5주차 1차시 스피닝공격

【학습목표】

1. 스니핑공격의 개념을 설명할 수 있다.
2. 스니퍼를 탐지하는 종류를 구분할 수 있다.

학습내용1 : 스피닝공격의 개념

1. 스니핑(Sniffing)

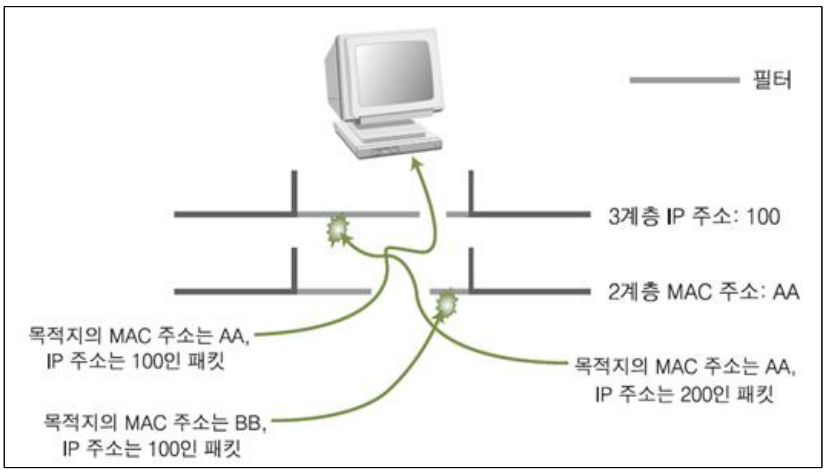
* 스피닝 : 수동적(Passive) 공격이라고도 부름

1) 스니핑 공격의 종류
- 드라마에서 주인공이 문 앞에서 다른 이의 대화를 엿듣는 것
- 도청(Eavesdropping)
- 전화선이나 UTP(Unshielded Twisted Pair)에 태핑(Tapping)을 해서 전기적 신호를 분석해 정보를 찾아내는 것
- 전기적 신호를 템페스트(Tempest) 장비를 이용해 분석하는 것

2) [그림] 스니핑 공격

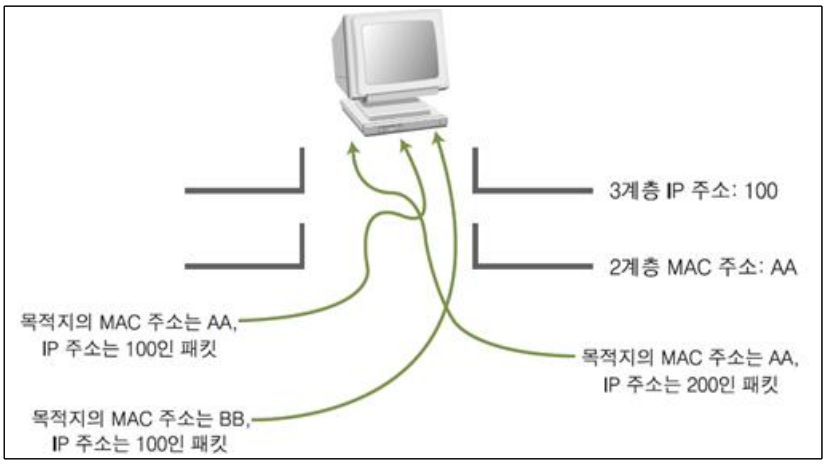
2. 스니핑 원리

1) [그림] 정상적인 네트워크 필터링



- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하기 때문에 2계층과 3계층 정보를 이용한 필터링은 방해물임
- 이럴 때 2, 3계층에서의 필터링을 해제하는 랜 카드의 모드를 프러미큐어스(Promicuous) 모드라고 함

2) [그림] 네트워크 필터링 해제 상태(프러미스큐어스 모드)



학습내용2 : 스피닝공격의 응용

1. 스위치 재밍 공격

<스위치의 주소 테이블의 기능을 마비시키는 공격>
- MACOF 공격이라고도 함
- 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 자연스레 저장 용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브처럼 작동하게 됨

2. SPAN 포트 태핑 공격

<SPAN은 포트 미러링(Port Mirroring)을 이용한 것>
- 포트 미러링 : 각 포트에 전송되는 데이터를 미러링 하고 있는 포트에도 똑같이 보내주는 것
- SPAN 포트는 기본적으로 네트워크 장비에서의 하나의 설정 사항으로 이뤄지지만, 포트 태핑(Tapping)은 하드웨어적인 장비로 제공되고 이를 스플리터(Splitter)라고 부르기도 함

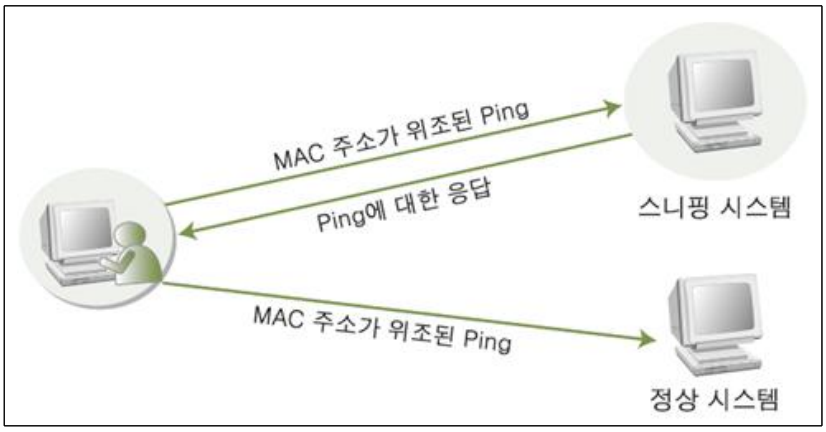
3. 스니퍼의 탐지

<자신의 이름이 아닌데도 아무 이름에나 받아들여 대답하다가 교수님께 걸리는 프리미스큐어스 모드의 학생>

1) [그림] 대출이 들키는 상황

2) Ping을 이용한 스니퍼 탐지
<대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 Request를 받으면 Response를 전달>
- 이를 이용해 의심이 가는 호스트에 ping을 보내면 되는데, 네트워크에 존재하지 않는MAC 주소를 위장하여 보냄
- 만약 ICMP Echo Reply를 받으면 해당 호스트가 스니핑을 하고 있는 것임

* [그림] Ping을 이용한 스니퍼 탐지



3) ARP를 이용한 스니퍼 탐지
<ping과 유사한 방법으로, 위조된 ARP Request를 보냈을 때 ARP Response가 오면 프러미스큐어스 모드로 설정되어 있는 것>

4) DNS를 이용한 스니퍼 탐지
<일반적으로 스니핑 프로그램은 사용자의 편의를 위해 스니핑한 시스템의 IP 주소에 DNS에 대한 이름 해석 과정(Inverse-DNS lookup)을 수행>
- 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지

5) 유인(Decoy)를 이용한 스니퍼 탐지
<스니핑 공격을 하는 공격자의 주요 목적은 ID와 패스워드의 획득에 있음>
- 가짜 ID와 패스워드를 네트워크에 계속 뿌리고 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지

6) ARP watch를 이용한 스니퍼 탐지
<ARP watch는 MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링>
- 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려주는 툴
- 대부분의 공격 기법이 위조된 ARP를 사용하기 때문에 쉽게 탐지할 수 있음

【학습정리】

1. 스니핑은 전화선이나 UTP(Unshielded Twisted Pair)에 태핑(Tapping)을 해서 전기적 신호를 분석해 정보를 찾아낸 후 전기적 신호를 템페스트(Tempest) 장비를 이용해 분석하는 것을 말한다.

2. 스위치 재밍 공격은 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 저장 용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브처럼 작동하게 만드는 공격을 말한다.

3. SPAN 포트 태핑 공격은 포트 미러링(Port Mirroring)을 이용하여 공격하는 것을 말한다.