Зертханалық сабақ №9: SELinux саясатының жұмыс механизмі. Қол жеткізу ережелерін сипаттау тілі

sudo apt install policycoreutils SE-Linux-пен жұмыс жасау барысында ақаулар болмас үшін консольға енгізіңіз

Security-Enhanced Linux (SELinux) - Linux Security (LSM) ядромодуліненегізделген Linux-қакірудібасқарудыңжаңаәдісі. SELinux әдепкібойынша Fedora, CentOS жәнет. б. сияқты rpm пакеттікбазасынқолданаотырып, Red Hat негізіндегікөптегендистрибуциялардақосылады.

SELinux практикалық мәні неде екенін түсіну үшін стандартты қол жеткізуді басқару жүйесі жеткіліксіз болған кезде бірнеше мысалды қарастырыңыз. Егер SELinux өшірулі болса, онда сіз тек DAC (селективті қол жеткізуді басқару) немесе ACL(қол жеткізуді басқару тізімдері) кіретін классикалық қол жетімділікті басқару жүйесіне қол жеткізе аласыз. Яғни, бұл кейбір жағдайларда жеткіліксіз болуы мүмкін пайдаланушылар мен пайдаланушылар топтары деңгейінде жазу, оқу және орындау құқықтарын басқару туралы. Мысалы

- Әкімші пайдаланушының әрекеттерін толық басқара алмайды. Мысалы, пайдаланушы барлық басқа пайдаланушыларға SSH кілттері сияқты жеке құпия файлдарды оқу құқығын бере алады.

- Процестер қауіпсіздік параметрлерін өзгерте алады. Мысалы, пайдаланушы поштасы бар файлдар тек бір нақты пайдаланушыға оқуға қол жетімді болуы керек, бірақ электрондық пошта клиенті бұл файлдарды барлығына оқуға болатындай етіп кіру құқығын өзгерте алады.

- Процестер оларды іске қосқан пайдаланушының құқықтарын мұра етеді. Мысалы, Firefox шолғышының троянмен жұқтырған нұсқасы пайдаланушының SSH кілттерін оқи алады, бірақ бұл үшін ешқандай себеп жоқ.

Негізінен, қол жеткізуді басқарудың дәстүрлі моделі (DAC) қол жетімділіктің тек екі деңгейін — пайдаланушы мен супер пайдаланушыны жақсы жүзеге асырады. Әрбір пайдаланушы үшін қажетті артықшылықтар минимумын орнатуға мүмкіндік беретін қарапайым әдіс жоқ.

Әрине, классикалық қауіпсіздік моделінде осы проблемаларды айналып өтудің көптеген әдістері бар, бірақ олардың ешқайсысы әмбебап емес.

SELinux-та қолданылатын негізгі терминдер:

Домен-бұл процесті орындай алатын әрекеттер тізімі. Әдетте, процесс жұмыс істей алатын ең аз мүмкін әрекеттер жиынтығы домен ретінде анықталады. Осылайша, егер процесс беделге ие болса, шабуылдаушы көп зиян келтіре алмайды.

Рөл-қолдануға болатын домендердің тізімі. Егер доменнің тізімінде қандай да бір рөл болмаса, онда осы доменнің әрекеттерін қолдану мүмкін емес.

Түрі-объектіге қатысты рұқсат етілетін әрекеттер жиынтығы. Түрі доменнен ерекшеленеді, өйткені оны пайпаларға, каталогтарға және файлдарға қолдануға болады, ал домен процестерге қолданылады.

Қауіпсіздік контексті — барлық SELinux атрибуттары-рөлдер, типтер және домендер.

1.2 дәстүрлі қауіпсіздік моделінің мәселелерін шешу.

SELinux әр қызмет, пайдаланушы және бағдарлама үшін ең аз қажетті артықшылықтар моделін қатаң сақтайды. Әдепкі бойынша," тыйым салу режимі " орнатылады, онда жүйенің әр элементінде оның жұмыс істеуі үшін қажетті құқықтар ғана болады. Егер пайдаланушы, бағдарлама немесе қызмет файлды өзгертуге немесе оларды шешу үшін қажет емес ресурсқа кіруге тырысса, онда оларға кіруден бас тартылады және мұндай әрекет журналда тіркеледі.

SELinux жұмыс режимдері

SELinux үш негізгі жұмыс режиміне ие, әдепкі бойынша Enforcing режимі орнатылған. Бұл өте қатаң режим және қажет болған жағдайда оны соңғы пайдаланушыға ыңғайлы етіп өзгертуге болады.

Enforcing: әдепкі Режим. Бұл режимді таңдағанда, Қазіргі қауіпсіздік саясатын қандай да бір жолмен бұзатын барлық Әрекеттер бұғатталады және бұзушылық әрекеті журналға жазылады.

Тұрақты: егер бұл режим қолданылса, қазіргі қауіпсіздік саясатын бұзатын барлық әрекеттер туралы ақпарат журналға жазылады, бірақ іс-әрекеттің өзі бұғатталмайды.

Disabled: мәжбүрлі қол жеткізуді басқару жүйесін толығымен өшіру.

Сіз ағымдағы режимді және басқа SELinux параметрлерін (қажет болған жағдайда оны өзгертіңіз) басқару мәзірінде қол жетімді арнайы GUI құралын (system-config-selinux) көре аласыз. Егер сіз консольде жұмыс істеуге дағдыланған болсаңыз, онда сіз sestatus командасымен ағымдағы күйді көре аласыз.

```
#sestatus

SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

Сондай-ақ, SELinux күйін getenforce командасының көмегімен білуге болады.

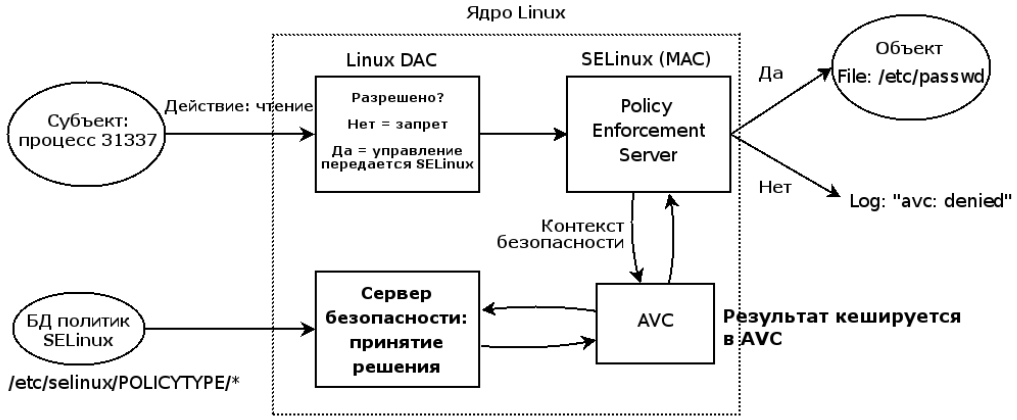
"Setenforce" командасы Enforcing және Permissive режимдерінің арасында жылдам ауысуға мүмкіндік береді, өзгерістер қайта жүктеусіз күшіне енеді. Бірақ егер сіз SELinux-ты қоссаңыз немесе өшірсеңіз, қайта жүктеу қажет, өйткені файлдық жүйеде қауіпсіздік белгілерін қайта орнату керек.

Жүйені әр жүктеу кезінде қолданылатын әдепкі режимді таңдау үшін /etc/selinux/config файлындағы 'SELinux=' жолының мәнін 'enforcing', 'permissive' немесе 'disabled'режимдерінің бірін орнату арқылы орнатыңыз. Мысалы: 'SELINUX=тұрақты'.

SELinux Саясаты

Жоғарыда айтылғандай, SELinux әдепкі бойынша Enforcing режимінде жұмыс істейді, онда рұқсат етілгеннен басқа кез-келген әрекеттер автоматты түрде бұғатталады, әр бағдарлама, пайдаланушы немесе қызмет тек жұмыс істеу үшін қажет артықшылықтарға ие, бірақ одан басқа ештеңе жоқ. Бұл өте қатаң саясат, оның артықшылықтары да бар — ақпараттық қауіпсіздіктің ең жоғары деңгейі де, кемшіліктері де-бұл режимдегі жүйені конфигурациялау жүйелік әкімшілердің үлкен еңбек шығындарымен байланысты, сонымен қатар, егер олар жүйені

пайдаланғысы келсе, пайдаланушылардың қол жетімділіктің шектеулеріне тап болу қаупі жоғары.тривиалды емес түрде. Бұл тәсіл кәсіпорын секторында қолайлы, бірақ соңғы пайдаланушылардың компьютерлерінде қолайсыз. Көптеген әкімшілер ұқсас мәселелерге тап болмас үшін SELinux-ті жұмыс станцияларында өшіреді.



Бұған жол бермеу үшін, мысалы, httpd, named, dhcpd, mysqld сияқты негізгі қосымшалар мен қызметтер үшін шабуылдаушыға маңызды деректерге қол жеткізуге мүмкіндік бермейтін алдын-ала конфигурацияланған мақсатты саясат анықталған. Саясат анықталмаған сол қосымшалар unconfined_t доменінде орындалады және SELinux қорғалмайды. Осылайша, дұрыс таңдалған мақсатты саясат пайдаланушыға қажетсіз проблемалар туғызбай, қауіпсіздіктің қолайлы деңгейіне қол жеткізуге мүмкіндік береді.

SELinux-қа кіруді бақылау

SELinux қол жеткізуді басқарудың келесі модельдерін ұсынады:

Type Enforcement (TE): мақсатты саясатта қолданылатын негізгі қол жеткізуді басқару механизмі. Рұқсаттарды ең төменгі деңгейде басқаруға мүмкіндік береді. Жүйелік әкімші үшін ең икемді, бірақ көп уақытты қажет ететін механизм.

Role-Based Access Control(RBAC): бұл модельде қол жеткізу құқықтары рөлдер ретінде жүзеге асырылады. Рөл-белгілі бір әрекеттерді жүйенің басқа бөліктеріне қарағанда жүйенің бір немесе бірнеше элементтерімен орындауға рұқсат беру. Негізінде, RBAC-бұл TE-дің одан әрі дамуы.

Multi - Level Security (MLS): көп деңгейлі қауіпсіздік моделі, онда жүйенің барлық нысандарына белгілі бір қол жетімділік деңгейі беріледі. Рұқсат немесе тыйым салу тек осы деңгейлердің арақатынасымен анықталады.

SELinux шеңберіндегі барлық процестер мен файлдарда қауіпсіздік контексті бар.

/Var/www/html/index мекен-жайы бойынша орналасқан Apache веб-серверінің бастапқы бетін егжей-тегжейлі қарап, іс жүзінде контекстті қарастырайық:

```
$ ls -Z /var/www/html/index.html
```

```
-rw-r--r--  username username system_u:object_r:httpd_sys_content_t
```

```
/var/www/html/index.html
```

Файлға қол жеткізудің стандартты құқықтарынан басқа, біз SELinux қауіпсіздік контекстін көре аламыз: system_u: object_r: httpd_sys_content_t.

Мәтінмән user:role:type:mls-ке негізделген, бірақ user:role:type өрістері MLS өрісі жасырылған кезде көрсетіледі. Сондай-ақ, біз мақсатты саясатты көре аламыз, бұл жағдайда httpd_sys_content_t.

Енді "httpd" процесі үшін SELinux қауіпсіздік контекстін қарастырыңыз (Apache веб-сервері):

```
$ ps axZ | grep httpd
```

```
system_u:system_r:httpd_t        3234 ?        Ss     0:00 /usr/sbin/httpd
```

Көріп отырғанымыздай, бұл процесс httpd_t доменінде іске қосылды.

Ал, енді үй каталогындағы файлдың қауіпсіздік мәнмәтінін қарастырайық:

```
$ ls -Z /home/username/myfile.txt
```

```
-rw-r--r--  username username user_u:object_r:user_home_t
```

```
/home/username/myfile.txt
```

Файлдың user_home_t түрі бар екенін көреміз, бұл түр үй каталогындағы барлық файлдарға әдепкі бойынша тағайындалады.

Тек бірдей типтегі элементтер арасында қол жеткізуге рұқсат етіледі, сондықтан Apache веб-сервері /var/www/html/index файлын еш қиындықсыз оқи алады.httpd_sys_content_t түрі бар html. сонымен қатар, Apache httpd_t доменінде іске қосылғандықтан және userid: username толтырылған өрістері болмағандықтан, ол home/username/myfile файлына кіре алмайды.txt, бұл файлды мақсатты саясат анықталмаған процестерге оқуға болады. Осылайша, егер Apache веб-сервері бұзылса, шабуылдаушы файлдарға қол жеткізе алмайды немесе httpd_t доменінде жоқ процестерді басқара алмайды.

SELinux проблемаларын жою

Ерте ме, кеш пе, SELinux сізге бір нәрсеге қол жеткізуге тыйым салатын жағдайға тап болған кезде жағдай орын алады. Қол жетімділіктің бірнеше негізгі себептері бар:

- Дұрыс таңбаланбаған файл.

- Процесс дұрыс емес контексте жұмыс істейді

- Саясаттағы қате. Процесс саясатты құру кезінде ескерілмеген файлға қол жеткізуді талап етеді.

- Басып кіру әрекеті.

Қол жеткізуден бас тартудың алғашқы үш себебі оңай шешіледі, ал басып кіру әрекеті кезінде дабыл естіледі және пайдаланушыға тиісті хабарлама жіберіледі.

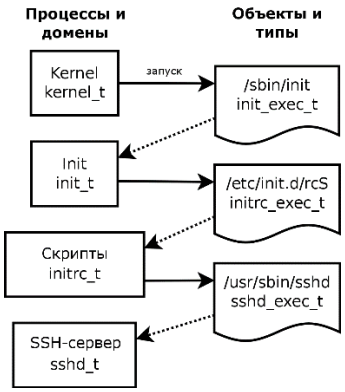
Кез-келген мәселені шешу үшін SELinux журналын қарау жеткілікті. Әдетте, auditd процесі /var/log/audit/audit файлына жазылады.log. Егер бұл процесс басталмаса, SELinux /var/log/messages файлында журнал жүргізеді, бұл жағдайда қол жеткізуді басқару жүйесінің барлық хабарламалары AVC кілтімен белгіленеді, мысалы, қажетті жолдарды тез сүзуге мүмкіндік береді. grep командасының көмегімен.

Дистрибуциялардың соңғы нұсқаларында (CentOS 5-тен бастап) SELinux журналын пайдаланушыға ыңғайлы және түсінікті етіп көрсетуге мүмкіндік беретін графикалық пайдаланушы интерфейсі бар қызметтік бағдарлама бар. Сіз оны консольден sealert-b теру арқылы шақыра аласыз. Егер X сервері іске қосылмаған болса, сіз келесі пәрменмен түсінікті және адамға ыңғайлы есептерді жасай аласыз:

```
sealert -a /var/log/audit/audit.log > /path/to/mylogfile.txt
```

Файл қауіпсіздігі мәтінмәнінің белгілерін өзгерту

"Chcon" пәрмені файлдарға немесе каталогтарға арналған SELinux контекстін "chown" және "chmod" пәрмендері стандартты кіруді басқару жүйесінде файл иесін немесе оған кіру құқығын өзгертуге мүмкіндік береді.



Бірнеше мысалды қарастырайық.

Жүйеде Apache веб-сервері орнатылған делік және сайттар сақталатын қалтаны (әдепкі бойынша /var/www/html/), мысалы, /html/ етіп өзгерту керек және осы каталогта индекс файлын жасау керек.html.

```
# mkdir /html
```

```
# touch /html/index.html
```

```
# ls -Z /html/index.html
```

```
-rw-r--r--  root root user_u:object_r:default_t        /html/index.html
```

```
# ls -Z | grep html
```

```
drwxr-xr-x  root root user_u:object_r:default_t        html
```

Жоғарыда біз каталог /html және файл / html / индекс екенін көреміз.бұл дегеніміз, егер біз Apache-ді іске қосып, осы каталогпен немесе файлмен жұмыс істеуге тырыссақ, онда SELinux бізге кіруден бас тартады. Бұл өте дұрыс болады, өйткені Apache-мен өзара әрекеттесетін файлдар үшін қауіпсіздіктің дұрыс контексті **httpd_sys_content_t.**

Мәтінмәнді өзгертіңіз және бәрі дұрыс жасалғанын тексеріңіз:

```
# chcon -v --type=httpd_sys_content_t /html
```

```
context of /html changed to user_u:object_r:httpd_sys_content_t
```

```
# chcon -v --type=httpd_sys_content_t /html/index.html
```

```
context of /html/index.html changed to user_u:object_r:httpd_sys_content_t
```

```
# ls -Z /html/index.html
```

```
-rw-r--r--  root root user_u:object_r:httpd_sys_content_t   /html/index.html
```

```
# ls -Z | grep html
```

```
drwxr-xr-x  root root user_u:object_r:httpd_sys_content_t    html
```

Әр файлды және әр каталогты қолмен өңдеудің қажеті жоқ, сіз жай ғана каталогты рекурсивті айналып өту опциясын қолдана аласыз-R:

```
# chcon -Rv --type=httpd_sys_content_t /html
```

Мұндай қауіпсіздік контекстіндегі өзгерістер қайта жүктеулер арасында сақталады, алайда файлдық жүйелердің белгілері өзгерген кезде өзгерістер жоғалады. Техникалық қызмет көрсету және пайдалану процесінде Бұл сирек емес. Мұндай жағдайда дұрыс шешім (тестілеуден кейін, әрине) қосымша ереже жасау, содан кейін оны жергілікті жергілікті ережелермен біріктіру болады. Осылайша, ол негізгі ережелерге қарағанда жоғары басымдыққа ие болады.

SELinux файлдық жүйенің белгілерін өзгерткеннен кейін де дұрыс жұмыс істеуі үшін біз SELinux C GUI интерфейсін басқару құралдарын да, semanage консолін де қолдана аламыз:

```
semanage fcontext -a -t httpd_sys_content_t "/html(/.*)?"
```

Жоғарыдағы мысалда біз httpd_sys_content_t мәтінмәнін католог /html құрамындағы барлық файлдарға тағайындадық.

SELinux қауіпсіздік мәнмәтінін қалпына келтіру

"Restorecon" пәрмені қауіпсіздік мәнмәтінін әдепкі бойынша тағайындалған етіп өзгертуге мүмкіндік береді.

Apache веб-серверін тағы да мысал ретінде пайдаланыңыз. Пайдаланушы үй каталогында index файлының көшірмесін өңдеді делік.html және оны (MV командасы) сайттар сақталатын каталогқа көшірді (/var/www / html).

Көшіру кезінде (CP командасы) файлдың қауіпсіздік контексті тағайындалған каталогтың мәтінмәніне сәйкес келеді, ал жылжыту кезінде қауіпсіздік контексті бастапқы мәтінмәнге сәйкес келеді. Әрине, біз қауіпсіздік контекстін өзгерту үшін chcon пәрменін қолдана аламыз, бірақ көшірілген файлдар қазір /var/www/html каталогында болғандықтан, біз осы каталогтағы барлық файлдар үшін мәтінмән параметрлерін қалпына келтіре аламыз.

Мәтінмәнді тек index файлына қалпына келтіру үшін.html, біз пәрменді қолдана аламыз:

```
# restorecon -v /var/www/html/index.html
```

Егер біз бүкіл каталогты рекурсивті түрде айналып өтіп, ондағы барлық файлдар үшін контекстті өзгерткіміз келсе, біз келесі пәрменді қолданамыз:

```
# restorecon -Rv /var/www/html
```

Бүкіл файлдық жүйе үшін белгілерді өзгерту

Кейде бүкіл файлдық жүйеде қауіпсіздік белгілерін қайта орнату қажет. Көбінесе мұндай операция SELinux қайта қосылған кезде, жүйе біраз уақыт ажыратылғаннан кейін жасалады. Егер біз саясатты басқару түрін strict-те өзгертсек, бұл қажет (бұл жағдайда барлық процестер арнайы домендерде жұмыс істейді, ешкім unconfined_t доменінде жұмыс істей алмайды).

Келесі қайта жүктеу кезінде файлдық жүйені автоматты түрде қайта анықтау үшін келесі пәрмендерді енгізіңіз:

```
# touch/.autorelabel
```

```
# rebootм
```

Кейде автоматты түрде түзету жұмыс істемейді (көбінесе SELinux жүйесі өшірілген дистрибуция жаңартылған жағдайда). Бұл жағдайда келесі пәрменді қолданыңыз:

```
# genhomedircon
```

```
# touch /.autorelabel
```

```
# reboot
```

Порттарға қол жеткізуді ұсыну

Көбінесе біз Apache сияқты қызметтердің стандартты емес порттарды тыңдауға және оларға кіретін қосылыстарды қабылдауға мүмкіндігі болғанын қалаймыз. SELinux-тің негізгі саясаты белгілі бір қызметке қатаң байланысты алдын-ала анықталған порттарға ғана қол жеткізуге мүмкіндік береді. Apache-дің 81 портты тыңдағанын қалаймыз делік. Бұл жағдайда біз semanage пәрменін пайдаланып ережені қосуымыз керек:

```
# semanage port -a -t http_port_t -p tcp 81
```

SELinux қол жеткізуге мүмкіндік беретін порттардың толық тізімін келесідей көруге болады:

```
# semanage port -l
```