10장

Network 및 보안 관리하기

전체 내용

Network Interface 정보 이해

Network Interface 구성

Network 상태 확인

방화벽 관리 및 보안 관리도구

1 – Network Interface 정보 이해

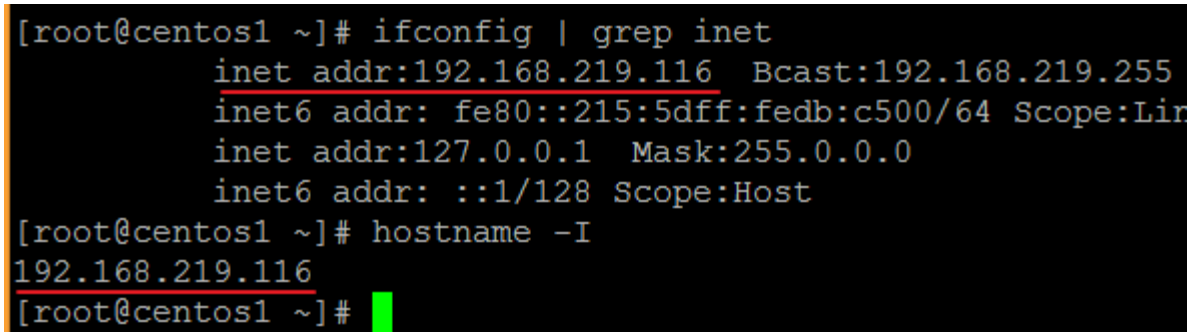
IP Address

Netmask

Port No

1 – Network Interface 정보 이해

- IP Address
  - Network ID + Host ID
  - IP Address는 전화 번호 체계와 비슷하다
  - 전화번호 = 국번 + 전화 번호
  - 국번이 같은 전화 번호는 같은 동네에 있듯이 Network ID가 같은 IP Address는 같은 Network에 존재한다
  - IP Address 확인하기
    - **ifconfig**
    - **ifconfig eth0**
    - **ifconfig eth0 | grep inet**
    - **hostname -I** (##대문자 i)



1 – Network Interface 정보 이해

- Netmask
  - Netmask는 Network ID와 Host ID를 구분하는 기준이다
  - IP Address Class별로 기본 Netmask가 있지만 필요에 따라 변경 가능
  - Netmask 확인하기
    - Ifconfig

```
[root@centos1 ~]# ifconfig
eth2      Link encap:Ethernet  HWaddr 00:15:5D:DB:C5:00
          inet addr:192.168.219.116  Bcast:192.168.219.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fedb:c500/64 Scope:Link
```

  - 예
    - **192.168.100**.10/24와 **192.168.100**.190/24는 Local Network에 존재하므로 Router의 도움 없이 통신이 가능하다
    - **192.168.10**.20/24와 **192.168.30**.127/24는 다른 Network ID를 가지므로 Router의 도움으로 통신할 수 있다(또는 수동 구성으로도 가능)

1 – Network Interface 정보 이해

- Port No.
  - 하나의 집 주소를 갖는 어떤 빌딩에 입점한 가게들을 구분하는 기준이 호수 번호이다
    - 울산 광역시 북구 신천동 181번지 **102호: 은행**
    - 울산 광역시 북구 신천동 181번지 **301호: 학원**
    - 이렇게 해야지 우편물이 정확히 배달된다
  - 각 서비스별로 고유한 Port 번호가 배정되어 있다
    - **/etc/services** 에서 확인할 수 있다
    - 네트워크 프로그램 개발자는 이 파일을 확인한 후 겹치지 않는 Port no를 사용해야 한다
    - ssh server: 22, web server: 80, ftp server: 20,21
    - 원하는 포트 번호를 찾기 위해
      cat /etc/services | grep ssh

```
[root@centos1 ~]# cat /etc/services | grep ssh
ssh             22/tcp
l
ssh             22/udp
l
x11-ssh-offset  6010/tcp
ssh             22/sctp                 # SSH
```

2 – Network Interface 구성

- Hostname 설정하기
- Network Interface 설정하기
- /etc/sysconfig/network-scripts/ifcfg-eth0 파일 이해
- Gateway 설정하기
- DNS 설정하기

2 – Network Interface 구성

- Hostname 설정하기
  - 시스템 이름 확인하기
    - **hostname**
    - **uname -n**
    - **cat /etc/sysconfig/network** (## CentOS)
    - **cat /etc/hostname** (## Ubuntu)

```
[root@centos2 ~]# hostname
centos2
[root@centos2 ~]# uname -n
centos2
[root@centos2 ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=centos2
[root@centos2 ~]# hostname os2
[root@centos2 ~]# hostname
os2
[root@centos2 ~]# uname -n
os2
[root@centos2 ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=centos2
```

  - 호스트 이름 변경하기
    - **임시적으로** 변경하기
      hostname *newname*
    - **영구적으로** 변경하기 (시스템 재시작 후 적용된다)
      vi /etc/hostname
    - **vi /etc/sysconfig/network** (## CentOS 6.x)

2 – Network Interface 구성

- Network Interface 설정하기
  - IP Address 확인하기
    - **ifconfig**
    - **ifconfig eth0**
    - **ip addr show**
  - **임시적으로** Interface를 Disable & Enable하기
    - **ifconfig eth0 down**
      ip link set eth0 down
    - **ifconfig eth0 up**
      ip link set eth0 up
  - **임시적으로** IP Address 설정하기 (##CentOS)
    - **ifconfig eth0 192.168.219.120 netmask 255.255.255.0 broadcast 192.168.219.255**
    - **ip addr add 192.168.50.5 dev eth0**
      ** 이렇게 설정한 후 재부팅하거나 service network restart를 실행하면 /etc/sysconfig/network-scripts/ifcfg-eth0의 설정으로 복귀된다

2 – Network Interface 구성

- Network Interface 설정하기
  - **임시적으로 특정한** IP Address **제거하기** (##CentOS)
    - **ip addr del 192.168.50.5/24 dev eth0**
  - **임시적으로 모든** IP Address **제거하기** (##CentOS)
    - **ip addr flush dev eth0**

2 – Network Interface 구성

- Network Interface 설정하기(계속)
  - IP Address **영구적으로** 설정하기 (##CentOS)
    - **vi /etc/sysconfig/network-scripts/ifcfg-eth0**
    - **BOOTPROTO=static**
      ONBOOT=yes
      IPADDR=192.168.219.115
      NETMASK=255.255.255.0
      NETWORK=192.168.219.0
      BROADCAST=192.168.219.255
      GATEWAY=192.168.219.1
      DNS1=8.8.8.8
  - 변경된 내용 적용하기 이해 Network Service 재시작하기
    - **service network restart**

2 – Network Interface 구성

- Network Interface 설정하기(계속)
  - IP Address 영구적으로 설정하기 (##Ubuntu)
    - **vi /etc/network/interfaces**
    - **auto eth0**
      iface eth0 inet static
      address 192.168.219.222
      netmask 255.255.255.0
      network 192.168.219.0
      broadcast 192.168.219.255
      gateway 192.168.219.1
  - 변경된 내용 적용하기 위해 Network Service 재시작하기 (##Ubuntu)
    - **sudo service networking restart**
      또는 **sudo /etc/init.d/networking restart**
    - 이것이 실패하면 시스템을 재부팅한다
      sudo shutdown –r now

2 – Network Interface 구성

- Network Interface 설정하기(계속)
  - **DHCP Server에서** IP Address 자동으로 받기 **(##CentOS)**
    - **vi /etc/sysconfig/network-scripts/ifcfig-eth0**
    - **BOOTPROTO=dhcp**
      ONBOOT=yes
      ** 나머지 부분은 모두 #으로 입력하여 주석으로 처리하여 둔다
      ** ONBOOT는 부팅할 때 자동으로 해당 NIC를 사용하도록 설정
  - DHCP Server에서 IP Address 자동으로 받기 **(##Ubuntu)**
    - **vi /etc/network/interfaces**
    - **auto eth0**
      iface eth0 inet dhcp

2 – Network Interface 구성

- /etc/sysconfig/network-scripts/ifcfg-eth0 파일 이해

```
DEVICE=eth0  #장치명: 첫 번째 이더넷카드
BOOTPROTO=static  #IP 할당 방식 결정: static 은 고정 IP, dhcp 는 자동 IP
HWADDR=XX:XX:XX:XX:XX:XX  #이더넷카드의 MAC 주소
NM_CONTROLLED=no  #GUI 모드에서의 편리한 네트워크설정 허용
ONBOOT=yes  #시스템 시작시 자동으로 해당 인터페이스를 활성화 여부 결정
TYPE=Ethernet  #Layer2 프로토콜 지정
UUID=XXXXXXX-XXX-XXX-XXX-XXXXXXX  #네트워크상에 유일한 장치로서 구분하기 위한
식별자로 사용, 자동 할당함
PEERDNS=yes  #DHCP 사용시 Name Server 를 DHCP 에서 받아온 것의 사용 여부
PEERROUTES=yes #DHCP 사용시 Default Gateway 를 DHCP 에서 받아온 것의 사용 여부
DEFROUTE=yes  #이 인터페이스를 Default Route 지정 여부 결정.이것을 yes 로 하면 다른
Interface 들은 모두 no 로 설정해야 한다
IPADDR=192.168.219.100  #IP 주소 지정
NETMASK=255.255.255.0  #subnet mask 지정
NETWORK=192.168.219.0  #network ID 지정
BROADCAST=192.168.219.255  #broadcast IP 지정
GATEWAY=192.168.219.1 #Default Gateway IP 지정
DNS1=8.8.8.8  #DNS Server 수동 지정
ETHTOOL_OPTS=wol g  #Wake On Lan 기능 활성화
USERCTL=no  #root 가 아닌 사용자의 eth0 on/off 제어 가능 여부
IPV6INIT=no  #IPV6 사용여부
```

2 – Network Interface 구성

- Gateway 설정하기
  - 대상 컴퓨터가 Remote Network에 있을 때는 네트워크 경로를 입력해주어야 한다
  - Remote Network 정보를 일일이 입력하지 않을 때는 Default Gateway만 설정하면 Router가 알아서 처리해 준다
  - Default Gateway 설정 보기- **Global 설정(영구적)**
    - 이 설정은 각 NIC 별로 설정하는 것이 아니고 모든 NIC에 동시에 적용된다
    - Global setting을 하지 않으면 각 NIC 별로 설정하면 된다
    - **cat /etc/sysconfig/network**
    - **vi /etc/sysconfig/network**
      내용 수정
      service network restart

```
[root@centos2 adminuser]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=centos2
GATEWAY=192.168.219.1
[root@centos2 adminuser]#
```

  - Default Gateway 설정의 우선 순위
    - 각 인터페이스에서의 GATEWAY 설정(/etc/sysconfig/network-scripts/ifcfg-eth0)과 Global 설정(/etc/sysconfig/network)이 겹치면 각 인터페이스 설정이 적용된다

2 – Network Interface 구성

- Gateway 설정하기-**임시 설정**
  - Routing Table **내용 보기**
    - **route –n**
      netstat –nr
      ip route show

route	
기능	라우팅 테이블을 편집하고 출력한다.
형식	route 명령
명령	add : 라우팅 경로나 기본 게이트웨이를 추가한다. del : 라우팅 경로나 기본 게이트웨이를 삭제한다.
사용 예	route route add default gw 192.168.0.1 dev eth0

  - Routing Table에 **Default Gateway 정보 추가하기**
    - **route add default gw 192.168.219.1**
    - **ip route add default via 192.168.219.1**
    - **route -n**
    - service network restart를 하면 /etc/sysconfig/network 또는 etc/sysconfig/network-scripts/ifcfg-eth0의 설정이 적용된다
  - Default Gateway 삭제하기
    - **route del default gw 192.168.219.1**
    - **ip route del default via 192.168.219.1**

2 – Network Interface 구성

- Routing Table 편집하기
  - Routing Table 편집하기-**임시적**

기능	명령 형식과 사용 예
라우팅 경로 추가(네트워크)	route add –net 네트워크 주소 netmask 넷마스크 dev 인터페이스명 route add –net 192.168.1.0 netmask 255.255.255.0 dev eth0
라우팅 경로 추가(호스트)	route add –host 호스트 주소 dev 인터페이스명 route add –host 192.168.1.5 dev eth0
라우팅 경로 제거(네트워크)	route del –net 네트워크 주소 netmask 넷마스크 [dev 인터페이스명] route del –net 192.168.1.0 netmask 255.255.255.0
라우팅 경로 제거(호스트)	route del –host 호스트 주소 route del –host 192.168.1.5
기본 게이트웨이 추가	route add default gw 게이트웨이 주소 dev 인터페이스명 route add default gw 192.168.1.1 dev eth0
기본 게이트웨이 제거	route del default gw 게이트웨이 주소 route del default gw 192.168.1.1
루프백(lo) 추가	route add –net 127.0.0.0 netmask 255.0.0.0 dev lo

- 특정한 Network **경로 추가**
  route add –net 192.168.1.0 netmask 255.255.255.0 dev eth0
  ip route add 192.168.1.0/24 via 192.168.1.1 dev eth0
- 특정한 Network **경로 제거**
  ip route del 192.168.1.0/24
- 특정한 Host **경로 추가**
  route add –host 192.168.1.100 dev eth0
- 특정한 Network에 **접근 불가**
  route add –net 192.168.1.0 netmask 255.255.255.0 reject
- 특정한 Host에 **접근 불가**
  route add –host 192.168.1.111 reject

2 – Network Interface 구성

- Gateway 설정하기(계속)
  - Routing Table에 특정한 네트워크 정보 추가하기-**영구적**
    - **CentOS**
      - /etc/sysconfig/network-scripts/**route-eth0**에서 다음 내용을 추가한다
        192.168.1.0/24 via 192.168.1.1 dev eth0
        default via 192.168.219.1 (## default gateway를 영구적으로 지정)
    - **Ubuntu**
      - /etc/network/interfaces에서 다음 내용을 추가한다
        up ip route add 192.168.1.0/24 via 192.168.1.1 dev eth0
    - 이렇게 수정한 후 **service network restart**를 하여 적용시킨다

2 – Network Interface 구성

- Gateway 설정하기(계속)
  - Routing Table을 수정하여 테스트하기-**임시적**
    - /etc/sysconfig/network-scripts/ifcfg-eth0에서 수동으로 GATEWAY정보를 입력한 것과 route add default gw로 입력한 것 중에서 충돌나면 파일의 내용이 우선한다.
    - **service network restart**를 하면 명령어로 입력한 것이 사라진다

```
[root@centos2 ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.219.0   *               255.255.255.0   U     1      0        0 eth2
[root@centos2 ~]# ping 8.8.8.8
connect: Network is unreachable
[root@centos2 ~]# route add default gw 192.168.219.1 dev eth2
[root@centos2 ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.219.0   *               255.255.255.0   U     1      0        0 eth2
default         192.168.219.1   0.0.0.0         UG    0      0        0 eth2
[root@centos2 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=42 time=93.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=42 time=75.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=42 time=69.1 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2279ms
rtt min/avg/max/mdev = 69.143/79.390/93.679/10.421 ms
[root@centos2 ~]# service network restart
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Active connection state: activated
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/5
                                                           [  OK  ]
[root@centos2 ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.219.0   *               255.255.255.0   U     1      0        0 eth2
[root@centos2 ~]#
```

2 – Network Interface 구성

- DNS 설정하기
  - Name Resolution하는 순서
    - **/etc/hosts**
    - **/etc/resolv.conf**

```
[root@centos2 network-scripts]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 1.214.68.2
nameserver 61.41.153.2
```

    ** 질의하는 DNS Server가 등록되어 있음
  - Name Resolution을 위한 **/etc/resolv.conf** 파일 수정하기- **Global 설정**
    - **echo "nameserver 207.62.187.54" > /etc/resolv.conf**
  - /etc/sysconfig/network-scripts/ifcfg-eth0에서 DNS1=8.8.8.8, DNS2=8.8.4.4로 설정하면 이것이 /etc/resolv.conf 설정보다 우선한다
  - Name Resolution이 제대로 되는지 확인하기
    - **nslookup**
    - **nslookup powershell.kr**

```
[root@centos2 network-scripts]# nslookup
> www.choongshin.or.kr
Server:         1.214.68.2
Address:        1.214.68.2#53

Non-authoritative answer:
Name:   www.choongshin.or.kr
Address: 210.118.26.172
> powershell.kr
Server:         1.214.68.2
Address:        1.214.68.2#53

Non-authoritative answer:
```

3 – Network 상태 확인

- Ping 테스트하기
- 통신 경로 확인하기
- Network 상태 정보 확인하기
- Nc(NetCat) 프로그램 사용하기

3 – Network 상태 확인

- Ping 테스트하기
  - Ping 명령은 두 컴퓨터간의 Layer3까지 통신이 되는지 확인하는 것이다
    - 즉, 원격 컴퓨터까지의 경로를 찾아서 통신할 수 있는지 확인하는 것이다
    - Ping이 성공하면 원격 컴퓨터가 켜져 있다는 뜻이지만, 그렇다고 해서 원격 컴퓨터의 서비스(web,ftp)에 접속할 수 있다는 보장을 제공하지는 않는다
  - 다양한 Ping 테스트
    - 아무 옵션 없이 사용하기: 종료하기 전까지 ping을 한다
      ping www.google.com
    - 통신이 되면 삐 소리를 내게 한다: **-a** 옵션
      ping –a www.google.com
      종료하려면 CTRL+C로 한다
    - 보낼 Packet 수량을 지정한다: **-c 숫자** 옵션
      ping –c 3 www.google.com
    - 아무 메시지도 표시하지 않게 하며 CTRL+C 로 종료할 때 요약 정보만 보여주기: **-q** 옵션
      ping –q www.google.com

3 – Network 상태 확인

- 통신 경로 확인하기
  - Traceroute를 사용하여 원격 컴퓨터에 도달할 때까지 통과하는 router 정보를 확인하다
    - 인터넷이 안될 때 중간에 통과하는 라우터의 고장 유무를 확인한다
    - 네트워크 정보를 알 수 있다
    - whois 명령어를 사용하면 중간에 나타나는 Router 주소를 통하여 어떤 업체를 통과하는 알 수 있다
  - Tracerout 사용하기
    - 원격 컴퓨터까지 통신할 때 어떤 Router를 통과하는지 확인하기
      traceroute www.google.com
    - 중간에 어떤 회사 네트워크를 통과하는지 확인하기
      yum install jwhois –y
      whois 211.53.88.185

3 – Network 상태 확인

- 네트워크 상태 정보 출력하기
  - netstat를 사용하여 다음 내용을 알 수 있다
    - 네트워크 연결 상태, 라우팅 테이블 정보
    - 인터페이스 관련 통계 정보 및 현재 시스템에 열려 있는 포트

netstat

기능	네트워크의 상태 정보를 출력한다.
형식	netstat [옵션]
옵션	-a : 모든 소켓 정보를 출력한다. -r : 라우팅 정보를 출력한다. -n : 호스트명 대신에 IP 주소를 출력한다. -i : 모든 네트워크 인터페이스 정보를 출력한다. -s : 프로토콜별로 네트워크 통계 정보를 출력한다. -p : 해당 소켓과 관련된 프로세스의 이름과 PID를 출력한다.
사용 예	netstat -rn netstat -s

  - 라우팅 테이블 내용 확인하기: **-r** 옵션
    - **netstat –r**
      ip route
    - **netstat –rn**
      (## n을 사용하면 이름 대신 IP 주소로 나타낸다)

3 – Network 상태 확인

- 네트워크 상태 정보 출력하기
  - 현재 열려 있는(서비스 하고 있는) 포트 확인: **-a** 옵션
    - **netstat –a**
    - **netstat –an**
      netstat –an | grep LISTEN (##강추)
      (## n을 사용하면 이름 대신 IP 주소로 나타낸다)
  - 현재 시스템에 연결된 컴퓨터 확인(connected): **-p** 옵션
    - **netstat –p**
    - **ss (##강추)**
  - 인터페이스별로 네트워크 통계 정보 확인하기: **-i** 옵션
    - **netstat –i**
      ip –s link
  - Protocol 별로 네트워크 통계 정보 확인하기: **-s** 옵션
    - **netstat –s**

3 – Network 상태 확인

- Nc(netcat) 프로그램 사용하기
  - nc 프로그램의 기능 요약
    - 원격 컴퓨터의 특정한 포트가 열려있는지 확인(서비스 여부 확인)
    - 로컬 컴퓨터에 특정한 포트를 Listening하도록 설정(방화벽에 특정한 포트 차단 여부 확인)
  - nc 프로그램 설치하기
    - **yum search nc**
    - **yum –y install nc.x86_64**
  - nc 프로그램 사용하기- **Listening하고 있는 Port 검사**
    - 원격 컴퓨터에 특정한 TCP 포트(80)가 열려 있는지 확인하기
      nc -zv www.google.com 80
    - 원격 컴퓨터에 어떤 TCP 포트(범위 지정)가 열려있는지 확인하기
      nc -zv www.choongshin.or.kr 20-80
    - 원격 컴퓨터에 특정한 UDP 포트(80)가 열려 있는지 확인하기
      nc –zu www.google.com 80
    - 원격 컴퓨터에 어떤 UDP 포트(범위 지정)가 열려있는지 확인하기
      nc –zu www.choongshin.or.kr 20-80

3 – Network 상태 확인

- Nc(netcat) 프로그램 사용하기
  - nc 프로그램 사용하기-**임시로 Port Listening하도록 설정**
    - 로컬 네트워크에 MySQL Database Server(1433 포트 사용)가 있는데, 원격에서 이 서버에 접속을 할 때 Firewall에서 차단하고 있는지 확인할 때 로컬 네트워크에 있는 리눅스에서 **nc –l**을 사용하면 유용하다
    - **DB Server와 같은 네트워크에 있는** Linux System에 가상으로 1433포트는 Listening 상태로 만들어 놓고 외부 컴퓨터에서 TCP 1433 포트로 접속이 되면 중간에 있을 것 같은 Firewall에서 1433 포트가 차단되지 않았다는 것을 증명한다
    - MySQL DB가 설치되지 않은 리눅스 시스템에 Tcp 1433 포트를 임시적으로 Listening하도록 설정하기
      service iptables stop (## 실습을 위해서 잠깐 동안 방화벽 끔)
      nc –l 1433

3 – Network 상태 확인

- Nc(netcat) 프로그램 사용하기
  - nc 프로그램 사용하기-**임시로 Port Listening하도록 설정**
    - **윈도우 컴퓨터에** tcp 포트에 ping을 하는 tcping.exe 프로그램을 설치한다
      - Tcping.exe을 다운로드하여 c:\windows\system32에 복사한다

    - 리눅스 컴퓨터랑 통신해본다
      tcping 192.168.1.116 1433
      이것이 성공하면 중간에 Firewall에서 1433 포트를 차단하지 않은 것이다

```
PS C:₩Windows₩system32> tcping 192.168.1.116 1433

Probing 192.168.1.116:1433/tcp - Port is open - time=5.376ms
Probing 192.168.1.116:1433/tcp - Port is open - time=1.545ms
```

    - **다른 리눅스에서 원격 컴퓨터에** 1433 포트가 열려있는지 확인한다
      nc –z 192.168.1.115 1433

```
[root@centos2 adminuser]# nc -z 192.168.1.116 1433
Connection to 192.168.1.116 1433 port [tcp/ms-sql-s] succeeded!
[root@centos2 adminuser]#
```

4 – 방화벽 관리 및 보안 관리 도구

방화벽 관리하기

보안 관리도구 사용하기

방화벽 관리하기

- 방화벽이 필요한 이유
  - Log는 시스템의 상태를 알려 주는 것으로서 이미 문제가 발생한 이후의 기록을 보는 것이다
    - Log는 사전에 외부의 공격을 차단할 수는 없다
    - 그래서 외부 공격을 지연하거나 차단하기 위해서 방화벽(Firewall)이 필요하다
  - centos6.x까지는 iptables라는 방화벽 서비스를 사용했지만 centos7.x부터는 firewalld를 도입하였다
    - centos7.x에서 firewalld를 중지하고 iptables를 사용할 수 있는 있지만 권장하지는 않는다
  - 방화벽이 켜져 있으면 시스템 접근이 모두 차단되지만, 시스템의 특정한 service에 접근을 허용하기 위해서는 service 및 port no.를 추가하면 된다

방화벽 관리하기

- 방화벽 설정 순서
  1) Firewall Rule 생성하기
  2) Zone 속성 변경하기
  3) Network Interface를 Zone에 할당하기

- 생성한 Rule 적용 방법
  - Immediate(RunTime)
    - rule 생성 및 편집하면 곧장 적용되는 것
    - 하지만 시스템 재시작하면 설정한 것이 해제되므로 주의한다
    - 방화벽 설정을 잘못한 경우에 시스템을 재시작하면 원상 복귀되기 때문에 문제 해결에 도움이 되기도 한다
  - Permanent
    - 시스템 원상 복귀되더라도 계속 rule을 적용할 때 사용한다

방화벽 관리하기

- 방화벽 동작 확인하기
  - 방화벽 서비스의 이름은 firewalld.service이다. 이 방화벽이 실행중인지 확인하려면 다음과 같이 하면 된다
    - **systemctl list-unit-files | grep firewall**
    - **systemctl status firewalld.service**
    - **firewall-cmd --state**

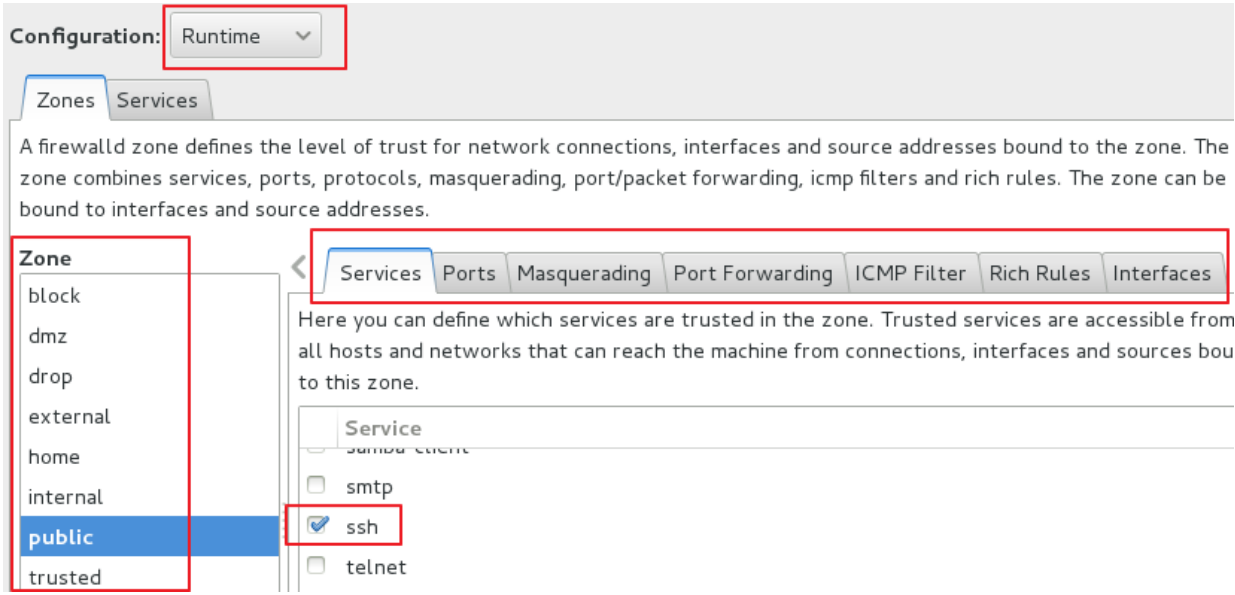
```
[root@centos1 ~]# systemctl list-unit-files | grep firewall
firewalld.service                           enabled
[root@centos1 ~]# systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since Tue 2015-12-08 05:07:43 KST; 3h 8min ago
 Main PID: 763 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─763 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Dec 08 05:07:43 centos1 systemd[1]: Started firewalld - dynamic firewall daemon.
[root@centos1 ~]# firewall-cmd --state
running
```

  - 방화벽을 중지하고 시작할 수 있다
    - **systemctl stop firewalld**
    - **systemctl start firewalld**

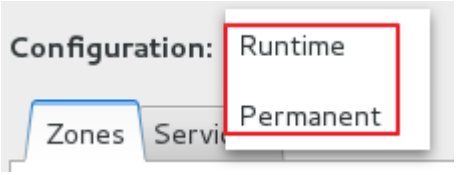
방화벽 관리하기

- GUI 도구로 방화벽 설정하기
  - Firewalld는 동적으로 방화벽을 관리하며, IPv4와 IPv6 모두 지원한다
  - 방화벽을 동적으로 관리한다는 뜻은....
    - 언제든지 방화벽의 설정을 변경할 수 있다는 것이다
    - 방화벽의 변경 내용을 실행하기 위해서 별도로 변경 내용을 저장하고 적용하는 과정이 필요 없다는 것이다
    - 방화벽을 다시 실행하기 위해 기존의 네트워크 연결이 중단되는 일이 없다
  - 방화벽의 GUI 관리도구를 실행하기
    - **firewall-config &**

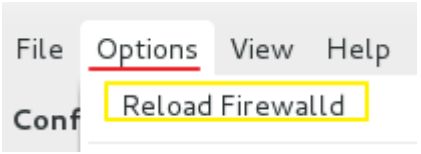


방화벽 관리하기

- GUI 도구로 방화벽 설정하기
  - 방화벽의 GUI 관리도구를 실행하기
    - current view



      - **Runtime**: 서비스나 포트 등의 항목을 변경했을 때 즉시 적용된다. 하지만 이렇게 하는 경우에 접속하여 시스템을 사용하는 사용자에게 영향을 줄 수 있으므로 주의가 필요하다
      - **Permanent**: 설정 변경한 내용을 적용하기위해서는 firewalld를 재시작하거나 system을 재시작해야 한다
        - **systemctl restart firewalld**
        - **reboot**



방화벽 관리하기

- GUI 도구로 방화벽 설정하기
  - 방화벽의 GUI 관리도구를 실행하기
    - zone
      - 네트워크를 신뢰도 수중에 따라 여러 개의 zone으로 구분하여 사용할 수 있다
      - 여러 개의 zone 중에서 하나 만을 선택하여 사용할 수 있다
      - zone은 관리자가 추가 삭제할 수 있다
      - **block:** 모든 네트워크 접속 요청이 거부된다
      - **drop:** 모든 접속 요청이 거부되고, 응답도 하지 않는다. 내부에서 외부로 접속하는 것만 가능하다

      - **dmz:** dmz로 구분된 영역에 있는 컴퓨터만 공개적으로 접근이 가능하다
      - **external:** [외부 네트워크]를 사용하는 zone으로 선택된 서비스만 접속을 허용
      - **internal:** [내부 네트워크]를 사용하는 zone으로 선택된 서비스만 접속을 허용

      - **public**: untrusted network에 있는 모든 컴퓨터에서 접속이 가능하다
      - **trusted**: trusted zone에 있는 모든 컴퓨터로부터의 연결을 허용한다
      - **home:** [home zone]를 사용하는 zone으로 선택된 서비스만 접속을 허용
      - **work**: [work zone]를 사용하는 zone으로 선택된 서비스만 접속을 허용

방화벽 관리하기

- Interface에 zone 설정하기
  - 특정한 NIC에 zone을 설정하여 방화벽 설정에 적용을 받게 한다
  - 현 세션에 대하여 임시적 설정
    - **firewall-cmd --zone=home --change-interface=eth0**
    - **firewall-cmd --get-active-zones**
    - 하지만 firewalld를 재시작하면 원상 복구된다
      - **systemctl restart firewalld.service**
      - **firewall-cmd --get-active-zones**
  - 영구적 설정
    - *vi /etc/sysconfig/network-scripts/ifcfg-eth0*
      - DNS1=8.8.8.8
      - DNS2=8.8.4.4
      - **ZONE=home**
    - **systemctl restart network.service**
    - **systemctl restart firewalld.service**

방화벽 관리하기

- 방화벽 관리하는 명령어
  - 허용하는 서비스 목록 보기
    - **firewall-cmd --list-services**
  - **서비스 추가하기**
    - firewall-cmd --add-service=http
    - firewall-cmd --list-services
  - 서비스 **삭제하기**
    - firewall-cmd --remove-service=telnet
    - firewall-cmd --list-services
  - **포트 추가하기**
    - firewall-cmd --add-port=5000/tcp
    - firewall-cmd --add-port=5000/udp
    - firewall-cmd --list-services
  - 포트 **삭제하기**
    - firewall-cmd --remove-port=5000/tcp
    - firewall-cmd --remove-port=5000/udp

방화벽 관리하기

- 방화벽 관리하는 명령어
  - Permanent 옵션 사용하기
    - --permanent 옵션은 바로 적용되지는 않지만 방화벽에 설정 내용을 저장한다
    - 이 옵션으로 지정한 항목을 적용하려면 reload를 하거나 firewalld를 다시 시작해야 한다
    - 방화벽에서 telnet 서비스 허용을 runtime으로 바로 적용하기와 저장하기를 함께 실행하려면 다음과 같이 한다
      - firewall-cmd --add-service=telnet (##즉각 적용)
      - firewall-cmd **--permanent** --add-service=telnet (##방화벽 재시작 후에 적용)
      - 이렇게 하면 방화벽 즉각 적용 및 시스템 재시작 후에도 계속 적용이 된다

방화벽 관리하기

- 방화벽 구성하기-1
  - 방화벽 켜기
    - **firewall-cmd** --state
    - systemctl start firewalld.service
  - 현재 방화벽 구성 상태 확인하기
    - **firewall-cmd** --get-default-zone
    - **firewall-cmd** --get-active-zones
      - 실제 방화벽이 적용된 NIC는 eth0이며, public zone 구성이 할당되어 있다

```
[root@centos1 ~]# firewall-cmd --get-default-zone
public
[root@centos1 ~]# firewall-cmd --get-active-zones
public
  interfaces: eth0
```

  - Default zone(public zone) 구성 내용 알아보기
    - firewall-cmd --list-all

```
[root@centos1 ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

방화벽 관리하기

- 방화벽 구성하기-1
  - 사용 가능한 모든 zone 조사하기
    - **firewall-cmd** --get-zones

```
[root@centos1 ~]# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

  - 특정한 zone(home zone)의 구성 내용 알아보기
    - **firewall-cmd --zone=home** --list-all

```
[root@centos1 ~]# firewall-cmd --zone=home --list-all
home
  interfaces:
  sources:
  services: dhcpv6-client ipp-client mdns samba-client ssh
  ports:
  masquerade: no
```

  - 사용 가능한 모든 zone의 구성 내용 한꺼번에 알아보기
    - **firewall-cmd** --list-all-zones | less

방화벽 관리하기

- 방화벽 구성하기-1
  - 특정한 Interface에 Zone 할당하기- NIC에 다른 Zone 할당하기
    - **firewall-cmd** --zone=home --change-interface=eth0
  - eth0의 Active zone이 home으로 지정되었는지 확인하기
    - **firewall-cmd** --get-active-zones
  - 동적으로 설정한 Firewall 설정을 초기화 하기(되돌리기)
    - **systemctl** restart firewalld.service
    - **firewall-cmd** --get-active-zones
    - firewalld 서비스를 재시작하면 모든 동적 설정이 초기화된다는 사실에 유의한다. 즉, eth0에 다시 public zone이 할당된다

방화벽 관리하기

- 방화벽 구성하기-2
  - VM에 NIC를 하나 더 추가한다
  - 특정한 zone(home zone)의 구성 내용 알아보기
    - **firewall-cmd --zone=home** --list-all
  - NIC에 영구적으로 특정한 Zone(home)을 할당하기
    - vi /etc/sysconfig/network-scripts/ifcfg-eth0
      DNS1=8.8.8.8
      ZONE=home
  - network 서비스와 방화벽 서비스 재시작하기
    - systemctl restart network.service
    - systemctl restart firewalld.service
  - eth0의 active zone이 home으로 변경되었는지 확인하기
    - **firewall-cmd** --get-active-zones

```
[root@centos1 ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
[root@centos1 ~]# systemctl restart network.service
[root@centos1 ~]# systemctl restart firewalld.service
[root@centos1 ~]# firewall-cmd --get-active-zones
home
  interfaces: eth0
[root@centos1 ~]#
```

방화벽 관리하기

- 방화벽 구성하기-2
  - 현재 Default zone 확인하기
    - firewall-cmd --get-default-zone

```
[adminuser@centos1 ~]$ firewall-cmd --get-default-zone
public
[adminuser@centos1 ~]$
```

  - 각 NIC에 할당된 zone 확인하기(active zone 확인하기)
    - firewall-cmd --get-active-zones

```
[adminuser@centos1 ~]$ firewall-cmd --get-active-zon
home
  interfaces: eth0
public
  interfaces: eth1
```

  - 특정한 zone을 지정하지 않은 NIC들에게는 Default zone 설정하기
    - firewall-cmd --set-default-zone=home
    - firewall-cmd --get-default-zone
  - Default zone이 제대로 eth1에 지정되었는지 확인하기
    - systemctl restart network.service
    - systemctl restart firewalld.service
    - firewall-cmd --get-active-zones

```
[root@centos1 adminuser]# firewall-cmd --get-active-zones
home
  interfaces: eth0 eth1
```

방화벽 관리하기

- 방화벽 구성하기-2
  - 다시 특정한 zone을 지정하지 않은 NIC들에게는 Default zone 설정하기
    - firewall-cmd --set-default-zone=public
    - firewall-cmd --get-default-zone
  - Default zone이 제대로 eth1에 지정되었는지 확인하기
    - systemctl restart network.service
    - systemctl restart firewalld.service
    - firewall-cmd --get-active-zones

```
[root@centos1 adminuser]# firewall-cmd --get-active-zones
home
  interfaces: eth0
public
  interfaces: eth1
[root@centos1 adminuser]#
```

방화벽 관리하기

- 방화벽 구성하기-3
  - 방화벽에서 설정 가능한 서비스 종류 확인하기
    - **firewall-cmd** --get-services
  - public zone으로 설정된 NIC의 접속 허용 목록 알아보기
    - firewall-cmd --zone=public --list-services
  - public zone으로 설정된 NIC에는 http 서비스 접속 허용하기
    - firewall-cmd --zone=public **--add-service=http**
    - firewall-cmd --zone=public --list-services

```
[root@centos1 adminuser]# firewall-cmd --zone=public --list-services
dhcpv6-client http ssh
```

  - firewalld 서비스 재시작하기
    - systemctl restart firewalld.service
    - firewall-cmd --zone=public --list-services

```
[root@centos1 adminuser]# firewall-cmd --zone=public --list-services
dhcpv6-client ssh
```

    - ## 설정이 원상 복귀된다는데 주의한다

방화벽 관리하기

- 방화벽 구성하기-3
  - public zone으로 설정된 NIC에는 영구적으로 http 서비스 접속 허용하기
    - firewall-cmd --zone=public **--permanent --add-service=http**
    - firewall-cmd --zone=public **--permanent** --list-services

```
[root@centos1 adminuser]# firewall-cmd --zone=public --permanent --list-services
dhcpv6-client http ssh
```

  - firewalld 서비스 재시작하기
    - systemctl restart firewalld.service
    - firewall-cmd --zone=public --list-services

```
[root@centos1 adminuser]# systemctl restart firewalld.service
[root@centos1 adminuser]# firewall-cmd --zone=public --list-services
dhcpv6-client http ssh
```

    - ## 설정이 영구적으로 할당된 것을 알 수 있다
  - https 서비스도 영구적으로 접속을 허용하도록 설정하기
    - firewall-cmd --zone=public --add-service=https
    - firewall-cmd --zone=public --permanent --add-service=https

방화벽 관리하기

- 방화벽 구성하기-3
  - 포트 번호를 사용하여 접속 허용하기
    - firewall-cmd --zone=public --add-port=5000/tcp
    - firewall-cmd --zone=public --add-port=4990-4999/udp
  - 접속을 허용한 포트 번호 목록 확인하기
    - firewall-cmd --list-ports

```
[root@centos1 adminuser]# firewall-cmd --list-ports
4990-4999/udp 5000/tcp
```

  - firewalld 서비스 재시작하기
    - systemctl restart firewalld.service
    - firewall-cmd --list-ports
    - ## 모든 설정이 초기화되었다는 사실에 주의한다

방화벽 관리하기

- 방화벽 구성하기-3
  - 영구 접속 허용하기
    - firewall-cmd --zone=public --permanent --add-port=5000/tcp
    - firewall-cmd --zone=public --permanent --add-port=4990-4999/udp
    - firewall-cmd --zone=public --permanent --list-ports
  - firewalld 서비스 재시작하기
    - systemctl restart firewalld.service
    - firewall-cmd --list-ports

```
[root@centos1 adminuser]# systemctl restart firewalld.service
[root@centos1 adminuser]# firewall-cmd --list-ports
4990-4999/udp 5000/tcp
```

    - ## 모든 설정이 영구적으로 구성되었다

방화벽 관리하기

- 방화벽 구성하기-4
  - 현재 사용 가능한 zone이 어떤 것들이 있는지 확인하기
    - firewall-cmd --get-zones
  - 필요한 Zone을 생성하여 **영구적으로** 사용하기
    - firewall-cmd --permanent --new-zone=publicweb
    - firewall-cmd --permanent --new-zone=privateDNS
    - firewall-cmd --permanent --get-zones

```
[root@centos1 adminuser]# firewall-cmd --permanent --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

    - firewall-cmd --get-zones

```
[root@centos1 adminuser]# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

  - 방화벽을 재시작한 후 zone 확인하기(영구 생성 여부 확인)
    - firewall-cmd --reload
    - firewall-cmd --get-zones

```
[root@centos1 adminuser]# firewall-cmd --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

방화벽 관리하기

- 방화벽 구성하기-4
  - 생성한 zone(publicweb)을 service에 할당하기
    - firewall-cmd --zone=publicweb --add-service=ssh
    - firewall-cmd --zone=publicweb --add-service=http
    - firewall-cmd --zone=publicweb --add-service=https
    - firewall-cmd --zone=publicweb --list-all

```
[root@centos1 adminuser]# firewall-cmd --zone=publicweb --list-all
publicweb
  interfaces:
  sources:
  services: http https ssh
  ports:
```

  - 생성한 zone(privateDNS)을 service에 할당하기
    - firewall-cmd --zone=privateDNS --add-service=dns
    - firewall-cmd --zone=privateDNS --list-all

```
[root@centos1 adminuser]# firewall-cmd --zone=privateDNS --list-all
privateDNS
  interfaces:
  sources:
  services: dns
  ports:
```

방화벽 관리하기

- 방화벽 구성하기-4
  - 생성한 zone(publicweb)을 eth0, 생성한 zone(privateDNS)은 eth1에 할당하기
    - firewall-cmd --zone=publicweb --change-interface=eth0
    - firewall-cmd --zone=privateDNS --change-interface=eth1
    - firewall-cmd --get-active-zones

```
[root@centos1 adminuser]# firewall-cmd --get-active-zones
privateDNS
  interfaces: eth1
publicweb
  interfaces: eth0
```

  - 방화벽 재시작하기
    - systemctl restart firewalld
    - firewall-cmd --get-active-zones
    - ## 설정이 초기화되었다

방화벽 관리하기

- 방화벽 구성하기-4
  - 생성한 zone(publicweb)을 eth0, 생성한 zone(privateDNS)은 eth1에 영구적으로 할당하기
    - firewall-cmd --zone=publicweb --permanent --add-service=ssh
    - firewall-cmd --zone=publicweb --permanent --add-service=http
    - firewall-cmd --zone=publicweb --permanent --add-service=https
    - firewall-cmd --zone=privateDNS --permanent --add-service=dns
    - vi /etc/sysconfig/network-scripts/ifcfg-eth0
      ZONE=publicweb
    - vi /etc/sysconfig/network-scripts/ifcfg-eth1
      ZONE=privateDNS
  - 네크워크 및 방화벽 재시작하기
    - systemctl restart network
    - systemctl restart firewalld

방화벽 관리하기

- 방화벽 구성하기-4
  - 생성한 zone(publicweb)을 eth0, 생성한 zone(privateDNS)은 eth1에 영구적으로 할당하기(계속)
    - firewall-cmd --get-active-zones
    - firewall-cmd --zone=publicweb --list-services
    - firewall-cmd --zone=privateDNS --list-services
    - firewall-cmd --set-default-zone=publicweb

보안 관리도구 사용하기

NMap

SELinux

보안 관리도구 사용하기

- NMap
  - Log 관리와 방화벽 설정은 리눅스 보안을 위해 가장 기본적으로 사용하는 도구이다.
  - nmap은 네트워크 탐색, 보안 스캔하기, 네트워크 감사, 원격 컴퓨터의 열려 있는 포트 찾아내기 등을 할 수 있다
  - nmap은 로컬 시스템이나 원격 서버가 사용중인 포트 또는 운영체제를 스캔하여 출력하는 유틸리티이다
  - nmap은 네트워크 관리용으로도 사용되고, 취약한 포트가 사용중인지 확인이 가능하여 보안용으로도 사용된다
  - 하지만 스캔하는 것만으로도 보안 침입을 위한 준비 과정으로 간주하므로 다른 회사의 서버를 함부로 스캔하면 안된다

- NMap 설치하기
  - yum install nmap nmap-frontend -y

보안 관리도구 사용하기

- NMap 사용 방법

nmap

기능	네트워크를 탐색하고 보안을 점검한다.
형식	nmap [옵션] 목적지 주소
옵션	-sS : TCP SYN을 스캔한다. -sT : TCP 연결을 스캔한다. -sP : ping을 스캔한다. -sU : UDP를 스캔한다. -sO : IP 프로토콜을 스캔한다. -O : 운영체제를 확인한다. -v : 스캔 결과를 상세하게 출력한다. -p 포트 번호 : 지정한 포트만 스캔한다(예 : -p22; -p1-65535; -p U:53,111,T:21-25,80). -F : 빠른 모드(fast mode)로 기본 스캔보다 적은 수의 포트만 스캔한다.
사용 예	nmap 192.168.0.1 nmap -O 192.168.0.1 nmap -sT -O -v 192.168.0.1

보안 관리도구 사용하기

- NMap 사용하기
  - 로컬 시스템에 열려 있는 포트를 요약하여 출력하기
    - **nmap localhost**
  - 원격 컴퓨터 스캔하기
    - **nmap 192.168.219.103**
    - **nmap 192.168.219.103 192.168.219.104 192.168.219.105**
    - **nmap 192.168.219.103,104,105**
    - **nmap 192.168.219.1-100**
  - 원격 컴퓨터 상세히 스캔하기
    - **nmap -v 192.168.219.103**
  - 파일에 있는 컴퓨터 목록을 보고 스캔하기
    - **cat > nmaphosts.txt**
    - **nmap -iL nmaphosts.txt**

보안 관리도구 사용하기

- NMap 사용하기
  - 네트워크 스캔하기
    - **nmap 192.168.219.***
    - **nmap 192.168.219.* --exclude 192.168.219.100**
  - 원격 서버 스캔하여 운영 체제 정보 확인하기
    - **nmap -O 192.168.219.103**
  - 원격 컴퓨터로 ping하기
    - **nmap -sP 192.168.219.103**
  - 로컬 컴퓨터에 UDP 포트가 열려 있는지 확인하기
    - **nmap -sU - v localhost**
  - 특정한 네트워크를 대상으로 tcp port 스캔하기
    - **nmap -sT -O -v 192.168.219.0/24**

보안 관리도구 사용하기

- NMap 사용하기
  - 원격 컴퓨터에 방화벽이 있는지 확인하기
    - **nmap -sA 192.168.219.104**

```
[root@localhost ~]# nmap -sA 192.168.219.104
                                                    Firewalld OFF
Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-10 08:09 KST
Nmap scan report for 192.168.219.104
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.219.104 are unfiltered
MAC Address: 00:15:5D:DB:67:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
[root@localhost ~]# nmap -sA 192.168.219.104
                                                    Firewall ON
Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-10 08:10 KST
Nmap scan report for 192.168.219.104
Host is up (0.00066s latency).
Not shown: 999 filtered ports
PORT   STATE      SERVICE
22/tcp unfiltered ssh  SSH Access Permitted
MAC Address: 00:15:5D:DB:67:02 (Microsoft)
```

  - 특정한 네트워크를 대상으로 포트 스캔하기
    - **nmap -O 192.168.219.103**

보안 관리도구 사용하기

- NMap 사용하기
  - 원격 컴퓨터가 켜지 있는지 확인하기
    - **nmap -sP 192.168.219.103**
    - **nmap -sP 192.168.219.103-105**
    - **nmap -sP 192.168.219.***
  - Fast Scan하기
    - **nmap -F 192.168.219.103**
    - **nmap -F 192.168.219.103-105**
    - **nmap -F 192.168.219.***
  - 특정한 포트만 Scan하기
    - **nmap -p 80 192.168.219.103**
    - **nmap -p 80,443 192.168.219.103**
    - **nmap -p 22-443 192.168.219.103**

보안 관리도구 사용하기

- NMap 사용하기
  - 특정한 TCP 포트만 Scan하기
    - **nmap -p T:80,443 192.168.219.103**
  - 특정한 UDP 포트만 Scan하기
    - **nmap -sU 53 192.168.219.103**
  - 원격 컴퓨터가 ping에 응답하지 않도록 icmp request에 응답하지 않도록 설정했는지 확인하기(TCP ACK and TCP Syn)
    - **nmap -PS 192.168.219.103**
  - stealthy Scan하기
    - **nmap -sS 192.168.219.103**

보안 관리도구 사용하기

- NMap 사용하기
  - TCP Syn를 사용하여 가장 많이 사용하는 포트만 검사하기
    - **nmap -sT 192.168.219.103**
  - tcp null scan을 사용하여 방화벽을 무력화하기
    - **nmap -sN 192.168.219.103**