|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | 과 정 명 | **SSH를 이용한 원격 접속 및 접속기록 확인** | |
| **[ 조 건 ]**   1. **SSH 접속을 이용, 여러 PC를 경유하여 목표 PC에 디렉토리 2개, 파일 2개를 숨길 것.** 2. **팀 PC에 상대팀이 침입한 흔적을 발견하고, 만들어진 디렉토리 및 파일을 확인할 것**   **[ 작업 내용 ]**   1. **공 격** 2. **여러 PC를 경유하여 출발지 IP 은폐 ( 팀 pc 4대를 경유하여 목적지 192.168.0.90 도착)**     Figure 1 192.168.0.90 -> 192.168.0.161->192.168.0.116 -> 192.168.0.109 -> 192.168.0.167 (경유)   * 192.168.0.90 도착  1. **첫 번째 폴더 및 파일 생성 mkdir /etc/udisks1, vi.udisks1**      1. **두 번째 폴더 및 파일 생성 mkdir /bin/xzcmz, vi .team2**      1. **방 어** 2. **상대팀의 사전 탐색활동 감지**     Figure 2 /var/log/secure 파일 내역 확인 : 192.168.0.177로부터 user1 접속기록 있음    Figure 3 who 명령어를 통해 user1 접속기록 확인 (위와 동일)   1. **상대팀의 공격**     Figure 4 공격자가 192.168.0.167(우리팀 ip)을 경유, user20 접속하였음 (28분동안 작업확인)    Figure 5 공격자가 접속한 계정(user20)의 history 내역  => /media 경로에서 [t.txt] 파일을, /home/hi 경로에서 [d] 파일을 만든 것 확인    Figure 6 공격받은 pc의 내역을 바탕으로 역추적하여, 공격의 최초접근경로 확인(CS8-167로 들어옴)   * CS8-167에 최초접근하여 공격자의 최종 목적지인 192.168.0.116으로 이동한 것 확인  1. **결 론**  * **여러 pc를 우회하여 접속하더라도, [who / last] , [tail -f /var/log/secure] , [cd /var/log] 등의 명령어 및 로그파일 등으로 기록이 남기 때문에, 대상 pc의 루트권한을 얻어서 삭제하지 않는 한 흔적이 발견된다. 이 흔적을 바탕으로 공격자가 이용한 user에 접속하여 history 명령어를 통해 손쉽게 행적들을 발견할 수 있었으며 이를 통해 숨기고자 했던 경로와 파일들이 발각되었다.** * **다음 실습 간에는, 보다 완성도 높은 접근 및 공격을 위해 방어자 입장에서 공격의 흔적을 발견할 수 있는 각종 명령어 및 로그파일들을 미리 고려해서 흔적을 삭제하거나 변조하는 식의 접근이 요망된다.** |