1. 기본 해킹 기술들
   1. 프로그래밍
      1. 근본적인 해킹 기술 -> 컴퓨터 언어 모르면 해킹 불가
   2. 유닉스 공부
   3. 웹, html 공부
2. 도입
   1. 기본 용어
      1. 해킹 – 컴퓨터에 대해 전문성을 발휘하는 행위
      2. 크래킹 – 소프트웨어 또는 시스템의 보안을 뚫는 것(breach – 위반)
      3. Phreaking – 통신망, 네트워크를 크래킹 하는 것
      4. Spoofing – 원래 IP 위조하는 것
      5. DoS – 인가된 사용자가 서비스를 이용하지 못하도록 하는 것
      6. 포트 스캔 – 취약점을 찾는 것
   2. 정찰(Reconnaissance)
      1. Passive Scanning
      2. Active Scanning
3. 일반적인 해킹 방법
   1. 아래의 순서대로
      1. 대상 시스템 식별
      2. 대상 시스템 정보 수집
      3. 취약점(loophole) 찾기
      4. 익스프로잇 코드(exploit code)이용
      5. 로그 파일 변조 -> 추적 없이 탈출
4. 포트 스캔 : 도입
   1. 무언가와 연결(통신)을 위해 열려있는 포트와 해당 포트에서 실행되는 서비스 목록을 얻기 위해 대상 시스템을 검색하는 것
   2. 일반적으로 해커가 가장 먼저 수행(undertake)
   3. 대상 시스템에서 실행중인 열린 포트, 서비스, 운영체제 등의 정보 얻는데 사용
   4. telnet프로그램을 사용하여 할 수 있다.
5. 포트 스캔 : 보안 위협
   1. 가져오는 정보들
      1. 오픈 포트 목록
      2. 실행중인 서비스들
      3. 모든 서비스, 데몬(사용자가 직접적으로 제어하지 않고, 백그라운드에서 돌면서 여러 작업을 하는 프로그램)의 정확한 이름 버전
      4. 운영체제 정보
   2. 위의 정보들 -> 해커가 침투하려 할 때 귀중한 정보들임.
6. 포트 스캔 : 핑 스캔
   1. 공격 대상 컴퓨터에게 ICMP 에코 요청
   2. 대상 컴퓨터 -> 별다른 이유(ICMP프로토콜 필터링 등)가 없는 한 ICMP 에코 응답
7. 포트 스캔 : TCP 연결 스캔
   1. 대상 시스템 과 연결하여 3-WAY-HANDSHAKE를 수행
   2. 정확하고 가장 빠른 포트 스캔 방법
   3. 탐지, 대책
      1. 동일한 원격 IP주소에서 많은 포트에 연결 -> 연결 초기화(Initialization) 및 종료(Termination)
      2. 모니터링
8. 포트 스캔 : SYN 스캔
   1. 핸드쉐이크를 모두 수행 하지X
   2. SYN 패킷을 보내고 열린 포트 알게되면 종료
   3. Half Open Scanning이라고도 함
9. 포트 스캔 : FIN스캔
   1. 대상에 FIN패킷 전송
   2. 해당 포트 수신X (열려 있지 X) -> 응답 X
   3. 수신 중 (열려있다면) -> 오류 응답 수신
10. SQL 인젝션
    1. 가장 흔한 공격 중 하나
    2. SQL 지식이 있어야 함
    3. 다재다능하다. 많은 것들을 할 수 있다
    4. 많은 웹 애플리케이션 form으로 유저들의 입력을 받음
    5. 이 유저들의 입력 -> SQL 데이터 베이스에 문자 그대로(LITERALLY) 사용됨
11. SQL
    1. 데이터 베이스 -> 각가 이름을 가진 테이블이 하나 이상 존재
    2. 테이블 -> 데이터 포함된 레코드(행)(RECORD(ROW))가 존재
    3. SQL ->ELECT, UPDATE, DELETE, INSERT, WHERE등의 명령어 사용
    4. 밑의 예 -> 테이블 이름 – USER, 행과 열에 분산된 데이포를 가짐
       1. Ex) SELECT \* FROM tblUsers WHERE USERNAME = ‘admin’
    5. 웹사이트 PHP와 같은 일부 프로그래밍 언어로 작성
    6. -> 프로그래머 SQL구문들 문자열로 코드안에 삽입
    7. 사용자 이름을 txtUsername이라는 텍스트 필드에, 암호를 txtPassword라는 텍스트 필드에 입력한다고 가정해보자
       1. SQL문을 문자열에 넣을 것인데 밑의 예처럼 보일것이다.
       2. Ex) “SELECT \* FROM tblUSERS WHERE UserName = ' “ + txtUsername.Text + ” ' ” + “ AND Password = ' ” + txtPassword.Text + ” ' ”;
       3. 위의 내용을 내포함
12. SQL Script Injection
    1. 사용자 이름, 암호 입력창에 다음을 추가
       1. ' or ‘1' =‘1
       2. OR
       3. ' or 'a' ='a
       4. Also try password’ or (1=1)
       5. Or people try
       6. anything' OR 'x'='x
       7. or people try
       8. password:’1=1- -
       9. ‘ -> 자동하지 않으면 “ 로 사용
    2. 이런 식으로 SQL INJECTION 공격을 함
    3. 비밀번호 쪽을 보면 Password = ‘ ‘ or ‘1’ = ‘1’이다 -> Password = ‘ ‘은 참이 아니나 ‘1’ = ‘1’은 참이고 앞에 OR이 있으므로 위의 표현 참인 명제가 되어 로그인 될 것
13. Cross Site Scripting (이것에 관해 조금 더 공부해보기)
    1. 공격 대상 도메인의 보안 컨텍스트(애플리케이션의 보안을 담당하는 부분)에서 공격자가 준비한 JAVASCRIPT의 일부를 실행
    2. 공격자 -> 웹페이지에(사용자와 상호작용하는 부분에) 스크립트 주입
    3. 스크립트를 주입한 부분으로 이동할 때 정상적인 기능이 실행되지 X -> 스크립트 실행