250709, 취약점 진단강의

// 강사님 소개

쉴더스 ITC 이동윤 수석님

시스템 엔지니어

리저널매니저

// Intro

취약점 진단은 7가지 분야로 나뉜다

> 시스템,웹,모바일,소스코드,클라우드,iot,개인정보

취약점 진단의 가장 큰 이유

> 보안성 검토

보안성 검토

> 서비스 런칭 전에 컴플라이언스,기술,관리적인 요소 진단 수행 및 취약점 점검

> 데이터, 고객의 자산, 발생할수있는 공격

서브넷팅

> 네트워크의 범위를 정하는 규격

> 진단수행에 네트워크에 대한 지식은 기본임

취약점 진단은 가이드가 있는 반면 모의해킹은 가이드가 없음

>취약점 가이드 : 주요정보통신,금취분평(금융보안원,비공개자료,담당자만활용,해당하는 금융업 기업만),사내자료

모의해킹 : 블랙박스(정보x),그레이박스(대상 어플리케이션 주소만),화이트박스(대상 주소,일반계정,관리자계정)

> 대상 : 웹 어플리케이션

리터널 무브먼트 : 금전편취,다른 사용자의 주요정보 획득

모의해킹은 어떤 시나리오를 도출해내냐에 따라서 측면이동분야가 아주 넓어질 수 있다.

모의해킹과 모의침투는 같은 의미이지만 현대적으로는 모의침투가 더 괜찮은 단어이지않을까

취약점진단과 모의해킹은 완전히 다른 업무

진단을 통한 래퍼런스 쌓기 3~4년 이후 부터 모의해킹 업무가 가능

AI의 정확도는 신뢰성이 떨어진다 : 머신 러닝의 결과에 대한 검증과정이 필요함 : 공부에 적용하여 질문을 많이 할 것

네트워크,인프라,개발에 대한 개념이 필요함

CVE 취약점이 발생할 수 있는 부분에 대해서 패치하기 위해서는 관련지식이 필요함

코드를 읽지 못하면 담당자나 개발자와 대화가 안됨 > 자바 공부 추천

웹 어플리케이션 : 시스템,클라우드,앱등을 통한 구성

// 취약점진단 관련개념

유닉스 계열 OS(4가지만 알면 됨)

> AIX = IBM 유닉스 (Power 서버용)

> Oracle Linux = 리눅스지만 유닉스 스타일로 운영, Oracle 제품 최적화

> HP-UX = HP 전용 유닉스 (서버 특화)

> Solaris = 안정성과 성능 강조, Sun → Oracle 인수

윈도우계열

> AD 서버: 중앙 집중식 사용자·정책 관리, 일반 서버는 서비스 제공 목적

> 12→16: 보안 기능 대폭 강화, 가상화·AD 고도화 (Credential Guard 등)

> 12→19: 클라우드/컨테이너/ATP 등 현대화 기능 강화

> 폐쇄망: 여전히 08 쓰는 곳 많음 → 보안 취약성 주의

DB

> Oracle / MSSQL / PostgreSQL = ORDBMS → 객체지향 지원

> MySQL = RDBMS → 제한적 객체지향

> MongoDB = NoSQL 문서형 → 객체 비슷하지만 객체지향 아님

웹 서버

> Apache : 대표적인 오픈소스 웹 서버

> Nginx : 성능·경량화에 강점, 비동기 처리

> IIS : Windows 플랫폼 기반 웹 서버

> WebtoB : 티맥스소프트 웹 서버 (국내에서 사용)

WAS

> 개념 : 클라이언트 단에 있으면 패킷조작 등이 가능해짐 > 백엔드에 있음

와스는 무조건 컨테이너로 동작함

> 예시 : 회원가입 버튼을 눌렀을 때 DB 가기전 거치는 API

> 대표적인 종류 :

tomcat : 오픈소스 Java WAS

WebSphere : IBM 상용 WAS

JEUS : 국산 WAS(티맥스소프트)

네트워크

> L2 : 스위칭 (MAC 기반), 허브/스위치

> L3 : 라우팅 (IP 기반), 지역 스위치

> L3와 L4 사이에 내부 방화벽 > 사용자·서버·관리자 간 출입 제어 (IP 접근통제 등)

> L4 : 전송 계층, 포트 기반 제어, 라우터

> L4 이후에 외부 방화벽 : 모든 트래픽 차단 및 화이트리스트만 허용

보안장비

> WAF(Web Application Firewall) : 웹 공격 탐지 및 차단 (XSS, SQLi 등)

> IDS(침입 탐지 시스템) : 이상 징후 탐지, 알림만 수행

> IPS(침입 방지 시스템) : 실시간 공격 차단 및 방어 조치 수행

대부분의 컨설팅 회사가 거의 유사한 진단 방법론을 가지고 취약점 진단을 진행한다.

최초진단·이행진단은 정보통신망법 및 ISMS 지침에 명시되어 있고 실제 수행되어야 심사가 가능해짐.

위험분석/평가 보고서 및 최초진단/이행진단 결과 보고서 등은 정보자산리스트에 필수적으로 포함되어야 함.

주요정보통신기반시설 가이드만으로는 진단 및 조치 기준이 부족하기 때문에 많은 사내 가이드 정보를 필요로 함.

반례로 금취분평(금융취약점보안평가) 같은 경우 많이 사용되지 않는 플랫폼 등에 대해서도 자체 진단·조치 기준이 포함되어 있음.

맨 먼스 (man-month, M/M) : 프로젝트에서 한 사람이 한 달 동안 작업할 수 있는 작업량을 의미하는 단위

8080 : 톰캣 관리자 포트

8443 : 톰캣 ssl 리다이렉션 포트

오픈된 포트로 진행중인 서비스 확인 가능

포트 열려있는데 서비스가 없다 > ip테이블에서 뭔가 잘못된거다. > 혹은 불필요한 서비스(데몬)가 구동중이다. > 담당자에게 얘기, 보고된 것과 다른 미들웨어 등이 발견되었다 > 보통 모른다고 한다 > 보통은 진단 하겠다고 하는데 너무 많으면 담당자의 의사결정 받아야됨 > 진단 대상 리스트도 잘못 되었다

진단 수행

결과는 > 양호,취약,인터뷰 > 그 중 인터뷰가 필요한 항목은 10프로 이상 > 진단을 하면서 인터뷰 항목 뽑아서 담당자 혹은 SE에게 요청함(최초진단 끝나고 하는게 아님) > 절차상으로는 보안담당자에게 전달하는 게 맞지만 실무에서는 미리 양해를 구하고 매니저님 포함해서 SE 분들에게 직접 소통하는 경우가 많음

최초 진단 이후 2개월~3개월 등의 기간 이후 조치 점검 수행함 > 공수가 보통 1/3로 줄어듦

질문이 명확하지 않으면 답변이 명확하지 않음

결과보고서 작성시 픽픽을 이용해서 빨간색박스로 양호,취약 표시

// 환경 구성 : 버추얼박스 + 제공된 vdi(CentOS) 이용

> Rocky9을 사용해 리눅스 및 네트워크에 대한 기본 조작을 공부했던 지난 실습과는 다르게 가상머신 원본 데이터를 따로 유지할 필요가 없음

(=취약점 진단은 다양한 경로로 조회만 할 뿐 데이터를 수정하지 않음)

IP Address 확인

cmd-ipconfig- 기본게이트웨이가 있는 이더넷의 IPv4 주소를 사용함

SSH 정보

HOSTIP/Port : 192.168.0.53/22

GUESTIP/Port : 10.0.2.15/22

로그인 계정 정보

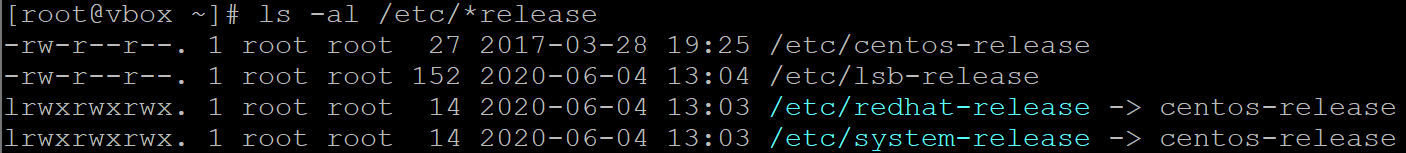
ID : root

PW : Pa55word!!@@

// 결과보고서에 입력하며 취약점 진단 진행

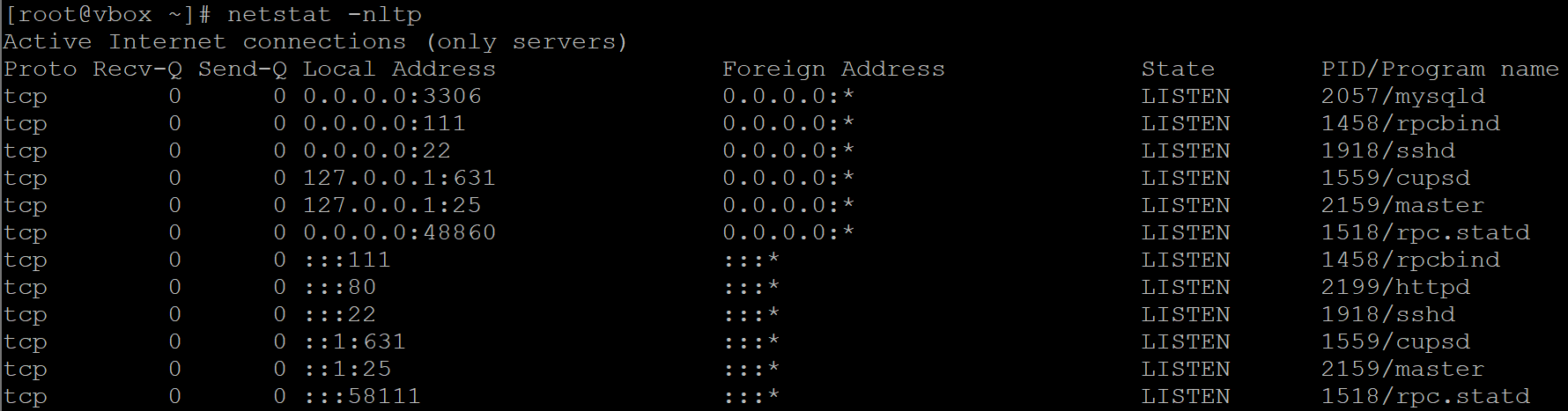
OS 서비스 및 버전 확인

cat /etc/\*release



DB 서비스 및 버전 확인

1. OpenPort 확인(을 통해 설치되어있는 서비스 확인)



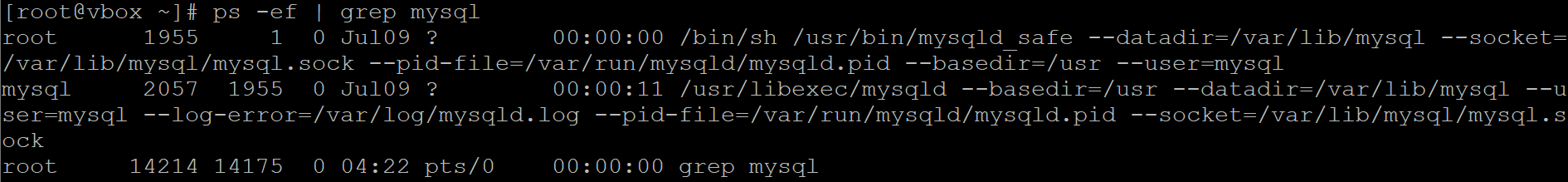
Port any/3306으로 mysqld 포트가 열려있음을 확인함

Local Address : 0.0.0.0/0 : Cloud 보안그룹 정책에서 전체를 허용했을 때(허용범위=Listen)

DB 서버에 접근 할 수 있는 IP가 명시되어 있어야 하는데 ANY로 설정되어 있음.(기반시설가이드에 있는 내용임.)

2. 실행 중인 Daemon 확인(해당하는 서비스, 이 경우 mysql)

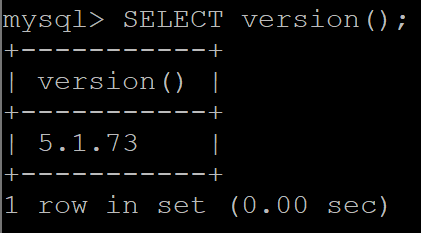
ps -ef | grep mysql



2번째 라인에서 프로세스 구동 중임을 확인함.

3. mysql -uroot -p > DB 서버 접속

SELECT version(); > 쿼리 문으로 DB 버전 확인



이 정보를 입력하면 안됨 > 아래와 같이 설치가 rpm 방식인지 Source 방식인지 확인할 필요가 있음.

UNIX 계열에서 Daemon을 설치하는 방법에는 아래와 같이 2가지가 있음

DB에 직접 로그인할 필요 없이 아래와 같은 방법으로 확인하면 됨.

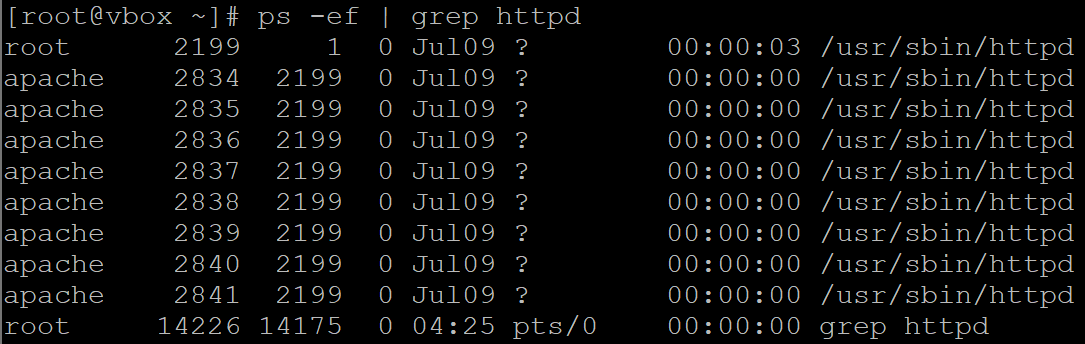
|  |
| --- |
| 가. Repository 설치방법  CentOS 6.9가 EOS 되어서 packege를 설치할 수 있는 rpm이 없음  - Mirror Site에 존재히야만 설치가 가능함  - 설치 경로도 FIX 되어있음.  - 무조건 확장자가 ".rpm"임  나. Source 설치방법  - 공식 홈페이지 > 설치 tar 파일 다운로드  > sftp(22) > 설치 경로 지정 또는 생성 > tar 압축해제  > 설치 패키지 파일 실행  참고1. SFTP 접속 방법  파일질라 프로그램(윈도우) 이용 > sftp://hostip  다. 2가지 방식의 차이점  - (Source 방식으로 설치하면)설치경로가 운영 및 담당자로 인해 달라질 수 있음.  - (Source 방식으로 설치하면)설치된 Daemon의 확장자가 ".RPM"을 가지고 있지 않음.(  > 아래와 같이 rpm 파일이 있는지 확인하여 구분함.  rpm -qa | grep mysql    mysql-5.1.73-8.el6\_8.x86\_64 > rpm 파일이 있으니 Repository 로 설치됨  5.1.73-8.el6\_8.x86\_64 > 버전.e(OS버전)\_(커널버전).(CPU버전)  5.1.73-8 > 메이저버전-마이너버전 |

Web Server 서비스 및 버전 확인

httpd에 80포트이면 Apache 가 설치되어 있다고 생각하면 됨

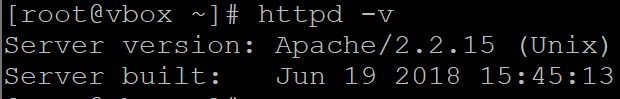
nginx의 경우 Program name이 nginx 임

ps -ef | grep httpd



아파치의 버전은 아래의 구문으로 확인

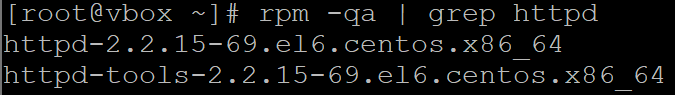
httpd -v



입력하면 메이저버전만 나옴

마이너버전 정보까지 확인하기 위해 아래의 구문으로 확인하는 것을 추천

rpm -qa | grep httpd



2.2.15-69 > 전체 버전

Web Server로 Apache가 설치되어 있는 것과 구동 중인 것을 확인하였고 결과보고서에 다음과 같이 입력함.

Web server : APACHE 2.2.15-69

WAS 서비스 및 버전 확인

환경변수 : 해당 데몬이 설치되어 있는 경로 저장, 설정하지 않으면 일일히 실행할 때마다 루트 지정해줘야함.

Tomcat은 Java(JDK)가 설치되어 있어야 구동됨.

톰캣이나 와스 서버를 구동하고 있을 경우 (netstat -nltp) 입력했을 때 프로그램명이 전부 java로 나옴.

자바에 대한 환경변수를 지정해줘야하고 톰캣인 경우 해당 환경변수도 지정해야함 > 사용자 환경변수에 들어감

톰캣 등 와스는 전부 다 설치 후 환경변수를 수동으로 등록해줘야함.

rpm -qa | grep tomcat



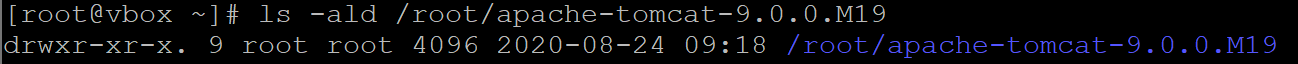
결과 없음.

rpm으로 검색해도 없을 때 (캡처2)와 같이 netstat 에 java가 보이면 WAS가 있는 것임

> netstat에 없으면 WAS 서비스가 없는 것임.

그런데 다음과 같이 확인해보니 디렉토리가 설치되어 있음

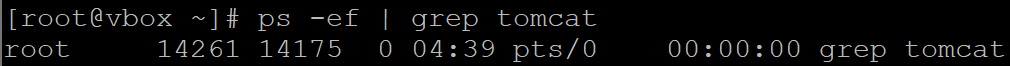
ls -ald /root/apache-tomcat-9.0.0.M19



디렉토리가 있는데 설치 되어 있는 건지 아닌지 모르겠음.

그래서 다음과 같이 구동중인 데몬을 확인함 >

ps -ef | grep tomcat



> 구동중인 데몬이 없음 > 진단 대상이 아님

서비스를 확인할 때는 1.포트오픈 되어있고(netstat) 2.데몬이 구동중인지(ps -ef) 확인하여야함.

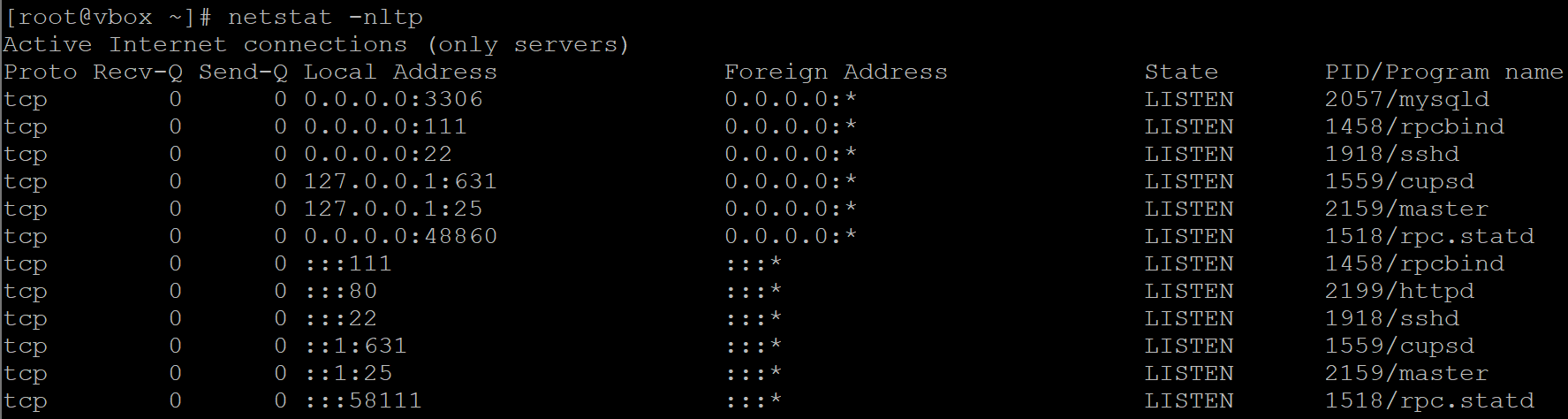
구동중인 WAS Server 서비스가 없음을 확인하였고 결과보고서에 다음과 같이 입력함.

WAS : N/A (/root/apache-tomcat-9.0.0.M19 설치 디렉터리만 존재함)

> 이런식으로 디렉터리 내용 추가해줄 수 있지만 크게 의미없음(N/A만 적어도 무방함.)

// 포트 분석

netstat -nltp



Program Name을 보고 해당 프로그램이 뭔지 알아야한다.

1.1. rpc : Remote Procedure Call

원격 프로시저 호출, 내부 네트워크 Private Client 요청 시 > RPC Daemon 실행(전제조건 : 서버 내 관련 RPC 데몬이 존재해야함) > Client 요청에 의해 서버에서 강제로 RPC Daemon이 실행됨.

원격 요청의 주체 : 내부네트워크(private)/외부네트워크(public)

(반대개념)XINETD(인터넷슈퍼데몬) : 외부 네트워크 Public Client 요청 시

관련이 없는 사용자가 내부 데몬을 실행할 수 있다는 건 > 침해임

Daemon은 1. 시스템 및 사용자 Base에 따른 구동이 있고 2. RPC에 따른 구동이 있음.

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

NFS 공유 드라이브가 잠금 상태인지 아닌지 모니터링 하는 추가 기능이 있음.

NFS(Network File System) : UNIX 계열 공유 디렉터리 개념, 디렉터리 또는 파티션이 공유 드라이브 형태로 사용됨

> AutoMount : 디렉터리 및 파티션을 Mount

> Cron : 시간/일/주/월 에 따른 주기적 예약 작업

> At : 일회성 예약 작업

> pam : Pluggable Authentication Modules : 리눅스 시스템에서 인증 및 접근 제어를 위한 모듈식 시스템

1.3. rpcbind : RPC Daemon 실행 시 자체 주소를 생성해서 별도의 프로세스 번호로 실행을 등록함(주소매핑)

2. mysqld : MySQL Daemon

3. sshd : SSH(SecureShell) Daemon (port 22)

(반대개념)telnet : 네트워크 패킷이 암호화 처리가 안되어 있어 보안 위협에 노출되어 있음, (port 23)

(예시) http <> https : http는 wireshark 켜놓고 패킷 다 보면 id,pw 등 전송되는 데이터를 전부 확인가능, 단순 View page등에만 사용할 것

내부 네트워크에 접근 하는 방법은 내부네트워크 접근 가능한 다른 네트워크를 통하거나, DMZ를 통하는 방법이 있음

(관련개념) Bastion Host(배스천 호스트) : 다 막고 내 IP만 접근 가능으로 설정해놓음 > IP접근통제

4. cupsd(Common Unix Printing System) : 프린터 구동 Daemon(Port 631)

요즘은 프린터 기기에 네트워크 카드가 다 들어있어서 사용 잘 안함 > 불필요하게 Open되어 있는 Port

5. master : SMTP(Simple Mail Transfer Protocol)(Port 25)

아래와 같은 구문으로 확인해보면 postfix라는 게 있음.

ps -ef | grep master

(캡처12)

postfix는 SMTP 메일 서버이며, master 프로세스는 postfix의 메인 컨트롤러임.

netstat에서 127.0.0.1은 로컬호스트만 송/수신 가능하여 보안상 안전하지만, 외부 메일 송/수신 불가한 상태임

0.0.0.0으로 되어 있다면

> Mail 송/수신 > Massage Queue에 저장됨, 송/수신별로 존재 > 사용자 사서함(Inbox) > FIFO라서 취약점이 되기도 했었음.

6. httpd : apach Daemon

(참고):::111 : IPv6 주소형식

(참고)결과보고서 예시의 색깔은 디폴트로 깔려있는것(빨간색), 사용자가 설치한 것(노란색)을 표시함.

// 데몬분석

[root@vbox ~]# ps -ef

|  |
| --- |
| [root@vbox ~]# ps -ef  UID PID PPID C STIME TTY TIME CMD  root 1 0 0 Jul09 ? 00:00:01 /sbin/init  root 440 1 0 Jul09 ? 00:00:00 /sbin/udevd -d  root 1371 1 0 Jul09 ? 00:00:00 auditd  root 1396 1 0 Jul09 ? 00:00:00 /sbin/portreserve  root 1407 1 0 Jul09 ? 00:00:00 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5  rpc 1458 1 0 Jul09 ? 00:00:00 rpcbind  dbus 1478 1 0 Jul09 ? 00:00:00 dbus-daemon --system  root 1492 1 0 Jul09 ? 00:00:00 NetworkManager --pid-file=/var/run/NetworkManager/NetworkManage  root 1498 1 0 Jul09 ? 00:00:00 /usr/sbin/modem-manager  rpcuser 1518 1 0 Jul09 ? 00:00:00 rpc.statd  root 1551 1 0 Jul09 ? 00:00:00 /usr/sbin/wpa\_supplicant -c /etc/wpa\_supplicant/wpa\_supplicant.  root 1559 1 0 Jul09 ? 00:00:00 cupsd -C /etc/cups/cupsd.conf  root 1591 1 0 Jul09 ? 00:00:00 /usr/sbin/acpid  68 1603 1 0 Jul09 ? 00:00:00 hald  root 1604 1603 0 Jul09 ? 00:00:00 hald-runner  root 1649 1604 0 Jul09 ? 00:00:00 hald-addon-input: Listening on /dev/input/event3 /dev/input/eve  68 1652 1604 0 Jul09 ? 00:00:00 hald-addon-acpi: listening on acpid socket /var/run/acpid.socke  root 1675 440 0 Jul09 ? 00:00:00 /sbin/udevd -d  root 1681 1 0 Jul09 ? 00:00:00 automount --pid-file /var/run/autofs.pid  root 1918 1 0 Jul09 ? 00:00:00 /usr/sbin/sshd  root 1955 1 0 Jul09 ? 00:00:00 /bin/sh /usr/bin/mysqld\_safe --datadir=/var/lib/mysql --socket=  mysql 2057 1955 0 Jul09 ? 00:00:11 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --u  root 2159 1 0 Jul09 ? 00:00:00 /usr/libexec/postfix/master  postfix 2164 2159 0 Jul09 ? 00:00:00 qmgr -l -t fifo -u  root 2173 1 0 Jul09 ? 00:00:00 /usr/sbin/abrtd  root 2199 1 0 Jul09 ? 00:00:03 /usr/sbin/httpd  root 2211 1 0 Jul09 ? 00:00:00 crond  root 2235 1 0 Jul09 ? 00:00:00 /usr/sbin/atd  root 2252 1 0 Jul09 ? 00:00:00 /usr/sbin/certmonger -S -p /var/run/certmonger.pid  root 2302 1 0 Jul09 ? 00:00:00 /usr/sbin/gdm-binary -nodaemon  root 2307 1 0 Jul09 tty2 00:00:00 /sbin/mingetty /dev/tty2  root 2311 1 0 Jul09 tty3 00:00:00 /sbin/mingetty /dev/tty3  root 2315 1 0 Jul09 tty4 00:00:00 /sbin/mingetty /dev/tty4  root 2317 440 0 Jul09 ? 00:00:00 /sbin/udevd -d  root 2318 1 0 Jul09 tty5 00:00:00 /sbin/mingetty /dev/tty5  root 2320 1 0 Jul09 tty6 00:00:00 /sbin/mingetty /dev/tty6  root 2338 2302 0 Jul09 ? 00:00:00 /usr/libexec/gdm-simple-slave --display-id /org/gnome/DisplayMa  root 2341 2338 0 Jul09 tty1 00:00:01 /usr/bin/Xorg :0 -br -verbose -audit 4 -auth /var/run/gdm/auth-  root 2365 1 0 Jul09 ? 00:00:00 /usr/sbin/console-kit-daemon --no-daemon  gdm 2435 1 0 Jul09 ? 00:00:00 /usr/bin/dbus-launch --exit-with-session  gdm 2436 1 0 Jul09 ? 00:00:00 /bin/dbus-daemon --fork --print-pid 5 --print-address 7 --sessi  gdm 2438 2338 0 Jul09 ? 00:00:00 /usr/bin/gnome-session --autostart=/usr/share/gdm/autostart/Log  root 2441 1 0 Jul09 ? 00:00:00 /usr/libexec/devkit-power-daemon  gdm 2446 1 0 Jul09 ? 00:00:00 /usr/libexec/gconfd-2  gdm 2463 2438 0 Jul09 ? 00:00:00 /usr/libexec/at-spi-registryd  gdm 2465 1 0 Jul09 ? 00:00:02 /usr/libexec/gnome-settings-daemon --gconf-prefix=/apps/gdm/sim  gdm 2467 1 0 Jul09 ? 00:00:00 /usr/libexec/bonobo-activation-server --ac-activate --ior-outpu  gdm 2474 1 0 Jul09 ? 00:00:00 /usr/libexec/gvfsd  gdm 2475 2438 0 Jul09 ? 00:00:00 metacity  gdm 2477 2438 0 Jul09 ? 00:00:01 /usr/libexec/gdm-simple-greeter  gdm 2480 2438 0 Jul09 ? 00:00:00 gnome-power-manager  gdm 2481 2438 0 Jul09 ? 00:00:00 /usr/libexec/polkit-gnome-authentication-agent-1  root 2485 1 0 Jul09 ? 00:00:00 /usr/libexec/polkit-1/polkitd  gdm 2489 1 0 Jul09 ? 00:00:00 /usr/bin/pulseaudio --start --log-target=syslog  rtkit 2491 1 0 Jul09 ? 00:00:00 /usr/libexec/rtkit-daemon  root 2499 2338 0 Jul09 ? 00:00:00 pam: gdm-password  apache 2834 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2835 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2836 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2837 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2838 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2839 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2840 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  apache 2841 2199 0 Jul09 ? 00:00:00 /usr/sbin/httpd  root 11632 1492 0 02:29 ? 00:00:00 /sbin/dhclient -d -4 -sf /usr/libexec/nm-dhcp-client.action -pf  postfix 14101 2159 0 03:59 ? 00:00:00 pickup -l -t fifo -u  root 14171 1918 0 04:19 ? 00:00:00 sshd: root@pts/0  root 14175 14171 0 04:19 pts/0 00:00:00 -bash  root 14275 14175 0 04:40 pts/0 00:00:00 ps -ef |

(기왕이면 메모장에 옮겨서 확인하기)

[kthreadd] 괄호 쳐져 있는 것은 시스템 데몬 : 분석 필요 없음 > 지워

UID : 어떤 계정으로 구동이 되었는지

PID : 프로그램이 구동된 순서 넘버링

CMD 에서 경로와 데몬을 구분하기

> /sbin/init : 경로 =/sbin/ , 데몬 = init

> auditd : 경로는 가려져 있음, 데몬 = auditd

> /sbin/rsyslogd -i /var/run/syslogd.pid -c 5 : 경로= /sbin/, 데몬 = rsyslogd

init : 커널 부팅 프로그램 또는 프로세스

APACHE 설치 > Demon Start > Port Open > Service Enable > OS 재시작 시 > Boot Loader > Device Info > Boot Partition > HAL Daemon > Run Level(INIT)

>(참고)HAL Daemon : Device 정보가 포함된 Deamon

OS 구성에 따른 로그

1. OS (SU로그/시스템로그)

2. OS + DBMS (SU로그/시스템로그) + DBMS-MySQL (mysqld.log/iddata\_logX.log)

mysqld\_safe > mysqld 동작 전에 데몬 정상여부판단

3. OS + WEB Server (SU로그/시스템로그) + WEB server-Apache(access\_log/errlr\_log)

4. OS + WAS (SU로그/시스템로그) + WAS Tomcat (access\_log/errlr\_log)

(r)syslog : RHEL 계열 서버 6.X 이하는 "syslog" 그 이상은 "rsyslog"

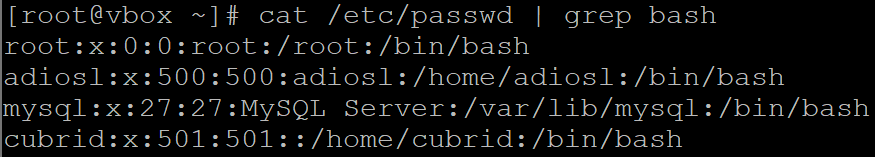
> 우리 테스트 시스템은 6.9버전임

> rsyslog.conf 파일 내 "/var/log/secure" su 로그가 저장되고 있고,

> 시스템 로그는 wtmp,utmp,lastlog,messages,cron,at

진단할 때 vi 등 편집기는 절대 사용하지 않음 > cat 만 사용함 > 마찬가지로 SELECT 만 사용

// 계정분석



id, 암호화된 password, uid,gid,desc, home dir, login status

\*\*/bin/bash : 로그인 가능

/sbin/nologin : 로그인 불가능

false : 로그인 불가능

> grep bash : 로그인 가능한 사용자 계정만 확인하기위해서

시스템 UID는 몇 번부터 몇 번까지 일까요? RHEL 6.x까지와 7.x이상의 범위가 다름

RHEL 6.x까지 : 0~499

RHEL 7.x이상 : 0~999

> OS를 구성하면서 자동적으로 생성된 계정

사용자 UID는

RHEL 6.x까지 : 500~

RHEL 7.x이상 : 1000~

그러면 로그인이 가능한 계정 수는 4개,시스템 UID는 2개, 사용자 UID는 2개

계정별 생성 사유는 위 정보만 봐서는 알 수 없음 > 인터뷰 대상

> 실제 진단 시에는 계정 갯수가 10개 이상 가는 경우가 많음

// 마무리

업로드 취약점 : 확장자 검증 필요 > 그러면 이중 확장자는? > Apache에 이중 확장자를 사용할 수 있는 기능이 있다

OWASP는 기본적으로 알고 다녀라

DNS

NAT

소규모 네트워크를 구성해봐라(VLAN,SUBNET,SWITCH,L4SWITCH)(Cisco packet tracer)

개인 프로젝트 추천

os+dbserver auth 등 기본 기능(공지사항,게시판등)

webserver front

wasserver tomcat>api

자격증 취득

정보처리기사,정보보안기사,

DVWA