1과목 : 과목 구분 없음

1. 네트워크 명령어에 대한 설명으로 옳지 않은 것은?
   ① hostname: 컴퓨터 이름을 확인한다.
   ② nslookup: DNS를 통해 도메인 이름을 검색한다.
   ③ ipconfig: 인터페이스에 설정된 라우팅 테이블을 검색한다.
   ④ ping: 컴퓨터의 네트워크 상태를 점검한다.

2. 다음에서 설명하는 네트워크 도구는?

> ○ IP 헤더에 있는 TTL의 특성을 이용한다.
> ○ TTL 값은 IP 패킷이 전송될 수 있는 최대 hop 수이다.
> ○ 최종 목적지까지의 라우터에 대한 경로 및 응답 속도를 표시해 준다.
> ○ 특정 사이트와의 접속이 느릴 경우 네트워크의 어느 구간에서 느린지 확인할 수 있다.

   ① wireshark ② tcpdump
   ③ traceroute ④ netstat

3. 비대칭키 암호화 알고리즘에서 수신자의 공개키로 데이터를 암호화하여 전송할 때 얻을 수 있는 보안성은?
   ① 가용성 ② 인증
   ③ 부인방지 ④ 기밀성

4. TCP 포트의 개방 여부를 확인하기 위한 스텔스 스캔으로 옳지 않은 것은?
   ① FIN 스캔 ② NULL 스캔
   ③ XMAS 스캔 ④ TCP Open 스캔

5. 스위치 재밍(switch jamming)에 대한 설명으로 옳은 것은?
   ① 스위치 MAC 테이블의 저장 용량을 넘으면 더미 허브(dummy hub)처럼 브로드캐스트(broadcast) 한다.
   ② 방어대책은 게이트웨이 MAC 주소를 동적으로 설정한다.
   ③ 공격자는 클라이언트가 DNS 서버로 전송하는 DNS Query 패킷을 중간에 가로챈다.
   ④ MAC flooding은 스위치에 이상이 있을 때 자동으로 모든 보안 기능을 차단하는 것이다.

6. 윈도시스템에서 다음과 같이 이더넷 인터페이스의 송수신 패킷 정보를 얻기 위한 netstat 명령어의 옵션은?

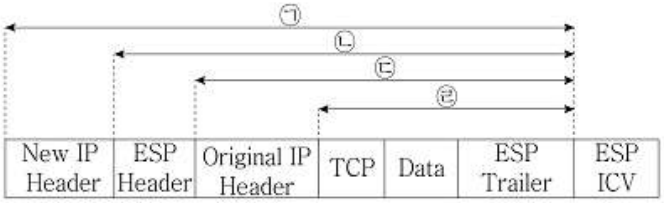
인터페이스 통계

	받음	보냄
바이트	3879974308	172124956
유니캐스트 패킷	1098604	985784
비유니캐스트 패킷	11306144	94056
버림	0	0
오류	0	0
알 수 없는 프로토콜	0	

   ① netstat -an ② netstat -e
   ③ netstat -r ④ netstat -s

7. SSL 프로토콜에 대한 설명으로 옳은 것은?
   ① ChangeCipherSpec 프로토콜은 오류와 비정상 상태를 알기 위해 사용한다.
   ② Handshake 프로토콜은 대기와 활성 상태 사이에서 이동되는 값들의 처리 과정을 규정한다.
   ③ Record 프로토콜은 기밀성과 메시지 무결성을 제공한다.
   ④ Alert 프로토콜은 암호 그룹 협의와 클라이언트와 서버 간 인증 정보를 교환하기 위해 사용한다.

8. IPSec의 ESP 터널 모드에서 암호화 범위로 옳은 것은?



   ① ㉠ ② ㉡
   ③ ㉢ ④ ㉣

9. TLS에 대한 설명으로 옳지 않은 것은?
   ① TLS는 SSL을 기반으로 만들어진 인터넷 표준이다.
   ② TLS의 의사난수 함수(pseudorandom function)는 데이터 확장 함수(data-expansion function)를 활용한다.
   ③ TLS의 의사난수 함수는 비밀(secret), 식별용 라벨(label), 종자(seed)를 입력받는다.
   ④ TLS의 마스터 비밀(master secret) 생성을 위해 데이터 확장 함수는 사전 마스터 비밀(pre-master secret), 'master secret' 문자, 2개의 임의의 수를 입력받는다.

10. 부채널 공격(side channel attack)에 대한 설명으로 옳은 것은?
   ① 하드웨어적인 공격 기법이며, 전력분석, 시차분석, 전자파분석 등의 공격이 있다.
   ② 은닉 채널을 이용해 암호화 알고리즘이나 시스템 동작에서 발생하는 다양한 누수 정보를 획득한다.
   ③ 역어셈블러, 디버거를 이용해 소프트웨어의 오류 및 결함을 찾아 악용하는 공격이다.
   ④ 숨겨진 메시지를 사진이나 동영상 속에 부호화하는 스테가노그래피는 부채널 공격에 대응하기 위해 개발되었다.

11. 디지털 포렌식(digital forensic)에서 '증거가 위조되거나 변조되지 않았다'는 것을 증명하는 원칙은?
   ① 무결성 ② 신속성
   ③ 재현성 ④ 정당성

12. 대칭키 암호화 알고리즘으로 옳지 않은 것은?
   ① ARIA ② SEED
   ③ DES ④ ECC

13. 네트워크 서비스의 기본 포트 번호로 옳지 않은 것은?
   ① SMTP(Simple Message Transfer Protocol):25
   ② DNS(Domain Name Service):53

③ RPC(Remote Procedure Call):111
④ SNMP(Simple Network Management Protocol):143

14. 침입탐지시스템(intrusion detection system)에 대한 설명으로 옳지 않은 것은?
① 침입탐지 유형에는 비정상행위 탐지(anomaly detection)와 오용 탐지(misuse detection) 등으로 구분된다.
② 비정상행위 탐지는 알려지지 않은 공격을 탐지하기에 효과적이지만 False Positive가 높아질 수 있다.
③ 오용 탐지는 알려진 공격 패턴을 기반으로 공격을 탐지하므로 알려지지 않은 공격 탐지에는 효과적이지 못하다.
④ 전문가 시스템 모델은 비정상행위 탐지에 널리 사용되는 기법이다.

15. 다음에서 설명하는 서비스 거부(denial of service) 공격은?

○ ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용해 패킷을 확장함으로써 서비스 거부 공격 수행
○ 다이렉트 브로드캐스트(direct broadcast) 악용

① 티어드롭 공격(teardrop attack)
② 스머프 공격(smurf attack)
③ 죽음의 핑 공격(ping of death attack)
④ SYN 플러딩 공격(SYN flooding attack)

16. 공격자가 TCP 세션 하이재킹(session hijacking)을 위해 대상 호스트에 첫 번째로 보내는 TCP 패킷 플래그(flag)는?
① RST ② FIN
③ ACK ④ SYN

17. ICMP에 대한 설명으로 옳은 것은?
① 전송 계층에서의 오류 탐지를 위해 사용한다.
② 송신자의 패킷이 목적지에 도달하지 못했을 때 송신자는 ICMP Echo Reply 메시지를 수신한다.
③ TTL이 0이 되면 ICMP 시간초과(time exceeded) 오류 메시지가 발생한다.
④ UDP에 의해 전송된다.

18. IKE 키 결정 알고리즘의 특징에 대한 설명으로 옳지 않은 것은?
① 방해 공격을 방지하기 위해 비표(nonce)를 사용한다.
② 두 당사자가 군(group)을 협상할 수 있다.
③ Diffie-Hellman 공개키 값의 교환이 가능하다.
④ 중간자 공격을 방지하기 위해 Diffie-Hellman 교환을 인증한다.

19. IPSec의 보안 연관(security association)을 식별하기 위한 매개변수로 옳지 않은 것은?
① 보안 매개변수 색인(security parameters index)
② 발신지 IP 주소
③ 수신지 IP 주소
④ 보안 프로토콜 식별자(security protocol identifier)

20. 다음의 설명에서 옳지 않은 것은?
① 스턱스넷(stuxnet): 사용자가 키보드로 입력하는 내용을 몰래 가로채어 기록한다.
② 랜섬웨어(ransomware): 시스템의 폴더 또는 파일 등을 암호화하여 금전을 요구한다.
③ 트로이 목마(trojan horse): 겉으로는 정상적인 프로그램으로 보이지만 악성코드가 숨겨져 있다.
④ 스파이웨어(spyware): 사용자 정보를 무단으로 수집하여 동의 없이 다른 곳으로 보낸다.

1	2	3	4	5	6	7	8	9	10
③	③	④	④	①	②	③	③	④	①
11	12	13	14	15	16	17	18	19	20
①	④	④	④	②	①	③	①	②	①