컴퓨터보안 실습

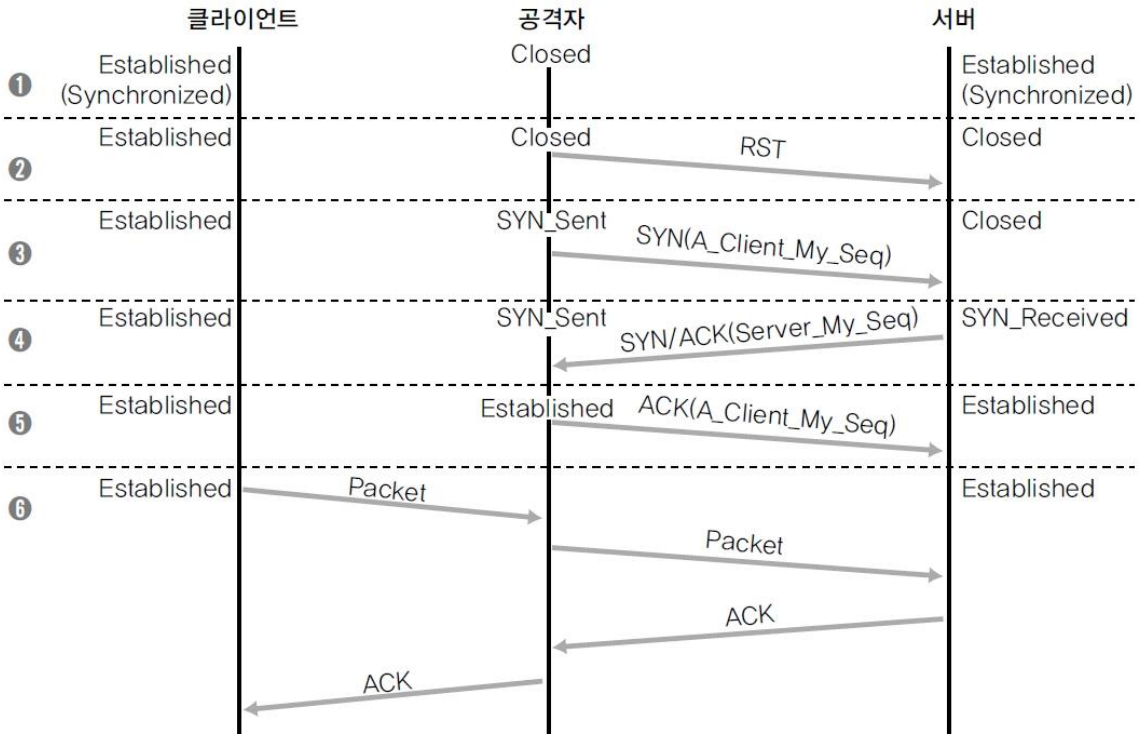
세션 하이재킹
(Session Hijacking)

4주차

참고문헌 : 정보보안개론과 실습-한빛미디어 (Hunt 툴사용)

세션 하이재킹(Session Hijacking)

- 사용자와 컴퓨터, 또는 두 컴퓨터 간의 활성화 상태인 세션**(session)** 가로채기
- **https://www.youtube.com/watch?v=MLaJCwIM8T0**
- **https://www.youtube.com/watch?v=TmJRTORmki4**



세션 하이재킹(Session Hijacking)

1. 클라이언트는 서버와 모두 접속되어 있는 Established 상태, 공격자는 적절한 시퀀스 넘버를 획득하기 위해 스니핑을 하고 있음

2. 공격 시점에 비동기화 상태 중 세션이 완전히 끊어지지 않는 시퀀스 넘버의 범위에서 RST 패킷을 생성하여 서버에 보냄 서버는 잠시 Closed 상태가 되나 클라이언트는 그대로 Established 상태

3. 공격자는A_Client_My_Seq를 생성하여 서버에 보냄

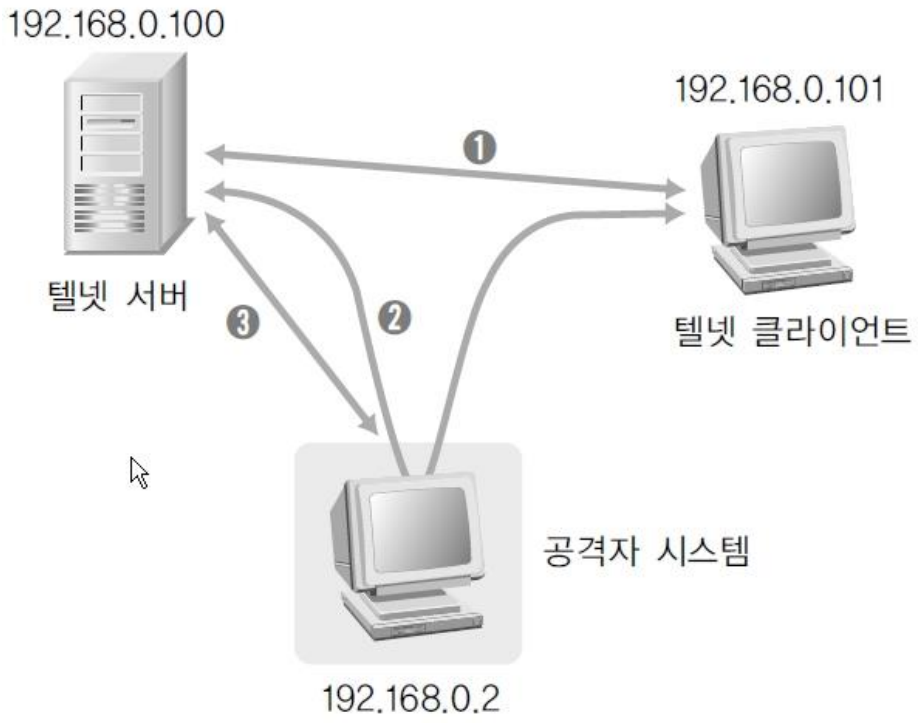
4. 서버는 새로운 A_Client_My_Seq를 받아들이고, Server_My_Seq를 재생성하여 공격자에게 보낸 후 Syn_Received 상태

5. 공격자는 정상 연결처럼 서버와 시퀀스 넘버를 교환하고, 공격자와 서버 모두 Established 상태. 원래의 클라이언트는 여전히 Established 상태고 서버의 네트워크 상태로 인한 잠시 동안의 연결 문제로 받아들임. 연결은 끊어졌지만 인증 세션은 열린 상태

hunt(세션 하이재킹 툴) 특징

- 관심 있는 접속 설정
- 자신의 시스템에 접속하려는 연결 탐지
- ACK Storm의 탐지를 통한 능동적 세션 하이재킹
- ARP 스푸핑 탐지
- 하이재킹한 후 서버와 클라이언트 간 동기화
- 접속 리셋
- 접속 감시

세션 하이재킹(Session Hijacking) 실습과정



❶ 클라이언트가 서버로 텔넷 접속을 한다.

❷ 공격자가ARP 스푸핑으로 패킷의 흐름을 공격자를 통과하도록 변경한다.

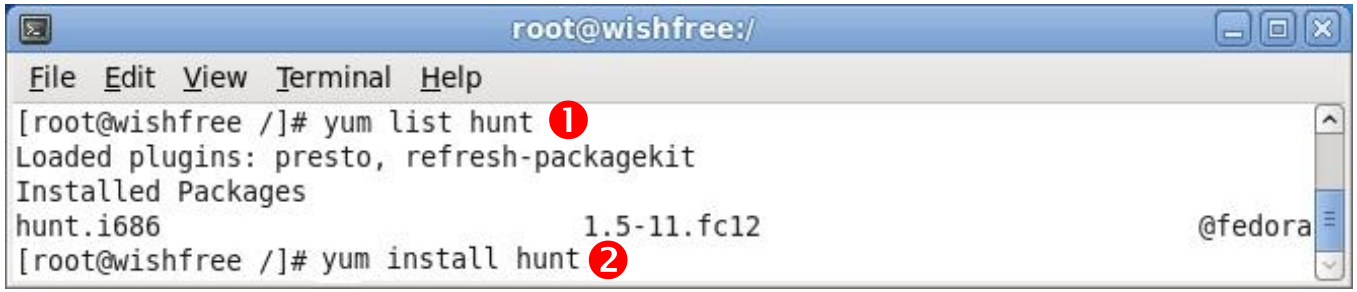
❸ 클라이언트와 서버의 통신을 끊고, 해당 세션을 클라이언트로부터 빼앗는다.

실습 환경

- 서버 : 리눅스 (레드햇, 페도라, 우분투 등)
- 클라이언트 : 윈도우
- 응용프로그램 : hunt.i686

hunt를 이용해 텔넷 세션 하이재킹하기

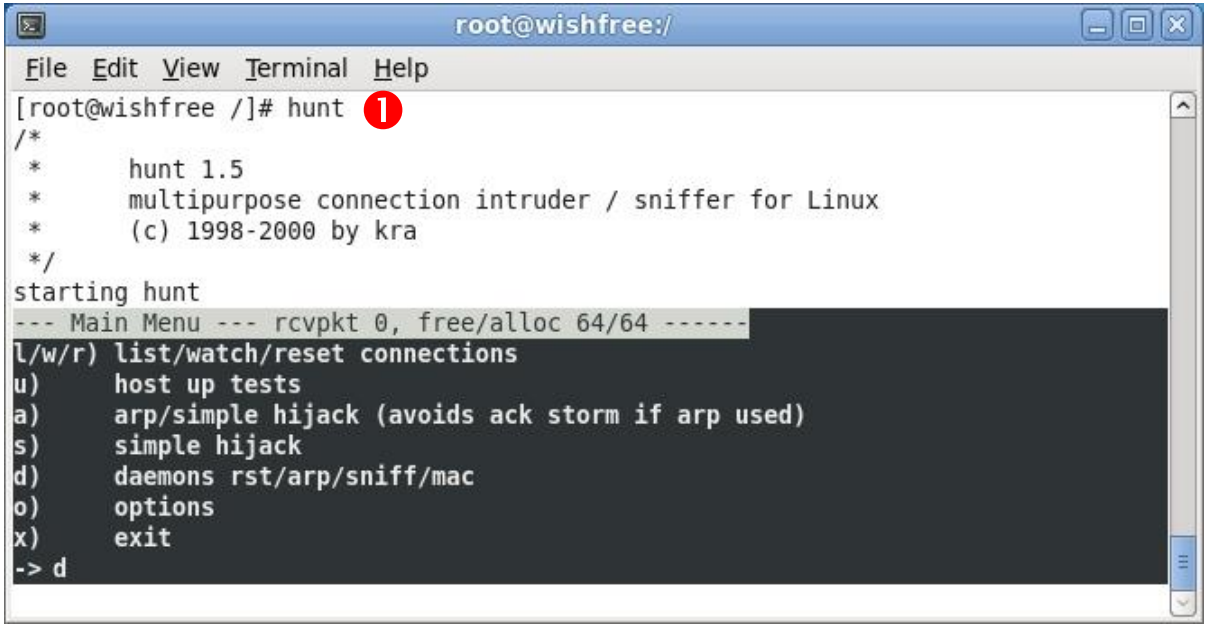
1 hunt 설치 ❶ `yum list hunt` ❷ `yum install hunt`



2 텔넷 접속 생성 : 텔넷 클라이언트로부터 텔넷 서버에 연결

3 ARP 스푸핑 & 패킷 릴레이 실행

3-1 hunt 실행 ❶ `hunt` ❷ `[d]` 입력

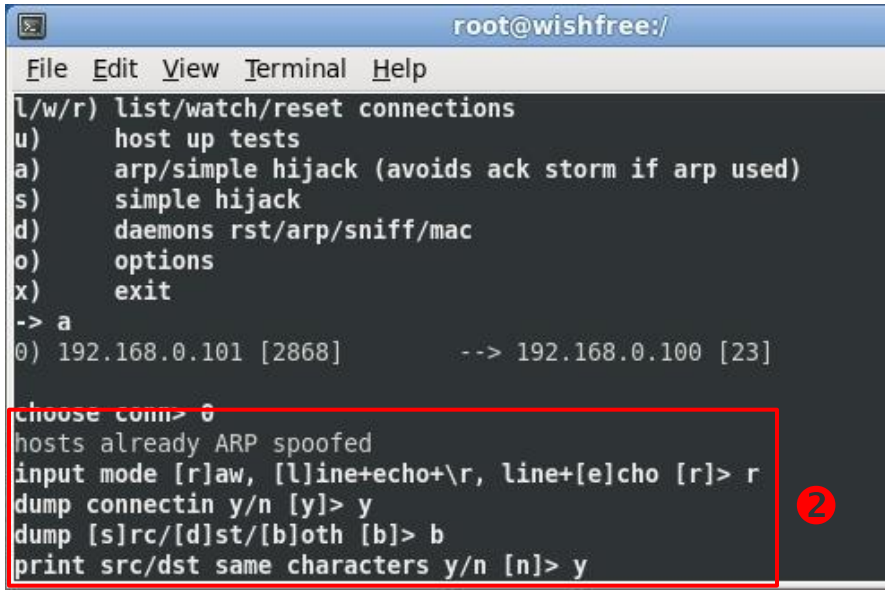


hunt 이용해 텔넷 세션 하이재킹하기

4 세션의 탐지 ❶ [x] 두 번 입력 ❷ [l] 입력

5 스니핑 모드 수행

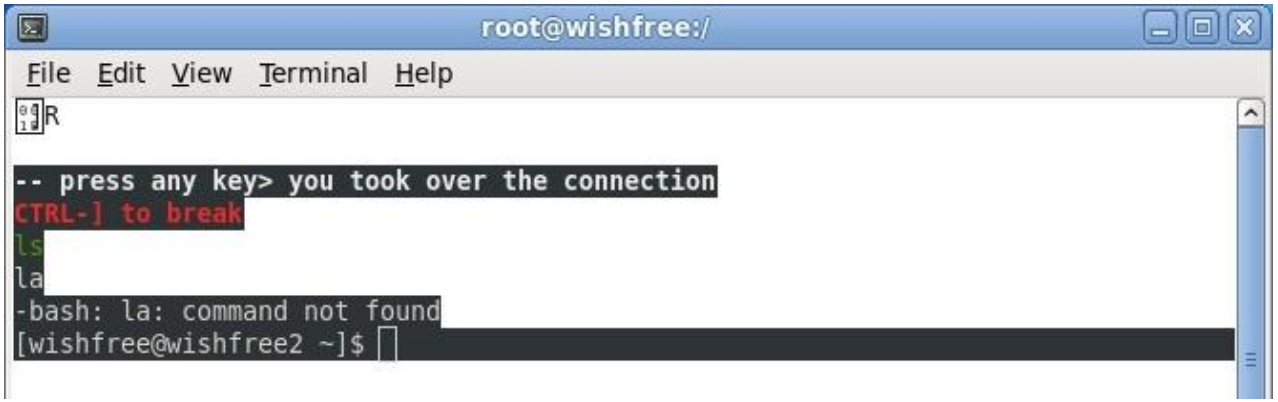
5-1 hunt 실행 ❶ [a] 입력 ❷ choose conn> 0



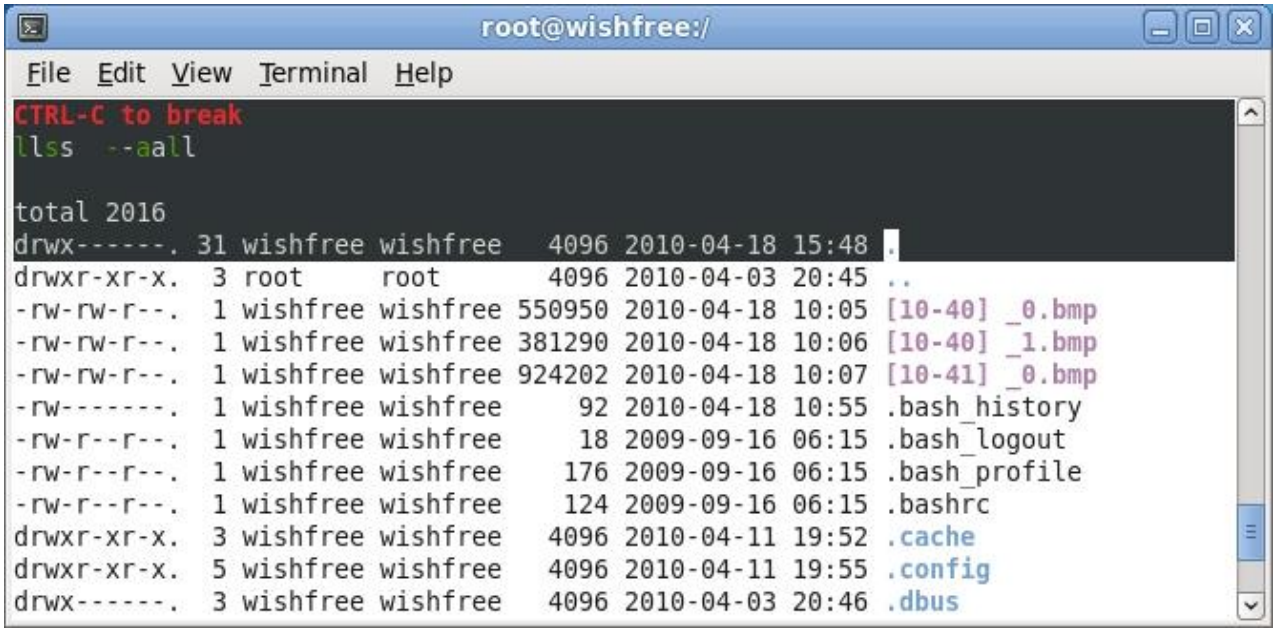

```
input mode : r
dump connectin : y
dump : b
print src/dst same characters : y
```

hunt를 이용해 텔넷 세션 하이재킹하기

5-2 공격 실행 후 피공격자 시스템에서 ls -al 명령 수행



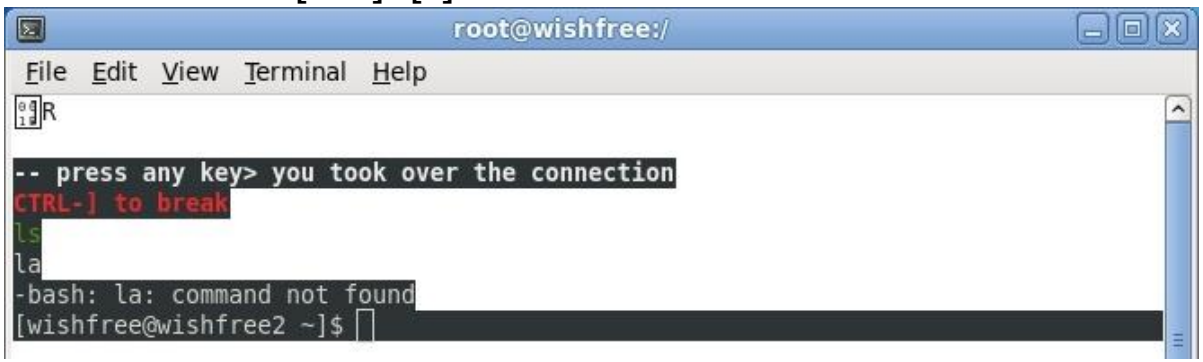
5-3 공격 실행 후 공격자 시스템 화면 확인



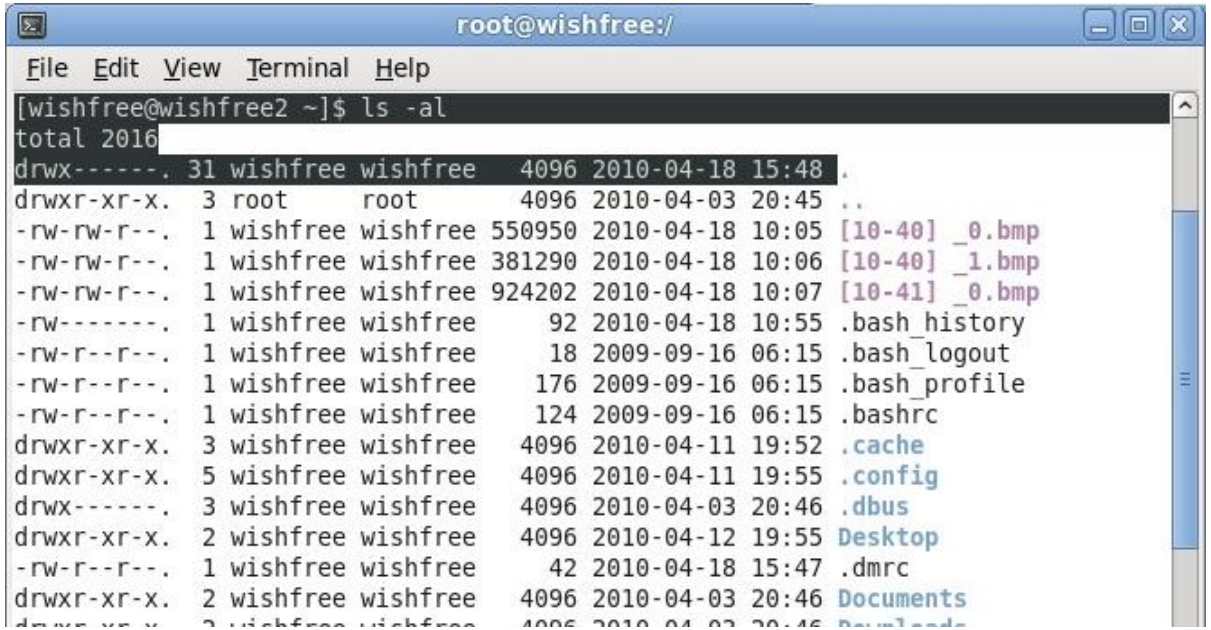
hunt를 이용해 텔넷 세션 하이재킹하기

6 세션 하이재킹 수행

6-1 hunt 실행 : [Ctrl]+[c]를 수행하고 피공격자가 글자 입력



6-2 TCP 세션 하이재킹 공격 완료 ls -al



참고문헌

1. 정보보안개론과 실습-한빛미디어 (Hunt 툴사용)

2. 웹 세션 하이 재킹 공격 실습 (Solatech- 김재벌)

Q & A