스니핑 스푸핑 분석

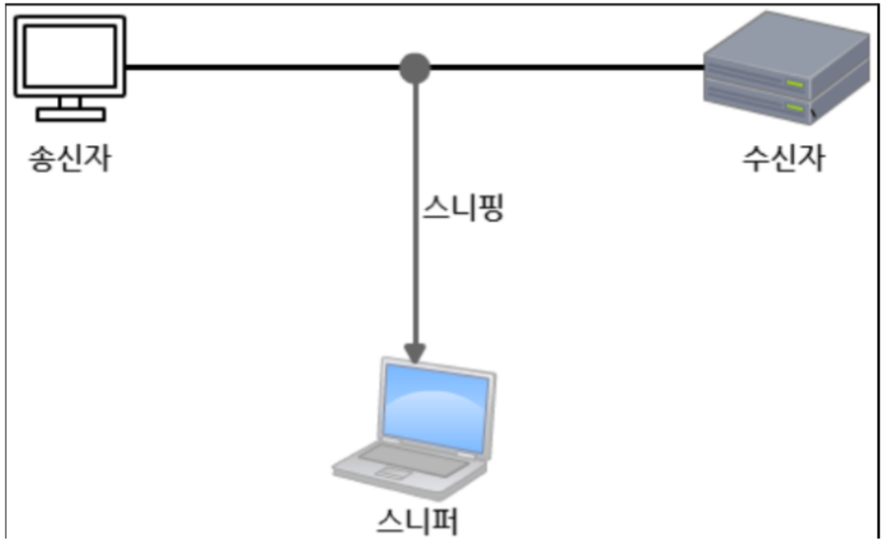
2024-03-20 IT정보공학과 이진규

Sniffing

Sniff　　코를 훌쩍이다, 킁킁거리다

네트워크 경로상에서 자신이 아닌 다른
상대방들의 전송되는 패킷을 훔쳐보는것

일반적으로 작동하는 IP 필터링과 MAC 주소 필터링을 수행하지 않고 랜 카드로 들어오는 전기 신호를 모두 읽어 다른 이의 패킷을 관찰

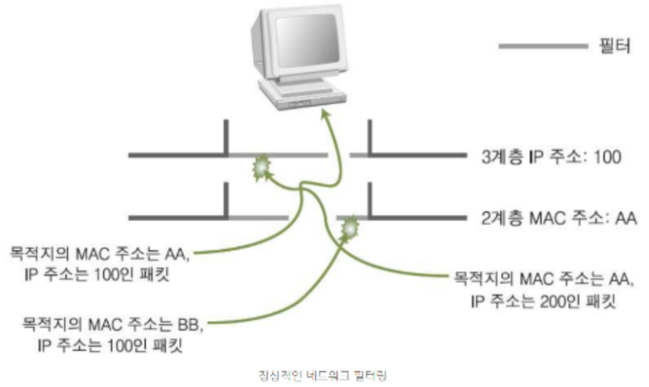


Sniffing

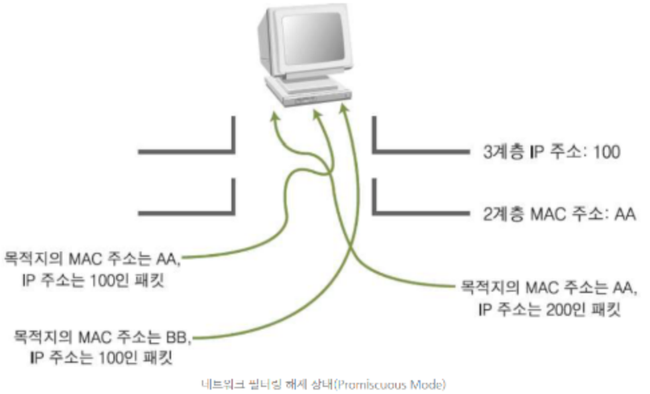
이더넷은 로컬 내트워크 내의 모든 호스트가 같은 선을 공유하도록 이루어짐

같은 네트워크 내의 모든 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있음

랜 카드는 전송된 패킷의 정보를 읽고 처리 여부를 결정하여 정보가 자신의 것과 일치하지 않으면 패킷을 무시



정상적인 네트워크 필터링



네트워크 랜카딩 해제 상태(Promiscuous Mode)

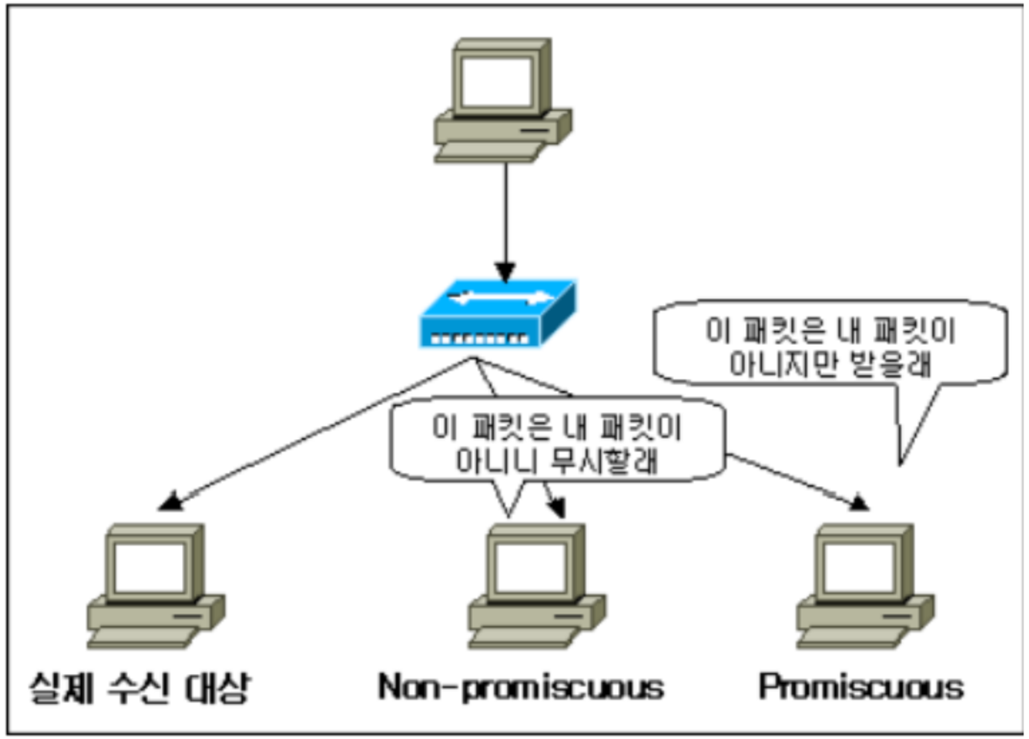
Sniffing

허브 환경

기본적으로 들어오는 패킷에 대하여 모든 포트로 패킷을 보냄

공격자가 Promiscuous Mode 로 동작하게 되면 스니핑 도구를 이용해 패킷을 저장 및 분석 가능

Promiscuous Mode
네트워크 상 랜카드가 패킷을 받을 때 IP 주소와 MAC 주소가 랜카드에 해당하는 정보와 다르더라도 패킷을 모두 수집

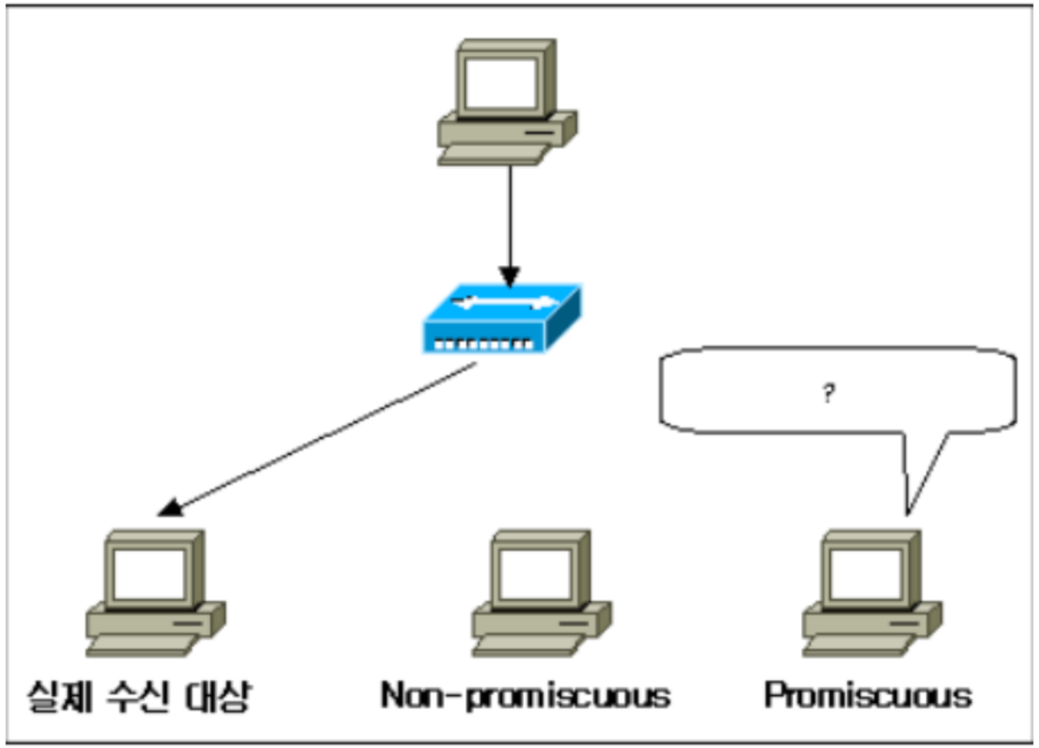


Sniffing

스위치 환경

스위치는 기본적으로 MAC 주소를 이용해 패킷 목적지를 결정

허브 환경에서와 다르게 스위치 환경에서는 실제 수신 대상에게만 패킷을 보내게 되어서 패킷을 받아볼 수 없게 됨



Sniffing

스위치 공격 및 스니핑 방법

switch jamming	스위치의 MAC address Table에 대해서 버퍼 오버플로우 공격을 수행해서 스위치가 허브처럼 동작하게 만듦
ICMP Redirect	ICMP Redirect 메세지를 발송하는 것으로 라우팅 경로를 자신의 주소로 위조한 ICMP Redirect 메세지를 대상에게 전송
ARP Redirect	Router의 MAC 주소로 변경하여 ARP Reply 패킷을 해당 네트워크에 브로드캐스트

Spoofing

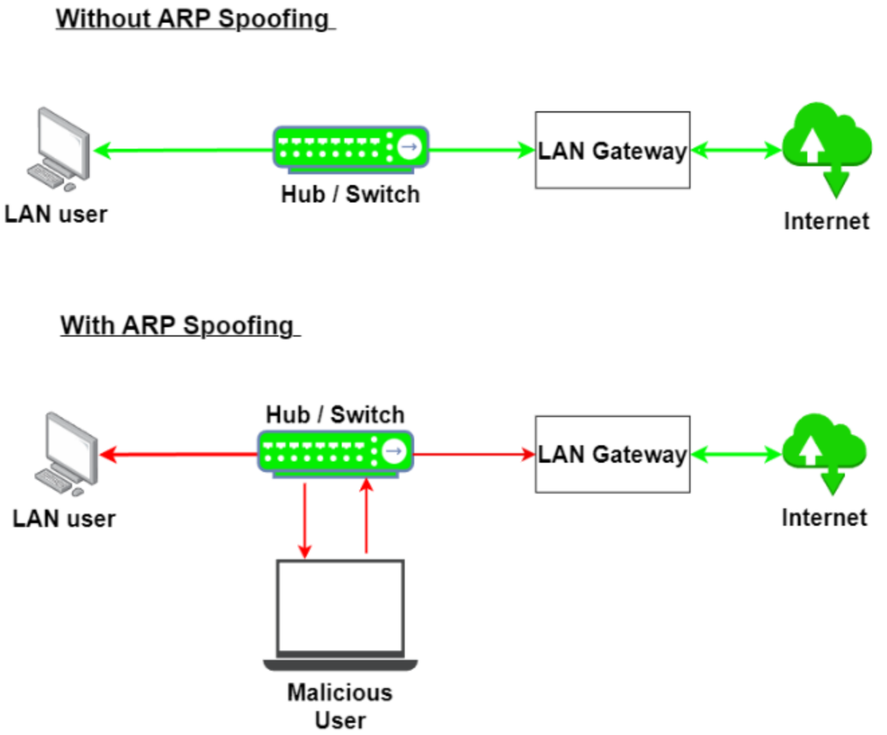
Spoof 패러디하다, 도용하다, 속여먹다

악용하고자 하는 호스트의 IP주소나 이메일의 송신 주소
를 변조하여 보내 이를 통해 해킹을 하는 것

ARP Spoofing

ARP: 상대방 IP 주소는 알지만 MAC 주소를 모를 때 사용하는 프로토콜

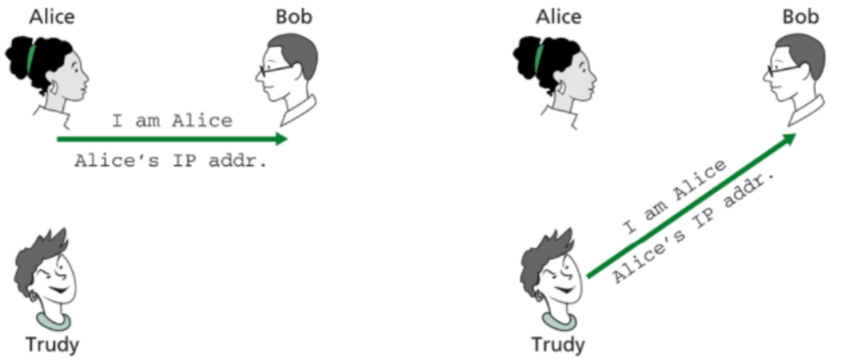
자신의 MAC주소를 다른 컴퓨터의 MAC주소인 것처럼 속이는 공격

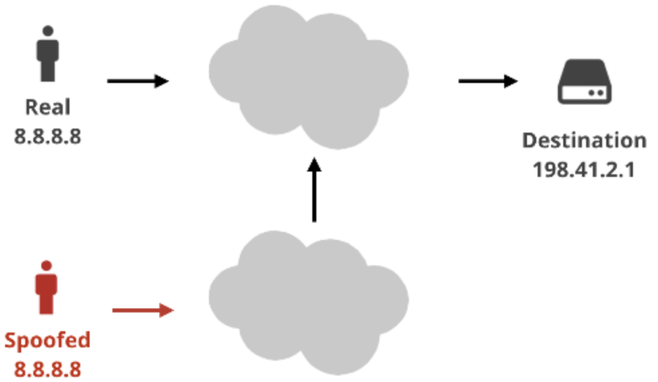


IP Spoofing

IP 정보를 속여서 다른 시스템을 공격

다른 사용자가 사용하는 IP를 악용해 권한을 획득

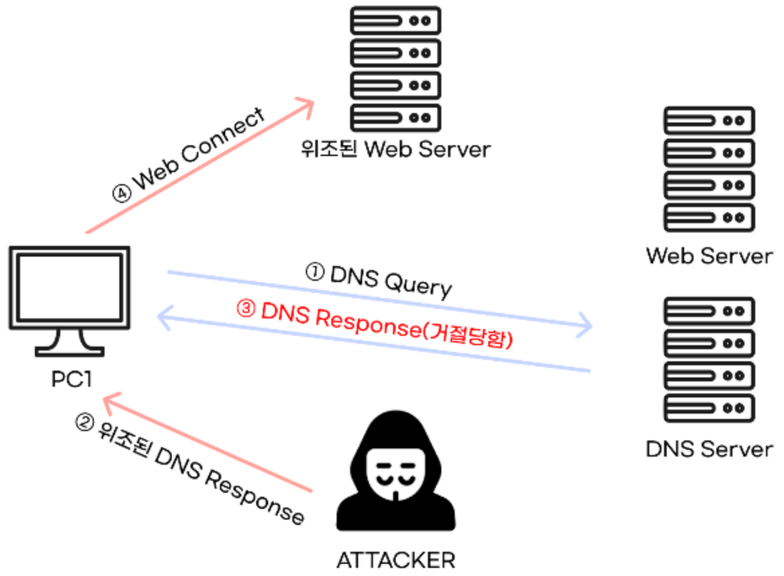




DNS Spoofing

DNS: 인터넷 연결 시 도메인 주소를 실제 IP 주소로 대응시켜 줌

실제 DNS 서버보다 빨리 공격 대상에게 DNS 응답 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도



공격 대응 방안

ARP Table 을 정적으로 구성하고 중요 패킷을 암호화 프로토콜을 사용하여 암호화

감사합니다