9장. 침입자

9.1 침입자

개요

- 침입자 분류
  - 신분위장자(Masquerader):
  - 불법 행위자(Misfeasor):
  - 은밀한 사용자(Clandestine user):

양성 침입과 심각한 침입

- 양성(benign) 침입
  - 손상을 초래하지는 않는 장난 수준
  - 많은 사람이 단순히 무엇이 있는지 보기 위해 인터넷을 탐색하는 행위
- 심각한(serious) 침입
  - 권한이 부여된 데이터를 권한 없이 읽으려고 시도하는 행위
  - 데이터를 불법적으로 수정하거나 혹은 시스템을 방해하는 행위

침입 목록 (1)

- 원격 루트로 이메일 서버 침해 시도
- 웹 서버 화면 변경
- 패스워드 추측 및 크래킹
- 신용카드 번호 데이터베이스 복사
- 허가 없이 민감 정보 열람하기
- 워크스테이션에서 패킷 스니퍼 구동하기

침입 목록 (2)

- 익명 FTP 서버의 허가 오류 이용하기
- 다이얼링 모뎀을 통한 미 보안 네트워크 접속하기
- 최고 관리자의 이메일 패스워드 리셋 및 새 패스워드 알아내기
- 잠시 자리를 비운 사이 로그인 상태의 워크스테이션 허가 없이 이용하기

침입자 행동 패턴 (1)

- 침입자 행동 패턴의 예
  - 해커
  - 범죄형 기업
  - 내부 위협

침입자 행동 패턴 (2)

- 해커

1. NSLookup, Dig 같은 IP 들여다보기 도구를 이용해서 목표물을 선택한다.
2. NMAP 같은 도구를 이용하여 접근 가능한 서비스 네트워크 지도를 만든다.
3. 약점을 가질 만한 서비스를 식별해낸다(이 경우, pcAnywhere).
4. pcAnywhere 패스워드를 전수공격하거나 추측한다.
5. DameWare라고 하는 원격 관리 도구를 설치한다.
6. 관리자가 로그온할 때까지 기다린 다음 그의 패스워드를 가로챈다.
7. 패스워드를 이용하여 나머지 네트워크에 접속한다.

침입자 행동 패턴 (3)

- 범죄형 기업

1. 신속하고 정확하게 행동해서 자신의 행동을 감지하기 어렵게 만든다.
2. 취약 포트를 통해 주변 환경을 이용한다.
3. 트로이목마(은닉 소프트웨어)를 이용해서 나중에 출입을 위해 백도어를 남겨둔다.
4. 스니퍼를 이용해서 패스워드를 가로챈다.
5. 감지될 때까지 남아 있지 말라.
6. 실수를 전혀 하지 않거나 하게 되더라도 조그만 실수여야 한다.

침입자 행동 패턴 (4)

- 내부 위협

1. 자신이나 친구에게 네트워크 계정을 개설해준다.
2. 일상의 업무시에는 잘 사용하지 않는 계정이나 응용프로그램에 접근한다.
3. 퇴직한 직원이나 새로 임용될 직원에게 이메일을 보낸다.
4. 은밀한 인스턴트-메시징 채팅을 한다.
5. f' dcompany.com 같은 불평분자 직원에게 제공되는 웹사이트를 방문한다.
6. 대규모 다운로드나 파일복사를 한다.
7. 일과시간 외에 네트워크에 접속한다.

침입자 행동 패턴 (5)

- 해커의 동기
  - 스릴
  - 자신의 위치 (실력주의)
    - 목표를 찾아 공격하고 그 정보를 공개
    - 예: 대형금융기관 침입
      - 시만텍의 pcAnywhere 응용프로그램(원격통제) 이용
- 해커 위협을 막기 위한 수단
  - 침입탐지시스템(IDS: intrusion detection system)
  - 침입예방시스템(IPS: intrusion prevention system)
  - 컴퓨터비상대응팀(CERT: Computer Emergency Response Team)

침입자 행동 패턴 (6)

- CERT (Computer Emergency Response Team)
  - 목적
    - 시스템 취약점에 대한 정보 수집
    - 시스템 관리자에게 배포
  - 신속한 패치설치의 필요성
    - 해커도 CERT 보고서 참조
  - 자동화된 패치 업데이트 필요
    - 패치 발표 시기 불분명
    - 시스템의 복잡성
  - 여러 계층의 방어막 필요
    - IT 시스템에 대한 보안 위협에 대응

침입자 행동 패턴 (7)

- 범죄자
  - 해커 범죄조직
    - 기업, 정부 또는 느슨하게 조직된 해커 집합체
    - DarkMarket.org나 theftservices.com 같은 음성적인 포럼을 통해서 접촉
    - 데이터나 유용한 정보를 교환하고 공격에 협력
  - 목표
    - 전자상거래 서버에 있는 신용카드 파일
    - 공격자는 루트 권한의 획득
  - 수사 방해
    - 카드 번호를 이용하여 고가 상품을 구매하고 카드 번호를 거래하는 사이트서 공유
    - 사용 흔적을 애매모호하게 만들어서 수사하기 어렵게 함

침입자 행동 패턴 (8)

- 범죄자에 대한 방어 수단
  - 침입탐지시스템(IDS: intrusion detection system)
  - 침입예방시스템(IPS: intrusion prevention system)
  - 고객정보 데이터베이스 암호화 필요
  - 신용카드 정보 암호화 절대 필요
  - 전자상거래 사이트
    - 전자상거래 조직은 반드시 지정된 서버 사용
    - 제공자의 보안 서비스에 대한 면밀한 모니터링 필요

침입자 행동 패턴 (9)

- 내부 공격자
  - 가장 감지하기 어렵고 방어하기 어려운 존재
    - 접근권한을 가지고 있고, 시스템의 구조와 내용도 알고 있음
  - 동기
    - 복수심
    - 그럴만한 자격이 있다는 감정
  - 사례
    - 정보통신관계자 해고시 기능 마비
    - 회사의 데이터 복사하여 경쟁사로 이직

침입자 행동 패턴 (10)

- 내부공격자 방어방법
  - 침입탐지시스템(IDS: intrusion detection system)
  - 침입예방시스템(IPS: intrusion prevention system)
  - 권한 최소화
    - 업무를 수행에 필요한 자원에만 접속
  - 로그 세팅으로 접근기록 보관
  - 민감한 자료 접근은 인증을 통해 제공
  - 자료 이용 종료 즉시 접근차단
  - 종료 즉시 재 접근 이전에 하드드라이브 미러 이미지 작성
    - 정보가 경쟁사로 넘어갔을 경우 이를 증거로 사용.

침입 기법 (1)

- 침입자의 목적
  - 시스템 접근 허락
  - 시스템에 대한 접근허용 범위 확대
- 목적 달성 방법
  - 보호된 정보 획득
  - 패스워드 파일 획득
- 제일 중요한 것은 패스워드 파일 보호
  - 일방향 암호화(One-way encryption):
  - 접근 제어(Access control):

침입 기법 (2)

- 일방향 암호화 (One-way encryption):
  - 일반적 패스워드 사용법
    - 사용자 패스워드 암호화된 형태로 저장
    - 접근 허락 받기
      - 사용자: 패스워드 입력
      - 시스템: 패스워드 암호화 후 저장된 값과 비교
  - 실제의 경우
    - 시스템: 일방향 변환 후 패스워드로 암호화 함수에 사용할 키 생성
- 접근 제어(Access control):
  - 한 사람이나 극소수의 사람에게만 패스워드 파일에 대한 접근을 허용

침입 기법 (3)

- 패스워드 알아내기 기술
  - (추측)

1. 시스템 설치 시 사용했던 표준 계정의 기본 패스워드를 시도(예: admin, abc 등)
2. 짧은 패스워드 모두 시도(한 문자에서 세 개의 문자로 구성되는 패스워드)
3. 시스템 온라인 사전에 있는 단어나 흔히 사용할 것 같은 패스워드 시도

침입 기법 (4)

- 패스워드 알아내기 기술 (계속)
  - (추측)
  4. 사용자와 관련된 정보 수집
     - 사용자의 full name, 배우자나 아이들의 이름, 사무실의 사진, 취미와 관련된 사무실 안의 책 같은
  5. 사용자의 전화번호, 사회보장번호(Social Security number), 방 번호
  6. 거주지의 합법적 자동차 번호판 번호 시도

침입 기법 (5)

- 패스워드 알아내기 기술
  - (접근제어 회피와 물리보안공격)
  7. 접근제한 우회에 트로이 목마 이용
  8. 원격 사용자와 호스트 시스템 사이의 연결선 도청