

[TCP/IP 단답형 기출문제 모음]

Q. Class 별 IP 주소

- A. A class : 0.0.0.0
- B Class : 128.0.0.0
- C Class : 192.0.0.0
- D Class : 224.0.0.0
- E Class : 240.0.0.0

**Q. 아래는 사설망 IP 에 사용되는 주소이다.
(가), (나), (다)에 들어갈 주소는 무엇인가?**

- A. A class : 0.0.0.0 ~ 0.255.255.255
- B Class : 172.(가).0.0 ~ 172.(나).255.255
- C Class : 192.(다).0.0 ~ 192.(다).255.255
- A. (가) : 16, (나) : 31, (다) : 168

Q. IPv4 와 IPv6 의 특징을 나열하시오.

[보기]

IPv4	IPv6
------	------

32bit

유니캐스트

멀티캐스트

브로드캐스트

128bit

유니캐스트

멀티캐스트

애니캐스트

Q. [보기]를 보고 OSI 7 Layer 의 계층별 프로토콜을 알맞게 나누어 보시오.

- 응용 계층의 프로토콜
- 전송 계층의 프로토콜
- 네트워크 계층의 프로토콜

[보기]

FTP, RIP, HTTP, SNMP, SMTP, ARP, IGMP, TCP, POP3, RARP, ICMP, UDP

- A. 응용 계층 프로토콜 : FTP, HTTP, SNMP, SMTP, POP3
- 전송 계층 프로토콜 : TCP, UDP
- 네트워크 계층 프로토콜 : RIP, ARP, RARP, IGMP, ICMP

Q. 매니지먼트와 에이전트 사이에 관리정보를 주고 받기 위한 프로토콜로 정보 교환 단위 메시지

A. SNMP

Q. TCP/IP 기반 네트워크상에서 서버나 라우터가 예러나 예상치 못한 사건들을 보고할 목적으로 만들어진 프로토콜로 RFC792 에 정의되어 있는 프로토콜은 무엇인가요?

A. ICMP

예러나 오류를 보고할 목적으로 만들어진 프로토콜, RFC792 이라고 하면 ICMP 를 뜻합니다.

*** ICMP (Internet Control Message Protocol)**

ICMP 의 C 는 컨트롤 한다는 뜻을 가지고 있으며, M 은 메시지를 의미합니다. 컨트롤하다가 오류가 발생하면 메시지를 보낸다고 외우시면 좋을것 같습니다.

Q. 로컬 네트워크상에서 라우터와 호스트간의 멀티캐스트 환경을 구축하는 프로토콜로 RFC112 에 정의되어 있는 프로토콜은 무엇인가요?

A. IGMP

라우터와 호스트 간의 멀티캐스트 환경구축, RFC112 이라고 하면 IGMP 를 뜻합니다.

*** IGMP (Internet Group Management Protocol)**

IGMP 의 G 는 그룹을 뜻하고 M 은 관리를 의미합니다.

라우터와 호스트를 그룹으로 생각하시고 관리한다고 생각하시면 좋을것 같습니다.

Q. IP 주소로 MAC 주소를 알아내는 프로토콜은 무엇인가?

A. ARP

*** IP 주소로 MAC 주소를 알아내는 프로토콜은 ARP**

반대로 MAC 주소로 IP 주소를 알아내는 프로토콜은 RARP 입니다.

Q. TCP/UDP 를 사용하는 프로토콜을 나열하시오.

TCP 사용 프로토콜

UDP 사용 프로토콜

TCP/UDP 둘다 사용하는 프로토콜

[보기]

FTP, DNS, HTTP, BOOTP, SMTP, Telnet, TFTP, POP3, SNMP, DHCP

A. TCP 사용 프로토콜 : FTP, Telnet, SMTP

UDP 사용 프로토콜 : DNS, TFTP, SNMP

TCP/UDP 둘다 사용하는 프로토콜 : HTTP, POP3, DHCP, BOOTP

Q. 아래의 보기중 UDP 프로토콜의 특징에 해당되는 것을 모두 선택하시오.

[보기]

비신뢰성, 비연결형, 비순서형, 신뢰성, 연결형, 순서형

A. UDP 프로토콜 특징 : 비신뢰성, 비연결형, 비순서형

TCP 프로토콜 특징 : 신뢰성, 연결형, 순서형

*** UDP 프로토콜은 서버와 클라이언트간의 소통없이 일방적인 송신하는 프로토콜입니다.**

따라서 신뢰성이 필요없고 비연결형이며, 순서가 없이 사용되는 프로토콜 입니다.

Q. (A)와 (B)는 무엇인가?

(A)는 임의로 구성된 웹 사이트를 통하여 이용자의 정보를 빼가는 해킹수법의 하나이다.

(B)는 네트워크상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로

파일을 복사할 수 있게 해주는 응용프로그램, 또는 그 프로토콜을 의미한다.

A. (A) : 스푸핑

(B) : SSH

Q. 제시 문제에서 설명하는 보안 기술을 입력하시오.

원격호스트에 접속하기 위해 텔넷을 사용할 경우 스피닝을 이용한 패스워드 유출이 가능하다. 이를 방지하기 위해 사용하는 텔넷과 유사한 암호화 접속방식을 말한다. 보안등급이 낮은 네트워크에서 보안 등급이 높은 원격접속 개시나 데이터를 전송을 실현하는 프로토콜

A. SSH

Q. 다음 설명하는 프로토콜은 무엇인가요?

응용계층 보안 프로토콜로 인증서를 기반으로 암호화된 데이터를 전송한다. 암호화 알고리즘은 비대칭형 암호화 시스템을 사용한다.

A. SSL

*** 데이터를 안전하게 주고받기 위한 프로토콜로 인증 암호화 기능이 있다.**

Q. 거짓 이메일을 발송하여 불법적으로 정보를 빼가는 수법은 무엇인가?

A. 피싱

Q. 보기 중 아래의 설명에 알맞는 장비를 선택하시오.

인터넷 웜등의 악성코드 해킹등을 통한 침입이 일어나기 전에 실시간으로 침입을 막고 알려지지 않은 방식으로

침입하는 것을 네트워크와 호스트 컴퓨터를 보호하는 솔루션은 무엇인가?

1) 방화벽

2) SQL 인젝션

3) IDS

4) 웹 어플리케이션 방화벽 (WAF)

5) XSS

A. 4) 웹 어플리케이션 방화벽(WAF)

* **WAF (Web Application Firewall)**은 웹 공격을 탐지하고 차단하는 방화벽을 의미합니다.

Q. 무선 랜 표준을 정의하는 **IEEE 802.11** 규약의 일부분으로 무선 LAN 운용간의 보안을 위해 사용되는 알고리즘으로 유선 랜에서 기대할 수 있는 것과 같은 보안과 프라이버시 수준의 무선 랜의 보안 프로토콜이다.

A. WEP

* **WEP (Wired Equivalent Privacy)**는 무선 LAN(Wireless) 이용시 취약한 보안을 위해 사용되는 알고리즘

Q. 네트워크에서 공격서명을 찾아내어 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안솔루션이다. 수동적인 방어 개념의 침입탐지시스템(IDS)와 달리 침입경고 이전에 공격을 중단시키는데 중점을 두는 시스템은 무엇인가?

A. IPS (Intrusion Prevention System)

Q. IDS(침입탐지시스템)은 크게 오용탐지와 비정상행위탐지 분류된다. 비정상행위탐지에 해당하는 특징은 무엇인가?

A. 새로운 침입유형을 탐지한다.

정상행위를 정의하고 이를 벗어나는 행동을 찾는다.

* **IDS(침입 차단 시스템)**에는 두가지 탐지 방법이 있습니다.

1. 오용탐지 : 새로운 침입유형은 탐지 불가능

비정상행위를 정의하고 이에 대한하는 행동을 찾는다.

2. 비정상 행위탐지 : 새로운 유형을 탐지

정상행위를 정의하고 이를 벗어나는 행동을 찾는다.

위 두가지를 잘 구별하실 수 있어야 합니다.

Q. 침입탐지시스템의 탐지기법 중 무엇인가?

이미 발견되어있는 공격 패턴을 미리 입력해두고, 해당하는 패턴을 탐지하는 기법. 알려진 기법 이외에는 탐지할 수 없기 때문에 새로운 공격에는 비효율적이다.

A. 오용탐지기법

Q. 인터넷망과 같은 공중망을 사설망처럼 이용하여 회선을 크게 절감할 수 있는 기업통신 서비스

A. VPN

Q. 2 개 이상의 다른, 혹은 같은 종류의 통신망을 상호 접속하여 통신망 간 정보를 주고 받을 수 있게 하는 기능의 단위 또는 장치

A. 게이트웨이(Gateway)

Q. IP 주소를 사용하는 것의 낭비를 막기 위해 모든 호스트에 공인 IP 주소를 설정하는 대신, 내부적으로 사설

IP 를 설정하여 사용하고, 인터넷에 접속할 때에만 공인 IP 로 변환하는 기술.

A. NAT

Q. '스위칭'이라는 LAN 기술을 기반으로 물리적 시간만 고려되었던 LAN 분야에 가상이라는 개념을 도입한 것이다. 네트워크 구성에 대한 지리적 제한을 최소화 하면서 사용자가 원하는 최대한의 논리적인 네트워크를 구성할 수 있도록 수단을 제공한다.

A. VLAN (Virtual LAN) 가상랜

* 키워드는 'LAN 분야에 가상' '지리적인 제한을 최소화' 하여 논리적인 네트워크 구성입니다.

Q. OSI 7 모델의 데이터링크계층 중 MAC 계층에서 일하며 두 세그먼트 사이에서 데이터링크 계층간의 패킷 전송을 담당하는 장비는 무엇인가요?

A. 브릿지 (Bridge)

Q. 네트워크 스위치의 어떠한 포트에서 보이는 모든 네트워크 패킷 혹은 전체 VLAN 의 모든 패킷들을 다른 모니터링 포트에 복제하는데 사용된다.

A. 포트 미러링

Q. 동적디스크 볼륨 중 볼륨자체에서 하나의 디스크 손상 시 다른 하드디스크의 DATA 로 손상된 부분을 복구할 수 있는 내결함성을 지원하는 볼륨. 해당 볼륨의 종류는 RAID1 과 RAID 0+1 이 있다.

A. 미러링

Q. 기존 유선랜(HUB 또는 스위치와 연결)과 무선랜을 연결하는 경우 사용하는 장비. 사용자가 이동하며 이동형 무선장치를 사용할 수 있다.

A. Access Point

Q. RFID 와 관계 없는 것은?

<보기> RFID 리더기, 태그, 태그안테나, Access Point

A. Access Point

* Access Point (AP)는 유선랜과 무선랜을 연결하는 장비입니다.

Q. HTTP 프로토콜을 통해 서버나 스크립트가 클라이언트 컴퓨터의 정보를 유지 관리하는 방법은 무엇인가?

A. 쿠키

Q. 다음은 IP 헤더를 나타낸 것이다. 단편화 기능과 관련된 3 가지 필드를 선택하시오.

A. Identification

Flag

Fragmentation Offset