【시스템네트워크보안】

1. 192.168.16.0/20의 IPv4 주소 블록을 동일한 크기의 8개 서브넷으로 나누었다. 8개의 서브넷 주소들로 가장 적절하지 **않은** 것은?

① 192.168.24.0/23 ② 192.168.16.0/23
③ 192.168.32.0/23 ④ 192.168.28.0/23

2. 유닉스 시스템의 'traceroute' 프로그램을 이용하여 발신지에서 목적지까지 IPv4 패킷의 전달 경로를 추적하고자 한다. 전달 경로 상의 라우터 장비들이 발신지에게 전달하는 패킷의 종류로 가장 적절한 것은?

① UDP 패킷 ② TCP 패킷
③ ICMP 패킷 ④ IGMP 패킷

3. SSL(Secure Socket Layer)에 대한 설명 중 가장 적절하지 **않은** 것은?

① 메시지 기밀성을 제공하기 위해서 대칭키 암호를 사용한다.
② UDP를 이용하여 신뢰할 수 있는 보안 서비스를 제공한다.
③ 클라이언트와 서버 간에 세션을 연결하고 유지하는 프로토콜이다.
④ HTTPS 프로토콜은 SSL을 사용하는 보안서비스이다.

4. 유닉스 로그 파일에 저장되는 정보로 가장 적절하지 **않은** 것은?

① wtmp - 사용자 로그인, 로그아웃 정보 및 시스템 부팅 정보
② utmp - 5번 이상 로그인 실패했을 경우의 로그인 실패 정보
③ lastlog - 사용자의 최근 로그인 시간 정보
④ sulog - su 명령어 사용 시 변경 전 사용자 계정과 변경 후 사용자 계정 정보

5. IPv6 프로토콜 헤더(Header)의 필드(Field)로 가장 적절하지 **않은** 것은?

① TTL(Time-To-Live) ② Source address
③ Flow label ④ Version

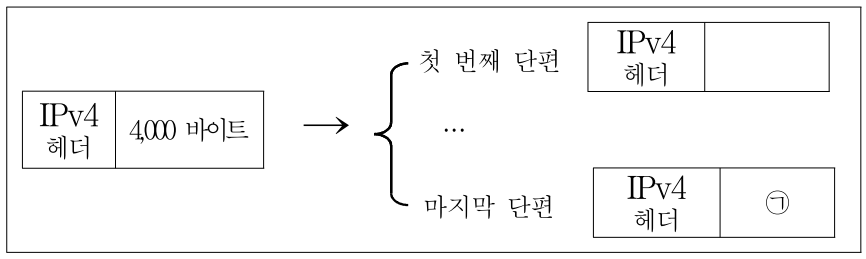
6. 침입탐지시스템(IDS : Intrusion Detection System)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 알려지지 않은 공격 행위도 이상탐지(Anomaly detection) 방식을 이용하여 탐지할 수 있다.
② IDS는 방화벽과 상호 보완적으로 사용될 수 있다.
③ 기존의 공격 패턴을 분석하여 침입을 탐지하는 오용탐지(Misuse detection) 방식을 사용할 수 있다.
④ IDS를 이용하면 공격 시도를 사전에 예방하고 차단할 수 있다.

7. TCP SYN flooding 공격의 대비책으로 가장 적절하지 **않은** 것은?

① 방화벽이나 IDS/IPS(Intrusion Prevention System) 시스템을 도입하여 침입을 탐지하고 차단한다.
② TCP 연결 타임아웃을 길게 설정한다.
③ CPU 성능이 지원하는 한도 내에서 백로그 큐(Backlog queue)를 늘려준다.
④ SYN cookie 기능을 활성화한다.

8. MTU(Maximum Transfer Unit)값이 1,500바이트로 설정되어 있는 이더넷(Ethernet)을 통해 그림과 같이 4,000바이트의 IPv4 패킷을 보내려고 한다. MTU값에 의해서 단편화(Fragmentation)된 패킷이 순서대로 전달된다고 가정할 때 마지막 단편으로 전송되는 데이터그램 ㉠의 크기(IPv4헤더는 제외)로 가장 적절한 것은?



① 1,000 바이트 ② 1,040 바이트
③ 1,480 바이트 ④ 1,500 바이트

9. 네트워크상의 특정 호스트를 발견하고 네트워크 서비스를 탐지하기 위해서 사용하는 포트 스캐닝(Port scanning) 도구로 가장 적절한 것은?

① wireshark ② netstat
③ nmap ④ nslookup

10. 다음 보안 공격의 설명에 포함되지 **않은** 것으로 가장 적절한 것은?

㉠ 공격자가 자신의 IP주소나 메일 주소를 변조하여 다른 사용자나 시스템인 것처럼 위장하여 공격
㉡ 네트워크상에서 자신이 아닌 다른 시스템들의 패킷 교환을 도청하는 공격
㉢ 공격자가 공격대상의 IP주소로 위장하여 다량의 ICMP echo request 패킷을 브로드캐스팅 함으로써, 공격대상이 다량의 ICMP echo reply 패킷을 받도록 하는 공격

① Smurf attack ② Sniffing
③ Spoofing ④ Teardrop

11. 다음 <보기>에서 패스워드 해독 공격(Password cracking attack)으로 적절한 것을 모두 고른 것은?

<보 기>

㉠ 사전공격(Dictionary attack)
㉡ 무차별 대입 공격(Brute-force attack)
㉢ 레이스 컨디션 공격(Race-condition attack)
㉣ 레인보우 테이블(Rainbow table)을 이용한 공격

① ㉠ ② ㉡㉢ ③ ㉠㉡㉢ ④ ㉠㉡㉣

12. 유닉스에서 파일의 정보를 <보기>와 같이 확인하였을 때, 파일의 소유자(owner)에게 실행 권한을 부여하는 명령으로 가장 적절한 것은?

<보 기>

-rw-rw-rw- 2 user staff 4096 2018-12-25 14:10 test.sh

① chmod u+x test.sh ② chmod o+x test.sh
③ chmod g=x test.sh ④ chmod 444 test.sh

13. 윈도우즈에서 ARP 스푸핑(spoofing)공격에 대응하기 위하여, 물리적 주소 30-A3-E2-43-12-54와 인터넷 주소 198.12.25.78을 정적으로 연결하는 명령으로 가장 적절한 것은?

① arp -v 198.12.25.78 30-A3-E2-43-12-54
② arp -d 198.12.25.78 30-A3-E2-43-12-54
③ arp -g 198.12.25.78 30-A3-E2-43-12-54
④ arp -s 198.12.25.78 30-A3-E2-43-12-54

14. 다음은 웹 클라이언트가 웹 서버에 접속할 때 발생하는 오류에 대한 설명이다. 이 설명의 상태코드로 가장 적절한 것은?

> 웹 클라이언트에서 웹 서버로 페이지를 요청 했을 때, 요청된 URL이 변경되거나 요청한 주소의 페이지가 없을 경우에 발생하는 오류이다.

① 204 No Content ② 304 Not Modified
③ 404 Not Found ④ 500 Internal Server Error

15. <보기 1>의 윈도우즈 레지스트리(Registry) 루트키와 <보기 2>의 설명을 연결한 것들 중에 가장 적절한 것은?

<보기 1>

(가) HKEY_USERS
(나) HKEY_CLASSES_ROOT
(다) HKEY_CURRENT_USER
(라) HKEY_LOCAL_MACHINE

<보기 2>

㉠ 시스템 관련 정보를 저장한다.
㉡ 컴퓨터에서 모든 계정에 관한 정보를 저장한다.
㉢ 현재 로그온 된 사용자와 관련된 데이터를 저장한다.
㉣ 파일 연관성과 COM(Component Object Model) 개체 등록 정보를 저장한다.

	(가)	(나)	(다)	(라)
①	㉢	㉡	㉣	㉠
②	㉡	㉠	㉢	㉣
③	㉡	㉣	㉢	㉠
④	㉢	㉣	㉠	㉡

16. 다음 <보기>에서 버퍼 오버플로(Buffer overflow)에 취약한 C언어의 함수들을 모두 고른 것으로 가장 적절한 것은?

< 보 기 >

㉠ strcat() ㉡ fgets() ㉢ sprintf()
㉣ strncpy() ㉤ strcmp() ㉥ realpath()

① ㉠㉢㉥ ② ㉡㉢㉤
③ ㉠㉣㉤ ④ ㉡㉣㉥

17. 리눅스에서 각종 서비스들을 제공하기 위한 데몬(Daemon)에 대한 설명으로 가장 적절하지 **않은** 것은?

① syslogd - 로그기록 서비스를 제공한다.
② ntpd - 네트워크 파일시스템 서비스를 제공한다.
③ crond - 주기적으로 실행하도록 예약한 명령을 실행한다.
④ systemd - 시스템의 상태를 종합적으로 관리하는 역할을 수행한다.

18. Apache 웹 서버를 사용할 때 웹 로그에 기록되는 정보로 가장 적절하지 **않은** 것은?

① 클라이언트 호스트 명 또는 IP 주소
② 클라이언트 운영체제 및 브라우저 버전 정보
③ 클라이언트 요청에 대한 처리 상태를 나타내는 상태코드
④ 클라이언트 요청을 처리하는데 소요된 시간과 메모리 사용량

19. 다음 <보기> 중 허니팟(Honeypot)에 대한 설명으로 적절한 것을 모두 고른 것은?

<보 기>

㉠ 공격자의 행동 패턴에 관한 정보를 수집한다.
㉡ 비정상적인 접근을 탐지하기 위하여 의도적으로 설치해 둔 시스템이다.
㉢ 허니팟이 공격자에게 쉽게 해킹당하지 않도록 취약점을 제거하는 보안조치를 취한다.
㉣ 침입자가 허니팟을 사용하는 동안 감시하는 역할을 한다.

① ㉠ ② ㉡㉢ ③ ㉢㉣ ④ ㉠㉡㉣

20. 다음 <보기>에서 가상 사설망(VPN : Virtual Private Network)이 제공하는 보안 서비스로 적절한 것을 모두 고른 것은?

<보 기>

㉠ 인증 ㉡ 터널링
㉢ 패킷 필터링 ㉣ 데이터 암호화

① ㉠㉢ ② ㉡㉣ ③ ㉡㉢㉣ ④ ㉠㉡㉣