20.

코드 보안과 관련된 설명으로 옳지 않은 것은?

① 버퍼 오버플로우 공격은 데이터 길이에 대한 불명확한 정의를 이용한 공격이다.
② gets()는 버퍼 오버플로우 공격에 취약하지 않은 함수이다.
③ 포맷 스트링 공격은 데이터 형태에 대한 불명확한 정의로 발생한다.
④ 버퍼 오버플로우 공격 방어 방법으로는 공격에 취약한 함수를 사용하지 않거나 최신 운영체제를 사용하는 것 등이 있다.

◦ 사용 자제를 권장하는 함수들
strcat(), strcpy(), gets(), scanf(), sscanf(), vscanf(), vsscanf(), sprintf(), vsprintf(),gethostbyname()
◦ 사용을 권장하는 함수들
strncat(), strncpy(), fgets(), fscanf(), vfscanf(), snprintf(), vsnprintf()

오답피하기 ② 버퍼오버플로우 공격에서 gets()는 사용 자제가 요구되는 함수이다.

정답 ②

2016년 국가직 9급
네트워크 보안

–2016년 4월 9일 시행

1.

㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

보기
◦ OSI 7계층에서 (㉠)은 물리 계층으로부터 제공되는 물리적 특성을 이용하여 인접한 두 장치 간에 데이터 송수신을 수행한다.
◦ (㉠)은 (㉡)와 (㉢)라는 두 개의 부계층으로 나뉜다.

	㉠	㉡	㉢
①	데이터링크 계층	논리링크제어	오류제어
②	데이터링크 계층	논리링크제어	매체접근제어
③	네트워크 계층	흐름제어	오류제어
④	네트워크 계층	흐름제어	매체접근제어

오답피하기 ② 데이터링크 계층은 논리적 연결제어를 담당하는 LLC(Logical Link Control sub layer, DLC(Data Link Control))와 장비와 장비 간의 물리적인 접속을 담당하는 MAC(Media Access Control)의 두 sub 계층으로 나뉘어진다.

정답 ②

2.

㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

보기

- (㉠) 기법은 이미 알려진 공격 패턴을 근거로 침입을 탐지하는 기법
- (㉡) 기법은 정상적인 활동에 대한 프로파일을 생성하고, 이 프로파일과 확률적으로 비교하여 벗어나는 행위를 탐지하는 기법
- (㉢) IDS(Intrusion Detection System)는 네트워크 상의 모든 패킷을 캡처링한 후 이를 분석하여 침입을 탐지하는 시스템

※ 이상탐지: Anomaly Detection, 오용탐지: Misuse Detection

	㉠	㉡	㉢
①	이상탐지	오용탐지	네트워크 기반
②	이상탐지	오용탐지	호스트 기반
③	오용탐지	이상탐지	네트워크 기반
④	오용탐지	이상탐지	호스트 기반

- 오용 침입탐지는 기존의 침입방법들을 데이터베이스에 저장해 두었다가 사용자 행동 패턴이 기존의 침입 패턴과 일치하거나 유사한 경우에 침입이라 판단한다.
- 비정상적 행위 탐지방법은 시스템과 사용자의 정상적인 행위 패턴을 프로파일로 생성하고 실제 시스템상에서의 행위가 프로파일 범위를 벗어날 경우를 탐지하는 방법이다.
- 네트워크 기반 IDS(Network-based IDS)는 네트워크에서의 패킷 헤더, 데이터 및 트래픽 양, 응용프로그램 로그 등을 분석하여 침입 여부를 판단한다. 즉, 시스템의 감사 자료가 아닌 네트워크를 통해 전송되는 패킷 정보를 수집 분석하여 침입을 탐지하는 시스템이다.

오답피하기 ③ 보기는 각각의 용어에 대한 정의로 반드시 구분하여 정리하여야 한다.

정답 ③

3.

다음에서 설명하는 보안 공격 유형은?

보기

- 먼저 목표를 정하여 사전 조사를 실시한다.
- 조사를 바탕으로 공격 대상 컴퓨터에 악성코드를 감염시킨다.
- 내부 인프라로 서서히 침투하여 몰래 드나들 수 있도록 백도어 및 툴을 설치한다.
- 내부 인프라 접속 권한을 상승시키고 정보를 탈취하기 시작한다.
- 이후 장기간에 걸쳐 내부 인프라를 장악한 후, 더 많은 정보를 유출하거나 시스템을 파괴하는 등 또 다른 보안사고를 유발한다.

① 루트킷(Rootkit) 공격
② 랜섬웨어(Ransomware) 공격
③ 지능적 지속 위협(APT) 공격
④ 블루스나프(BlueSnarf) 공격

- 미국에서 발견된 스파이웨어 등의 신종 악성 프로그램. 컴퓨터 사용자의 문서를 볼모로 잡고 돈을 요구한다고 해서 '랜섬(ransom)' 이란 수식어가 붙었다. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레이시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접촉해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하기도 한다.
- 블루스나핑(bluesnarfing)은 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.

오답피하기 ③ 지능형 지속 위협(APT, Advanced Persistent Threats)은 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 정보를 외부로 빼돌리는 형태의 공격들을 총칭하는 말이다. 공격 방법은 내부자에게 악성코드가 포함된 이메일을 오랜 기간 동안 꾸준히 발송해 한번이라도 클릭되길 기다리는 형태나, 스턱스넷(Stuxnet)과 같이 악성코드가 담긴 이동식디스크(USB) 등으로 전파하는 형태, 악성코드에 감염된 P2P 사이트에 접속하면 악성코드에 감염되는 형태 등이다. APT를 효과적으로 방어하기 위해서는 기업 내 모든 파일에 대한 가시성을 확보하고, 파일을 실시간으로 행위분석을 실시해야 한다.

정답 ③

4.

다음에서 설명하는 네트워크는?

보기

- 일반적으로 안전하지 않은 공용 네트워크를 이용하여 사설 네트워크를 구성하는 기술로서, 전용선을 이용한 사설 네트워크에 비해 저렴한 비용으로 안전한 망을 구성할 수 있다.
- 공용 네트워크로 전달되는 트래픽은 암호화 및 메시지 인증 코드 등을 사용하여 기밀성과 무결성을 제공한다.

① LAN(Local Area Network)
② WAN(Wide Area Network)
③ MAN(Metropolitan Area Network)
④ VPN(Virtual Private Network)

오답피하기 ④ VPN은 공중 네트워크를 이용하여 사설 네트워크가 요구하는 서비스를 제공할 수 있도록 네트워크를 구성한 것이기 때문에 가상 사설 네트워크라고 한다. 즉, 인터넷과 같은 공중 네트워크를 마치 전용회선처럼 사용할 수 있게 해주는 기술 혹은 네트워크를 통칭한다. 공중망을 경유하여 데이터가 전송되더라도 외부인으로부터 안전하게 보호되도록 주소 및 라우터 체계의 비공개, 데이터 암호화, 사용자 인증 및 사용자 액세스 권한 제한 등의 기능을 제공한다.

정답 ④

5.

다음의 실행 결과를 제시하는 명령어는?

보기

```
프로토콜  로컬 주소          외부 주소          상태
TCP 111.111.111.111:49217 222.222.222.221:ms-sql-s ESTABLISHED
                    (중략)
TCP 111.111.111.111:49216 222.222.222.222:ftp TIME_WAIT
```

① nslookup
② route
③ tracert
④ netstat

◦ netstat 명령은 UNIX 시스템의 TCP/IP 프로토콜 진단 시 다양한 용도로 사용한다. 네트워크 인터페이스(LAN 카드)에 대한 성능 정보, 시스템의 라우팅 정보, 소켓 사용 정보 등 지정 옵션에 따라서 네트워크 정보를 제공한다.
◦ nslookup 명령어는 특정 도메인명에 대한 IP 주소를 조회할 때 사용하는 명령어이다.
◦ traceroute(tracert)는 목적지까지의 데이터 도달여부를 확인하는 도구이다.

오답피하기 ④ netstat 명령에서 옵션을 지정하지 않으면 UNIX 시스템에 생성된 네트워크의 연결정보를 출력한다. 여기서 연결정보란 응용 프로그램이 데이터를 송수신하기 위하여 상대 응용 프로그램과 사용한 프로토콜과 소켓에 대한 정보이다.

정답 ④

6.

패킷 필터 방화벽이 네트워크 계층에서 검사할 수 없는 정보는?

① TCP 연결 상태
② 송수신지 IP주소
③ 송수신지 포트 번호
④ TCP 플래그 비트

◦ 패킷필터링은 방화벽의 가장 기본적인 형태의 기능을 수행하는 방식이다. 패킷필터링은 설정된 규칙에 의해 패킷의 통과여부를 결정하는 것으로 외부 침입에 대한 1차적 방어수단으로 활용된다. 패킷필터링 방식의 방화벽은 OSI 모델에서 네트워크계층(IP 프로토콜)과 전송층(TCP 프로토콜)에서 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스에 port 번호, TCP Sync 비트를 이용한 접속제어를 한다.

오답피하기 ① TCP 연결에 관한 정보를 기록하는 것은 스테이트풀 패킷 검사 침입차단시스템(상태기반 검사 방화벽, stateful packet inspection firewall)의 특징이다.

정답 ①

7.

무선랜의 보안을 강화하기 위한 대책으로 안전하지 않은 것은?

① 무선랜 AP 접속 시 데이터 암호화와 사용자 인증 기능을 제공하도록 설정한다.
② 무선랜 AP에 지향성 안테나를 사용한다.
③ 무선랜 AP에 MAC 주소를 필터링하여 등록된 MAC 주소만 허용하는 정책을 설정한다.
④ 무선랜 AP의 이름인 SSID를 브로드캐스팅하도록 설정한다.

◦ 무선 AP는 기존 유선랜의 가장 마지막에 위치하여 무선 단말기의 무선랜 접속에 관여한다. 무선 AP는 무선랜의 보안에도 많은 비중을 차지하는 중요한 장비로서, 무선 단말기의 접속에 필요한 관련 설정 값을 갖는다. 무선 AP의 서비스 범위는 무선AP가 지원하는 무선 표준에 따라 달라지며, 사용된 무선 표준에 따라 사용할 수 있는 무선랜의 인증방식과 무선 전송 데이터 암호화 방식을 설정할 수 있다.
◦ 무선랜 안테나는 무선 전파를 더 멀리 송수신하기 위해서 사용한다. 무선랜 안테나를 사용하면, 무선랜 전파를 더 멀리까지 전송할 수 있으나 늘어난 전파 전송범위 안에서 무선랜 데이터에 대한 도청과 감청의 위험이 더 높아질 수 있는 단점이 있으므로 지향성 안테나를 사용하는 것이 좋다.

오답피하기 ④ 무선랜 AP의 이름인 SSID를 브로드캐스팅하도록 설정하지 말고, 숨김으로 설정하고 폐쇄시스템을 운영하면, SSID를 모르는 사용자의 접속 시도가 현저하게 줄어든다.

정답 ④

8.

IPSec 프로토콜의 인증 헤더(AH)와 보안 페이로드 캡슐화(ESP)에서 제공하는 보안서비스 중 ESP에서만 제공하는 보안서비스는?

① 재전송 공격 방지(Replay Attack Protection)
② 메시지 기밀성(Confidentiality)
③ 메시지 무결성(Integrity)
④ 개체 인증(Entity Authentication)

오답피하기 ② AH 프로토콜은 발신지 인증과 데이터 무결성을 제공하며, ESP는 발신지 인증, 데이터 무결성 외에 프라이버시(암호화) 기능까지 제공한다.

정답 ②

9.

NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

① 한정된 공인 IP주소 부족 문제의 해결이 가능하다.
② 공인 IP와 NAT IP의 매핑이 1 : 1만 가능하다.
③ 주소 변환 기능을 제공한다.
④ 내부 시스템에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.

〈NAT(Network Address Translation)〉
◦ 라우터에 의해 적은 숫자의 유효 IP 주소만으로도 많은 시스템들이 인터넷에 접속할 수 있게 하는 네트워크 서비스이다.
◦ NAT에서 내부 네트워크와 외부 네트워크는 자연스럽게 두 개의 네트워크로 분리된다.
◦ 외부에서 내부 네트워크로 직접적인 접근이 불가능하게 되므로 네트워크 보안효과를 가져올 수 있다.

오답피하기 ② NAT는 1:1로 매핑하는 Static NAT외에 Dynamic NAT, PAT 등이 있다.

정답 ②

10.

SSL(Secure Socket Layer)의 레코드 프로토콜에서 응용 메시지를 처리하는 동작 순서를 바르게 나열한 것은?

※ MAC : Message Authentication Code

① 압축→단편화→암호화→MAC 첨부→SSL 레코드 헤더 붙이기
② 압축→단편화→MAC 첨부→암호화→SSL 레코드 헤더 붙이기
③ 단편화→MAC 첨부→압축→암호화→SSL 레코드 헤더 붙이기
④ 단편화→압축→MAC 첨부→암호화→SSL 레코드 헤더 붙이기

〈Record 프로토콜 처리절차〉

◦ 메시지를 여러 개의 짧은 단편(fragment)으로 분할하고 단편 단위로 압축을 행한다. 압축에 사용하는 알고리즘은 상대와 합의한 것을 이용한다.

◦ 압축한 단편에 메시지 인증코드를 부가한다. 이것은 무결성을 확보하고 데이터의 인증을 수행하기 위한 것이다. 메시지 인증코드의 MAC 값을 부가하는 것으로 전송 도중에 조작된 것을 검출할 수 있다.

◦ 재전송 공격을 막기 위해 단편에 붙여진 번호를 포함해서 메시지 인증코드를 계산한다. 일방향 해시함수 알고리즘과 메시지 인증코드에서 사용하는 키는 상대와 합의한 것을 이용한다.

◦ 다음으로 압축한 단편과 메시지 인증코드를 합치고 그것을 대칭키 암호로 암호화한다. 암호화에는 CBC 모드를 이용한다.

◦ CBC 모드의 초기화 벡터(IV)는 마스터 비밀로부터 생성하고 대칭키 암호 알고리즘과 공통키는 상대와 합의한 것을 이용한다.

◦ 마지막으로 「데이터 타입, 버전 번호, 압축한 길이로 이루어진 헤더」를 부가한 것이 송신 데이터가 된다.

오답피하기 ④ Record(레코드) 프로토콜은 상위계층(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용 계층)에서 오는 메시지를 단편화, 압축, MAC 첨부, 암호화, 헤더 추가 후에 전송계층에 전달한다.

정답 ④

11.

㉠과 ㉡에 들어갈 용어를 바르게 연결한 것은?

보기

◦ (㉠)는(은) 네트워크 중간에서 상대방의 패킷 정보를 도청하는 수동적 공격이다.

◦ (㉠) 공격의 대응 방안으로 텔넷의 경우 원격 접속 시 평문 패킷의 암호화를 지원하기 위해 (㉡)를(을) 사용한다.

	㉠	㉡
①	ARP watch	SSH
②	ARP watch	PGP
③	Sniffing	SSH
④	Sniffing	PGP

◦ ARP watch : 초기에 MAC 주소와 IP 주소의 매칭 값을 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.

오답피하기 ③ 스니핑은 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하여 네트워크 트래픽을 도청(eavesdropping)하는 과정을 스니핑이라고 할 수 있다. SSH는 TELNET과 같이 TCP를 하부 전송 프로토콜로 사용하나 더 안전하고 TELNET 보다 더 많은 서비스를 제공한다. 네트워크상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 응용 프로그램 또는 프로토콜을 가리킨다.

정답 ③

12.

정보보호 시스템들의 로그를 수집하여 분석 및 모니터링을 통해 전사적 차원의 정보시스템 보안성을 향상시키고 안전성을 높이는 시스템은?

① ESM(Enterprise Security Management)

② NAC(Network Access Control)

③ MAM(Mobile Application Management)

④ MDM(Mobile Device Management)

◦ MDM(Mobile Device Management) : 모바일 컴퓨팅 기기 혹은 통신 플랫폼의 관리 정책 및 기기 환경 설정 등을 위한 도구이다. 기기 원격 제어, 보안 이벤트 모니터링, 기기 환경 설정, 사용자 인증, 소프트웨어 업데이트, 버전 관리, 모니터링, 자산 정보 관리 등의 다양한 기능을 포함한다.

오답피하기 ① ESM은 기업과 기관의 보안 정책을 반영하고 다양한 보안 시스템을 관제·운영·관리함으로써 조직의 보안 목적을 효율적으로 실현하는 시스템이다. 각종 네트워크 보안제품의 인터페이스를 표준화하여 중앙 통합 관리, 침입 종합대응, 통합 모니터링이 가능한 지능형 보안 관리 시스템이다.

정답 ①

13.

방화벽의 구축 형태 중 베스천 호스트 방식에 대한 설명으로 옳지 않은 것은?

① 외부와 내부 네트워크를 연결해주는 역할을 수행한다.
② 외부에서 내부 네트워크로 접속할 때 원하지 않는 접근은 차단할 수 없다.
③ 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.
④ 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

오답피하기 ② 배스천 호스트(Bastion Host)는 침입차단 S/W가 설치되어 내·외부 네트워크 사이에서 게이트웨이 역할을 수행하며 철저한 보안 방어기능이 구축되어 있는 컴퓨터시스템으로 외부에서 내부 네트워크로 접속할 때 원하지 않는 접근을 차단할 수 있다.

정답 ②

14.

〈보기 1〉의 보안 위협과 〈보기 2〉의 그에 대한 설명을 바르게 연결한 것은?

보기1

ㄱ. 방해(Interruption)
ㄴ. 가로채기(Interception)
ㄷ. 변조(Modification)

보기2

A. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 수신측과 연결할 수 없도록 하는 행위
B. 송신측과 수신측이 메시지를 주고받는 사이에 제3자가 도청하는 행위
C. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 일부 또는 전부를 변경하여 수신측에 전송하는 행위

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

◦ 가로채기(interception) : 비인가된 당사자가 자산으로의 접근을 획득한 것을 의미(불법 복사, 도청 등) → 기밀성에 영향
◦ 가로막음(interruption) : 시스템 자산은 손실되거나, 손에 넣을 수 없거나, 사용 불가능하게 됨(하드웨어 장치의 악의적 파괴, 파일 삭제, 서비스 거부 등) → 가용성에 영향
◦ 변조(modification) : 비인가된 당사자가 접근하여 그 내용을 변경(데이터베이스 특정값 변경, 특정 프로그램 변경 등) → 무결성에 영향
◦ 위조(fabrication) : 비인가된 당사자가 컴퓨팅 시스템상에 불법 객체의 위조 정보를 생성(네트워크 통신에 가짜 거래 정보 만듦 등) → 무결성에 영향

오답피하기 ① 보안위협의 공격유형과 보안서비스는 연관하여 정리하여야 한다.

정답 ①

15.

HTTPS에 대한 설명으로 옳지 않은 것은?

① HTTPS 연결로 명시되면 포트 번호 443번이 사용되어 SSL을 호출한다.
② HTTPS는 웹 브라우저와 웹 서버 간의 안전한 통신을 구현하기 위한 것이다.
③ HTTPS는 HTTP over TLS 표준 문서에 기술되어 있다.
④ HTTPS 사용 시 요청된 문서의 URL은 암호화할 수 없다.

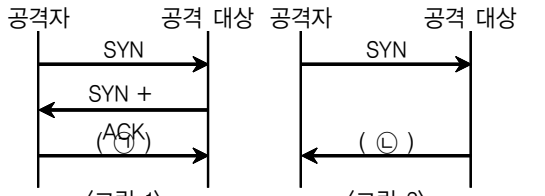
오답피하기 ④ HTTPS를 사용하면 다음과 같은 통신요소가 암호화된다.
◦ 요청 문서 URL
◦ 문서 내용
◦ (브라우저 사용자가 입력한)브라우저 양식 내용
◦ 브라우저가 서버에게 보낸 쿠키와 서버가 브라우저로 보낸 쿠키
◦ HTTP헤더 내용

정답 ④

16.

다음 그림은 TCP half open 스캔 절차이다. ㉠과 ㉡에 들어갈 패킷을 바르게 연결한 것은?

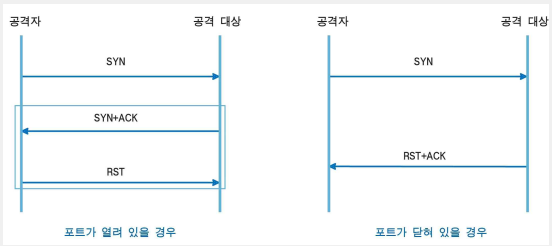
보기



※ 〈그림 1〉은 공격 대상 서버의 포트가 열린 경우이고, 〈그림 2〉는 공격 대상 서버의 포트가 닫힌 경우임.

	㉠	㉡
①	ACK	ACK
②	ACK	RST
③	RST	RST+ACK
④	RST	SYN+ACK

〈TCP half open 스캔〉



오답피하기 ③ TCP Half Open Scan은 세션에 대한 로그가 남는 TCP Full Open 스캔의 단점을 보완하기 위해 나온 기법으로 로그를 남기지 않아 추적이 불가능하도록 하는 기법이다. TCP Half Open 스캔은 TCP Full Open 스캔과 달리 세션을 완전히 연결하지 않고, TCP Half Connection만으로 포트의 활성화 여부를 판단한다. 즉, 먼저 공격자가 SYN 패킷을 공격대상 서버에 보낸 후 포트가 열려있는 서버로부터 SYN/ACK 패킷을 받으면 공격자는 즉시 RST 패킷을 보내 연결을 끊음으로써 연결 시도 세션에 대한 로그를 남기지 않도록 한다.

정답 ③

17.

네트워크 보안 공격에 대한 설명으로 옳은 것은?

① Smurf 공격은 공격대상의 IP주소로 위장된 다량의 ICMP echo reply 패킷을 전송하여 서비스를 거부하는 공격이다.

② MITM 공격은 네트워크에 에러 메시지를 전송하거나 네트워크 흐름을 통제하는 공격이다.

③ Salami 공격은 위조된 ARP reply 패킷을 전송하여 서비스를 거부하는 공격이다.

④ Teardrop 공격은 출발지와 목적지의 IP주소가 동일하게 위조된 SYN 패킷을 전송하는 공격이다.

◦ 살라미 공격 : 많은 사람들로부터 눈치 채지 못할 정도의 적은 금액을 빼내는 컴퓨터 사기수법의 하나이다. 이탈리아 음식 살라미 소시지를 조금씩 얇게 썰어 먹는 모습을 연상시킨다고 해서 붙은 이름이다.

◦ 스머프 공격은 공격대상의 주소로 소스 IP 주소를 만들고 임의의 브로드캐스트 주소로 ICMP echo 패킷을 전송하여 스푸핑 된 IP 호스트는 ICMP reply 패킷을 동시 다발적으로 수신하여 시스템 부하를 증가시킨다.

오답피하기 ① 위조된 ARP reply 패킷을 전송하여 서비스를 거부하는 공격은 ARP Spoofing 공격에 대한 설명이고, 출발지와 목적지의 IP주소가 동일하게 위조된 SYN 패킷을 전송하는 공격은 Land Attack에 대한 설명이다.

정답 ①

18.

ARP Spoofing 공격에 대응하기 위한 명령어로 옳은 것은?

① arp -a IP주소 MAC주소

② arp -d IP주소 MAC주소

③ arp -s IP주소 MAC주소

④ arp -v IP주소 MAC주소

◦ ARP 스푸핑 공격의 대응책 중 static 옵션의 지정은 중요 시스템의 보안에 중요한 역할을 한다. 그러나 관리하는 모든 시스템에 이런 작업을 할 수는 없다. 또한, 리부팅하면 static 옵션이 사라지므로 계속 사용하려면 배치 파일 형태로 만들어두고 리부팅 시마다 자동으로 수

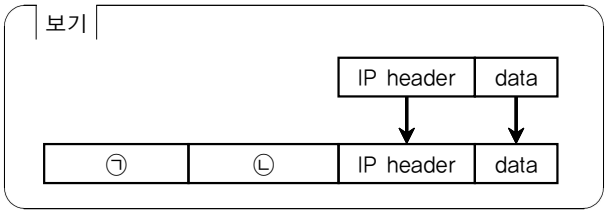
행되도록 설정해야 한다.

오답피하기 ③ tatic 옵션 지정은 arp –s 〈IP 주소〉 〈MAC 주소〉 형식으로 명령을 입력한다.

정답 ③

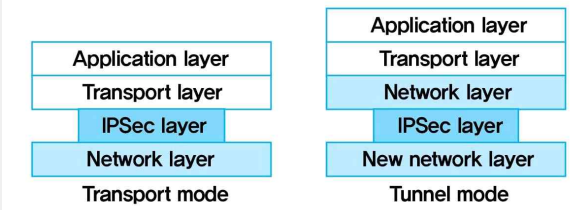
19.

다음은 IPSec 터널모드에서 IP 패킷을 암호화하고 인증 기능을 수행하는 그림이다. ㉠과 ㉡에 추가되는 헤더 정보를 바르게 연결한 것은?



	㉠	㉡
①	new IP header	ESP/AH
②	ESP/AH	new IP header
③	IKE header	new IP header
④	new IP header	IKE header

〈전송 모드 대 터널 모드〉



오답피하기 ① 전송모드는 (IP헤더, AH헤더, 페이로드), 터널모드는 (New IP헤더, AH헤더, IP헤더, 페이로드) 패킷의 모양을 갖는다.

정답 ①

20.

OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 옳지 않은 것은?

① 네트워크 계층–IPsec
② 응용 계층–SSH
③ 데이터링크 계층–TLS
④ 전송 계층–SSL

오답피하기 ③ SSL은 TCP/IP 프로토콜의 전송 계층(Transport Layer)에서 보안 기능을 수행하며 전송 계층과 응용 계층(Application Layer) 사이에 위치하며 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜이다.

정답 ③