

1과목 : TCP/IP

1. 프로토콜 분석에서 사용되는 도구 중 사용 용도와 기능이 다른 하나는?

- ① WinPcap ② Tcpdump
- ③ Wireshake ④ Pktbuilder

2. TCP/IP 프로토콜에 대한 설명 중 IP의 특징으로 올바른 것은?

- ① 계층적 주소(Hierarchical Addressing Scheme)를 사용하여 경로 결정을 수행한다.
- ② 데이터의 에러 검출 기능을 포함하고 있다.
- ③ Connetionless 서비스를 제공하지 않는다.
- ④ UDP Datagram에 대해서 꼭 단편화 작업을 수행해야 한다.

3. 다음 중 무선 LAN(Wi-Fi) 표준 기술과 사용하는 변조 방식의 연결로 옳지 않은 것은?

- ① IEEE 802.11n (Wi-Fi 4) : OFDM
- ② IEEE 802.11ac (Wi-Fi 5) : OFDM
- ③ IEEE 802.11ax (Wi-Fi 6) : OFDMA
- ④ IEEE 802.11be (Wi-Fi 7) : DSSS

4. 네트워크 ID '210.182.73.0'을 6개의 서브넷으로 나누고, 각 서브넷마다 적어도 30개 이상의 Host ID를 필요로 한다. 적절한 서브넷 마스크 값은?

- ① 255.255.255.224 ② 255.255.255.192
- ③ 255.255.255.128 ④ 255.255.255.0

5. IPv6의 특징 중 옳지 않은 것은?

- ① 브로드 캐스트가 가능하다.
- ② 128bit의 주소 길이를 갖는다.
- ③ 16bit씩 8부분으로 16진수로 표시한다.
- ④ IPSec을 기본적으로 지원한다.

6. TCP 세션의 성립에 대한 설명으로 옳지 않은 것은?

- ① 세션 성립은 TCP Three-Way Handshake 응답 확인 방식이라 한다.
- ② 실제 순서번호는 송신 호스트에서 임의로 선택된다.
- ③ 세션 성립을 원하는 컴퓨터가 ACK 플래그를 '0'으로 설정하는 TCP 패킷을 보낸다.
- ④ 송신 호스트는 데이터가 성공적으로 수신된 것을 확인하기까지는 복사본을 유지한다.

7. TCP/IP 계층 중 다른 계층에서 동작하는 프로토콜은?

- ① IP ② ICMP
- ③ UDP ④ IGMP

8. IP 프로토콜의 헤더 체크섬(Checksum)에 대한 설명 중 올바른 것은?

- ① 체크섬 필드를 '0'으로 하여 계산한다.
- ② 네트워크에서 존재하는 시간을 나타낸다.
- ③ 데이터그램의 총 길이를 나타낸다.
- ④ IP 헤더에 대해서만 포함되며 데이터 필드를 포함한다.

9. ICMP의 메시지 유형으로 옳지 않은 것은?

- ① Destination Unreachable ② Time Exceeded
- ③ Echo Reply ④ Echo Research

10. IGMP에 대한 설명 중 올바른 것은?

- ① 호스트가 멀티캐스트 그룹에 가입하거나 데이터를 수신하기 위해 라우터와 통신할 때 사용된다.
- ② 호스트가 자신에게 할당된 IP 주소를 브로드캐스트로 요청할 때 사용하는 프로토콜이다.
- ③ 두 지점 간 전송의 신뢰성과 흐름 제어를 보장하기 위해 3-way 핸드셰이크를 사용하는 프로토콜이다.
- ④ IP 패킷의 경로 상 오류 발생 시 오류 메시지를 생성하여 송신자에게 알리는 프로토콜이다.

11. RARP에 대한 설명 중 올바른 것은?

- ① 시작지 호스트에서 여러 목적지 호스트로 데이터를 전송할 때 사용된다.
- ② TCP/IP 프로토콜의 IP에서 접속없이 데이터의 전송을 수행하는 기능을 규정한다.
- ③ 하드웨어 주소를 IP Address로 변환하기 위해서 사용한다.
- ④ IP에서의 오류제어를 위하여 사용되며, 시작지 호스트의 라우팅 실패를 보고한다.

12. UDP에 대한 설명 중 옳지 않은 것은?

- ① 가상선로 개념이 없는 비연결형 프로토콜이다.
- ② TCP보다 전송속도가 느리다.
- ③ 각 사용자는 16비트의 포트번호를 할당받는다.
- ④ 데이터 전송이 블록 단위이다.

13. IP Address 중 Class가 다른 주소는?

- ① 191.235.47.35 ② 128.128.105.4
- ③ 169.146.58.5 ④ 195.204.26.34

14. 라우터가 자신을 네트워크의 중심점으로 간주하여 최단 경로의 트리를 구성하는 방식으로, 사용자에게 의한 경로의 지정, 가장 경제적인 경로의 지정, 복수경로 선정 등의 기능을 제공하는 라우팅 프로토콜은?

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

15. (A)에 해당되는 용어는?

클라이언트는 'icqa.or.kr' 웹 사이트에 접근하려고 한다. 시스템 내 저장되어 있는 DNS 캐시 정보를 확인 후 Entry 정보가 없는 경우 DNS 서버에 해당 도메인에 대한 IP address를 질의하는 (A) 쿼리를 보내게 된다.

- ① 재귀 ② 반복
- ③ 선택 ④ 동적

16. DNS 레코드 중 도메인의 메일 서버를 식별하기 위해 사용되는 레코드는?

- ① NS 레코드 ② Host 레코드
- ③ Point 레코드 ④ MX 레코드

2과목 : 네트워크 일반

17. TCP/IP 환경에서 사용하는 도구인 'Netstat' 명령에서 TCP 및 UDP 프로토콜에 대한 통계를 확인할 때, 올바른 명령은?
- ① Netstat -e ② Netstat -s
 - ③ Netstat -o ④ Netstat -r

18. 다음은 SDN(Software Defined Network)에 대한 설명이다. (A)와 (B)에 들어갈 용어는 무엇인가?

SDN은 개방형 API(오픈플로우)를 통해 네트워크의 트래픽 전달 동작을 소프트웨어 기반 컨트롤러에서 제어/관리하는 접근방식이다. SDN은 트래픽 경로를 지정하는 (A)과 트래픽 전송을 수행하는 (B)으로 분리되어 있다.

- ① (A) 제어 기능, (B) 데이터 기능
- ② (A) 데이터 기능, (B) 제어 기능
- ③ (A) 라우팅 기능, (B) 포워딩 기능
- ④ (A) 포워딩 기능, (B) 라우팅 기능

19. 다음은 Home Network에 사용되는 기술 중 WPAN(Wireless Personal Area Network)에 대한 설명이다. (A), (B), (C) 안에 들어갈 표준을 순서대로 나열한 것은?

네트워크 관리 담당자인 Kim 사원은 회사 소속 직원들이 거주하는 아파트의 홈네트워크 시스템을 통합하기 위해 다양한 관련 기술 표준을 조사하고 있다. 사용할 수 있는 기술은 기존의 Wireless LAN 이외에 WPAN으로 통칭하는 기술이 있으며, 이는 크게 블루투스, 고속 WPAN 및 저속 WPAN으로 분류할 수 있다. (A)는 WPAN/블루투스를 (B)는 고속 WPAN에 대한 표준이며, (C)는 저속 WPAN에 대한 표준이다.

- ① 802.11.1 - 802.11.3 - 802.11.4
- ② 802.11a - 802.11b - 802.11c
- ③ 802.15.1 - 802.15.3 - 802.15.4
- ④ 802.16.1 - 802.16.3 - 802.16.4

20. 다음 중 클라우드 컴퓨팅에서 제공하는 GSLB (Global Server Load Balancing)의 특징 중 가장 거리가 먼 것은?

- ① 트래픽 분산 ② 서비스 서버 상태 체크
- ③ 응답 성능 향상 ④ 서비스 콘텐츠 캐싱

21. 다음 중 클라우드 컴퓨팅 환경에서 보안 관리 서비스를 On-Demand 형태로 제공하는 것은?

- ① SaaS ② SECaaS
- ③ DevSecOps ④ PaaS

22. (A)에 들어갈 용어로 가장 적절한 것은?

(A)은/는 소스IP 변환이 주목적이다. 퍼블릭 유형과 프라이빗 유형이 있으며 퍼블릭 유형은 프라이빗 IP만 소유한 서비스가 인터넷 접속이 필요할 때 사용하고, 프라이빗 유형은 인터넷 접속과 관계없이 소스 주소 변환의 목적으로만 사용한다.

- ① 인터넷 게이트웨이 ② NAT 게이트웨이
- ③ 로드밸런싱 ④ VPC 피어링

23. 클라우드 네트워크 관리 기술은 일반적으로 ISO/ITU-T 기준에 따라 구성 관리, 성능 관리, 계정 관리, 장애 관리, 보안 관리 등으로 나뉘며, 각각의 기능이 명확히 정의되어 있다. 다음 중 각 관리 영역의 설명으로 부적절한 것은?

- ① 구성 관리는 네트워크 구성에 관한 정보를 수집하고 이러한 정보를 바탕으로 장치의 구성을 업데이트하여 최신 정보를 유지하고 보고서를 작성하는 기능을 담당한다.
- ② 성능 관리는 통계 정보를 수집하고, 시스템 상태 이력 기록을 유지·검사하며, 시스템 성능을 측정하고, 시간과 대역폭 사용률, 패킷 처리율 등을 단계별 또는 시간별로 관리한다.
- ③ 계정 관리는 개방 시스템에서 일어나는 활동에 따라 소비하는 자원에 관한 모든 정보를 관리하고, 자원 사용량과 관련이 있는 네트워크 데이터를 수집하는 것을 말한다.
- ④ 보안 관리는 네트워크 장치 설정 및 변경, 가입 변경 시 구성 정보 변경, 네트워크 장치 구성 정보의 버전 관리, 네트워크 관리 체계 소프트웨어의 백업 등이 해당된다.

24. OSI에서 표준 모델로 정한 컴퓨터 상호간 연결을 위한 계층 구조 중, 통신을 위한 물리적 전송로의 설정, 유지 및 해제를 담당하는 계층은?

- ① Physical Layer ② Data Link Layer
- ③ Network Layer ④ Session Layer

25. CRC(Cyclic Redundancy Checking) 에러검출 방법에 대한 설명으로 옳지 않은 것은?

- ① 프레임이 수신되면 수신기는 같은 제수(Generator)를 사용하여 나눗셈의 나머지를 검사한다.
- ② CRC 비트를 만들기 위해 논리함 연산을 수행한다.
- ③ 전체 블록 검사를 위해 메시지는 하나의 긴 이진수로 간주한다.
- ④ 메시지를 특정한 이진 소수에 의해 나눈 후 나머지를 송신 프레임에 첨부하여 전송한다.

26. 광케이블을 이용하는 통신에서 저손실의 파장대를 이용하여 광 파장이 서로 다른 복수의 광 신호를 한 가닥의 광섬유에 다중화 시키는 방식은?

- ① 코드 분할 다중 방식(CDM)
- ② 직교 분할 다중 방식(OFDM)
- ③ 시간 분할 다중 방식(TDM)
- ④ 파장 분할 다중 방식(WDM)

27. 오류 검출 방식인 ARQ 방식 중에서 일정한 크기 단위로 연속해서 프레임을 전송하고, 수신측에 오류가 발견된 프레임에 대하여 재전송 요청이 있을 경우 잘못된 프레임만을 다시 전송하는 방법은?

- ① Stop-and-Wait ARQ ② Go-back-N ARQ
- ③ Selective-repeat ARQ ④ Adaptive ARQ

정책

- ② GROUP_MGMT : 보안 템플릿에 지정된 관리 그룹
- ③ USER_RIGHTS : 사용자 로그인 권한 및 사용 권한 부여
- ④ SERVICES : 정의된 모든 서비스

40. 서버 담당자 Kang 사원은 Windows Server 2016의 이벤트 뷰어를 통해 감사 정책에 따른 로그 정보를 확인하여 서버의 상태를 지속적으로 체크하고 있다. 하드웨어 이벤트와 관련한 항목으로 올바른 것은?

- ① 사용자 지정 보기
- ② 보안 로그
- ③ 응용 프로그램 및 서비스 로그
- ④ 구독

41. Windows Server 2016 파일 서버를 운영 중인 관리자 Park 사원은 사용자에게 기본 접근 권한을 부여하려고 한다. 다음 중 NTFS 기본 권한 항목에 해당하지 않는 것은?

- ① Read
- ② Write
- ③ List folder contents
- ④ Write &Execute

42. 'runlevel 5' 로 로그인 되어 있는 상태에서 Apache에 소스 컴파일 설치를 하여 '/etc/init.d' 의 경로에 httpd 데몬 shell script를 생성하여 정상적인 실행을 확인하였다. 해당 데몬을 재부팅 후에 자동 실행되도록 설정하는 명령어는?

- ① systemctl restart httpd.service
- ② /etc/init.d/httpd restart
- ③ chkconfig --list | grep httpd
- ④ chkconfig --level 5 httpd on

43. 서버 담당자 Park 사원은 Windows Server 2016에서 공인 인증기관(CA)에 인증서를 요청하기 위해, 실행 중인 IIS(인터넷 정보 서비스)를 통해 CSR(Certificate Signing Request)을 생성하려고 한다. 이 작업을 수행하기 위해 IIS 관리자에서 선택해야 하는 항목으로 가장 적절한 것은?

- ① HTTP 응답 헤더
- ② MIME 형식
- ③ 기본 문서
- ④ 서버 인증서

44. 다음은 Linux에서 사용자 계정을 생성하는 명령어이다. 이 명령어에 대한 설명 중 잘못된 것은?

```
adduser -u 550 -g 13 -d /home/test -s /bin/sh -f 40 test
```

- ① 사용자 계정은 test이다.
- ② 홈 디렉터리는 '/home/test'를 사용한다.
- ③ 셸은 본셀을 사용한다.
- ④ 40일마다 패스워드를 변경하도록 설정한다.

45. Windows와 UNIX는 다른 로그 체계를 갖추고 있다. Windows는 이벤트(event)라고 불리는 중앙 집중화된 형태로 로그를 수집하여 저장한다. Windows 이벤트 뷰어에 표시되는 항목과 설명이 잘못 설명되어 있는 것은?

- ① 컴퓨터 : 관련 로그를 발생시킨 시스템
- ② 원본, 범주 : 로그와 관계있는 영역
- ③ 사용자 : 관련 로그를 발생시킨 사용자
- ④ 날짜 및 시간 : 파일 생성 시간

4과목 : 네트워크 운용기기

46. 라우터(Router)와 L3 스위치의 특징을 비교한 내용 중 바르게 설명한 것은?

- ① 모든 L3스위치는 NAT(Network Address Translation)기능을 제공한다.
- ② L3스위치 및 라우터의 패킷전송구조는 하드웨어 기반이다.
- ③ 라우터는 WAN구간 연동을 위한 인터페이스 제공이 어렵다.
- ④ 라우터는 L3 스위치보다 다양한 WAN 연동용 인터페이스(Ethernet, 광 링크, 고속 시리얼 등)를 제공한다.

47. 네트워크 스위치 다수의 포트를 하나의 포트로 사용하여 대역폭을 늘릴 수 있고 여러 포트를 하나로 사용하기에 STP로 Blocking되지 않고 포트를 전부 사용할 수 있는 기술은?

- ① 이더 채널(Ether Channel)
- ② 가상랜(Virtual Local Area Network)
- ③ POE(Power Over Ethernet)
- ④ 게이트웨이(Gateway)

48. 서로 다른 형태의 네트워크를 상호 접속하는 장치로 필요할 경우 프로토콜 변환을 수행하는 장치는?

- ① Frame Relay Access Device
- ② Remote Access Server
- ③ Gateway
- ④ Switching Hub

49. RAID의 기능 중에서 Hot Swap의 기능을 올바르게 설명한 것은?

- ① 전원이 꺼진 상태에서 디스크를 백업하는 기능이다.
- ② 전원이 꺼진 상태에서 디스크를 교체하는 기능이다.
- ③ 전원이 켜진 상태에서 데이터를 여분의 디스크에 백업하는 기능이다.
- ④ 전원이 켜진 상태에서 디스크를 교체하는 기능이다.

50. 라우팅 프로토콜은 목적지까지의 최적 경로를 결정하기 위해 다양한 메트릭(Metric) 값을 사용한다. 다음 중 메트릭으로 사용되지 않는 항목은?

- ① 회선의 최대 전송속도(Bandwidth)
- ② 라우터의 종류(Vendor)
- ③ 목적지까지의 홉 수(Hop Count)
- ④ 회선 사용량(Load)

5과목 : 정보보호개론

51. 다음 지문이 설명하는 제도는?

클라우드 서비스 제공자가 제공하는 서비스에 대해 '클라우드컴퓨팅법' 제 23조 제 2항에 따라 정보보호 기준의 준수 여부를 인증기관이 평가 인증하며 이용자들이 안심하고 클라우드컴퓨팅 서비스를 이용할 수 있도록 지원하는 제도

- ① CASP
- ② K-ISMS
- ③ ISO27001
- ④ BS7799

52. PAM(Pluggable Authentication Modules) 설정파일 중 제어 플래그에 대한 설명으로 옳은 것은?

- ① required: 모듈 인자로 지정한 설정 파일에서 모든 행을 읽어온다.

- ② requisite: 해당 모듈은 인증을 계속하기 위해 반드시 성공해야 한다.
- ③ include: 모듈 인자로 지정한 설정 파일에서 모든 행을 읽어온다.
- ④ sufficient: 이 모듈의 결과는 무시된다. 만약 이 모듈이 성공하고 앞선 required 모듈 중 실패가 없으면 인증 성공을 리턴한다.

53. 지문과 같이 rsyslog 필터를 구성하고자 한다. 지문에 맞게 필터를 올바르게 작성한 것은?

cron에서 info와 debug를 제외한 모든 로그 메시지를 선택한다.

- ① cron.!info,!debug
- ② info.!cron,!debug
- ③ debug.!info,!cron
- ④ info.!debug,!cron

54. (A) 안에 들어가는 용어 중 옳은 것은?

보안관리자 Kim 대리는 회사의 중요한 데이터를 인가된 사용자에게만 제공하고, 인가되지 않은 사용자에게 데이터가 제공되지 않도록 하기 위해 보안 솔루션을 도입하고자 한다. (A)을/를 도입함으로써 매체, 통신 인터페이스 제어를 통해 사용자 수준에서 회사의 데이터가 외부로 유출되는 것을 예방할 수 있을 것으로 기대한다.

- ① PMS (Patch Management System)
- ② DLP(Data Loss Prevention)
- ③ IDS (Intrusion Detection System)
- ④ IPS (Intrusion Prevention System)

55. 보안 담당자 Kim은 SSL 3.0 기반의 암호화 통신 환경에서 CBC 모드의 패딩 처리 방식 취약점을 악용한 공격으로 사용자의 세션 쿠키 등 민감 정보가 유출될 수 있음을 확인하였다. 다음 중 이러한 패딩 오라클(padding oracle) 공격에 사용되는 SSL 3.0의 대표적인 취약점 이름은?

- ① POODLE 취약점
- ② Heartbleed 취약점
- ③ Bicycle 취약점
- ④ FREAK 취약점

56. 침해사고 유형에 대한 설명으로 옳지 않은 것은?

- ① botnet : 스팸메일이나 악성코드 등을 전파하도록 하고 해커가 마음대로 제어할 수 있는 좀비 PC들로 구성된 네트워크를 말한다.
- ② Trojan horse: 정상기능의 프로그램으로 가장하여 프로그램 내에 숨어있는 코드로, 의도하지 않은 기능을 수행하는 프로그램 또는 실행코드
- ③ 이메일 스크 : 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 이용자들의 금융정보 등을 빼내는 신종 사기 수법
- ④ APT : 지능적 지속 위협 공격으로, 지능적이고 지속적으로 위협을 가해 피해를 주는 공격을 의미한다.

57. MitM(Man in the Middle) 공격의 종류가 아닌 것은?

- ① ARP Spoofing
- ② Distributed Denial of Service
- ③ DNS Spoofing
- ④ Sniffing

58. Session Hijacking이라는 웹 해킹 기법과 비슷하나, 사용자의 권한을 탈취하는 공격이 아니라 사용자가 확인한 패킷의

내용만을 훔쳐보는 기법은?

- ① Spoofing
- ② Side jacking
- ③ Sniffing
- ④ Strip attack

59. 다음 지문과 같은 특성을 갖는 전자우편 보안 기술은?

보안 담당자 Kim은 전자우편의 기밀성과 무결성을 동시에 보장할 수 있는 보안 기술을 도입하고자 한다. 해당 기술은 전자우편을 입수하더라도 내용을 해독할 수 없게 암호화하고, 해시 함수를 이용해 무결성을 확인하며, 송신자의 개인키 기반 전자서명을 통해 신원을 검증한다. 또한, 인증기관(CA) 대신 웹 오브 트러스트(Web of Trust) 기반으로 키를 관리하며, 개인 사용자 중심으로 활용되는 특징이 있다.

- ① PEM(Privacy Enhanced Mail)
- ② S/MIME(Secure Multi-Purpose Internet Mail Extensions)
- ③ PGP(Pretty Good Privacy)
- ④ SMTP(Simple Mail Transfer Protocol)

60. 다음은 방화벽의 구성 요소 중 무엇을 설명하는 것인가?

- 보호된 네트워크에서 유일하게 외부의 공격에 노출된 컴퓨터 시스템을 말한다.
 - 네트워크 보안 상 가장 중요한 위치를 차지하므로 관리자에 의해 철저하게 감시되며 불법적인 침입 의도를 가지고 접속한 모든 시스템의 기록들에 대해서 주기적인 검사가 이루어져야 한다.
 - 클라우드 환경에서는 외부에서 내부 VPC 또는 가상 네트워크로 SSH 접속을 중계하는 서버(Jump Host)로 활용된다.

- ① 방어선 네트워크 (Perimeter Network)
- ② 베스천 호스트 (Bastion Host)
- ③ 스크리닝 라우터 (Screening Router)
- ④ DMZ (Demilitarized Zone)

1	2	3	4	5	6	7	8	9	10
④	①	④	①	①	③	③	①	④	①
11	12	13	14	15	16	17	18	19	20
③	②	④	①	①	④	②	①	③	④
21	22	23	24	25	26	27	28	29	30
②	②	④	②	②	④	③	②	④	①
31	32	33	34	35	36	37	38	39	40
④	④	②	②	③	③	③	①	②	③
41	42	43	44	45	46	47	48	49	50
④	④	④	④	④	④	①	③	④	②
51	52	53	54	55	56	57	58	59	60
①	③	①	②	①	③	②	②	③	②