2019-국회직-정보보호론-가형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

1. 다음 설명에서 제시하는 공격의 명칭은?

사용자가 특정 웹 사이트에 접속하기 위해 올바른 URL을 입력하였지만, 실제로는 해커가 만들어 놓은 웹 사이트에 접속되었다. 해커의 웹 사이트에서는 불법적으로 개인정보가 수집되고 있었다. 사용자의 컴퓨터는 공격자에게 점유되어 정상적인 URL을 입력해도 이에 해당하는 IP 주소가 공격자의 웹 서버로 연결되도록 되어 있었다.

① Pharming
② Smishing
③ QRshing
④ Phishing
⑤ SQL Injection

정답 체크 :

(1) Pharming : Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다.

오답 체크 :

(2) Smishing : SMS(문자 메시지)와 Phishing의 약자이다. Phishing은 Private Data(개인정보)와 Fishing(낚시)의 약자이다. 공격자가 문자 메시지에 URL을 보내고, 사용자가 이를 클릭하면 해킹 툴이 스마트폰에 설치되어 개인 정보가 탈취된다.

(3) QRshing : QR code와 Phishing의 약자이다. QR code에 기반한 Phishing을 의미한다.

(4) Phishing : rivate data(개인 정보)와 fishing(낚는다)의 합성어이다. 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보와 같은 개인정보를 빼내는 사기기법을 말한다.

(5) SQL Injection : 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.

2. 네트워크 보안과 관련된 다음 설명에서 ㉠, ㉡에 들어갈 용어는?

네트워크 인터페이스 카드가 가지고 있는 모드 중 (㉠) 모드를 설정하여 네트워크 인터페이스 카드를 거치는 모든 데이터를 확인하는 스니핑 공격을 수행할 수 있다. 이 모드 설정을 위해서 Linux 환경에서는 (㉡) 명령어를 활용한다.

	㉠	㉡
①	non-promiscuous	netstat
②	promiscuous	netstat

③ non-promiscuous ifconfig
④ promiscuous ifconfig
⑤ non-promiscuous ipconfig

정답 체크 :

(4)

promiscuous : 자신의 IP와 MAC에 상관없이 패킷을 수신한다.

ifconfig : 유닉스 혹은 리눅스에서 일반적으로 네트워크 인터페이스의 IP 주소와 넷마스크의 설정 및 인터페이스의 활성화/비활성화 등을 위해 사용된다.

오답 체크 :

(1), (2), (3), (5)

non-promiscuous : 자신의 IP와 MAC을 비교해서 일치하지 않으면 패킷을 수신하지 않는다.

netstat : 유닉스, 리눅스, 윈도우에서 전송 제어 프로토콜, 라우팅 테이블, 수많은 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결을 보여주는 명령 줄 도구이다. 예를 들면, 현재 내 컴퓨터가 맺고 있는 TCP/UDP 연결 정보를 확인하기 위해 사용한다.

ipconfig : ifconfig와 동일한 기능을 수행하지만 윈도우에서 사용하는 명령어이다.

3. RSA 암호 시스템에서 밥이 앨리스의 공개키 (e, N)= (11, 143)을 취득하여 앨리스에게 평문 4를 암호화하여 보내고자 한다. 이때 전송되는 암호문은?

① 11^4 mod 143
② 4^{11} mod 143
③ 4^{143} mod 11
④ 11^{143} mod 7
⑤ 4^{143} mod 7

정답 체크 :

(2) 암호문 = 평문^e mod N = 4^{11} mod 143

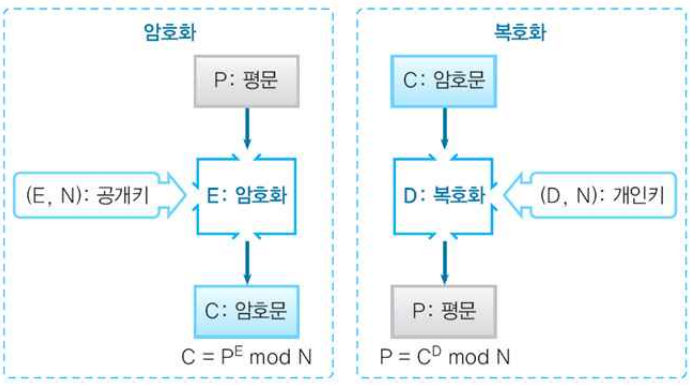


그림 6-6 • RSA 암호화와 복호화

4. 다음과 같은 정보보안 요구사항이 존재할 때 필요한 정보보호 시스템들을 짝지은 것으로 옳은 것은?

공인 IP 주소 자원의 효율적인 관리를 위해 사설 IP와의 연계를 수행하고 조직 내부의 네트워크 구조를 외부에서 알 수 없도록 하고 싶다. 또한, 내부에서 외부로의 정보유출을 탐지하여 개인정보 및 민감 정보의 유출을 차단하고자 한다.

① NAT-VPN
② IPS-DLP
③ NAT-SSL
④ IPS-SSL
⑤ NAT-DLP

정답 체크 :
(5)
NAT : 대부분의 가정에서 설치된 유무선 공유기나 방화벽에서 동작한다. 유무선 공유기 내부인 가정에서는 사설 IP를 사용하고 해당 패킷이 외부로 나갈 때는 공유기를 통해 NAT 과정을 거쳐 공인 IP로 변환되어 나간다. 외부에서 패킷이 들어올 때는 공인 IP가 NAT에 의해 사설 IP로 바뀐다.
DLP(Data Loss Prevention) : 기업 내에서 이용하는 다양한 주요 정보인 기술 정보, 프로젝트 계획, 사업 내용, 영업 비밀, 고객 정보 등을 보호하고 외부 유출을 방지하기 위해서 사용된다.
오답 체크 :
(1), (2), (3), (4)
VPN : 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.
IPS : 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다.
SSL : 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있다.

5. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?
① 신뢰받는 제3자인 키 배포 기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션 키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 토큰을 이용한 인증 프로토콜이다.
④ 인증 서버가 사용자에게 발급한 티켓(즉, 티켓-승인 티켓)은 유효기간 내에 재사용할 수 있다.
⑤ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

정답 체크 :
(5) kerberos에서 발급되는 티켓들(TGT, Ticket)은 재사용이 가능하기 때문에 SSO를 구축할 수 있다.

오답 체크 :

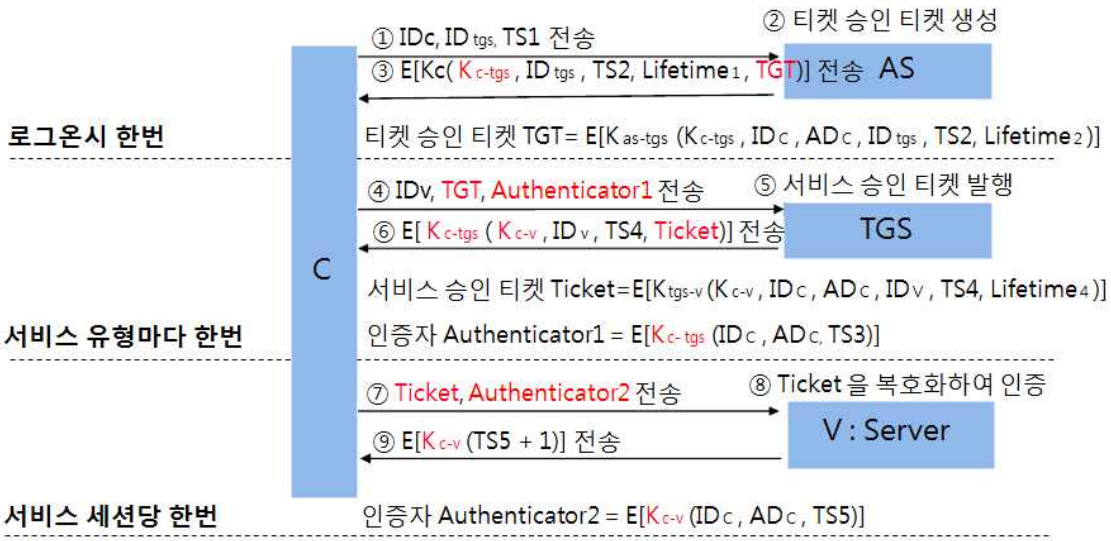
(1) 신뢰받는 제3자인 AS와 TGS가 중간에 개입한다.

(2) 세션키인 Kc-tgs와 Kc-v를 사용한다. (아래 그림 참조)

(3) 여기서 토큰은 티켓을 의미한다.

(4) TGT는 유효기간(Lifetime2) 내에 재사용이 가능하다. (아래 그림 참조)

Tip! : Kerberos 버전 4의 인증 프로토콜을 그림으로 나타내면 다음과 같다.



6. 다음 설명에서 제시하는 목적으로 활용되는 네트워크 보안 기술은?

조직 내에 운영되는 다양한 정보보안 장비 및 IT 시스템들의 이벤트 로그를 수집, 분석하여 이상 징후 및 위험사항을 파악한다. 이렇게 파악된 결과를 인지하기 쉬운 형태로 가공하여 경영진에 보고하기도 한다. 이상 징후의 도출에 전문가의 경험을 활용하거나 인공지능 기술을 활용한다.

① SIEM

② DLP

③ VPN

④ NAT

⑤ IPS

정답 체크 :

(1) SIEM : 로그 분석해서 이상 징후 파악한 후 결과를 경영진에게 보고할 수 있도록 해주는 시스템이다. 이벤트 로그 데이터를 실시간 수집/분석한다. 침해 공격 로그에 대한 포렌식(디지털 증거)과 컴플라이언스(보안에 대한 방향성 제시) 또는 법적 조사를 위해 해당 데이터의 신속한 검색, 리포팅한다. 원본 이벤트 정보 분석하기보다, 정규화 과정을 통해 데이터 표준화해서 분석한다.

오답 체크 :

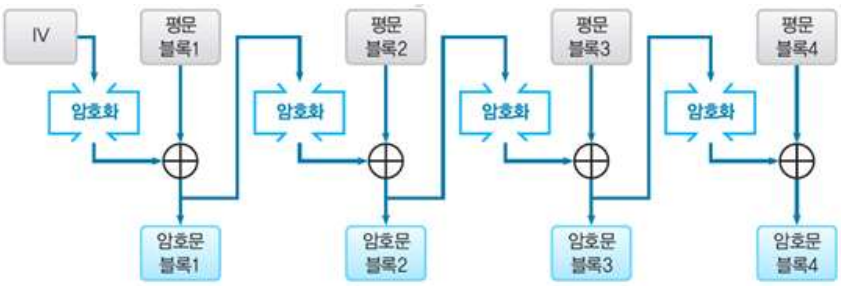
(2) DLP(Data Loss Prevention) : 기업 내에서 이용하는 다양한 주요 정보인 기술 정보, 프로젝트 계획, 사업 내용, 영업 비밀, 고객 정보 등을 보호하고 외부 유출을 방지하기 위해서 사용된다.

(3) VPN : 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.
(4) NAT : 대부분의 가정에서 설치된 유무선 공유기나 방화벽에서 동작한다. 유무선 공유기 내부인 가정에서는 사설 IP를 사용하고 해당 패킷이 외부로 나갈 때는 공유기를 통해 NAT 과정을 거쳐 공인 IP로 변환되어 나간다. 외부에서 패킷이 들어올 때는 공인 IP가 NAT에 의해 사설 IP로 바뀐다.
(5) IPS : 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다.

7. 보안 프로토콜에 대한 설명으로 옳지 않은 것은?
① 경량 프로토콜인 CoAP는 DTLS를 사용하여 보안성을 제공한다.
② 사물인터넷 프로토콜인 MQTT는 TLS 프로토콜을 사용한다.
③ TLS 프로토콜은 UDP 상에서 동작하므로 많은 인터넷 응용에서 사용된다.
④ HTTPS는 HTTP 프로토콜에 SSL/TLS를 적용한 것이다.
⑤ SSH은 TCP 프로토콜 상에서 사용되며, telnet의 안전성 보장에 사용된다.
정답 체크 :
(3) TLS는 TCP 상에서 동작하고, DTLS는 UDP 상에서 동작한다.
오답 체크 :
(1) CoAP(리소스 제약이 있는 기기들이 인터넷 상에서 TCP 대신 UDP를 사용해 커뮤니케이션 할 수 있도록 개발)는 DTLS를 사용한다.
(2) MQTT(퍼블리시/섭스크라이브 메시징 프로토콜로, 자원 제약이 있는 기기를 타깃으로 개발)는 TLS를 사용한다.
(4) HTTPS는 HTTP의 보안이 강화된 버전이다(443 포트, SSL/TLS를 적용). HTTPS는 통신의 인증과 암호화를 위해 넷스케이프 커뮤니케이션즈 코퍼레이션이 개발했으며, 전자상거래에서 널리 쓰인다.
(5) SSH는 두 호스트(Host) 사이의 통신 암호화 관련 인증 기술들을 사용하여, 안전한 접속과 통신을 제공하는 프로토콜을 의미한다. 안전한 ftp 혹은 telnet을 사용할 수 있다.

8. 블록 암호(Block Cipher) 모드에 대한 설명으로 옳지 않은 것은?
① ECB(Electronic CodeBook) 모드는 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.
② CBC(Cipher Block Chaining) 모드는 암호화 전에 XOR 연산을 수행한다.
③ CFB(Cipher FeedBack) 모드는 평문 블록을 암호 알고리즘으로 직접 암호화한다.
④ OFB(Output FeedBack) 모드는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.
⑤ CTR(CounTeR) 모드는 스트림 암호의 일종으로 카운터의 값이 암호화의 입력이 된다.
정답 체크 :
(3) CFB : 그림에서 보는 바와 같이 전단계의 암호문 블록을 암호화하고, 평문 블록을 직

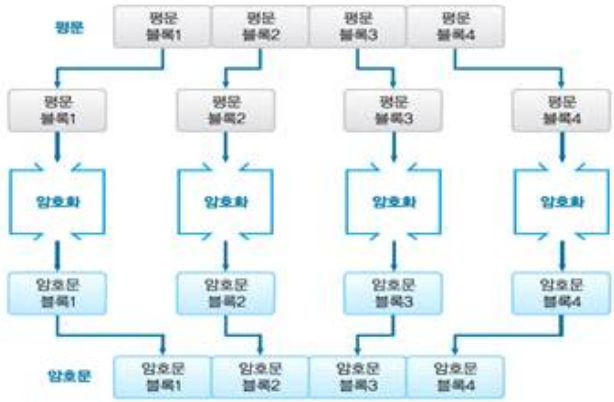
접 암호화하지 않는다.



(a) CFB 모드에 의한 암호화

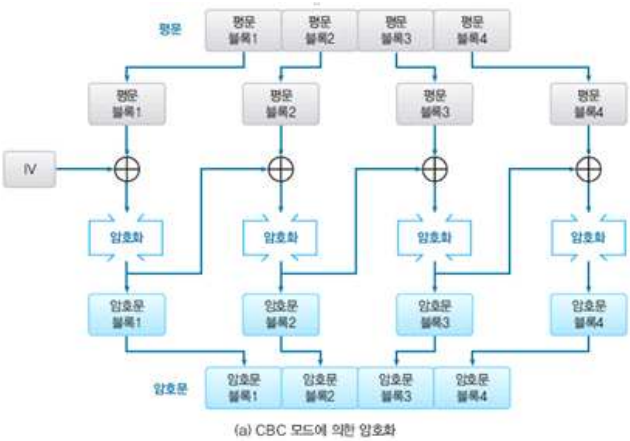
오답 체크 :

(1) ECB : 그림에서 보는 바와 같이 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.

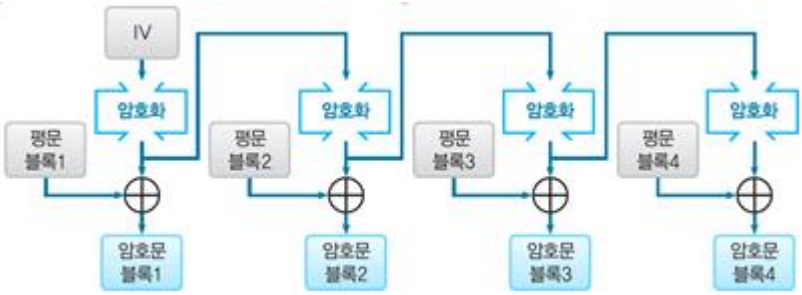


(a) ECB 모드에 의한 암호화

(2) CBC : 그림에서 보는 바와 같이 암호화 전에 XOR 연산을 수행한다.

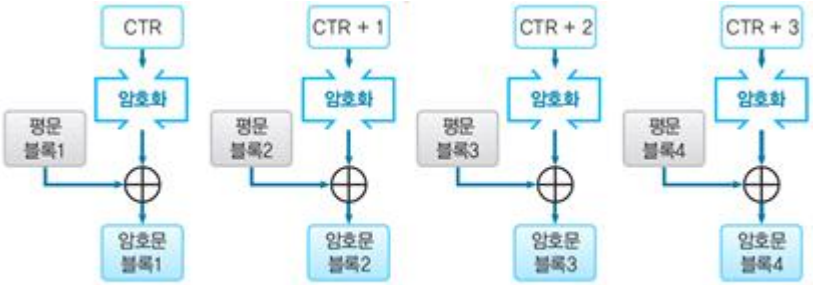


(4) OFB : 그림에서 보는 바와 같이 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.



(a) OFB 모드에 의한 암호화

(5) CTR : 그림에서 보는 바와 같이 카운터의 값이 암호화의 입력이 된다.



(a) CTR 모드에 의한 암호화

9. 파일을 실행시킬 때 사용자의 권한이 아닌 일시적으로 파일 소유자(특히 관리자)의 권한을 가지기 때문에 공격에 많이 사용되는 것은?

① setuid
② setgid
③ uid
④ gid
⑤ sticky bit

정답 체크 :

(1) setuid : 8진수로 4000으로 표현한다. 사용자가 실행 파일의 사용자 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.

오답 체크 :

(2) setgid : 8진수로 2000으로 표현한다. 사용자가 실행 파일의 그룹 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.

(3) uid : user id를 의미한다.

(4) gid : group id를 의미한다.

(5) sticky bit : 8진수로 1000으로 표현한다. 디렉토리에 sticky bit가 설정되면 디렉토리 안의 파일들은 파일 소유자, 디렉토리 소유자 또는 관리자(root)만이 수정하거나 삭제할 수 있다.

10. 개인정보 비식별화 조치로 볼 수 없는 것은?

① 가명 처리
② 총계 처리

③ 데이터 값 삭제
④ 범주화 수행
⑤ 공개키 암호 기반 서명값 생성
정답 체크 :
(5) 공개키 암호 기반 서명값 생성은 디지털 서명으로 개인정보 비식별화 조치와 무관한다.
오답 체크 :
(1), (2), (3), (4)
아래의 표를 참고하기 바란다(KISA : 개인정보 비식별 조치 가이드라인).

• 〈 예시 〉 비식별 조치 방법 •

처리기법	예시	세부기술
가명처리 (Pseudonymization)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대, 서울 거주, 국제대 재학	① 휴리스틱 가명화 ② 암호화 ③ 교환 방법
총계처리 (Aggregation)	• 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm	④ 총계처리 ⑤ 부분총계 ⑥ 라운딩 ⑦ 재배열
데이터 삭제 (Data Reduction)	• 주민등록번호 901206-1234567 → 90년대 생, 남자 • 개인과 관련된 날짜정보(합격일 등)는 연단위로 처리	⑧ 식별자 삭제 ⑨ 식별자 부분삭제 ⑩ 레코드 삭제 ⑪ 식별요소 전부삭제
데이터 범주화 (Data Suppression)	• 홍길동, 35세 → 홍씨, 30~40세	⑫ 감추기 ⑬ 랜덤 라운딩 ⑭ 범위 방법 ⑮ 제어 라운딩
데이터 마스킹 (Data Masking)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 홍○○, 35세, 서울 거주, ○○대학 재학	⑯ 임의 잡음 추가 ⑰ 공백과 대체

11. TCP/IP 기반의 네트워크에서 목적지 호스트까지의 경로를 파악하기 위해서 데이터그램의 TTL 값과 ICMP Time Exceeded 메시지를 기반으로 동작되는 도구는?
① ipconfig
② traceroute
③ nslookup
④ netstat
⑤ telnet
정답 체크 :
(2) traceroute : 리눅스에서 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시해 준다. 윈도우에서는 tracert를 사용한다.
오답 체크 :
(1) ipconfig : 윈도우에서 일반적으로 네트워크 인터페이스의 IP 주소와 넷마스크의 설정

및 인터페이스의 활성화/비활성화 등을 위해 사용된다.
(3) nslookup : 인터넷 서버 관리자나 사용자가 호스트 이름을 입력하면 그 IP 주소를 알려주는 프로그램이고, 그 반대의 경우에도 가능하다. DNS에 비해 다양한 정보를 확인할 수 있다.
(4) netstat : 유닉스, 리눅스, 윈도우에서 전송 제어 프로토콜, 라우팅 테이블, 수많은 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결을 보여주는 명령 줄 도구이다. 예를 들면, 현재 내 컴퓨터가 맺고 있는 TCP/UDP 연결 정보를 확인하기 위해 사용한다.
(5) telnet : 인터넷을 통하여 원격지의 호스트 컴퓨터에 접속할 때 지원되는 인터넷 표준 프로토콜이다.

12. 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 옳지 않은 것은?
① 물리적 망분리와 논리적 망분리 기법이 존재한다.
② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.
③ 논리적 망분리 기법으로는 SBC 및 CBC 기반의 망분리 기법이 존재한다.
④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.
⑤ 데이터 다이오드 기반 데이터 일방향성을 이용하여 망분리 실현이 가능하다.
정답 체크 :
(4) 애플리케이션 가상화 및 데스크톱 가상화는 물리적 망분리가 아니라 논리적 망분리이다.
오답 체크 :
(1) 물리적 망분리는 물리적으로 2대의 PC를 사용하고, 논리적 망분리는 SBC, CBC를 이용하여 논리적으로 1대의 PC를 사용한다.
(2) 물리적으로 2대의 PC를 사용한다고 하더라도 USB와 같은 저장 매체를 통해 악성 코드 침입이 가능하다(사회공학기법 : 누군가 회사앞에 USB를 떨어뜨려놓고 회사 사람이 그것을 주워 자신의 회사 PC에 꽂아봄).
(3) 논리적 망분리에서는 SBC(서버 기반 가상화)와 CBC(클라이언트 기반 가상화) 기법이 존재한다.
(5) 데이터 다이오드(Data Diode, 단방향 네트워크, 단방향 보안 게이트웨이)는 오로지 한 방향으로 데이터가 흐르며 정보의 보안을 보증하기 위해 사용되는 네트워크 장비 또는 데이터를 허용하는 기기이다. 해당 기술을 망분리에 적용할 수 있다.

13. 다음 설명에서 제시하고 있는 공격기법과 연관된 네트워크 프로토콜은?

중간자(MITM: Man-In-The-Middle) 공격의 일종으로 같은 네트워크에 설치된 컴퓨터에 “피해 대상 IP 주소를 소유한 컴퓨터의 MAC 주소”를 “공격자의 MAC 주소”로 대체하는 공격을 수행한다. “피해 대상 컴퓨터”로 전달되는 메시지는 “공격자 컴퓨터”를 통해서 “피해 대상 컴퓨터”에 전달된다.

① TCP
② IP

③ ARP
④ ICMP
⑤ HTTP
정답 체크 :
(3) ARP : IP 주소(논리 주소)에 대한 MAC 주소(물리 주소)를 제공한다. 참고로, rarp는 MAC 주소에 대한 IP 주소를 제공한다.
오답 체크 :
(1) TCP : 근거리 통신망이나 인트라넷, 인터넷에 연결된 컴퓨터에서 실행되는 프로그램 간에 일련의 옥텟을 안정적으로, 순서대로, 에러없이 교환할 수 있게 한다. 연결 설정을 수행하고, 흐름 제어와 혼잡 제어를 수행한다. TCP는 웹 브라우저들이 월드 와이드 웹에서 서버에 연결할 때 사용되며, 이메일 전송이나 파일 전송에도 사용된다.
(2) IP : 1개의 패킷에 대한 E2E(end-to-end) 전송을 담당하며, 논리적인 주소 지정(주소를 바꿀 수 있음)과 경로 설정(best route)을 담당하는 네트워크 계층 프로토콜이다.
(4) ICMP : 인터넷 제어 메시지 프로토콜은 RFC 792에서 정의한 인터넷 프로토콜 모음 중의 하나이다. ICMP 메시지들은 일반적으로 IP 동작에서 진단이나 제어로 사용되거나 오류에 대한 응답으로 만들어진다. 예를 들어, 핑(ping) 유틸리티는 ICMP "에코 요청(Echo request)"과 "에코 응답(Echo reply)" 메시지를 사용해 구현할 수 있다.
(5) HTTP : 웹 브라우저와 웹 서버 사이에서 웹 문서(HTML)을 전송하기 위한 프로토콜이다.

14. 전문가의 경험과 지식을 활용하여 빠르게 진행되는 위험 분석 접근법은?
① 비정형 접근법(Informal Approach)
② 상세 위험 분석 접근법(Detailed Risk Analysis)
③ 기준 접근법(Baseline Approach)
④ 수학 공식 접근법(Math Formula Approach)
⑤ 단위 접근법(Unit Approach)
정답 체크 :
(1) 비정형(비형식적) 접근법 : 모든 정보자산에 기업이외의 전문가 지식 및 경험을 활용하는 방법이다. 비용 대비 효과가 우수하며 소규모 조직에 적합하고 상세 위험 분석보다 빠르게 수행된다.
오답 체크 :
(2) 상세 위험 (분석) 접근법 : 모든 정보자산에 대해 상세 위험 분석을 하는 방법이다. 자산가치, 위협, 취약점의 평가에 기초한 위험을 산정하므로 근거가 명확하지만, 상당힌 시간과 노력이 소요된다.
(3) 기준(선) 접근법 : 모든 시스템에 대하여 표준화딘 정보보호대책 세트를 제공(체크리스트 형태)한다. 비용 및 시간을 절약할 수 있지만 과보호 또는 부족한 보호가 될 가능성이 상존한다.
(4) 수학 공식 접근법 : 위협의 발생 빈도를 계산하는 식을 이용하여 위험을 계량하는 방법이다. 과거 자료의 획득이 어려울 경우, 위협 발생 빈도를 추정하여 분석하는데 유용하다. 위험을 정량화 하여 매우 간결하게 나타낼 수 있으나, 기대 손실을 추정하는 자료의 양이 낮다는 단점이 있다.

(5) 단위 접근법 : 예를 들어 손실크기를 화폐 단위로 측정이 가능할 때 사용하는 분석법이다(과거자료, 수학공식, 확률분포).

15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?
① 사용할 수 있는 대칭 암호 알고리즘에는 IDEA, CAST, 트리플 DES 등이 있다.
② 공개키의 취소 증명서를 발행할 수 있다.
③ 데이터의 압축은 ZIP 형식을 사용한다.
④ RSA, MD5 등의 알고리즘을 이용하여 전자서명을 한다.
⑤ 한 명의 사용자는 다수의 공개키/개인키 쌍을 사용할 수 없다.
정답 체크 :
(5) 한 명의 사용자는 다수의 공개키/개인키 쌍을 사용할 수 있다(PKI 구조가 아닌 신뢰망 방식).
오답 체크 :
(1) 사용할 수 있는 대칭 암호 알고리즘에는 AES, IDEA, CAST, 3-DES, Blowfish, Twofish 등이 있다.
(2) 인증서는 OpenPGP에서 정해진 형식의 인증서와, X.509 호환용 인증서를 작성한다. 그리고 공개키의 취소 증명서(revocation certificate) 발행한다.
(3) 압축에 이용되는 형식은 ZIP이다.
(4) 디지털 서명 알고리즘은 RSA, DSA 등을 사용하고, 서명 시간을 단축하기 위해 MD5, SHA-1, RIPEMD-160 등의 해시를 사용한다.

16. 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?
① 메시지 자체를 암호화 또는 복호화할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.
② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.
③ 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.
④ 공개키 알고리즘을 사용하여 공개키와 개인키를 생성하고, 공개키를 상대방에게 전달한다.
⑤ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화할 수 있다.
정답 체크 :
(3) 하이브리드 암호 시스템은 공개키 암호를 이용하여 대칭키를 암호화하므로 대칭키 암호의 키 교환 문제가 발생하지 않는다.
오답 체크 :
(1) 메시지 암호화/복호화에는 대칭키를 사용한다.
(2) 암호화에 사용된 대칭키를 상대방에게 전달할 때 상대방의 공개키로 암호화를 수행한다.
(4) 수신자는 공개키 알고리즘을 사용하여 공개키와 개인키를 생성하고, 공개키를 상대방에게 전달한다.
(5) 수신자를 암호화된 대칭키를 수순자의 개인키로 복호화할 수 있다.

17. <보기>에서 XSS 공격을 수행하는 과정을 나타낸 설명 중 옳지 않은 것은?

<보 기>

ㄱ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.

ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.

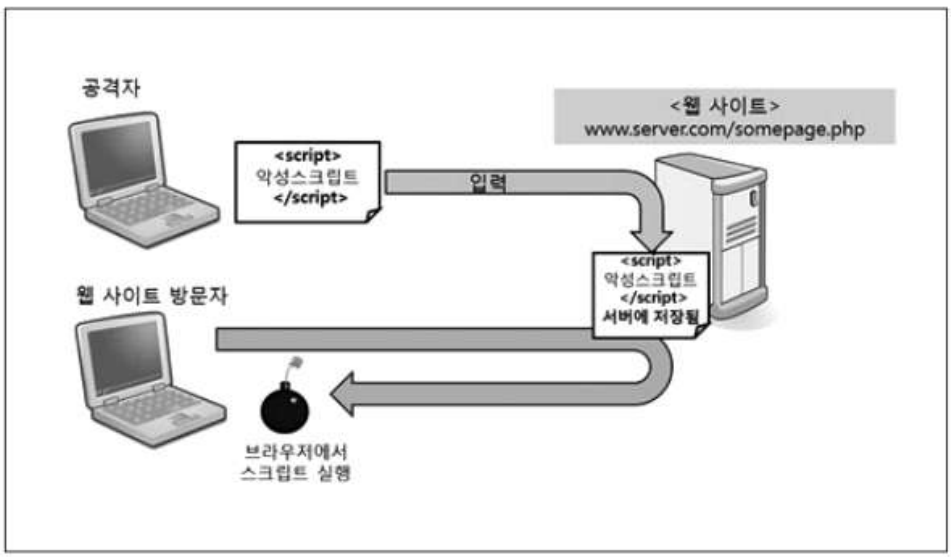
ㄷ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.

ㄹ. 웹 서버에서 XSS 코드가 실행된다.

ㅁ. 공격 결과가 공격자에게 전달된다.

① ㄱ
② ㄴ
③ ㄷ
④ ㄹ
⑤ ㅁ

정답 체크 :
(4) 클라이언트에서 XSS 코드가 실행된다.
오답 체크 :
(1), (2), (3) 저장 XSS 공격에 해당한다(아래 그림 참조).
(5) 사용자가의 정보(쿠키)가 공격자에게 전달된다.
Tip! : 저장 XSS 공격 방법을 그림으로 나타내면 다음과 같다.



[그림 4] 저장 XSS 공격 방법

18. CEK(Contents Encrypting Key)와 KEK(Key Encrypting Key)에 대한 설명으로 옳지 않은 것은?

① KEK를 이용하여 지켜야 할 키의 개수를 줄일 수 있다.
② 통상적으로 CEK에는 세션 키(Session Key)가, KEK에는 마스터 키(Master Key)가 사용된다.

③ 암호문과 KEK만 있다면 원래의 콘텐츠를 알 수 있다.
④ KEK를 이용하여 CEK를 암호화한다.
⑤ KEK의 기밀성을 유지하기 위하여 PBE(Password Based Encryption)를 이용하기도 한다.
정답 체크 :
(3) 암호문, KEK, CEK가 있다면 원래의 콘텐츠를 알 수 있다. KEK로 CEK를 복호화하고, 복호화된 CEK로 암호문을 복호화한다(아래 그림 참조).
오답 체크 :
(1) KEK는 키를 암호화는 키로서 다수의 키를 한 개의 키(KEK)로 암호화하여 보관한다.
(2) CEK에는 세션키(통신 때마다 한번만 사용되는 키)를 사용하고, KEK는 마스터키(반복적으로 사용되는 키)를 사용한다.
(4) KEK를 이용하여 CEK를 암호화한다(아래 그림 참조).
(5) PBE란 의사난수 생성기로 솔트(salt)라는 난수를 생성하고 솔트와, 사용자가 입력한 패스워드를 순서대로 일방향 해수 함수에 입력한다. 여기서 얻어진 해시 값이 키의 암호화를 위한 키(KEK)가 되고 해당 KEK는 사전 공격에 안전하다.
Tip! : 아래 그림은 콘텐츠를 암호화하는 키(CEK)와 키를 암호화하는 키(KEK)를 나타낸다.

그림 12-5 • 콘텐츠를 암호화하는 키(CEK)와 키를 암호화하는 키(KEK)

19. '개인정보의 안전성 확보 조치 기준' 고시에서 5만 명의 고유식별정보를 공공기관의 내부망에 저장할 경우, 해당 고유식별정보의 암호화 의무 여부를 결정하기 위해 필요한 조치에 해당하는 용어는?
① ISMS
② 취약점 점검
③ 침투 테스트
④ 개인정보 영향평가
⑤ 자산 평가
정답 체크 :
(4)
"개인정보의 안전성 확보 조치 기준" 제7조(개인정보의 암호화) 상 ④ 개인정보처리자가 내

부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. "개인정보 보호법" 제33조(개인정보 영향평가) 상에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과
"개인정보 보호법" 제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.
② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.
1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항

20.「개인정보 보호법」 제38조 권리행사의 방법 및 절차에 대한 설명으로 옳지 않은 것은?
① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 없다.
③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.
정답 체크 :
(2) "개인정보 보호법" 제38조(권리행사의 방법 및 절차) 상 ② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.
오답 체크 :
(1) "개인정보 보호법" 제38조(권리행사의 방법 및 절차) 상 ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
(3) "개인정보 보호법" 제38조(권리행사의 방법 및 절차) 상 ③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
(4) "개인정보 보호법" 제38조(권리행사의 방법 및 절차) 상 ④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

(5) "개인정보 보호법" 제38조(권리행사의 방법 및 절차) 상 ⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.