1. 운영 환경 구축 절차

* 공격자(Kali linux1), 서버(Kali linux2), 클라이언트(Window 10)
* 서버측에서 SSH 프로토콜 version 1,2 모두 사용할 수 있도록 설정해야한다.

( vi /etc/ssh/sshd\_config 에서 Protocol 2 -> Protocol 1,2로 변경)

* SSH version 협상시 정보 변경을 위해 Filter 생성

/usr/local/share/Ettercap 디렉터리에 etterfilter etter.filter.ssh -o etter.filter.co 명령어로 etter.filter.ssh 파일을 etterfilter 프로그램을 이용하여 컴파일 해준다. 공격자가 공격시 Ettercap 프로그램에서 만든 필터를 이용해 SSH 연결을 알 수 있다.

1. 공격 관련 기술과 취약점

* 리눅스, 유닉스 서버는 안전한 쉘 접속을 위해 SSH를 많이 사용하는데 보안성의 문제로 기존 사용하던 SSH version 1 보다 SSH version 2를 사용한다. SSH downgrade 공격은 SSH version을 강제로 1로 낮추어 정보를 훔치는 공격이다.
* SSH version 1은 공개 키를 이용하여 세션 키를 암호화하는 방식을 사용하기 때문에 암호화된 세션 키가 노출된다면 공개 키를 이용해 누구나 알 수 있는 문제가 있다. 따라서 SSH version 2는 Diffie-Helman 암호화 방식을 이용하여 정보를 암호화하여 SSH version 1보다는 보안성을 높혔다.

1. 예상 공격 시나리오와 공격 대응 방법

* 공격 시나리오

1. 클라이언트가 서버로 SSH 암호화 통신을 한다는 패킷 전송
2. 공격자는 중간에서 클라이언트의 대화내용을 스니핑하여 서버에 전달
3. 서버는 SSHv1, SSHv2 모두 사용 가능하다고 클라이언트에 전송
4. 공격자가 서버의 메시지를 가로채 SSHv1만 가능하다고 클라이언트에게 전달
5. 클라이언트는 SSHv1 사용을 허락
6. 클라이언트의 메시지를 보고 서버도 SSHv1로 통신 시작

* 공격 대응 방법

1. /etc/ssh/sshd\_config 파일의 Protocol 부분을 2로 변경하여 SSHv1을 사용할 수 없게 한다.
2. 클라이언트에서 SSH 통신을 서버 접속 프로그램을 사용하여 진행할 때 SSH version을 only 2로 설정하면 SSHv2로만 통신이 가능해진다.