취약점 진단 실습(2일차)

// Intro

진단 잘 하려면 현황에 대한 충분한 분석 및 이해 후 맞춰서 진행해야 좋은 결과를 얻을 수 있음.

캡처에 명령줄을 같이 찍는 이유는 해당 사항 조치해야할 SE에게 어떤 명령줄을 사용했는지 전달하기 위함임.

결과보고서에 현황 및 대응방안을 기입하는 것도 많이 연습해봐야함.

// 취약점 진단 및 결과보고서 작성 실습

결과보고서를 왜 이렇게 열심히 써야하나

이후에 증적으로 활용됨, 아주 중요함

이행진단 들어가도 환경분석은 똑같이 한다 > 그런데 다른 취약점이 발견된다면?

! 당연 해당 취약점에 대해서도 진단해야함. > 바로 조치하면 조치된 것으로 보고서 작성하여 "양호"로 처리함.

U-44 : root 이외의 UID가 '0' 금지

어떤 계정의 UID 값이 "0"이라는 건 최고 관리자 계정을 의미함.

일반 사용자 계정의 UID가 "0"이 되면 해당 권한을 사용할 수 있음.

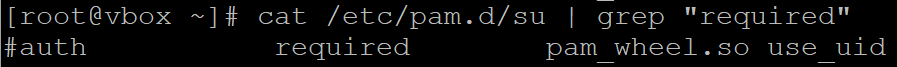
>(결과) UID가 0인 "root" 외 다른 계정이 없음을 확인 > 양호

U-45 : root 계정 su 제한

1. root 계정을(혹은 권한을) 획득하려면 로그인이 가능한 일반 사용자 계정으로 로그인을 수행해야 함.

2. "/etc/pam.d/su" 내 "su" 관련 설정의 주석을 제거해야 함.

cat /etc/pam.d/su | grep "required"



3. "/etc/group" 내 "wheel" 그룹 내에 root 권한이 필요한 사용자만 추가되어 있어야 함.



"wheel" 그룹에 추가된 일반사용자만 로그인한 후 "su" 명령어를 입력했을 경우 "root" 권한을 획득할 수 있음.

4. "/bin/su" 파일의 권한이 4750 권한으로 설정되어 있어야함.



“/bin/su” 파일의 권한이 4755로 설정되어 있음.

참고개념1. 파일 및 디렉터리의 권한 기본개념

|  |
| --- |
| 소유자 그룹소유자 타사용자 : -rwxrwxrwx = 0777  SetUID : -rwsr-xr-x =4755  SetGID : -rwxr-sr-x =2755  StickyBit : -rwxr-xr-s =1755 |

5. "/bin/su" 파일 그룹소유자가 "wheel"로 설정되어 있어야함.

위의 캡처에서 보면 “bin/su” 파일의 그룹소유자가 “root” 그룹임을 확인할 수 있음.

결과.

세팅이 완료되면 "wheel" 그룹 사용자만 "su"를 사용할 수 있고, 패스워드 없이 "root" 권한을 획득함.

참고2. 규모가 있는 회사의 경우 "서버접근제어솔루션"을 사용함.

위의 U-45 내용이 솔루션에 포함되어 있음. 비쌈.

U-50

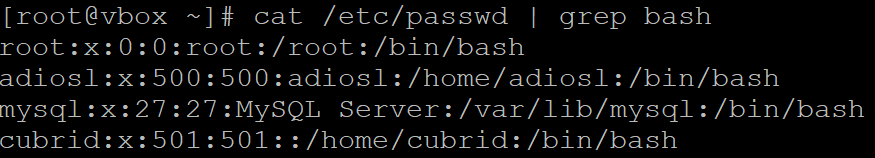
"root" 그룹에 일반 사용자가 포함되어 있다면 바로 취약.

자기 자신이 포함되어 있는 것은 상관없음. (포함되어 있지 않은 것과 굳이 다른 의미는 없음.)



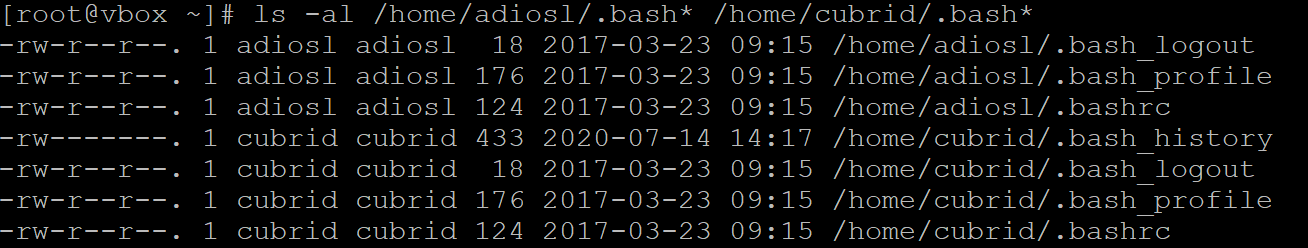
U-53 : 사용자 Shell 점검

어려운 항목임. 초급 진단자가 해당 항목의 응용 분야까지 처리 가능하면 OS에 대한 개념 이해를 인정받을 수 있음.



위와 같이 해당 명령 구문을 사용하여 현재 로그인 가능한 사용자 목록 확인.

시스템 계정 2개(root,mysql) 및 일반 사용자 계정(adiosl, cubrid) 2개로 총 4개 계정 확인.



그 중 일반 사용자 계정 2개에 대해 위와 같이 .bash\_history 파일 확인.

최초에 계정을 생성하면 제일 처음 생성되는 파일 : ".bash\_profile" 그 다음 ".bash\_logout" 생성

.bash\_history : shell 명령어가 기록되는 파일, 로그인 shell 도 기록됨

> 파일의 수정날짜를 확인해 최근사용일,사용여부 확인 가능함.

> 파일이 없다면 한 번도 로그인한 적이 없음을 의미함.

오랫동안 사용되지 않았다고 판단되는 경우 "취약" 진단

? lastlog로 확인하는 것과 어떤 차이가 있나

A. 실제적으로 출력되는 정보의 차이는 없으나 로그분석은 침해사고 원인분석의 영역이고 취약점 진단의 방향성과는 맞지 않음.

참고개념2.

|  |
| --- |
| umask(user mask) : 공통적인 권한을 지정하기 위해서 사용됨.  (예시) 디렉터리는 777-, 파일은 666-  (적용대상) 사용자 홈 디렉터리(/home/\*)에 새로운 디렉터리 혹은 파일 생성 시 적용됨. |

U-05 : root 홈, 패스 디렉터리 권한 및 패스 설정

참고개념3.

|  |
| --- |
| 환경변수  1. 시스템 ~  - repository를 통해 패키지(.rpm) 설치를 진행하였을 때 자동으로 설치됨.  2. 사용자 ~  - Daemon 설치부터 동작까지의 모든 과정을 완료하고 난 후 자동으로 바이너리를 실행할 수 있도록 사용자가 직접 추가해야 함.    위와 같은 명령 구문으로도 확인할 수 있지만 실제로는 환경변수를 확인하기위해 다음과 같은 명령 구문을 사용함.    각 PATH 는 “:”으로 구분됨. |

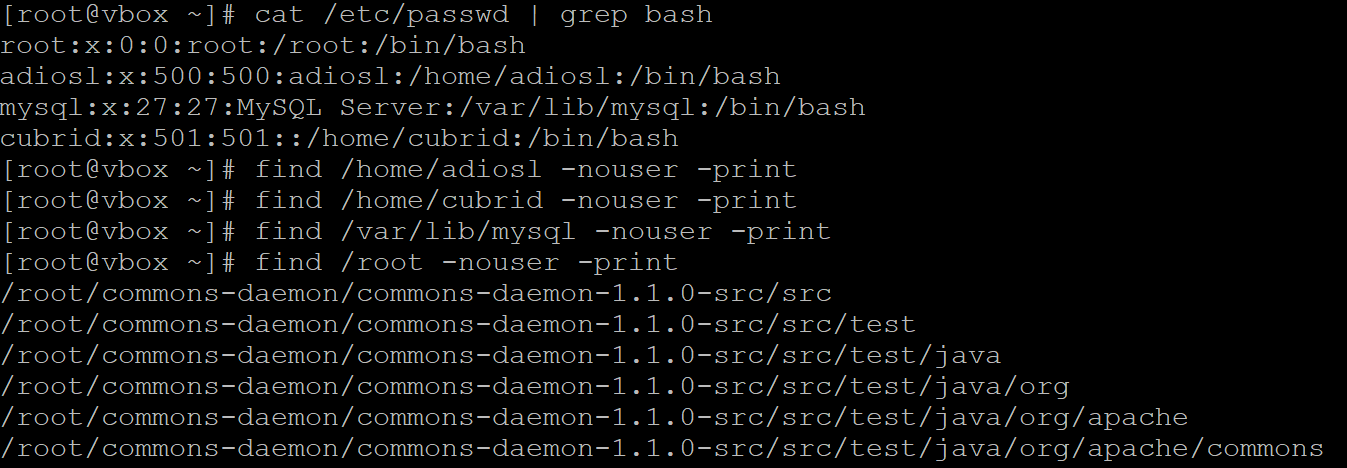
시스템 환경변수 맨 앞 혹은 중간에 “.”이 포함되어 있지 않음을 확인함

맨 뒤에 오는 “.”은 상관없음.

U-06 : 파일 및 디렉터리 소유자 설정

가이드에는 전체 디렉터리 및 파일에 대해 find 명령을 통해 확인하지만 출력이 너무 많아서 전체 디렉터리 및 파일을 확인한다는 것은 말이 안됨.

실제로는 아래와 같이 로그인이 가능한 사용자 확인 후 해당 사용자 계정(root,mysql,adiosl,cubrid)의 홈 사용자 디렉터리에서 하위 디렉터리 및 파일을 확인함.



“root” 계정의 홈 디렉터리 “/root” 디렉터리 내에 소유자 및 그룹이 존재하지 않는 다수의 파일이 남아있음. > “취약” 진단

U-07 : /etc/passwd 파일 소유자 및 권한 설정

“/etc/passwd” 파일은 단순히 계정 정보를 보관만 하는게 아니라 계정의 생성/수정/삭제가 가능함.

위 개념을 모르면 타사용자가 볼 수 있으니 “취약”으로 진단할 수 있으나, 실제로는 읽기권한만 있는 것은 정상적인 상태임. > 644 권한은 안전함.

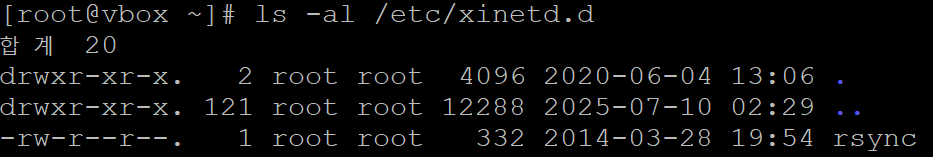
U-10 /etc/(x)inetd.conf 파일 소유자 및 권한 설정

참고개념4.

|  |
| --- |
| XINETD(인터넷슈퍼데몬) : 외부 네트워크 Public Client의 요청 시 원격 프로시저 호출  RPC(Remote Procedure Call)의 반대 개념  (전제조건) 서버 내에 /etc/xinet.d/ 디렉터리에 관련 Daemon에 관련 데몬이 존재하고 있어야함.  RHEL 5.X 이하 버전에서는 inetd, 6.X 버전 이상부터는 xinetd |

아래와 같은 명령 구문을 사용하여 해당 서비스의 데몬이 구동 중인지 확인하고, 해당 디렉터리 내에 .conf 파일이 있는지 직접 확인 > xinetd.conf 파일 존재 시 권한 확인 해야함.





U-12 /etc/servies 파일 소유자 및 권한 설정

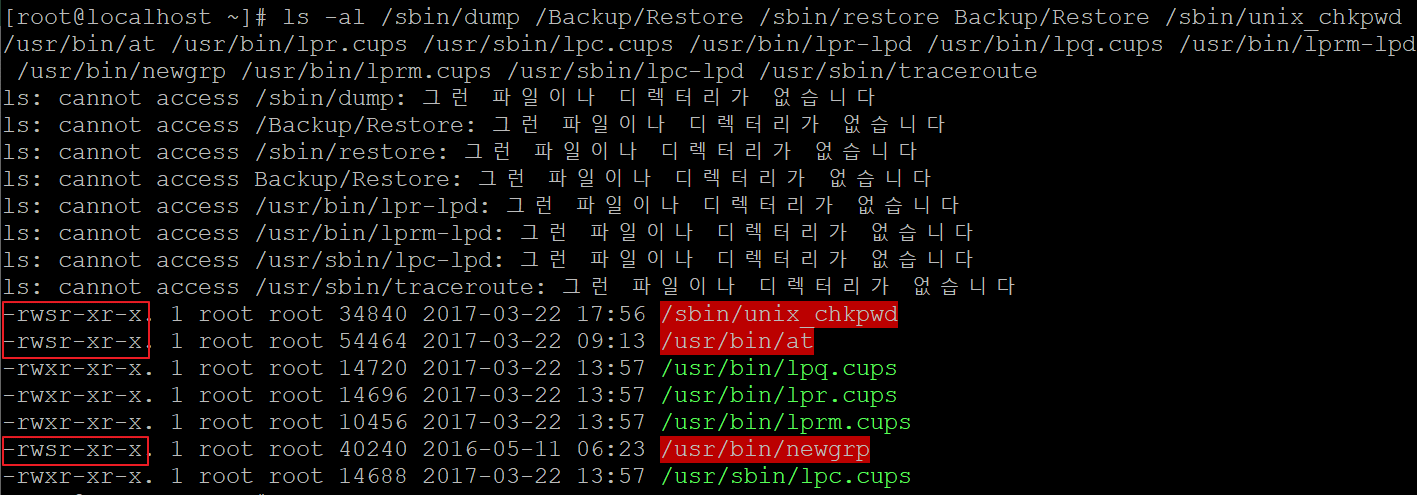
/etc/servies : 구동중이지 않은 데몬 포함 전체 데몬 리스트 되어 있음.



위와 같은 명령 구문을 사용해 권한이 644로 설정되어 있음을 확인함. > 양호

U-13 SUID/SGID 설정 파일 점검

특수권한이 있으면 안되는 디렉토리 리스트 (기반시설가이드 p.154 '불필요한 SUID/SGID 목록' 중 LINUX 해당 내용 참고) 를 가지고 아래와 같은 명령 구문을 구성하여 특수권한이 설정된 파일이 있는지 확인



심볼릭링크의 경우 대상 디렉터리로 치환하여 리스트업 > 심볼릭링크는 실재하는 파일이 아님. > 링크에 링크에 링크 끝까지 찾아서 해당 디렉터리의 권한 확인할 것.

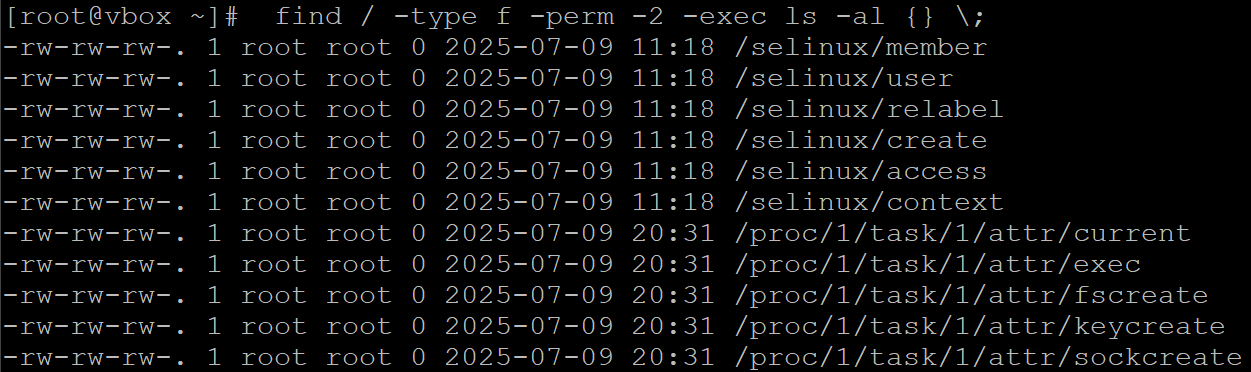
? 실무에서 이런 식으로 하는지 혹은 함수나 프로그램을 통해 처리하는지

! 기반시설가이드를 참고하여 작성된 리스트업 명령구문이 준비되어있음.

U-15 world writable 파일 점검

world writable 파일 : 특정 파일이나 디렉토리가 모든 타사용자에게 쓰기권한이 부여되어 있는 경우 > 취약점

아래와 같이 기반시설가이드에서 제공된 명령 구문은 전체 디렉터리에서 find 명령을 수행하기 때문에 실 사용중인 시스템에 이 명령 구문을 사용하면 시스템이 뻗을 수 있음.



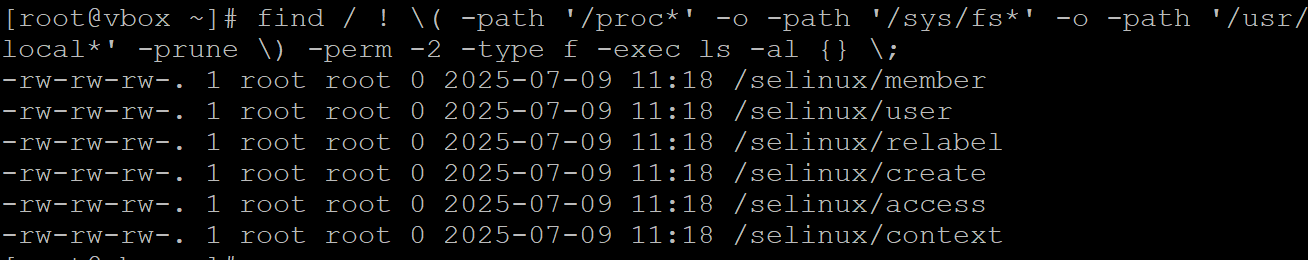
이 경우 예시로 주어진 가벼운 가상머신이기 때문에 문제가 발생되지 않음.

proc : 캐시 형태로 프로세스를 기록 > 캐시 파일이기 때문에 권한 수정이 의미가 없음.

/sys/fs : 파티션 캐시 저장 경로

/usr/local\* : 사용자 로그인 관련 캐시 저장 경로

proc 등 위와 같이 진단 대상이 아닌 캐시 파일이 너무 많이 포함되어 있음 > 아래 명령 구문을 사용하여 진단 대상이 아닌 캐시 파일을 제외하고 리스트업하여 확인.



-prune : 빼고 찍겠다

위와 같이 확인 결과 SELinux 관련 몇 가지 world writable 파일이 발견됨 > “취약” 진단

실제로는 커널에서 동작하는 파일들이라 조치 불가능한 항목이지만 진단은 하는 것

+ 초급진단자의 경우 취약점으로 잡지만 경력진단자의 경우 커널 수준에서 동작하는 파일이라는 것을 증명하고 '양호'로 진단할 수 있음.

+ 기술문서 링크를 찾아 해당 파일 수정 시 Side Effect(역효과, 서비스가 동작불능 상태가 된다던가 하는)가 발생할 수 있다는 내용을 첨부하여 변경 불가능함을 증명, '양호'로 진단함.

U-16 : /dev에 존재하지 않는 device 파일 점검

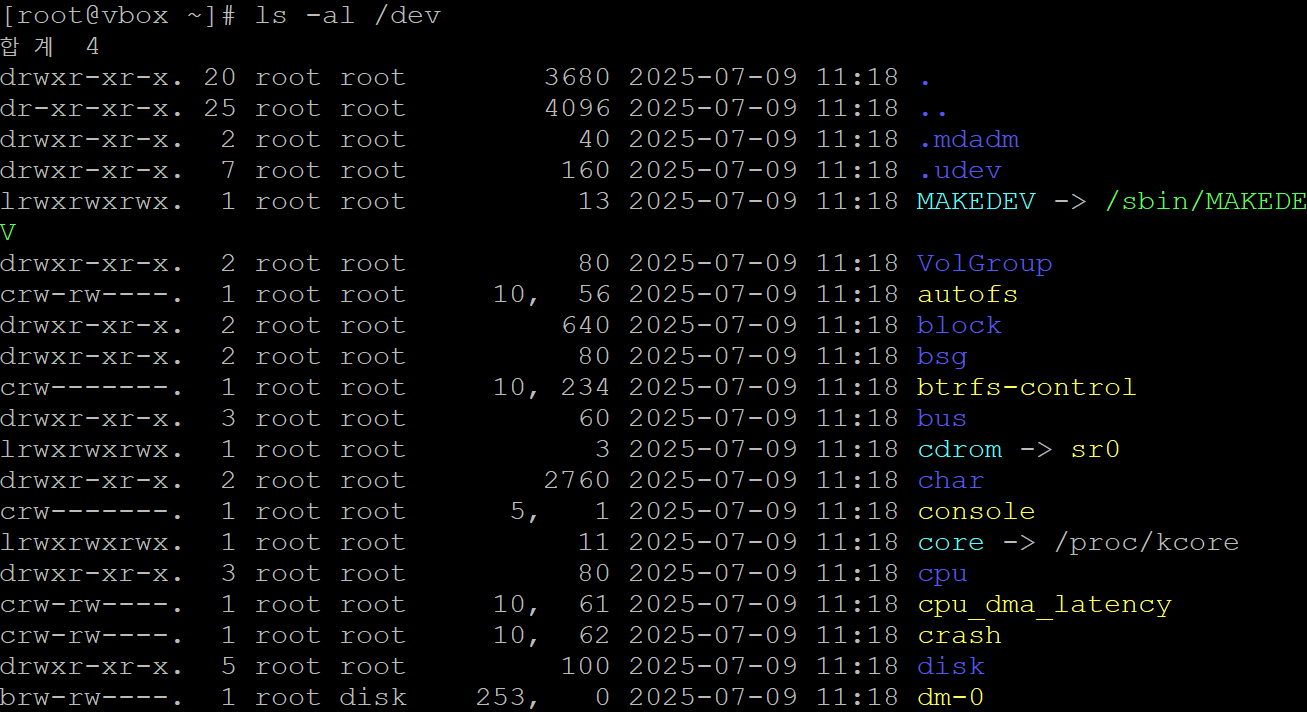
아래와 같은 명령 구문을 통해 “/dev” 디렉터리의 내용을 확인할 수 있음.

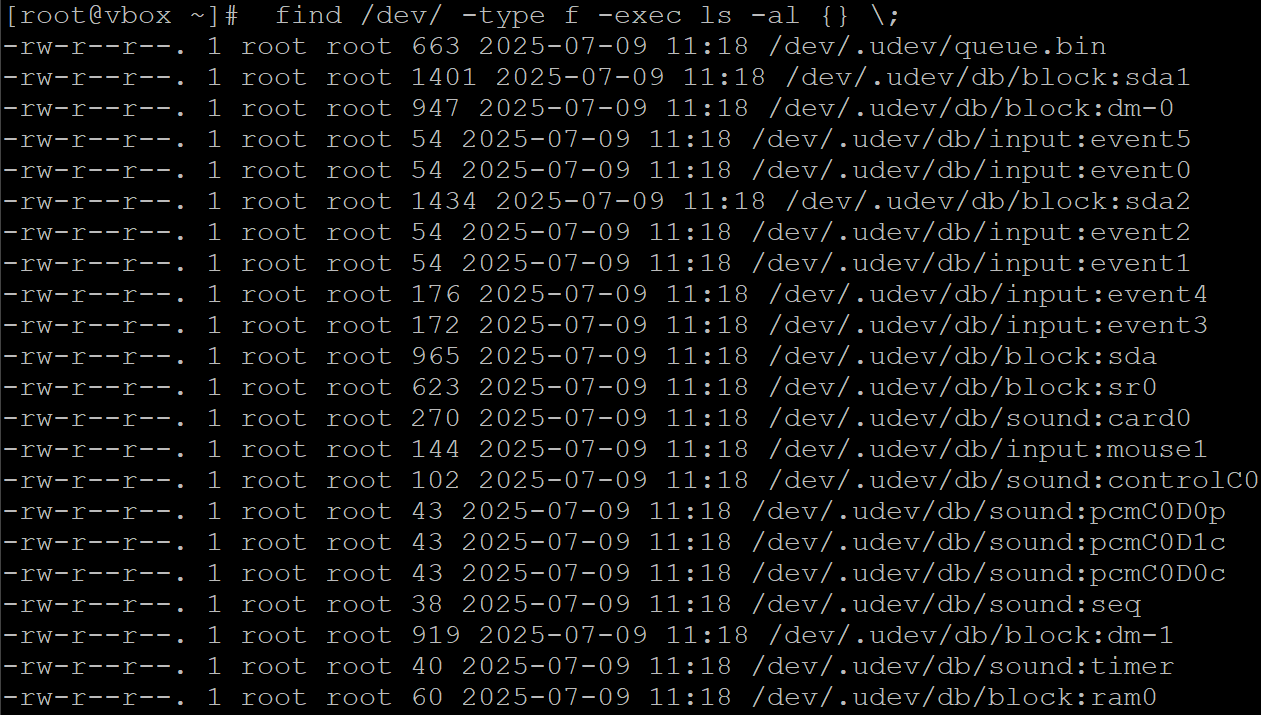
디바이스에 대한 정보는 텍스트로 이루어져있지 않음 > 파일권한에 b 혹은 c 라고 되어있는 것들이 있음.

> b : block special file, c : character special file

> 6.X 버전까지만 있고

> 7.X이상부터는 /dev 에 내용이 없음. > 추가 명령어가 필요함.





위와 같은 명령 구문을 이용해 “/dev/.udev/” 디렉터리 내에 디바이스 관련 파일을 확인할 수 있음.

U-17 : $HOME/.rhosts, hosts.equiv 사용 금지

참고개념5.

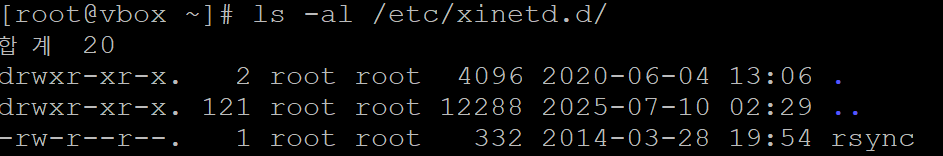
|  |
| --- |
| 'r'command : 인증 없이 관리자 원격접속이 가능함.  > Daemon 앞에 'r' 이 붙으면 보통 'remote'  서버 내부에서 DoS 공격을 일으킬 수 있는 방법  1. rbash or rsh  2. rlogin  3. rexec  'r'커맨드는 인터넷슈퍼데몬과 관련이 있음. |

1. 데몬 구동 여부 확인



구동 중인 데몬이 없음

만약 구동 중인 데몬이 발견되면 다음과 같은 명령 구문을 통해 해당 데몬 파일을 확인해야함.

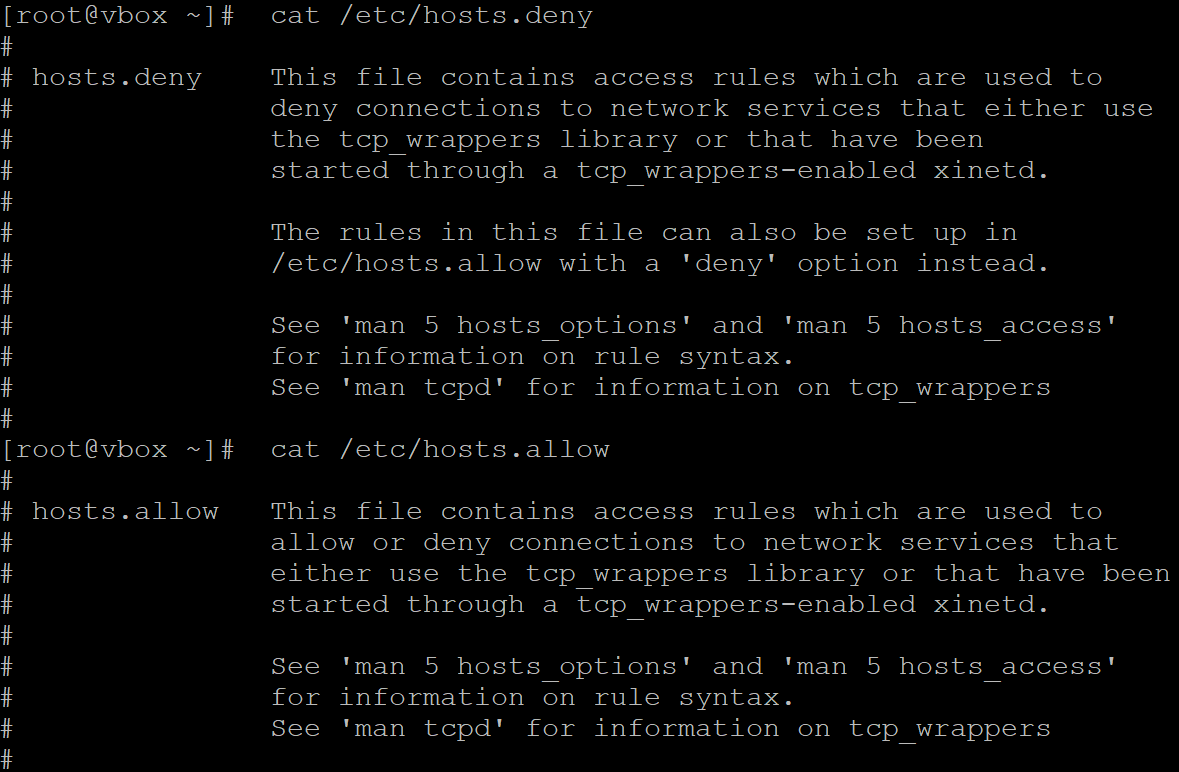
 해당 디렉터리에 rlogin, rbash, rexec이 없음을 확인함. > “양호” 진단

U-18 : 접속 IP 및 포트 제한

오탐률이 가장 높은 항목 중 하나임.

서버접근제어솔루션이 없다면 직접적으로 접근이 가능함.

아래와 같은 명령 구문을 사용하여 설정파일 확인.



"/etc/hosts.deny" 및 "/etc/hosts.allow" 파일 내 설정 값이 존재하지 않는 상태임을 확인.

하지만 내부 방화벽 Rule-Set 혹은 서버접근제어솔루션을 사용하고 있는지는 판단할 수 없음.

해당 내용에 대하여 인터뷰 요청이 필요함. 답변이 허술할 경우 클라이언트 단에서 접근 시도를 통해 접근통제를 직접확인해야함.

! 실제로 강의 간 강사님이 직접 내 IP주소를 사용하여 내 테스트 서버 환경에 접속하였음.

U-55 : hosts.lpd 파일 소유자 및 권한 설정

예전에 사용하던 로컬 프린터 관련 파일

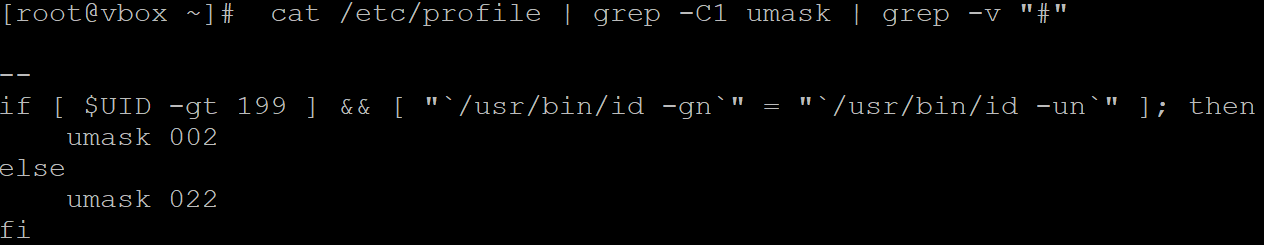


위와 같은 명령 구문으로 확인할 수 있으며 현재는 없는 경우가 많음 > 가이드에서 아직 수정되지 않은 부분

U-56 : UMASK 설정 관리

cat /etc/profile | grep umask | grep -v "#"

> 위와 같이 입력하면 2줄이 나오는데 각각의 대상을 알 수 없어 아래와 같이 입력함

 -C1 : 위아래로 추가적으로 출력하겠다는 옵션

199 초과하고 UID == GID 인 계정에 대해 umask 002를 적용하겠다는 의미임

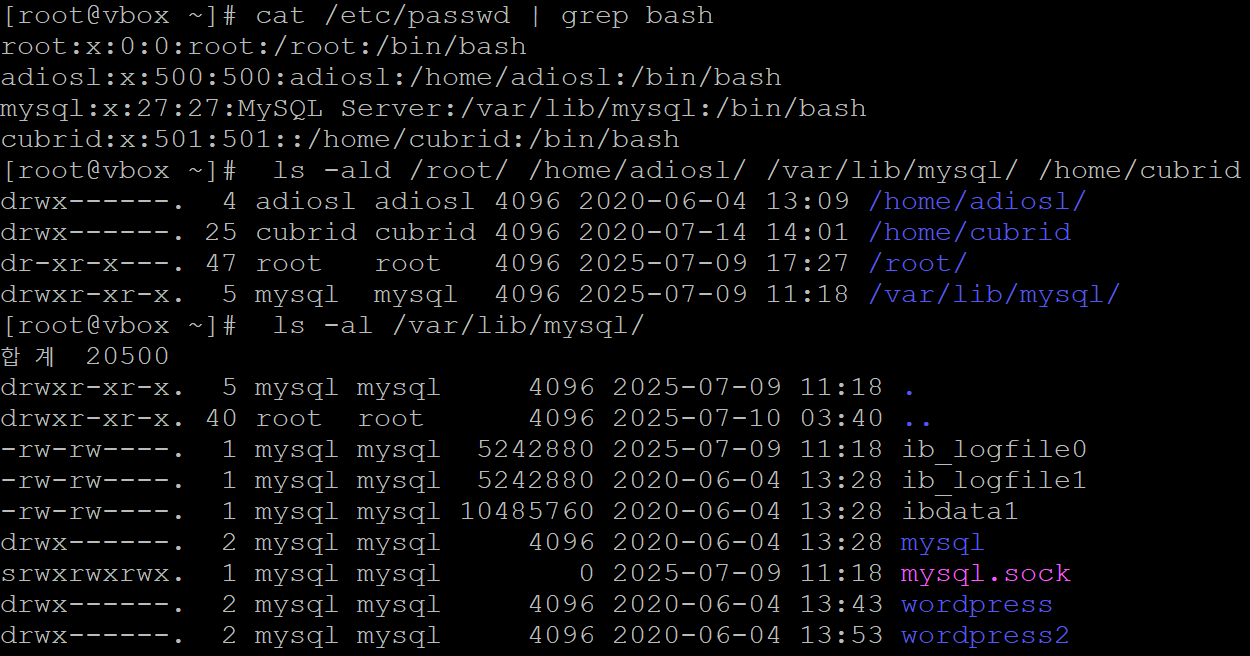


“umask” 명령 구문 입력 시 현재 로그인한 계정의 umask 확인 가능

(대응방안) 기존 UMASK 설정 구문 최하단에 "umask 022" 값을 추가하여 주시기 바랍니다. > 경험적으로 밝혀진 최선책임.

U-57 : 홈디렉토리 소유자 및 권한 설정

아래와 같은 명령 구문으로 현재 로그인 가능한 사용자 리스트를 확인하고, 각 사용자의 홈 디렉터리를 확인하였음.



확인결과 "var/lib/mysql/" 디렉터리의 권한이 755로 설정되어 있고, 일반 사용자 계정만 탈취하면 mysql 홈 디렉터리를 접근할 수 있음. “mysql.sock” 파일을 외부 클라이언트가 변경하면 서비스 장애가 발생함. > 취약점

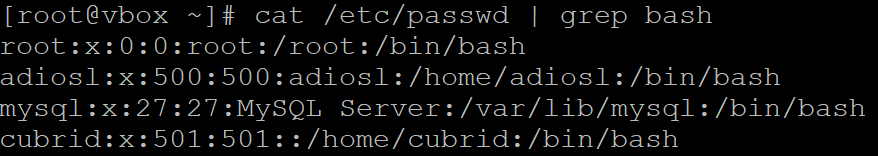
가이드에서는 타 사용자 쓰기 권한에 대해서만 점검하도록 되어 있지만, 실제로는 디렉터리에 타 사용자 읽기 권한이 있는 경우 하위 파일 및 폴더의 권한까지 전부 확인하여야 함.

참고개념6. 윈도우 OS와 UNIX 계열 OS의 권한 종속성 비교

|  |
| --- |
| 윈도우는 최상위 디렉터리에 권한이 있을 경우 하위 디렉터리 및 파일에 대해 모든 권한을 가짐(종속성이 있음)  윈도우에 비해 UNIX 계열은 권한 종속성이 없어 접근 가능한 디렉터리의 파일도 해당 파일의 권한에 따름 > 보안적으로 더 안전함. |

U-58 : 홈 디렉터리로 지정한 디렉터리의 존재 관리

아래와 같은 명령 구문으로 로그인 가능한 사용자 계정 중 홈 디렉터리의 존재여부 확인



홈 디렉터리가 없으면 .bash\_history등 어디에 기록이 남나?

> 침해사고 등 발생 시 확인할 수 있는 기록(tracing)이 없음.

추가로 사용자 계정이 없는 홈 디렉터리가 있는 경우 이것도 취약점이며, 해당 홈 디렉터리에 대한 코멘트(“미사용시 삭제 필요” 등)가 필요함.

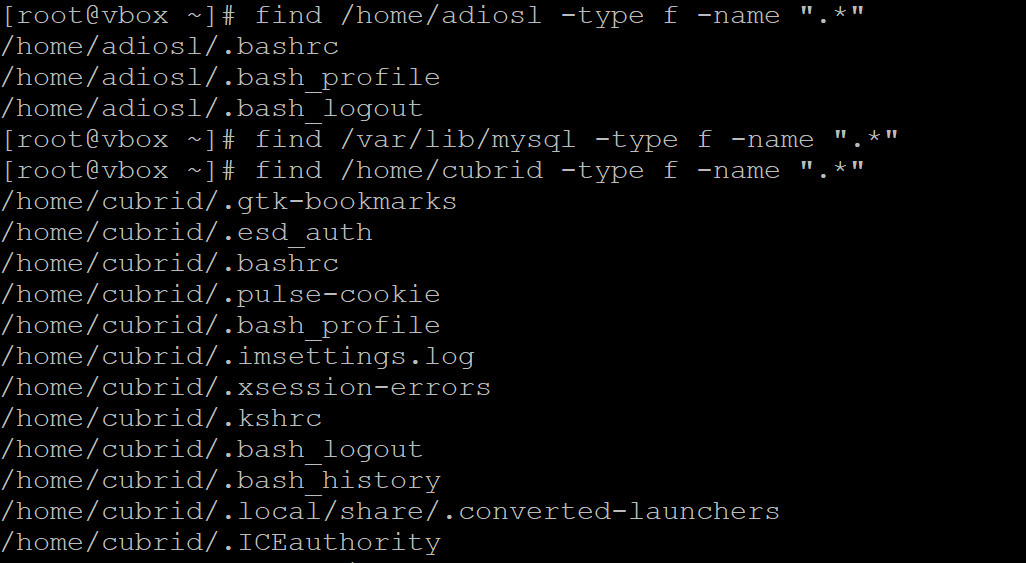
U-59 : 숨겨진 파일 및 디렉토리 검색 및 제거

아래와 같은 명령 구문으로 find 명령을 수행시키는 것은 시스템을 마비시킬 수 있음.

find / -type f -name ".\*"

find / -type d -name ".\*"

다음과 같이 변경이 가장 많은 홈 디렉터리를 아래와 같은 명령 구문으로 전부 리스트업하여 파일 및 디렉터리 확인하여야함.



위와 같이 다른 홈 디렉터리는 파일이 없거나 잘 알려진 필요한 파일(.bash\*) 포함되어 있는 반면에 “/home/cubrid” 디렉터리나 “/root” 디렉터리에는 사용목적 및 실제 사용여부를 알 수 없는 파일 들이 다수 포함되어 있음.

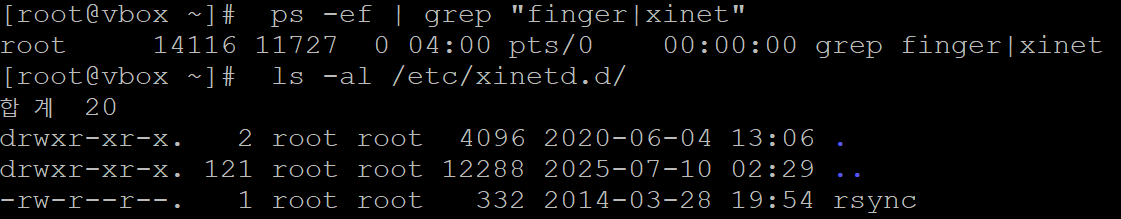
해당 파일들의 사용목적 및 실제 사용여부에 대하여 운영 및 담당자의 코멘트 요청이 필요함.

U-19 : Finger 서비스 비활성화

Finger 서비스 : UNIX 계열 시스템에서 사용자 정보를 조회하는 용도로 사용하던 오래된 네트워크 프로토콜임(Port 79)

사용자 정보를 너무 쉽게 노출하기 때문에 취약점으로 판단되었고 현재는 대부분 비활성화 되어 있음.

원격에서 Public Client의 요청에 대한 내용이므로 인터넷슈퍼데몬 xinet에 대해서 같이 확인해야함.



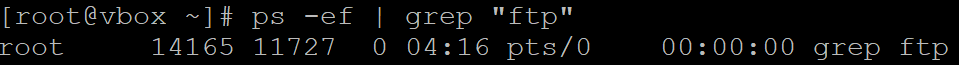
위와 같은 명령 구문을 사용하여 Finger 서비스 및 xinet 관련하여 구동중인 Deamon이 없음을 확인하였고, xinet Deamon 관련 설정 파일이 들어있는 디렉터리에 Finger 서비스 관련 파일이 없음을 확인하였음.

U-20 : Anonymous FTP 비활성화

참고개념7. FTP를 안전하게 사용할 수 있는 방법

|  |
| --- |
| 1. Anonymous FTP 비활성화(디폴트로 설치되어 있음)  무조건 비활성화 하여야 함, 여기서 Anonymous는 인증절차를 거치지 않은 아무나를 의미함.  2. FTP에 접근하는 계정을 "root"로 사용하지 않아야 하고 Default 계정(ftp)를 통해서 로그인이 되선 안된다.  "root" 계정은 시스템 영역에서 OS 만을 핸들링 하기위해 사용하여야 함. 특정 서비스에 "root" 계정을 사용하여 접근하면 "root"권한을 얻을 수 있는 다수의 일반 사용자가 해당 서비스를 사용할 수 있게 됨. 그리고 Default 계정(ftp)를 통해서 로그인이 가능할 시 잘 알려진 계정이므로 브루트포스 공격의 주요 대상이 됨. 또한 디폴트 홈 디렉터리가 노출되고, 다수가 계정을 공유하여 사용하기 때문에 로그를 통한 사용자 식별이 불가능함. 그래서 ftp 계정은 default로 nologin 셸로 설정되어 있으며, FTP에는 별도의 계정을 생성하여 접근하여야 함.  3. FTP에 대한 UMASK를 077로 설정해야만 함, 이를 통해 소유자만 권한을 얻어야 함. 이유는 위의 항목과 동일한 보안 취약점 이슈임. |

FTP의 종류는 sftp, ftp, vsftp, WU-ftp, pro-ftp, tftp(X)등이 있으며, 보통 VSFTP(Very Secure ~)를 많이 사용함. SFTP (Secure ~)는 암호화 처리 기능이 포함된 FTP임.

 위와 같은 명령 구문을 사용하여 구동 중인 FTP 관련 Daemon이 없음을 확인함.

FTP 서비스 구동 중이면 해당 서비스의 설정 파일에 "anonymous\_enable" 설정값을 "no"로 설정하여야 함.

U-21 : r 계열 서비스 비활성화

'r'3종 중 하나라도 구동 중이면 무조건 "취약" 으로 진단함.

U-17 항목의 참고개념5(‘r’ command)를 참고할 것.