안기사

정보보안기사] 2023년 22회 보보안기사 실기 기출문제 복원

gPrimrose 2023. 7. 14. 01:30

정보보안기사 22회 실기 복원

1. 라우팅 프로토콜에 대한 설명이다. ( )에 들어갈 프로토콜명을 기술하시오.

(A) : 거리 벡터 알고리즘을 사용하며, 가장 오래되고 널리 사용되는 내부 라우팅 프로토콜
(B) : 링크 상태 알고리즘을 사용하며, 링크 상태 변화시에만 라우팅 정보를 교환하는 내부 라우팅 프로토콜

(C) : 시스코에서 제안하였으며, 거리벡터와 링크 상태 알고리즘의 장점을 수용한 하이브리드 라우팅 프로토콜. 효율성과 수렴 속도가 개선되어 안정적인 라우팅을 지원함

- (A) : RIP, (B) : OSPF, (C) : EIGRP

2. 다음 ( )에 들어갈 유닉스 로그 파일명을 기술하시오.(경로는 생략해도 됨)

(A) : 사용자의 가장 최근 로그인 시각, 접근 호스트 정보 기록
(B) : SU(Swift User) 권한 변경(성공 or 실패) 로그 기록
(C) : 시스템에 로그인한 모든 사용자가 실행한 명령어 정보 기록

- (A) : lastlog, (B) : sulog, (C) : acct / paact

3. 유닉스의 /etc/passwd에 등록된 정보이다. 밑줄 친 값의 의미를 설명하시오.

test01:x:100:**1000:/home/exam:/bin/bash**

- 1) 1000 : GID(그룹 ID)
2) /home/exam : 사용자 홈디렉토리
3) /bin/bash : 로그인 쉘

4. HTTP Request 입력값에 개행문자가 포함되면 HTTP 응답이 2개 이상으로 분리되어, 공격자는 첫 응답을 종료시킨 후 다음 응답에 악의적인 코드를 삽입/실행할 수 있는 HTTP 응답 분할 공격이 가능해진다. 위에서 언급한 개행 문자 2가지를 기술하시오.
- CR(Carriage Return, \r, %0D), LF(Line Feed, \n, %0A)

5. 파일 삽입 취약점은 공격자가 악성 스크립트를 서버에 전달하여 해당 코드가 실행되도록 할 수 있다. PHP를 사용하는 경우 이에 대한 대응책에 대하여 ( )에 들어갈 값을 기술하시오.

1) PHP 소스 코드에 (A) 함수가 존재하는지 확인
2) PHP 설정 파일 (B)에서 allow_url_fopen 값을 (C)로 설정

- (A) : require or include, (B) : PHP.ini, (C) : Off

6. Snort에서는 대량의 패킷에 대응하기 위하여 Threshold 옵션을 type(action 수행 유형), track(소스/목적지 IP), count(횟수), second(시간)으로 설정할 수 있다. 이 중 threshold type 3가지를 기술하시오.

> threshold <(1) | (2) | (3)>, track <by_src | by_dst>, count <c>, seconds <s>

- threshold, limit, both
- (threshold) : 매 s초 동안 c번째 이벤트마다 action을 수행한다.
- (limit) : 매 s초 동안 c번째 이벤트까지 action을 수행한다.
- (both) : 매 s초 동안 c번째 이벤트 시 한번 action을 수행한다.

7. ARP request 요청을 보내는 경우 목적지 주소를 형식에 맞춰서 기술하시오.
- FF:FF:FF:FF:FF:FF

8. DNS 서비스와 관련하여 ( ) 안에 들어갈 용어를 기술하시오.

> 1) DNS 서비스는 53번 포트를 사용하고 전송 계층 프로토콜로 (A) 를 사용한다.
> 2) DNS 서버는 반복적인 질의로 상위 DNS에 가해지는 부하를 줄이기 위해 (B) 를 사용하는데, 해당 정보가 유지되는 기간을 (C) 이라고 한다.

- (A) : UDP / TCP, (B) : Cache(DNS 캐시), (C) : TTL(Time To Live)
- UDP는 전송데이터가 512바이트 이하인 경우, TCP는 전송데이터가 512바이트 초과 또는 Zone Transfer 수행

9. 애플리케이션의 소스 코드를 보지 않고 외부 인터페이스나 구조를 분석하여 취약점을 발견하는 방식을 (A) 라 하고, 개발된 소스 코드를 살펴봄으로써 코딩 상의 취약점을 찾는 방식을 (B) 라고 한다.
- (A) : 블랙박스 테스트, (B) : 화이트박스 테스트
- 실행을 하느냐 하지 않느냐라고 물어본다면, 정적분석과 동적분석임

10. SW 개발과정에서 DBMS 조회를 위한 질의문 생성 시 사용되는 입력값과 조회 결과에 대한 검증방법(필터링 등)을 설계하는 경우 고려해야 할 사항이다. ( )에 들어갈 용어를 기술하시오.

1) 애플리케이션에 DB연결을 통해 데이터를 처리하는 경우 (A)이 설정된 계정을 사용해야 한다.
2) 외부 입력값이 삽입되는 SQL 쿼리문을 (B)으로 생성해서 실행하지 않도록 해야 한다.
3) 외부 입력값을 이용해 동적으로 SQL 쿼리문을 생성해야 하는 경우, (C)에 대한 검증을 수행한 뒤 사용해야 한다.

- (A) : 최소권한, (B) : 동적, (C) : 입력값

11. 개인정보의 안전성 확보조치 기준에 대하여 ( )에 들어갈 용어를 기술하시오.

[제8조(접속기록의 보관 및 점검)] ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 (A)년 이상 보관·관리하여야 한다. 다만, (B) 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 (C)를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

- (A) : 1년, (B) : 5만, (C) : 민감정보

12. 위험관리와 관련하여 ( )에 들어갈 용어를 기술하시오.

(A) : 내외부 위협과 취약점으로 인해 자산에서 발생 가능한 위험을 감소시키기 위한 관리적, 물리적, 기술적 대책
(B) : (A)을 적용한 이후에 잔재하는 위험
(C) : 조직에서 수용 가능한 목표 위험 수준을 의미하며 경영진의 승인을 받아 관리해야 함

- (A) : 정보보호대책, (B) : 잔여 리스크(위험), (C) : DoA(수용 가능한 위험 수준)

13. BYOD 환경에서 모바일 오피스 서비스를 하려고 한다. 관련된 다음의 3가지 보안 기술에 대하여 설명하시오.

1) MDM(Mobile Divice Management)
2) 컨테이너화
3) 모바일 가상화

- 1) MDM : 모바일 기기를 도난, 분실, 악용 등으로부터 보호하기 위하여 강화된 보안 정책(인증, 앱 화이트 리스트, 원격 삭제, 탈옥 탐지, 스크린 캡처 방지, 카메라 제어 등)을 적용하여 관리하기 위한 기술
- 2) 컨테이너화 : 하나의 모바일 기기 내에 업무용과 개인용 영역을 컨테이너라는 별도의 공간으로 분리하여 프라이버시를 보호하는 기술
- 3) 모바일 가상화 : 가상화 기술을 이용하여 하나의 모바일 기기에서 개인용 OS 영역과 업무용 OS 영역을 완전히 분리하는 기술. 평상시에는 개인용 OS 영역에서 모바일 기기를 이용하다가, 필요 시 업무용 OS로 전환하여 사용

14. 다음의 위험 분석 방법에 대하여 개념과 장단점을 설명하시오

1) 기준선 접근법
2) 상세 위험 분석법

1) 기준선 접근법
- (개념) 모든 시스템에 대해 보호의 기본 수준을 정하고 이를 달성하기 위한 일련의 보호대책을 표준화된 체크리스트를 기반으로 선택하는 방식
- (장점) 체크리스트의 각 항목별 준수 여부를 점검하는 방식으로 간단하게 위험분석을 수행할 수 있어, 위험 분석 시간을 절약할 수 있음. 소규모 조직에 적합함
- (단점) 조직의 현황이 반영되지 않은 일률적인 기준으로 통제를 적용하는 경우 과보호 또는 부족한 보호가 될 가능성이 상존함. 체크리스트를 지속적으로 갱신하지 않으면 새로운 취약점과 같은 보안 환경의 변화를 적절하게 반영하기 어려움. 따라서, 자산 변동이 적거나 보안 환경의 변화에 크게 영향을 받지 않는 자산에 한정하여 사용하는 것이 권장됨

2) 상세 위험 분석법
- (개념) 정형화되고 구조화된 프로세스를 기반으로 자산 분석, 위협 분석, 취약성 분석의 각 단계를 수행하여 모든 정보자산에 대한 위험을 상세하게 분석하는 방식
- (장점) 자산가치, 위협, 취약점의 평가에 기반하여 위험을 산정하므로 허용가능 수준까지 위험을 줄이는 근거를 명확히 할 수 있음. 계량적 수치화가 가능하며 평가의 완전성이 높음. 보안 환경의 변화에 따른 새로운 위험에 대한 분석도 용이하게 할 수 있음
- (단점) 위험 분석 방법론을 잘 이해하고 있는 인적 자원이 필요하며, 위험분석에 시간, 노력, 비용이 많이 소요됨

15. 다음의 쿠키 설정값의 의미를 보안 측면에서 설명하시오.

1) Secure
2) HttpOnly
3) Expires

- 1) Secure 통신(SSL/TLS)을 수행하는 경우에만 클라이언트에서 해당 쿠키를 전송함으로써 기밀성을 보장함. 스니핑 공격을 통한 쿠키 정보 탈취에 대응이 가능함
- 2) 웹브라우저에서 자바스크립트(document.cookie) 등을 통한 해당 쿠키 접근을 차단함. 쿠키 탈취를 위한 XSS(Cross Site Scripting) 공격에 대응 가능함
- 3) 쿠키가 만료되는 날짜 및 시간을 설정함. 쿠키가 탈취당하여 재사용되는 리스크를 최소화할 수 있음

16. DNS 증폭 공격에 사용되는 IP 공격 기법을 설명하고, 해당 공격 기법을 사용하는 이유를 설명하시오
1) IP 공격 기법 : 출발지 IP를 공격 대상의 서버 IP로 위조하는 IP스푸핑을 수행 후, DNS 쿼리 타입을 ANY로 지정하여 request를 대량으로 수행하면, 다양한 Type의 레코드들이 Response 되므로 응답이 증폭되어 공격 대상 서버에 부하를 주게 됨
2) 해당 공격 기법 사용 이유
- 출발지 IP가 위조되고, 반사 서버를 통해 공격이 수행되므로 공격의 출처를 파악하기 어렵기 때문임. 특히 UDP는 별도의 인증 절차가 없으므로 공격 수행이 용이함.
- 다수의 좀비 PC를 동원하지 않더라도 대량의 공격 패킷을 공격 대상 서버로 향하도록 만들어 낼 수 있어 효율이 높기 때문임.

17. 다음의 HTTP Request 로그를 보고 물음에 답하시오

[HTTP request]
GET /member/login.php?user_id=1' or '1' = '1'# &user_pw=foo HTTP/1.1
GET /member/login.php?user_id=1' or '1' = '1' &user_pw=foo HTTP/1.1

1) 해당 취약점은 무엇인가?
- SQL Injection

2) 그렇게 판단한 이유는?
- user_id에 특수문자를 포함한 1' or '1'='1'#을 넣어서 로그인 검증을 하기 위한 SQL 문을 참으

로 만들어 인증 로직을 우회하려는 시도를 하고 있기 때문임

3) 대응 방안은?
- 입력값에 특수 문자가 포함되지 않도록 필터링 로직을 구현(이 경우 클라이언트 단이 아닌 서버에 검증 로직을 반드시 넣어야 함. 자바스크립트로 클라이언트 단에서만 검증하는 경우 Paros, Burpsuite와 같은 proxy툴로 검증 로직을 우회할 수 있기 때문임)
- 서버의 DB connection 구문을 Prepared Statement 방식으로 변경(사용자가 입력한 값이 SQL 명령의 일부가 아닌 매개 변수로 처리되기 때문에 해당 컬럼에만 들어가고 SQL문 전체에 영향을 주지 않음)

18. 개인정보의 기술적, 관리적 보호 조치 기준에서 요구하고 있는 보호 조치 5가지를 기술하시오.
1) 접근통제
- 권한 부여, 변경 말소에 대한 내역을 기록하고 최소 5년 보관
- 외부에서 개인정보처리시스템 접속 시 안전한 인증 수단 적용
- 개인정보취급자를 대상으로 비밀번호 작성 규칙 수립 및 적용
- 개인정보취급자 컴퓨터에 대한 물리적 또는 논리적 망 분리
2) 접속기록의 위/변조 방지
- 개인정보취급자가 개인정보처리시스템에 접속한 기록 월 1회 점검, 6개월 이상 접속기록 보존
- 접속 기록 위변조 방지를 위해 정기적인 백업 수행
3) 개인정보의 암호화
- 비밀번호에 대한 일방향 암호화 저장
- 안전한 암호화 알고리즘으로 암호화 저장(주민등록번호 외 고유식별번호, 신용카드번호, 계좌번호, 바이오정보)
4) 악성프로그램 방지
- 백신 소프트웨어 등의 보안 프로그램 설치 및 운영
- 보안 프로그램 자동 업데이트 기능 사용 또는 일 1회 이상 업데이트
5) 물리적 접근 방지
- 개인정보를 보관하고 있는 물리적 장소에 대한 출입통제 절차 수립, 운영
- 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

※ 이전회차 정보보안기사 기출문제

정보보안기사 21회 실기 복원

버튼을 클릭하시면 정보보안기사 21회 실기 복원으로 이동합니다.

정보보안기사 20회 실기 복원

버튼을 클릭하시면 정보보안기사 20회 실기 복원으로 이동합니다.

정보보안기사 19회 실기 복원

버튼을 클릭하시면 정보보안기사 19회 실기 복원으로 이동합니다.

'정보보안기사' 카테고리의 다른 글

[정보보안기사] 2023년 23회 정보보안기사 실기 기출문제 복원 (0) 2023.11.10
[정보보안기사] 2023년 2회차(23회) 정보보안기사 실기 불합격 후기 (4) 2023.07.30
[정보보안기사] 2023년 1회차(22회) 정보보안기사 실기 불합격 후기 (1) 2023.04.23
[정보보안기사] 2022년 21회 정보보안기사 실기 기출문제 복원 (0) 2023.04.07
[정보보안기사] 2022년 4회차(21회) 정보보안기사 실기 시험 불합격 후기 (0) 2022.11.27

Tag acct/pacct byod crlf DNS 증폭 공격 DOA EIGRP php.ini Threshold 기준선 접근법 상세 위험 분석법

'정보보안기사'의 다른글

이전글 [정보보안기사] 2023년 1회차(22회) 정보보안기사 실기 불합격 후기
현재글 : [정보보안기사] 2023년 22회 정보보안기사 실기 기출문제 복원
다음글 [정보보안기사] 2023년 2회차(23회) 정보보안기사 실기 불합격 후기

관련글

[정보보안기사] 2023년 23회 정보보안기사 실기 기출문제 복원
2023.11.10

[정보보안기사] 2023년 2회차(23회) 정보보안기사 실기…
2023.07.30

[정보보안기사] 2023년 1회차(22회) 정보보안기사 실기…
2023.04.23

댓글 0

이상향
취미는 라이센스 :)
구독하기

이름 비밀번호

내용을 입력해주세요.

비밀글 등록

취미는 라이센스 :)

검색내용을 입력하세요.