우분투 리눅스

시스템 & 네트워크

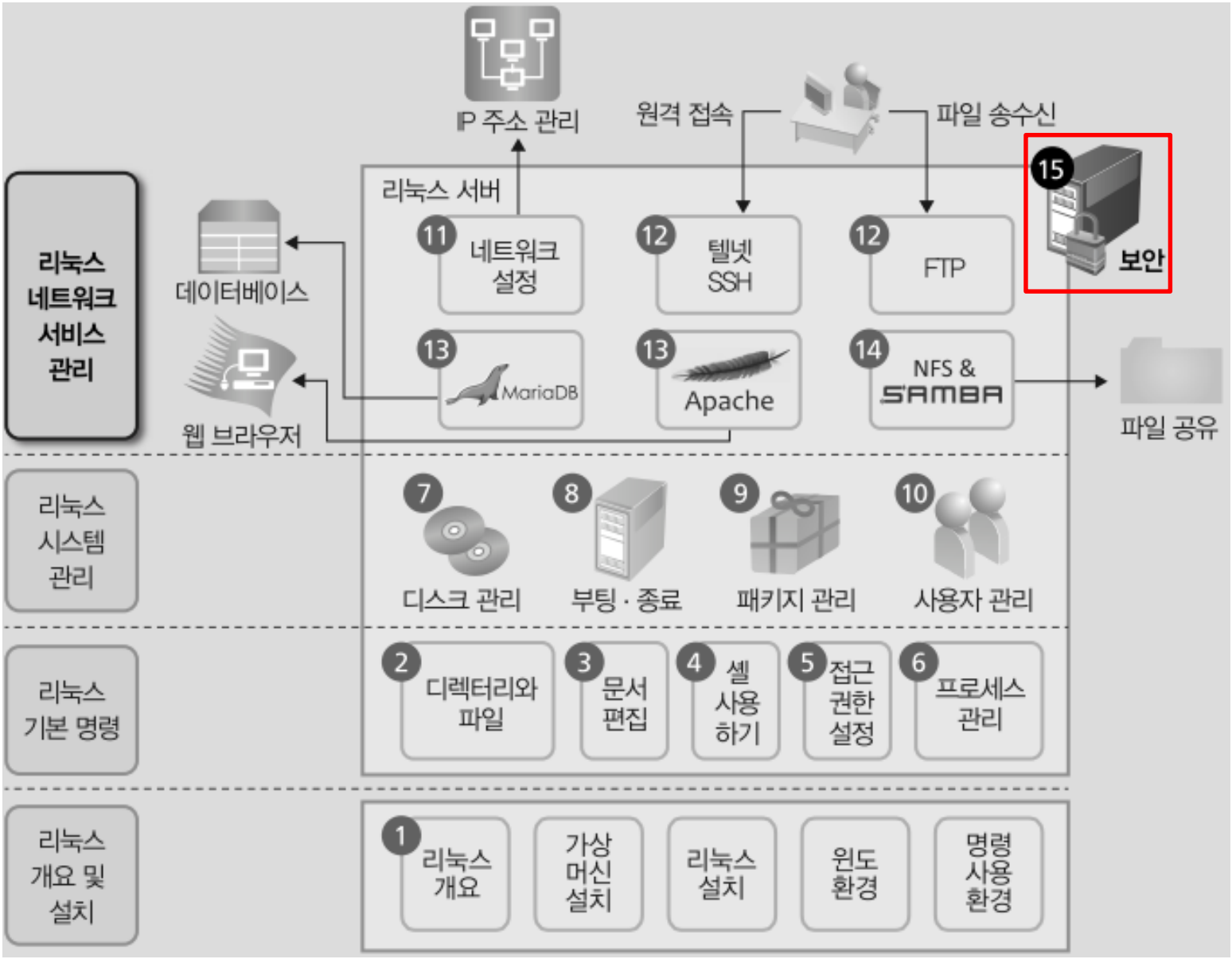
Chapter 15. 리눅스 보안의 기초

목차

학습목표

- 정보 보안의 3요소가 무엇인지 설명할 수 있다.
- 로그가 무엇인지 설명할 수 있다.
- 로그 파일을 확인하고 내용을 분석할 수 있다.
- 로그 관리 데몬을 설정할 수 있다.
- GUI 도구를 사용하여 방화벽을 설정할 수 있다.
- 명령을 사용하여 방화벽을 설정할 수 있다.
- NMap을 사용하여 시스템에서 열려 있는 포트가 무엇인지 확인할 수 있다.
- PAM이 무엇인지 이해하고 설정 파일을 설명할 수 있다.

리눅스 실습 스터디 맵


IP 주소 관리
원격 접속
파일 송수신
리눅스 서버
15
보안
리눅스 네트워크 서비스 관리
데이터베이스
11 네트워크 설정
12 텔넷 SSH
12 FTP
웹 브라우저
13 MariaDB
13 Apache
14 NFS & SAMBA
파일 공유
리눅스 시스템 관리
7 디스크 관리
8 부팅 · 종료
9 패키지 관리
10 사용자 관리
리눅스 기본 명령
2 디렉터리와 파일
3 문서 편집
4 셸 사용하기
5 접근 권한 설정
6 프로세스 관리
리눅스 개요 및 설치
1 리눅스 개요
가상 머신 설치
리눅스 설치
윈도 환경
명령 사용 환경

00 개요

[그림 15-1] 15장의 내용 구성

01 정보 보안의 기초

정보 보안의 정의

- 정보 보안에는 물리적인 보안, 기술적인 보안, 관리적인 보안 등 다양한 측면
- 정보 보안은 정보 자산을 여러 가지 위협으로부터 보호하여 기밀성, 무결성, 가용성을 유지하는 것

정보 보안의 3요소: CIA 삼각형

- 기밀성(confidentiality)은 허가받은 사용자만이 해당 정보에 접근할 수 있도록 하는 것
- 무결성(integrity)은 정보가 무단으로 변조되지 않았음을 의미
- 가용성(availability)은 필요할 때 인가를 받은 사용자가 정보나 서비스에 접근할 수 있는 것

[그림 15-2] 정보 보안의 3요소

01 정보 보안의 기초

보안 기본 조치

- 불필요한 서비스 통제하기
  - 꼭 필요하지 않은 서비스 포트는 모두 차단
  - 서비스를 통제하는 데는 불필요한 서비스 자체를 제거하는 방법과 방화벽에서 패킷을 필터링하는 방법을 함께 사용하는 것이 바람직
- 소프트웨어 패치 실시하기
  - 시스템 관리자는 패치의 발표에 주의를 기울이고 있다가 패치가 나오면 즉시 설치
- 주기적으로 점검하기
  - 프로세스의 목록과 사용자의 상태, 서비스의 동작 상태, 네트워크 연결 상태, 디스크의 남은 용량 등을 주기적으로 확인
- 백업하기
  - 주요 시스템 설정과 소프트웨어, 사용자 데이터 등을 주기적으로 백업
  - 문제가 발생했을 때 빠르게 복구하는 방법도 연습해둬야
- 공부하는 시스템 관리자
  - 시스템 관리자는 늘 공부하는 자세로 신기술에 대한 검토와 적용, 안정적인 서비스 운영 등을 위해 꾸준히 노력

02 시스템 로그

- **로그**
  - 로그는 커널과 리눅스 시스템이 제공하는 여러 서비스와 응용 프로그램이 발생시키는 메시지
  - 로그를 저장하고 있는 파일을 로그 파일: 대부분 /var/log 디렉터리에 위치
  - 로그 파일을 통해 시스템의 상태를 확인 가능
- **주요 로그파일**

```
user1@myubuntu:~$ ls -F /var/log
Xorg.0.log             btmp            kern.log.1         speech-dispatcher/
Xorg.0.log.old         btmp.1          kern.log.2.gz      syslog
Xorg.1.log             cups/           kern.log.3.gz      syslog.1
Xorg.1.log.old         dist-upgrade/   kern.log.4.gz      syslog.2.gz
alternatives.log       dmesg           lastlog            syslog.3.gz
alternatives.log.1     dmesg.0         lightdm/           syslog.4.gz
apache2/               dmesg.1.gz      mail.err           syslog.5.gz
apport.log             dmesg.2.gz      mail.err.1         syslog.6.gz
apport.log.1           dmesg.3.gz      mail.log           syslog.7.gz
apport.log.2.gz        dmesg.4.gz      mail.log.1         udev
apt/                   dpkg.log        mail.log.2.gz      ufw.log
aptitude               dpkg.log.1      mail.log.3.gz      ufw.log.1
auth.log               faillog         mysql/             unattended-upgrades/
auth.log.1             fontconfig.log  mysql.err          upstart/
auth.log.2.gz          fsck/           mysql.log          vsftpd.log
auth.log.3.gz          gdm/            news/              wtmp
auth.log.4.gz          hp/             pm-powersave.log   wtmp.1
boot.log               installer/      pm-powersave.log.1
bootstrap.log          kern.log        samba/
user1@myubuntu:~$
```

02 시스템 로그

주요 로그 파일

- 로그 파일의 소유자는 거의 대부분 root 계정
- 접근 권한은 대부분의 경우 600으로 설정
- 보안의 측면에서도 일반 사용자 계정에서 로그 파일의 내용을 함부로 볼 수 없게 하는 것이 바람직

```
user1@myubuntu:~$ ls -l /var/log/dmesg*
-rw-r----- 1 root adm 93691  3월 29 15:43 /var/log/dmesg
-rw-r----- 1 root adm 93691  3월 29 15:13 /var/log/dmesg.0
-rw-r----- 1 root adm 18516  3월 29 13:16 /var/log/dmesg.1.gz
-rw-r----- 1 root adm 18421  3월 28 09:38 /var/log/dmesg.2.gz
-rw-r----- 1 root adm 18511  3월 28 09:32 /var/log/dmesg.3.gz
-rw-r----- 1 root adm 18533  3월 28 09:29 /var/log/dmesg.4.gz
user1@myubuntu:~$
```

02 시스템 로그

■ 주요 로그 파일 용도

[표 15-1] 리눅스의 주요 로그 파일

로그 파일	내용
/var/log/boot.log	부팅 시 서비스 데몬의 실행 상태를 기록한다.
/var/log/apache2/*	아파치 웹 서버와 관련된 로그를 기록한다.
/var/log/apt/*	apt-get 명령으로 패키지를 설치하고 삭제한 로그를 기록한다.
/var/log/auth.log	telnet, ssh, su, sudo 등의 사용자 로그인 인증을 기록한다.
/var/log/dmesg	시스템이 부팅할 때 생성한 로그를 기록한다.
/var/log/lastlog	각 계정의 가장 최근 로그인 정보를 기록하고 lastlog 명령으로 확인한다.
/var/log/mail.*	메일 관련 로그를 기록한다.
/var/log/Xorg.#.log	X윈도 관련 로그를 기록한다.
/var/log/btmp	실패한 로그인 기록이며 바이너리 파일이므로 last -f btmp 또는 lastb 명령으로 확인이 가능하다.
var/log/cups/*	cupsd 데몬이 생성하는 로그를 기록한다. cupsd 데몬은 인터넷 프린팅 프로토콜을 지원하는 데몬이다.
/var/log/wtmp	로그인 기록이며 last 명령으로 내용을 확인할 수 있다.
/var/log/samba/*	Samba에 의해 생성된 로그를 기록한다.
/var/log/syslog	syslog가 생성하는 공통 로그를 기록한다.
/var/log/mysql*	MariaDB에서 생성한 로그를 기록한다.
/var/log/ufw.log	방화벽이 생성하는 로그를 기록한다.
/var/log/vsftpd.log	FTP 서버의 데이터 전송 로그를 기록한다.

02 시스템 로그

로그 파일 예: /var/log/syslog 파일

- 커널이나 데몬에서 발생하는 대부분의 메시지가 기록
- 로그는 날짜와 시간, 로그를 발생시킨 호스트 이름, 데몬 이름, 메시지 내용 등으로 구성되며 한 행씩 기록

```
user1@myubuntu:~$ cat /var/log/syslog
(생략)
Mar 29 15:11:41 myubuntu kernel: [    0.710306] fuse init (API version 7.22)
Mar 29 15:11:41 myubuntu kernel: [    0.710416] msgmni has been set to 1738
Mar 29 15:11:41 myubuntu kernel: [    0.712009] Key type asymmetric registered
(생략)
Mar 30 04:53:23  dhclient: last message repeated 5 times
Mar 30 04:54:23  dhclient: last message repeated 4 times
Mar 30 04:55:23  dhclient: last message repeated 5 times
Mar 30 04:56:23  dhclient: last message repeated 4 times
user1@myubuntu:~$
```

02 시스템 로그

로그 관리 데몬

- 리눅스 시스템의 로그 파일 중 일부는 로그 관리 데몬에 의해 통제: rsyslog

```
user1@myubuntu:~$ dpkg -l | grep rsyslog
ii  rsyslog                                    5.8.11-2ubuntu4
      i386         reliable system and kernel logging daemon
user1@myubuntu:~$ ps -ef | grep rsyslog
syslog      490     1  0  3월29  ?        00:00:03  rsyslogd -c5
user1     21793 21426  0  05:01  pts/12   00:00:00  grep --color=auto rsyslog
user1@myubuntu:~$
```

- rsyslog 서비스를 설정하는 파일은 /etc/rsyslog.d 디렉터리에 있는 *.conf 파일
  - 어떤 로그를 어떻게 처리할 것인지를 규칙(rule)으로 정의

02 시스템 로그

로그 관리 데몬

- 규칙은 한 행에 선택자와 동작으로 작성하며 공백 문자나 탭으로 구분

선택자

- rsyslog의 선택자는 기능명(facility)과 우선순위(priority)를 기반

기능명.우선순위

- 기능명: 로그 메시지를 생성하는 프로그램을 지정
- 우선순위: 메시지의 심각도

[표 15-3] rsyslog 메시지의 우선순위

심각도	의미
emerg	매우 긴급한 비상 상태
alert	긴급한 상태
crit	중대한 상태
err	오류 상태
warning	경고 메시지
notice	단순 메시지
info	정보성 메시지
debug	디버깅용 메시지

[표 15-2] rsyslog 선택자의 기능명

기능명	관련 프로그램
*	모든 기능
auth	인증 관련 명령
authpriv	보다 민감한 보안 메시지
cron	cron 데몬
daemon	일반적 시스템 데몬
kern	시스템 커널
lpr	인쇄 시스템
mail	sendmail과 기타 메일 관련 프로그램
news	유즈넷 뉴스 시스템
security	auth와 동일, 사용하지 않음
syslog	rsyslog 데몬 내부 메시지
user	사용자 프로세스
uucp	uucp 통신, 현재는 사용하지 않음
local0~7	여덟 가지 로컬 메시지
mark	일정 주기로 타임 스탬프 메시지 생성(rsyslog 내부용)

02 시스템 로그

■ 선택자 적용

- 기능명과 우선순위를 결합하는 방법

[표 15-4] rsyslog 선택자 구성의 예

선택자	의미
kern.*	우선순위에 상관없이 커널의 모든 로그 메시지를 선택한다.
mail.crit	메일에서 crit 이상의 우선순위(crit, alert, emerg)를 가진 모든 로그 메시지를 선택한다.
cron.!info,!debug	cron에서 info와 debug를 제외한 모든 로그 메시지를 선택한다.
mail.=info	메일에서 심각도가 info인 경우만 로그 메시지를 선택한다.

02 시스템 로그

■ 동작: 선택자가 선택한 메시지를 어떻게 처리할 것인지를 정의

[표 15-5] rsyslog 동작의 종류

선택자와 동작	의미
. @192.168.0.1	메시지를 192.168.0.1의 rsyslog 데몬으로 보낸다.
. @abc.com:18	메시지를 abc.com의 18번 포트로 TCP를 통해 보낸다.
. 파일명	메시지를 지정한 파일에 저장한다.
. user1, user2	메시지를 user1, user2 사용자의 화면에 출력한다.
. *	메시지를 현재 로그인하고 있는 모든 사용자에게 보낸다.
cron.* ~	~는 cron이 발생시킨 모든 메시지를 무시한다.
kern.* ^exe:form	커널이 발생시킨 메시지를 form이 형식을 조정하여 exe 프로그램에 전달하고 exe 프로그램을 실행한다.

- 예: 커널이 발생시킨 메시지 중 우선순위가 crit 이상인 메시지를 /var/log/kern.log 파일에 저장

```
kern.crit      /var/log/kern.log
```

- 예: 메시지를 파일에도 저장하고 user1 사용자에게도 메시지를 출력

```
kern.crit      /var/log/kern.log
kern.crit      user1
```

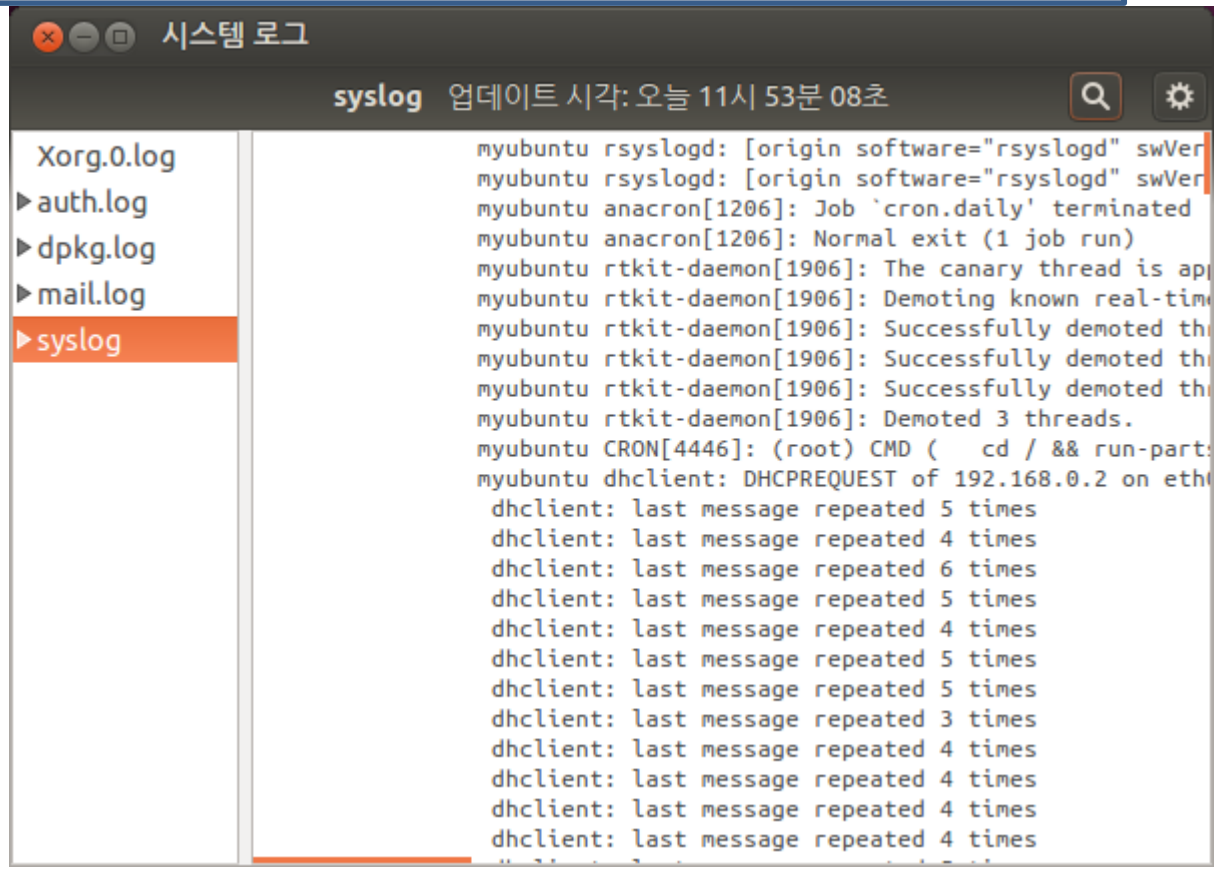
02 시스템 로그

로그 관리 도구

- 그놈은 로그를 관리할 수 있는 GUI 도구인 로그뷰어를 제공: gnome-system-log

```
user1@myubuntu:~$ dpkg -l | grep gnome-system-log
ii  gnome-system-log                          3.8.1-1svn1
     i386         system log viewer for GNOME
user1@myubuntu:~$
```

- gnome-system-log 실행



[그림 15-3] 로그뷰어

03 방화벽 관리

방화벽

- 네트워크를 통한 외부의 접속을 차단하려면 방화벽(firewall)을 사용해야 함
- 우분투의 방화벽 명령은 ufw

방화벽 동작 확인하기: ufw

```
user1@myubuntu:~$ dpkg -l | grep ufw
ii  ufw                                          0.33-0ubuntu4
    all          program for managing a Netfilter firewall
user1@myubuntu:~$
user1@myubuntu:~$ sudo ufw status
상태: 비활성
user1@myubuntu:~$
```

- 방화벽 시작과 종료

```
sudo ufw enable
```

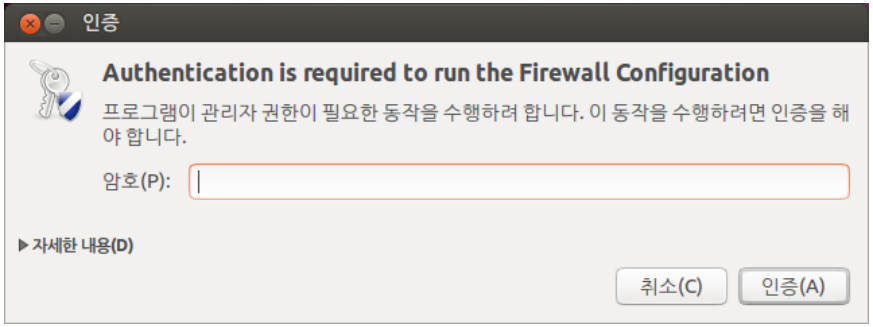
```
sudo ufw disable
```

03 방화벽 관리

GUI 도구로 방화벽 설정하기

- 방화벽을 관리하기 위한 GUI 도구로 gufw

```
user1@myubuntu:~$ sudo apt-get install gufw
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
(생략)
```



[그림 15-4] gufw 접속인증창

03 방화벽 관리

- **gufw 사용하기**

(a) 방화벽 비활성 상태

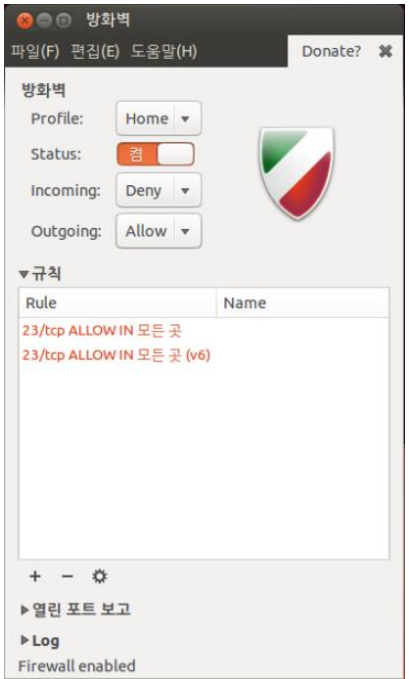
(b) 방화벽 활성 상태

[그림 15-5] gufw 동작 화면

03 방화벽 관리

gufw 사용하기

- Profile
  - 현재 설정하는 내용을 적용할 환경을 설정
  - 설정할 수 있는 값은 Home, Office, Public
- Status : 방화벽 전체를 켜거나 끌 수 있음
- Incoming과 Outgoing
  - 시스템으로 들어오는 트래픽과 시스템에서 밖으로 나가는 트래픽을 어떻게 할 것인지 기본 값을 설정
  - 일반적으로 시스템으로 들어오는 트래픽은 모두 거부하고(deny) 밖으로 나가는 트래픽은 허용하는(allow) 것이 기본 값
  - 허용과 거부 외에 거절(reject)과 제한(limit)이 있음
    - 거절은 접속을 거부하고(deny) 거절된 이유를 알려줌
    - 제한은 같은 IP에서 반복적으로 접속을 시도할 때 트래픽이 거부되는 경우
- 규칙
  - 방화벽에서 규칙을 선택하면 현재 적용 중인 규칙을 보여줌
  - +를 선택하여 규칙을 추가하거나, -를 선택하여 규칙을 삭제할 수 있음



[그림 15-6] gufw 규칙화면

03 방화벽 관리

gufw 사용하기

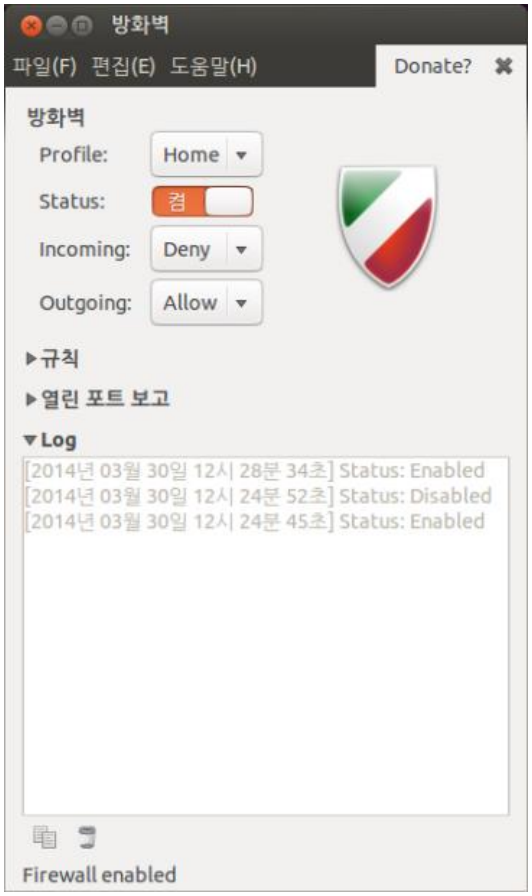
- 규칙을 추가하는 방법
  - 편리하게 모드: 방화벽을 적용할 응용 분야를 게임, 오디오/비디오, 시스템, 오피스 등으로 구분하고 다시 세부 카테고리를 정해 방화벽 정책을 정할 수 있도록 함
  - 간단하게 모드: 규칙의 이름을 사용자가 정할 수 있으며, TCP/UDP 선택과 포트 번호나 서비스명을 사용자가 직접 지정하고 정책을 적용할 수 있음
  - 자세하게 모드: 규칙의 이름, 번호, 정책, 방향, 인터페이스 선택, 로그 기록 여부, TCP/UDP 선택뿐만 아니라 출발지와 목적지의 주소, 포트 번호 등을 자세하게 설정할 수 있음

[그림 15-7] gufw 규칙을 정하는 3가지 모드 화면

03 방화벽 관리

gufw 사용하기

- 열린 포트 보고: 현재 열려 있는 포트를 보고
- 로그 : 방화벽과 관련된 로그 기록 출력



[그림 15-7] gufw 로그

[그림 15-8] gufw 열린포트보고

03 방화벽 관리

방화벽 관리 명령

ufw

기능	방화벽을 설정한다.
형식	ufw 서브 명령
서브 명령	enable : 방화벽을 활성화한다. disable : 방화벽을 비활성화한다. default allow|deny|reject [incoming|outgoing] : 방화벽의 기본 동작을 설정한다. status [verbose] : 방화벽의 상태를 출력한다. allow 서비스명|포트/프로토콜 : 지정한 서비스나 포트를 허용한다. deny 서비스명|포트/프토로콜 : 지정한 서비스나 포트를 거부한다. delete 명령 : 명령으로 설정한 규칙을 삭제한다.
사용 예	ufw deny telnet　　ufw allow 23/tcp　　ufw status

03 방화벽 관리

- **방화벽의 상태 보기 : status**

```
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action   From
--                         ------   ----
23/tcp                     ALLOW    Anywhere
22/tcp                     ALLOW    Anywhere
23/tcp                     ALLOW    Anywhere (v6)
22/tcp                     ALLOW    Anywhere (v6)
user1@myubuntu:~$
```

03 방화벽 관리

규칙 추가하기

```
user1@myubuntu:~$ sudo ufw allow http
Rule added
Rule added (v6)
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action      From
--                         ------      ----
23/tcp                     ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80                         ALLOW       Anywhere
23/tcp                     ALLOW       Anywhere (v6)
22/tcp                     ALLOW       Anywhere (v6)
80                         ALLOW       Anywhere (v6)
user1@myubuntu:~$
```

03 방화벽 관리

서비스 거부하기

```
user1@myubuntu:~$ sudo ufw deny telnet
규칙 갱신됨
규칙 갱신됨 (v6)
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action   From
--                         ------   -----
23/tcp                     DENY     Anywhere
22/tcp                     ALLOW    Anywhere
80                         ALLOW    Anywhere
23/tcp                     DENY     Anywhere (v6)
22/tcp                     ALLOW    Anywhere (v6)
80                         ALLOW    Anywhere (v6)
user1@myubuntu:~$
```

03 방화벽 관리

규칙 삭제하기

```
user1@myubuntu:~$ sudo ufw delete deny telnet
규칙 삭제됨
규칙 삭제됨 (v6)
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action   From
--                         ------   -----
22/tcp                     ALLOW    Anywhere
80                         ALLOW    Anywhere
22/tcp                     ALLOW    Anywhere (v6)
80                         ALLOW    Anywhere (v6)
user1@myubuntu:~$
```

03 방화벽 관리

포트 추가하기

```
user1@myubuntu:~$ sudo ufw allow 5000/tcp
Rule added
Rule added (v6)
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80                         ALLOW       Anywhere
5000/tcp                   ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere (v6)
80                         ALLOW       Anywhere (v6)
5000/tcp                   ALLOW       Anywhere (v6)
user1@myubuntu:~$
```

03 방화벽 관리

■ 특정 IP 주소의 접속 설정하기

```
user1@myubuntu:~$ sudo ufw allow from 192.168.0.17 to any port ftp
Rule added
user1@myubuntu:~$ sudo ufw status
상태: 활성
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80                         ALLOW       Anywhere
5000/tcp                   ALLOW       Anywhere
21/tcp                     ALLOW       192.168.0.17
22/tcp                     ALLOW       Anywhere (v6)
80                         ALLOW       Anywhere (v6)
5000/tcp                   ALLOW       Anywhere (v6)
user1@myubuntu:~$
```

04 보안 관리 도구

NMap : 포트 스캔 도구

- NMap은 내 서버나 원격의 서버가 사용 중인 포트, 운영체제 등을 스캔하여 출력
- NMap은 네트워크 관리용으로도 사용되고, 취약한 포트가 사용 중인지 확인이 가능하여 보안용으로도 사용
- 스캔하는 것만으로도 보안 침입을 위한 준비 과정으로 간주하므로 원격 서버를 마구 스캔하면 안됨

NMap 설치하기

```
user1@myubuntu:~$ sudo apt-get install nmap
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음 패키지를 더 설치할 것입니다:
  libblas3 liblinear-tools liblinear1
(생략)
nmap (6.40-0.1ubuntu1) 설정하는 중입니다 ...
libc-bin에 대한 트리거를 처리하는 중입니다 ...
user1@myubuntu:~$
```

04 보안 관리 도구

nmap 명령의 기본 형식

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

04 보안 관리 도구

옵션 없이 nmap 실행하기

- 지정한 호스트에서 현재 열려 있는 포트를 요약하여 출력

```
user1@myubuntu:~$ nmap localhost
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-30 13:56 KST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
user1@myubuntu:~$
```

04 보안 관리 도구

특정 서버 스캔하기

- 특정 서버를 IP 주소를 사용하여 지정하고 -O 옵션도 지정했다. -O 옵션은 해당 시스템의 운영체제 정보출력

```
user1@myubuntu:~$ sudo nmap -O 192.168.0.2
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-30 14:08 KST
Nmap scan report for 192.168.0.2
Host is up (0.000061s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.9
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
user1@myubuntu:~$
```

04 보안 관리 도

- 윈도가 설치되어 있는 PC를 스캔

```
user1@myubuntu:~$ sudo nmap -O 192.168.0.17
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-30 14:02 KST
Nmap scan report for 192.168.0.17
Host is up (0.00076s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
5357/tcp open  wsdapi
MAC Address: B4:B6:76:AB:F7:48 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 7|2008|Vista|2012|Phone|Longhorn (96%)
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/
o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/
o:microsoft:windows_vista::sp1:home_premium cpe:/o:microsoft:windows_2012 cpe:/
o:microsoft:windows
Aggressive OS guesses: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or
Windows 8 (96%), Microsoft Windows Vista Home Premium SP1, Windows 7, or Windows
Server 2008 (95%), Microsoft Windows 7 or Windows Server 2008 R2 (94%), Microsoft
Windows Vista (92%), Microsoft Windows Server 2008 SP2 (92%), Microsoft Windows
Vista Enterprise (91%), Microsoft Windows 7 or Windows Server 2012 (91%),
Microsoft
Windows 7 Ultimate (91%), Microsoft Windows Vista SP2 (90%), Microsoft Windows
Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.30 seconds
user1@myubuntu:~$
```

04 보안 관리 도구

- **UDP 포트 스캔하기: -sU 옵션을 사용**

```
user1@myubuntu:~$ sudo nmap -sU -v localhost
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-30 14:05 KST
Initiating UDP Scan at 14:05
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 137/udp on 127.0.0.1
Discovered open port 111/udp on 127.0.0.1
Completed UDP Scan at 14:05, 1.22s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 995 closed ports
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
111/udp open          rpcbind
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
631/udp open|filtered ipp
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
           Raw packets sent: 1003 (28.851KB) | Rcvd: 2002 (85.874KB)
user1@myubuntu:~$
```

04 보안 관리 도구

- 특정 네트워크를 대상으로 포트 스캔하기

```
user1@myubuntu:~$ sudo nmap -sT -O -v 192.168.0.0/24
Starting Nmap 6.40 ( http://nmap.org ) at 2014-03-30 14:06 KST
Initiating ARP Ping Scan at 14:06
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 14:06, 3.04s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 14:06
Completed Parallel DNS resolution of 255 hosts. at 14:06, 0.03s elapsed
Nmap scan report for 192.168.0.0 [host down]
Nmap scan report for 192.168.0.3 [host down]
Nmap scan report for 192.168.0.4 [host down]
Nmap scan report for 192.168.0.6 [host down]
Nmap scan report for 192.168.0.7 [host down]
Nmap scan report for 192.168.0.8 [host down]
Nmap scan report for 192.168.0.9 [host down]
(생략)
Initiating Parallel DNS resolution of 1 host. at 14:06
Completed Parallel DNS resolution of 1 host. at 14:06, 0.01s elapsed
Initiating Connect Scan at 14:06
Scanning 4 hosts [1000 ports/host]
Discovered open port 445/tcp on 192.168.0.17
Discovered open port 135/tcp on 192.168.0.21
Discovered open port 445/tcp on 192.168.0.21
Discovered open port 554/tcp on 192.168.0.21
Discovered open port 139/tcp on 192.168.0.21
Discovered open port 139/tcp on 192.168.0.17
(생략)
Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 36.03 seconds
           Raw packets sent: 687 (32.622KB) | Rcvd: 123 (10.312KB)
user1@myubuntu:~$
```

04 보안 관리 도구

PAM

- PAM은 'pluggable authentication modules'의 약자 -> 삽입형 인증 모듈
- PAM은 모듈 방식으로 구성되어 있어 시스템 관리자가 필요에 따라 인증 모듈을 추가·삭제·편집 가능

PAM 설정 파일

- /etc/pam.d 디렉터리에 각 서비스별로 설정 파일 존재

```
user1@myubuntu:~$ ls /etc/pam.d
accountsservice                 cups-daemon                     login
atd                             gdm                             newusers
chfn                            gdm-autologin                   other
chpasswd                        gdm-launch-environment          passwd
chsh                            gdm-password                    polkit-1
common-account                  gnome-screensaver               ppp
common-auth                     lightdm                         samba
common-password                 lightdm-autologin               sshd
common-session                  lightdm-greeter                 su
common-session-noninteractive   lightdm-remote-freerdp          sudo
cron                            lightdm-remote-uccsconfigure    vsftpd
user1@myubuntu:~$
```

04 보안 관리 도구

PAM 설정 파일 형식

```
<모듈 인터페이스> <제어 플래그> <모듈 이름> <모듈 인자>
```

- 모듈 인터페이스
  - auth : 사용자를 인증하는 데 사용, 예를 들어 암호가 정확한지를 확인
  - account : 이 모듈은 접근이 허용되는지를 확인, 예를 들어 사용자 계정이 유효한지 또는 사용자가 해당 날짜에 로그인할 수 있는지를 확인
  - password : 이 모듈은 사용자 계정의 암호를 바꾸는 데 사용
  - session : 이 모듈은 사용자의 세션을 설정하고 관리, 또한 사용자의 홈 디렉터리를 마운트하는 것과 같이 접근을 허용하는 데 필요한 부가적인 작업을 수행
- 제어 플래그: 특정 모듈의 성공과 실패를 어떻게 처리할 것인지를 알려줌
  - required : 해당 모듈은 인증을 계속하기 위해 반드시 성공해야 한다. 만약 실패하면 사용자는 다른 모든 모듈의 테스트가 끝날 때까지 결과를 받지 못한다.
  - requisite : 해당 모듈은 인증을 계속하기 위해 반드시 성공해야 한다. 그러나 만약 이 지점에서 실패하면 사용자는 실패에 대한 메시지를 즉시 받는다.
  - sufficient : 실패하면 이 모듈의 결과가 무시된다. 만약 이 모듈이 성공하고 앞선 required 모듈 중 실패가 없으면 인증 성공을 리턴한다.
  - optional : 이 모듈의 결과는 무시된다. 이 모듈은 오직 해당 인터페이스에 다른 모듈이 없는 경우에만 인증에 성공하는 데 필요하다.
  - include : 인자로 지정된 설정 파일의 내용을 모두 포함한다.
  - substack : include와 같이 인자로 지정된 설정 파일의 내용을 모두 포함하나, 서브 스택의 동작 결과에 따라 나머지 모듈을 통과하지 않는다는 점이 다르다.

04 보안 관리 도구

PAM 설정 파일 형식

- 모듈 이름: 삽입 가능한(pluggable) 것을 지정

```
user1@myubuntu:~$ ls /lib/i386-linux-gnu/security
pam_access.so           pam_issue.so        pam_permit.so        pam_tally2.so
pam_cap.so              pam_keyinit.so      pam_pwhistory.so     pam_time.so
pam_debug.so            pam_lastlog.so      pam_rhosts.so        pam_timestamp.so
pam_deny.so             pam_limits.so       pam_rootok.so        pam_tty_audit.so
pam_echo.so             pam_listfile.so     pam_securetty.so     pam_umask.so
pam_env.so              pam_localuser.so    pam_selinux.so       pam_unix.so
pam_exec.so             pam_loginuid.so     pam_sepermit.so      pam_userdb.so
pam_faildelay.so        pam_mail.so         pam_shells.so        pam_warn.so
pam_filter.so           pam_mkhomedir.so    pam_stress.so        pam_wheel.so
pam_ftp.so              pam_motd.so         pam_succeed_if.so    pam_xauth.so
pam_gnome_keyring.so  pam_namespace.so  pam_systemd.so
pam_group.so            pam_nologin.so      pam_tally.so
user1@myubuntu:~$
```

- 모듈 인자: 인증 과정에서 정보가 필요한 일부 모듈에 정보를 전달

04 보안 관리 도구

PAM 파일의 예

```
1 #%PAM-1.0
2 auth       required  pam_securetty.so
3 auth       required  pam_unix.so nullok
4 auth       required  pam_nologin.so
5 account    required  pam_unix.so
6 password   required  pam_cracklib.so retry=3
7 password   required  pam_unix.so shadow nullok use_authtok
8 session    required  pam_unix.so
```

- 1행은 주석이다. 주석은 #로 시작
- 2행부터 4행은 로그인 인증을 위한 모듈
  - pam_securetty.so : 사용자가 root로 로그인하려고 할 때 해당 터미널이 /etc/securetty 파일에 등록되어 있어야 한다. 터미널이 등록되어 있지 않다면 'Login incorrect' 메시지가 출력되고 로그인 실패
  - pam_unix.so nullok : 사용자에게 암호를 입력하도록 프롬프트를 출력하고 입력한 암호가 /etc/shadow에 등록된 암호와 같은지를 확인한다. nullok 인자는 pam_unix.so 모듈이 빈 암호도 허용한다는 것을 의미한다.
  - pam_nologin.so : 인증의 마지막 단계로 /etc/nologin 파일이 존재하는지를 확인한다. 만약 존재할 경우 사용자가 root가 아니면 인증에 실패한다.
- 5행의 account required pam_unix.so는 계정의 정상 여부를 확인하기 위해 필요한 모듈
- 6행의 password required pam_cracklib.so retry=3은 만약 암호가 만료된 경우 pam_cracklib.so 모듈이 새 암호를 입력하도록 프롬프트를 출력하고, 새로 입력한 암호가 사전 기반으로 쉽게 해독될 수 있는 것인지를 검사
- 7행의 password required pam_unix.so shadow nullok use_authtok는 만약 프로그램이 사용자의 암호를 바꾸려면 반드시 pam_unix.so 모듈의 password 인터페이스를 사용하도록 하는 것
- 8행의 session required pam_unix.so는 전체 세션을 관리하기 위해 pam_unix.so 모듈을 사용함을 의미

우분투 리눅스

시스템 & 네트워크