[리눅스 명령어]

< grub >

- 리눅스 부트로더

< man >

- 리눅스 메뉴얼을 확인하는 명령어

< init >

- 리눅스 커널 부팅이 완료된 뒤 실행되는 첫번째 프로세스
- 커널이 직접 실행하는 유일한 프로세스이다.

< runLevel의 init >

- 런레벨과 관련있는 명령어
- init 0 : 시스템 종료
- init 1 : 단일 사용자 모드(윈도우 안전모드와 같음)
- init 2 : 다중 사용자 텍스트 모드 (네트워크 사용불가)
- init 3 : 다중 사용자 텍스트 모드 (네트워크 사용가능)
- init 4 : x
- init 5 : 다중 그래픽 사용자 모드 (윈도우 GUI와 같음)
- init 6 : 시스템 재부팅

< /etc/fstab >
- 리눅스 부팅시 자동으로 마운트 되도록 설정해야 하는 파일

< etc/named.conf >
- DNS 서버 및 존 파일 설정 관련 파일

< /etc/mtab >
- 현재 마운트 되어져있는 정보가 저장된 파일

< 데몬 : Daemon >
- 서버의 역할을 수행하거나 그 기능을 도와줌
- 백그라운드로 동작해 시스템 서비스를 지원함
- 이벤트 발생시 동작하며 서비스 제공 후 대기 상태로 전

< passwd >
- 리눅스 사용자 비밀번호 변경

< pwd >
- 현재 디렉토리

< df >
- 디스크 사용량

< top >
- 실시간 cpu 사용량
- 가장 우선순위 높은 프로세스 보여주는 명령어

< free >
- 메모리 사용량
- 시스템 메모리 체크

< netstat : network status >
- 프로토콜 통계 및 네트워크 연결 상태 파악
- 네트워크 인터페이스 상태 정보
- a : 모든 연결들과 수신 포트 표시
- 라우팅 테이블, 네트워크 인터페이스 또는 네트워크 연결 보여주는 리눅스 명령어

< tracert >
- 패킷이 라우팅되는 경로의 추적에 사용되며 유틸리티 목적지 경로까지(경유지)의 응답속도 확인 가능 명령어
- tracer는 ICMP 기반의 윈도우에서 사용하고, traceroute는 UDP기반의 유닉스 기반에서 사용한다.

< traceroute >
- 명령어를 실행하는 컴퓨터에서 목적지 서버로 가는 네트워크 경로를 확인해주는 명령어

< chmod 775 [파일이름]>
- 파일 권한 변경

< ping 사용 >
- #echo (A) /proc/sys/net/ipv4/icmp_echo_ignore_all
- ignore : 무시하다
- 즉, (A)에 들어갈 값은 ping 무시인 경우 1, ping 응답인경우 0으로 하면 됨

[단답형 및 선택형]

< ICMP : Internet Control Message Protocol >
- 인터넷 제어 메시지 프로토콜
- L2와 L3사이에서 에러보고를 하는데 사용됨
- 운영체제에서 오류 메시지를 전송 받는데 사용됨
- 즉, 시스템간 자료를 주고받는 TCP , UDP와는 성질이 다름
- Ping , Tracert 명령이 대표적인 ICMP 명령어이다.
- 메시지 타입 : 0, 8, 11, 3, 4, 5
8 : Echo Request 요청
0 : Echo Reply 응답
3 : Destinaction Unreachable. (도달할 수 없는 목적지에 패킷보낼때의 에러 메시지)
4 : Source Quench (발신제안. 서버 불안정시 전송 중단하라는 에러 메시지)
5 : Redirect (라우트 변경. 라우터의 목적지 설정보다 더 짧은 경로가 존재함을 알리고자 하는 메시지)
11 : Time exeeded (TTL 로, 타임초과 에러메시

지)

< IPsec >
- 인터넷 가상의 전용회선을 데이터 도청하는 행위를 방지하기 위한 보안 통신규약
- 3 계층에서 동작하는 AH (인증헤더) 와 ESP (캡슐 보안 페이로드) 프로토콜로 구성됨
- 구성 정보
1. AH : ip패킷에 대한 인증 제공
2. ESP : IP 패킷에 대한 인증 및 암호 캡슐화 제공
3. SA : IPsec 서비스 구현시 암호화 및 인증에 사용할 요소 정의

< VPN >
- 인토넷망과 같은 공중망을 사설망처럼 이용해 회선 비용을 크게 절감할 수 있는 기업통신 서비스

< VLAN >
- 물리적인 네트워크 구성에 제한 받지 않고 네트워

크 구성요소가 삭제되었을 때 논리 네트워크를 구성함으로써 유연하게 대응하는 기술
- 스위칭 이라는 LAN기반으로 가상이라는 개념을 도입해 네트워크 구성에 대한 지리적 제한을 최소화하면서 사용자가 원하는 최대한의 논리적 네트워크를 구성할 수 있도록 수단을 제공하는 기술
- vtp에서의 v가 vlan을 의미한다.
- vtp(VLan Trunking Protocol) : 연결된 스위치들끼리 VLan 정보를 주고받아 자동으로 동기화하는 프로토콜

< 포트 미러링 >
- 네트워크 스위치의 어떤 포트에서 보이는 모든 네트워크 패킷이나 전체 VLAN 의 패킷들을 다른 모니터링 포트로 복제하는데에 사용되는 것

< 방화벽 : Firewall >
- 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템

< 웹 방화벽 : WAF >
- 웹 서비스와 주고받는HTTP 트래픽을 필터링, 모니터링 및 차단하는 특정 형태의 애플리케이션 방화벽

< SNMP >
- 매니지먼트와 에이전트 사이에 관리 정보를 주고받기 위한 프로토콜
- 정보교환 단위는 메시지이다.

< NAT >
- IP 주소를 효율적으로 사용하기 위해 사설IP주소를 공인 IP주소 로 변환해주는 기술

< DHCP >
- 네트워크에 연결된 장치에 IP주소를 자동 할당하기 위해 사용되는 네트워크 관리 프로토콜

< SSL >
- 브라우저 사이에 전송되는 데이터를 암호화하여 인터넷 연결을 보호하기 위한 기술
- 즉, 네트워크로 데이터 송수신 시 그 내용을 암호화함(HTTPS와 연관)

< SSH >
- 원격 접속시 암호화 기술통해 보안화된 환경에서 다른 호스트로 접속

< HTTPS >
- 인증서 기반으로 암호화된 데이터를 전송하는 프로토콜
- 웹 사이트가 SSL/TLS 인증서로 보호되는 HTTP 통신하는 프로토콜이다.

< TCP 특징 >
- 연결성
- 신뢰성

- 송수신 동일
- sliding window 방식으로 데이터 크기 조절
- ack 이용해 3-handshake 연결

< TCP/IP 네트워크 프로토콜 종유 >
1. 네트워크 연결 (물리, 데이터 링크)
2. 네트워트 (네트워크)
- ICMP, ARP, RARP, RIP, OSPF, IPsec, IGMP, BGP
3. 전송 (전송)
4. 응용 (세션, 표현, 응용)
- SMTP, TELNET, FTP, HTTP

< RIP와 OSPF >
1.RIP
  거리 벡터 라우팅 프로토콜
  벨만 포드 알고리즘
  최대 홉수 15
  인접 라우터와 주기적 정보 교환
  RIPv1은 브로드캐스트 이용해 라우팅 업데이트
  RIPv2은 멀티캐스트 이용해 라우팅 업데이트
2.OSPF

링크 상태 라우팅 프로토콜
다익스트라 알고리즘
홉수 제한 없음
최단경로, 최소 지연, 최대 처리량
하나의 AS를 여러개의 작은 Area 로 나누어 계층적 라우팅 수행

< 라우터 >
- 브릿지와 같이 서로 다른 네트워크 대역간 통신을 지원

< 브릿지 >
- 데이터링크 계층에서 두 세그먼트 사이에서 데이터 링크 계층간 패킷 전송을 담당

< RFID : 무선 인식 기술 >
- 무선 주파수로 물건이나 사람을 식별하는 인식 기술
- RFID태그 가 데이터를 안테나 이용해 리더로 전달하고 호스트가 받아서 본다.

< IPS >
- 네트워크 공격 서명을 찾아내서 자동으로 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션

< 오용탐지기법 >
- 이미 발견되어있는 공격 패턴을 미리 입력하고, 해당하는 패턴을 탐지하는 기법

< 스푸핑 >
- 웹사이트에서 눈속임을 이용해 이용자의 정보를 빼가는 해킹수법

< RAM >
- 휘발성 메모리로, ROM 보다 속도가 빠르다.
- 라우터에도 RAM 이 사용되며 IOS운영체제와 라우팅 테이블이 저장된다.
- DRAM : 동적 RAM으로, 재충전이 필요하며 구조가 간단해 용량이 크고 전력소모가 적다.

- SRAM : 정적 RAM으로, DRAM보다 빠르며 재충전이 없어 계속 전력을 공급시킬 수 있어 용량이 작다.
- cpu의 캐쉬 메모리로 SRAM 이 많이 사용된다.

< NV RAM >
- 비휘발성 메모리를 총칭하는 것으로, 별도 배터리가 있어 전원이 꺼져도 데이터를 유지한다.
- 라우터에도 사용되며 구성파일이 주로 저장되어 라우터가 켜지면 RAM으로 올라와 구성파일대로 움직이게 한다.
- 전원 여부와 상관없이 정보를 저장한다.
- m.2 nvme 나 sata 같은 SSD가 NVRAM이다.

< Flash >
- 라우터를 움직이는 IOS 운영체제가 저장되는 메모리
- 전원이 꺼져도 지워지지 않은 메모리
-NVRAM 보다 용량이 크다(NVRAM은 구성파일만 저장하기 때문에)

- 라우터 전원 켜지면 운영체제는 RAM으로 올라가고, 전원 꺼지면 플래시 메모리에 머무른다.

< ROM >
- 라우터가 켜졌을 때 어디서 운영체제를 가져오고 어떤 순서로 상태를 점검하는지에 대한 내용이 저장된다.
- 즉, pc켜지면 메모리 얼마고, 하드가 몇메가고를 계산하는 역할을 한다.
- ROM 이 먼저 동작 '-> NVRAM에서 구성파일 RAM에 적재 -> Flash 에서 운영체제 꺼내서 RAM 적제

< UTM >
- 통합 위협 관리
- 여러 보안 기능과 서비스가 네트워크 내의 단일 장치로 통합되는 것을 의미한다.
- 바이러스 방지, 콘텐츠 필터링, 스팸 방지 기능을 통해 네트워크 사용자를 보호한다.
- IPS 침입방지 와 IDS 침입탐지 기능 제공

< 피씽 : fishing >
- 불특정 다수의 이메일 사용자에게 거짓 이메일 보내 낚는 방법