16011069 장지혁

10.1 과제 주제

3-way-handshaking 이란 무엇인가?

TCP 프로토콜을 사용하는 장치들 사이에서 논리적인 접속을 성립하기 위한 과정

성립 과정

1. 클라이언트 > 서버 (SYN 패킷 전송)

   클라이언트에서 서버 측으로 통신요청 메시지(SYN)를 전송

2. 서버 > 클라이언트 (SYN, ACK 패킷 전송)

   클라이언트의 요청에 대한 응답(ACK)과 서버에서 클라이언트 측으로 통신요청 메시지(SYN) 전송

3. 클라이언트 > 서버 (ACK 패킷 전송)

   클라이언트가 2.에서 받은 요청에 대한 응답(ACK)를 서버측으로 전송

이 과정을 통해 클라이언트와 서버가 통신준비를 마치고, 통신이 연결되어 있음을 보장하게 된다.

10.2 과제 주제

ARP 스푸핑과 관련된 해킹 사례 조사

http://m.boannews.com/html/detail.html?idx=50078 보안뉴스-2016/03/27

'꿀뷰' 다운로드 받으려다 200 여명 악성코드 감염

반디소프트의 이미지 뷰어 프로그램 '꿀뷰'를 다운받은 200 여명의 사용자들이 악성코드를 다운받게 된 사례입니다. 약 두시간 동안 반디소프트 홈페이지가 외부로부터 ARP 스푸핑 공격을 받아 꿀뷰 대신 악성코드를 다운받도록 했습니다. 악성 코드 실행시 꿀뷰 설치파일 실행과 동시에 악성코드가 시스템에서 자동실행 되면서 시스템의 정보를 유출했습니다.

이에 대한 대응책으로 반디소프트측은 MAC 어드레스를 고정시켜 놓은 대응책을 내놓았고, https 로만 접근 가능하게 홈페이지를 변경했습니다.

10.3 과제 주제

IP 스푸핑과 관련된 해킹 사례 조사

https://www.boannews.com/media/view.asp?idx=51970&kind=4 보안뉴스-2016/10/05

도널드 트럼프 폭로 기사 내보낸 뉴스위크, 디도스 공격 당해

미국 언론매체 뉴스위크(Newsweek)가 도널트 트럼프 기업의 불법 행위를 폭로한 직후 IP 스푸핑을 통해 디도스 공격을 당한 사례입니다. 디도스 공격 직후 몇시간 동안 사이트가 다운되었으며, 사이버 수사에서 IP 주소들을 분석한 결과 러시아 IP 가 다량 검사되었지만 IP 스푸핑 으로 IP 를 속였기 때문에 섣불리 러시아측에서 공격했다고 단정지을 수 없었습니다.