보안의 가장 효과적인 방법은 웹 서버같이 비무장 지대에 위치하는 서버는 네트워크를 사내 네트워크와 분리하고 웹 서버의 권한을 낮추고 접근할 수 있는 네트워크를 최소화 하는 것. 즉, 화이트리스트기반 보안.

Selniux를 이해하기 위한 필수 지식

**접근 통제**

운영체제에서 접근 통제(Access Control)이란 디렉터리나 파일, 네트워크 소켓 같은 시스템 자원을 적절한 권한을 가진 사용자나 그룹이 접근하고 사용할 수 있게 통제하는 것을 의미한다.

접근 통제에서는 시스템 자원을 객체(Object)라고 하고 그 자원에 접근하는 사용자나 프로세스는 주체(Subject)라고 한다.

Ex) /etc/passwd 파일을 객체(Object)이고 이 파일에 접근해서 암호를 변경하는 passwd는 주체(Subject)

**임의 접근 통제(DAC: Discretionary Access Control)**

시스템 객체에 대한 접근을 사용자나 또는 그룹의 신분을 기준으로 제한하는 방법이다.

즉, 객체의 소유자가 다른 주체(Subject)에 대해 이 객체(Object)에 대한 접근 권한을 설정할 수 있다.

소유자가 판단에 의해서 권한을 줄 수 있어서 구현에 용이하고 사용에 간편하기 때문에 전통적으로 유닉스나 윈도우등 대부분의 OS 에서 기본 접근 통제 모델을 사용하고 있다.

하지만 단점으로는 사용자의 권한을 탈취당하면 사용자가 소유 하고 있는 모든 객체의 권한을 가질 수 있다.

**Setuid/setgid 문제**

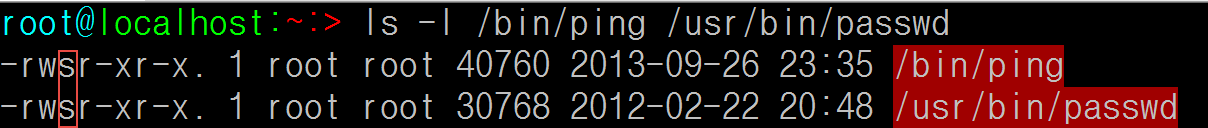
사용자들의 암호는 /etc/shadow에 저장되어 있고 루트만 읽고 쓸수 있다.

하지만 사용자들을 passwd 명령어를 실행하면 자신의 암호를 변경할 수 있고 이때 /etc/shadow 파일이 수정이 된다.

상대방 호스트가 동작하는지 확인하기 위해 사용하는 ping 또한 ICMP(Internet Control Message Protocol) 패킷을 사용하므로 루트 권한이 필요하지만 일반 사용자들도 ping 명령어를 사용하여 상대 호스트의 이상 여부를 확인 할 수 있다.

setuid(Set user ID upon execution) 또는 setgid(set group ID upon execution)는 비트라는 것을 설정할 수 있으며 이 비트가 설정되어 있을 경우 해당 프로그램을 실행하면 실행시점에 설정된 사용자(setuid) 또는 그룹(setgid) 권한으로 동작한다.

즉, passwd 나 ping 같이 실행시 루트 권한이 필요한 프로그램은 소유자를 root로 하고 setuid를 설정하면 실행 시점에 root 사용자로 전환되므로 root만이 가능한 동작을 수행할 수 있다.



파일의 사용자 퍼미면 부분의 s는 setuid 비트이고 그룹의 퍼미션 부분에 s 표시가 있을 경우 setgid 비트로 passwd 와 ping은 setuid 비트만 설정되어 있는 것을 알 수 있다.

**잘 알려진 포트 daemon 문제**

Well-know port는 IANA에서 할당한 TCP 및 UDP 포트 번호의 일부로 1024 미만의 포트 번호를 갖게 된다.

예를 들어 웹에서 사용하는 http(80), 메일 전송 smtp(25), 파일전송 ftp(20,21)

전통적으로 알려진 포트는 루트만이 사용할 수 있으므로 데몬 서비스는 모두 루트의 권한으로 가동된다.

즉, 보안문제는 여기서 발생이 된다. 루트로 구동이 되었으므로 만약 서비스 데몬이 보안 취약점이 있거나 잘못된 설정이 있을 경우 서비스 데몬을 통해서 공격자는 루트 권한을 획득하게 되며 시스템의 모든 자원에 접근이 가능해 진다.

**강제 접근 통제**

강제 접근 통제(MAC – Mandatory Access Control)는 미리 정해진 정책과 보안 등급에 의거하여 주체에게 허용된 접근 권한과 객체에게 부여된 허용등급을 비교하여 접근을 통제하는 모델이다.

높은 보안을 요구하는 정보는 낮은 보안 수준의 주체가 접근할 수 없으며 소유자라고 할지라도 정책에 어긋나면 객체에 접근할 수 없으므로 강력한 보안을 제공한다.

MAC 정책에서는 루트로 구동한 http 서버라도 접근 가능한 파일과 포트가 제한이 된다. 즉 취약점을 이용하여 httpd의 권한을 획득 했어도 /var/www/html, /etc/httpd등의 사전에 허용한 폴더에만 접근 가능하며 80,443,8080 등의 포트만 접근이 허용되므로 ssh로 다른 서버로 접근을 시도하는 등 2차 피해가 최소화된다.

단점으로는 구현이 복잡하고 어려우며 모든 주체와 객체에 대해서 보안 등급과 허용 등급을 부여하여야 하므로 설정이 복잡하고 시스템 관리자 접근 통제 모델에 대해 잘 이해하고 있어야 한다.

**SELinux란**

NSA(National Security Agency)에서 개발한 플라스크(Flask)라는 MAC 기반의 보안 커널을 리눅스에 이식한 커널 레벨의 보안 모듈이다.

RHEL 기반의 배포판에서 4 버전부터 공식적으로 포함 되어있다.

**SELinux는 기존 접근 통제 규칙보다 먼저 동작하므로** SELinux의 보안 정책에 맞이 않을 경우 차단해 버린다.

**장점**

1. 사전 정의된 접근 통제 정책 탑재
   1. 사용자,역할, 타입, 레벨 등의 다양한 정보를 조합하여 어떤 프로세스가 어떤 파일, 디렉터리, 포트 등에 접근 가능 한지에 대해 사전에 잘 정의된 접근 통제 정책이 제공됨
2. “Deny All, Permit Some” 정책으로 잘못된 설정 최소화
   1. SELinux는 위 방식으로 사전에 설정되어 있으므로 설정이 기본 포함돼 있을여지가 적다.
3. 권한 상승 공격에 의한 취약점 감소
   1. Setuid 비트가 켜져 있거나 루트로 실행되는 프로세스처럼 위험한 프로그램들은 샌드박스 안에서 별도의 도메인으로 격리되어 실행되므로 루트 권한을 탈취해도 해당 도메인에만 영향을 미치고 전체 시스템에 미치는 영향이 최소화된다

Ex) 아파치 httpd 서버의 보안 취약점을 통해 권한을 획득 했어도 아파치 같은 서버 데몬은 낮은 등급의 권한을 부여 받으므로 공격자는 일반 사용자의 홈 디렉토리를 읽을 수 없고 /tmp 임시 디렉터리에 파일을 쓸수가 없다.

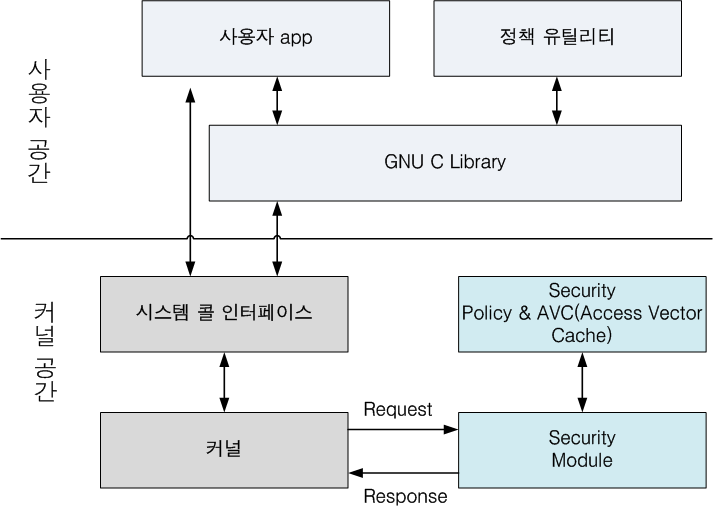
1. 잘못된 설정과 버그로부터 시스템 보호
   1. 잘못된 설정이나 신뢰할 수 없는 입력을 아굥한 공격에서 프로세스를 보호할 수 있습니다.

**SELinux 사용하기**

**동작모드**

AVC(Access Vector Cache)라는 이름으로 커널의 기본 기능으로 동작한다.

모든 시스템 콜이 보안 정책을 확인하기 위해 AVC라는 이름으로 커널 내부에서 캐싱한다.



SELinux는 enforce, permissive, disable 3가지 모드가 있다. 기본설정은 enforce mode이므로 보안 정책에 위배되는 모든 액션을 차단한다.

Permissive mode는 경고 메시지를 내고 차단하지는 않는다.

setenforce 명령어를 사용하여 1을 주면 enforce모드 0을 주면 permissive mode로 전환할수 있다.

**Security Context**

**SELinux는 모든 프로세스와 객체마다 보안 컨텍스트(Security Context)이라고 부르는 정보를 부여하고 있다.**

**이 정보는 접근 권한을 확인하는데 사용하고 있으면 SELinux를 이해하기 위한 핵심요소이다.**

총 4가지로 이루어져 있다.

|  |  |
| --- | --- |
| 요소 | 설명 |
| 사용자 | 시스템의 사용자와는 별도의 SELinux 사용자이고 역할이나 레벨과 연계하여 접근 권한을 관리하는데 사용. |
| 역할  (Role) | 하나 혹은 그 이상의 타입과 연결되어 SELinux의 사용자의 접근을 허용할지 결정하는데 사용 |
| 타입  (Type) | Type Enforcement의 속성중 하나로 프로세스의 도메인이나 파일의 타입을 지정하고 이를 기반으로 접근 통제를 수행한다. |
| 레벨  (Level) | 레벨은 MLS(Multi Level System)에 필요하고 강제 접근 통제보다 더 강력한 보안이 필요할 때 사용하는 기능. 적은 사람도 모른다고 한다. |

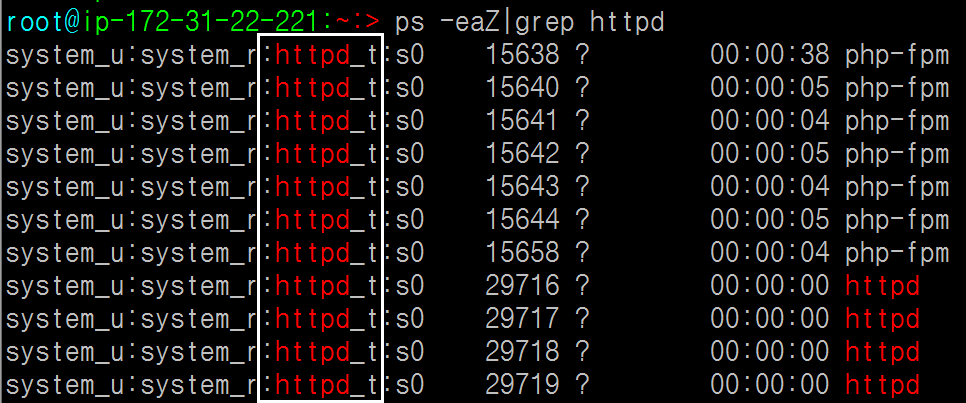
제일 중요한 부분은 타입(Type)이다. SELiux를 활성화하면 파일이나 디렉터리등의 객체마다 보안 컨텍스를 부여한다.

SELinux가 도입되면서 ls, ps, cp, mv등의 유틸리티에는 -Z, --context옵션이 추가 되었다.



Ls -ldz 명령어로 컨텍스트를 볼수 있다.

Httpd\_sys\_content\_t 이므로 보안 컨텍스트가 부여된 객체에 접근이 허용되므로 nginx는 /var/www/html/ 에 있는 컨턴츠를 읽을 수 있다.



Ps -ezZ|grep httpd 명령어를 실행해서 프로세스의 컨텍스를 확인할 수 있다.

**Type Enforcement**

TE(Type Enforcement)는 SELinux의 기본적인 접근 통제를 처리하는 매커니즘으로 **주체(Subject)가 객체(Object)에 접근할려고 할 때 주체(Subject)에 부여된 보안 컨텍스트가 객체에 접근할 권한이 있는지 판단하는 역할을 수행한다.**

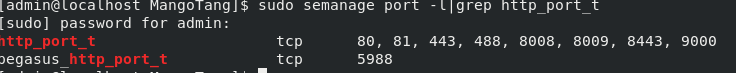
Ex) httpd가 /static/images/banner.jpg에 접근하려고 할 때 웹서버 nginx는 주체(subject)가 되며/static/images/banner.jpg는 객체(object)가 되며 nginx 웹 서버에 부여된 보안 컨텍스트는 httpd\_t가 된다.

Httpd\_sys\_content\_t 이므로 보안 컨텍스트가 부여된 객체에 접근이 허용되므로 nginx는 /var/www/html/ 에 있는 컨턴츠를 읽을 수 있다.

즉, 사전에 탑재된 httpd에 대한 정책에 의하면 httpd\_sys\_content\_t 가 붙은 컨텐츠만 읽을 수 있고 /var/www 아래에 파일을 생성하면 자동으로 httpd\_sys\_content\_t가 붙게 됩니다.

그러므로 /data/myweb-app 폴더를 만들고 이 안에 웹 서비스할 파일을 넣고 httpd에 DocumentRoot를 설정해도 SELinux는 미리 허용된 경로가 아니므로 차단시켜서 permission denied에러만 나게 된다.

**마찬가지로 httpd가 접근할 수 있게 사전에 허용된 context는 http\_port\_t 이며** semanage 명령어로 해당 포트 목록을 조회할 수 있다. Semanage port -l | grep http\_port\_t



즉, Type Enforcement로 인해 공격자가 “제로 데이 취약점”을 사용하여 httpd의 권한을 획득해도 다른 ssh 서버로 연결이 불가능하다. 왜냐하면 위 포트들 빼고 권한이 없기 때문이다.

**Context 정보 얻기**

SELinux의 문제를 해결하기 위해서 context 정보를 확인하고 이를 맞춰 주는게 중요하다.

이작업을 용이하게 하기 위해 context 정보를 확인할 수 있는 패키지를 설치한다.

Yum install setools-console

**seinfo**

seinfo 는 policy를 조회하고 출력해주는 유틸리티이다.

-a 옵션으로 조회할 속성을 지정할 수 있으며 다음 명령어는 전체 도메인을 출력한다.

Seinfo -adomain -x

**sesearch**

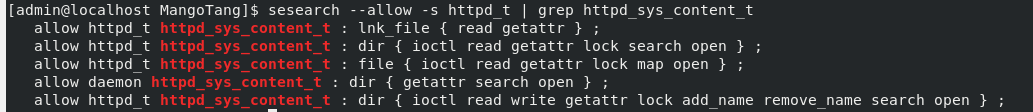
sesearch는 정책에서 지정한 룰을 조회할 수 있는 유틸리티입니다.

다음 명령어는 httpd\_sys\_content\_t 객체에 접근할 수 있는 룰그룹을 표시한다.

Sesearch --role\_allow -t httpd\_sys\_content\_t

--allow 옵션을 사용하면 특정 context에 허용된 액션을 알 수 있다.

Sesearch –allow -s httpd\_t



Httpd\_sys\_content\_t 가 설정된 파일에 대해 ioctl, read, getattr, lock, open system call 이 가능하다.즉, httpd\_t는 http\_sys\_content\_t 컨텐츠를 읽을 수 가 있습니다.

**semanage**

SELinux 에서 서비스가 안 도는 것은 보안 정책에 어긋나서이고 위에서 설명한 seinfo, sesearch 로 정책을 조회한 후 조치를 해야한다.

Ex) mysql을 3307 로 구동했다면 허용된 포트가 아니므로 web서버가 mysql에 연결할 수 없으며 허용된포트를 사용하거나 정책을 수정하는 semanage. 명령어로 변경된 정보를 SELinux 에게 알려주면 됩니다.

Semanage.는 SELinux의 보안 정책을 조회하고 추가/변경/삭제할 수 있는 명령행 기반의 유틸리티입니다.

보안 컨텍스트는 파일이나 네트워크 포트, 네트워크 인터페이스 등이며 이중에서 서비스 데몬이 SELinux 에서 문제 없이 동작하려면 꼭알아 두어야 할것이 파일과 네트워크 포트 컨텍스트이다.

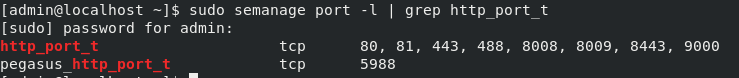
Semanage 를 사용하기 위해서 아래 패키지를 설치해야한다.

Yum install -y policycoreutils-python

**포트 컨텍스트**

Httpd 가 연결할 수 있는 포트 정보를 알아보는 명령어다

Semanage port -l | grep http\_port\_t



즉, 위 포트 이외의 접근은 SELinux가 막는다.

포트를 추가하는 방법은

Semanage port -a -p tcp -t http\_port\_t 9876

만약 이미 할당된 context가 있으면 -a 대신 -m 사용

Semanage port -m -p tcp -t http\_port\_t 9876

포트 삭제 명령어

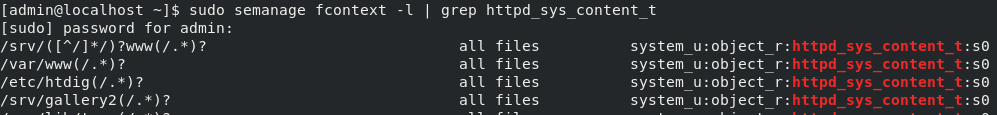
Semange port -d -p tcp -t http\_port\_t 9876

포트 삭제 추가 과정


**파일 컨텍스트**

파일 컨텍스트는 fcontext 아규먼트를 추가하면 된다. 웹 서버의 컨텐츠에 지정하는 httpd\_sys\_content\_t 가 할당된 파일 경로 찾는 명령어는 아래 명령어이다.

Semanage fcontext -l | grep httpd\_sys\_content\_t



/var/www(/.)? 의 의미는 /var/www 밑에 생성되는 모든 파일과 폴더는 http\_sys\_content\_t\* 를 붙이라는 의미이다.

즉, 웹서버 컨텐츠가 /opt/mycontent에 있다면 이후에 이 폴더에 생성한 모든 파일과 폴더에 httpd\_sys\_content\_t를 붙여야 정상적으로 서비스가 가능하다. 설정하는 명령어는 아래와 같다.

Semanage fcontext -a -t httpd\_sys\_content\_t “/opt/mycontent(/.\*)?”





sudo setsebool -P httpd\_read\_user\_content 1

**파일 컨텍스트**

로그보기

yum install audit

ausearch -m AVC,USER\_AVC -ts 05/13/2016

간편보기

yum install setroubleshoot-server

sealert -a /var/log/audit/audit.log

Ausearch -m AVC | audit2why 왜 차단했는지 보여줌

Ausearch -c ‘nginx’ –raw | audit2allow -M my-nginx

Semodule -I my-nginx.pp