4 네트워크 관리

실험 영역	네트워크 관리 영역
실험 제목	Inetd를 이용한 네트워크 서비스 관리
실험 요약	/etc/inetd.conf 에서 정의하고 있는 네트워크 서비스 중 보안상 불필요한 서비스를 제거하고 이를 inetd 데몬 프로세스에 반영하는 실험

4.1 이론

목적지를 향하여 보내진 패킷을 서비스 포트 번호에 따라 응용 프로그램(서버)에게로 중재하는 프로세스가 바로 인터넷 수퍼 서버인 inetd 이다. inetd 는 이러한 포트의 요청을 중재해 주는 서버의 서버로서 자신에게 등록된 서비스 포트들을 감시하고 있다가 특정 포트에 요청이 들어오면 그 포트에 해당하는 응용 프로그램(telnet, ftp 등)을 깨워서 서비스 요청을 전달하게 된다.

이러한 포트와 응용 프로그램간의 정보를 등록하는 파일은 /etc/inetd.conf 이다. /etc/inetd.conf 파일은 시스템에서 서비스할 서비스의 명칭들과 그것들의 위치들이 설정되어 있다. FTP, telnet, gopher, remote shell(rsh), remote rogin(rlogin), remote exec(rexec), talk, POP2, POP3, IMAP, finger, time(tcp), time(udp)등 여러 서비스를 제공한다.

4.1.1 inetd 구동 원리

inetd daemon 은 FTP, telnet, POP2/3, finger 등과 같은 여러 인터넷 서비스 제공에 사용되기 때문에 'super server'로 불린다. inetd daemon 은 다중사용자 부팅 프로세스 중 일정 지점에서 구동된다. 구동시에 inetd daemon 은 /etc/inetd.conf 설정을 읽고, /etc/services 에 나열되어 있는 모든 표준 포트에 대한 요구 사항을 읽는다. 특정 포트에 들어오면, inetd 는 적절한 서비스를 실행시켜 요청을 처리한다.

예를 들어 사용자가 telnet 서비스를 요청할 경우 inetd 는 아래와 같이 동작한다.

① 사용자가 TCP 포트 23 를 사용하여 telnet 서비스를 요청한다.

② inetd 는 /etc/services 파일을 참조하여 telnet 서비스를 TCP 포트 23 에 매핑시킨다.

/etc /services 파일의 구성은 아래와 같다.

③ Inetd 는 TCP 포트 23 에 대한 접속 요청을 받으면 /usr/sbin/tcpd 서비스를 in.telnetd 인자와 함께 실행시킨다. tcpd 프로그램은 in.telnetd telent 서버를 구동시키고 telnet 서버는 요청에 적절하게 응답한다.

4.1.2 /etc/services

IP 의 헤더는 보내는 호스트와 받는 호스트의 IP 주소를 지니며, TCP 나 UDP 의 헤더는 보내는 포트와 받는 포트에 대한 정보를 지닌다. 16 비트로 구성되는 이 포트 번호는 응용 프로그램의 고유한 ID 로 사용되며, 보내는 응용 프로그램에서 받는 응용 프로그램을 지칭하는 데 사용된다. 일반적인 UNIX 시스템의 포트 번호에 관한 정보는 /etc/services 에 정의된다. 이 중에서 1 에서 1023 까지의 포트 번호는 `well-known services'라 하는 시스템을 위하여 이미 할당된 포트 번호들이다. 이 중에서 telnet 은 TCP 포트 23 번을, ftp 는 TCP 포트 21 번을, 그리고 talk 는 UDP 포트 517 번을 사용한다. 1024 번부터 5000 번 이상까지는 이미 사용되고 있지 않다면 일반 사용자의 응용 프로그램에서 사용할 수 있다.

/etc/services 파일은 아래와 같이 구성되어 있다.

```
# @(#)$Header: services,v 1.23.109.6 92/09/21 11:53:07 ash Exp $
#
# This file associates official service names and aliases with
# the port number and protocol the services use.
#
# Some of the services represented below are not supported on HP-UX.
# They are provided soley as a reference.
#
# The form for each entry is:
# <official service name>   <port number/protocol name>   <aliases>
#
# See the services(4) manual page for more information.
# Note: The entries cannot be preceded by a blank space.
#
echo              7/tcp                    # Echo
echo              7/udp                     #
discard           9/tcp   sink null        # Discard
discard           9/udp   sink null         #
systat           11/tcp   users             # Active Users
daytime          13/tcp                    # Daytime
daytime          13/udp                     #
qotd             17/tcp   quote            # Quote of the Day
chargen          19/tcp   ttytst source    # Character Generator
```

```
chargen          19/udp   ttytst source   #
ftp-data         20/tcp                   # File Transfer Protocol (Data)
ftp              21/tcp                   # File Transfer Protocol (Control)
telnet           23/tcp                   # Virtual Terminal Protocol
smtp             25/tcp                    # Simple Mail Transfer Protocol
time             37/tcp   timeserver      # Time
time             37/udp   timeserver      #
rlp              39/udp   resource        # Resource Location Protocol
whois            43/tcp   nicname          # Who Is
domain           53/tcp   nameserver       # Domain Name Service
domain           53/udp   nameserver       # Domain Name Service

.........................
```

4.1.3 /etc/inetd.conf

/etc/inetd.conf 파일의 구성은 아래와 같다.

<service_name> <socket_type> <proto> <flags> <user> <server_pathname> <args>

- service : 서비스 이름을 명시하며 /etc/services에 등록되어 있어야 한다.
- socket type : TCP일 경우에는 stream, UDP일 경우에는 dgram이라 명시한다.
- protocol : tcp 혹은 udp의 프로토콜을 명시하며 /etc/protocols에 등록되어 있어야 한다.
- wait flag : inetd가 서비스 요청을 받은 경우, 이후에 즉시 또다른 요청을 처리할 것인지 아닌지의 여부에 따라 nowait 또는 wait로 구분한다. stream일 경우에는 반드시 nowait이어야 한다.
- login name : 어떤 사용자의 권한으로 프로그램을 수행시켜줄 것인지 명시한다.
- server : 어떤 응용 프로그램을 수행시킬 것인지 명시한다. 절대 경로를 모두 명시하여야 한다. (예: /usr/etc/in.fingerd)
- argument : 응용 프로그램의 인자를 지정하며 5개까지 가능하다. 일반적으로 argv[0]는 프로그램 자신의 이름이 되므로 첫번째 인자는 응용 프로그램 자신의 이름이 된다.

```
# @(#)inetd.conf 1.23 90/01/03 SMI
#
# Configuration file for inetd(8). See inetd.conf(5).
#
# Internet services syntax:
```

```
# <service_name> <socket_type> <proto> <flags> <user> <server_pathname> <args>
# Ftp and telnet are standard Internet services.
# ftp stream tcp nowait root /usr/etc/in.ftpd in.ftpd
telnet stream tcp nowait root /usr/etc/in.telnetd in.telnetd
nntp stream tcp nowait root /etc/nntpd nntpd
#
# Tnamed serves the obolete IEN-116 name server protocol.
#
name dgram udp wait root /usr/etc/in.tnmaed in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.

.................
```

4.1.4 inetd 를 통한 서비스 통제

inetd 를 통해 이용할 수 있는 모든 서비스는 잠재적인 공격에 문을 열어 놓은 것이라 할 수 있다. 그래서 inetd.conf 사용시 서버의 용도에 맞게 서비스를 제한해야 하며 제공해야 할 서비스와 그렇지 않은 서비스를 구별해야 한다. Inetd 를 통한 서비스 통제 방법은 다음과 같다.

가. 서비스 생성 및 제거

특정서비스 ftp 와 같은 서비스를 제한하기 위해선 /etc/inetd.conf 파일에서 주석처리(#)를 하거나 혹은 그 라인을 제거한다.

```
#ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
```

반대로 특정 서비스를 제공하기 위해선 /etc/inetd.conf 파일에서 주석처리(#)를 제거하거나 혹은 그 라인을 삽입한다.

```
ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
```

나. 서비스 구동

/etc/inetd.conf 를 변경한 후에는 inetd 을 kill 시킨 후 /usr/sbin/inetd 를 재실행시켜야 한다.

```
#kill -9 <process 번호>
#/usr/sbin/inetd –s
```

Inetd 을 kill 시킨 후 바로 재실행시키기 위해서는 아래 명령어를 사용할 수 있다.

```
#kill  -HUP inetd
```

4.2 실험

본 실험에서는 특정 서비스를 제공하여야 할 경우 특정 포트의 네트워크 서비스를 활성화시키고 보안상 불필요할 경우 이를 비활성화할려고 한다.

[주의] 실습자들간의 간섭을 피하기 위해서는 실습자 ID 가 user001 일 경우 10001 번 포트를, user002 번일 경우 10002 번 포트를 사용해야만 한다.

네트워크 상태는 netstat 명령어나 PC 에서 scan 도구를 이용하여 확인할 수 있으며 프로세스는 ps 명령어를 통하여 확인할 수 있다.

```
# netstat .na // 현재 시스템의 모든 네트워크 연결상태 확인

# ps .ef // 현재 시스템의 모든 프로세스를 확인
```

가. 기관에서 특정 목적을 위하여 새로운 네트워크 서비스를 제공하여야 한다. 실습 서버에서 명령어를 통하여 네트워크 서비스 상태를 분석하고 실습자에 해당되는 네트워크 서비스를 활성화시키시오.

나. windows 또는 Linux 환경의 PC 에서 실습 서버의 해당 포트가 열려있는지 스캔하시오.

다. 기관에서 제공하던 서비스가 보안상 문제점이 발생하여 이를 비활성화 시켜야 한다. 실습 서버에서 명령어를 통하여 네트워크 서비스 상태를 분석하고 실습자에 해당되는 네트워크 서비스를 비활성화시키시오.

라. windows 또는 Linux 환경의 PC 에서 실습 서버의 해당 포트가 닫혀있는지 스캔하시오.