목차

finger 서비스 비활성화

점검목적 Finger(사용자 정보 확인 서비스)를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회되는 것을 차단하고자 함 보안위협 비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 함

※ Finger(사용자 정보 확인 서비스): who 명령어가 현재 사용 중인 사용자들에 대한 간단한 정보만을 보여주는 데 반해 finger 명령은 옵션에 따른 시스템에 등록된 사용자뿐만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌

점검방법

rhel inetd일 경우

```
#cat /etc/inetd.conf
#finger stream tcp nowait bin /usr/lbin/fingered
```

fingerd 주석처리 확인

Step 1) /etc/inetd.conf 파일에서 finger 서비스 라인 #처리(주석처리)

```
 (수정 전) finger stream tcp nowait bin /usr/lbin/fingered fingerd
 (수정 후) #finger stream tcp nowait bin /usr/lbin/fingered fingerd
```

Step 2) inetd 서비스 재시작

```
#ps -ef | grep inetd
 root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP [PID]
```

rhel xinetd일 경우

```
#ls -alL /etc/xinetd.d/* | egrep "echo finger"
```

finger 서비스가 활성화 되어 있을 경우

Step 1) vi 편집기를 이용하여 /etc/xinetd.d/finger 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)

```
service finger
{
```

```
     socket_type = stream
     wait = no
     user = nobody
     server = /usr/sbin/in.fingerd
     disable = yes
}
```

Step 3) xinetd 서비스 재시작

```
 #service xinetd restart
```

Anonymous FTP 비활성화

점검목적 실행중인 FTP 서비스에 익명 FTP 접속이 허용되고 있는지 확인하여 접속허용을 차단하는 것을 목적으로 함

보안위협 Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 함

점검방법

일반 FTP

/etc/passwd 파일 내에 ftp 또는 anonymous 계정이 존재할 경우 삭제

```
#userdel ftp
```

ProFTP

conf/proftpd.conf파일의 anonymous 관련 설정 중 User, Useralias 항목 주석처리
(proftpd.conf 파일의 위치는 운영체제 종류별로 상이함)

```
<Anonymous ~ftp> <- Anonymous 설정 구간
 # User ftp <- anonymous로 사용되는 계정
 Group ftp
 # UserAlias anonymous ftp <- 별칭으로 사용되는 계정
</Anonymous>
```

vsFTP

vsFTP 설정파일(/etc/vsftpd/vsftpd.conf 또는, /etc/vsftpd.conf)에서

```
 anonymous_enable=NO 설정
```

참조링크 https://access.redhat.com/solutions/2048173

r 계열 서비스 비활성화

점검목적 r-command 사용을 통한 원격 접속은 NET Backup 또는 클러스터링 등 용도로 사용되기도 하나, 인증 없이 관리자 원격접속이 가능하여 이에 대한 보안위협을 방지하고자 함

보안위협 rsh, rlogin, rexec 등의 r command를 이용하여 원격에서 인증절차 없이 터미널 접속, 쉘 명령어를 실행이 가능함

점검방법 rsh, rlogin, rexec (shell, login, exec) 서비스 구동 확인

```
#ls -alL /etc/xinetd.d/* | egrep "rsh|rlogin|rexec" | egrep -v
"grep|klogin|kshell|kexec"
```

Step 1) vi 편집기를 이용하여 /etc/xinetd.d/ 디렉터리 내 rlogin, rsh, rexec 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정) • /etc/xinetd.d/rlogin 파일 • /etc/xinetd.d/rsh 파일 • /etc/xinetd.d/rexec 파일

```
service rlogin
{
   socket_type = stream
   wait = no
   user = nobody
   log_on_success += USERID
   log_on_failure += USERID
   server = /usr/sdin/in.fingerd
   disable = yes
}
```

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

r-command 사용시 보안설정($HOME/.rhosts, hosts.equiv 사용 금지 점검항목 참고) Step 1) r command 사용을 허용하는 호스트 및 계정 설정 - .rhosts, hosts.equiv 파일에 접근을 허용하는 hostname(IP) 명시 ※ IP 등록시 공인 IP 설정은 금지 - .rhosts, hosts.equiv 파일의 퍼미션을 600 이하로 설정 - 필요시 TCP_Wrapper를 이용하여 접근을 허용하는 IP를 등록하여 추가 보안 설정

rlogin, rshell, rexec 서비스는 backup, 클러스터링 등의 용도로 종종 사용되고 있으므로 해당 서비스 사용 유무를 확인하여 미사용시 서비스 중지 (/etc/hosts.equiv 또는 각 홈 디렉터리 밑에 있는 .rhosts 파일에 설정 유무를 확인하여 해당 서비스 사용여부 확인 - 파일이 존재하지 않거나 해당파일 내에 설정이 없다면 사용하지 않는 것으로 파악)

참조링크 https://access.redhat.com/solutions/7321

cron 파일 소유자 및 권한설정

점검목적 관리자외 cron 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 함

보안위협 root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음

점검방법

cron 관련 파일 /etc/crontab ← 예약작업을 등록하는 파일 /etc/cron.hourly ← 시간단위 실행 스크립트 등록 /etc/cron.daily ← 일단위 실행 스크립트 등록 /etc/cron.weekly ← 주단위 실행 스크립트 등록 /etc/cron.monthly ← 월 단위 실행 스크립트 등록 /etc/cron.allow ← crontab 명령어 허용 사용자 /etc/cron.deny ← crontab 명령어 차단 사용자

조치사항

Step 1) crontab 명령어 일반사용자 권한 삭제 (crontab 명령어 위치는 OS별 다를수 있음) ※ crontab 명령어는 SUID가 설정되어 있으므로 SUID 설정 제거

```
# ls -l /usr/bin/crontab
# chmod 750 /usr/bin/crontab
```

Step 2) cron 관련 설정파일 소유자 및 권한 설정

```
# chown root <cron 관련 파일>
# chmod 640 <cron 관련 파일>
```

■ crontab 명령어를 일반사용자에게 허용하는 경우 Step 1) `/etc/cron.d/cron.allow` 및 `/etc/cron.d/cron.deny` 파일의 소유자 및 권한 변경

```
#chown root /etc/cron.d/cron.allow
#chmod 640 /etc/cron.d/cron.allow
#chown root /etc/cron.d/cron.deny
#chmod 640 /etc/cron.d/cron.deny
```

Step 2) `/etc/cron.d/cron.allow` 및 `/etc/cron.d/cron.deny` 파일에 사용자 등록

```
# cat /etc/cron.allow (crontab 명령어 사용을 허용하는 사용자 등록)
# cat /etc/cron.deny (crontabl 명령어 사용을 차단하는 사용자 등록)
```

Dos 공격에 취약한 서비스 비활성화

점검목적 시스템 보안성을 높이기 위해 취약점이 많이 발표된 echo, discard, daytime, chargen, ntp, snmp 등 서비스를 중지함

보안위협 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있음

점검방법 LINUX (xinetd일 경우)

Step 1) vi 편집기를 이용하여 `/etc/xinetd.d/` 디렉터리 내 echo, discard, daytime, chargen 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정)

• `/etc/xinetd.d/echo` 파일(echo-dgram, echo-stream) • `/etc/xinetd.d/discard` 파일(discard-dgram, discard-stream) • `/etc/xinetd.d/daytime` 파일(daytime-dgram, daytime-stream) • `/etc/xinetd.d/chargen` 파일(chargen-dgram, chargen-stream)

```
service echo
{
   disable = yes
   id = echo-stream
   type = internal
   wait = no
   socket_type = stream
}
```

Step 3) xinetd 서비스 재시작

```
 #service xinetd restart
```

NFS 서비스 비활성화

점검목적 NFS 서비스는 한 서버의 파일을 많은 서비스 서버들이 공유하여 사용할 때 많이 이용되는 서비스이지만 이를 이용한 침해사고 위험성이 높으므로 사용하지 않는 경우 중지함

보안위협 NFS 서비스는 서버의 디스크를 클라이언트와 공유하는 서비스로 적정한 보안설정이 적용되어 있지 않다면 불필요한 파일 공유로 인한 유출위험이 있음

점검방법 NFS 서비스 데몬 확인 (NFS 동작 SID 확인)

```
#ps -ef | egrep "nfs|statd|lockd"
root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nfs/nfsd
```

Step 1) NFS 서비스 데몬 중지

```
#systemctl stop nfs
#systemctl disable nfs
#kill -9 [PID]
```

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경

```
1. 위치 확인
 #ls -al /etc/rc.d/rc*.d/* | grep nfs
2. 이름 변경
 #mv /etc/rc.d/rc2.d/S60nfs /etc/rc.d/rc2.d/_S60nfs
```

NFS 접근 통제

점검목적 접근권한이 없는 비인가자의 접근을 통제함

보안위협 접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있음

점검방법 불가피하게 NFS 서비스를 사용하여야 하는 경우 NFS 접근제어 파일에 꼭 필요한 공유 디렉터리만 나열하고, everyone으로 시스템이 마운트 되지 않도록 설정 /etc/exports 설정 예문

Step 1) /etc/exports 파일에 접근 가능한 호스트명 추가

```
(예) #/stand host1(또는 IP주소) host2
```

Step 2) 접속시 인증 및 클라이언트 권한 nobody 설정

```
 # vi /etc/export
 # /stand host1 (root_squash)
```

※ () 옵션에 인증되지 않은 엑세스를 허용하는 “insecure“ 구문 설정 금지

Step 3. NFS 서비스 재구동

```
 #/etc/exportfs –u
 #/etc/exportfs –a
```

automountd 제거

점검목적 로컬 공격자가 automountd 데몬에 RPC(Remote Procedure Call)를 보낼 수 있는 취약점이 존재하기 때문에 해당 서비스가 실행중일 경우 서비스를 중지시키기 위함

보안위협 파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있음

점검방법

```
automountd 서비스 데몬 확인
#ps -ef | grep automount(or autofs)
root 1131 1 0 jun 15 ? 32:11 /usr/sbin/automountd
Step 1) automountd 서비스 데몬 중지
 #kill -9 [PID]
Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경
 1. 위치 확인
 #ls -al /etc/rc.d/rc*.d/* | grep automount(or autofs)
 2. 이름 변경
 #mv /etc/rc.d/rc2.d/S28automountd /etc/rc.d/rc2.d/_S28automountd
```

RPC 서비스 확인

점검목적 다양한 취약성(버퍼 오버플로우, Dos, 원격실행 등)이 존재하는 RPC 서비스를 점검하여 해당 서비스를 비활성화 하도록 함

보안위협 버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 함

※ 불필요한 RPC 서비스: rpc.cmsd, rpc.ttdbserverd, sadmind, rusersd, walld, sprayd, rstatd, rpc.nisd, rexd, rpc.pcnfsd, rpc.statd, rpc.ypupdated, rpc.rquotad, kcms_server, cachefsd

점검방법

LINUX (inetd일 경우) Step 1) `/etc/inetd.conf` 파일에서 해당 라인 #처리(주석처리)

```
(수정 전) rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
(수정 후) #rpc.cmsd/2-4 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
```

Step 2) inetd 서비스 재시작

```
#ps -ef | grep inetd
root 141 1 0 15:03:22 ? 0:01 /usr/sbin/inetd -s
#kill -HUP 141
```

LINUX (xinetd일 경우) Step 1) vi 편집기를 이용하여 /etc/xinetd.d/ 디렉터리 내의 불필요한 RPC 서비스 파일 열기 Step 2) 아래와 같이 설정 (Disable = yes 설정)

```
service finger
{
   disable = yes
   socket_type = stream
   wait = no
- 이하 생략 -
}
```

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

NIS, NIS+ 점검

점검목적 안전하지 않은 NIS 서비스를 비활성화 하고 안전한 NIS+ 서비스를 활성화하여 시스템 보안수준을 향상하고자 함

보안위협 보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타시스템의 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보다 NIS+를 사용하는 것을 권장함

점검방법 NIS, NIS+ 서비스 구동 확인

```
#ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd |rpc.ypupdated”
root 3809 3721 0 08:44:40 ? 0:00 /usr/lib/nis/ypserv
```

Step 1) NFS 서비스 데몬 중지

```
#kill -9 [PID]
```

Step 2) 시동 스크립트 삭제 또는, 스크립트 이름 변경 1. 위치 확인

```
#ls -al /etc/rc.d/rc*.d/* | egrep
"ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated”
```

2. 이름 변경

```
#mv /etc/rc.d/rc2.d/S73ypbind /etc/rc.d/rc2.d/_S73ypbind
```

tftp, talk 서비스 비활성화

점검목적 안전하지 않거나 불필요한 서비스를 제거함으로써 시스템 보안성 및 리소스의 효율적 운용

보안위협 사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격 시도 가능

점검방법

Linux [inetd] 불필요한 서비스 데몬 확인

```
#cat /etc/inetd.conf | grep “tftp|talk|ntalk"
tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n
```

Step 1) vi 편집기를 이용하여 ”/etc/inetd.conf“ 파일 열기

```
#vi /etc/inetd.conf
```

Step 2) tftp, talk, ntalk 서비스 주석 처리

```
#tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd -n
#talk dgram udp wait root /usr/sbin/talkd talkd
#ntalk dgram udp wait root /usr/sbin/talkd talkd
```

Step 3) inetd 데몬 재시작

```
#kill -HUP [inetd pid]
```

Linux [xinetd] tftp, talk, ntalk 서비스 활성화 여부 확인

```
#vi /etc/xinetd.d/tftp
#vi /etc/xinetd.d/talk
#vi /etc/xinetd.d/ntalk
```

Step 1) vi 편집기를 이용하여 /etc/xinetd.d/ 디렉터리 내 tftp, talk, ntalk 파일 열기

Step 2) 아래와 같이 설정 (Disable = yes 설정) /etc/xinetd.d/tftp 파일 /etc/xinetd.d/talk 파일 /etc/xinetd.d/ntalk 파일

```
service tftp
{
   socket_type = dgram
   protocol = udp
   wait = yes
   user = root
   server = /usr/sbin/in.tftpd
   server_args = -s /tftpboot
   disable = yes
}
```

Step 3) xinetd 서비스 재시작

```
#service xinetd restart
```

Sendmail 버전 점검

점검목적 Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무 점검으로 최적화된 Sendmail 서비스의 운영

보안위협 취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있음

점검방법

1. Sendmail 서비스 실행 여부 점검

```
#ps -ef | grep sendmail
```

2. Sendmail 버전 점검

```
#telnet localhost 25
```

Sendmail 서비스 실행 여부 및 버전 점검 후, http://www.sendmail.org/ 또는, 각 OS 벤더사의 보안 패치

설치

스팸 메일 릴레이 제한

점검목적 스팸 메일 서버로의 악용방지 및 서버 과부하의 방지를 위함

보안위협 SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸 메일 서버로 사용하거나 Dos공격의 대상이 될 수 있음

점검방법 SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인

```
#ps -ef | grep sendmail | grep -v "grep"
#cat /etc/mail/sendmail.cf | grep "R$\*" | grep "Relaying denied"
R$* $#error $@ 5.7.1 $: "550 Relaying denied"
```

Step 1) vi 편집기를 이용하여 /etc/mail/sendmail.cf 또는 /etc/sendmail.cf설정파일 열기

Step 2) 아래와 같이 주석 제거

```
(수정 전) #R$* $#error $@ 5.7.1 $: "550 Relaying denied"
(수정 후) R$* $#error $@ 5.7.1 $: "550 Relaying denied"
```

Step 3) 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인 (없을시 파일생성)

```
 #cat /etc/mail/access
예)
 localhost.localdomain RELAY
 localhost RELAY
 127.0.0.1 RELAY
 spam.com REJECT
```

Step 4) 수정을 했거나 생성했을 경우 DB 파일 생성

```
 #makemap hash /etc/mail/access.db < /etc/mail/access
```

일반사용자의 Sendmail 실행 방지

점검목적 일반사용자의 q 옵션을 제한하여 Sendmail 설정 및 메일큐를 강제적으로 drop 시킬 수 없게 하여 비인가자에 의한 SMTP 서비스 오류 방지

보안위협 일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제적으로 drop

시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있음

점검방법 SMTP 서비스 사용 여부 및 restrictqrun 옵션 확인

```
#ps -ef | grep sendmail | grep -v "grep"
#grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions
```

Step 1) vi 편집기를 이용하여 /etc/mail/sendmail.cf 설정파일 열기

Step 2) O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가

```
(수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn
(수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun
```

Step 3. Sendmail 서비스 재시작

DNS 보안 버전 패치

점검목적 취약점이 발표되지 않은 BIND 버전의 사용을 목적으로 함 보안위협 최신버전(2016.01 기준 9.10.3-P2) 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재함 점검방법 DNS 서비스 사용 및 BIND 버전 확인 #ps -ef | grep named named -v

“DNS” 서비스를 사용하지 않는 경우 서비스 중지 “DNS” 서비스 사용 시 BIND 버전 확인 후 아래의 보안 설정방법에 따라 최신 버전으로 업데이트

DNS Zone Transfer 설정

점검목적 허가되지 않는 사용자에게 Zone Transfer를 제한함으로써 호스트 정보, 시스템 정보 등 정보 유출의 방지를 목적으로 함 보안위협 비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있음 점검방법 DNS 서비스 사용 시 /etc/named.conf 파일의 allow-transfer 및 xfrnets 확인 #ps -ef | grep named | grep -v “grep” #cat /etc/named.conf | grep 'allow-transfer' #cat /etc/named.boot | grep “xfrnets” < DNS 서비스를 사용하지 않는 경우 > DNS 서비스 데몬 확인 (DNS 동작 SID 확인) #ps -ef | grep named root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/in.named “DNS” 서비스를 사용하지 않는 경우 서비스 데몬 중지 #kill -9 [PID]

웹서비스 디렉토리 리스팅 제거

점검목적 외부에서 디렉터리 내의 모든 파일에 대한 접근 및 열람을 제한함을 목적으로 함 보안위협 디렉터리 검색 기능이 활성화 되어 있을 경우, 사용자에게 디렉터리내 파일이 표시되어 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일, 공개되어서는 안되는 파일 등이 노출 가능함 점검방법 Indexes 옵션 사용 여부 확인 #vi /[Apache_home]/conf/httpd.conf Options Indexes FollowSymLinks 위에 제시한 파일에 “Indexes” 옵션이 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경 Step 1) vi 편집기를

이용하여 /[Apache_home]/conf/httpd.conf 파일 열기 #vi /[Apache_home]/conf/httpd.conf Step 2) 설정된 모든 디렉터리의 Options 지시자에서 Indexes 옵션 제거 (수정 전) Option 지시자에 Indexes 옵션이 설정되어 있음 <Directory /> Options Indexes FollowSymLinks AllowOverride None Order allow, deny Allow from all </Directory> (수정 후) Option 지시자에 Indexes 삭제 또는 -Indexes 변경 후 저장 <Directory /> Options Indexes 삭제 (또는 -Indexes) AllowOverride None Order allow, deny Allow from all </Directory>

웹서비스 웹 프로세스 권한 제한

점검목적 Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 구동함으로써 침해사고 발생 시 피해범위 확산 방지를 목적으로 함 보안위협 웹서비스 데몬을 root 권한으로 실행시 웹서비스가 파일을 생성, 수정하는 과정에서 웹서비스에 해당하지 않는 파일도 root 권한에 의해 쓰기가 가능하며 해킹 발생 시 root 권한이 노출 될 수 있음 점검방법 Apache 데몬 구동 권한(User 및 Group) 확인 #vi /[Apache_home]/conf/httpd.conf User [root가 아닌 별도 계정명] Group [root가 아닌 별도 계정명] 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) 데몬 User & Group 변경 User & Group 부분에 root가 아닌 별도 계정으로 변경 ※ 웹서비스 실행 계정은 로그인이 불가능하도록 쉘 제한 필수 User [root가 아닌 별도 계정명] Group [root가 아닌 별도 계정명] Step 2) Apache 서비스 재시작

웹서비스 상위 디렉토리 접근 금지

점검목적 상위 경로 이동 명령으로 비인가자의 특정 디렉터리에 대한 접근 및 열람을 제한하여 중요 파일 및 데이터 보호를 목적으로 함 보안위협 상위 경로로 이동하는 것이 가능할 경우 접근하고자 하는 디렉터리의 하위경로에 접속하여 상위경로로 이동함으로써 악의적인 목적을 가진 사용자의 접근이 가능함 점검방법 AllowOverride 지시자 Authconfig 옵션 확인 #vi /[Apache_home]/conf/httpd.conf AllowOverride None “AllowOverride” 옵션이 “None”으로 설정된 경우 아래의 보안설정방법에 따라 옵션 설정 변경 Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기 #vi /[Apache_home]/conf/httpd.conf Step 2) 설정된 모든 디렉터리의 AllowOverride 지시자에서 AuthConfig 옵션 설정 (수정 전) AllowOverride 지시자에 None 옵션이 설정되어 있음 <Directory “/usr/local/apache2/htdocs”> AllowOverride None Allow from all </Directory> (수정 후) AllowOverride 지시자에 AuthConfig 옵션이 설정되어 있음 <Directory “/usr/local/apache2/htdocs”> AllowOverride AuthConfig Allow from all </Directory> Step 3) 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성 (아래 내용 삽입) AuthName “디렉터리 사용자 인증” AuthType Basic AuthUserFile /usr/local/apache/test/.auth Require valid-user 지시자 설명 AuthName 인증 영역(웹 브라우저의 인증창에 표시되는 문구) AuthType 인증 형태(Basic 또는, Digest) AuthUserFile 사용자 정보(아이디 및 패스워드) 저장 파일 위치 AuthGroupFile 그룹 파일의 위치(옵션) Require 접근을 허용할 사용자 또는, 그룹 정의 Step 4) 사용자 인증에 사용할 아이디 및 패스워드 생성 htpasswd -c /usr/local/apache/test/.auth test New password: Re-type new password: Adding password for user test [root@localhost apache]# Step 5) 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작

웹서비스 불필요한 파일 제거

점검목적 Apache 설치 시 디폴트로 설치되는 불필요한 파일을 제거함을 목적으로 함 보안위협 Apache 설치 시 htdocs 디렉터리 내에 매뉴얼 파일은 시스템 관련정보를 노출하거나 해킹에 악용될 수 있음 점검방법 불필요한 파일 및 디렉터리 존재 여부 확인 #ls -ld /[Apache_home]/htdocs/manual #ls -ld /[Apache_home]/manual 위에 제시한 불필요한 파일 및 디렉터리가 존재하는 경우 아래의 보안설정방법에 따라 불필요한 파일 및 디렉터리 제거 또는, 설정을 변경함 Step 1) #ls 명령어로 확인된 매뉴얼 디렉터리 및 파일 제거 #rm -rf /[Apache_home]/htdocs/manual #rm -rf /[Apache_home]/manual Step 2)

#ls 명령어로 정상적인 제거 확인 #ls -ld /[Apache_home]/htdocs/manual #ls –ld /[Apache_home]/manual Step 3) 추가적으로 웹서비스 운영에 불필요한 파일이나 디렉터리가 있을 시 제거

웹서비스 링크 사용 금지

점검목적 무분별한 심볼릭 링크, aliases 사용제한으로 시스템 권한의 탈취 방지를 목적으로 함 보안위협 웹 루트 폴더(DocumentRoot)에 root 디렉터리(/)를 링크하는 파일이 있으며 디렉터리 인덱싱 기능이 차단되어 있어도 root 디렉터리 열람이 가능함 점검방법 Options 지시자 FollowSymLinks 옵션 제거 여부 확인 #vi /[Apache_home]/conf/httpd.conf Options Indexes FollowSymLinks 위에 제시한 옵션이 적용되어 있는 경우 아래의 보안설정방법에 따라 옵션을 제거함 Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기 #vi /[Apache_home]/conf/httpd.conf Step 2) 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거 (수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음 <Directory /> Options Indexes FollowSymLinks AllowOverride None Order allow, deny Allow from all </Directory> (수정 후) Options 지시자에 FollowSymLinks 삭제 또는 -FollowSymLinks 변경 후 저장 <Directory /> Options FollowSymLinks 삭제 또는 -FollowSymLinks AllowOverride None Order allow, deny Allow from all </Directory>

웹서비스 파일 업로드 및 다운로드 제한

점검목적 기반시설 특성상 원칙적으로 파일 업로드 및 다운로드를 금지하고 있지만 불가피하게 필요시 용량 사이즈를 제한함으로써 불필요한 업로드와 다운로드를 방지해 서버의 과부하 예방 및 자원을 효율적으로 관리하기 위함 보안위협 악의적 목적을 가진 사용자가 반복 업로드 및 웹 쉘 공격 등으로 시스템 권한을 탈취하거나 대용량 파일의 반복 업로드로 서버자원을 고갈시키는 공격의 위험이 있음 점검방법 LimitRequestBody 파일 사이즈 용량 제한 설정 여부 확인 #vi /[Apache_home]/conf/httpd.conf LimitRequestBody 5000000 (※ 업로드 및 다운로드 파일이 5M를 넘지 않도록 설정 권고함) 위에 제시한 설정이 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기 #vi /[Apache_home]/conf/httpd.conf Step 2) 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정 예) <Directory /> LimitRequestBody 5000000 (※ “/” 는 모든 파일 사이즈를 5M로 제한하는 설정 단위:byte) </Directory>

웹서비스 영역의 분리

점검목적 웹 서비스 영역과 시스템 영역을 분리시켜서 웹 서비스의 침해가 시스템 영역으로 확장될 가능성을 최소화하기 위함 보안위협 웹 서버의 루트 디렉터리와 OS의 루트 디렉터리를 다르게 지정하지 않았을 경우, 비인가자가 웹 서비스를 통해 해킹이 성공할 경우 시스템 영역까지 접근이 가능하여 피해가 확장될 수 있음 점검방법 DocumentRoot의 별도 디렉터리 지정 여부 확인 #vi /[Apache_home]/conf/httpd.conf DocumentRoot ”/usr/local/apache/htdocs“ 또는 DocumentRoot ”/usr/local/apache2/htdocs“ 또는 DocumentRoot ”/var/www/html“ DocumentRoot가 별도의 디렉터리로 지정되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일 열기 #vi /[Apache_home]/conf/httpd.conf Step 2) DocumentRoot 설정 부분에 “/usr/local/apache/htdocs”, ”/usr/local/apache2/htdocs“, ”/var/www/html“ 셋 중 하나가 아닌 별도의 디렉터리로 변경 DocumentRoot “디렉터리 ”

ssh 원격접속 허용

점검목적 비교적 안전한 SSH 프로토콜을 사용함으로써 스니핑 등 아이디/패스워드의 누출의 방지를 목적으로 함 보안위협 원격 접속 시 Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기 때문에 아이디/패스워드 및 중요 정보가 외부로 유출될 위험성이 있음 점검방법 Step 1) SSH 서비스 활성화 명령어 실행 #service start sshd 또는, #service start ssh Step 2) SSH 설치가 필요할 경우 각 OS 벤더사로부터 SSH 서비스 설치 방법을 문의한 후 서버에 설치

ftp 서비스 확인

점검목적 취약한 서비스인 FTP서비스를 가급적 제한함을 목적으로 함 보안위협 FTP 서비스는 통신구간이 평문으로 전송되어 계정정보(아이디, 패스워드) 및 전송 데이터의 스니핑이 가능함 점검방법 일반 ftp 서비스 비활성화 여부 확인 #ps -ef | grep ftp vsftpd 또는 ProFTP 서비스 데몬 확인(vsftpd, proftpd 동작 SID 확인) #ps -ef | egrep “vsftpd|proftp” root 3809 3721 0 08:44:40 ? 0:00 /usr/sbin/vsftpd 불필요한 “ftp” 서비스 실행 시 아래의 보안설정방법에 따라 서비스 중지 vsftpd 또는 ProFTP 서비스 데몬 중지 # service vsftpd(proftp) stop 또는 /etc/rc.d/init.d/vsftpd(proftp) stop 또는 kill -9 [PID]

ftp 계정 shell 제한

점검목적 FTP 서비스 설치 시 기본으로 생성되는 ftp 계정은 로그인이 필요하지 않은 계정으로 쉘을 제한하여 해당 계정으로의 시스템 접근을 차단하기 위함 보안위협 불필요한 기본 계정에 쉘(Shell)을 부여할 경우, 공격자에게 해당 계정이 노출되어 ftp 기본 계정으로 시스템 접근하여 공격이 가능해짐 점검방법 ftp 계정에 대한 /bin/false 부여 확인 #cat /etc/passwd ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash “passwd” 파일 내 로그인 쉘 설정이 “/bin/false”가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) vi 편집기를 이용하여 “/etc/passwd” 파일 열기 Step 2) ftp 계정의 로그인 쉘 부분인 계정 맨 마지막에 /bin/false 부여 및 변경 (수정 전) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/sbin/bash (수정 후) ftp:x:500:100:Anonymous FTP USER:/var/ftp:/bin/false Step 3) # usermod –s /bin/false [계정ID] 부여로 변경 가능 * Step 2 로 적용이 되지 않을 경우는 Step3의 usermod 명령어를 사용하여 쉘 변경

Ftpusers 파일 소유자 및 권한 설정

점검목적 비인가자들의 ftp 접속을 차단하기 위해 ftpusers 파일 소유자 및 권한을 관리해야함 보안위협 ftpusers 파일에 인가되지 않은 사용자를 등록하여 해당 계정을 이용, 불법적인 FTP 서비스에 접근이 가능함 점검방법 ftpusers 파일에 대한 일반사용자 쓰기권한 확인 #ls -al /etc/ftpusers #ls -al /etc/ftpd/ftpusers rw-r—– root <ftpusers 파일> “ftpusers“ 파일의 소유자가 root가 아니거나 파일의 권한이 640 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 FTP 종류 별 ftpusers 파일 위치 기본 FTP /etc/ftpusers 또는, /etc/ftpd/ftpusers ProFTP /etc/ftpusers 또는, /etc/ftpd/ftpusers vsFTP /etc/vsftpd/ftpusers, /etc/vsftpd/user_list 또는, /etc/vsftpd.ftpusers, /etc/vsftpd.user_list Step 1) “/etc/ftpusers” 파일의 소유자 및 권한 확인 #ls -l /etc/ftpusers Step 2) “/etc/ftpusers” 파일의 소유자 및 권한 변경 (소유자 root, 권한 640) #chown root /etc/ftpusers #chmod 640 /etc/ftpusers ※ vsFTP를 사용할 경우 FTP 접근제어 파일 (1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.user_list 또는 ftpusers, user_list 파일의 소유자 및 권한 확인 후 변경 (ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨) (2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers 또는 ftpusers 파일의 소유자 및 권한 확인 후 변경 (ftpusers 파일에 등록된 계정들만 접속이 차단됨)

Ftpusers 파일 설정

점검목적 root의 FTP 직접 접속을 방지하여 root 패스워드 정보를 노출되지 않도록 하기 위함 보안위협 FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑에 의해서 관리자 계정의 아이디 및 패스워드가 노출될 수 있음 점검방법 아래 파일에서 ftp에 대한 root 계정으로의 접속 가능 여부 확인 #cat /etc/ftpusers #cat /etc/ftpd/ftpusers #root (주석처리) 또는, root 계정 미등록 ProFTP #cat /etc/proftpd.conf RootLogin on vsFTP #cat /etc/vsftp/ftpusers #cat /etc/vsftp/user_list 또는 #cat /etc/vsftpd.ftpusers #cat /etc/vsftpd.user_list #root (주석처리) 또는, root 계정 미등록 root 계정으로 FTP 접속이 가능하도록 위와 같이 설정된 경우 아래의 보안설정방법에 따라 설정을 변경함 < 일반 FTP 서비스 root 계정 접속 제한 방법 > Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/ftpusers” 또는 “/etc/ftpd/ftpusers”) #vi /etc/ftpusers 또는 /etc/ftpd/ftpusers Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root < ProFTP 서비스 ROOT 접속 차단 > Step 1) vi 편집기를 이용하여 proftpd 설정파일(“/etc/proftpd.conf”) 열기 #vi /etc/proftpd.conf Step 2) proftpd 설정파일 (“/etc/proftpd.conf”)에서 RootLogin off 설정 (수정 전) RootLogin on (수정 후) RootLogin off Step 3) ProFTP 서비스 재시작 < vsFTP 서비스 ROOT 접속 차단 > Step 1) vi 편집기를 이용하여 ftpusers 파일 열기 (“/etc/vsftp/ftpusers” 또는, “/etc/vsftpd.ftpusers”) #vi /etc/vsftp/ftpusers Step 2) ftpusers 파일에 root 계정 추가 또는, 주석제거 (수정 전) #root 또는, root 계정 미등록 (수정 후) root Step 3) vsFTP 서비스 재시작 ※ vsFTP를 사용할 경우 FTP 접근제어 파일 (1) vsftpd.conf 파일에서 userlist_enable=YES인 경우: vsftpd.ftpusers, vsftpd.user_list 또는 ftpusers, user_list (ftpusers, user_list 파일에 등록된 모든 계정의 접속이 차단됨) (2) vsftpd.conf 파일에서 userlist_enable=NO 또는, 옵션 설정이 없는 경우: vsftpd.ftpusers 또는 ftpusers (ftpusers 파일에 등록된 계정들만 접속이 차단됨)

at 파일 소유자 및 권한 설정

점검목적 관리자외 at 서비스를 사용할 수 없도록 설정하고 있는지 점검하는 것을 목적으로 함 보안위협 root 외 일반사용자에게도 at 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있음 점검방법 /etc/at.allow ← at 명령어 허용 사용자 /etc/at.deny ← at 명령어 차단 사용자 “cron” 접근제어 설정이 적절하지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) at 명령어 일반사용자 권한 삭제 (at 명령어 위치는 OS별 다를수 있음) ※ at 명령어는 SUID가 설정되어 있으므로 SUID 설정 제거 # ls -l /usr/bin/at # chmod 4750 /usr/bin/at Step 2) cron 관련 설정파일 소유자 및 권한 설정 # chown root <at 관련 파일> # chmod 640 <at 관련 파일> ■ at 명령어를 일반사용자에게 허용하는 경우 Step 1) “/etc/cron.d/at.allow” 및 “/etc/cron.d/at.deny” 파일의 소유자 및 권한 변경 #chown root /etc/cron.d/at.allow #chmod 640 /etc/cron.d/at.allow #chown root /etc/cron.d/at.deny #chmod 640 /etc/cron.d/at.deny Step 2) “/etc/cron.d/at.allow” 및 “/etc/cron.d/at.deny” 파일에 사용자 등록 # cat /etc/at.allow (at 명령어 사용을 허용하는 사용자 등록) # cat /etc/at.deny (at 명령어 사용을 차단하는 사용자 등록)

SNMP 서비스 구동 점검

점검목적 불필요한 SNMP 서비스 활성화로 인해 필요 이상의 정보가 노출되는 것을 막기 위해 SNMP 서비스를 중지해야함 보안위협 SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법수정이 발생할 수 있음 점검방법 Step 1) ps –ef | grep snmp로 검색 root 2028 1 0 Nov 24 ? 0:00 /usr/sbin/snmpdm Step 2) snmp 사용하지 않을 시 서비스 중지 #service snmpd stop

SNMP 서비스 커뮤니티스트링의 복잡성 설정

점검목적 Community String 기본 설정인 Public, Private는 공개된 내용으로 공격자가 이를 이용하여 SNMP 서비스를 통해 시스템 정보를 얻을 수 있기 때문에 Community String을 유추하지 못하도록 설정해야함 보안위협 Community String은 Default로 public, private로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 환경설정 파일 열람 및 수정을 통한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 Dos공격까지 다양한 형태의 공격이 가능함 점검방법 #vi /etc/snmp/snmpd.conf com2sec notConfigUser default public 위의 설정과 같이 디폴트 커뮤니티명인 “public” 또는, ”private“을 사용하는 경우 아래의 보안설정방법에 따라 설정을 변경함 Step 1) vi 편집기를 이용하여 SNMP 설정파일 열기 #vi /etc/snmp/snmpd.conf Step 2) Community String 값 설정 변경 (추측하기 어려운 값으로 설정) (수정 전) com2sec notConfigUser default public (수정 후) com2sec notConfigUser default <변경 값> Step 3) 서비스 재구동 # service snmpd rstart

로그온 시 경고 메시지 제공

점검목적 비인가자들에게 서버에 대한 불필요한 정보를 제공하지 않고, 서버 접속 시관계자만 접속해야 한다는 경각심을 심어 주기위해 경고 메시지 설정이 필요함 보안위협 로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음 점검방법 Step 1) 서버 로그온 메시지 설정: vi 편집기로 ”/etc/motd“ 파일을 연 후 로그온 메시지 입력 #vi /etc/motd 경고 메시지 입력 Step 2) Telnet 배너 설정: vi 편집기로 ”/etc/issue.net“ 파일을 연 후 로그온 메시지 입력 #vi /etc/issue.net 경고 메시지 입력 Step 3) FTP 배너 설정: vi 편집기로 ”/etc/vsftpd/vsftpd.conf“ 파일을 연 후 로그인 메시지 입력 #vi /etc/vsftpd/vsftpd.conf ftpd_banner=“경고 메시지 입력” Step 4) SMTP 배너 설정: vi 편집기로 ”/etc/mail/sendmail.cf“ 파일을 연 후 로그인 메시지 입력 #vi /etc/mail/sendmail.cf O Smtp GreetingMessage=“경고 메시지 입력” Step 5) DNS 배너 설정: vi 편집기로 ”/etc/named.conf“ 파일을 연 후 로그인 메시지 입력 #vi /etc/named.conf 경고 메시지 입력

NFS 설정파일 접근 제한

점검목적 비인가자에 의한 불법적인 외부 시스템 마운트를 차단하기 위해 NFS 접근제어 파일의 소유자 및 파일 권한을 설정 보안위협 NFS 접근제어 설정파일에 대한 권한 관리가 이루어지지 않을 시 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있음 점검방법 #ls -al /etc/exports rw-r–r– root <nfs 접근제어 파일> “NFS” 접근제어 설정파일의 소유자가 root가 아니거나 파일의 권한이 644 이하가 아닌 경우 아래의 보안설정방법에 따라 설정을 변경함 “/etc/exports” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644) #chown root /etc/exports #chmod 644 /etc/exports

expn, vrfy 명령어 제한

점검목적 SMTP 서비스의 expn, vrfy 명령을 통한 정보 유출을 막기 위하여 두 명령어를 사용하지 못하게 옵션을 설정해야함 보안위협 VRFY, EXPN 명령어를 통하여 특정 사용자 계정의 존재유무를 알 수 있고, 사용자의 정보를 외부로 유출 할 수 있음 점검방법 noexpn, novrfy 옵션 설정 확인 #vi /etc/mail/sendmail.cf O PrivacyOptions= (noexpn, novrfy 또는 goaway 옵션 설정 여부) ※ goaway 옵션 : authwarnings, noexpn, novrfy, noverb, needmailhelo, needexpnhelo, needvrfyhelo, nobodyreturn 통합하는 단축 옵션 <서비스 필요 시> Step 1) vi 편집기를 이용하여 “/etc/mail/sendmail.cf” 파일을 연 후 (단, AIX는 /etc/sendmail.cf) #vi /etc/mail/sendmail.cf Step 2) “/etc/mail/sendmail.cf” 파일에 noexpn, novrfy 옵션 추가 (수정 전) O PrivacyOptions=authwarnings (수정 후) O PrivacyOptions=authwarnings, noexpn, novrfy 또는 goaway Step 3) SMTP 서비스 재시작 < 서비스 불

필요 시> Step 1) 실행중인 서비스 중지 #ps –ef | grep sendmail root 441 1 0 Sep19 ? 00:00:00 sendmail: accepting connections #kill -9 [PID] Step 2) 시스템 재시작 시 SMTP 서버가 시작되지 않도록 OS별로 아래와 같이 설정함 1. 위치 확인 #ls –al /etc/rc*.d/* | grep sendmail 2. 이름 변경 #mv /etc/rc2.d/S88sendmail /etc/rc2.d/_S88sendmail

Apache 웹 서비스 정보 숨김

점검목적 HTTP 헤더, 에러페이지에서 웹 서버 버전 및 종류, OS 정보 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위함 보안위협 불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수집할 수 있음 점검방법 ServerTokens, ServerSignature 옵션 설정 여부 확인 # vi /[Apache_Home]/conf/httpd.conf ServerTokens Prod ServerSignature off “httpd.conf” 파일 내에 ServerTokens, ServerSignature 지시자가 위와 같이 설정되어 있지 않은 경우 아래의 보안설정방법에 따라 옵션 추가 Step 1) vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후 #vi /[Apache_home]/conf/httpd.conf Step 2) 설정된 모든 디렉터리의 ServerTokens 지시자에서 Prod 옵션 설정 및 ServerSignature Off 지시자에 Off 옵션 설정 (없으면 신규 삽입) <Directory /> Options Indexes FollowSymlinks ServerTokens Prod ServerSignature Off - 이하 생략- </Directory> ServerTokens 지시자 옵션 키워드 제공하는 정보 예문 Prod 웹 서버 종류 Apache Min 웹 서버 버전 Apache/2.2.3 OS 웹 서버 버전 + 운영체제 Apache/2.2.3 (CentOS) (기본값) Full 웹 서버의 모든 정보 Apache/2.2.3 (CentOS) DAV/2 PHP/5.16