스니핑(Sniffing)

유튜브: https://youtu.be/MLOC6v_awKA

사이버보안트랙 1971362 이준희

스니핑 이란?

- **스니핑**
  - sniff의 사전적 의미 : 코를 킁킁거리다
  - 수동적(Passive) 공격 : 공격할 때 아무것도 하지 않아도 충분하기 때문

  - **스니핑**의 개념
    - 도청(Eavesdropping)과 엿듣기가 스니핑
    - 전화선이나 UTP에 탭핑(Tapping)해서 전기 신호를 분석하여 정보를 찾아냄.
    - 전기 신호(Emanation)을 템페스트(Tempest) 장비를 이용해 분석하는 일

그림 6-1
스니핑의 개념

스니핑 이란?

- 쉽게 설명하면, **스니핑**이란 네트워크 상에서 데이터를 가로채어 보는 것을 의미
  - => 데이터가 네트워크를 통과할 때 그 내용을 복사하거나 기록하여 정보를 탈취하는 것

  - 스니핑은 주로 네트워크 보안을 침해하는 데 사용되며, 공격자가 정보를 얻거나 사용자의 개인 정보를 탈취하는 데 사용

  - 일반적으로 스니핑은 악의적인 목적을 가진 공격자가 네트워크 트래픽을 감시하고 정보를 훔치기 위해 사용하는 기술적인 방법

스니핑 공격의 원리

- **정상적인 네트워크 필터링**
  - 네트워크 카드에 인식된 데이터 링크 계층과 네트워크 계층의 정보가 자신의 것과 일 치하지 않는 패킷은 무시

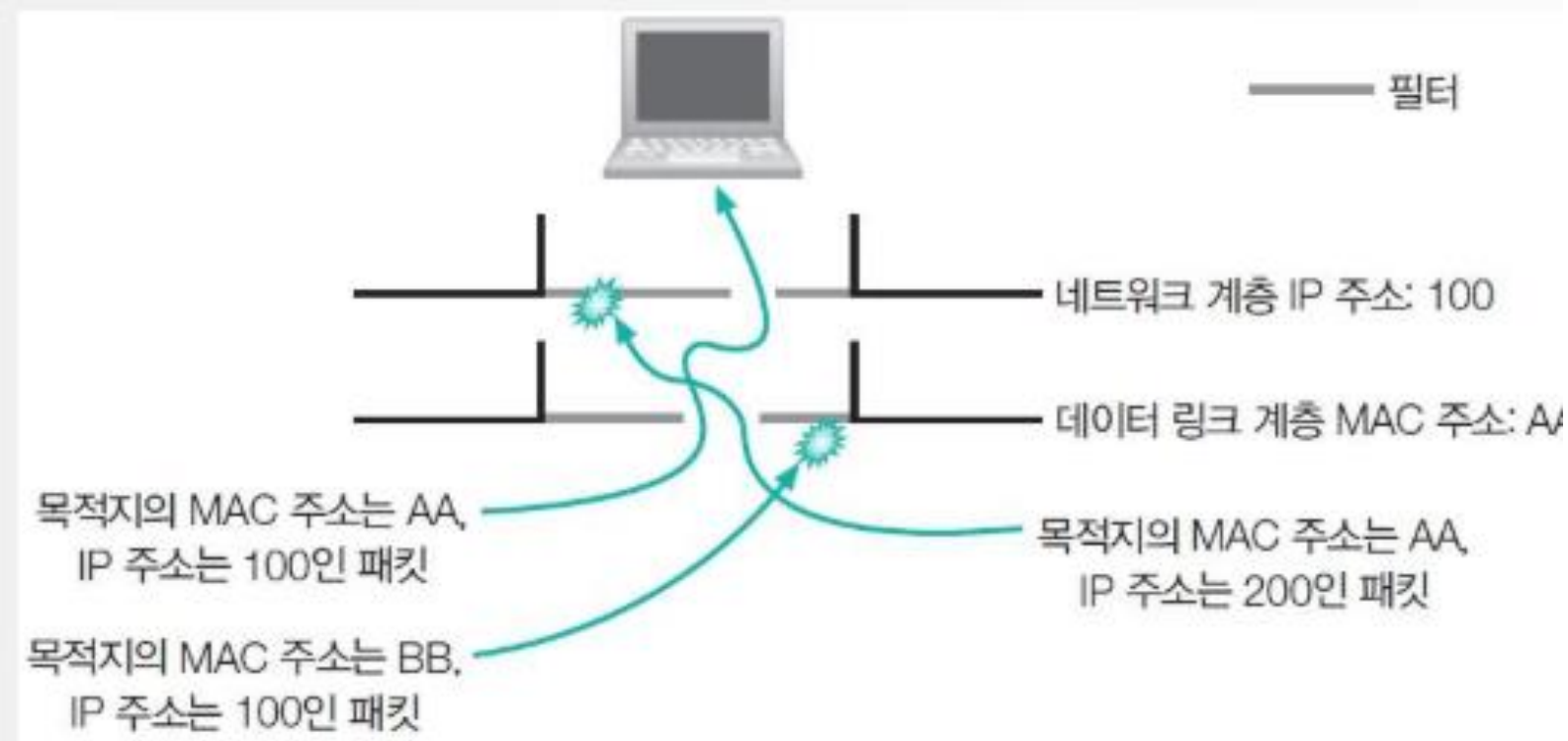

그림 6-2 정상적인 네트워크 필터링의 예

스니핑 공격의 원리

- **네트워크 필터링 해제 상태**의 예
  - 스니핑을 수행하는 공격자는 모든 정보를 볼 수 있어야 하므로 필터링은 방해물일 뿐
  - **프러미스큐어스 모드**: 데이터 링크 계층과 네트워크 계층의 필터링을 해제해 랜 카드나 스니핑이 가능한 상태
    - => 프러미스큐어스 모드 상태에서는 MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨준다

프러미스큐어스 모드(Promiscuous Mode)

- **프러미스큐어스 모드(Promiscuous Mode)**
  - MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨주는 것
  - 리눅스나 유닉스 등의 운영체제에서는 랜 카드에 대한 모드 설정이 가능
  - 윈도우에서는 스니핑을 위한 드라이버를 따로 설치
  - 스니핑을 하려면 좋은 랜 카드가 필요
    - MAC 주소의 고유성 유지
    - 버퍼의 크기가 커서 많은 프레이, 패킷의 저장이 가능
    - 특정 연산을 위한 처리장치 유무

  - **바이패스 모드(Bypass Mode)**
    - 패킷에 대한 분석까지 하드웨어로 구현되어 있는 랜 카드
    - 기가바이트(GByte) 단위의 백본 망에서 스니핑을 하기 위한 장비로 고가임.

스니핑 공격 툴

- **TCP Dump**
  - 리눅스에서 가장 기본이 되는, 하지만 강력한 스니핑 툴
    - ➢ 명령줄 인터페이스를 통해 네트워크 트래픽을 캡처하는 도구
  - 처음에는 네트워크 관리를 위해 개발되었기 때문에 관리자 느낌이 강함.
  - TCP Dump로 획득한 증거 자료는 법적 효력이 있음.

스니핑 공격 툴

- **Fragrouter(프래그라우터)**
  - 스니핑을 보조해주는 툴로, 받은 패킷을 전달하는 역할
  - 스니핑을 하거나 세션을 가로챘을 때 공격자에게 온 패킷을 정상적으로 전달하려면 패킷 릴레이가 반드시 필요함

스니핑 공격 툴

- **DSniff(디스니프)**
  - 스니핑을 위한 다양한 툴이 패키지처럼 만들어진 것
  - 한국계 미국인으로 해커이자 정보보호기술 전문가인 미국 미시건 대학교의 송덕준 교수가 개발
  - 알트보어(Altvore)와 함께 대표적인 스니핑 툴로 알려져 있음
  - 암호화된 계정과 패스워드까지 읽어낼 수 있음.

  - dsniff가 읽어낼 수 있는 패킷

ftp, telnet, http, pop, nntp, imap, snmp, ldap, rlogin, rip, ospf, pptp, ms-chap, nfs, yp/nis+, socks, x11, cvs, IRC, ATM, ICQ, PostageSQL, Citrix ICA, Symantec pcAnywhere, MS SQL, auth, info

스위칭 환경에서의 스니핑

- **스위칭 환경과 스니핑**

  - 스위치는 각 장비의 **MAC 주소**를 확인하여 **포트에 할당**

  - 자신에게 향하지 않은 패킷 외에는 받아볼 수 없어 **스니핑을 막게 됨**
    - 스위치가 스니핑을 막기 위해 만들어진 장비는 아니지만 결과적으로는 저지하는 치명적인 장비가 됨.

ARP 리다이렉트와 ARP 스푸핑

- **ARP 리다이렉트**
  - 공격자가 **자신을 라우터라고 속이는 것**
  - 기본적으로 **2계층 공격**으로, **랜에서 공격**
  - 공격자 자신은 원래 라우터의 **MAC 주소**를 알고 있어야 하며, 받은 모든 패킷은 다시 라우터로 **릴레이**해줘야 함.

  - **ARP 스푸핑**은 **호스트 대 호스트 공격**, ARP 리다이렉트는 랜의 모든 호스트 대 라우터라는 점 외에는 큰 차이가 없음

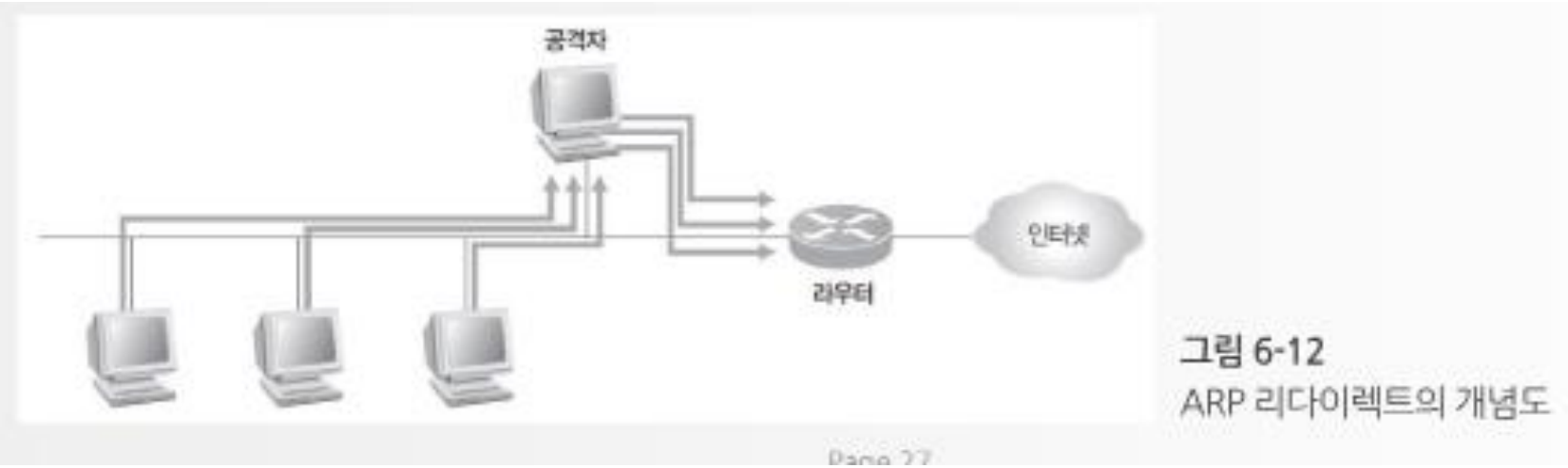

그림 6-12
ARP 리다이렉트의 개념도

ICMP 리다이렉트

- **ICMP 리다이렉트**
  - 공격 대상에게 패킷을 보낸 후 라우터 A에 다시 릴레이시켜 스니핑함.
  - 3계층에서 패킷을 주고받기 때문에 랜이 아니더라도 공격이 가능
  - 최근에는 운영체제에서 ICMP 리다이렉트를 기본적으로 차단함.

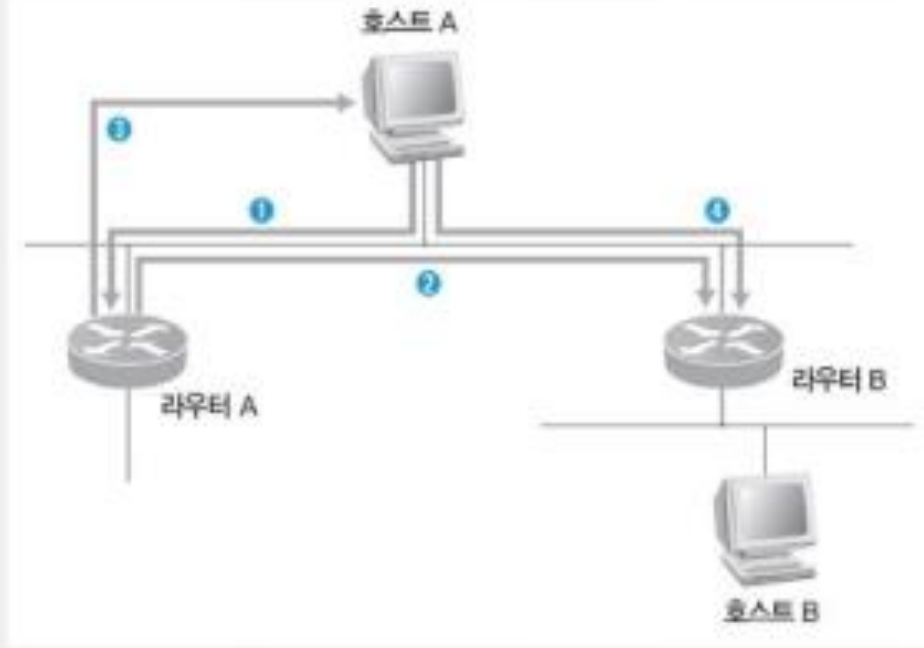

그림 6-19
ICMP 리다이렉트의 개념도

스위치 재밍(Switch Jamming)

- 스위치 재밍(Switch Jamming)

  - **스위치를 직접 공격**
  - MAC 테이블을 위한 캐시 공간에 **버퍼 오버플로우 공격**을 실시
  - 일부 고가의 스위치는 MAC 테이블의 캐시와 연산 장치가 사용하는 캐시가 **독립적으로 나뉘어 있어** 스위치 재밍 공격이 통하지 않음

SPAN 포트 태핑

- **SPAN(Switch Port Analyzer)**
  - 각 포트에 전송되는 데이터를 미러링하는 포트에도 똑같이 보내주는 **포트 미러링(Port Mirroring)**을 이용한 것
  - 주로 **IDS**를 설치할 때 많이 사용
  - SPAN은 주로 시스코에서 사용하는 용어이며, 다른 벤더에서는 'Port Roving' 이라 부르기도 함

  - **태핑**
    - SPAN은 상당히 많은 문제점을 가져서 효과적인 모니터링을 하는데 어려움이 있는데, 이를 해결할 수 있는 것이 태핑
    - 허브와 같이 포트를 모니터링하기 위한 장비
    - Splitter(스플리터)라고 부르기도 함.

스니핑 대응책

- **능동적인 대응책 – 스니퍼 탐지**

(1) ping을 이용한 탐지

- 의심이 가는 호스트에 ping을 보낼 때 **네트워크에 존재하지 않는 MAC 주소를 위장**하여 보냄
- 만약 **ICMP Echo Reply**를 받으면 해당 호스트가 스니핑을 하고 있는 것

(2) ARP를 이용한 탐지

- 위조된 ARP Request를 스니퍼임을 확인하고자 하는 시스템에 보냄
- 대상 시스템이 응답으로 **ARP Response**를 보내면 이를 통해 **프러미스큐어스 모드**로 동작 중인 스니퍼임을 확인

스니핑 대응책

- **능동적인 대응책 – 스니퍼 탐지**

(3) DNS를 이용한 탐지

- 테스트 대상 네트워크로 **Ping Sweep**을 보내고 들어오는 **Inverse-DNS lookup**을 감시

- 일반적으로 스니핑 프로그램은 사용자의 편의를 위하여 스니핑한 시스템의 IP 주소를 보여주지 않고 도메인 네임을 보여주기 위하여 **Inverse-DNS lookup**을 수행하게 된다. 따라서 DNS 트래픽을 감시하여 스니퍼를 탐지할 수도 있다.

- 이 방법은 원격 또는 로컬 네트워크 모두에서 할 수 있는 방법이다. 원격에서 테스트 대상 네트워크로 **Ping sweep**을 보내고, 들어오는 **Inverse-DNS lookup을 감시**하여 스니퍼를 탐지할 수 있다. 로컬에서 할 경우에는 **위조된 IP 주소로 IP datagram을 보내고** 이에 대한 **DNS lookup**이 있는지 감시하여 스니퍼를 탐지할 수 있다.

스니핑 대응책

- **능동적인 대응책 – 스니퍼 탐지**

(4) 유인을 이용한 탐지

➢ 가짜 계정과 패스워드를 뿌려 공격자가 이 가짜 정보로 접속을 시도하면, **접속을 시도하는 시스템을 탐지**

(5) ARP watch를 이용한 탐지

➢초기에 MAC 주소와 IP 주소의 매칭 값을 저장하고 **ARP 트래픽을 모니터링**하여 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려줌.

스니핑 대응책

- **수동적인 대응책 – 암호화**

(1) SSL(Secure Socket Layer)

- 암호화된 웹 서핑을 가능하게 함
- 40비트, 128비트, 256비트 암호화 사용(현재 우리나라 금융 거래 사이트의 대부분은 128 비트 암호화 방법을 사용)

스니핑 대응책

- **수동적인 대응책 – 암호화**

(2) PGP, PEM, S/MIME

- PGP, PEM, S/MIME 모두 **이메일을 전송할 때 사용하는 암호화 방법**

- **PGP** : 내용을 암호화하는 데에 IDEA, IDEA 키와 전자 서명을 암호화하는 데에 RSA(Rivest, Shamir, Addleman) 알고리즘 사용. 기본적으로 ‘ Web of Trust’ 개념 사용

- **PEM** : 공개키 암호화 표준을 따르고, CA에서 키를 관리 데이터 암호화에는 DES-EDE, 키를 위한 암호화 알고리즘에는 RSA, 전자 인증을 위한 해시 함수에는 MD2, MD5 사용

- **S/MIME** : 이메일 표준인 MIME 형식에 암호화 서비스만을 추가한 것 PKCS를 기반으로 만들어져 있으며, 디지털 인증에 X.509를 사용

스니핑 대응책

- **수동적인 대응책 – 암호화**

(3) SSH(Secure Shell)

- 텔넷과 같은 서비스 암호화를 위해 사용하는 것
- OpenSSL 라이브러리가 SSH를 지원
- SSH를 이용한 암호화 프로토콜은 계속 발전하고 있으며 텔넷보다는 훨씬 더 안전

스니핑 대응책

- **수동적인 대응책 – 암호화**

(4) VPN(Virtual Private Network)

- 한 회선을 여러 회사가 공유하여 비용을 절감하려는 목적으로 개발
- 암호화된 트래픽 제공
- VPN을 제공하는 시스템이 해킹을 당할 경우 암호화되기 이전에 데이터가 스니핑이 될 수 있음

Q & A