U-22

crontab 명령어는 750 이어야 함.

crontab 관련 파일 > 소유자 "root" 및 권한 "640" 이하

(취약)"/etc/crontab" 및 "cron" 명령 실행 파일의 소유자가 "root"지만 "/etc/crontab" 파일 권한이 644(-rw-r--r--), 일부 "cron" 명령 실행 파일 권한이 755(-rwxr-xr-x)로 설정되어 있는 상태입니다.

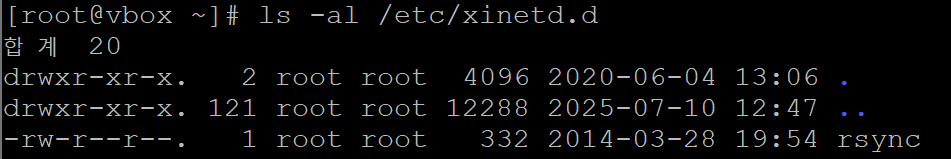
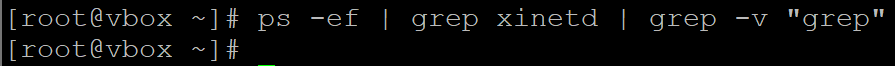
(대응방안)~참고하시어 "/etc/crontab" 파일 권한을 640(-rw-r-----), 일부 "cron" 명령 실행 파일 권한을 750(-rwxr-x---)으로 설정하여 주시기 바랍니다.

U-23 : DoS 공격에 취약한 서비스 비활성화

NTP,DNS,SNMP 등 서비스는 정말 사용하지 말아야 할까 > 아니지

SNMP : 관제 관련 서비스, 많은 곳에서 사용되는 중

echo : 많이 씀, 어제도 씀( echo $PATH )



구동 중 이고 해당 파일이 있으면 취약인가 > 아님. 판단 근거가 부족함.

해당 사항에 대한 SideEffect 설명을 추가하는 것이 중요함.

(양호) "xinetd(인터넷 슈퍼 데몬)"이 구동중이지 않고, "/etc/xinetd.d" 디렉터리 내 "rsync"만 존재하는 상태입니다.

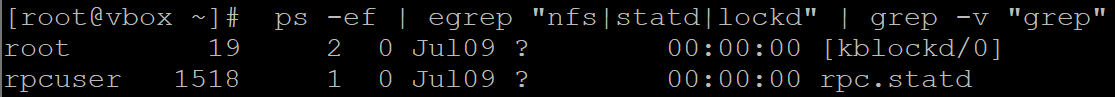
(취약) "xinetd(인터넷 슈퍼 데몬)"이 구동중이지 않지만 "/etc/xinetd.d" 디렉터리 내 "echo"가 존재하는 상태입니다.

※ "xinetd(인터넷 슈퍼 데몬)"를 구동하게 될 경우 "/etc/xinetd.d" 디렉터리 내 "DoS" 공격을 유발할 수 있는 "echo" 데몬을 Client가 원격에서 실행을 요청할 수 있음

(대응방안)주요정보통신기반시설 가이드를 참고하시어 "/etc/xinetd.d" 디렉터리 내 "DoS" 공격을 유발할 수 있는 "echo" 데몬을 제거하여 주시기 바랍니다.

U-24 : NFS 서비스 비활성화

NFS 데몬 확인



rpc.statd : RPC 데몬의 실행상태를 모니터링 (기본 기능)

NFS 공유 드라이브가 잠금 상태인지 아닌지 모니터링 하는 추가 기능이 있음. (1일차 내용 중)

rpc.lockd : NFS 공유 드라이브가 잠겼을 때 해제해주는 역할

> nfs가 구동중이지 않고, lockd도 없는데 statd가 왜 구동중인지 확인이 필요함.

기반시설가이드에는 추가적으로 불필요한 데몬에 대한 내용을 확인하는 부분이 없음.



(양호) "nfs" Daemon이 구동중이지 않고, "/etc/exports" 파일 내 "nfs" 관련 설정이 존재하지 않는 상태입니다.

U-25 : NFS 접근 통제

구동을 안하고 있는 상태에서 한번 더 짚고 나가는 방법은

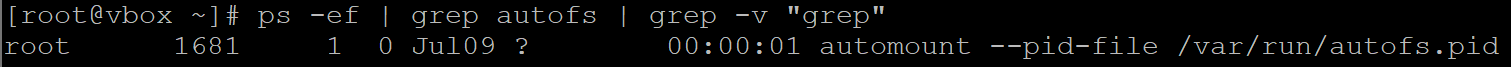


U-24 항목을 양호로 설정하면 NFS 관련 논리가 전부 무너짐.

(대안) U-24 항목과 U-25 항목을 합치는 방식.

U-26 : automountd 제거

AutoMount : 디렉터리 및 파티션을 Mount ,NFS에 필수적인 개념



|  |
| --- |
| - "automount" Daemon이 구동중인 상태입니다.  [대응방안]  주요정보통신기반시설 가이드를 참고하시어 "automount" Daemon을 비활성화 하여 주시기 바랍니다. |

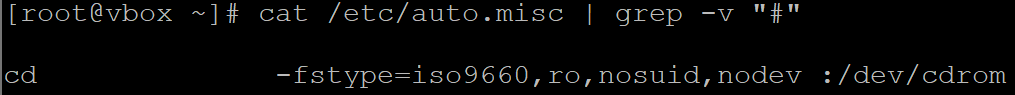
위와 같이 진단 결과를 내면 안됨.

nfs Daemon이 없음을 위에서 확인했지만, automount Daemon을 사용중인 다른 서비스가 있는지에 대한 확인이 필요함.

|  |
| --- |
| 현재 마운트 되어 있는 디바이스에 따른 디스크 공간 사용 현황을 확인하는 명령어 |

|  |
| --- |
| 현재 마운트 되고 있는 디바이스(findmnt) 중 자동마운트(autofs)타입만 출력함.  autofs: 필요할 때만 특정 디렉터리를 자동으로 마운트함. |

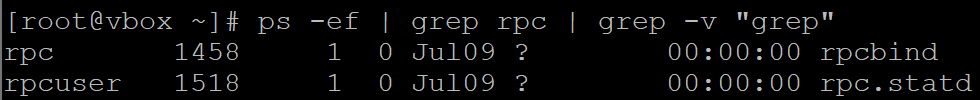
net은 네트워크 공유(NFS 등)을 위한 가상 마운트 포인트이며, misc는 어떤 디바이스가 연결되어있는지 모르겠어서 아래와 같은 명령 구문으로 확인함.



해당 마운트 포인트에 cdrom이 연결되어 있는 것을 확인함.

(양호) 마운트 되어 있는 디렉터리 및 디바이스 정보에 대해 전부 확인했고, 사용목적 및 실제사용여부를 확인하였음.

U-27 : RPC 서비스 확인

 rpcbind : RPC Daemon 실행 시 자체 주소를 생성해서 별도의 프로세스 번호로 실행을 등록함(주소매핑)(1일차 내용중)

(잠깐 다른 얘기)

SLA(서비스수준계약) : 자신 혹은 자신의 회사가 놓친 부분은 어떻게든 드러남 > 결국에는 꼼꼼하게 작업해라

(돌아옴)

불필요한 rpc 서비스에 rpcbind는 포함되어 있지 않음.

rpc.statd 에 대해 rpc 데몬 모니터링 기능이 있지만 실행중인 rpc 데몬이 없음을 설명하고,

nfs 잠금 설정 확인 기능이 있지만 실행중인 nfs 관련 데몬이 없음을 설명함 > "양호" 진단

U-28 : NIS, NIS+ 점검

잘 사용되지 않는 옛 서비스



구동 중인지만 확인하면 됨 > 구동되고 있는 데몬이 없음을 확인 > "양호" 진단

U-29 : tftp, talk 서비스 비활성화

잘 사용되지 않는 옛 서비스



구동 중인지만 확인하면 됨 > 구동되고 있는 데몬이 없음을 확인 > "양호" 진단

앞에 t가 붙는 경우(tftp,ttalk 등) 암호화 하지 않고 사용하겠다는 의미임.

U-30 : Sendmail 버전 점검

|  |
| --- |
| UNIX 계열 OS에서 메일을 보낼 수 있는 방법  1. Sendmail  2. postfix |
| 메일 서버(Sendmail)를 안전하게 사용할 수 있는 방법 3가지(  1. 사용자가 Relay 설정을 추가하거나 변견해선 안된다. Relay를 제한해야함.  ex : 이어달리기 > 무한루프 가능성 있음  2. 사용자가 Message 송/수신 Queue에 임시 보관된 메일을 Drop해서는 안된다. (Queue 방지)  메일 서비스의 중요한 부분은 적시에 받는 것, 확실하게 받는 것, ??  3. VRFY, EXPN (ABUSE) 기능의 방지가 필요함.  ex : 수신확인 : 메일 서버가 제공하는 기능  ABUSE : 다른 사용자가 메일의 송/수신 상태를 확인 가능 |

아래와 같은 명령 구문으로 구동중인 “sendmail” 관련 데몬 확인



아래와 같은 명령 구문으로 설치되어있는 버전 확인(rpm 이용)



최신버전 확인 : 미러에서 패키지 최신 버전(메이저버전 및 마이너버전)을 확인하여 비교

U-31 : 스팸 메일 릴레이 제한

위에서 설명한 relay 기능 제한해야함

relay 설정 확인(sendmail Deamon이 구동중이라면)

cat etc/mail/sendmail.cf | grep "Relay"

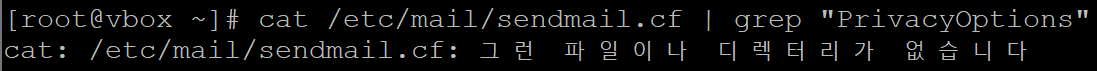
(양호) "sendmail" Daemon이 구동중이지 않고, "sendmail" RPM이 설치되어 있지 않은 상태입니다.

(취약) "sendmail" Daemon이 구동중으로 "etc/mail/sendmail.cf" 파일 내 Relay 설정 값( R$\* $#error $@ 5.7.1 $: "550 Relaying denied")이 주석으로 설정되어 있는 상태입니다.

(대응방안) ~ 참고하시어 "etc/mail/sendmail.cf" 파일 내 Relay 설정의 주석을 제거하여 주시기 바랍니다.

U-32 : 일반사용자의 Sendmail 실행 방지

위에서 설명한 메일 서버 안전하게 사용하기 2번째 Drop 기능을 방지해야함.



(양호)"sendmail" Daemon이 구동중이지 않고, "sendmail" RPM이 설치되어 있지 않은 상태입니다.

(취약)"sendmail" Daemon이 구동중으로 "etc/mail/sendmail.cf" 파일 내 설정 값(O PrivacyOptions=authwarnings)에 "restrictqrun" 값이 존재하지 않는 상태입니다.

(대응방안) ~ 참고하시어 "etc/mail/sendmail.cf" 파일 내 설정 값에 "restrictqrun"값을 추가하여 주시기 바랍니다.

U-33 : DNS 보안 버전 패치

BIND(Berkeley Internet Name Domain)는 인터넷에서 가장 널리 사용되는 DNS 서버 소프트웨어임.

DNS 서비스는 named Daemon으로 구동됨.

Daemon 구동 여부 및 BIND 버전 확인

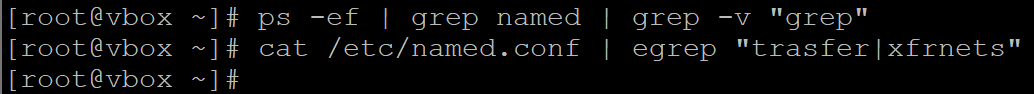
(양호)"named" Daemon이 구동중이지 않고, "named" RPM이 설치되어 있지 않은 상태입니다.

※NVD, CVE Details, KISA 보호나라와 같은 CVE 주요취약점에 대한 정보도 함께 확인하여 주시기 바랍니다.

|  |
| --- |
| CVE : POCE 환경을 통해 계속 제보되고 있고, 넘버링이 계속 올라가고 있음  DNS는 Domain 및 연결된 IP 주소를 가지고 있음.  BIND 취약점 : DNS 내의 정보를 다른 외부 사용자들과 공유  BIND는 거의 모든 버전이 취약한 상태로서 지속적인 최신 버전 업데이트가 필요함.  기반시설가이드에는 이렇게 지속적으로 보고되는 최신 취약점에 대한 내용이 적용이 안되어 있음.  기반시설가이드가 21년 개정되었으니 그 후 보고된 CVE 취약점 등에 대한 전체적인 확인이 필요함. |

U-34 : DNS Zone Transfer 설정

|  |  |
| --- | --- |
| DNS는 여러 영역이 존재하고 그에 따라 영역별로 맡고 있는 역할이 다름.  1. 정방향 조회 영역  - CNAME(별칭), PTR(포인터) : IP 주소를 도메인 주소로 치환함  2. 역방향 조회 영역  - CNAME(별칭), PTR(포인터) : 도메인 주소를 IP주소로 치환함  > 정방향,역방향 각각 CNAME이 다르게 들어가 있음.  3. 영역 전송  이중화(Active-Standby) DNS Active 1, 4, 5 -  Standby 6  ? 1~6번까지는 모두다 동일한 데이터를 보유하고 있어야 함.  로드밸런싱 : 부하분산, 컨테이너 서비스를 통해 사용자 접근이 많아질 경우 자원을 추가하여 서비스의 원활한 접근이 가능하게 함.  DMZ Zone에 외부 DNS가 있을 것임. > 외부 DNS 서버가 죽으면 서비스가 마비됨. > 5~6대 정도로 구성하여 로드밸런싱 구성 3대는 이중화(Data, 똑같이 구성)  이중화 : 연속성 보장  영역 전송(Zone Transfer)   |  | | --- | | RAID Controller  RAID : 파티션 나누..  ~1 : HDD 3개 중 1개에 그대로 백업  ~2 : Hot spare  ~5 : 최소 3개 하드, 3개는 Data 2개 이상을 Hot spare로 사용되는 | |



(양호) "named" Daemon이 구동중이지 않고, "named" RPM이 설치되어 있지 않은 상태입니다.

(취약) "named" Daemon이 구동중으로 "etc/named.conf" 파일 내 설정 값"allow-transfer"에 목적이 확인되지 않은 Host IP 주소가 설정되어 있는 상태입니다.

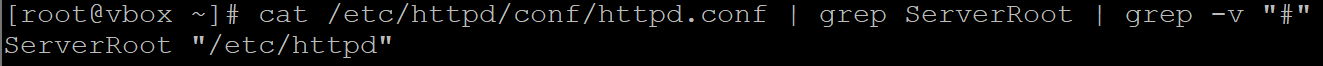
(인터뷰) "etc/named.conf" 파일 내 "allow-transfer"에 등록된 Host IP를 어떤 목적으로 사용되는 서비스인지 담당자 확인이 필요합니다.

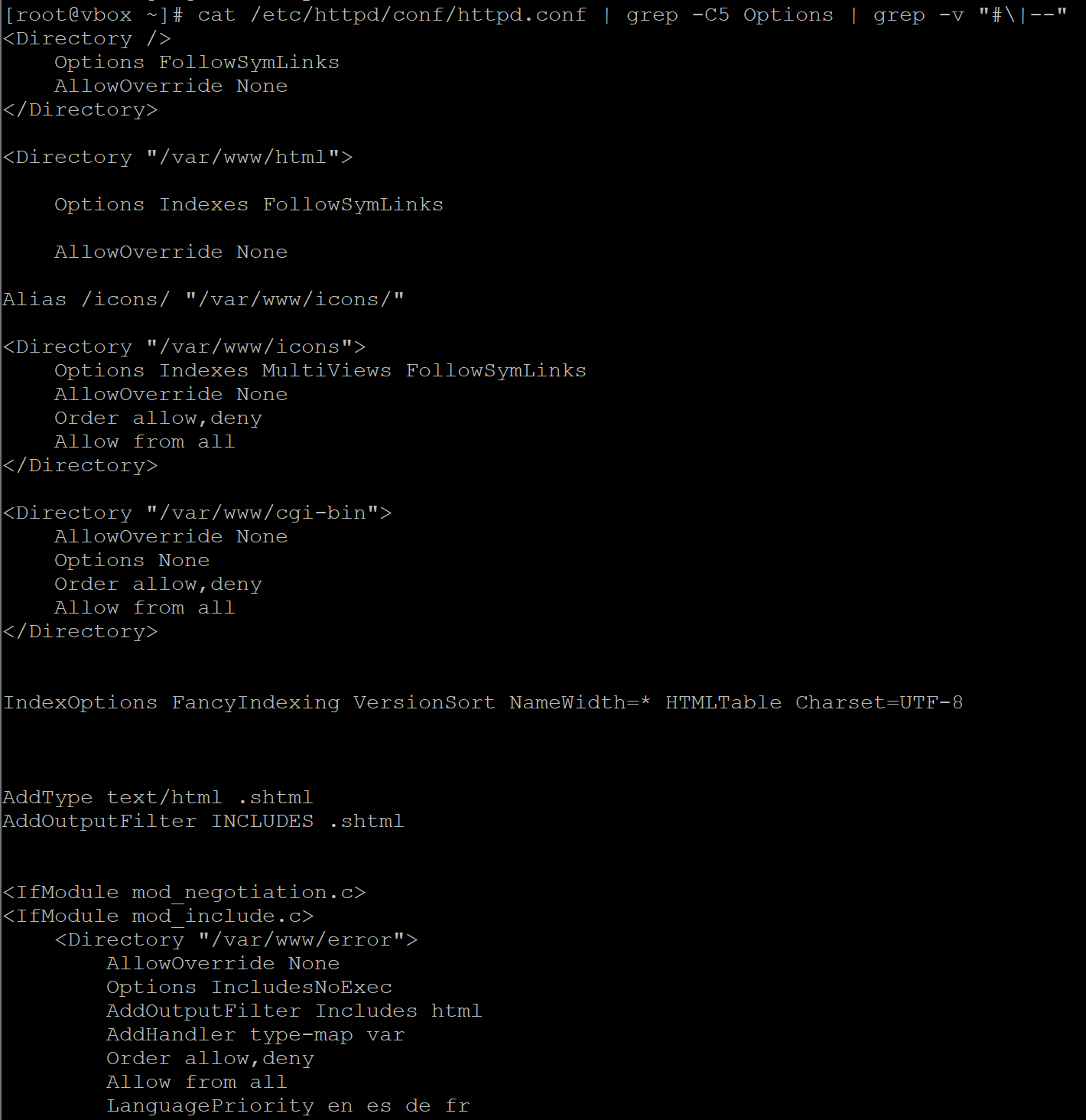
> 이행진단 시 보조 DNS라는 코멘트를 확인한 경우 "양호" 진단

(대응방안)~를 참고하시어 "allow-transfer"에 등록된 목적이 확인되지 않은 Host IP를 제거하여 주시기 바랍니다.

U-35 : 웹서비스 디렉토리 리스팅 제거(Apache)

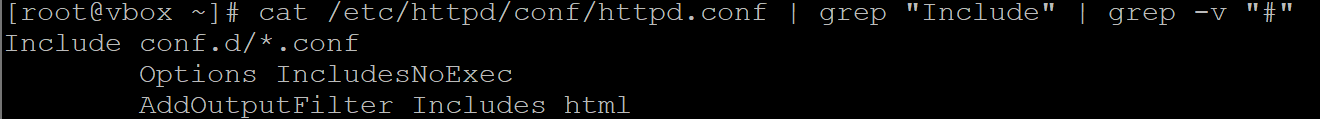
디렉터리 리스팅 : 웹 어플리케이션에서 동적 화면으로 디렉터리가 출력되는 기능

 \*\*ServerRoot : Apache 설치 디렉터리

 (판단기준) 디렉터리 검색 기능은 : Indexes 옵션을 의미함. 위의 명령 구문을 통해 몇몇 설정(“Options”)에 “Indexes”가 설정되어 있는 것을 확인함.

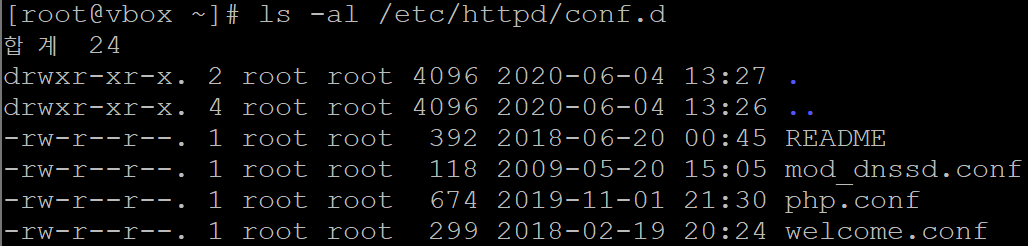
여기에 더해 “Include” 옵션을 확인해야함

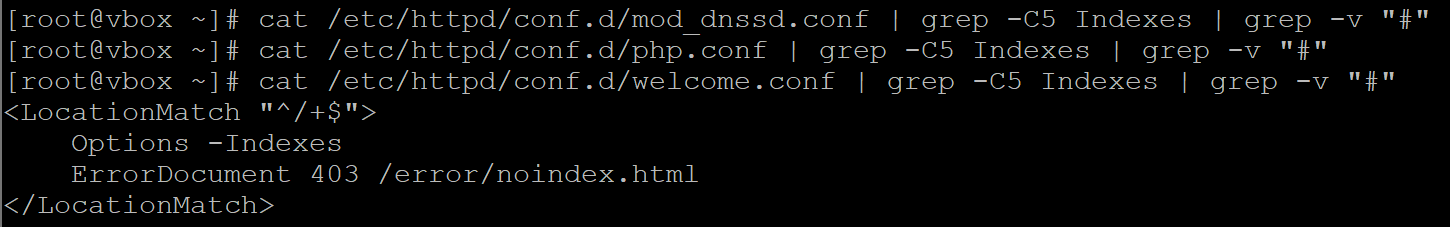
\*\*Include : 하나 혹은 다수의 특정 파일이 설정되어 있으며, 해당 파일의 환경 설정을 전부 포함하여 설정하겠다는 기능임, 기반시설가이드에는 없지만 빼먹고 진단하면 40%만 진단한 것으로 볼 수 있음.



위와 같은 명령 구문으로 확인한 결과 “conf.d/\*.conf” 해당 디렉터리에 .conf 파일을 모두 포함해서 사용하도록 설정되어 있는 것을 확인함.

아래 명령어로 해당 디렉터리 "/etc/httpd/conf.d/\*.conf"의 파일 확인

 해당하는 각각의 파일들(\*.conf)에 대해 "Indexes" 옵션 설정 확인



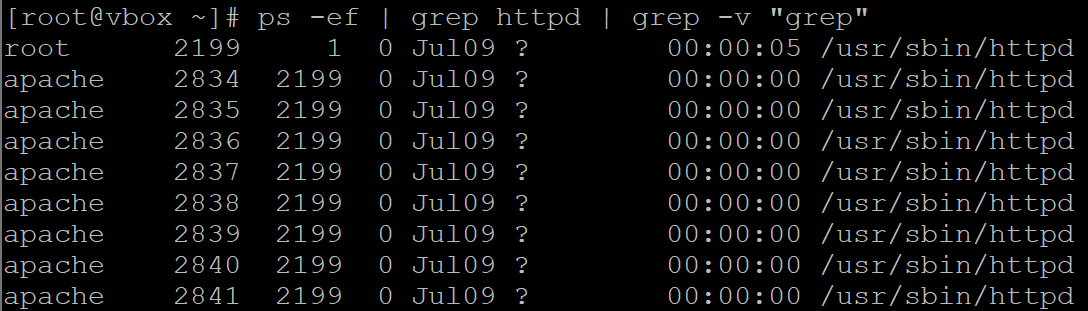
위와 같은 명령 구문을 통해 위의 2개 파일에는 해당 옵션관련 내용이 없는 것을 확인하였고, “welcome.conf” 파일에 해당 설정 구문은 있으나 “-“처리되어 적용되지 않고 있음을 확인함.

(취약)"etc/httpd/conf/httpd.conf" 파일 내 일부 웹 Source 디렉터리에 "Indexes" 옵션이 활성화되어 있는 상태입니다.

※ 현재 대상 Apache에서 include 하고 있는 파일(mod\_dnssd.conf, php.conf, welcome.conf)에서도 같은 명령어를 실행하였을 때 "Indexes" 옵션이 활성화되어 있는 구문은 존재하지 않았습니다.

(대응방안)~참고하시어 일부 웹 Source 디렉터리 옵션 값을 "-Indexes"로 설정하시거나 제거하여 주시기 바랍니다.

U-36 : 웹서비스 웹 프로세스 권한 제한



위와 같은 명령 구문으로 확인해본 결과 "root" 로 쓰고 있는 것 같은데 "양호" 진단임.

왜냐하면 위와 같이 확인해본 결과 1번 PID 는 init 과정에서 호출되는 것이고 수정 불가능한 부분임. 그리고 그 외의 Daemon은 전부 “apache” 계정으로 구동되고 있음을 확인함.

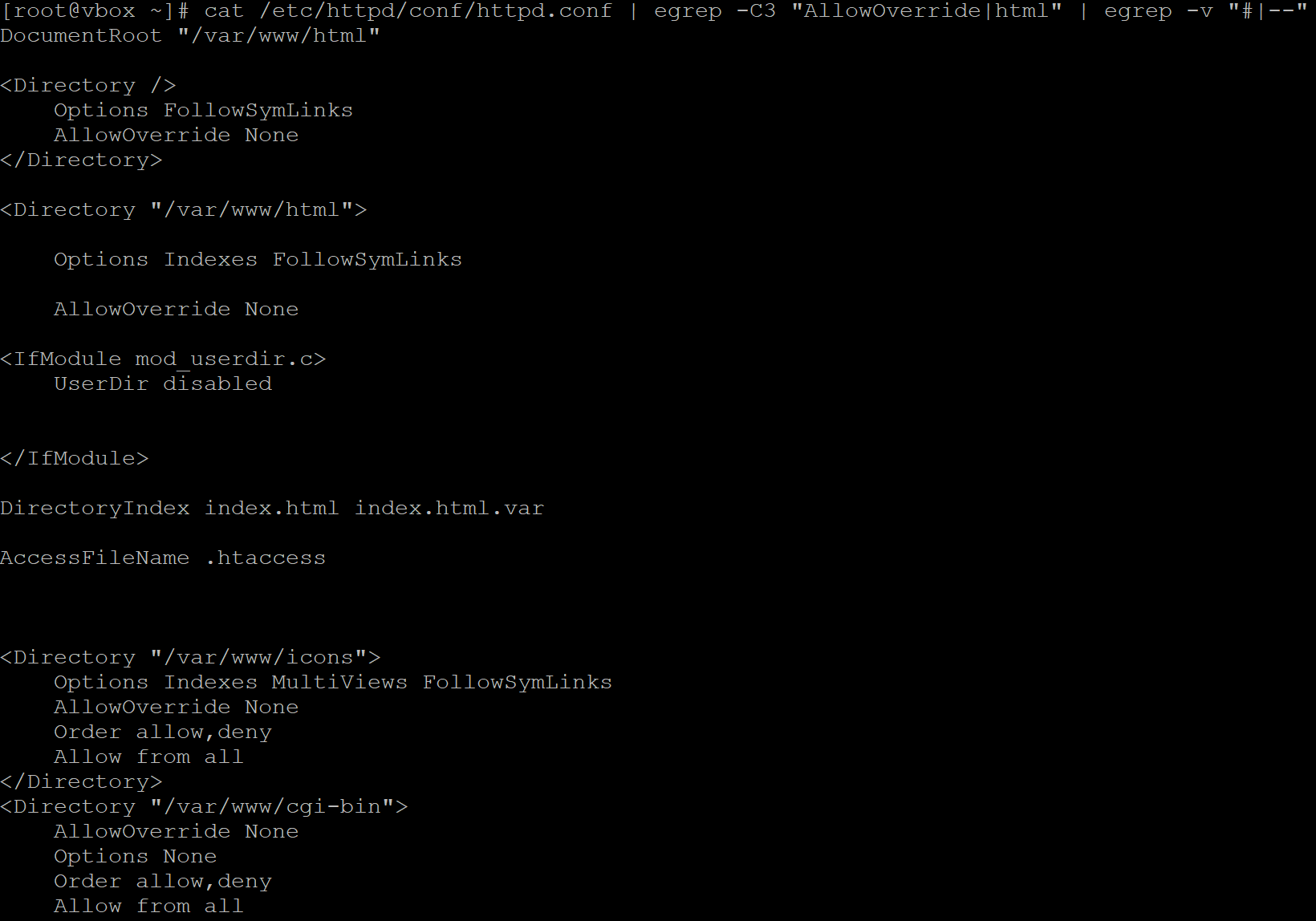


위와 같은 명령 구문을 통해 “httpd” Deamon의 “User” 및 “Group” 계정이 “apache”로 설정되어 있음을 확인함.

(양호) "apache" Deamon이 웹 서버 전용 계정(apache)으로 구동중이고, "User" 및 "Group" 계정이 "apache"로 설정되어 있는 상태입니다.

U-37 : 웹서비스 상위 디렉토리 접근 금지

내용을 찍어내는 것이 어려워 아래와 복잡한 명령 구문을 사용함.

위와 같이 출력 내용이 너무 많아 내용을 확인할 수 있는 상단의 내용만 캡처 및 표시하여 첨부한 후 결과보고서의 해당 셀에 메모를 추가하여 전체 출력결과 첨부함.

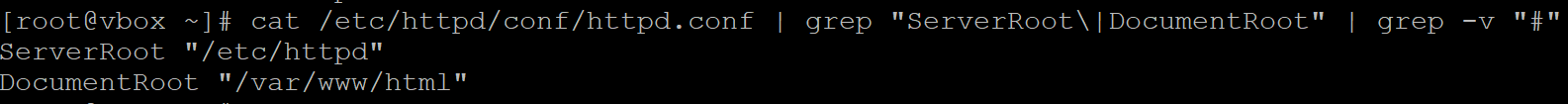
(취약)일부 웹 Source 디렉터리에 상위 경로로 이동이 가능한 "AllowOverride"값이 "None"으로 설정되어 있는 상태입니다.

(대응방안)~참고하시어 "AllowOverride" 값을 "AuthConfig"로 변경하여 주시기 바랍니다.

U-38 : 웹서비스 불필요한 파일 제거

아파치 설치 디렉터리만 표시되어 있지만

htdocs : 웹 사이트의 실제 소스 파일들을 저장하는 디렉터리 > 아파치 설치 디렉터리에 있지 않음



위와 같은 명령 구문으로 Apache 설치 디렉터리 및 Source 저장 디렉터리를 확인함

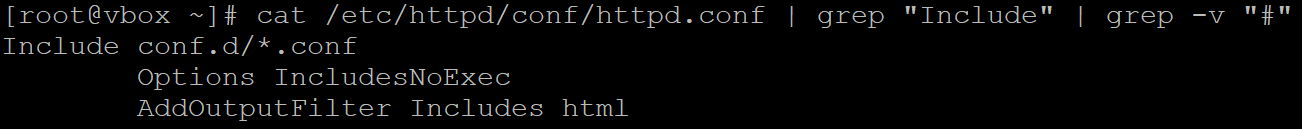


위와 같은 명령 구문으로 두 가지 디렉터리에 “htdocs” 혹은 “manual” 파일이 없는 것을 확인함.

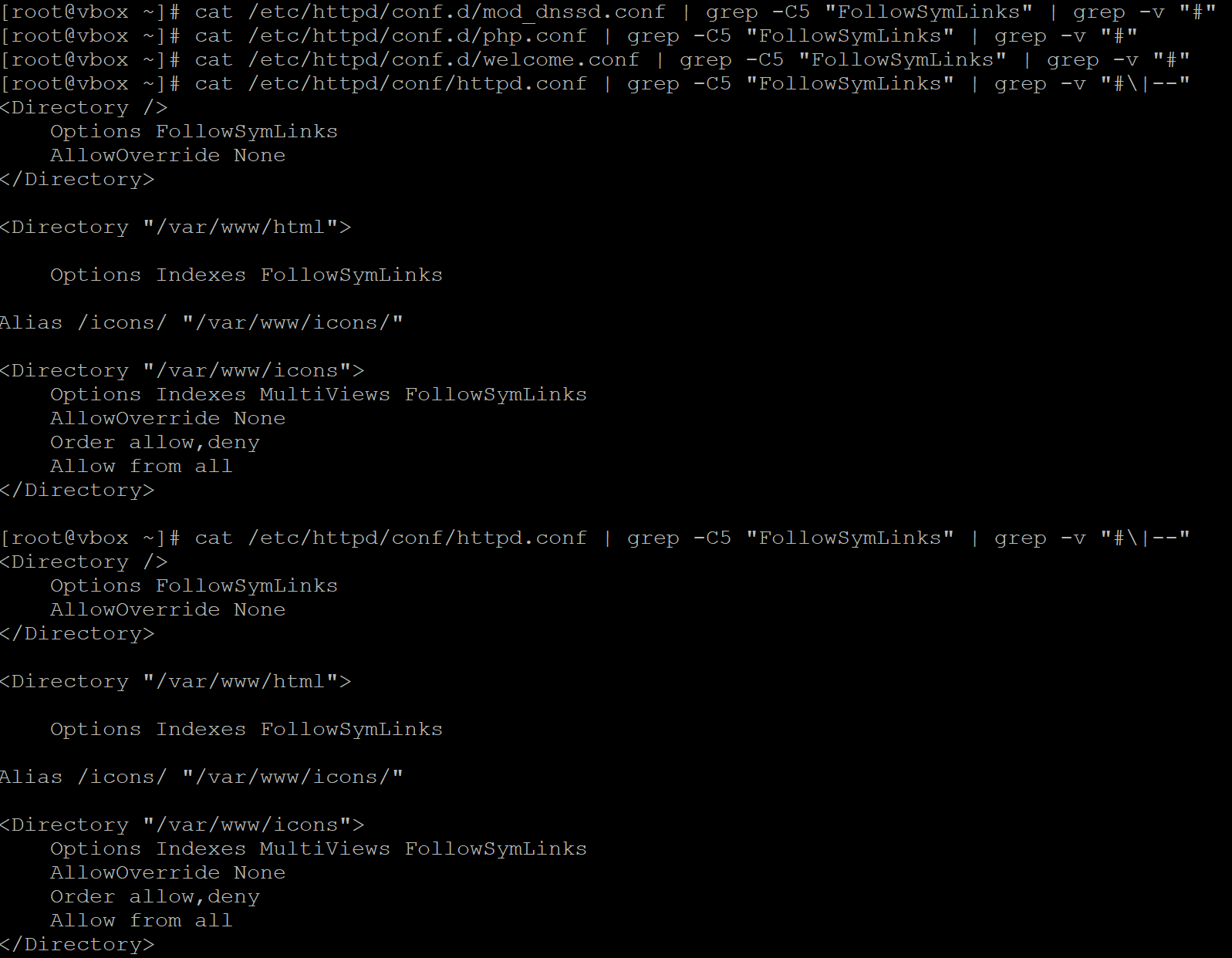
(양호) "apache" 설치 디렉터리 및 웹 Source 디렉터리 내 "htdocs", "manual" 디렉터리가 존재하지 않는 상태입니다.

U-39 : 웹서비스 링크 사용금지

기반시설가이드에서는 …/httpd.conf 파일에 대해서만 확인하라고 했지만 실제로 “httpd” 설정 파일은 더 있음.



위와 같은 명령 구문을 사용하여 U-35에서 확인한 것과 같이 “Include” 설정에 “conf.d/\*.conf” 파일들이 지정되어 있는 것을 확인함.



위와 같은 명령 구문을 통해 Apache 설치 디렉터리의 “httpd.conf” 설정 파일에 “FollowSymLinks” 옵션이 있는 것을 확인하였고, Inculde 되어 있는 3개의 파일에는 “FollwSymLinks” 옵션이 없음을 확인함.

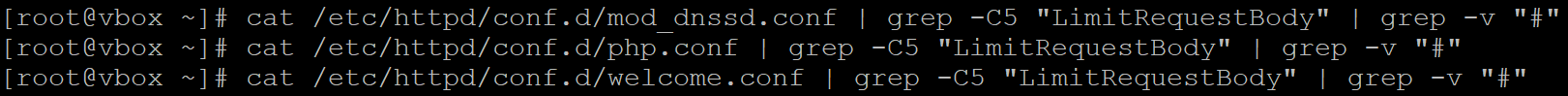
(취약)"etc/httpd/conf/httpd.conf" 파일 내 일부 웹 Source 디렉터리에 "FollowSymLinks" 옵션이 활성화되어 있는 상태입니다.

※ 현재 대상 Apache에서 Include하고 있는 파일(mod\_dnssd.conf, php.conf,welcome.conf)을 확인해보니 "FollowSymLinks" 옵션이 활성화되어 있는 상태입니다.

(대응방안)~참고하시어 "FollowSymLinks" 값을 제거하여 주시기 바랍니다.

U-40 : 웹서비스 파일 업로드 및 다운로드 제한





위와 같은 명령 구문을 통해 Apache 설치 디렉터리의 “httpd.conf” 설정 파일에 “LimitRequestBody” 옵션이 없는 것을 확인하였고, Include 된 3개의 설정파일에도 해당 옵션이 없는 것을 확인하였음.



위와 같은 명령 구문으로 해당 디렉터리의 하위 디렉터리에 “LimitRequestBody”을 가진 파일이 없음을 확인함.

(취약1) 전체 웹 Source 디렉터리에 업/다운로드 용량 제한 설정이 존재하지 않는 상태입니다.

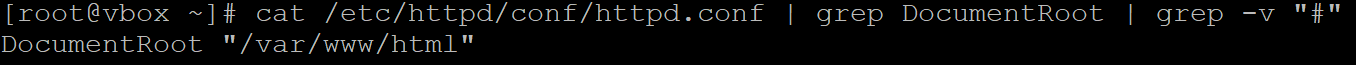
(취약2) 대상 웹 애플리케이션(http://176.16.0.58) 내 게시판 기능이 존재하는 웹 Source 경로(/var/www/html/wordpress/upload)에 업/다운로드 용량 제한 설정이 존재하지 않는 상태입니다.

(대응방안)

주요정보통신기반시설 가이드를 참고하시어 업/다운로드 기능이 존재하는 웹 Source 디렉터리에만 용량(5MB)을 제한하여 주시기 바랍니다.

주요정보통신기반시설 가이드를 참고하시어 게시판 기능이 존재하는 웹 Source 경로(/var/www/html/wordpress/upload)에 용량(5MB)을 제한하여 주시기 바랍니다.

U-41 : 웹서비스 영역의 분리

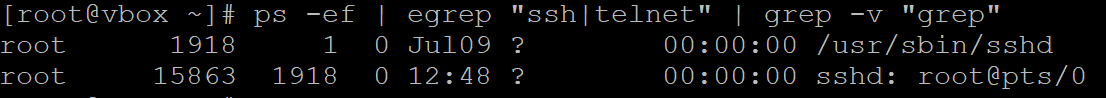
왜 디폴트 디렉터리를 이용하지 말라고 할까 > 잘 알려진 경로이기도 하지만 상위 디렉터리로 타고 들어가면 시스템 디렉터리에 도달할 수 있기 때문임

(취약) "DocumentRoot" 경로가 "var/www/html"로 설정되어 있는 상태입니다.

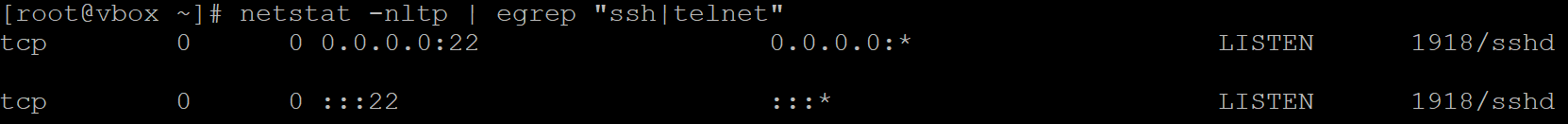
(대응방안)~참고하시어 "DocumentRoot" 경로를 유추할 수 없는 다른 경로로 변경하시거나 시스템 경로와 무관한 다른 파티션으로 경로를 재설정하여 주시기 바랍니다.

※ "DocumentRoot" 경로는 실제 웹 Source가 보관된 경로로써 웹 동적 페이지를 직접 호출할 수 있어 조치 시 웹 개발자와 Comm.및 영향도를 파악하시어 설정 적용하시기 바랍니다.

U-60 : ssh 원격접속 허용



위와 같은 명령 구문으로 “telnet” Deamon은 구동중이지 않은 상태이고, “ssh” Deamon만 구동중인 것을 확인함.



위와 같은 명령 구문으로 “telnet” 관련 OpenPort가 없음을 확인함.

(양호) "telnet" Daemon이 존재하지 않고 "ssh" Daemon이 구동중인 상태입니다.

U-61 : ftp 서비스 확인



위와 같은 명령 구문으로 “ftp” 관련 Daemon이 구동중이지 않음을 확인함.

(양호1) "ftp" Daemon이 구동중이지 않은 상태입니다.

구동중이지 않으니 "양호"이긴 한데 구동중일 때는 <FTP를 안전하게 사용하는 방법>을 참조하여 해당 3가지 중 하나라도 지켜지지 않으면 "취약" 진단함.



위와 같은 명령 구문을 통해 "anonymous\_enable" 설정이 없음을 확인함.

(양호2) "ftp" Daemon이 구동중이지만 "anonymous\_enable"값이 "no", "ftp" 전용 계정(XXX) 사용, UMASK 값이 "077"로 설정되어 있는 상태입니다.

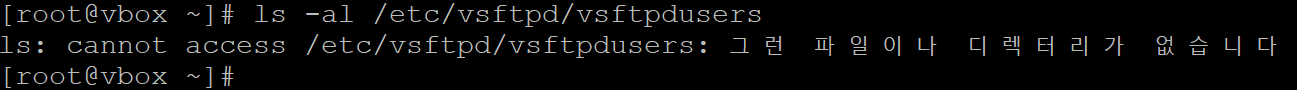
(취약) "ftp" Daemon이 구동중으로 "Anonymous enable"값이 "yes"로 설정되어 있는 상태입니다.

(대응방안)~참고하시어 "ftp" Daemon이 구동중으로 "Anonymous enable"값을 "no"로 변경하여 주시기 바랍니다.

U-62 : ftp 계정 shell 제한

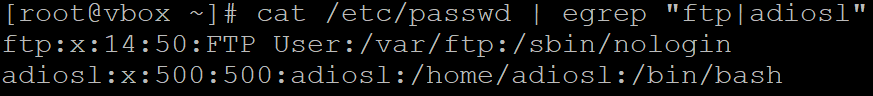
로그인이 안되는 계정의 shell은 nologin 혹은 false임.

위와 같은 명령 구문으로 "ftp" Daemon이 구동중이지 않은 상태임을 확인함.

해당 서비스를 사용할 수 있는 사용자 계정을 확인할 수 있는 설정 파일은 물론 디렉터리 자체가 없음.

(양호)"ftp" Daemon이 구동중이지 않은 상태입니다.

만약 해당 파일이 있고 파일 안에 로그인이 가능한 사용자(예시 : “adiosl”)가 있다면 다음과 같은 구문으로 해당 사용자가 로그인 가능한지 확인함.

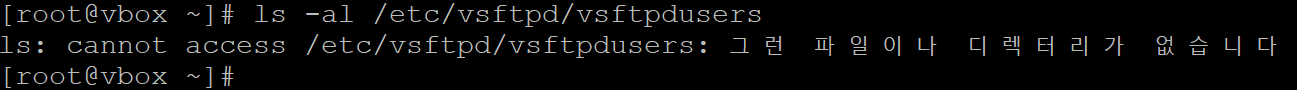


(취약)"ftp" Daemon이 구동중이고 Default 계정은 로그인이 불가능 하도록 "nologin"으로 설정되어 있지만, "etc/vsftpd/vsftpdusers" 파일 내 불필요하게 사용되고 있는 계정이 존재하는 상태입니다.

(대응방안)~참고하시어 "etc/vsftpd/vsftpdusers" 파일 내 불필요하게 사용되고 있는 계정을 제거하여 주시기 바랍니다.

U-64 : ftpusers 파일 설정(FTP 서비스 root 계정 접근제한)







(양호)"ftp" Daemon이 구동중이지 않고 "ftpusers" 파일이 존재하지 않는 상태입니다.

U-65 :at 서비스 권한 설정



위와 같은 명령 구문으로 “at.allow” 파일은 존재하지 않아 진단 대상이 아니며, “at.deny” 파일의 권한이 644(-rw-r--r--)로 설정되어 있음을 확인함.

(취약) "etc/at.allow" 파일은 존재하지 않지만, "etc/at.deny" 파일의 권한은 644(-rw-r--r--)로 설정되어 있는 상태입니다.

(대응방안)~참고하시어 "etc/at.deny" 파일의 권한을 640(-rw-r-----)으로 변경하여 주시기 바랍니다.

U-66 : SNMP 서비스 구동 점검

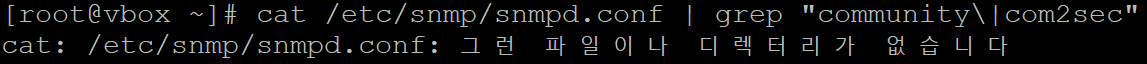
 (양호)"snmp" Deamon이 구동중이지 않은 상태입니다.

U-67 : SNMP 서비스 Community String의 복잡성 설정

SNMP(Simple Network Management Protocol) : 원격 모니터링 및 관리를 위한 프로토콜이며, 관제에서 많이 사용.

|  |
| --- |
| SNMP Server to Client (Network)  Community String (Public/Private) - 유추가 되지 않는 복잡도 기준에 맞게 설정을 변경  SNMPv1 : TEXT Plain  SNMPv2c : 인증절차가 포함된 TEXT Plain  SNMPv3 : 암호화    >v1과 v2c를 사용하면 안전하지 않음.  >v2c까지 안전하다고 하기도 하는 보안장비를 사용할 때는 v3이어야 안전하다고 판단함. |





위와 같은 명령 구문으로 “snmp” Daemon이 구동중이지 않은 상태임을 확인하였으며, 인증 비밀번호인 Community String 설정 값이 들어있는 해당 설정 파일이 존재하지 않음을 확인함.

(양호)"snmp" Deamon이 구동중이지 않은 상태입니다.

(취약)"snmp" Deamon이 구동중인 상태로 "etc/snmp/snmpd.conf"파일 내 "community string" 값이 "public"으로 설정되어 있는 상태입니다.

(대응방안)~참고하시어 "etc/snmp/snmpd.conf"파일 내 "community string" 값을 복잡도 기준에 맞게 유추할 수 없는 값으로 변경하여 주시기 바랍니다.

또는

(양호)"snmp" Deamon을 "NMS(중앙모니터링관리시스템)"에서 네트워크 정보를 수집하도록 구동중입니다.

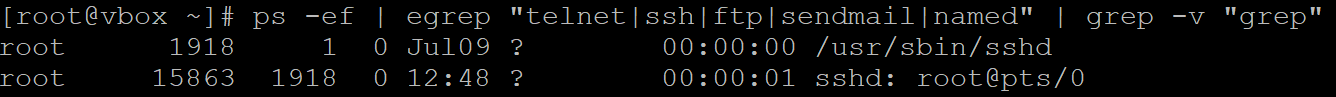
(취약)"snmp" Deamon을 "NMS(중앙모니터링관리시스템)"에서 네트워크 정보를 수집하도록 구동중이지만 "etc/snmp/snmpd.conf"파일 내 "community string" 값이 복잡도 기준에 맞게 설정되어 있지 않은 상태입니다.

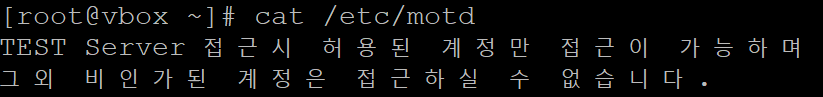
U-68 : 로그온 시 경고 메시지 제공

경고메세지를 제공하는 것은 2가지 측면에서 생각할 수 있음. OS 및 Web 서비스의 버전이 노출되기 때문에 보안 취약점으로 지정, 기반시설가이드에서 진단 대상으로 나와있지만

로그인 가능한 사용자(혹은 공격자)가 접속 시 관계자만 접속해야 한다는 경각심을 위한 경고 메세지가 필요함.

ex : 통제구역이라는 안내 등이 없는데 들어갔다고 해서 사내 정책 등에 처벌을 받을 수 있을까

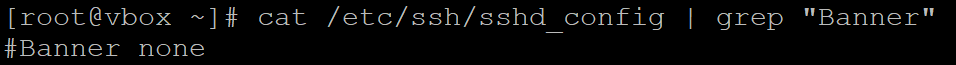




위와 같은 명령 구문으로 “ssh”Daemon이 구동중임을 확인하였고, 해당 서비스에 로그온 메시지가 설정되어 있는 것을 확인함.

Default 로는 해당 설정이 없는데 테스트를 위해 추가되어 있는 상황임.

각 서비스별 설정파일에서 배너 정보가 최상단에 위치하여있고, 해당 파일을 확인하여 서비스 별 배너 정보가 설정되어 있는지 확인할 수 있음



위와 같은 명령 구문으로 확인한 결과 “ssh” 접속 시 배너 설정이 없는 것으로 확인됨.

(양호) "telnet","ftp","sendmain","named" Deamon이 구동중이지 않고 "ssh"만 구동중인 상태로 "etc/motd"파일 내 배너가 등록되어 있는 상태입니다.

(취약) "telnet","ssh","ftp","sendmain","named" Deamon이 구동중인 상태로 모든 Daemon의 로그인이 표시되는 배너가 등록되어 있지 않은 상태입니다.

(대응방안)~참고하시어 "telnet","ftp","sendmain","named" Deamon을 사용하실 경우 배너정보를 등록하여 주시고 사용하지 않으실 경우 해당 Deamon을 중지하여 주시기 바랍니다.

U-69 : NFS 설정파일 접근권한



위와 같은 명령 구문으로 “nfs”의 설정 파일인 “etc/exports”의 권한 및 소유자 확인

(양호)"etc/exports" 파일 소유자 "root", 권한 644(-rw-r--r--)로 설정되어 있는 상태입니다.

U-70 : expn, vrfy 명령어 제한

(U-30의 sendmail을 안전하게 사용하는 방법 3번째 내용)

위에서 설명한 abuse 기능을 방지해야함.







(양호)"sendmail" Daemon이 구동중이지 않고, "sendmail" RPM이 설치되어 있지 않은 상태입니다.

(취약)"sendmail" Daemon이 구동중으로 "etc/mail/sendmail.cf" 파일 내 설정 값( O PrivacyOptions=authwarnings)에 "expn","vrfy" 값이 존재하지 않는 상태입니다.

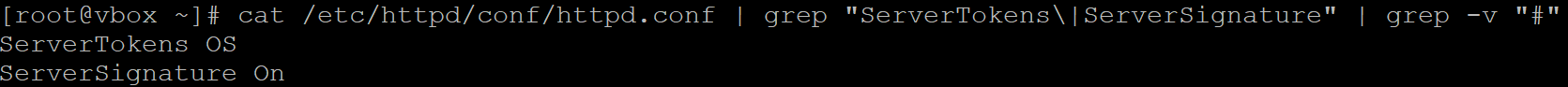
(대응방안) ~ 참고하시어 "etc/mail/sendmail.cf" 파일 내 설정 값에 "expn","vrfy" 값을 추가하여 주시기 바랍니다.

U-71 : Apache 웹 서비스 정보 숨김

Burp Suite 프로그램 활용하여 보여주심.(패킷 캡처 프로그램)

Request 패킷에 따른 Response 패킷을 확인하니 OS 및 웹 서비스 의 버전 정보를 확인할 수 있었음.

“ServerTokens” 설정 값을 “Prod”로 설정하면 HTTP 응답 헤더의 Web Server 버전 및 OS 정보를 최소한으로 줄일 수 있고, “ServerSignature” 설정 값을 “Off”로 설정하면 오류 페이지 하단의 Web Server 버전 및 OS 정보를 출력되지 않게 할 수 있음.



위와 같은 명령 구문으로 확인하니 해당 설정값이 위와 같이 되어있어 보안 취약점에 노출되어 있음.

(취약) "etc/httpd/conf/httpd.conf" 설정 파일 내 "ServerTokens" 값이 "OS", "ServerSignature" 값이 "On"으로 설정되어 있는 상태입니다.

(대응방안)~참고하시어 "ServerTokens" 값을 "Prod", "ServerSignature" 값을 "Off"로 설정하여 주시기 바랍니다.

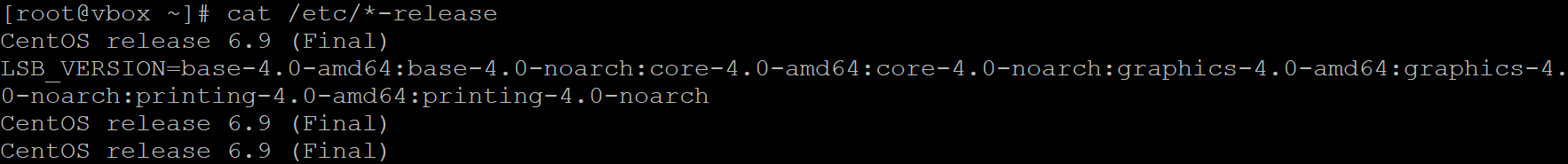
U-42 : 최신 보안패치 및 벤더 권고사항 적용

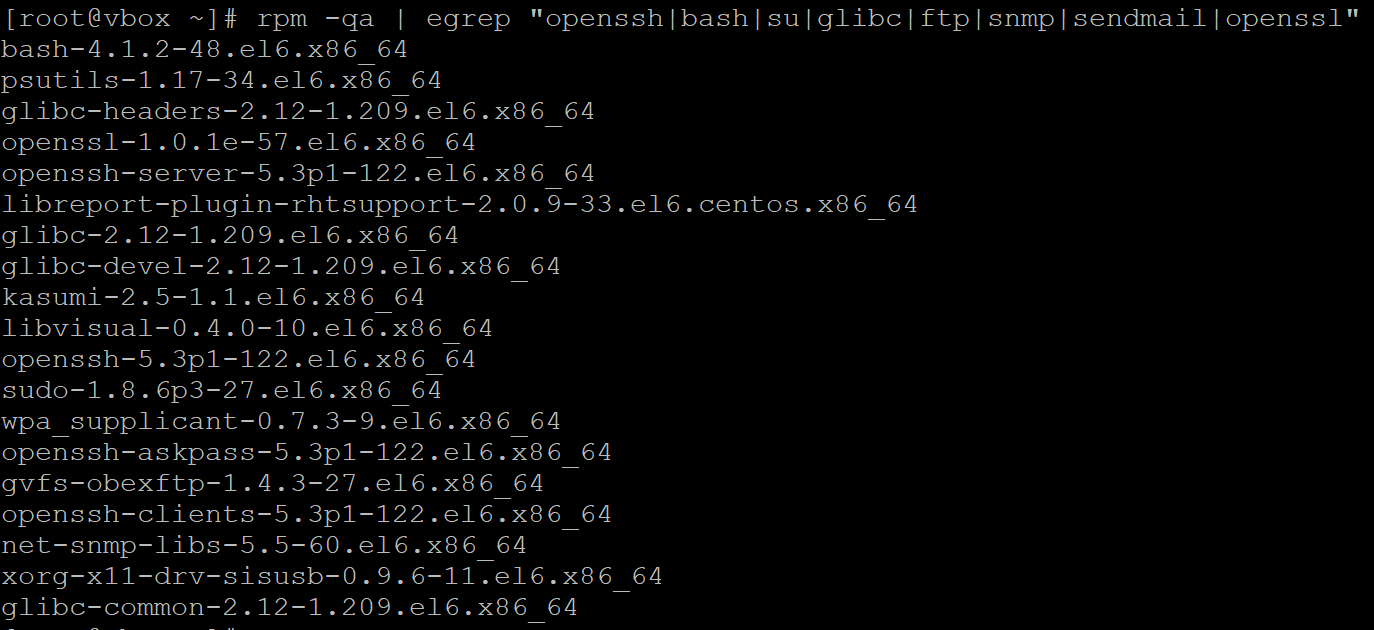
윈도우는 자동 업데이트를 돌리면 되지만 UNIX 계열은 패치를 각각의 서비스에 대해 개별적으로 수동 패치를 해줘야 하는 상황이 발생함.

\*\*CVE 취약점이 발생할 수 있는 Daemon : openssh, bash, su, glibc(고스트취약점), ftp, snmp, sendmail,openssl(Secure Socket Layer)

“named” Daemon은 U-33, U-34, U-68 항목에서 확인했으니 이 항목에서는 제외함.

openssh|bash|su|glibc|ftp|snmp|sendmail|openssl

 위와 같은 명령 구문으로 OS가 CentOS 6.9 임을 확인하였고, 해당 OS는 EoS(End of Service) 되었음을 확인함.



위와 같은 명령 구문으로 해당 서비스들에 대한 rpm 검색을 통해 release 버전을 확인하였음.

(현황) 운영중인 OS(CentOS 6.9)는 2020년 11월 30일 기준으로 EOS(End of Service) 되어 repository가 존재하지 않는 상태로 최신 패치가 불가능한 상태입니다.

※ 공식문서 Link : https://access.redhat.com/support/policy/updates/errata/#RHEL6

(대응방안)~참고하시어 최신 패치 적용을 위해 상위 버전으로의 OS 신규 구축을 진행하시기 바랍니다.

※ 시스템 및 서비스 변경 시 서비스 영향도를 파악하시어 설정 적용하시기 바랍니다.

OS 버전 업데이트시 다양한 문제가 발생함(사용하던 어떤 Deamon은 사용이 안되던가 등)

이행진단 시 "~~까지 OS 업데이트 하겠습니다" 라는 코멘트를 받게됨. 이후의 취약점 진단에서 지속적으로 체크됨.

ISMS에서 "중" 결함이 2개이상 나오면 심사 취소되고 이 U-42 항목은 “중” 중요도이기 때문에 중요하고 어려운 항목이며 지속적으로 확인해야함.

U-43 : 로그의 정기적 검토 및 보고

기반시설가이드의 설명이 부족한 점은 잘 보관하고 있는지를 정기적으로 검토하는지만 체크함. 잘 보관하고 있는지 아닌지는 진단 대상이 아님.

|  |
| --- |
| 로그를 안전하게 보관 및 관리하는 방법(OS, WebServer, WAS, Services 등 전부 포함)  1. 로그의 최소보관 기간(1년)에 맞춰 보관해야 함. (법적으로 근거가 있음 찾아보셈)  2. 보관하고 있는 로그를 주기적(1개월)으로 로그의 문제가 있는지 검토하고 상위 직책자에게 이를 결재 받는 절차가 존재해야함.  (기반시설가이드와 동일)  3. 저장하고 있는 모든 로그는 서버 내에만 존재해선 안되며, 해당 로그를 별도 장치 별도 보관해야함.(로그의 무결성)  4. 기존 서버에서 보관중인 로그와 별도 장치에 보관하고 있는 로그는 그 누구도 수정해선 안됨.  ex. 공격자의 첫 번째 할 일을 자신의 접속 로그를 변조 혹은 삭제 하는 것임. |

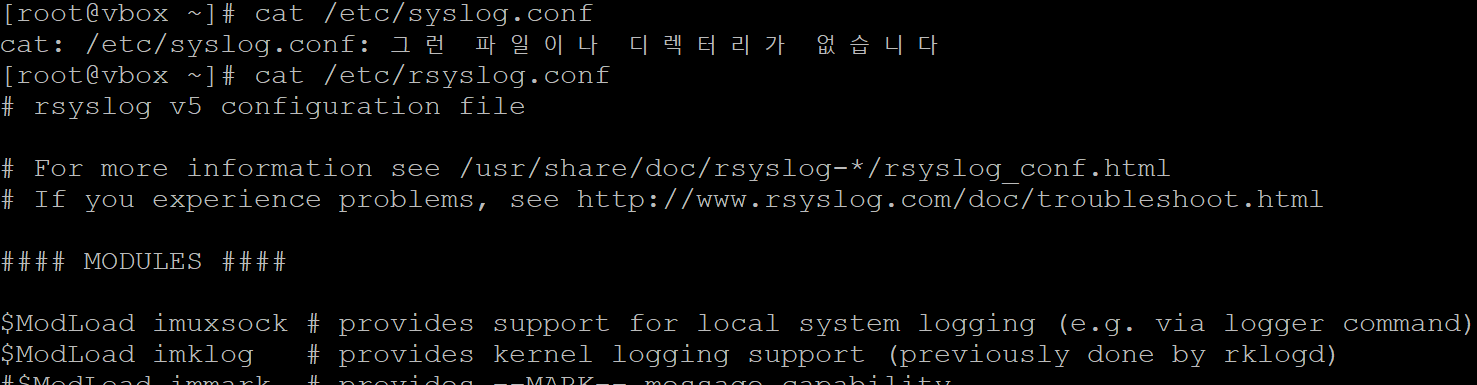
(인터뷰)

- 시스템 로그, 사용자 접속 기록 등의 로그를 정기적(1개월)으로 감사하고 있고 문제 발생 시 보고 체계가 마련되어 있는지 담당자 확인이 필요합니다.

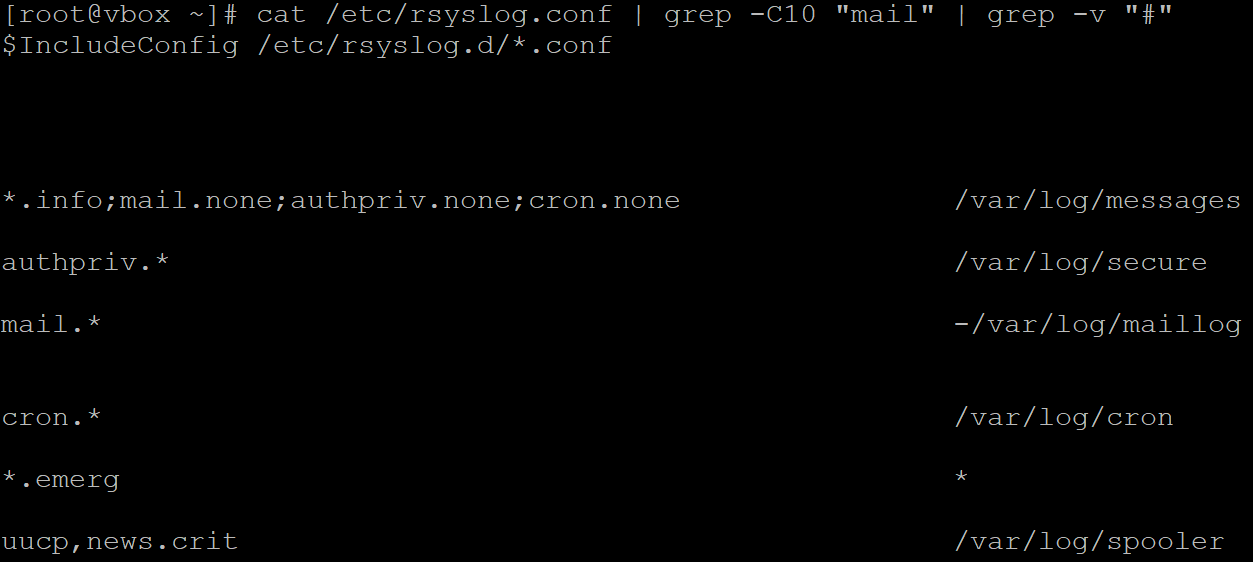
: 로그의 정기적 감사 여부

: 정기적 감사에 따른 보고체계 유무

U-72 : 정책에 따른 시스템 로깅 설정



위와 같은 명령구문으로 시스템 로깅 설정 파일 “etc/rsyslog.conf” 파일을 확인, CentOS 6.9 버전이기 때문에 “etc/syslog.conf” 파일은 없음을 확인함.



위와 같은 명령 구문으로 “\*.info”, ”authpriv.\*”, “mail.\*”, “cron.\*”, “\*.emerg”의 시스템 로깅 설정이 되어있음을 확인함. 그 중 “authpriv.\*” 로그는 개인 인증, 즉 su에 관련된 로그임.(/var/log/secure 디렉터리 에 저장됨)

“\*.alert” 가 없다고 "취약"으로 잡으면 안됨. 경고 로그이며 ".info" 내에 포함되어 있음.

(양호) 'su' 로그 및 시스템 로그(alert, cron, info 등)를 기록하도록 기준에 맞게 설정되어 있는 상태입니다.