Operating Systems Security (524870)

Assignment #1

(Level up challenge in Free Training Zone)

Seong-je Cho

Fall 2018

Computer Security & Operating Systems Lab, DKU

Free Training Zone (F.T.Z.) 문제 풀이

- 목적
  - Buffer Overflow 관련 실습을 통한 원리 파악
  - Setuid progra을 통한 권한 상승
  - 기타 유용한 명령어 실습

- 첫 번째 과제
  - F.T.Z. 로컬 환경을 구축하여 level up 문제 해결
  - F.T.Z. 20개의 level 중에서 세 개의 level 문제 풀이
    - Level 9, Level 11, Level 12 풀이
  - 개별과제임

F.T.Z. 로컬 환경 구축하기

- 다음 사이트 참고하여 F.T.Z 이미지를 다운로드하여 설치
  - http://noplanlife.com/?p=606
  - https://betteridea-bank.blogspot.com/2017/09/x-1.html

- Red Hat 리눅스
  - ID: root, Password: hackerschool
  - Ifconfig 명령어로 IP 주소 확인

- PuTTY 이용
- 한글이 깨져서 나오면
  - Configuration 메뉴에서 [Window]-[Translation]-[Remote character set]을 “UTF-8” 에서 “Use font encoding”을 변경,

  또는

  $ export LANG=EUC-KR

Level 1 of F.T.Z.

- ID/Password: level1/level1
- Home director에 hint 파일이 존재
  - vi 나 cat, more 등의 명령으로 hint 파일 확인

"level2 권한에 setuid가 걸린 파일을 찾는다"

- Solution:

  $ find / -perm -4000 –user level2 2> /dev/null

  파일들이 보임. (my-pass, chmod 파일들은 제외)
  한 파일을 실행하면 됨.

  - "2> /dev/null"은 standard error를 /dev/null로 보내라
  - my-pass 명령은 해당 레벨의 비밀번호를 알려줌.
  - 즉, level2가 가진 setuid 프로그램을 실행하고, my-pass를 실행하여 level2의 password를 획득

F.T.Z. level up challenges

- Level 2: Setuid 프로그램 + command injection on editor
- Level 3: Command injection
- Level 4: Backdoor
- Level 5: race condition
- Level 6: ??? (Ctrl + C)
- Level 7: Simple password cracking
- Level 8: password cracking
- Level 9: Simple BoF
- Level 10: Shared memory (IPC)
- Level 11: BoF with shellcode, NOP, …
- Level 12: BoF
- Level 13: BoF (Detour Stack canary)
- Level 14: BoF
- Level 15: …

첫 번째 과제: F.T.Z. 3개의 문제 풀이

- Level 9 – Simple Buffer overflow
- Level 11 – Buffer overflow using srtcpy() (Shellcode + NOP + …)
- Level 12 – Buffer overflow using gets()

- 개별 과제임
- 과제 보고서는 문제 풀이의 원리에 대한 체계적인 설명을 포함해야
  - Level 9와 level 11, level 12의 차이점을 구체적으로 설명해야 함.
  - 방어 기법도 설명하기 바람.
  - 창의적 풀이 기법 또는 방어 기법에 대해서는 가산점 있음

- 제출기한: 10월 16일(화)
- 표지에는 다음 내용을 포함해야 함
  - 교과목 명, 학번, 이름
  - 과제 제목
  - 제출 일

첫 번째 과제: F.T.Z. 3개의 문제 풀이

- Level 9 및 level 11의 password는 수업시간에 알려 줌

- 제출처 및 문의 사항:
  - 미디어센터 505호 정재민 (s17orlax@gmail.com)
  - 미디어센터 504호 박민재 (souling4you@gmail.com)
  - 10월 16일(화) 수업시간에 제출 가능