
RedHat
취약점 진단
김용학

INDEX

1
개요

1. Red Hat 7.0 서버 취약점 점검은 Default로 설정된 Red Hat 7.0 서버의 실질적인 진단과 보고서 작성

2. 실무에서 활용될 수 있는 추가적인 경험을 목표로 하며 이를 통하여 Linux 취약점 점검에 대한 최종교육 결과산출 및 종합적인 이해도를 고취시키는데 목적을 둡니다.

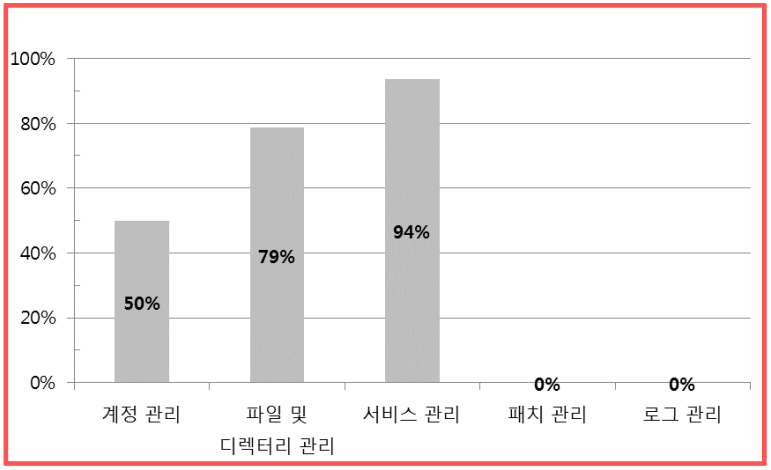
1-2 점검항목 및 점검대상

구분		점검항목	점검대상
기술적 점검	RedHat 서버	5개 분야 43개 점검 항목	1
합계		43개 점검 항목	1

1 개요

No	호스트명	OS	용도	비고
1	Localhost	RedHat 7.0	실습용	192.168.52.130

2-1 총평



분류	항목 통계						점검 점수		
	전체	점검	양호	취약	부분 만족	해당없음	전체	평가	수준
계정 관리	4	4	2	2	0	0	40	20	50%
파일 및 디렉터리 관리	14	14	11	3	0	0	140	30	79%
서비스 관리	23	16	15	1	0	7	160	10	94%
패치 관리	1	1	0	1	0	0	10	10	0%
로그 관리	1	1	0	1	0	0	10	10	0%
전체 보안 수준	43	36	28	8	0	7	360	80	78%

2 취약점 진단결과

U-02 패스워드 복잡성 설정

수정 전

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        sufficient    /lib/security/pam_unix.so likeauth nullok md5 shadow
auth        required      /lib/security/pam_deny.so
account     sufficient    /lib/security/pam_unix.so
account     required      /lib/security/pam_deny.so
password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shado
w
password    required      /lib/security/pam_deny.so
session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
```

수정 내용

- 모든 계정 암호 유추가 쉬운 경우
- 비인가자의 시스템 접근이 허용 될 가능성 up
- Pw는 영문, 숫자, 특수 문자를 혼합하여 설정

조치 결과

```
[root@localhost /root]# passwd
New UNIX password:
BAD PASSWORD: it's WAY too short
Retype new UNIX password:
Sorry, passwords do not match
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
[root@localhost /root]# _
```

2 취약점 진단결과

2-2 취약점 조치결과

U-03 계정 잠금 임계값 설정

수정 전

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        sufficient    /lib/security/pam_unix.so likeauth nullok md5 shadow
auth        required      /lib/security/pam_deny.so
account     sufficient    /lib/security/pam_unix.so
account     required      /lib/security/pam_deny.so
password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok md5 shado
w
password    required      /lib/security/pam_deny.so
session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
```

수정 내용

해당 값 설정 옵션 deny 설정 돼어있지 않아 취약

auth required pam_tally.so deny=5 unlock_time=120 no_magic_root

account required pam_tally.so no_magic_root reset

조치 결과

```
[root@localhost /]# su test
[test@localhost /]$ su test2
Password:
su: incorrect password
[test@localhost /]$ su test2
Password:
su: incorrect password
[test@localhost /]$ su test2
Password:
su: incorrect password
[test@localhost /]$ su test2
Password:
su: incorrect password
[test@localhost /]$ su test2
Password:
su: incorrect password
[test@localhost /]$ su test2
Password:
su: incorrect password
```

2-2 취약점 조치결과

U-19 /etc/shadow 파일 소유자 및 권한 설정

수정 전

```
[root@localhost /]# ls -l /etc/shadow
-rw-------    1 root     root          632 Aug  6 17:39 /etc/shadow
[root@localhost /]#
```

수정 내용

수정 전 root 권한 600 → 관리자만이 제어할 수 있도록 root 권한 재 설정 → 수정 후 root 권한 400

조치 결과

```
[root@localhost /etc]# ls -al shadow
----------    1 root     root          775 Jan  3 11:32 shadow
[root@localhost /etc]#
```

2-2 취약점 조치결과

U-20 /etc/host 파일 소유자 및 권한 설정

수정 전

```
[root@localhost /root]# ls -l /etc/hosts
-rw-r--r--    1 root     root           49 Aug  7 02:22 /etc/hosts
[root@localhost /root]#
```

수정 내용

수정 전 root 권한 644 → 관리자만이 제어할 수 있도록 root 권한 재 설정 → 수정 후 root 권한 600

조치 결과

```
[root@localhost /etc]# ls -al hosts
-rw-------    1 root     root           48 Jan  3  2019 hosts
[root@localhost /etc]#
```

2-2 취약점 조치결과

U-21 /etc/(x)inetd.conf 파일 소유자 및 권한 설정

수정 전

```
[root@localhost /]# ls -al /etc/xinetd.d/*
-rw-r--r--    1 root     root          344 Aug 24  2000 /etc/xinetd.d/linuxconf-
web
[root@localhost /]#
```

수정 내용

수정 전 root 권한 644 → 관리자만이 제어할 수 있도록 root 권한 재 설정 → 수정 후 root 권한 600

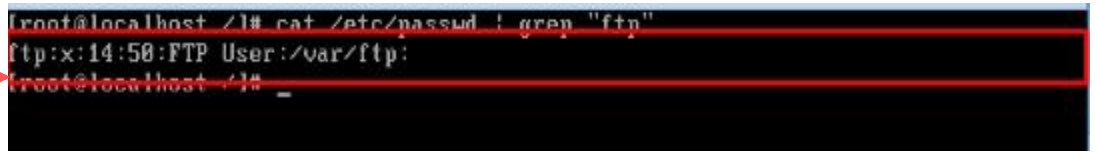
조치 결과

```
[root@localhost xinetd.d]# ls -l
total 4
-rw-------    1 root     root          344 Aug 24  2000 linuxconf-web
```

2-2 취약점 조치결과

U-37 Anonymous FTP 비활성화

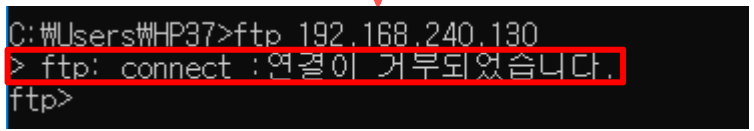
수정 전



수정 내용

- FTP 서비스가 존재하여 Anonymous FTP 접속 가능
- 관리자만이 제어할 수 있도록 root 권한 재 설정
- 수정 후 root 권한 600

조치 결과



2 취약점 진단결과

2-2 취약점 조치결과

U-71 최신 보안패치 및 벤더 권고사항 적용

수정 전 → 악의적인 사용자가 알려진 취약점의 공격 기법을 통해 서버 장악 가능

수정 내용, **조치 결과** → OS 관리자, 서비스 개발자의 패치적용 → 서비스 영향 정도 정확히 파악 → 주기적인 패치 적용 정책 수립 및 적용

2-2 취약점 조치결과

U-72 로그의 정기적인 검토

수정 전

시스템의 로그를 정기적으로 검토하고 보안담당자에게
보고되는 시스템이 구축되어 있지 않음.

수정 내용

조치 결과

정기적인 로그 검토 및 분석 주기 수립

로그 분석에 대한 결과 보고서 작성

로그 분석 결과보고서 보고 체계 수립

Question and Answer

서비스들이 설치되어 있지 않아 취약점 진단을 못함.

서비스 설치를 시도

Yum, apt, wget 등 패키지 관리자 없음.
공유 폴더 설정을 위한 vmware 업데이트 실패.

서비스 설치 및 실행 실패

다양한 서버스 환경에 대응하지 못함.


Thank you