네트워크보안

1. 다음에서 설명하고 있는 네트워크 공격은 무엇인가?

> · ICMP의 echo 패킷을 이용하여 reply 패킷의 폭주를 통해 시스템을 마비시킨다.
> · 공격자는 ping의 목표주소를 네트워크 브로드캐스트 주소로 할당하고 자신을 공격할 호스트로 위장한 후 echo 패킷을 전송한다.

① Teardrop 공격
② UDP flooding 공격
③ Smurf 공격
④ ICMP redirection 공격

2. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 적절한 프로그램은 무엇인가?
① ps
② Nmap
③ nslookup
④ traceroute

3. VPN(Virtual Private Network)에 대한 설명으로 가장 옳지 않은 것은?
① 공중망을 사용하여 사설망과 같은 효과를 얻는다.
② 서로 다른 통신 프로토콜을 사용하여 네트워크 사이에서 데이터를 전송한다.
③ RSVP 프로토콜을 사용하여 터널을 만들고 암호화를 수행한다.
④ 터널링 기법은 IPsec, SSL 등의 방법을 사용한다.

4. 컴퓨터의 내부 자료를 탈취하는 수법으로 프로그램 개발 시에 내용을 볼 수 있는 부정루틴을 삽입하여 컴퓨터의 정비나 유지보수를 핑계 삼아 악의적인 행위를 하는 방법은 무엇인가?
① Trap Door
② TRINOO
③ Trojan Horse
④ Teardrop

5. 다음의 설명에 해당되는 시스템은 무엇인가?

> 기업 데이터 유출 방지를 의미하며 사용자가 사무실, 현장 및 집 어느 곳에서 업무 중이라도 사용자의 PC에서 기업 내 기밀 데이터가 외부로 반출되는 것을 항시 감시하고 기록하며, 정책에 따라 유출을 차단시키는 것을 주 기능으로 구현한 솔루션이다.

① DLP ② IDS ③ IDC ④ EIP

6. 다음에서 설명하는 것을 올바르게 짝지은 것은?

> (가)은/는 악의적인 프로그램을 건전한 프로그램처럼 포장하여 일반 사용자들이 의심 없이 자신의 컴퓨터 안에서 이를 실행시키고 실행된 (가)은/는 특정 포트를 열어 공격자의 침입을 돕고 추가적으로 정보를 자동 유출하며 자신의 존재를 숨긴다.
> (나)은/는 OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격 코드 및 프로그램을 의미한다.

① (가) Exploit (나) Trojan
② (가) Trojan (나) Hoax
③ (가) Trojan (나) Exploit
④ (가) Exploit (나) Hoax

7. 다음에서 설명하는 것은 무엇인가?

> 무선네트워크 액세스포인트 이름을 의미하며 각 액세스포인트에 하나씩 할당되어 있다. 기본적으로 AP와 Client는 이것이 일치해야만 통신이 가능하게 되는데 액세스포인트가 자신들의 이것을 브로드캐스팅하기 때문에 보안에 취약할 수밖에 없다.

① SSID ② MAC ③ WEP ④ WPA

8. 이더넷 물리 주소가 될 수 있는 것은 다음 중 어떤 것인가?
① 01:02:01:2C:4B
② 07:01:02:01:2C:4B:2C
③ 07:01:02:01:2C:4B
④ 07:02:01:02:3B:4C:3C:2B

9. 아래의 하드웨어 장비 중 OSI 2계층에 해당하는 장비는 무엇인가?

리피터, 허브, 브리지, 라우터, 스위치, L4 스위치

① 리피터, 허브
② 브리지, 스위치
③ 라우터, 스위치
④ 스위치, L4 스위치

10. 다음 지문의 필터링 규칙을 설명한 것 중에서 가장 옳지 않은 것은?

가. iptables -A INPUT -s 201.1.1.1 -j DROP 나. iptables -A INPUT -p TCP -j ACCEPT 다. iptables -A INPUT -i eth0 -p TCP -dport 80 -j DROP 라. iptables -A INPUT -i eth0 -p TCP -dport 80 -j REJECT

① “가”번은 201.1.1.1에서 유입되는 모든 패킷을 DROP 시킨다.
② “나”번은 TCP 프로토콜을 사용하는 모든 서비스의 요청을 허용한다.
③ “다”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP 시킨다.
④ “라”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP하고 송신자는 차단 여부를 확인할 수 없게 한다.

11. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호
③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간

12. 다음 중 IPsec(IP Security Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① IPsec 정책 설정 과정에서 송·수신자의 IP주소를 입력한다.
② 전송(Transport) 모드에서는 IP헤더가 암호화된다.
③ 재전송 공격을 막기 위해 IP 패킷별로 순서번호를 부여한다.
④ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.

13. 다음 설명에 해당하는 블루투스 공격 방법은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여, 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf)
② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug)
④ 블루재킹(BlueJacking)

14. 다음의 보기에서 설명하고 있는 접근제어(Access Control) 방법은 무엇인가?

· 주체(사용자)의 객체(정보)에 대한 접근이 주체의 비밀취급인가 레이블과 각 객체에 부여된 민감도 레이블에 따라 접근 허용 여부를 결정하는 방식 · 중앙집중적 관리가 가능하고, 기밀성이 매우 중요한 조직에서 사용 · 다단계 보안 모델이라고 부르기도 함

① 임의적 접근제어
② 강제적 접근제어
③ 역할기반 접근제어
④ 자율적 접근제어

15. 침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는데 적합한 기법은 무엇인가?

① 규칙 기반의 오용 탐지
② 통계적 분석에 의한 이상 탐지
③ 전문가 시스템을 이용한 오용 탐지
④ 시그니처 기반(Signature based) 탐지

16. VPN(Virtual Private Network)에서 “터널링”이라는 용어가 의미하는 내용에 가장 부합하는 것은?

① 선택사항으로서 작동 시 네트워크 성능을 향상시킬 수 있는 기능이다.
② 가상회선을 생성하고 유지할 목적으로 상이한 프로토콜의 패킷 안에 패킷을 캡슐화하는 기능이다.
③ 네트워크상 해커를 탐지하기 위해 시스템 관리자가 사용하는 기능이다.
④ 네트워크 침입이 탐지되면 바로 차단 조치를 취해 비정상 행위를 통제하는 기능이다.

17. 침해대응 과정에서 다음의 패킷로그를 기준으로 검토해 보았다. 어떤 공격 기법인가?

- Source IP : 203.234.212.10
- Destination IP : 203.234.212.10
- Protocol : 6
- Source Port : 21845
- Destination Port : 21845

① Land Attack
② Syn flooding Attack
③ Smurf Attack
④ Ping of Death Attack

18. ESM(Enterprise Security Management)에 대한 설명으로 가장 올바른 것은 무엇인가?

① 개별 솔루션 간의 별도 연동작업이 추가적으로 요구되지 않는다.
② Agent에서 읽어온 로그를 분석 없이 Manager가 수신 받고 콘솔로 표출한다.
③ 각 종 로그를 통합적으로 관리하여 통합 보안관제 서비스를 제공한다.
④ 이기종의 보안시스템을 통합하여 관리할 수 없다.

19. 특정 기관에서 사용자가 누구인가는 확인하지 않고, 그 기관이 인가한 장비이면 기관 네트워크에 접근이 가능하도록 하는 정책을 수행하고자 할 때, 적용할 수 있는 장비 인증기술로 적절한 것은?

① ID/PW 기반 인증기술
② MAC 주소 값 인증기술
③ SSID 인증기술
④ WEP 인증기술

20. 다음에서 설명하는 보안 장비는 무엇인가?

- 엔드포인트(Endpoint)가 처음 내부망 네트워크에 접근을 시도할 때 내부망에 피해가 없도록 엔드포인트에 일련의 보안정책을 적용하는 보안 솔루션이다.
- 내부 백신 설치여부, 컴퓨터 이름 등을 바탕으로 제한한다.

① IDS(Intrusion Detection System)
② IPS(Intrusion Prevention System)
③ NAC(Network Access Control)
④ NFS(Network File System)