BoB Linux의 차별성

BoB 9기 보안제품개발 노무승

BoB Linux에서 정보보안의 어떤 것을 학습할 수 있을까?

1. CTF/워게임 실습 위주 라면
   -> 전체적으로 입문자에게는 윈도우 환경이 더 편할 것.
      (그럼에도 리눅스 환경으로 생각해본다면..)
      리버싱 : 리눅스용 어셈블러가 존재.
      (EDB(Evans Debugger), gdb, ida, radare)
      웹해킹 : OS와 무관으로 접하기 쉬운 편.
      (BurpSuite, 브라우저 내장 개발자 도구, ...)
      포렌식 : 헥스에디터로 GUI로는 ghex2(Gnome), KHexEdit(KDE),
      CUI로는 hexedit, vim 등이 존재.
      자바(.jar) 위주의 분석 도구는 리눅스에서도 돌아감.
      포너블/리버싱(리눅스) : 환경이 리눅스면 오히려 분석하기 편함.
2. 리눅스/ 서버(네트워크 보안) 위주 라면
   -> 직접 서버를 구축하고 방화벽 설정도 학습 가능.
      웹해킹과 연계하여 직접 해킹 실습 환경을 구축해보는 것도 가능.
3. 리눅스/ 포너블(시스템 해킹) 위주 라면
   -> 해커스쿨 FTZ라는 이미지가 이미 존재.
      해커스쿨 FTZ와도 차별성이 필요함.

BoB Linux의 차별성

분야별 기초 트레이닝 기능 (모든 분야는 기초 정도만 진행)
(기반 지식이 없어 문제를 풀 수 없는 경우, 힌트를 볼 수 있는 기능 제공)

-> 리눅스 학습
   쉘 스크립트나 프로그래밍 언어로 학습 환경 구축 가능
   자주 사용하는 명령어를 선별하여 학습 환경 구축
   (알아두면 편한 기능인 find, grep 등도 포함하면 좋을 것)

-> 리버싱(리눅스) 학습
   분석용 ELF 샘플과 어셈블러 제공 / 매뉴얼 제작
   분석용 ELF 샘플은 직접 C언어 등을 활용해 제작.
   (단순 비교 문부터 아스키코드 활용, xor 연산 활용 등의 문제)

-> 포렌식 학습
   분석용 파일과 포렌식 도구 (헥스에디터) 제공 / 매뉴얼 제작
   기초적인 이미지 포렌식부터, 파일 시스템 포렌식 샘플까지 제작.
      이미지 포렌식
         JPEG EOI 끝에 Flag 이미지 SOI 진행
         PNG 헤더 손상 / 청크 손상
         EXIF 값을 통한 위치 유추
         특정 픽셀의 색상, 채도, 명도에 flag 숨겨둠

채도, 명도를 조절하면 flag가 나타남
BMP 파일 구조의 크기 영역을 조절
gif에서 flag가 적힌 이미지 추출
파일 시스템 포렌식
파일시스템 별 파일 복구
운영체제 별 아티팩트 분석
…

-> 웹해킹 학습
OWASP TOP 10 중에서 기초적인 부분만 뽑아서 진행.
파일 업로드 취약점 (웹쉘)
디렉터리 리스팅 취약점
쿠키 / 파라미터 값 / 개체 속성 변조
JS 우회
PHP 트릭 (기초)
SQL 인젝션 (기초)
…
구축된 로컬 웹서버를 활용해 공격을 막는 방법까지도 실습.

-> 포너블(시스템 해킹) 학습
해커스쿨 FTZ를 직접 해보고 비슷하게 환경을 구축해줌.
(문제는 참고만 하되, 배끼지는 않을 것)

-> 802.11 무선 보안 학습
WEP 패스워크 크래킹 매뉴얼 제공.
패스워드 브루트포싱 매뉴얼 제공.
(단순 브루트포싱, 딕셔너리 어택 등)
모니터 모드 지원 랜카드 선별 매뉴얼 제공.
DeAuth 공격 매뉴얼 제공.
매뉴얼 제공시 대비방안도 함께 제시.

-> 서버 보안
ssh, ftp, telnet 등 다양한 원격 접속 서버 구축 매뉴얼 제공
아파치, Nginx 등 웹 서버 구축과 방화벽 설정 매뉴얼 제공
기본적인 보안 수칙 가이드라인 (데이터 3법 등)

-> 정보보안 로드 맵 (부록)
정보보안 직종에 대한 로드맵 첨부
(이강석님 자료, KISA 정보보호 진로 가이드 북 안내)
국가 지원 인재 사업 소개 : SW마에스트로, BOB, 케쉘주
정보보안 관련 대학 학과 소개
(KUCIS, 암호학 동아리 선정된 대학 중점으로 소개)

-> 각종 워게임 리스트 제공 (부록)
난이도별, 유형별 워게임 리스트를 정리하여 제공

-> 국내 보안인 블로그 리스트 (부록)

https://docs.google.com/spreadsheets/d/1syGhYGWHNnV2jgnGALLorzE__NdGxl44Arh_qOkpnJw/edit#gid=0