정보보호론

문 1. 송·수신자의 MAC 주소를 가로채 공격자의 MAC 주소로 변경하는 공격은? 1

① ARP spoofing
② Ping of Death
③ SYN Flooding
④ DDoS

[해설]

- ARP Spoofing 공격은 스위칭 환경의 랜상에서 패킷의 흐름을 바꾸는 공격 방법이다. 대응책으로는 ARP 테이블이 변경되지 않도록 arp -s [IP 주소][MAC 주소] 명령으로 MAC 주소 값을 고정시키는 것이다.

문 2. 스니핑 공격의 탐지 방법으로 옳지 않은 것은? 4

① ping을 이용한 방법
② ARP를 이용한 방법
③ DNS를 이용한 방법
④ SSID를 이용한 방법

[해설]

스니핑 공격 탐지 방법
- Ping을 이용한 스니퍼 탐지 : 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 Request를 받으면 Response를 전달한다. 이를 이용해 의심이 가는 호스트에 ping을 보내면 되는데, 네트워크에 존재하지 않는 MAC 주소를 위장하여 보낸다. (만약 ICMP Echo Reply를 받으면 해당 호스트가 스니핑을 하고 있는 것이다.)
- ARP를 이용한 스니퍼 탐지 : ping과 유사한 방법으로, 위조된 ARP Request를 보냈을 때 ARP Response가 오면 프러미스큐어스 모드로 설정되어 있는 것이다.
- DNS를 이용한 스니퍼 탐지 : 일반적으로 스니핑 프로그램은 사용자의 편의를 위하여 스니핑한 시스템의 IP 주소에DNS에 대한 이름 해석 과정(Inverse-DNS lookup)을 수행한다. 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지한다.
- 유인(Decoy)을 이용한 스니퍼 탐지 : 스니핑 공격을 하는 공격자의 주요 목적은 ID와 패스워드의 획득에 있다. 가짜 ID와 패스워드를 네트워크에 계속 뿌려 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 공격자를 탐지할 수 있다.
- ARP watch를 이용한 스니퍼 탐지 : ARP watch는 MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려주는 툴이다. 대부분의 공격 기법이 위조된 ARP를 사용하기 때문에 이를 쉽게 탐지할 수 있다.

문 3. 공격자가 해킹을 통해 시스템에 침입하여 루트 권한을 획득한 후, 재침입할 때 권한을 쉽게 획득하기 위하여 제작된 악성 소프트웨어는? 4

① 랜섬웨어
② 논리폭탄
③ 슬래머 웜
④ 백도어

[해설]

- 백도어(backdoor)는 시스템의 보안이 제거된 비밀 통로로서 서비스 기술자나 유지 보수 프로그래머들이 접근 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 통로이다. 이를 정상적인 보안 절차를 우회하는 악성 소프트웨어로 악용하는 경우가 있다.
- 슬래머 웜 : 윈도 서버(MS-SQL 서버)의 취약점을 이용해 대량의 네트워크 트래픽을 유발하여 네트워크를 마비시키는 바이러스이다.

문 4. 다음에서 설명하는 용어는? 2

> ○ 한 번의 시스템 인증을 통해 다양한 정보시스템에 재인증 절차 없이 접근할 수 있다.
> ○ 이 시스템의 가장 큰 약점은 일단 최초 인증 과정을 거치면, 모든 서버나 사이트에 접속할 수 있다는 것이다.

① NAC(Network Access Control)
② SSO(Single Sign On)
③ DRM(Digital Right Management)
④ DLP(Data Leak Prevention)

[해설]

- SSO(Single Sign On) : 단일사용승인은 하나의 아이디로 여러 사이트를 이용할 수 있는 시스템이다. SSO은 사용자의 편의성을 증가시키고, 기업의 관리자 입장에서도 회원에 대한 통합관리가 가능해서 마케팅을 극대화시킬 수 있는 장점이 있다. SSO을 채택한 인증서버 시스템으로는 커버로스(Kerberros), 세사미(SESAME), 크립토나이트(Kriptonight)가 있다.

문 5. 보안 공격 유형에는 적극적 공격과 소극적 공격이 있다. 다음 중 공격 유형이 다른 하나는? 1

① 메시지 내용 공개(release of message contents)
② 신분 위장(masquerade)
③ 메시지 수정(modification of message)
④ 서비스 거부(denial of service)

[해설]

- 메시지 내용 공개(release of message contents, 메시지 내용 갈취) : 민감하고 비밀스런 정보를 취득하거나 열람할 수 있으며, 이는 소극적인 위협에 해당된다.

문 6. X.509 인증서 폐기 목록(Certificate Revocation List) 형식 필드에 포함되지 않는 것은? 2

① 발행자 이름(Issuer name)
② 사용자 이름(Subject name)
③ 폐지된 인증서(Revoked certificate)
④ 금번 업데이트 날짜(This update date)

[해설]

- X.509 인증서 폐기 목록(Certificate Revocation List) 형식 필드에 포함되는 내용은 발행자 이름(Issuer name), 폐지된 인증서(Revoked certificate), 금번 업데이트 날짜(This update date), 다음 업데이트 날짜(Next update date), 버전(Version), 시그니처(Signature) 가 있다.

문 7. AES 알고리즘에 대한 설명으로 옳지 않은 것은? 4

① 블록 암호 체제를 갖추고 있다.
② 128/192/256bit 키 길이를 제공하고 있다.
③ DES 알고리즘을 보완하기 위해 고안된 알고리즘이다.
④ 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.

[해설]

- 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 XOR 연산을 수행한다.

문 8. 정보기술과 보안 평가를 위한 CC(Common Criteria)의 보안 기능적 요구 조건에 해당하지 않는 것은? 2

① 암호 지원
② 취약점 평가
③ 사용자 데이터 보호
④ 식별과 인증

[해설]

- CC 의 구성

구성	세부설명
1부	-소개 및 일반 모델 : 용어정의, 보안성 평가개념 정의, PP/ST 구조 정의
2부	- 보안 기능 요구사항 - 11개 기능 클래스 : 보안감사, 통신, 암호지원, 사용자 데이터 보호, 식별 및 인증, 보안관리, 프라이버시, TSF 보호, 자원 활용, ToE 접근, 안전한 경로/채널,
3부	- 보증 요구사항 - 7개 보증 클래스 : PP/ST 평가, 개발, 생명주기 지원, 설명서, 시험, 취약성 평가, 합성

문 9. 커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은? 4

① 사용자를 인증하기 위해 사용자의 패스워드를 중앙집중식 DB에 저장하는 인증 서버를 사용한다.
② 사용자는 인증 서버에게 TGS(Ticket Granting Server)를 이용하기 위한 TGT(Ticket Granting Ticket)를 요청한다.
③ 인증 서버가 사용자에게 발급한 TGT는 유효기간 동안 재사용할 수 있다.
④ 네트워크 기반 인증 시스템으로 비대칭 키를 이용하여 인증을 수행한다.

[해설]

- 커버로스는 신뢰할 수 있는 제 3자 인증 프로토콜로서, 인증과 메시지 보호를 제공하는 보안 시스템의 이름이며. 대칭키 암호 방식을 사용하여 분산 환경에서 개체 인증 서비스를 제공한다.

문 10. 다음에서 설명하는 보안 공격은? 3

> ○ 정상적인 HTTP GET 패킷의 헤더 부분의 마지막에 입력되는 2개의 개행 문자(\r\n\r\n) 중 하나(\r\n)를 제거한 패킷을 웹 서버에 전송할 경우, 웹 서버는 아직 HTTP 헤더 정보가 전달되지 않은 것으로 판단하여 계속 연결을 유지하게 된다.
> ○ 제한된 연결 수를 모두 소진하게 되어 결국 다른 클라이언트가 해당 웹 서버에 접속할 수 없게 된다.

① HTTP Cache Control ② Smurf
③ Slowloris ④ Replay

[해설]

- SLOWLORIS 공격 : 비정상 HTTP 헤더(완료되지 않은 헤더)를 전송함으로써 웹 서버 단의 커넥션 자원을 고갈 시키는 공격이다.
- HTTP Cache Control 공격 : 서버에 전달 되는 HTTP Get 패킷에 캐싱 장비가 응답하지 않도록 설정하여 서버의 부하를 증가시켜서 다른 클라이언트 시스템이 해당서버의 서비스를 받을수없도록 하는 공격이다.

문 11. (가), (나)에 들어갈 접근통제 보안모델을 바르게 연결한 것은? 2

> (가)은 허가되지 않은 방식의 접근을 방지하는 모델로 정보 흐름 모델 최초의 수학적 보안모델이다.
> (나)은 비즈니스 입장에서 직무분리 개념을 적용하고, 이해가 충돌되는 회사 간의 정보의 흐름이 일어나지 않도록 접근통제 기능을 제공하는 보안모델이다.

	(가)	(나)
①	Bell-LaPadula Model	Biba Integrity Model
②	Bell-LaPadula Model	Brewer-Nash Model
③	Clark-Wilson Model	Biba Integrity Model
④	Clark-Wilson Model	Brewer-Nash Model

[해설]

- Bell-LaPadula Model : 군사용 보안구조의 요구 사항을 충족하기 위해 설계된 모델이다. 가용성이나 무결성 보다 비밀유출(Disclosure, 기밀성) 방지에 중점이 있다. MAC 기법이며, 최초의 수학적 모델이다.
- Brewer-Nash(Chinese Wall) Model : - 여러 회사에 대한 자문서비스를 제공하는 환경에서 기업 분석가에 의해 이해가 충돌되는 회사 간에 정보의 흐름이 일어나지 않도록 접근통제 기능을 제공한다. 직무 분리를 접근통제에 반영한 개념이며, 상업적으로 기밀성 정책의 견해를 받아들였다. 이익 충돌을 회피하기 위해서 사용되고 이해 상충 금지가 필요하다.

문 12. 리눅스 시스템에서 umask값에 따라 새로 생성된 디렉터리의 접근 권한이 'drwxr-xr-x'일 때 기본 접근 권한을 설정하는 umask의 값은? 3

① 002
② 020
③ 022
④ 026

[해설]

umask를 이용한 파일권한 설정
- 새롭게 생성되는 파일이나 디렉터리는 디폴트 권한으로 생성된다. 이러한 디폴트 권한은 umask 값에 의해서 결정되어 진다.
- 파일이나 디렉터리 생성시에 기본 권한을 설정해준다. 각 기본권한에서 umask 값만큼 권한이 제한된다.(디렉터리 기본권한 : 777, 파일 기본권한 : 666)

문 13. (가), (나)에 해당하는 침입차단시스템 동작 방식에 따른 분류를 바르게 연결한 것은? 1

> (가) 각 서비스별로 클라이언트와 서버 사이에 프록시가 존재하며 내부 네트워크와 외부 네트워크가 직접 연결되는 것을 허용하지 않는다.
> (나) 서비스마다 개별 프록시를 둘 필요가 없고 프록시와 연결을 위한 전용 클라이언트 소프트웨어가 필요하다.

	(가)	(나)
①	응용 계층 게이트웨이 (application level gateway)	회선 계층 게이트웨이 (circuit level gateway)
②	응용 계층 게이트웨이 (application level gateway)	상태 검사 (stateful inspection)
③	네트워크 계층 패킷 필터링 (network level packet filtering)	상태 검사 (stateful inspection)
④	네트워크 계층 패킷 필터링 (network level packet filtering)	회선 계층 게이트웨이 (circuit level gateway)

[해설]

- Application Level 방화벽
① 패킷을 응용계층까지 검사해서 패킷을 허용하거나 Drop하는 방식이다.
② 어플리케이션 계층에서 각 서비스별로 프록시가 있어서 Application Level Gateway라고도 한다.
③ 클라이언트는 프록시를 통해서만 데이터를 주고 받을 수 있으며 프록시는 클라이언트가 실제서버와 직접 연결하는 것을 방지한다.

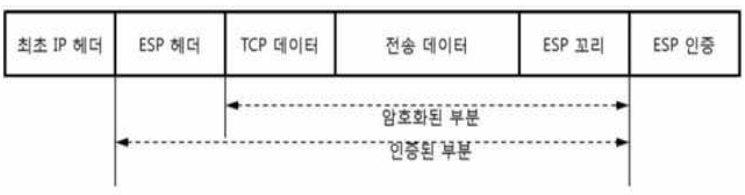
- 회로레벨 프록시(서킷게이트웨이(Circuit Gateway)) 방화벽
① OSI 모델의 세션층에서 작동하는 방화벽이다.
② 각 서비스별로 프록시가 존재하는 어플리케이션 방식과 달리 어느 어플리케이션도 사용할 수 있는 프록시를 사용한다.
③ 대표적으로 SOCKS(Socket Secure)가 있다.

문 14. IPSec에 대한 설명으로 옳지 않은 것은? 3

① AH는 인증 기능을 제공한다.
② ESP는 암호화 기능을 제공한다.
③ 전송 모드는 IP 헤더를 포함한 전체 IP 패킷을 보호한다.
④ IKE는 Diffie-Hellman 키 교환 알고리즘을 기반으로 한다.

[해설]

- ESP의 전송모드



문 15. 보안 공격에 대한 설명으로 옳지 않은 것은? 4

① Land 공격은 패킷을 전송할 때 출발지와 목적지 IP를 동일하게 만들어서 공격 대상에게 전송한다.

② UDP Flooding 공격은 다수의 UDP 패킷을 전송하여 공격 대상 시스템을 마비시킨다.

③ ICMP Flooding 공격은 ICMP 프로토콜의 echo 패킷에 대한 응답인 reply 패킷의 폭주를 통해 공격 대상 시스템을 마비시킨다.

④ Teardrop 공격은 공격자가 자신이 전송하는 패킷을 다른 호스트의 IP 주소로 변조하여 수신자의 패킷 조립을 방해한다.

[해설]

TearDrop 공격
- TearDrop은 IP패킷 전송이 잘게 나누어졌다가 다시 재조합하는 과정의 약점을 악용한 공격이다. 보통 IP패킷은 하나의 큰 자료를 잘게 나누어서 보내게 되는데, 이때 offset을 이용하여 나누었다 도착지에서 offset을 이용하여 재조합하게 된다. 이때 동일한 offset을 겹치게 만들면 시스템은 교착되거나 충돌을 일으키거나 재시동 되기도 한다.
- 시스템의 패킷 재전송과 재조합에 과부하가 걸리도록 시퀀스 넘버를 속인다.

문 16. 다음은 「지능정보화 기본법」 제6조(지능정보사회 종합계획의 수립)의 일부이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은? 1

> 제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 "종합계획"이라 한다)을 [(가)] 단위로 수립하여야 한다.
>
> ② 종합계획은 [(나)]이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

(가)	(나)
① 3년	과학기술정보통신부장관
② 3년	행정안전부장관
③ 5년	과학기술정보통신부장관
④ 5년	행정안전부장관

[해설]

- 지능정보화 기본법 제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 "종합계획"이라 한다)을 3년 단위로 수립하여야 한다.
② 종합계획은 과학기술정보통신부장관이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

문 17. 「개인정보 영향평가에 관한 고시」상 용어의 정의로 옳지 않은 것은? 2

① "대상시스템"이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.

② "대상기관"이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관 및 민간기관을 말한다.

③ "개인정보 영향평가 관련 분야 수행실적"이란 「개인정보 보호법 시행령」 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

④ "개인정보 영향평가"란 「개인정보 보호법」 제33조제1항에 따라 공공기관의 장이 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

[해설]

- 개인정보 영향평가에 관한 고시 제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음과 각 호와 같다.
1. "개인정보 영향평가(이하 "영향평가"라 한다)"란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.
3. "개인정보 영향평가기관(이하 "평가기관"이라 한다)"이란 영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보 보호위원회(이하 "보호위원회"라 한다)가 지정한 기관을 말한다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
5. "개인정보 영향평가 관련 분야 수행실적(이하 "영향평가 관련 분야 수행실적"이라 한다)"이란 영 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

문 18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의4(본인확인업무의 정지 및 지정취소)상 본인확인업무에 대해 전부 또는 일부의 정지를 명하거나 본인확인기관 지정을 취소할 수 있는 사유에 해당하지 않는 것은? 4

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3 제4항에 따른 지정기준에 적합하지 아니하게 된 경우

② 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우

③ 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우

④ 지정받은 날부터 3개월 이내에 본인확인업무를 개시하지 아니하거나 3개월 이상 계속하여 본인확인업무를 휴지한 경우

[해설]

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4(본인확인업무의 정지 및 지정취소) ① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

문 19. 메일 보안 기술에 대한 설명으로 옳지 않은 것은? 1

① PGP는 중앙 집중화된 키 인증 방식이고, PEM은 분산화된 키 인증 방식이다.

② PGP를 이용하면 수신자가 이메일을 받고서도 받지 않았다고 발뺌할 수 없다.

③ PGP는 인터넷으로 전송하는 이메일을 암호화 또는 복호화하여 제3자가 알아볼 수 없게 하는 보안 프로그램이다.

④ PEM에는 메시지를 암호화하여 통신 내용을 보호하는 기능, 메시지 위·변조, 검증 및 메시지 작성자를 인증하는 보안 기능이 있다.

[해설]

- PEM은 중앙 집중화된 키 인증 방식이고, PGP는 분산화된 키 인증 방식이다.

문 20. (가)~(다)에 해당하는 트리형 공개키 기반 구조의 구성 기관을 바르게 연결한 것은? (단, PAA는 Policy Approval Authorities, RA는 Registration Authority, PCA는 Policy Certification Authorities를 의미한다) 2

(가) PKI에 대한 정책을 결정하고 하위 기관의 정책을 승인하는 기관
(나) Root CA 인증서를 발급하고 CA가 준수해야 할 기본 정책을 수립하는 기관
(다) CA를 대신하여 PKI 인증 요청을 확인하고, CA 간 인터페이스를 제공하는 기관

	(가)	(나)	(다)
①	PAA	RA	PCA
②	PAA	PCA	RA
③	PCA	RA	PAA
④	PCA	PAA	RA

[해설]

PKI의 구성요소 : PAA, PCA, CA, RA, Directory, User

① PAA(Policy Approving Authority; 정책 승인 기관)
- PKI 전반에 사용되는 정책과 절차를 생성 수립하고, PKI 내/외에서의 상호 인증을 위한 정책을 수립하고 승인한다.
- 하위 기관들의 정책 준수 상태 및 적정성을 감사하고, 하위 기관의 공개키를 인증한다.

② PCA (Policy Certification Authority; 정책 인증 기관)
- 도메인 내의 사용자와 인증기관이 따라야 할 정책을 수립하고, 인증기관의 공개키를 인증한다.
- 인증서, 인증서 취소목록 등을 관리한다.

③ CA(Cerification Authority; 인증 기관)
- RA의 요청에 의해 사용자의 공개키 인증서를 발행/취소/폐기, 상호 인증서를 발행한다.
- 인증서, 소유자의 데이터베이스를 관리한다.

④ RA (Registration Authority; 등록 대행 기관)
- 인증서 등록 및 사용자 신원 확인을 대행한다.
- 인증 기관에 인증서 발행을 요청한다.

⑤ Directory
- 인증서와 사용자 관련 정보, 상호 인증서 쌍, CRL 등을 저장하고, 검색하는 장소이다.
- 주로 LDAP를 이용하여 X.500 디렉토리 서비스를 제공한다.

⑥ 사용자(PKI Client)
- 인증서를 신청하고 인증서를 사용하는 주체이다.
- 인증서의 저장, 관리 및 암호화/복호화 기능을 함께 가지고 있다.