익스플로잇 시나리오 & 스터디 보고서

ARP 스푸핑(ARP spoofing)

근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 **상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법**

데이터 링크 상의 프로토콜인 ARP 프로토콜을 이용하기 때문에 근거리상의 통신에서만 사용할 수 있는 공격

이 기법 사용한 공격의 경우 사용자가 **자신이 공격당하고 있다는 사실을 확인하기 힘들다**.

과정

로컬 영역 네트워크에서 각 장비의 IP 주소와 MAC 주소간의 대응은 ARP 프로토콜을 통해 이루어진다.

1. 공격자가 의도적으로 특정 IP 주소와 자신의 MAC 주소로 대응하는 ARP 메시지를 발송
2. 그 메시지를 받은 장비는 IP 주소를 공격자 MAC 주소로 인식
3. 해당 IP 주소로 보낼 패킷을 공격자로 전송
4. 이때 공격자는 그 패킷을 원하는 대로 변조, 원래 목적지 MAC 주소로 발송하는 공격도 가능

흔히 사용되는 공격 방식은 **게이트웨이 IP를 스푸핑**하는 것으로, 이 경우 외부로 전송되는 모든 패킷이 공격자에 의해 가로채거나 변조될 수 있다. 또는, 두 노드에 각각 ARP 스푸핑을 하여 두 장비의 통신을 중간에서 조작하는 기법도 자주 사용된다.

은닉성

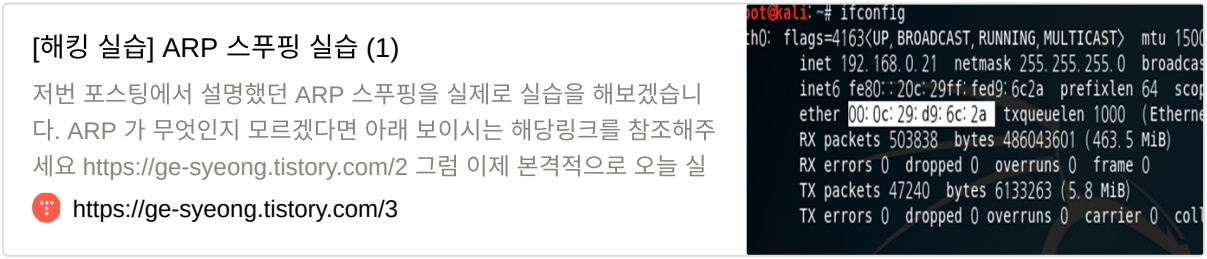
와이어샤크와 같은 패킷 감지 프로그램 이용해 주기적으로 자신의 주소가 아님에도 불구하고 ARP신호를 보내는 패킷 확인 가능

방어 방법 : 정적 ARP 엔트리 사용

로컬 방식에서 사용되는 공격 방식이기 때문에, 로컬 ARP 캐시를 정적으로 정의 가능

—> 이 경우 ARP 신호를 받으면 자신의 ARP테이블을 먼저 확인하고, Static(정적)으로 입력된 MAC주소에 대해서는 갱신하지 않는다.

ARP 스푸핑을 확인하는 소프트웨어는 ARP 응답을 상호 확인하는 방법이나, 특별한 형식의 인증서를 사용한다. 인증되지 않은 ARP 응답은 차단



- 우분투, 칼리, 윈도우 환경에서 실습

아두이노 취약점을 이용한 센서값 조작

소스코드가 호스트 컴퓨터에서 빌드되면서 실행 가능한 Hex 코드가 임시로 저장되며 이를 이용하여
업로딩이 이루어진다. Windows 환경에서 실행된 아두이노 IDE의 경우 임시파일이 저장되는 경로는

Windows 운영체제의 사용자 임시 디렉터리(예: C:\Users\사용자명\AppData\Local\Temp)에 “프로젝트 명칭의 알파벳명칭+임시번호.tmp” 라는 이름의 디렉터리가 임시파일이 저장되는 위치다

이와 같이 저장되는 Hex 코드에 대한 조작을 통하여 공격자가 원하는 내용의 실행코드를 아두이노 보드에 업로드 시킬 수 있는 취약성

analogRead()는 아두이노 보드의 아날로그 핀으로부터 입력받는 값을 처리하는 함수

analogRead()함수는 5가지 종류의 레지스터를 이용하여 데이터를 계측

아날로그 센서로부터 입력되는 ADCL, ADCH 두 개의 레지스터 값을 조작하게 되면 아두이노 보드는
센서를 통해 입력된 습도, 조도, 고도 등의 환경 정보를 오인식하여 잘못된 처리를 수행

[IDE 모니터링] 기능을 수행하는 Dll_injection.exe 파일

아두이노 IDE에서 실행되고 있는 Arduino_builder.exe에 의해서 실행되는 프로세스를 실시간으로
모니터링한다. 이를 통해 아두이노 프로그램이 컴파일이 실행되는 순간을 알아낼 수 있다.

[임시파일 변조] 기능을 수행하는 d.exe 파일

아두이노 프로그램이 컴파일되어 호스트컴퓨터에 임시로 생성된 wiring_analog.c.o 파일을 변조analogRead()함수의 ADCH와 ADCL 레지스터의 값을 “0xFF”로 초기화

이를 통해 임시파일의 레지시터 값 조작이 가능함을 보여준다.

- spoofing, 센서값 조작 공격 시나리오 구성 → 러프하게 1-2개

  센서값 조작 공격 시나리오 : 물체와의 거리를 인식할 수 있는 초음파 센서의 값을 공격자가 조작하여 자율주행 자동차가 장애물을 인지하지 못하고 충돌 유발

  arp spoofing 시나리오 : 위 센서값 조작으로 충돌 발생 후(충격 감지 센서) 사고 발생 메시지를 전송하는 패킷을 조작하여 관리 서버에서 사고 발생 사실을 인지하지 못하도록