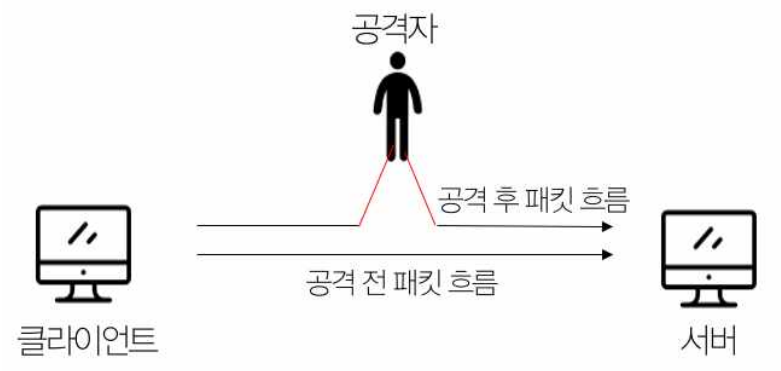
< ARP 스푸핑 및 센서조작 스터디 보고서 >

2022111354 한아림

1. ARP Spoofing 공격 개요

- 정의 및 개요

: 로컬 네트워크(LAN)에서 사용하는 ARP 프로토콜의 허점을 이용하여 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격

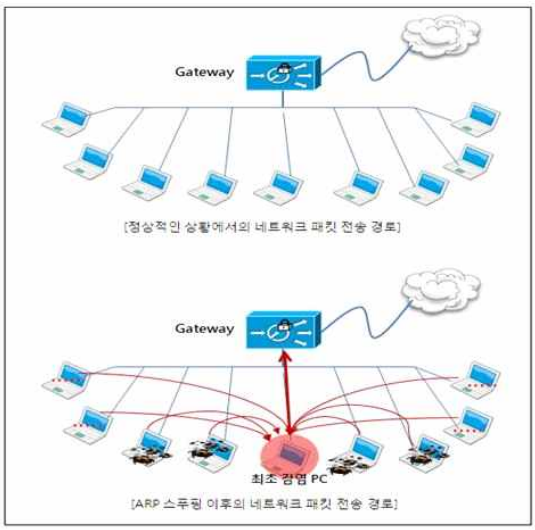


+ IP 주소와 이에 해당하는 물리적 네트워크 주소 정보는 각 IP 호스트의 ARP 캐시라 불리는 메모리에 테이블 형태로 저장된 후 패킷 전송 시 사용

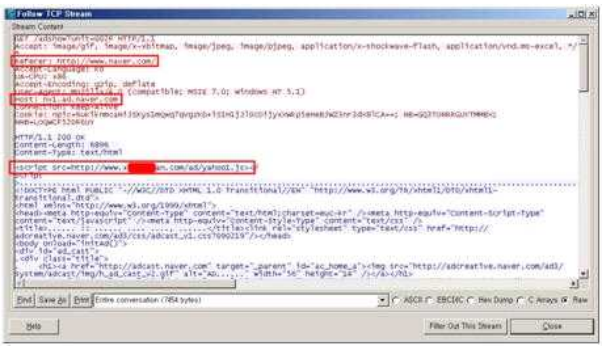
+ ARP 스푸핑에서의 ARP는 Address Resolution Protocol의 약자

+ 명령 프롬포트에서 arp -a 명령어를 통해 맥과 아이피 주소 확인 가능 vs 만일 리눅스 환경에서 실습할 경우는 arp 명령어를 사용

+ 여기서 MAC란 랜 카드의 고유한 주소를 의미하며, 단 하나의 고유한 주소를 부여하여 통신을 가능하게 한 일종의 하드웨어 주소이다.
--> 의미 참고 : https://whatismyipaddress.com/mac-address



+ 네트워크 패킷과 APR 패킷 상세
--> 악성코드 전파로 악성코드에 감염된 시스템에서의 패킷 생성 시 추가적인 피해 발생 가능



+ ARP 스푸핑 공격과 기존의 타 공격들의 대표적인 차이점

--> 해당 네트워크에 연결된 웹 서버들이 직접적으로 해킹을 당하지 않은 상태여도(직접 해킹 당한 상태 포함) 이 웹 서버들을 방문하는 모든 취약한 사용자들이 악성코드 등에 감염되는 피해를 야기한다는 것

- 공격 진행 과정

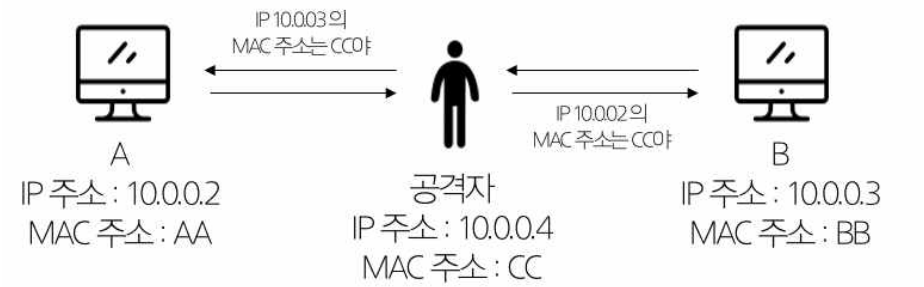
a. 임의의 공격자가 공격 대상 A에게 자신의 MAC 주소를 B의 MAC 주소인 것처럼 위장한다. 즉 이 과정에서 A는 공격자의 MAC 주소를 B의 주소라고 착각하게 된다.

b. 공격자가 반대로 B에게 자신의 MAC 주소를 A의 MAC 주소인 것처럼 속이는 과정을 진행한다. 이 과정에서 과정 a와 마찬가지로 B는 공격자의 MAC 주소를 A의 주소라고 인식하게 된다.

c. A가 공격자에게 메시지를 전송하면 공격자가 그 메시지를 수령한 후 B에게 전송하는 과정을 거친다.

d. 반대로 B가 공격자에게 메시지를 전송하면 공격자가 그 메시지를 수령하여 A에게 전달한다.

e. 위와 같은 과정을 반복하며 정상적인 통신이 진행되고, 공격자는 A와 B사이에 전달되는 메시지의 내용을 모두 알 수 있게 된다.



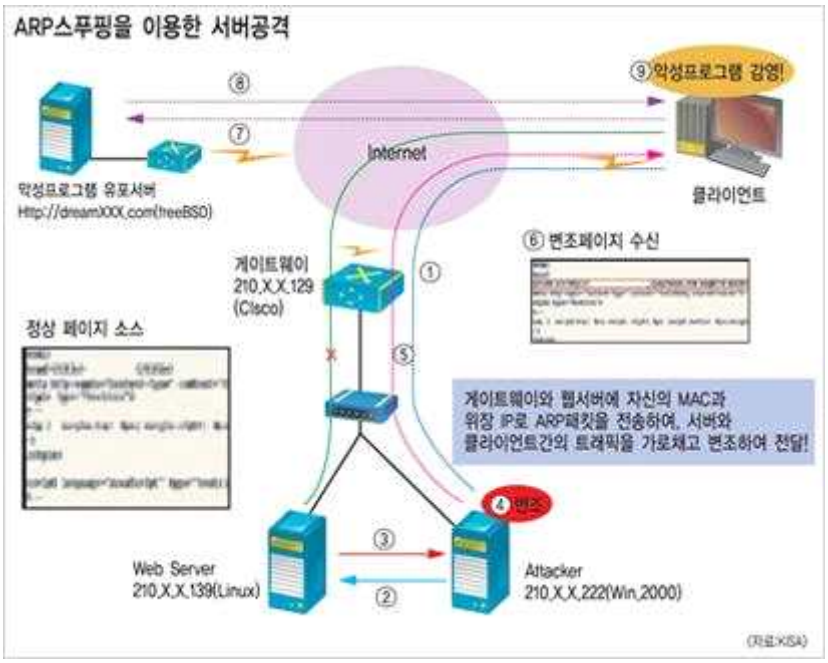
- **공격 발생 원인과 예방법**

: 기존에 쓰이는 대부분의 MAC 주소는 동적으로 유지되는데, 이런 유동적인 MAC 주소의 특성을 이용한 공격 빈도가 증가하고 있음(APR 스푸핑과 연관이 높음)

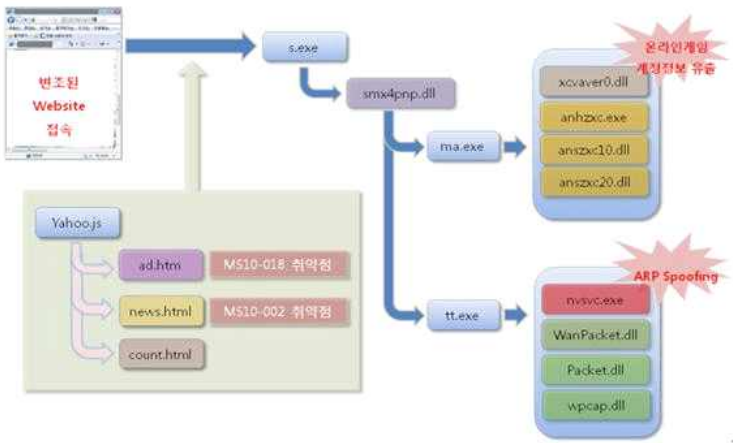
--> 공격에서의 주요 요건인 MAC 주소가 정적으로 사용되는 경우 ARP Spoofing 공격을 사전에 예방할 수 있음

+ 추가적으로 공격에 취약한 유저의 PC들은 웹 서버들이 연동되는 네트워크에 자동적으로 연동되지 않도록 관리해야 함.

--> 주된 공격 타깃은 보안 패치가 미설치된 PC이니 패치의 실시간 업데이트도 필수적인 요소



- **ARP 스푸핑 악성코드의 구조 상세**



a. 사용자가 보안에 취약한 웹 사이트에 접속

b. 악성코드인 yahoo.js 파일이 실행

c. 이어 다른 악성코드가 다운로드 및 실행

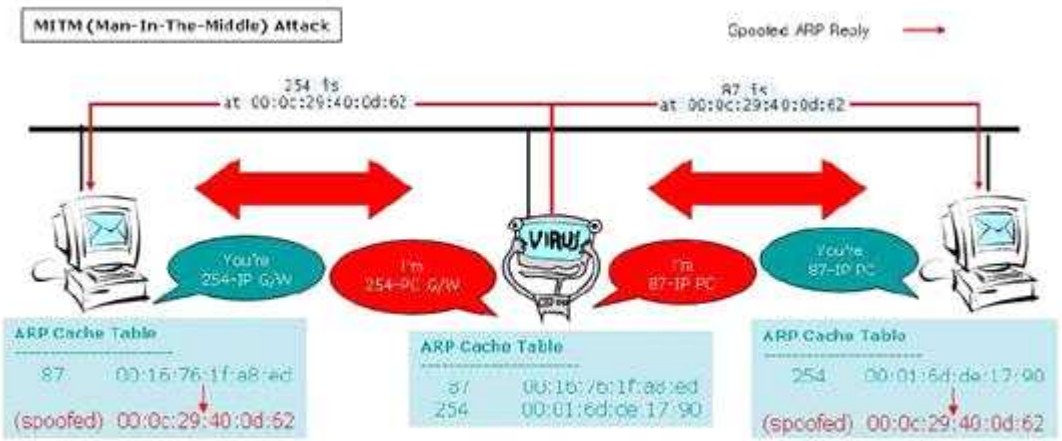
d. Yahoo.js 파일 코드 해독 --> ad.htm, news.html, count.html 파일로 다시 접근

e. Ad.htm 파일 실행 (위 경우에는 MS 인터넷 익스플로러의 MS10-018 취약점 이용)

f. News.html 파일은 MS10-002 취약점을 이용해 s.exe 파일 다운로드 및 실행

g. s.exe 파일이 C:\Windows\System32 폴더에 xcvarver0.dll 파일 생성

- ARP 스푸핑 공격의 위험성 (중간자 공격)



: ARP 스푸핑 공격은 스푸핑 공격 기법을 이용한 악성코드가 위협적이기에 문제가 된다. 스푸핑 공격 기법을 이용하여 만들어진 악성코드는 데이터를 탈취하는 기능을 가지고 있는데, 이 때문에 위험도가 높아진다.

: 일반적으로 ARP 스푸핑 기법은 MITM(Man-In-The-Middle) 공격을 수반하여 동일 네트워크 상에서 공격 대상 시스템에 오고 가는 통신 내용을 스니핑하기 위한 목적으로 이용됨.

--> 위의 공격 진행 방식에 기반, 공격자는 이 MITM 공격을 이용하여 전송되는 데이터를 스니핑할 수 있고, 그로 인해 중요한 정보를 획득할 수 있을 뿐만 아니라 데이터를 삽입, 수정, 삭제하는 등 변조 작업도 수행할 수 있음

2. 시나리오 기술

- 시나리오 A_차량 목적지 및 위치 조작 (센서 조작 응용)

공격자	C
공격 대상 IoT 기기	A
기존 목적지 or 정상 위치	D
조작 목적지 or 변조 위치	N

시나리오에서의 설정이 위 표를 따를 때, 목적지 D를 향해 운행 중인 자율주행자동차 A에 대해 외부의 공격자 C가 A의 센서(목적지 탐지 및 설정 센서)르 조작하여 새로운 목적지인 N을 본래 목적지로 인식하도록 만듦.

--> 시나리오 개요에서는 조작할 대상이 되는 데이터를 차량의 목적지로 설정하였으나, 만일 목적지가 아닌 현 위치 데이터를 조작 대상으로 설정할 경우에도 변하는 점은 X

+ 위 시나리오의 경우 공격자는 외부 PC에 위치하도록 함. 공격 툴은 크게 결과에 영향을 주지 않으나, 속도를 고려했을 때 버프스위트 권장

+ 아이디어 참고
https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=netandhi&logNo=220443639500

- 시나리오 B_차량 상태 및 산하 데이터 조작 (센서 조작 응용)

공격자	C
공격 대상 IoT 기기	A
정상적인 상태	O
변조된 상태	K

시나리오에서의 설정이 위 표를 따를 때, 정상 운행 중인 자율주행자동차 A에 대해 외부에 위치한 공격자 C가 A에 탑재된 계기판 데이터 및 차량 속도를 조작하여 차량을 공격하는 것을 가정

+ 위 시나리오의 경우 시나리오 1과 동일하게 공격자는 외부 PC에 위치하도록 하며, 공격 툴은 마찬가지로 버프스위트를 사용

+ 아이디어 참고
https://www.boannews.com/media/view.asp?idx=109385

3. 관련 용어 및 개념 정리

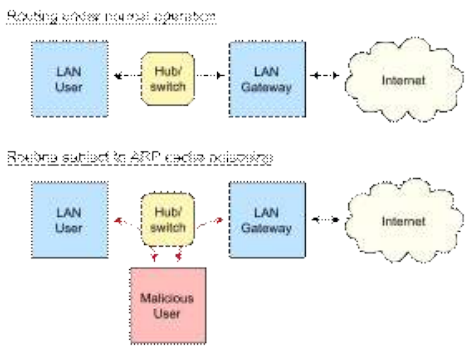
- **ARP Protocol (= ARP 프로토콜)**

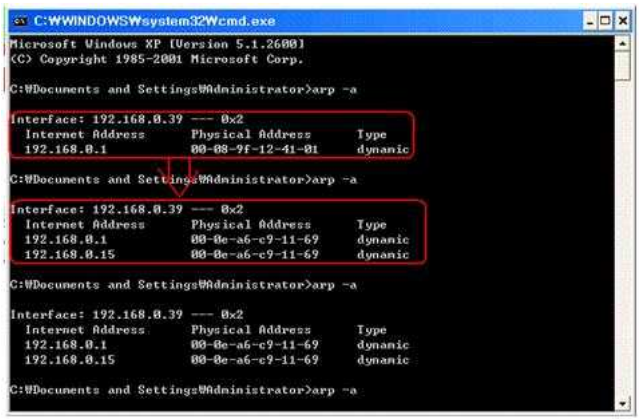
: Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.

--> 요약 : SW적으로 할당된 논리 주소를 실제적 물리 주소로 바꾸어주는 역할을 하는 주소 해석 프로토콜

+ ARP의 종류

ARP	IP를 기반으로 MAC 주소 획득
RARP	MAC 주소를 기반으로 IP 주소 획득
Gratuitous ARP	IP 충돌 감지 및 GW 이중화에 사용
Proxy ARP	IP 대역은 동일하나 물리적으로 분리된 네트워크 통신을 위해 사용





- **스푸핑(spoofing)**

: Spoofing is the act of disguising a communication from an unknown source as being from a known,

--> 속임 기술을 이용한 공격 기법의 총칭

+ 스푸핑의 'Spoof'는 '속여먹다, 골탕먹이다'라는 의미를 가지며, 공격 대상으로부터 갈취할 시스템의 권한은 DNS 주소, MAC 주소, IP 주소 등 매우 다양하다.

- MiTm 공격

: 공격자가 2명의 사용자 사이에 자리잡고 대화를 엿듣거나 데이터 전송을 가로채는 공격으로, 일반적인 사이버공격에 해당하며 말 그대로 공격자가 2개 당사자 사이에 '말없는 관찰자'이자 '조작자'로 끼어들어 통신 및 메시지 교환 내용을 가로채는 양상을 보임

--> 중간자 공격에는 다양한 유형이 존재하는데, 대표적인 유형은 아래와 같음

이메일 탈취	와이파이 도청	DNS 스푸핑
IP 스푸핑	세션 탈취	불량 엑세스 포인트
HTTPS 스푸핑	SSL 탈취	브라우저 쿠키 탈취

+ MiTm은 중간자 공격이라고도 불리우기도 하며, ARP 스푸핑을 유형 중 하나로 가지고 있음.

+ 중간자 공격은 크게 VPN을 사용하거나, 강력한 인증 프로토콜을 사용하거나 통신 과정에서 종단간 암호화를 실시함으로써 예방이 가능하다.

- 프로토콜 (= Protocol)

: In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers.

--> 컴퓨터나 원거리 통신 장비 사이에서 메시지를 주고받는 양식과 규칙의 체계로, 통식 규약 및 약속을 의미함

: 프로토콜은 기본적으로 3가지 요소로 이루어짐

a. 구문(Syntax) = 전송하고자 하는 데이터의 형식 및 신호 레벨, Coding 등을 규정

b. 의미(Semantics) = 두 기기 간 효율적이고 정확한 정보 전송을 위한 협조 사항과 오류 관리를 위한 제어 정보 규정

c. 시간(TIming) = 두 기기 간의 통신 속도 및 메시지의 순서 제어 등을 규정하는 요소

: 프로토콜의 종류 및 계층

응용	HTTP, FTP, SMTP
표현	ASCII, MIDI, MPEG
세션	SAP, SDP, NWLink
전송	TCP, UDP, SPX
네트워크	IP, IPX
데이터 링크	FDDI, Ethernet, Apple Talk

+ 프로토콜은 캡슐화, 연결 제어, 순서 결정, 주소 설정, 흐름 제어, 오류 제어, 단편화, 재합성, 동기화, 다중화, 전송 서비스 등의 기능을 수행함

4. 참고 자료

- 디지털타임스_ARP 스푸핑 공격과 대응
http://www.dt.co.kr/contents.html?article_no=2007120602011860713002

- imperva_ARP Spoofing
https://www.imperva.com/learn/application-security/arp-spoofing/

- Forcepoint_What is Spoofing?
https://www.forcepoint.com/cyber-edu/spoofing

- Ahnlab_[White Paper] ARP Spoofing을 통해 전파되는 악성코드 차단과 해결책
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=16777

- Britannica_protocol (computer science)
https://www.britannica.com/technology/protocol-computer-science

-appsealing_중간자(MiTm) 공격: MiTm 공격의 종류와 예방 전략
https://www.appsealing.com/kr/%EC%A4%91%EA%B0%84%EC%9E%90-%EA%B3%B5%EA%B2%A9/

-데일리시큐_한국 자동차 센서 교란 공격에 성공...후방감지센서 조작 가능해
https://www.dailysecu.com/news/articleView.html?idxno=16945

- Academy_other threats
https://www.avast.com/c-spoofing#:~:text=Spoofing%20is%20a%20cybercrime%20that,to%20access%20sensitive%20personal%20information.

- CLOUDFLARE_What is a protocol? | Network protocol definition
https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/

- ROOT INSTALL_A List of ARP Spoofing Tools
https://www.rootinstall.com/tutorial/a-list-of-arp-spoofing-tools/

- GitHub - alandau_arpspoof
https://github.com/alandau/arpspoof

- CYBR_Windows 10 ARP Spoofing with Ettercap and Wireshark
https://cybr.com/cybersecurity-fundamentals-archives/windows-10-arp-spoofing-with-ettercap-and-wireshark/