주소형 기자(sochu@boannews.com)]

<저작권자: 보안뉴스(http://www.boannews.com/) 무단전재-재배포금지>

4. 자살 프로그램은 가능한가?

모든 메모리를 삭제해야하고 또, 자기 자신조차도 메모리에서 삭제해야하기 때문에 불가능한가?

모순발생?

1. 삭제 프로그램 실행⇒을 위해 또 프로그램 필요.
2. but 프로그램이 남아 있으면 안됨.

해결 : 마지막에 실행하는 명령어로 메모리 삭제 기능을 지워버리면 새로운 프로그램 필요없음!

5. 프로그램이 서로를 망가뜨리는 게임은 가능한가?

사례 : core war

전략>

1. 폭격기 : 규칙적으로 폭탄 복사, 적 공격

2. 뱀파이어 : 상대방의 프로세스가 구덩이에 뛰어들도록
3. q-scan : 상대를 조기에 잡을 때 사용.