

8. VPN에 관련된 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

— < 보 기 > —

- ㉠ VPN 연결로 원격지 노드를 LAN으로 묶을 수 있다.
- ㉡ VPN의 보안 기밀 수준은 선택한 암호화 알고리즘에 따라 결정된다.
- ㉢ PPTP, L2F, L2TP는 2계층 수준, IPSec, SOCKS v5 프로토콜은 5계층 수준에서 연결성을 제공한다.
- ㉣ IPSec의 전송모드의 패킷은 터널모드 패킷에 비하여 상대적으로 더 큰 크기가 된다.

- ① ㉠, ㉡ ② ㉡, ㉣
- ③ ㉢, ㉣ ④ ㉠, ㉣

9. 다음 보안 장비에 관련한 <보기> 중 가장 옳은 내용으로 선택된 것은?

— < 보 기 > —

- ㉠ 방화벽(Firewall)은 내부의 컴퓨터가 트로이 목마 등 침입에 감염되었을 때 보안성이 급격히 하락한다.
- ㉡ 배스천 호스트(Bastion Host)는 내부 네트워크와 인터넷 간 연결되는 유일한 경로이므로 외부에서 내부로 전송되는 모든 패킷은 이 호스트를 경유하여야만 한다.
- ㉢ NAT를 이용하면 외부 네트워크로부터 내부 네트워크상 기기에 대한 직접 액세스가 제한되도록 구성할 수 있다.

- ① ㉠, ㉡ ② ㉡, ㉣
- ③ ㉠, ㉣ ④ ㉠, ㉡, ㉣

10. 다음 <보기> 에서 설명하는 보안 기술은?

— < 보 기 > —

- 빅데이터의 방대한 정보 속에서 단순한 로그 수집 및 분석이 아닌, 사후에 추적이 가능하도록 상관분석과 포렌식 기능을 제공하는 등 지능적 위협에 대한 조기 경고 모니터링 체계

- ① TMS(Threat Management System)
- ② SIEM(Security Information Event Management)
- ③ SOAR(Security Orchestration Automation and Response)
- ④ NGFW(Next Generation Firewall)

11. 다음 <보기>에서 포렌식의 원칙에 관련한 서술로 가장 옳게 짝지어진 것은?

— < 보 기 > —

- ㉠ 재현의 원칙 ㉡ 적절한 절차를 거쳐 획득한 것만이 증거력을 가짐.
- ㉢ 무결성의 원칙 ㉣ 획득 후 이송/분석/보관/법정제출과정이 명확하고 추적 가능해야 함.
- ㉤ 정당성의 원칙 ㉥ 같은 환경에서는 같은 결과가 얻어져야 함.
- ㉦ 연계 보관성의 원칙 ㉧ 수집정보는 연계보관성 및 단계과정에서의 위조, 변조가 일어나지 않아야 함.

- ① ㉠-㉢, ㉡-㉤, ㉣-㉡, ㉥-㉣
- ② ㉠-㉡, ㉢-㉣, ㉤-㉤, ㉥-㉣
- ③ ㉠-㉢, ㉡-㉤, ㉣-㉡, ㉥-㉣
- ④ ㉠-㉡, ㉢-㉤, ㉤-㉡, ㉥-㉣

12. 다음 <보기>에서 공격형태와 이에 관련한 설명으로 가장 옳게 짝지어진 것은?

— < 보 기 > —

- ㉠ Ping of Death ㉡ OpenSSL 패키지 최신버전 업데이트로 보안.
- ㉢ Heartbleed ㉣ 분할된 패킷을 탐지, 공격 여부를 의심, 제거.
- ㉤ Bonk, Boink ㉥ 응용수준의 대응방법으로 방어.
- ㉦ GET Flooding ㉧ TCP 패킷의 순서번호를 조작하는 공격방법.

- ① ㉠-㉡, ㉢-㉤, ㉤-㉡, ㉥-㉣
- ② ㉠-㉢, ㉡-㉤, ㉣-㉡, ㉥-㉣
- ③ ㉠-㉡, ㉢-㉡, ㉤-㉤, ㉥-㉣
- ④ ㉠-㉡, ㉢-㉤, ㉤-㉡, ㉥-㉣

13. ARP(Address Resolution Protocol)에 관한 설명 중 가장 옳지 않은 것은?

- ① ARP 패킷은 데이터링크 프레임에 캡슐화된다.
- ② 호스트의 ARP 테이블을 정적으로 유지하면 ARP 스푸핑(Spoofing) 공격을 막을 수 있다.
- ③ ARP는 MAC 주소에 대응되는 IP 주소를 구할 때 사용되는 프로토콜이다.
- ④ ARP 패킷에는 발신자와 해당 수신자의 물리 주소와 논리주소가 포함된다.

14. 다음 <보기>의 설명에 해당하는 라우팅 프로토콜은 무엇인가?

— < 보 기 > —

- 모든 라우터가 동일한 네트워크 토폴로지 데이터 베이스를 기반으로 경로를 계산한다.
- 거리 벡터가 아닌 링크 상태를 활용하는 자율 시스템 도메인 내의 라우팅 프로토콜이다.

- ① IGRP(Interior Gateway Routing Protocol)
- ② RIP(Routing Information Protocol)
- ③ BGP(Border Gateway Protocol)
- ④ OSPF(Open Shortest Path First)

15. 다음 <보기> 설명에 해당하는 용어를 바르게 나열한 것은?

— < 보 기 > —

- ㉠ 블루투스 공격장치의 검색 활동을 뜻한다.
- ㉡ 블루투스의 취약점을 이용하여 기기의 정보에 접근하는 공격이다.
- ㉢ 블루투스 장비간의 취약한 연결 관리를 악용한 공격이다.
- ㉣ 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼트리는 것이다.

구분	㉠	㉡	㉢	㉣
①	블루재킹	블루스나핑	블루프린팅	블루버깅
②	블루프린팅	블루버깅	블루스나핑	블루재킹
③	블루프린팅	블루스나핑	블루버깅	블루재킹
④	블루재킹	블루버깅	블루프린팅	블루스나핑

16. 다음 중 라우터가 송신 측 노드에 적합하지 않은 경로로 설정되어 있을 경우 해당 노드에 대한 최적화된 경로를 다시 지정해주는 ICMP(Internet Control Message Protocol) 메시지로 가장 옳은 것은?

- ① Time Exceed
- ② Redirection
- ③ Destination Unreachable
- ④ Source Quench

17. SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?

- ① TCP/IP 프로토콜을 사용하는 인터넷에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.
- ② 에이전트는 Trap 메시지를 관리자에 보냄으로써 비정상적인 상황을 경고할 수 있다.
- ③ SMI는 객체의 이름을 붙이고 유형을 정의하며, 부호화하는 등의 일반적인 규칙을 정의한다.
- ④ SMI는 공통된 정보 표현방식을 규정해서 장비간 통신이 이루어질 수 있도록 하며 객체의 유형과 연결에 관여한다.

18. 다음 <보기>는 보안을 위해 필요로 하는 기능 요구 사항에 대하여 제시한 것이다. 괄호 안 내용으로 가장 옳은 것은?

— < 보 기 > —

“우리 원에서 대외 홈페이지를 열기로 했습니다. 그런데 민원인이 인터넷으로 접속할 수 있어야 하니 보안장비를 구입해야 합니다.
사용자 게시판도 구축해야 하고, 민원 게시물도 업로드 할 수 있도록 해야 하니 필요한 장비는 () 입니다.”

- ① 네트워크 방화벽
- ② 게이트웨이
- ③ 웹 방화벽
- ④ 침입탐지 시스템

19. 203.230.15.0과 같은 IPv4의 C클래스 네트워크를 30개의 서브넷으로 나누고, 각각의 서브넷에는 5개의 호스트를 연결하려고 한다. 30개의 서브넷에서 사용되는 서브넷 마스크는?

- ① 255.255.255.192
- ② 255.255.255.248
- ③ 255.255.255.240
- ④ 255.255.255.224

20. 스위치의 MAC Address Table 버퍼를 오버플로우 시켜서 스위치가 허브처럼 동작하게 강제적으로 만드는 기법은?

- ① 스위치 Jamming
- ② ICMP Redirect
- ③ ARP Spoofing
- ④ ARP Redirect