리눅스 보안체계 연구

지도교수 : 한 상 훈
연 구 자 : 한 민 규

< 목 차 >

요 약

본 연구는 운영체제의 한 종류인 리눅스의 보안체계를 알아보고자 하는 것에 그 목적이 있다. 리눅스는 윈도우나 맥과 더불어서 세계 3대 운영체제 중 하나이며 여러 가지 배포판들이 존재하고 있다. 본 연구에서는 이러한 리눅스가 분야별로 어떻게 활용되는지, 또 취약점은 어떤 것들이 있는지 심도 있게 살펴보고자 한다. 본 연구를 진행함으로써 리눅스의 사용성이 높아지고 그로 인해 리눅스가 가지는 역량을 전체적으로 제고시키는 데에도 효과적일 것이라 본다.

주요어 : 리눅스, 보안 정책, 해킹 사례, 리눅스 배포판

1. 서론

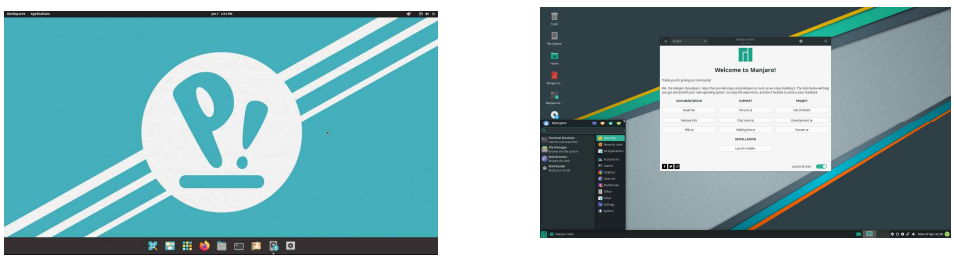
오늘날 FTP 서버나 메일 서버 등과 같은 서버의 사용이 늘어남에 따라 비용 절감, 불필요한 자원 절약 등의 이유로 리눅스의 사용이 선호되고 있다. 그러한 리눅스가 사용자들을 해킹 등의 안전으로부터 보호하는 등의 지킴이로서 할 수 있는 일과, 리눅스가 노출된 각종 취약점과 예방책에 대해 알아봄으로써 리눅스 사용의 거부감을 없애고 리눅스가 운영체제로서 사용자에게 주는 장점을 살리기 위해 본 연구를 진행하였다.

1.1 리눅스의 개요

리눅스란, 운영체제의 일종으로 사용자와 컴퓨터 간의 소통을 담당하는 소프트웨어이다. 여러 가지 배포판들이 있으며 설치하는 방법도 다양하다. 리눅스 배포판의 예시로 우분투(Ubuntu) 의 경우에는 1)데스크탑 버전(GUI) 과 2)서버 버전(CLI)을 용도에 맞게 선택할 수 있도록 제공한다.

1.2 리눅스의 특징

리눅스에도 여러 가지 특징이 있다. 첫째, 오픈 소스이고 무료이기에 서버 운영 비용이 절감된다. 여기서 오픈 소스란, 소스 코드가 공개되어 있다는 것을 의미한다. 예를 들어, 사용자가 MS-DOS 파일시스템을 쓰고 싶다면 3)커널(Kernel)을 컴파일해서 MS-DOS 파일시스템을 지원하도록 만들 수 있다. 소스 코드가 공개되어 있기 때문에 가능한 일이다. 둘째, 다중 접속을 지원한다. 따라서 여러 명의 사용자가 접속해 작업하는 것이 가능하다. 셋째, 배포본마다 점유율이 다양하다. 따라서 특정 배포판에 구애받지 않는다. 해외 커뮤니티 DigitalOcean에 노트북을 위한 최고의 7가지 배포판이 올라왔는데, 팝 OS, 만자로 리눅스 등 다양한 배포판이 존재하는 것을 확인할 수 있었다.



[사진 1] 팝 OS(좌) 와 만자로 리눅스(우)

1.3 리눅스 배포판의 종류

리눅스에는 여러 가지 종류의 배포판이 존재하고 있다. 그 중 몇 가지를 알아보자.

1) GUI, Graphic User Interface : 아이콘이나 배경화면 등의 그림을 보면서 사용하는 방식, 초심자에게 권장된다.
2) CLI, Command Line Interface : 아이콘이나 배경화면 등을 보지 않고 명령어만 사용하여 컴퓨터를 제어하는 방식, 명령어에 대한 이해가 필요하며 숙련자에게 적합함.
3) 커널(Kernel) : 리눅스를 포함한 모든 운영체제의 핵심부

1.3.1 우분투(Ubuntu)

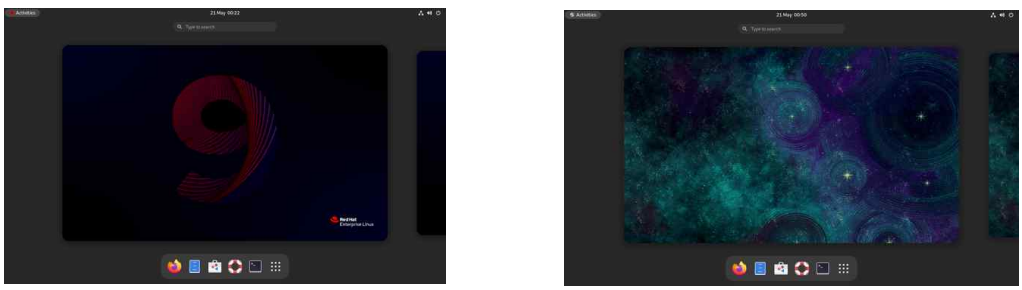
우분투(Ubuntu)는 캐노니컬 재단에서 발표한 배포판으로, 그놈(GNOME) 데스크탑 환경을 사용한다. 데비안 계열의 리눅스이며 최신 버전은 22.04 버전이다. 용도에 맞게 데스크탑 버전과 서버 버전을 제공하기 때문에 버전 선택이 용이하다는 점과, [1]LTS 버전이 있어서 다른 배포판보다 오랜 시간 업데이트를 지원 받는다는 점 등이 우분투의 장점이다.

[사진 2] 우분투 최신 버전 22.04 LTS

1.3.2 CentOS

다음으로 레드햇 계열의 리눅스 배포판인 CentOS를 살펴보자.

CentOS는 레드햇 엔터프라이즈 리눅스에서 파생된 배포판으로, 최신 버전은 CentOS Stream 9이다. 네이버나 카카오 등 대기업에서도 사용할 만큼 점유율이 높다는 장점이 있으나, 한글 지원이 미비하다는 단점도 존재한다. 레드햇 엔터프라이즈 리눅스의 무료버전으로 잘 알려져 있었으나 최근 CentOS Stream으로 전환되면서 그 부분이 사라졌다.



[사진 3] 레드햇 엔터프라이즈 리눅스(좌)와 CentOS(우)

이 밖에도 계열별로 리눅스 배포판을 정리하면 다음 표와 같다.

1) LTS(Long Term Support) 버전 : 일반 버전보다 지원 기간이 긴 버전, 장기적으로 업데이트가 지원되어 더 안전하다.

리눅스 배포판 계열	배포판 종류
데비안 계열	Linux Mint, Kali Linux, 크런치뱅 등
레드햇 계열	Fedora, Oracle Linux 등

[표 1] 그 밖의 리눅스 배포판

2. 리눅스의 분야별 보안 정책

2.1. 사용자 보안

이제 본격적으로 리눅스가 분야별로 어떻게 활용되는지 알아보기로 한다. 먼저 리눅스에서 사용할 수 있는 사용자 계정은 무엇이 있으며 보안 측면에서 어떻게 사용되는지 알아보자.

리눅스의 사용자 계정은 유형별로 슈퍼유저, 일반 사용자, 시스템 계정으로 나누어진다.

첫째로 슈퍼유저는 이름에서도 알 수 있듯이 모든 권한이 부여된 사용자이다. 모든 권한이 부여되어 있는 만큼 신중하게 사용해야 하며, 일반적인 경우는 슈퍼유저를 사용할 일이 거의 없고, 시스템의 관리나 유지보수 등에만 사용해야 한다. 리눅스에서 슈퍼유저만 할 수 있는 일이 몇 가지 있는데 대표적으로 두 가지 정도만 살펴보면 다음과 같다.

1. 비밀번호 변경 : 슈퍼유저만이 비밀번호를 변경할 수 있다. 비밀번호를 암호화하여 저장하는 파일로 /etc/shadow 라는 파일이 있는데 그 파일을 변경할 권한이 슈퍼유저에게만 있기 때문이다. 사용자 자신의 패스워드는 자신이 변경할 수 있지만 그마저도 슈퍼유저의 권한을 빌려와서 변경하게 된다.

2. 프로세스 종료 : 프로세스를 종료하는 권한도 슈퍼유저의 고유 권한 중 하나이다. 컴퓨터의 프로그램이 작동하는 것을 프로세스라고 부르는데, 프로세스는 일반적으로 실행이 종료되거나 사용자가 인위적으로 컨트롤+C 등의 키를 누르거나 하게 되면 정상적으로 종료되어야 하는 것이 맞지만, 개중에는 정상적으로 종료가 되었음에도 반응을 보이지 않는 좀비 프로세스 또한 존재할 수 있다, 그런 프로세스들을 강제로 종료하는 권한도 슈퍼유저의 고유 권한이다.

이와 같이 시스템의 유지/보수에 사용하는 계정이 슈퍼유저, 혹은 루트라고 하는 계정이다.

둘째로 일반 사용자 계정은 관리자 외에 시스템을 사용하는 모든 사용자를 말한다. /etc/passwd 파일에 정보를 저장하며 권한 설정의 영향을 받는다. (권한에 대한 것은 2.2 시스템 보안 파트에서 설명한다)

셋째로 시스템 계정은 데몬(서비스)를 실행할 때 사용하는 계정으로, 사용자가 직접적으로 로그인할 수는 없으며 데몬 실행 시에만 사용되는 계정이다. 종류로는 시스템 로그 관련 adm 계정, 명령어 관련 bin 계정 등이 있다.

또한, 리눅스에서 사용자 정보를 저장하는 파일을 네 가지만 정리해 보면 다음 표와 같다.

파일명(1)절대 경로)	역할
/etc/passwd	사용자 정보를 저장하는 파일
/etc/shadow	사용자의 패스워드를 암호화하여 저장하는 파일, 루트만이 접근할 수 있다.
/etc/group	그룹 정보를 저장하는 파일
/etc/skel	사용자 추가 시 홈 디렉터리에 기본으로 복사되는 파일들을 모아놓은 디렉터리

[표 2] 리눅스 사용자 관련 파일

2.2. 시스템 보안

다음으로 리눅스 시스템 분야에서의 보안 정책에 대해 알아보자. 서론에서 살펴보았듯 리눅스는 다중 접속을 지원하는 운영체제이기 때문에 여러 명의 사용자가 동시에 같은 리눅스 시스템에 접속하여 작업할 수 있다. 그렇기에 사용자마다 권한을 설정해 특정 파일을 읽을 수 없게 하거나 특정 디랙토리로 접근하지 못하게 하는 등의 제약을 설정할 수가 있다. 그것을 Access Control List, 즉 ACL이라고 부른다. 이번 파트에서는 ACL 에 관해서 중점적으로 알아본다.

우선, 권한을 알아보기 전에 소유자(Owner)라는 개념과 그룹(Group), 그리고 기타 사용자(Other User)라는 개념을 필수적으로 이해해야 한다. 아래 표를 통해 정리하고 넘어가자.

아래 표는 컴퓨터정보보안과 교수님이 만든 test라는 파일이 있을 때, 그 역할을 구분해 놓은 표이다.

역할	설명
소유자(Owner)	파일의 최초 제작자, 기본적으로 소유자는 모든 권한을 갖는다.
그룹(Group)	파일을 소유하는 그룹, 부서와 동일한 기능이다. 회계부, 인사부 등
기타 사용자(Other User)	그 밖의 모든 사용자

[표 3] 리눅스의 권한별 역할

즉, 컴퓨터정보보안과 교수님이 소유자, 컴퓨터정보보안과 구성원 그룹이 소유그룹, 유니버설디자인과 학생은 기타 사용자가 되는 식이다.

이제 권한에는 어떤 것들이 있는지 자세히 알아보자. 리눅스의 권한은 읽기((Read), 쓰기(Write), 실행(Execute)의 세 가지로 나뉜다.

1) 절대 경로(Absolute Location) : 최상위 디렉토리부터 사용자가 위치한 경로, 현재 위치한 곳으로부터 목적지까지의 경로는 상대 경로이다.

권한	의미
읽기(Read)	파일의 내용을 읽는 권한(열람)
쓰기(Write)	파일의 내용을 수정하거나 디렉터리에 파일을 넣을 수 있는 권한
실행(Execute)	실행 파일을 실행하거나 디렉터리에 진입할 수 있는 권한

[표 4] 리눅스 권한의 의미

이제 권한에 관련된 명령어들을 알아보자. 권한 관리 명령은 슈퍼유저만 사용 가능하다.

명령	사용 예
chmod(change mode) - 파일의 권한 변경	구문 : # chmod [권한] [파일명] 예제 : # chmod u-r test 의미 : 사용자로부터 test 파일의 읽기 권한을 박탈
chgrp(change group) - 파일의 소유그룹 변경	구문 : # chgrp [변경할 그룹명] [파일명] 예제 : # chgrp knuw test 의미 : test파일을 knuw 그룹 소유로 변경
chown(change owner) - 파일의 소유자 변경	구문 : # chown [소유자]:[소유그룹] [파일명] 예제 : # chown test:knuw test 의미 : test 파일을 test 사용자와 knuw 그룹 소유로 변경

[표 5] 리눅스 권한 관리 명령

이렇게 파일과 디렉터리의 권한을 설정하는 것으로 제3자로의 파일 유출 및 해킹 등을 막을 수 있다.

2.3. 네트워크 보안

다음으로 네트워크 분야의 리눅스 보안 정책에 대해 알아보자, 우선 방화벽에 대해 살펴보겠다.

방화벽이란 대부분의 운영체제에 내장되어 있는 네트워크 트래픽을 제어하는 기능으로, 방화벽을 사용하면 외부에서 해킹을 시도할 경우 막아내는 기능을 한다.

리눅스의 방화벽 명령으로는 ufw, iptables, firewall-cmd 등이 존재한다. 차례로 살펴보자.

방화벽 역시 관리용 명령어이므로 슈퍼유저만 사용할 수 있다.

2.3.1. ufw - 우분투의 방화벽 명령

역 할	명령 사용 예
기본 구문	구문 : # ufw [allow/deny] [포트/프로토콜], 비활성화는 disable 예제 : # ufw deny 22 의미 : 22번 포트를 거부(SSH) 프로토콜을 생략할 경우 모든 프로토콜에 반영된다(TCP/UDP)
기본 규칙 보기	구문 : # ufw show raw 의미 : 기본 룰을 보여준다.
기본 규칙 허용/차단	구문 : # ufw default [allow/deny] 의미 : 기본/규칙을 허용 또는 차단한다.
규칙 제거	구문 : # ufw delete [규칙] 예제 : # ufw delete deny 22/tcp 의미 : TCP 프로토콜의 22번 포트를 거부하는 규칙을 제거, 즉 다시 허용
서비스명으로 허용/차단	구문 : 허용/차단 구문과 동일하지만 서비스명을 적는다. 예제 : # ufw [allow/deny] ssh 의미 : ssh를 허용하거나 거부하기 서비스명을 모를 경우 /etc/services를 확인
특정 아이피 허용/차단	구문 : # ufw [allow/deny] from [아이피] to any port [포트] proto tcp 예제 : # ufw allow from 192.168.0.123 to any port 22 proto tcp 의미 : 192.168.0.123 TCP 22번 허용
ping 허용/거부	기본은 허용으로 되어 있다 거부 방법 : /etc/ufw/before.rules 파일을 수정하여 ACCEPT를 DROP으로 변경

[표 6] ufw 명령

2.3.2. firewall-cmd - CentOS의 방화벽

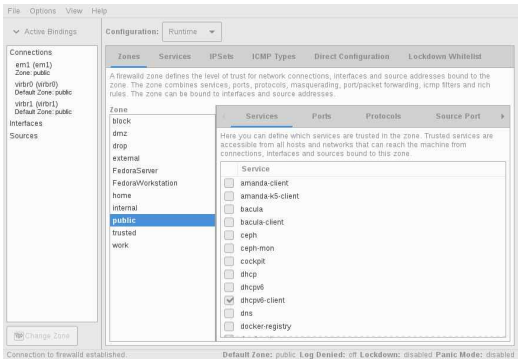
규칙을 Zone으로 명명해서 사용 가능하며 기본 Zone은 public(허용)이다.

역 할	명령 사용 예
Zone 목록 출력하기	# firewall-cmd --get-zones
기본 Zone 출력하기	# firewall-cmd --get-default-zone
현재 활성화된 Zone 출력하기	# firewall-cmd --get-active-zones
서비스 목록 보기	# firewall-cmd --list-all (특정 zone의 서비스 정보를 보려면 —zone=존이름 옵션을 추가)
서비스 추가/제거	구문 : # firewall-cmd --permanent --add-service=서비스명 예제 : # firewall-cmd --permanent --add-service=ftp 의미 : FTP서비스를 방화벽에 추가[1)] (제거는 add부분을 remove로 바꾸면 된다)
포트 추가	구문 : # firewall-cmd --permanent --add-port=포트번호/프로토콜 예제 : # firewall-cmd —permanent --add-port=21/tcp 의미 : tcp 21포트 추가[2)]
방화벽 리로드(재시작)	# firewall-cmd --reload
실행 여부 확인	# firewall-cmd --state
zone 추가	구문 : # firewall-cmd —permanent --new-zone=[zone 이름] 예제 : # firewall-cmd —permanent --new-zone=sanghoon 의미 : sanghoon zone 생성 (재시작 후 반영됨) (제거는 new를 delete로 변경)

[표 7] firewall-cmd

1) (이때 permanent를 생략하면 한시적으로 추가된다, 그 때는 방화벽을 리로드하면 사라진다)
2) (이때 permanent를 생략하면 한시적으로 추가된다, 그 때는 방화벽을 리로드하면 사라진다)

firewall-config로 GUI로도 사용 가능하다.



[사진 4] firewall-config 명령

2.3.3. iptables - 모든 리눅스 배포판의 NetFilter 정책 관리 도구

다음으로 iptables 명령을 살펴보겠다. iptables는 리눅스 커널에 있는 Net Filter의 정책을 관리하는 도구이다. Net Filter는 리눅스 커널에 있는 패킷 필터링을 담당하는 기능이다.

다시 말해서 패킷 필터링 규칙을 관리하는 도구가 iptables이다.

기본 구문은 다음과 같이 사용한다.

iptables -t [테이블] [엑션] [체인] [매치] -j [타겟]

1. 테이블

규칙들이 모인 그룹을 나타내며 3가지가 있다.

테이블	설 명
Filter	가장 많이 사용하는 테이블이며, 트레픽 통제를 한다. 명시하지 않으면 기본으로 사용하는 테이블
NAT	들어오는 패킷을 다른 포트나 다른 호스트 서버로 라우팅하는 역할이다.
Mangle	패킷의 헤더를 바꾼다.

[표 8] iptables - 테이블

2. 액션

액션은 명령을 가리키는 말로 아래 7가지 옵션이다.

액션	설명
-A(APPEND)	정책을 추가한다(가장 마지막에)
-I(INSERT)	정책을 삽입한다(임의로 순서 지정 가능)
-D(DELETE)	정책을 삭제한다.
-F(FLUSH)	모든 정책을 삭제한다.
-R(REPLACE)	정책을 교체한다.
-P(POLICY)	기본 정책을 설정한다.
-L(LIST)	정책을 나열한다.

[표 9] iptables - 액션

3. 체인

체인은 패킷의 흐름을 제어하는 것이다. FILTER 테이블의 체인은 아래 3가지이다.

체인	설명
INPUT	들어오는 패킷
OUTPUT	나가는 패킷
FORWARD	통과하는 패킷

[표 10] iptables - 체인(Filter 테이블)

NAT 테이블의 체인은 2가지이다.

체인	설명
POSTROUTING	내부 네트워크에서 방화벽을 통해 외부로 나갈 때
PREROUTING	외부에서 방화벽으로 내부로 들어갈 때

[표 11] iptables - 체인(NAT 테이블

4. 매치

매치는 조건을 가리키는 것으로 아래 5가지이다.

매치	설명
-s(source)	출발지를 지정
-d(destination)	도착지를 지정
-p(protocol)	프로토콜 지정
-i(input)	입력 인터페이스 지정
-o(output)	출력 인터페이스 지정

[표 12] iptables - 매치

5. 타겟

타겟은 동작을 나타내고 아래 5가지이다.

타겟	설명
ACCEPT	패킷을 받아들인다.
DROP	패킷을 버린다.
REJECT	패킷을 버리고 이와 동시에 적절한 응답 패킷을 전송한다.
LOG	패킷을 syslog에 기록한다.
RETURN	호출 체인 내에서 패킷 처리를 계속한다.

[표 13] iptables - 타겟

살펴본 구문으로 iptables 명령의 사용 예를 살펴보면 다음과 같다.

명령	설명
# iptables -A INPUT -s [아이피] -j DROP	특정 아이피를 차단한다.
# iptables -A INPUT -p tcp --dport [포트] -j ACCEPT	특정 포트를 허용한다, -p tcp 이니 tcp 프로토콜

[표 14] iptables - 종합 예제

이렇게 리눅스에서 방화벽을 이용하면 해킹으로부터 시스템을 지킬 수 있다.

3. 리눅스의 보안 취약점

다음으로 리눅스 서버의 취약점에는 어떤 것들이 있는지 사례와 함께 살펴보자.

3.1. 리눅스 툴 해킹 위험 사례

카퍼스키(Kaspersky)는 러시아에 소재하는 사이버 보안 연구 기업이다. 해당 기업의 연구진들이 최근 리눅스 툴을 겨냥한 해킹 방식이 더욱 다양화되고 있다고 밝혔다.

서론에서 살펴보았듯 대기업이나 정부 기관 등에서 리눅스를 사용하기에 많은 주의가 필요하다. 또한 연구진 중 한 명인 유리 나메스트니코프는 해커들이 리눅스의 활용성을 악용해 공격 툴을 생성하고 시스템을 공격하는 것에 대한 걱정을 표현했다.

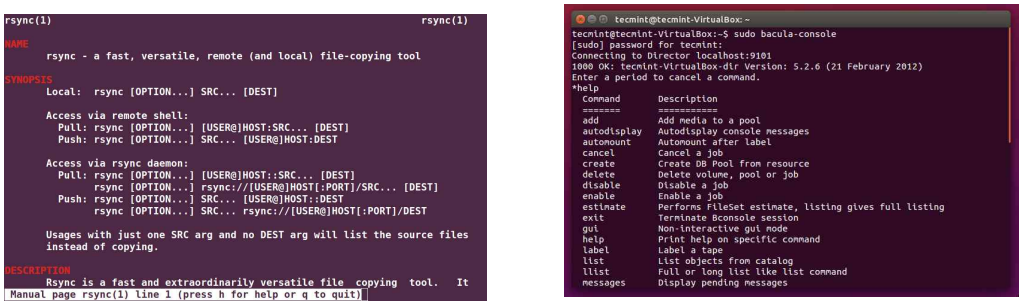
카퍼스키 측은 리눅스를 사용하는 기관에 신뢰할 수 없는 소프트웨어 소스 사용을 자제하는 등의 조치를 권고했다. 한편 가장 최근의 해킹 사례는 라이트스파이나 웰메스를 이용한 해킹 사례가 있다. 두 가지 모두 윈도우와 리눅스를 대상으로 삼았으며 라이트스파이의 경우 iOS 기기와 맥OS 기기에서도 발견되었다.

해당 취약점을 해결하기 위해서는, 첫째. 소프트웨어 소스 목록과 프로그램들을 항상 최신으로 유지해야 한다. 관련 명령은 다음과 같다.

명령	설명
# apt update	패키지 저장소 목록 갱신
# apt upgrade	프로그램 업그레이드

[표 15] 리눅스 패키지 관련 명령(우분투)

둘째. 해킹 시 데이터가 유실될 것을 대비해 상시 백업해 놓아야 한다. 해킹을 당하게 될 시 공격자가 마음먹은 대로 뭐든지 할 수 있게 되기 때문에 데이터가 유실될 가능성을 염두해 두고 상시 백업해 놓아야 한다. 일부 백신 프로그램에서 백업 기능을 제공하거나 전문 백업 소프트웨어가 많이 존재하니 참고하자. 아래 그림은 일부 백업 소프트웨어이다.



[사진 5] 백업 툴 Rsync(좌) 와 Bacula(우)

3.2 OpenWRT 포럼 해킹 사례

다음으로 OpenWRT 포럼이 해킹을 당한 사례를 살펴보자.

OpenWRT 포럼은 리눅스 기반 임베디드 운영 체제를 위한 오픈 소스 프로젝트이다. 지난 해 1월 19일자 데일리시큐의 보도에 따르면 OpenWRT 포럼의 사용자 데이터가 해커에 의해 유출되는 사고가 발생한 것으로 나타났다. 유출된 정보는 이메일 주소, 포럼 사용자에 대한 기타 통계 정보가 포함된 사용자 목록 사본이다. 이에 대한 대책으로 포럼 관리자는 비밀번호와 API 키를 재설정하는 등의 조치를 취했다.

해당 취약점을 해결하기 위해서는, 첫째. 출처가 불분명한 메일은 스팸일 수 있으므로 열지 않도록 한다. 어떤 위험이 있을지 모르기 때문이다. 따라서 스팸 메일을 받으면 지인에게 연락하여 확인하고 삭제하는 것이 좋다.

둘째. API 키나 토큰 등은 절대 노출하지 않도록 주의한다. API 키 또는 토큰이라고 함은 개발자가 앱 등을 개발할 때 앱에서 해당 서비스에 접근할 수 있도록 하는 열쇠 역할을 한다. 따라서 API 키나 토큰을 노출하면 제삼자가 해당 서비스에 접근할 수 있게 되기에 위험하다.

3.3 11년 묵은 버그 사례

다음으로 리눅스 개발 초기 단계에서 발생한 버그가 11년이 지난 지금까지 방치되고 있는 사례를 살펴보자. 버그(Bug)란 사전적 정의로는 '벌레' 라는 의미로 프로그램이나 운영체제의 개발 소스 코드의 자잘한 오류를 의미한다. 16년 10월 25일 디지털타임스의 보도에 의하면, DirtyCow(번호 CVE-2016-5195)라는 취약점이 리눅스 개발 초기부터 지금까지 해결되지 않고 방치되고 있는 것으로 나타났다.

보안 전문가 필 외스터는 리눅스의 초기 개발자 리누스 토발즈가 이를 발견하여 패치를 시도했으나 잘 해소되지 않고 있다고 말했다. 이를 악용할 경우 리눅스의 커널 단계에서 메모리 운영 중에 메모리 시스템을 파괴해 시스템에 장애를 가져올 수 있다는 설명이다. 또 루트 서버 접근 권한을 탈취해 서버를 조작할 수도 있게 된다.

해당 취약점을 해결하기 위해서는 커널을 최신 버전으로 업그레이드하여야 한다. kernel.org 사이트에서 커널 파일을 다운로드 받을 수 있는데, 현재 최신 버전은 5.19.12 버전이다. 커널을 업그레이드하는 이유는 새로운 기능이나 장치를 정상적으로 활용하고 이전에 발견된 취약점으로부터 시스템을 보호하기 위함이다. 필자는 이 사례가 시간이 지나도 버그는 버그라는 점을 상기시켜 주는 사례라고 본다.

3.4 리눅스와 컨테이너 해킹 사례

다음 사례를 보자. 트렌드 마이크로(Trend Micro)는 미국 LA에 소재하는 보안 업체이다. 작년 8월 24일 보안뉴스의 기사에 따르면, 트렌드 마이크로가 멀웨어를 심기 위해 리눅스 시스템과 컨테이너를 해킹하는 200개 취약점을 조사해 정리한 것으로 밝혀졌다.

그 결과 43%가 아마존 리눅스, 29%가 레드햇 엔터프라이즈 리눅스, 15%가 우분투, 8%가 CentOS에서 발생하였다. 또한 웹 기술 연구 기업인 W3Techs가 발표한 바에 따르면 모든 웹사이트들의 77%가 유닉스(Unix)를 운영하고 있으며, 대다수가 리눅스를 운영하고 있다고 한다. 트랜드 마이크로는 인터넷에 노출된 애플리케이션들과 워크로드의 경우 대부분 '웹 애플리케이션 공격'이라는 유형의 해킹 공격을 받습니다. 웹 애플리케이션 공격을 제대

로 수행해 성공시켰을 경우 공격자들은 대부분 임의 스크립트를 실행시키거나, 기밀을 침해하거나, 각종 데이터를 조작 및 파괴, 유출시킬 수 있게 됩니다." 라고 설명했다.

해당 취약점의 해결책으로는 첫째. 알려지지 않은 링크는 클릭하지 말도록 한다. 웹 애플리케이션은 대부분 웹사이트에서 구동되기 때문에 알려지지 않은 링크를 방문할 경우 취약점에 노출될 우려가 있다. 알고 있는 링크이거나 본 적이 있는 링크가 아니라면 주의하자.

둘째, 해당 링크가 SSL[1]을 지원하는지 확인한다. SSL이 적용되면 프로토콜이 https가 되며, 연결이 암호화되어 더 안전하다. SSL이 없으면 연결이 되지 않는 것은 아니지만 암호화가 되지 않아 인터넷에 입력한 정보(카드번호, 생년월일 등)가 노출될 우려가 있다.

무료인 리눅스이지만 지속적인 패치와 보안 업데이트가 필요하다고 본다.

3.5 리눅스 권한 상승(sudo) 명령 취약점

마지막으로 리눅스에서 권한을 승격하는 명령인 sudo 명령에서 발견된 취약점에 대해서 살펴보자.

리눅스에는 /etc/sudoers 라는 파일이 있는데, 이 파일은 어떤 사용자가 관리자로 승격할 권한이 있는지 설정하는 파일이다. 해당 파일에서 루트 엑세스를 허용하지 않았음에도 승격이 되는 문제가 이 취약점이다.

'superuser do'의 약자인 SUDO는 사용자가 환경을 전환하지 않고 다른 사용자의 권한으로 응용 프로그램 또는 명령을 실행할 수 있게 하는 시스템 명령으로, 대부분 루트 사용자로 명령을 실행하기 위해 이용된다.

해당 취약점은 사용자 아이디가 음수가 되거나 최대값으로 오버플로우 되면서 루트권한을 획득한다. 해결책으로는, 첫째. 중요한 일을 하는 사용자가 아니라면 표준 사용자로 만들어야 한다. 그 이유는 표준 사용자 계정은 시스템 파일에 접근할 수 없게 되어 있기 때문에 문제를 사전 차단할 수 있다.

둘째. 어떠한 경우에도 패스워드는 노출해선 안 된다. 특히 슈퍼유저의 비밀번호가 노출되면 비밀번호를 취득해 로그인만 하면 모든 일을 할 수 있기 때문에 각별한 주의가 요구된다. 심지어 시스템을 파괴할 수도 있다.

셋째. 본 논문에서 살펴본 권한 변경 명령으로 sudoers를 막어놓는 것도 방법이 될 수 있다. 그러면 슈퍼유저와 관리자 외에는 건드릴 수가 없게 되어 보안의 방패가 더 탄탄해진다고 할 수가 있다.

4. 결론

지금까지 리눅스가 여러 보안 분야에서 어떻게 활용되는지 분야별로 자세히 살펴보았다. 이처럼 여러 분야에서 활용되지만 취약점도 존재하므로 안심할 수는 없는 운영체제가 바로 리눅스인 것이다. 무료이고 사용성도 높은 리눅스인 만큼 본 연구에서 살펴본 것들을 적재적소에 잘 활용한다면 리눅스가 가지는 장점들도 잘 다듬어 나갈 수 있을 것이며, 또 리눅스 고유의 보안 정책을 활용해 해킹으로부터 시스템을 지키는 등 나만의 보안 지킴이 운영체제로도 사용할 수 있을 것이고, 결국 리눅스 전체의 위상을 드높여 리눅스를 MS 윈도 못지않게 안심하고 사용할 수 있는 운영체제로 탈바꿈시키는 데 큰 역할을 할 것으로 기대된다.

---

1) SSL(Secure Socket Layer) : 인터넷 연결을 암호화하는 프로토콜

참고문헌

[1] https://ko.wikipedia.org/wiki/우분투 -> 1-3. 리눅스 배포판의 종류[사진3. 우분투)
[2] https://www.plesk.com/blog/business-industry/industry-insights-ubuntu-vs-centos-linux-os-matter/ -> 1-2 리눅스의 특징[사진2)

[3] https://ko.wikipedia.org/wiki/우분투 -> 1-3. 리눅스 배포판의 종류[사진3. 우분투)
[4] https://ko.wikipedia.org/wiki/레드햇_엔터프라이즈_리눅스
[5] https://ko.wikipedia.org/wiki/CentOS -> 그림4. CentOS
[6] https://m.blog.naver.com/jypit/221100878526 -> 사용자 계정 설명
[7] https://firewalld.org/documentation/utilities/firewall-config.html -> 방화벽
[8] http://www.codingworldnews.com/news/articleView.html?idxno=1514 -> 3.1 취약점
[9] https://www.dailysecu.com/news/articleView.html?idxno=119773 -> 3.2
[10] http://www.dt.co.kr/contents.html?article_no=2016102502109960813001 -> 3.3
[11] https://www.boannews.com/media/view.asp?idx=100087&direct=mobile -> 3.4
[12] https://itwiki.kr/w/%EB%A6%AC%EB%88%85%EC%8A%A4_iptables -> iptables
[13] https://bcho.tistory.com/1366 -> iptables
[14] https://www.digitalocean.com/community/tutorials/top-best-linux-distros-for-laptops -> 배포판 점유율 부분 부가 설명
[15] https://www.tecmint.com/linux-system-backup-tools/ -> 3.1 백업 설명 자료
[16] https://kernel.org/ -> 3.3 커널 설명 자료(캡처)
[17] https://namu.wiki/w/Pop!_OS