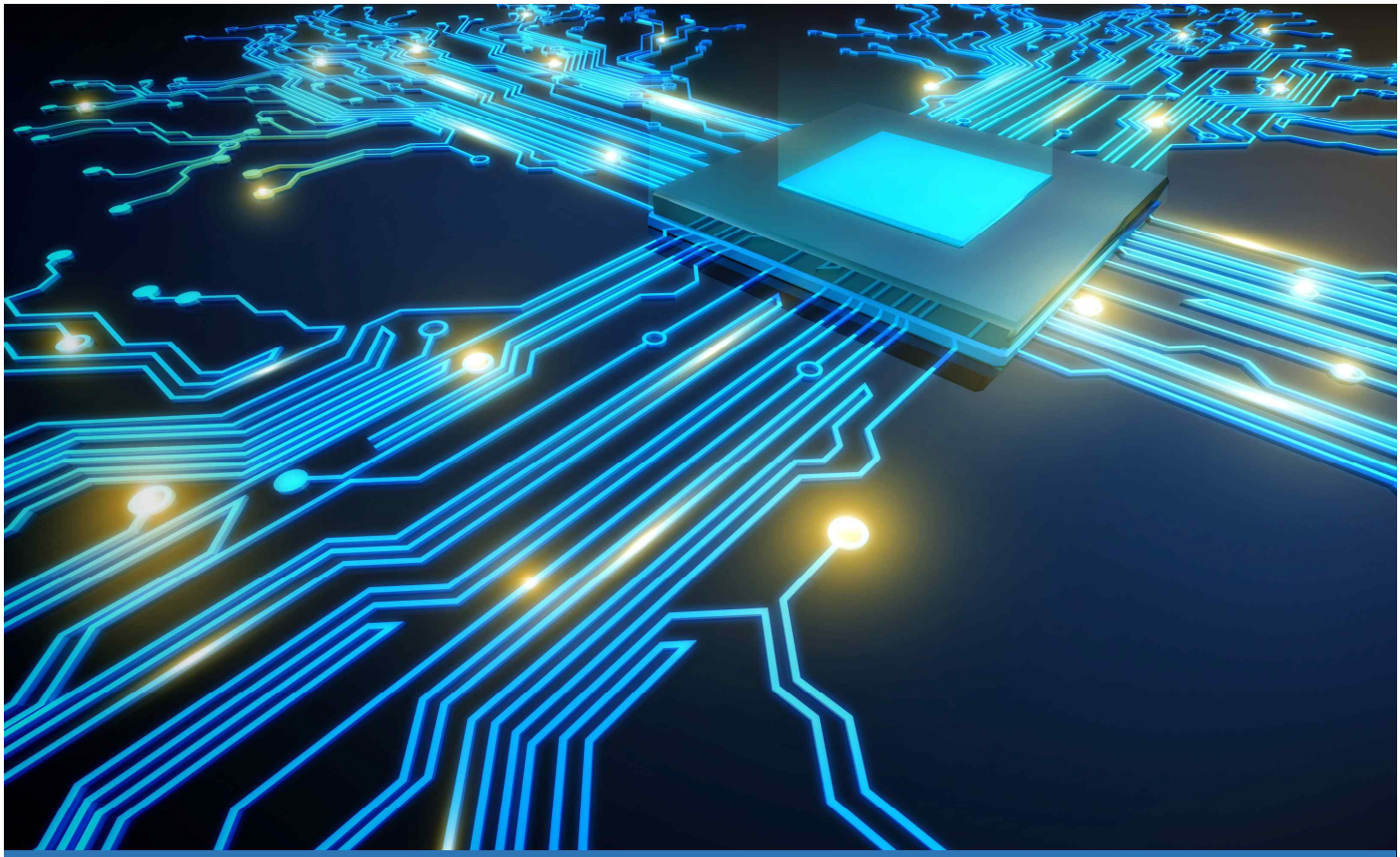
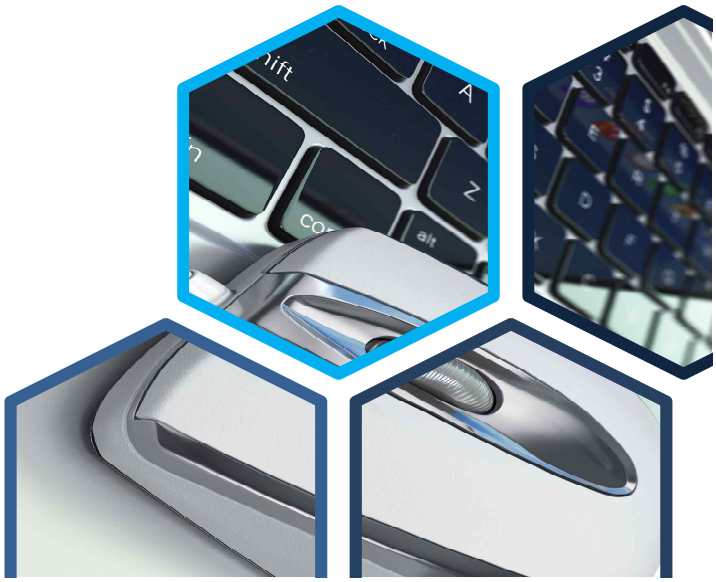


컴퓨터시스템

리눅스 보안



학습목표

- 정보 보안과 보안의 기본조치에 대해 설명할 수 있다.
- 시스템 로그 방법을 설명할 수 있다 .
- ufw와 nmap 명령의 사용방법을 설명할 수 있다.

학습내용

- 정보 보안의 이해
- 시스템 로그
- ufw와 nmap

정보 보안의 이해

1 정보 보안의 정의

정보 보안의 개념

- 정보 보안의 다양한 측면

물리적인 보안	기술적인 보안	관리적인 보안

- 정보 자산을 여러 가지 위협으로부터 보호하여 기밀성, 무결성, 가용성을 유지하는 것

정보 보안의 3요소: CIA 삼각형으로 표시함

정보 보안의 이해

1 정보 보안의 정의

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 바람직함

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

백업하기

- 주요 시스템 설정과 소프트웨어, 사용자 데이터 등을 주기적으로 백업
- 문제가 발생했을 때 빠르게 복구하는 방법도 연습해 둘 필요가 있음

시스템 로그

1 주요 로그 파일

로그

- 커널과 리눅스 시스템이 제공하는 여러 서비스와 응용 프로그램이 발생시키는 메시지
- 로그를 저장하고 있는 파일을 로그 파일이라고 하는데 대부분 /var/log 디렉터리에 위치
- 로그 파일을 통해 시스템의 상태 확인 가능

주요 로그 파일

로그 파일의 소유자	접근 권한	보안의 측면
대부분 root 계정임	**대부분의 경우 600으로 설정함**	일반 사용자 계정에서 로그 파일의 내용을 함부로 볼 수 없게 하는 것이 바람직함

시스템 로그

1 주요 로그 파일

리눅스의 주요 로그 파일 용도

/var/log/boot.log	부팅 시 서비스 데몬의 실행 상태를 기록함
/var/log/apache2/*	아파치 웹 서버와 관련된 로그를 기록함
/var/log/apt/*	apt-get 명령으로 패키지 설치 및 삭제한 로그를 기록함
/var/log/auth.log	telnet, ssh, su, sudo 등의 사용자 로그인 인증을 기록함
/var/log/dmesg	시스템이 부팅할 때 생성한 로그를 기록함
/var/log/lastlog	각 계정의 가장 최근 로그인 정보를 기록하고 lastlog 명령으로 확인함
/var/log/mail.*	메일 관련 로그를 기록함
/var/log/Xorg#.log	X윈도 관련 로그를 기록함
/var/log/btmp	실패한 로그인 기록이고 바이너리 파일이므로 last -f btmp 또는 lastb 명령으로 확인이 가능함
/var/log/cups/*	• cupsd 데몬이 생성하는 로그를 기록함 • cupsd 데몬은 인터넷 프린팅 프로토콜을 지원하는 데몬
/var/log/wtmp	로그인 정보를 기록하며 last 명령으로 확인 가능함
/var/log/samba/*	삼바에 의해 생성된 로그를 기록함
/var/log/syslog	syslog가 생성하는 공통 로그를 기록함
/var/log/mysql*	MariaDB에서 생성한 로그를 기록함
/var/log/ufw.log	방화벽이 생성하는 로그를 기록함
/var/log/vsftpd.log	FTP 서버의 데이터 전송 로그를 기록함

시스템 로그

1 주요 로그 파일

로그 파일 관리하기

- 전통적인 로그 관리방법은 journal 기능으로 대체
- journal은 기존의 syslog 형식에 따라 로그를 저장하고, 저장된 로그에 접근하기 위해 journalctl 명령을 사용함
- journal에서 messages 파일을 대체하는 것: journalctl 명령

시스템 로그

2 rsyslog 데몬

개요

- 시스템의 로그 파일 중 일부는 rsyslog라는 로그 관리 데몬에 의해 통제
- rsyslog 서비스를 제공하는 데몬: rsyslogd
- rsyslog 서비스를 설정하는 파일: /etc/rsyslog.d 디렉터리에 있는 *.conf 파일
- 어떤 로그를 어떻게 처리할 것인지 기본 규칙을 설정한 파일: 50-default.conf

```
user1@myubuntu:~$ ls  /etc/rsyslog.d
20-ufw.conf    50-default.conf    postfix.conf
```

rsyslog의 규칙 파일

- 텍스트 파일이므로 관리자가 vi로 수정
- 규칙은 한 행에 필터와 동작으로 작성하고 공백문자나 탭으로 구분

선택자

- rsyslog의 선택자: 기능명(facility)과 우선순위(priority)를 기반

기능명.우선순위

기능명	우선순위
로그 메시지를 생성하는 프로그램 지정	메시지의 심각도

시스템 로그

2 rsyslog 데몬

메시지의 심각도를 나타내는 rsyslog 메시지의 우선순위

심각도	의미
emerg	매우 긴급한 비상 상태
alert	긴급한 상태
crit	중대한 상태
err	오류 상태

심각도	의미
warning	경고 메시지
notice	단순 메시지
info	정보성 메시지
debug	디버깅용 메시지

시스템 로그

2 rsyslog 데몬

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)

시스템 로그

2 rsyslog 데몬

선택자 적용

- 기능명과 우선순위를 결합하는 방법
- rsyslog 선택자 구성의 예

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

시스템 로그

2 rsyslog 데몬

rsyslog 필터의 기능명

기능명	코드	관련 프로그램
*	-	모든 기능
mark	-	rsyslog 내부용
kern	0	시스템 커널
user	1	사용자 프로세스
mail	2	sendmail과 기타 메일 관련 프로그램
daemon	3	일반적인 시스템 데몬
auth	4	인증 관련 명령
syslog	5	rsyslog 데몬 내부 메시지
lpr	6	인쇄 시스템
news	7	유즈넷 뉴스 시스템
uucp	8	uucp 통신(현재는 사용하지 않음)
cron	9	cron 데몬
authpriv	10	보다 민감한 보안 메시지
ftp	11	ftp 데몬
local0~7	16~23	여덟 가지 로컬 메시지

시스템 로그

3 journal 기능

개요

- systemd 데몬의 구성 요소로 로그 파일의 관리를 담당
- 전통적으로 로그를 관리해온 rsyslog 데몬과 병행하여 사용
- 로깅 데이터는 journald 데몬이 수집·가공하여 journals라고 불리는 바이너리 파일로 저장
- journald 데몬의 실행 파일: systemd-journald
- journal이 저장한 로그를 보려면 journalctl 명령 사용

시스템 로그

3 journal 기능

journal이 저장한 로그를 보기 위한 명령: journalctl

- 기능: journal 로그를 관리함
- 형식: journalctl [옵션]
- 옵션

-n 행수	가장 최근에 기록된 로그 중 행수만큼 출력함
-r	가장 최근 로그가 먼저 출력됨
-o {short | verbose} short: verbose	지정한 형식으로 출력함 syslog 형식으로 출력함 로그의 상세한 내용을 출력함
-f	최근 로그를 자동으로 출력함
-p 우선순위	우선순위로 필터링하여 출력함
-b 시간	현재 부팅 이후의 로그만 출력함
--since=시간 --until==시간	시간을 필터링하여 출력함
필드명=값	필드명으로 필터링하여 출력함

- 사용 예

```
journalctl
journalctl -o verbose
```

시스템 로그 실습 영상은
학습 콘텐츠에서 확인하실 수 있습니다.

ufw와 nmap

1 ufw

GUI 도구로 방화벽 설정하기

- 방화벽을 관리하기 위한 GUI 도구: gufw(별도로 설치해야 함)

```
user1@myubuntu:~$ dpkg -l | grep gufw
```

- 인증을 위해 암호를 요구함

gufw 사용법

- 프로필(P)
  - 현재 설정하는 내용을 적용할 환경 설정
  - 설정할 수 있는 값: 홈, 사무실, 공용
- 상태(S): 방화벽 전체를 켜거나 끌 수 있음
- 내부로 들어옴(I)/ 외부로 나감(O)
  - 시스템으로 들어오는 트래픽과 시스템에서 밖으로 나가는 트래픽을 어떻게 할 것인지 기본 값을 설정
  - 기본 값: 거부, 허용, 거절

거부(deny)	허용(allow)	거절
시스템으로 들어오는 트래픽은 모두 거부	시스템 밖으로 나가는 트래픽은 허용	접속을 거부하고 거절된 이유를 알려줌

ufw와 nmap

1 ufw

gufw 사용법

- 규칙: 방화벽에서 규칙을 선택하면 현재 적용 중인 규칙을 보여줌

+를 선택	→	규칙을 추가
-를 선택	→	규칙을 삭제

- 규칙을 추가하는 방법

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

ufw와 nmap

1 ufw

방화벽 관리 명령: ufw

- 기능: 방화벽을 설정함
- 형식: ufw 서브 명령
- 옵션

enable	방화벽을 활성화
disable	방화벽을 비활성화
default allow | deny | reject [incoming | outgoing]	방화벽의 기본 동작을 설정
status [verbose]	방화벽의 상태를 출력
allow 서비스 | 포트/프로토콜	지정한 서비스나 포트를 허용
deny 서비스 | 포트/프로토콜	지정한 서비스나 포트를 거부
delete 명령	명령으로 설정한 규칙을 삭제

- 사용 예

```
ufw deny telnet        ufw allow 23/tcp        ufw status
```

ufw와 nmap

2 nmap

nmap: 포트 스캔 도구

- 내 서버나 원격의 서버가 사용 중인 포트, 운영체제 등을 스캔하여 출력
- 네트워크 관리용으로도 사용
- 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 install nmap
```

ufw와 nmap

2 nmap

nmap 명령의 기본 형식

- 기능: 네트워크를 탐색하고 보안을 점검함
- 형식: nmap [옵션] 목적지 주소
- 옵션

-sS	TCP SYN을 스캔
-sT	TCP 연결을 스캔
-sP	ping을 스캔
-sU	UDP를 스캔
-sO	IP 프로토콜을 스캔
-O	운영체제를 확인
-v	스캔 결과를 상세하게 출력
-p 포트 번호	지정한 포트만 스캔
-F	빠른 모드(Fast mode)로 기본 스캔보다 적은 수의 포트만 스캔

- 사용 예

```
nmap 192.168.1.1
nmap -0 192.168.1.1
nmap -sT -0 -v 192.168.1.1
```

ufw와 nmap 실습 영상은
학습 콘텐츠에서 확인하실 수 있습니다.

핵심요약

1 정보 보안의 이해

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

2 시스템 로그

- 로그는 커널과 리눅스 시스템이 제공하는 여러 서비스와 응용 프로그램이 발생시키는 메시지임
- 로그 파일 관리: journal 기능
- rsyslog 데몬: 로그 통합 서버를 관리할 수 있음

핵심요약

3 ufw와 nmap

- 네트워크를 통한 외부의 접속을 차단하려면 방화벽(firewall)을 사용해야 함
- 우분투의 방화벽 명령: ufw
- nmap은 내 서버나 원격의 서버가 사용 중인 포트, 운영체제 등을 스캔하여 출력함
- nmap은 네트워크 관리용으로도 사용되고 취약한 포트가 사용 중인지 확인이 가능하여 보안용으로도 사용됨