**ARP   
Spoofing**

**디지털포렌식  
김현민**

**일시 : 2016.07.19(화)**

**목차**

1. **개요**
2. **목적**
3. **구성**
4. **결과**
5. **느낀점**

**그림 목차**

**그림1. 프로그램의 실행 모습**

**그림2. 프로그램을 실행했을 때 wireshark로 캡처한 모습**

**그림3. Victim의 화면**

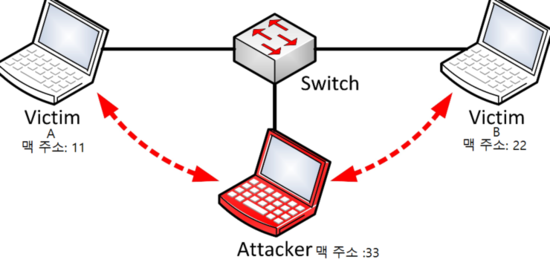
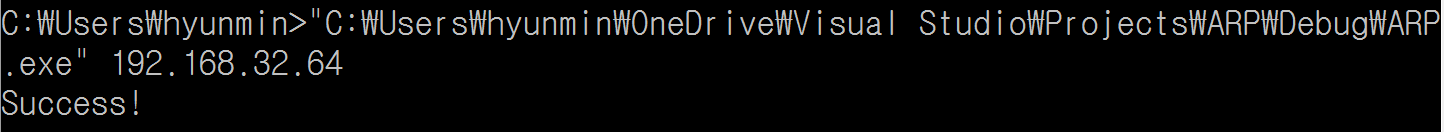
1. **개요**  
   네트워크 패킷(Ethernet과 ARP)에 대한 구조를 이해하고 ARP Spoofing 공격에 대해 이해한다.
2. **목적**ARP 스푸핑을 위한 패킷 구조를 파악하고 직접 네트워크 정보를 가져와 값을 대입해 같은 네트워크 상에 잇는 사용자(Victim)에게 ARP 스푸핑 공격을 하는 코드를 보내. 자신을 게이트웨이로 착각하게 만든다.
3. **구성**  
   위 그림처럼 원래 사용자들 (맥주소 11, 맥주소 22)이 Switch를 이용해 통신을 하는 도중 Attacker는 각 Victim에게 Switch의 IP주소와 함께 자신의 MAC 주소를 가진 패킷을 날린다. 이때 Vimctim의 IP는 Input으로 입력을 받고 MAC주소는 ARP패킷을 통해 직접 값을 확인한다. 후에 각 Victim에게 ARP Spoofing을 위한 패킷을 보내게 되면 Victim은 패킷을 Swtich로 보내지 않고 Attacker에게 보내게 된다.
4. **결과**  
   

Figure 1. 실행

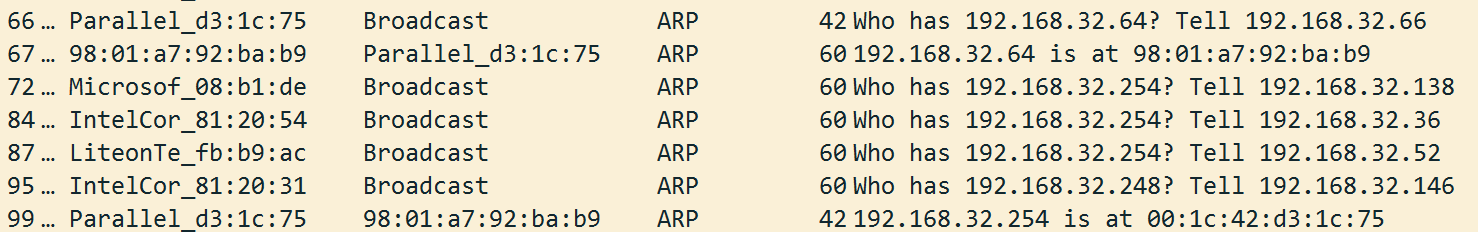
해당 소스코드를 실행시키면 그림1과 같은 결과가 나온다.  
  


Figure 2 네트워크 정보

그림2는 프로그램을 실행시켰을 당시 Wireshark로 패킷을 캡처한 모습이다. 위에 보는 것과 같이 MAC주소를 얻기 위한 Send/Receive와 스푸핑 공격을 위한 패킷을 볼 수 있다.

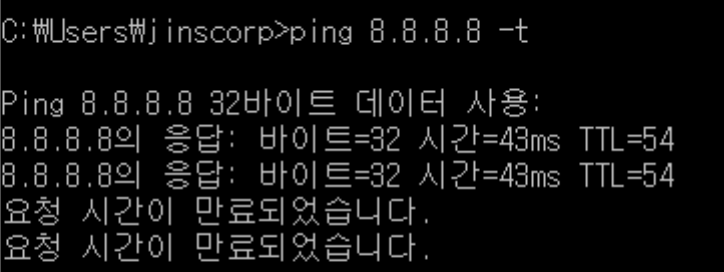


Figure 3 Victim 화면

마지막으로 Victim의 ping 명령어를 수행한 모습이다. 정상적으로 실행이 되다가 ARP 스푸핑 공격이 들어왔을 때 패킷이 정상적으로 나가지 않는 것을 볼 수 있다.

1. **느낀점**처음 공격 코드를 작성 하라고 과제를 내주셨을 때는 생각만 했던 때라 금방 할 것 같았다. 하지만 막상 코딩을 해보니 네트워크 장치를 선택하는 것부터 IPHlpApi.h를 사용하는 것과 스레드를 이용하는 것까지 처음 해보는 기능이 많이 있었다. 특히 가장 어려웠던 것은 pcap이나 IPHlpApi.h를 설치하는 과정이었는데 원인을 알 수 없는 에러가 많이 일어났었다. 하지만 많은 검색을 통해 설치를 했고 로우 소켓을 통해 진행을 하였기 때문에 코드가 조금 길지 않았나.. 라고 생각을 해봤다.   
    거의다 작성을 한 뒤에 안 것이지만 파이썬으로 arp 패킷 구조만 바꿀 수 있다고 들었다.. 30몇줄이었다고 하는데.. 슬펐다..