정보보호론	국가 전산 7급	2020년 9월 26일

♠ 필기합격인원/합격선(46명/76.66점) - 선발예정인원 33명 ♠

1. 패스워드 공격에 해당하지 않는 것은? [2020년 국가 7급]

① 사전 대입 공격
② 이블 트윈 공격
③ 무작위 대입 공격
④ 레인보우 테이블을 이용한 공격

♤ **패스워드 공격에 해당하지 않는 것**

◈ **전수조사 공격(brute-force attack, 무차별 공격)**
- 암호문이 이해할 수 있는 평문으로 전환될 때까지 가능한 모든 **비밀번호**를 대입한다.
- 조합 가능한 모든 경우의 수를 처음부터 끝까지 대입하는 방식이다.
- 전수조사 공격은 단순하지만 컴퓨터 성능이 향상되면서 무시할 수 없는 기법이다.
- 전수조사 공격에 안전하기 위해서는 조합 가능한 키의 수가 매우 커야 한다.

◈ **Evil Twin(이블 트윈) - 악의적 쌍둥이**
- 이블 트윈은 합법적인 네트워크처럼 가장한 무선 네트워크를 가리킨다.
- 이블 트윈은 로그온한 사람들을 **속이고,** 비밀번호나 신용카드번호를 훔치기 위한 공격이다.
- 이블 트윈은 **피싱 사기의 무선 버전**이다.
- 공격자는 합법적인 제공자로 가장하여, 노트북이나 휴대폰으로 AP에 연결한 사용자들을 공격한다.

◈ **사전 공격(dictionary attack)**
- 통상적으로 자주 사용하는 **비밀번호**를 사전식으로 모아서 직접 대입하는 방식이다.
- 1111, 1234, 4321, 9999, east, love 등으로 구성된 비밀번호 목록을 이용한다.
- 비밀번호 구성은 "문자, 숫자, 특수기호"를 조합하여야 높은 강도를 가지게 된다.
- "p#5w8*$s97"은 강도가 높은 비밀번호이다.

◈ **레인보우 테이블을 이용한 공격**
- 레인보우 테이블은 해시함수를 사용하여 생성된 값들을 대량으로 저장한 표이다.
  → 해시함수 MD5, SHA-1, SHA-2 등을 이용
  → 레인보우 테이블 크기는 작은 것도 기본적으로 100GB이상이 된다.(보통 TB 단위)
- 레인보우 테이블을 이용한 공격도 일종의 **사전 공격**이다.
  → 미리 만들어진 테이블에서 해시값을 뽑아서 대입하므로
  → Rainbow Table을 이용하면 해시값 계산 시간이 절약되어 신속한 공격 가능
  → Rainbow Table을 이용하면 12자리 숫자로 된 **비밀번호**를 순식간에 뚫을 수 있다.
- 레인보우 테이블은 R(reduction) 함수를 이용하여 충분히 작은 크기로 줄일 수 있다.
- 레인보우 테이블은 크기를 줄여도 기본적으로 수십 GB이상이 된다.
- R 함수는 비밀번호로 사용되는 문자열을 해시값으로 만드는 함수이다.

정답 : ②

2. 역할기반 접근제어(RBAC)에 대한 설명으로 옳은 것은? [2020년 국가 7급]

① 정보의 소유자가 특정 사용자와 그룹에 특정 권한을 부여한다.
② 사용자에게 부여된 권한에 따라 사용자를 역할로 분류하여 각 사용자에게 하나의 역할만 할당되도록 한다.
③ 역할 및 역할이 수행할 권한을 정의하고, 사용자를 역할에 할당하는 방식이다.
④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.

♤ **역할기반 접근제어(RBAC)**

① **정보의 소유자**가 특정 사용자와 그룹에 특정 권한을 부여한다.**(×)**
→ **관리자**가 그룹에 권한을 부여하고, 사용자를 그룹별로 분류한다.
② 사용자에게 부여된 권한에 따라 사용자를 역할로 분류하여 각 사용자에게 **하나의 역할**만 할당되도록 한다.**(×)**
→ 각 사용자의 접근권한은 사용자가 속한 그룹에 할당된 역할에 기초한다.
④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.**(×)** → 정부, 군 같은 복잡한 조직에는 **강제적** 접근통제(MAC)를 적용한다.

◈ **접근통제 정책 정리**

정책	모델	특징
DAC	• 접근제어행렬 • 접근가능목록 • 접근제어목록	• 주체가 객체에 대한 접근권한을 자율적으로 다른 주체에게 부여하거나 철회 가능 ↓ ↓ 보안 취약점 ↓ • 악의적인 목적에 이용 가능(트로이 목마)
MAC	• BLP 모델 : 기밀성 • Biba 모델 : 무결성	• 관리자에 의한 보안 등급 결정 ↓ ↓ 엄격한 보안 제한 ↓ • 다중사용자 보안요구사항 표현에 부적절 • 일반적인 분야 적용은 부적절
RBAC	• T-RBAC (Task-RBAC)	• 객체에 대한 접근권한은 사용자 역할(업무)에 기반 ↓ ↓ 상업적 측면이 강화된 정책 ↓ • 직원 500명이상의 기업에 사용

정답 : ③

3. 정보시스템의 침입자를 속이는 기법의 하나로, 가상의 정보시스템을 만들어 놓고 실제로 공격을 당하는 것처럼 보이게 하여 해커나 스팸, 바이러스를 유인하여 침입자들의 정보를 수집하고 추적하는 역할을 수행하는 것은? [2020년 국가 7급]

① Honeypot ② IPS
③ ESM ④ DRM

♤ **허니팟(honeypot)**

- 허니팟은 비정상적인 접근 탐지를 위해 **의도적으로 설치해 둔 시스템**이다.
- 허니팟은 실제 서비스는 지원되지 않지만, 서비스들이 사용 가능한 것처럼 꾸며 놓는다.
- 허니팟은 **침입자를 속이는 침입탐지기법**이다.
- 허니팟은 침입자를 유인하는 함정을 꿀단지에 비유하여 붙인 이름이다.**(유인 정책)**
- 허니팟은 실제로 공격을 당하는 것처럼 보이게 하여 공격자를 추적하고 정보를 수집한다.
- 허니팟은 침입자를 가능한 오래 머물게 하여 추적이 가능하므로 능동적 방어가 가능하다.
- 허니팟은 공격자의 정보를 얻기 위한 하나의 개별 시스템을 뜻한다.
- 허니팟은 공격자에게 쉽게 노출되어야 한다.
- 허니팟은 시스템의 **모든 구성요소**를 갖추고 있어야 한다.
- 허니팟은 시스템을 통과하는 모든 패킷을 감시해야 한다.

정답 : ①

4. 공개키 기반구조(PKI)에 대한 설명으로 옳지 않은 것은? [2020년 국가 7급]

① PKI는 인증기관, 등록기관, 저장소, 사용자 등으로 구성된다.
② 인증서의 폐지 여부를 확인하기 위해 인증기관은 인증서 폐지목록(CRL)을 주기적으로 관리한다.
③ 유효기간 내의 인증서를 가지고 있다면, 사용자는 별도로 CRL을 조사할 필요가 없다.
④ 한 인증기관이 다른 인증기관의 공개키를 검증하는 것이 가능하므로, 사용자는 모든 인증기관의 공개키를 사전에 가지고 있을 필요가 없다.

♤ **공개키 기반구조(PKI)**

- 유효기간 내의 인증서를 가지고 있다면, 사용자는 별도로 CRL을 조사할 필요가 없다.(×)
  → 유효기간 내의 인증서도 유효하지 않은 것이 존재하므로 **CRL을 조사할 필요가 있다.**

정답 : ③

4 http://cafe.daum.net/pass365(홍재연)

5. HTTP 응답 메시지 상태코드의 의미가 옳지 않은 것은? [2020년 국가 7급]

① 201 - Created
② 301 - Moved Permanently
③ 401 - Unauthorized
④ 501 - Bad Request

♤ HTTP 응답코드

• HTTP는 클라이언트와 서버 사이에 **요청/응답**(request/response) 원리이다.**(80 포트 사용)**

◈ HTTP 응답코드 (일부 내용)

코드	메시지	설명
100	Continue	계속, 나머지 요청 정보를 계속 보내주길 바람
101	Switching Protocol	프로토콜 전환, 요청자가 서버에 프로토콜 전환을 요청했다.
200	OK	성공, 오류 없이 전송 성공(서버가 클라이언트에게)
201	Created	작성됨, 성공적으로 요청되었으며 서버가 새 리소스를 작성했다.
202	Accepted	허용됨, 서버가 클라이언트의 요청을 수락 - 접수
300	Multiple Choices	복수 선택, 서버가 요청에 따라 여러 조치를 선택할 수 있다.
301	Moved Permanently	영구 이동, 요청한 페이지를 새 위치로 영구적으로 이동했다.
400	Bad Request	잘못된 요청. 문법 오류로 서버가 이해 못함
401	Unauthorized	권한 없음, 인증되지 않았음 - 접속실패
402	Payment Required	결재 필요, 요금 지불 요청
404	Not Found	찾을 수 없음, 요청한 문서를 찾을 수 없음(오류 메시지)
500	Internal Server Error	서버 내부 오류, 서버에 오류가 발생하여 요청을 수행할 수 없다.
501	Not Implemented	구현 불가, 서버에 요청을 수행할 수 있는 기능이 없다.
502	Bad gateway	불량 게이트웨이, 게이트웨이 상태 나쁨

// HTTP 응답코드는 5개의 클래스(분류)로 구분된다. 첫 번째 숫자는 응답 클래스를 정의한다.
1xx (정보) : 요청을 받았으며, 프로세스를 계속한다.
2xx (성공) : 요청을 성공적으로 받았으며, 인식했고 수용하였다
3xx (리다이렉션) : 요청 완료를 위해 추가 작업 조치가 필요하다
4xx (클라이언트 오류) : 요청의 문법이 잘못되었거나 요청을 처리할 수 없다
5xx (서버 오류) : 서버가 명백히 유효한 요청에 대해 충족을 실패했다

정답 : ④