**[SSH]**

**- 원격 컴퓨터에 안전하게 엑세스하기 위한 유닉스 기반의 명령 Interface 및 Protocol**

**- 패킷이 암호화되어 전송되어 암호화되기 때문에 Sniffing 된다 하여도 해독 키가 없어 내용을 파악하기 어렵다.**

**[SSH MITM 공격 (Ver.1 downgrade 공격)]**

**- 대부분의 서버 관리자는 서버 보안 접속을 위해서 SSH를 사용하여 접속**

**- SSH Version 1은 public-key를 이용하여 Session-Key를 암호화 하는 방식을 사용한다.**

**- 그런데 SSH Version 1은 키를 노출시키는 문제가 있어서 보안성이 낮아서 MiTM 공격에 취약**

**- 요즘은 SSH Version 2로 사용**

**- SSH MITM 공격은 중간에 MITM 환경을 만들어 SSH Version 2를 쓰는 사용자에게 다운그레이드 공격을 통해서 Version 1로 다운그레이드 하는 공격을 말함**

**- Ettercap 툴을 활용해 MiTM을 수행한다.**

**- 서버에서 보내는 1.99 패킷을 1.5로 변경해서 타겟에게 포워딩 하므로, 공격자는 패킷을 잡는 것 뿐만 아니라 수정까지 해야한다.**

**[SSH MITM 공격 시나리오]**

**- arp poisoning 공격을 통해서 서버와 클라이언트간의 통신에 끼어 들어서 중간에 데이터를 가로채는 방법을 통해서 해당 공격을 성사**

**-**

**- 공격자로는 Kali linux가 필요, 피공격자는 Windows 7 with putty - 이하 Vic C 조건, 서버는 Centos Server with SSH 이하 Vic S 조건**

**[SSH MITM 공격 방법]**

**- SSH 버전에 따라 다르다.**

**1) SSH가 2.0으로만 통신하게 되어 있는 경우에는 통신을 차단**

**(SSH v2/ssh – 2.0) -> 공격 안전**

**2) SSH가 1.0, 2.0 다 접속할 수 있게 되는 경우 1.0으로 접속할 수 있게 함**

**(SSH v1 or SSH v2/ssh – 1.99) -> 공격 취약**

**3) 1.0을 접속하는 경우 정상적으로 통신할 수 있게 함**

**(SSH v1/ssh – 1.5) -> 공격 취약**