네트워크보안

1. 다음 중 무선 AP(Access Point)에 전송데이터의 암호화 방식이나 인증절차가 설정되지 않은 경우 보안 강화책이 아닌 것은?
   ① WEP(Wired Equivalent Privacy) 설정한다.
   ② WAP2(Wi-Fi Protected Access v2) 설정한다.
   ③ Rogue AP로 대체한다.
   ④ 무선 AP에 SSID값을 'NULL'로 설정한다.

2. 다음 중 무선 LAN보안에 AES 128비트를 사용하여 최상의 암호수준을 제공하는 것은?
   ① WEP(Wired Equivalent Privacy)
   ② EAP(Extensible Authentication Protocol)
   ③ WPA2(Wi-Fi Protected Access v2)
   ④ WPA(Wi-Fi Protected Access)

3. 다음 중 기기 인증기술 중에서 보안수준은 하위수준이지만, 접속이 가장 용이하고, 추가적인 프로토콜이 필요치 않고, 접속지연이 최소인 것은?
   ① ID/PW기반 인증기술
   ② MAC(Media Access Control)주소 인증기술
   ③ Challenge/Response 인증기술
   ④ PKI(Public Key Infrastructure)기반 기기 인증서를 활용한 인증기술

4. 다음은 무선 AP(Access Point)가 태생적으로 보안에 취약하기 때문에 신규로 설치 시 고려할 사항을 나열한 것이다. 틀린 것은?
   ① AP 기본계정의 패스워드를 재설정한다.
   ② 누구나 접근이 가능한 장소에 설치한다.
   ③ DHCP(Dynamic Host Configuration Protocol)에 의한 IP주소 할당을 중지한다.
   ④ AP에 접속이 가능한 무선 랜카드 MAC주소를 기록하여 이를 반영하여 접속을 통제한다.

5. 다음 중 응용계층에서 동작되는 보안프로토콜이 아닌 것은?
   ① S/MIME(Secure/Multipurpose Internet Mail Extensions)
   ② SSH(Secure SHell)
   ③ SSL(Secure Socket Layer)
   ④ S-HTTP(Secure Hyper Text Transper Protocol)

6. VPN(Virtual Private Network)은 인터넷에 보안채널(Secure Channel)을 만들어 공용인터넷을 사설망처럼 사용하는 기술이다. 통신프로토콜 3계층(네트워크계층)에 보안프로토콜을 추가하여 VPN을 구현하는 기술은?
   ① IPSec(Internet Protocol Security)
   ② SSL(Secure Socket Layer)
   ③ DNSsec(DNS Security)
   ④ S-HTTP(Secure Hyper Text Transper Protocol)

7. 다음 중 산재되어 있는 수많은 컴퓨터를 동원하여 동일시간에 특정 컴퓨터에 트래픽 폭탄을 보내어 특정 컴퓨터가 정상적인 작동을 못하게 하는 공격은?
   ① APT(Advanced Persistence Threat) 공격
   ② DOS(Denial Of Service) 공격
   ③ IP Spoofing 공격
   ④ DDOS(Distributed Denial Of Service) 공격

8. 다음 <보기>의 설명과 가장 가장 가까운 장비는?

< 보 기 >

방화벽과 침입탐지시스템의 장점만을 결합하여 실시간 방어체제를 구축한 장비이다. 이 장비는 실시간으로 네트워크 트래픽을 모니터링하여 분석하고 해킹으로 판단되면 패킷이 내부로 유입되는 것을 사전에 차단한다.

   ① DDOS(Distributed Denial Of Services) 보안장비
   ② VPN(Virtual Private Network) 보안장비
   ③ IPS(Intrusion Prevention System) 보안장비
   ④ NAC(Network Access Control) 보안장비

9. 다음 중 방화벽으로 할 수 있는 것은?
   ① 악성코드 침입 차단
   ② 내부자 공격 차단
   ③ 방화벽을 우회하는 트래픽 차단
   ④ 외부자의 내부 네트워크에 대한 접근통제

10. 다음 중 공격 대상시스템의 로그에 흔적을 남기지 않은 포트 스캔 기술은?
    ① ICMP Scan
    ② UDP Scan
    ③ TCP Scan
    ④ Stealth Scan

11. 다음 중 공격자가 공격대상자에게 자신을 노출시키지 않고 제3의 사용자인 것처럼 MAC주소, IP주소, E-Mail 주소, DNS 이름 등을 속여서 공격하는 것을 통칭하여 무엇이라 하는가?
① 스니핑(Sniffing) 공격
② 스푸핑(Spoofing) 공격
③ 하이재킹(Hijacking) 공격
④ 인터셉트(Intercept) 공격

12. 다음 중 조직내 다수의 IT시스템과 보안시스템에서 발생하는 모든 로그들을 실시간으로 수집하여 종합적인 분석을 통해 이상징후를 파악하고 대응을 위해 마련한 장비는?
① SIEM(Security Information Event Management) 장비
② NAC(Network Access Control) 장비
③ MDM(Mobile Device Management) 장비
④ SAC(System Access Control) 장비

13. 리눅스 운영체제가 탑재된 컴퓨터에 랜카드를 설치한 다음, 리눅스운영체제를 통해서 랜카드를 'Promiscuous' 모드로 동작하도록 설정하였다. 설정 결과 랜카드 동작을 가장 잘 설명한 것은?
① 랜카드에 도착된 프레임내의 IP주소와 MAC주소가 랜카드가 장착된 컴퓨터의 IP주소와 MAC주소가 동일한 것만 컴퓨터로 받아들인다.
② 랜카드에 도착된 프레임내의 IP주소와 랜카드가 장착된 컴퓨터의 IP주소가 동일한 것만 컴퓨터로 받아들인다.
③ 랜카드에 도착된 프레임내의 MAC주소와 랜카드가 장착된 컴퓨터의 MAC주소가 동일한 것만 컴퓨터로 받아들인다.
④ 랜카드에 도착한 모든 프레임을 컴퓨터로 받아들인다.

14. 다음 중 사설 네트워크 용도로 사용되는 사설 IPv4 주소에 해당하는 것은?
① 10.10.20.300
② 168.10.40.11
③ 172.16.10.20
④ 192.10.20.30

15. 다음 중 조직내 네트워크에 기기/사용자 인증절차를 통해 네트워크에 접근을 통제하고, 네트워크에 접속되는 기기들의 백신관리 및 패치관리, 자산관리를 점검을 통해 무결성 유무에 따라 네트워크 접속 허용유무를 결정하고, 해킹, 웜 유해트래픽 탐지 및 차단하는 등의 기능을 하는 네트워크 보안장비는?
① SAC(System Access Control) 장비
② AAC(Account Access Control) 장비
③ NAC(Network Access Control) 장비
④ ESM(Enterprise Security Management) 장비

16. 다음 중 이더넷 물리 주소(MAC)가 될 수 있는 것은?
① 00:0C:29:97:13:8C:48:A0
② 00:0C:29:97:13:8C:48
③ 00:0C:29:97:13:8C
④ 00:0C:29:97:13

17. 다음 중 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격 기법은?
① 스위치 재밍
② IP 스푸핑
③ DNS 스푸핑
④ ARP 스푸핑

18. 다음 <보기>의 내용은 DDoS 공격 직후가 발생하였을 경우 긴급 대응 절차를 나열한 것이다. 순서를 올바르게 나열하고 있는 것은?

< 보 기 >

ㄱ. 모니터링
ㄴ. 상세분석
ㄷ. 공격탐지
ㄹ. 초동조치
ㅁ. 차단조치

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

19. 다음 중 침입차단시스템(Firewall)에서 아래와 같이 주소에 의한 패킷 필터링 규칙을 적용 시 필터링 된 패킷의 결과가 가장 올바르지 않은 것은?
(단, 적용순서는 A, B, C 순)

규칙	출발지주소	목적지 주소	동작
A	10.12.99.0/24	165.15.0.0/16	Deny
B	10.12.0.0/8	165.15.6.0/24	Allow
C	any	any	Deny

① 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.
② 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.
③ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.
④ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.

20. 다음 중 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로 TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?

① Ping
② netstat
③ nmap
④ nbstat