**\*과목명: 시스템 네트워크 보안 기술**

|  |
| --- |
|  |
|  |
| 문제 상황 |
| 서버 로그 분석으로 시스템에 접속한 또는 접속하고자 했던 사용자들의 정보를 파악한다. |
| 학습목표 |
| 목적에 맞는 적절한 명령어들을 통해 관리자가 확인하고자 하는 로그들을 확인할 수 있다. |
| 문제 정의 및 요구사항 |
| 다음은 리눅스 시스템의 로그 파일에 관한 문제들이다.  1) 빈 칸에 들어갈 명령어들을 확인한다.  - 명령어들을 통해 점검할 수 있는 로그 내용의 차이점을 써라.  텍스트, 스크린샷, 폰트이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다.  2) 다음은 리눅스 시스템에서 로그 명령어를 실행했을 때의 결과이다.  설정 상 어떠한 취약점이 있는지 두 가지를 써라.  블랙, 어둠이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다. |
| 문제 해결 가이드 |
| 1. 로그 파일 utmp, wtmp, btmp 파일 내용의 차이점을 확인한다. 2. USER, TTY, IDLE 필드 값들을 중심으로 해당 취약점을 확인한다. |
| 제출 방법 및 평가 기준 |
| <<제출방법>>  ·파일명 : 본인이름.pdf  ·실행 과정 및 결과 화면 캡쳐  <<평가기준>>  ·문제 (1) : 정확성(30%) + 기술 가독성(20%)  ·문제 (2) : 기술 가독성(50%)  \*기술 가독성🡺 이해하기 쉽게 설명하고 있는가?  다양한 서식들을 활용했는가? (예) 명령어 추가 설명, 표 또는 그림 삽입 등  ·기간 외 제출 없음 |
| 모범 답안 |
| 1)   |  |  | | --- | --- | | 1. w | 로그파일 utmp  로그인을 수행할 때 utmp 파일에 로그인 정보가 기록  주요필드 : 로그인 사용자ID, 사용터미널, 로그인시간 | | 1. lastb | 로그파일 btmp  Btmp는 로그인 시 실패한 정보를 기록하는 파일로 lastb명령어를 실행하여 확인 | | 1. last | 로그파일 wtmp  Wtmp는 사용자의 로그인과 로그아웃 정보를 가지고 있는 파일로 last 명령어로 로그 정보를 확인  -사용자 로그인 및 로그아웃 정보, 시스템 관련 정보  - 시스템 종료 및 부팅 정보, 재부팅 정보  - telnet 및 ftp등의 통한 로그인 정보 |   2)  ① 해당 화면 결과로 알 수 있는 시스템 취약점은 root의 원격 접속 허용이다.  스크린샷, 직사각형, 그래픽, 디자인이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다.  root 계정은 시스템의 중요한 계정이기 때문에 원격에서의 직접 접근을 차단하고 있다. 즉, 일반  사용자로 원격 로그인 후 명령어 su를 통해서 제한적으로 접근하도록 해야 한다. 이에 반해 해당  명령의 결과를 보면 root 유저의 TTY 칼럼이 pts 타입으로 되어 있다. 이것은 원격터미널(pts)로  root 계정으로 접속하고 있음을 의미한다.    ② 해당 화면 결과로 알 수 있는 시스템 취약점은 세션 TIMEOUT이 권고 값 범위를 초과했다.  스크린샷, 그래픽, 디자인이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다.  모든 계정의 세션 타임아웃이 장시간 유지되지 않도록 해야 한다. 권고하는 IDLE TIMEOUT은 600초(10분) 이다. 하지만 실행 결과를 보면 IDEL이 장시간 유지되고 있음을 알 수 있다. |

|  |
| --- |
|  |
|  |
| 문제 상황 |
| 사용자 계정을 비인가자에게 노출되거나 시스템 점검 소홀 등과 같은 시스템 관리자 부주의로 발생하는 공격 위협을 보안 설정을 통해 줄이고자 한다. |
| 학습목표 |
| ·시스템 환경 설정 파일들의 기능을 이해한다.  ·리눅스 잡(job) 스케쥴링 정책을 구성하고 설정할 수 있다. |
| 문제 정의 및 요구사항 |
| 1. 관리자 뿐만 아니라 일반 사용자들이 콘솔로 로그인 후 로그아웃 하는 것을 잊었다면, 보안상 위험한 상황이 벌어질 수 있다.   -이 같은 상황을 피하기 위해 일정 시간동안 사용되지 않은 계정들을 자동 로그아웃을 가능케 서버를 설정한다. (단, 모든 사용자들은 bash 쉘을 사용하고 있다.)   1. 월요일부터 금요일까지 매일 저녁 6시부터 11시까지 2시간마다   /usr/local/scripts/backup 스크립트를 실행하여 시스템을 주기적으로 점검 가능케 한다. |
| 문제 해결 가이드 |
| * 환경 변수 TMOUT 사용   -환경변수 TMOUT은 세션 타임아웃을 설정할 수 잇다.  - 권장 설정 시간은 600초이하로 설정한다.   * 환경설정 파일 /etc/profile 또는 /etc/bashrc   -해당 환경 설정파일은 모든 사용자가 로그인 시에 적용되는 설정파일이다.   1. crontab 명령어 형식   \*　　　　　　\*　　　　　　\*　　　　　　\*　　　　　　\*  분(0-59)　　시간(0-23)　　일(1-31)　　월(1-12)　　　요일(0-7)  /2는 2시간간격 또는 2분 간격 계산된 환전 금액을 사용자에게 표시한다. |
| 제출 방법 및 평가 기준 |
| <<제출방법>>  ·파일명 : 본인이름.pdf  ·실행결과(또는 설정과정) 화면 캡쳐  <<평가기준>>  ·설정 정확성(80%)  ·기술 가독성(20%)  ·기간 외 제출 없음 |
| 모범 답안 |
| 1. #vi /etc/profile   TMOUT=600  Export TMOUT   1. #crontab -e 2. 18-23/2 \* \* 1-5 /usr/local/scripts/backup   #crontab -l |

|  |
| --- |
|  |
|  |
| 문제 상황 |
| * Dictionary password cracking |
| 학습목표 |
| * 패스워드 크래킹 원리를 이해한다. * 패스워드 크래킹 실습을 통해 패스워드 복잡도에 대한 이해를 높인다. |
| 문제 정의 및 요구사항 |
| John the ripper를 이용하여 /etc/passwd에 저장되어 있는 일반 계정자들의 패스워드 크래킹을 시도한다. |
| 문제 해결 가이드 |
| * 명령어 실행 순서는 다름과 같다.   ❶ /etc/passwd와 /etc/shadow에서 일반 사용자 계정 정보만 추출하여 파일  (psword.txt)을 아래 명령어를 기반으로 수행한다.  unshadow /etc/passwd /etc/shadow | egrep ‘(^user.)’ > psword.txt   * + 명령어 수행 후 password.txt의 내용을 반드시 확인한다.   ❷ John the ripper를 이용하여 패스워드 크래킹을 시도한다.  ❸ 크래킹된 결과를 확인한다. |
| 제출 방법 및 평가 기준 |
| <<제출방법>>  ·파일명 : 본인이름.pdf  ·실행 과정 화면 캡쳐  <<평가기준>>  ·결과 완성도(70%)  ·기술 가독성(30%)  ·기간 외 제출 없음 |
| 모범 답안 |
| ❶ /etc/passwd와 /etc/shadow에서 일반 사용자 계정 정보만 추출하여 파일(psword.txt)  을 생성한다.  #unshadow /etc/passwd /etc/shadow | egrep ‘(^user.)’ > psword.txt  #cat psword.txt  텍스트, 스크린샷, 폰트이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다.  ❷ John the ripper를 이용하여 패스워드 크래킹을 시도한다.  #john --format=crypt psword.txt  ❸ 크래킹된 결과를 확인한다.  #john --show psword.txt  *텍스트, 스크린샷, 폰트이(가) 표시된 사진  AI가 생성한 콘텐츠는 부정확할 수 있습니다.* |