|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:문관필 | | |  | |
|  | <TCP Session Hijacking> | | | | | | |  |
|  | |  | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |

Session은 송수신 네트워킹을 위해 상호 인증에 필요한 정보를 교환 후 두 컴퓨터 간의 연결된 활성화 상태를 말한다.

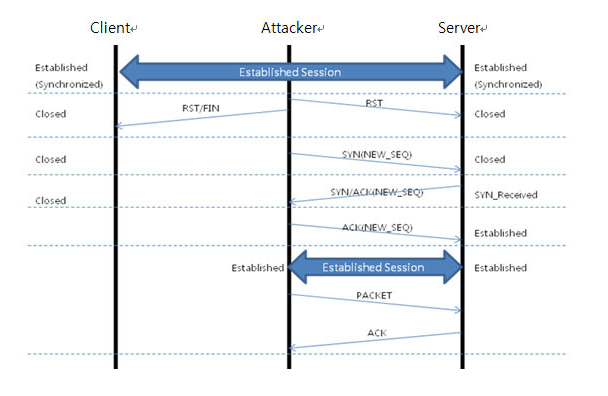
TCP Session Hijacking은 서버와 클라이언트가 통신할 때 TCP의 시퀀스 넘버를 제어하는데 문제점이 있음을 알고 이를 파고든 공격이다.

클라이언트와 서버 간의 통신을 관찰할 수 있을 뿐만 아니라 Telnet, FTP 등 TCP를 이용한 거의 모든 세션을 갈취하는 것이 가능하다.

또한 인증에 관한 문제를 해결하기 위해 도입된 일회용 패스워드, 토큰 기반 인증을 이용한 세션 갈취도 가능하다.

단순히 훔쳐보는 것이 아니라, 해당 PC의 권한으로 명령어를 사용할 수 있음에서 강력한 공격기법 중 하나이다.

<공격 원리>



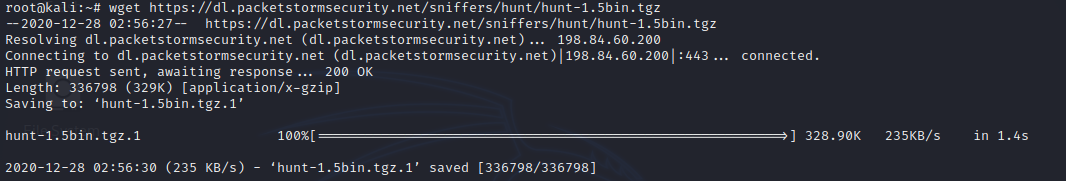
1. 현재 클라이언트와 서버간에 세션이 성립되어 있는 상태
2. 공격자는 스니핑을 통해서 세션을 확인하고, 시퀀스 번호를 훔쳐 알아낸다.
3. 공격자는 클라이언트에게 RST/FIN 패킷을 보내 연결을 끊어버리고, 서버에게는 RST패킷을 보내서 잠시 연결 중지 상태로 만든다.
4. 그리고 공격자는 새로운 시퀀스 번호를 생성해서 SYN패킷을 보내어 서버와 새로운 세션의 생성 시도를 한다.
5. 서버는 해당 시퀀스 번호를 받아들이고 정상적인 연결처럼 공격자와 세션을 형성.

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| |  |  |  | | --- | --- | --- | | 실습 환경 | IP Address | OS | | 서버 | 192.168.0.100/24 | CentOS 8 | | 사용자 | 192.168.0.101/24 | CentOS 7 | | 공격자 | 192.168.0.102/24 | Kali Linux |  1. 공격 환경   Client  1  TELNET SERVER  3 2  Attaker |
| 1. 공격 |
|  |

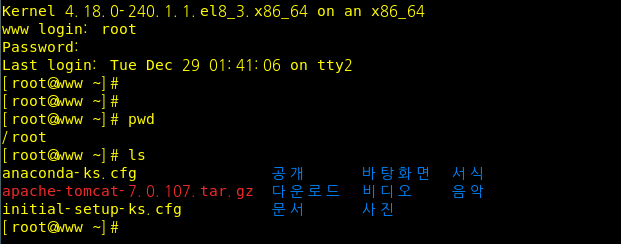
1. 서버에 telnet-server를 설치



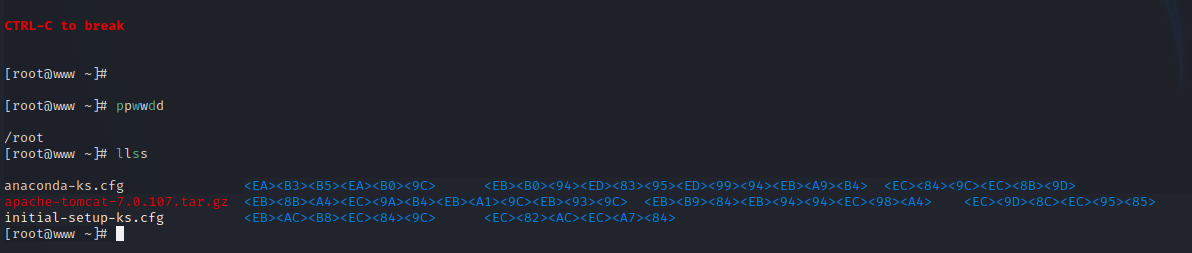
1. telnet.socket 실행



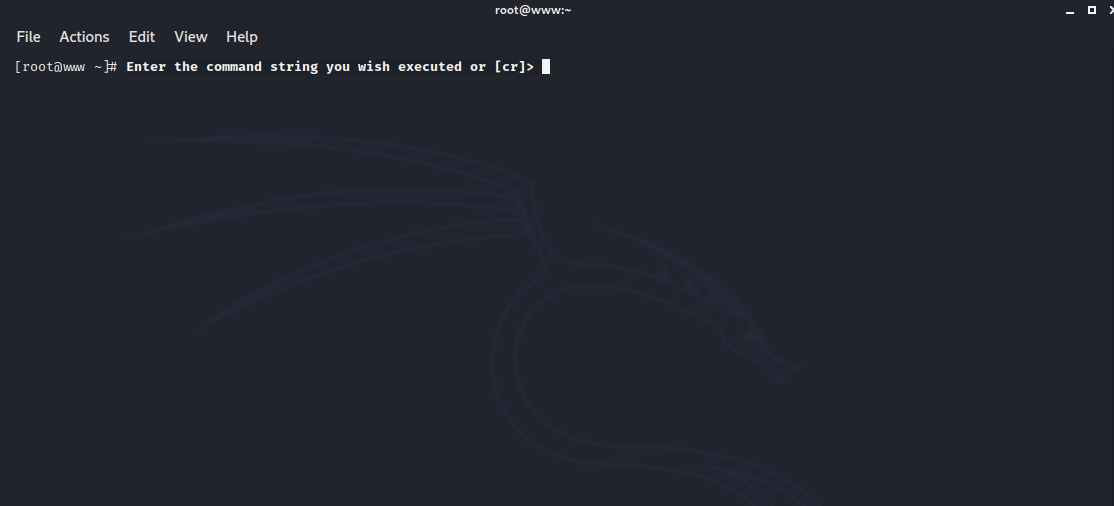
|  |
| --- |
| 1. 공격자 Kali에서 wget <https://dl.packetstormsecurity.net/sniffers/hunt/hunt-1.5bin.tgz> 입력 후 다운로드      1. 다운로드 완료 후 tar 명령으로 다운로드 받은 hunt 압축 해제      1. 압축해제 한 디렉터리에 들어간 후 make 명령으로 컴파일 실행      1. ./hunt\_static -I eth0 입력 후 아래 목록 뜨는 것까지 확인 후 대기      1. 사용자 PC로 가서 서버로 텔넷 접속      1. 다시 공격자 PC로 돌아와 l(소문자 L) 입력 후 사용자PC IP 확인      1. IP 확인이 됐으면 s 입력 후 0, y, b, y 순으로 입력 후 엔터      1. 위 화면이 뜨면 공격 성공 |
| 3. 공격 결과 |
|  |



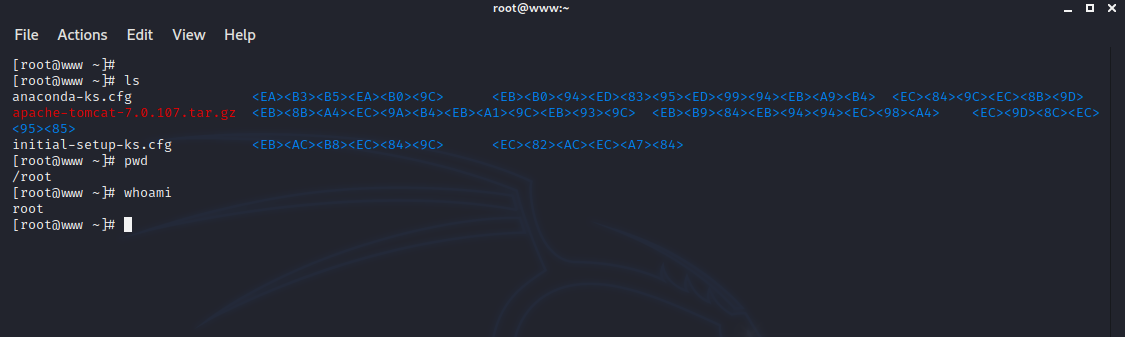
1. 사용자 PC에서 명령어들을 입력해본다.



1. 그 결과들이 그대로 공격자의 PC에서도 확인 할 수 있는 것을 알 수 있다.



1. Ctrl+C를 누르고 대기한 후 사용자의 PC에서 명령어들을 입력 한 후 공격자의 PC로 돌아오면 정상적으로 세션을 가로채기 한 것을 확인 할 수 있다.



1. 공격자의 PC에서도 명령어들이 잘 작동하는 것을 확인 할 수 있다.

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |

1. 메시지 내용의 암호화

* SSH 사용!!

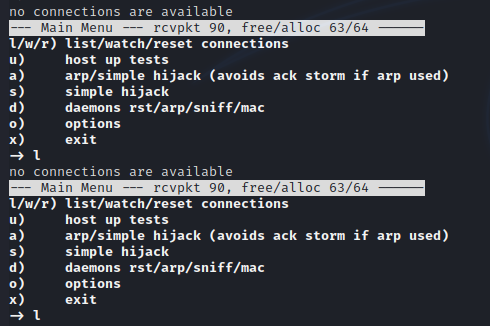
1. 지속적인 인증 요구

* 처음 로그인 후 일정 시간 내에 다시 로그인을 실시하는 방안

1. 시퀀스 넘버 체크

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |

* 사용자 PC에서 SSH로 Telnet-server에 접속



* 공격자 PC에서 list를 출력해도 나오지 않음