23.01.10 ARP스푸핑 스터디 &시나리오

1. ARP spoofing(네트워크), 취약점으로 센서값 조작(기기단) 스터디 진행

▼ ARP spoofing

- 근거리 통신망(LAN)에서 주소 결정 프로토콜(Address Resolution Protocol, ARP) 메시지를 이용해 **상대방의 데이터 패킷을 중간에서 가로채는** 일종의 중간자 공격(MITM) 기법

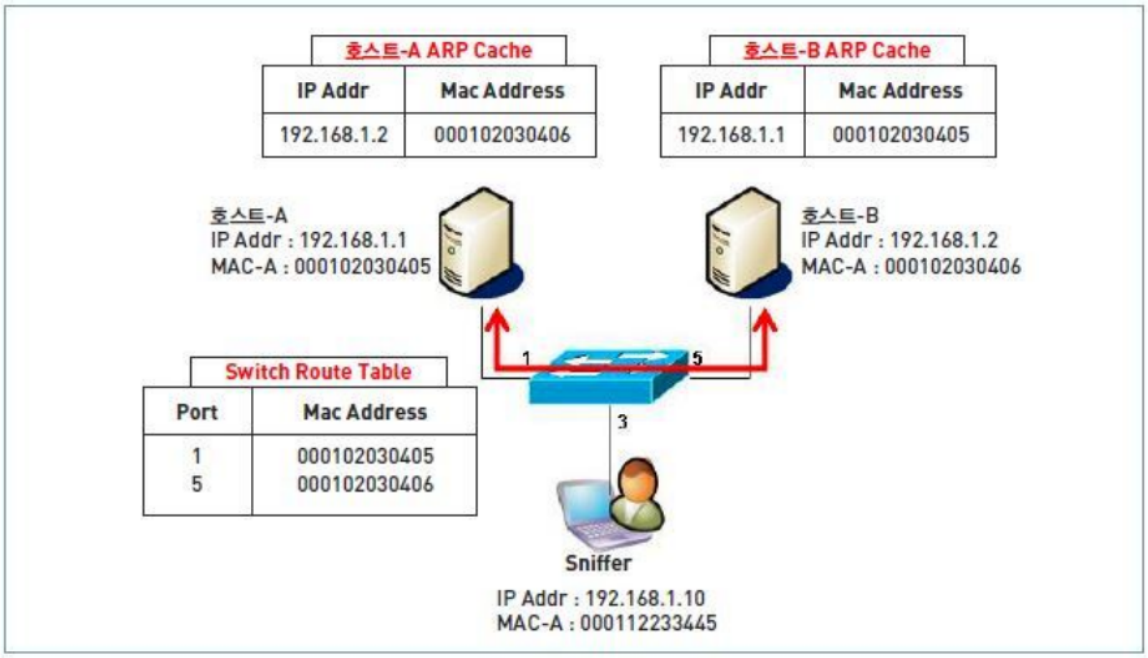
  → A와 B가 대화하는 것을 C가 엿듯는 것. 이것을 통해 사용자가 인터넷에서 무엇을 하는지 알 수 있음.

  - 네트워크에 속한 모든 기기는 게이트웨이를 통과해야 하는데, **이때 해커가 자신을 게이트웨이라고 속이는 것**
  - 해커는 게이트웨이를 지나는 모든 패킷을 보게 되는 것이다. 그리고 패킷을 정상적인 게이트웨이로 보내준다면, 정상적인 통신이 가능하기 때문에 클라이언트는 자신이 감청당하고 있는 사실을 인지하지 못한다.
  - ARP란?

    실질적인 데이터 이동은 IP 주소를 사용하는 L3단이 아닌 MAC 주소를 사용하는 L2단을 거쳐 발생한다. ARP란 **이때 IP 주소와 MAC 주소를 이어주는 프로토콜**.

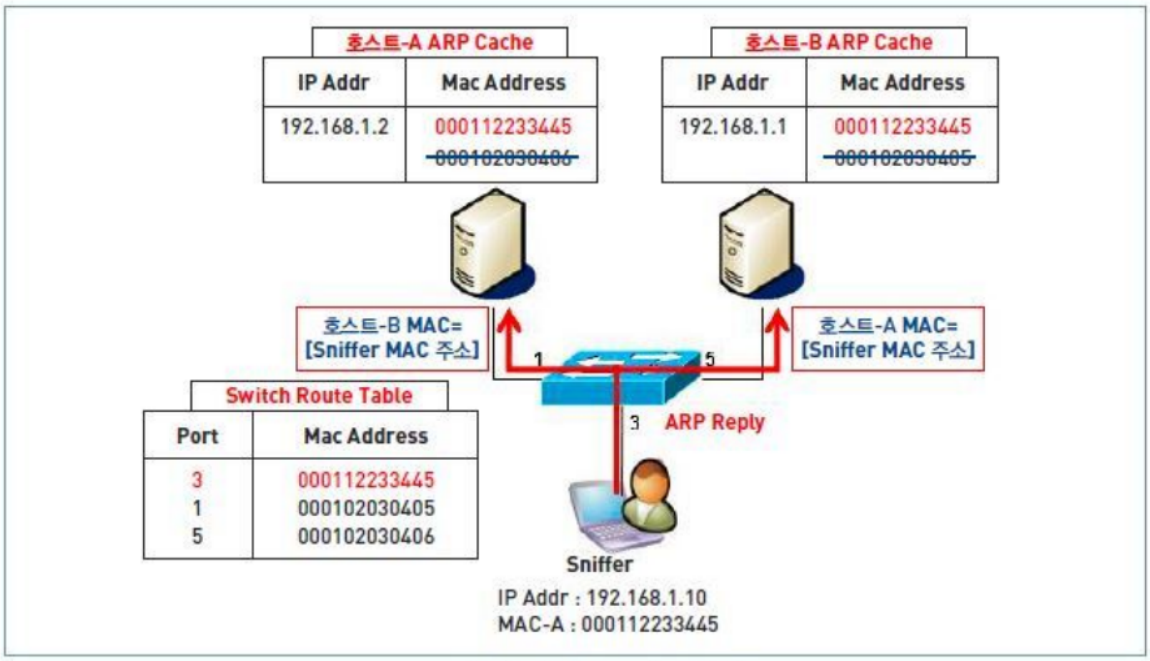
    ARP 스푸핑은 이 ARP의 허점을 이용해 클라이언트에게 게이트웨이의 MAC 주소가 공격자의 MAC 주소라고 알리는 것

▼ 정상적인 통신 & ARP스푸핑 비교



(그림) 정상적인 통신

- 정상적인 통신이라면 ARP테이블에 MAC주소가 제대로 기록되지만 ARP Spoofing공격을 하게 되면 ARP테이블이 잘못된 것을 거르지 못함.
  ARP 프로토콜은 인증을 요구하는 프로토콜이 아니기 때문에 쉽게 테이블에 업데이트를 시킬 수 있음.
- 스니퍼는 계속해서 cache정보가 사라지기 전에 변조된 ARP Reply를 지속적으로 보내고, 결국 MAC table 에는 계속해서 변조된 주소가 유지
- 공격이 성공시 두 호스트는 서로의 MAC주소를 변조된 MAC주소로 인식하기 때문에 모든 트래픽을 스니퍼에게 전달하고 스니퍼는 두 호스트로부터 정보를 도청 가능하며, 재전송, 캡쳐까지도 가능하게 된다.



(그림) ARP Spoofing 공격

- ARP 스푸핑 실습

  ▼ 실습 환경

  사용 툴: Ettercap (0.8.3.1), Wireshark(테스트 용도)

  - **공격자**

    OS: Kali-Linux-2021.2-vmware-amd64

    공격자 IP 주소: 192.168.50.253

    공격자 MAC 주소: 00:0c:29:XX:XX:XX

  - **클라이언트**

    OS: macOS Big Sur 11.2.3

    클라이언트 IP 주소: 192.168.50.173

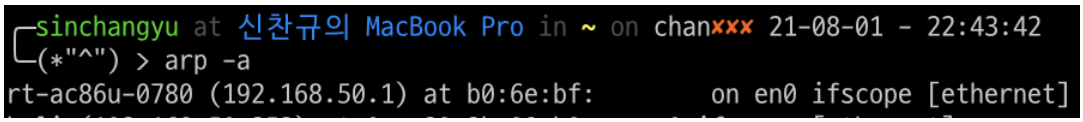
  - **게이트웨이**

    게이트웨이 IP 주소: 192.168.50.1

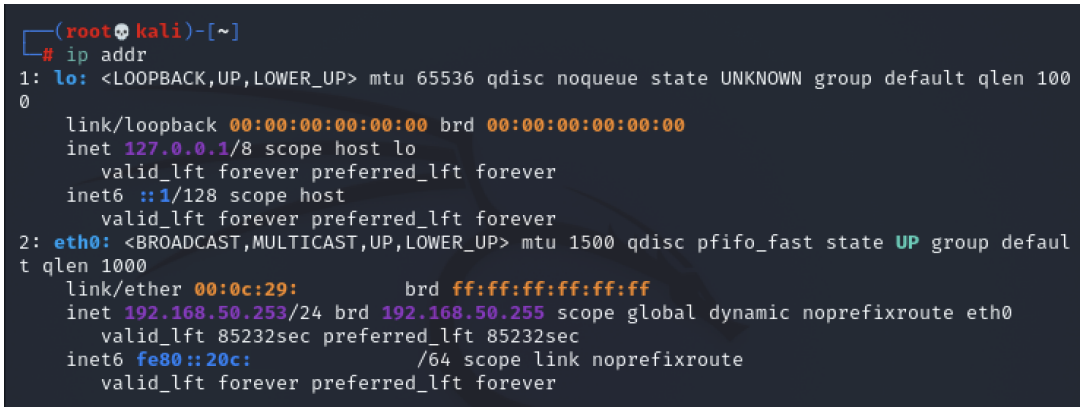
    게이트웨이 MAC 주소: b0:6e:bf:XX:XX:XX

▼ 실습 과정

1. 클라이언트의 터미널에서 `arp -a` 로 현재 게이트웨이 MAC 주소를 확인한다.현재 MAC 주소는 b0:6e:bf:XX:XX:XX 이다.



1. Kali Linux에서 `ip addr` 로 Kali Linux의 MAC 주소를 확인한다.Kali Linux의 MAC 주소는 00:0c:29:XX:XX:XX 이다.

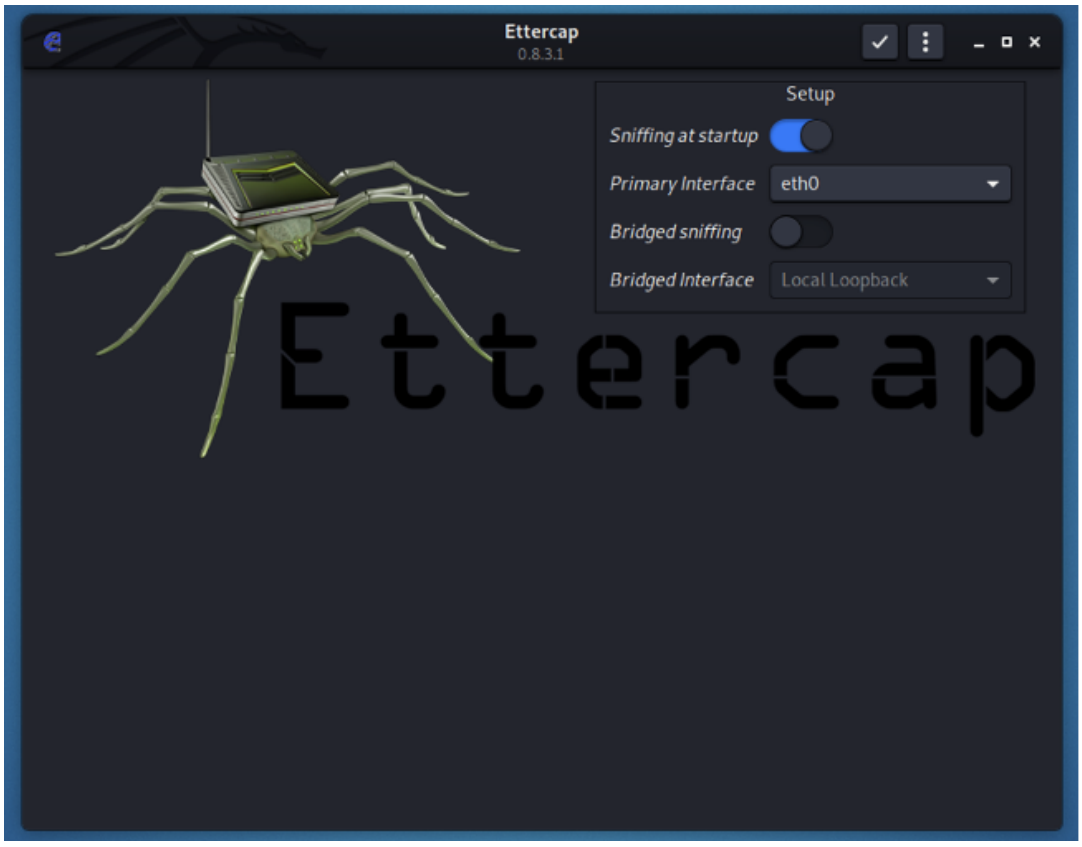


2. `vi /etc/ettercap/etter.conf` 로 `etter.conf` 를 수정한다.ettercap이 sudo 권환으로 실행될 수 있도록 `ec_uid=0`, `ec_gid=0` 으로 수정한다.

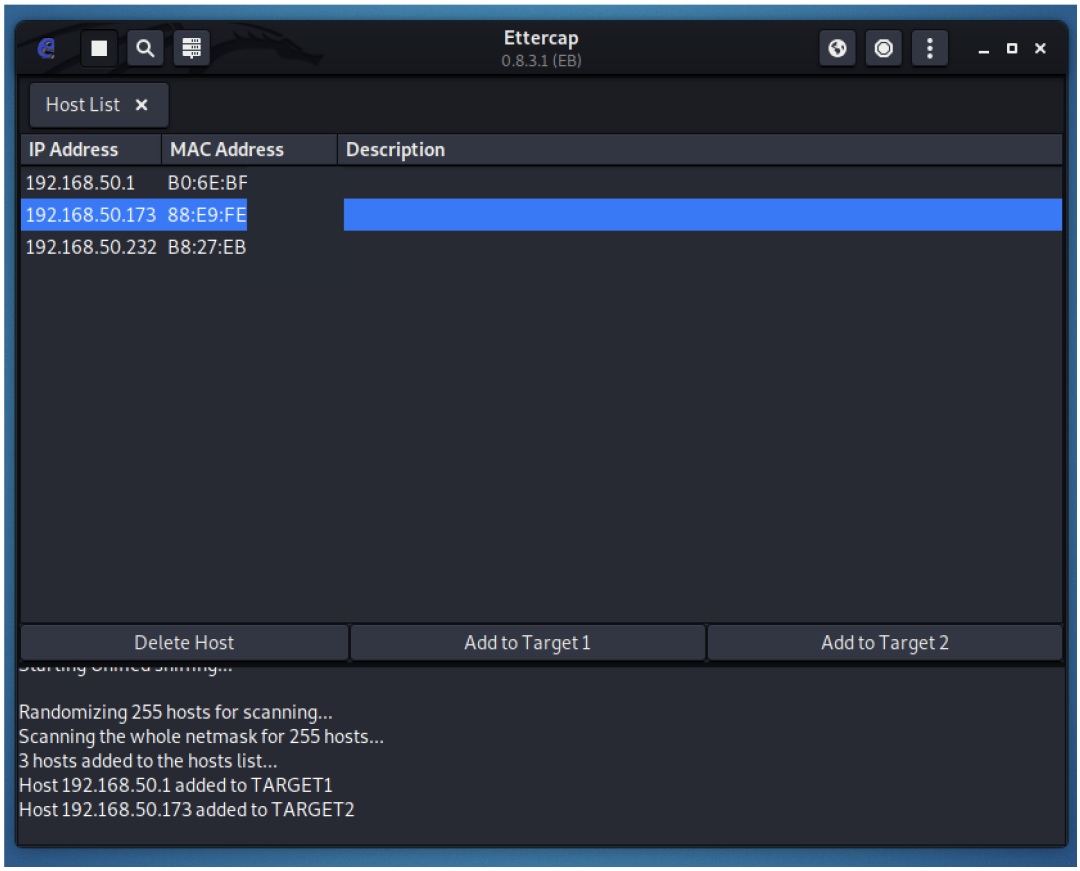
```
#############################################################################
#                                                                           #
#  ettercap -- etter.conf -- configuration file                             #
#                                                                           #
#  Copyright (C) ALoR & NaGA                                                #
#                                                                           #
#  This program is free software; you can redistribute it and/or modify     #
#  it under the terms of the GNU General Public License as published by     #
#  the Free Software Foundation; either version 2 of the License, or        #
#  (at your option) any later version.                                      #
#                                                                           #
#                                                                           #
#############################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default
```

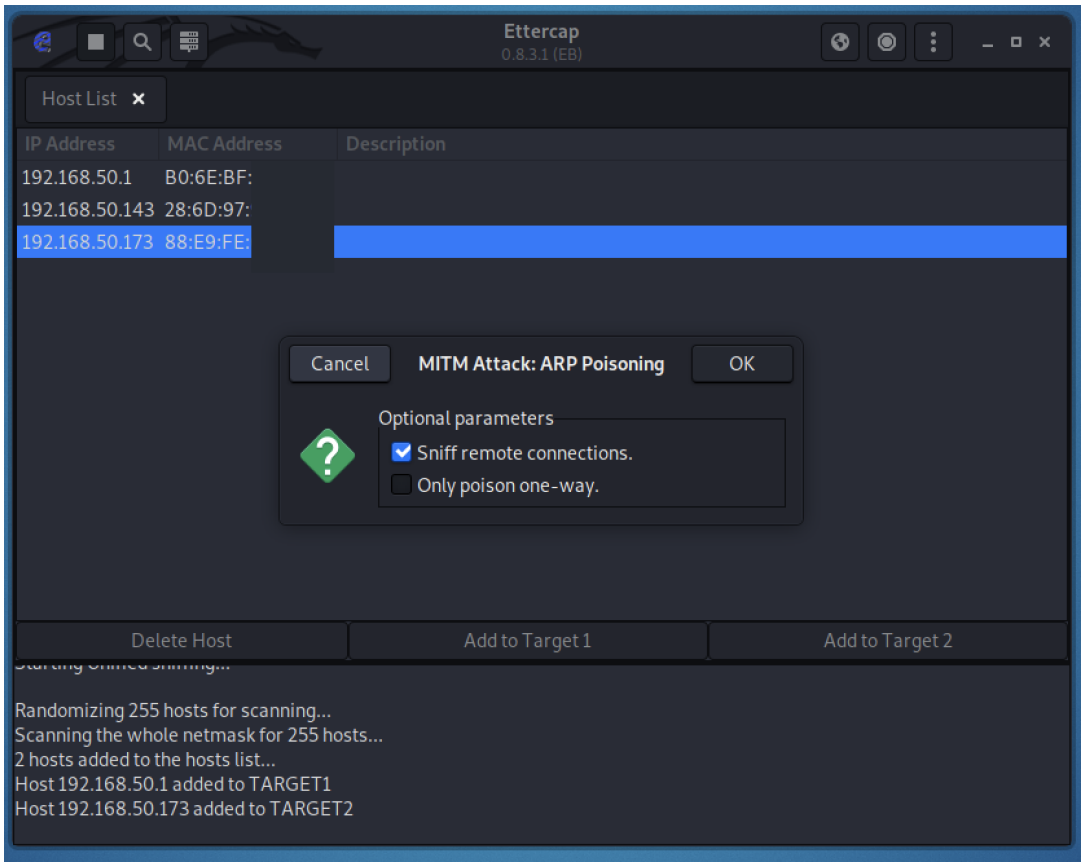
3. `ettercap -G` 로 ettercap을 실행한다.Primary Interface는 eth0으로 설정 후 체크박스를 누른다.



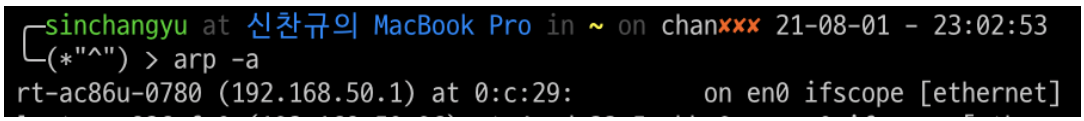
4. `Ctrl + S` 로 Host Scan을 하고, `Ctrl + H` 로 Hosts List를 연다. `Add to Target` 로 게이트웨이는 Target 1, 클라이언트는 Target 2로 설정한다.



5. 지구본 버튼을 눌러 `MITM` -> `ARP Poisoning`...에서 `Sniff remote connections.` 만 체크하고 `OK` 를 누른다.

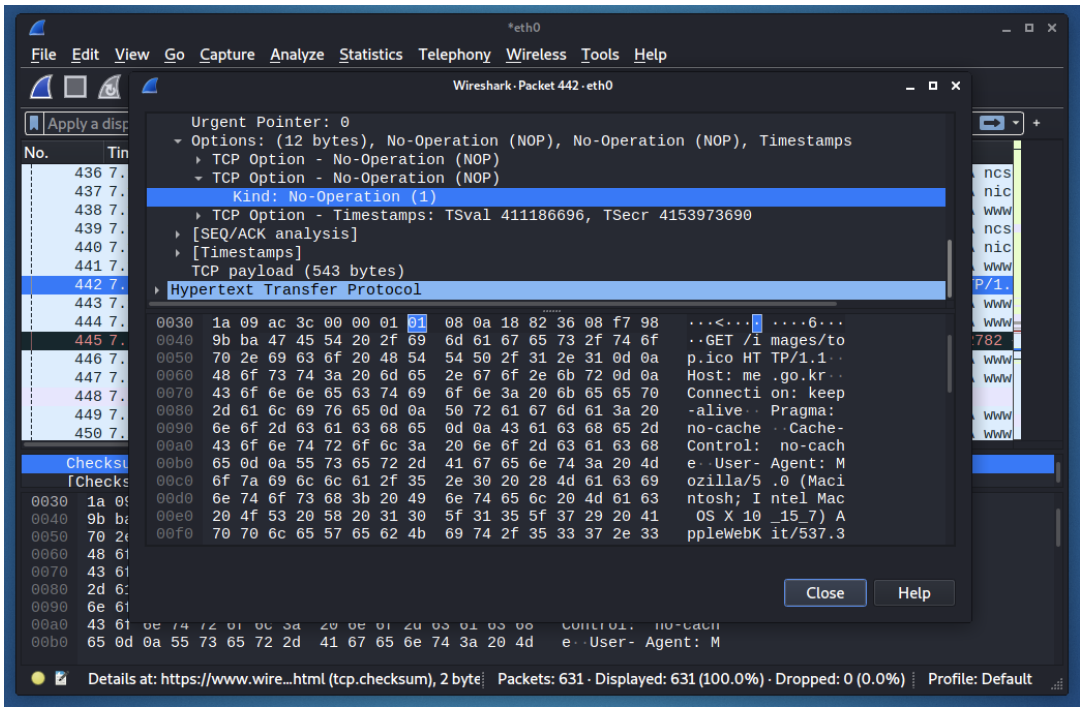


이렇게 되면 ARP 스푸핑이 이루어지게 된다.



클라이언트에서 `arp -a` 로 게이트웨이의 MAC 주소를 확인해보면 Kali Linux의 MAC 주소로 변한 것을 확인 가능

테스트를 위해, 클라이언트에서 http 프로토콜을 사용하는환경부홈페이지에 접속하고 Kali Linux에서 Wireshark로 패킷을 분석



ARP 스푸핑이 성공적으로 이루어진 것을 확인할 수 있다.

▼ 대책

- 중요한 정보는 SSL 프로토콜을 통해 **암호화 통신**한다.
- `arp -s [IP 주소] [MAC 주소]` 로 ARP 캐시 테이블을 **static**으로 구성한다.

[보안] ARP 스푸핑이란?

ARP 스푸핑이 뭘까? 우리의 친구 위키백과에 물어보자. ARP 스푸핑(spoofing)이란, 근거리 통신망(LAN)에서 주소 결정 프로토콜(Address Resolution Protocol, ARP) 메시지를 이용해 상대방의 데

https://velog.io/@scv1702/%EB%B3%B4%EC%95%88-ARP-%EC%8A%A4%ED%91%B8%ED%95%91%EC%9D%B4%EB%9E%80

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

- 시나리오1

  네비게이션으로 목적지가 설정된 자율주행 자동차가 이동하는 경우, 공격자가 자율주행 자동차의 목적지를 해킹한 뒤에 이를 조작하는 시나리오

- 시나리오2

  자율주행자동차 A

  네비게이션 B

  - A와 B가 통신하는 중간에 공격자가 끼어들어 둘의 통신을 읽은 뒤에 중간자 공격을 통해 A로 B에 입력된 목적지가 아닌 다른 목적지를 향하도록 한다.
  - 또는 A와 B가 통신하는 것을 읽은 뒤에 위치 정보를 유출한다.