OpenWrt를 활용한 ARP Spoofing IDS

IDSs_b

빅데이터 전공 20175337 정연선

목차

프로젝트 개요

- 동일한 WLAN(Wireless Local Area Network) 안에 있는 모든 디바이스는 AP(Access Point)를 통해 통신하며,
  IP(Internet Protocol) 주소를 MAC(Media Access Control) 주소로 변환해주는 ARP(Address Resolution Protocol) 과정을 거침

- ARP Cache Table을 이용한 ARP Spoofing 공격이 쉽게 이루어지고 있음

- ARP Spoofing에서 더 나아가 Sniffing, DoS(Denial-of-Service), MITM(Man-In-The-Middle) 등의 공격이 발생할 수 있음

- ARP Spoofing 공격을 탐지 및 방지하는 기존 연구들이 존재하지만, 고가의 추가 장비나 프로토콜 수정을 요구함

프로젝트 목표

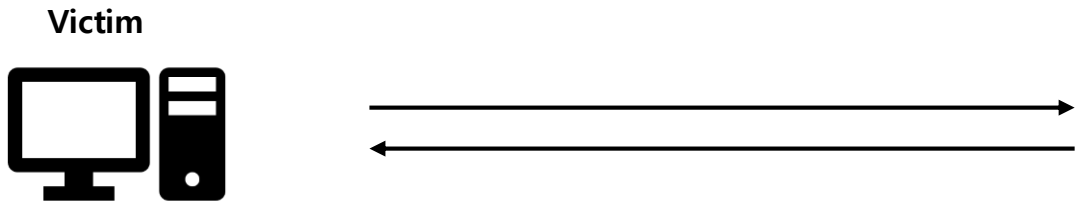
- 무선랜 라우터를 위한 리눅스 기반 운영체제인 OpenWrt를 활용하여 ARP Spoofing IDS(Intrusion Detection System)을 구축하는 것을 목표로 함
- 하드웨어적인 추가 장비 없이 AP 자체에서 ARP Spoofing 공격을 탐지함
- ARP Spoofing 공격과 VM(Virtual Machine) 연결을 구별하기 위한 알고리즘을 제시함
- 추가적으로, AP와 연결된 모든 디바이스를 실시간으로 모니터링하는 프로그램을 구축함

프로젝트 구현

- 공격 시나리오
  - 피해자 PC와 공유기 간의 정상적인 통신

IP 주소	MAC 주소
192.168.1.1	aa-aa-aa-aa-aa-aa
192.168.1.30	cc-cc-cc-cc-cc-cc

IP 주소	MAC 주소
192.168.1.20	bb-bb-bb-bb-bb-bb
192.168.1.30	cc-cc-cc-cc-cc-cc



IP Address : 192.168.1.20
MAC Address : bb-bb-bb-bb-bb-bb

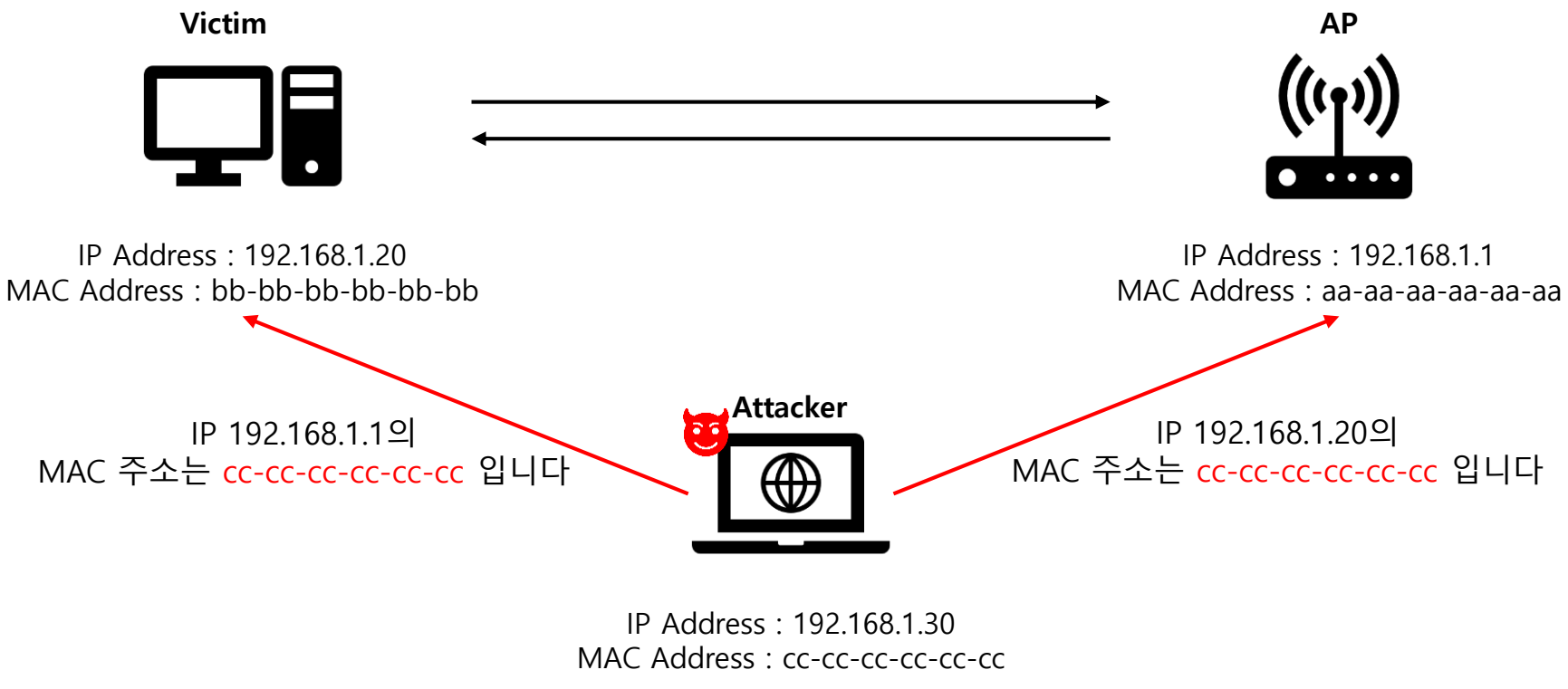
IP Address : 192.168.1.1
MAC Address : aa-aa-aa-aa-aa-aa

프로젝트 구현

- 공격 시나리오
  - ARP Spoofing 공격 과정

IP 주소	MAC 주소
192.168.1.1	aa-aa-aa-aa-aa-aa
192.168.1.30	cc-cc-cc-cc-cc-cc

IP 주소	MAC 주소
192.168.1.20	bb-bb-bb-bb-bb-bb
192.168.1.30	cc-cc-cc-cc-cc-cc

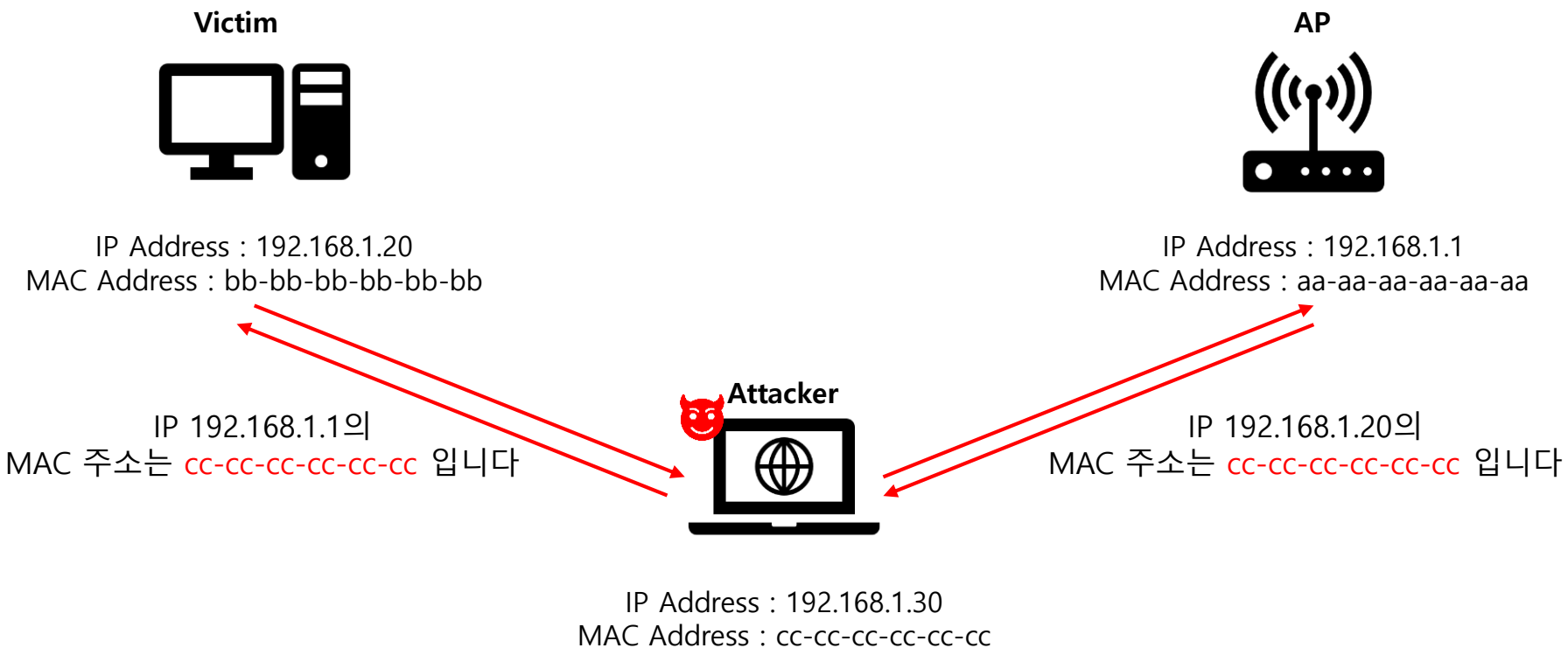


프로젝트 구현

- 공격 시나리오
  - ARP Spoofing으로 인한 MITM

IP 주소	MAC 주소
192.168.1.1	cc-cc-cc-cc-cc-cc
192.168.1.30	cc-cc-cc-cc-cc-cc

IP 주소	MAC 주소
192.168.1.20	cc-cc-cc-cc-cc-cc
192.168.1.30	cc-cc-cc-cc-cc-cc



프로젝트 구현

- Problem Statement
  - VM의 Bridge모드로 새로운 OS를 생성 시, AP의 ARP Table에서 VM의 MAC 주소가 아닌 호스트의 MAC 주소로 나타남

VM →

호스트 →

```
root@OpenWrt:~# arp -a
IP address       HW type     Flags       HW address            Mask     Device
192.168.1.181    0x1         0x2         f8:63:3f:             *        br-lan
210.115.226.4    0x1         0x2         00:e0:b4:             *        eth0.2
192.168.1.180    0x1         0x2         88:36:6c:             *        br-lan
192.168.1.161    0x1         0x0         f8:63:3f:             *        br-lan
192.168.1.238    0x1         0x2         ac:15:f4:             *        br-lan
210.115.226.1    0x1         0x2         94:f1:28:             *        eth0.2
210.115.226.91   0x1         0x2         e0:d5:5e:             *        eth0.2
192.168.1.208    0x1         0x0         88:36:6c:             *        br-lan
192.168.1.195    0x1         0x2         dc:08:0f:             *        br-lan
```

프로젝트 구현

- Problem Statement
  - ARP Spoofing으로 인한 ARP Table의 변화와 VM으로 인한 ARP Table의 변화를 구분할 수 없음

ARP Spoofing

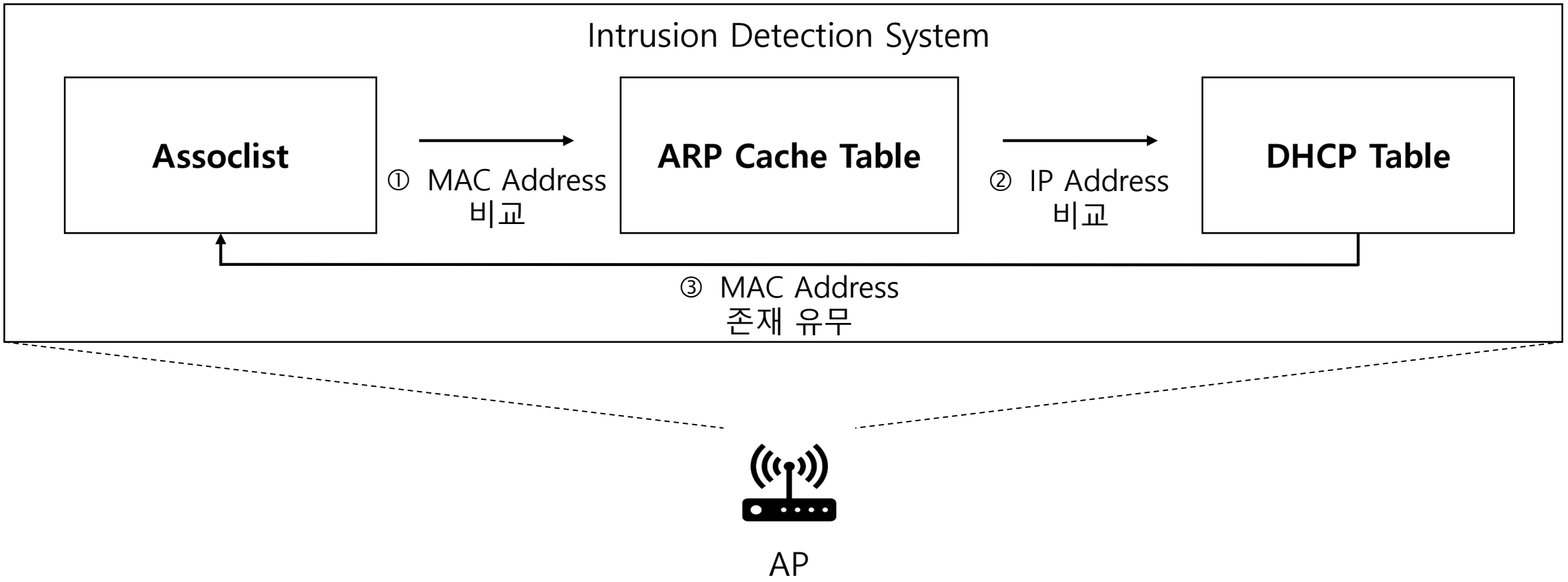
	IP 주소	MAC 주소
피해자	192.168.1.20	cc-cc-cc-cc-cc-cc
공격자	192.168.1.30	cc-cc-cc-cc-cc-cc

Virtual Machine

	IP 주소	MAC 주소
게스트	192.168.1.40	cc-cc-cc-cc-cc-cc
호스트	192.168.1.30	cc-cc-cc-cc-cc-cc

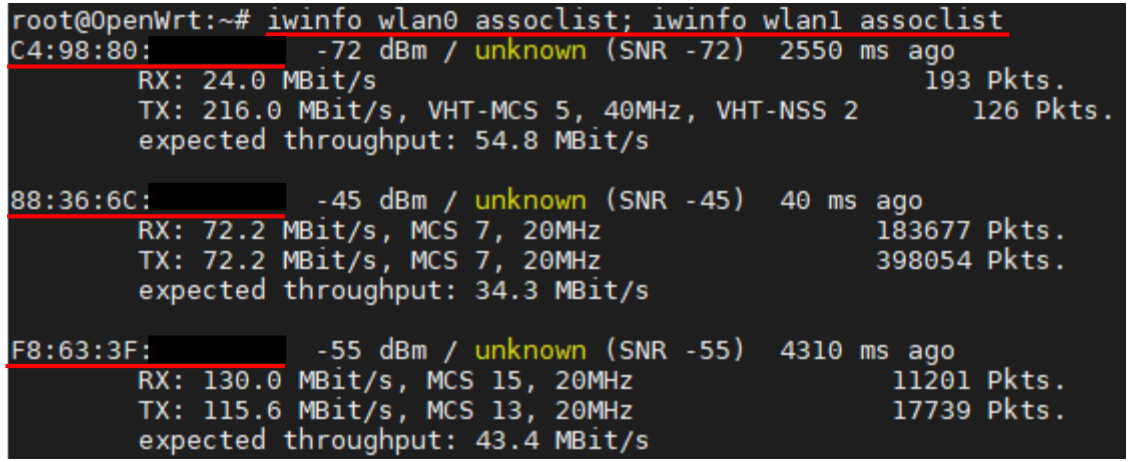
프로젝트 구현

- 시스템 구성도



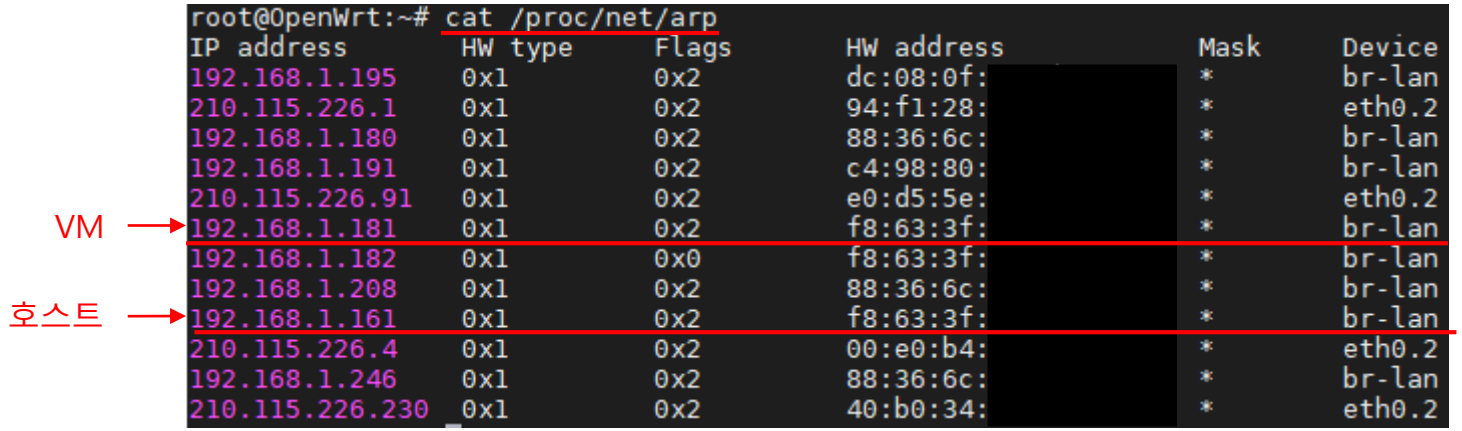
프로젝트 구현

- Assoclist
  - iwinfo wlan0/wlan1 assoclist
  - 무선 인터페이스(IEEE 802.11)에 현재 연결된 사용자의 정보(MAC, 신호세기 등)를 담고 있음
  - **VM 접속 시, VM의 MAC 주소가 나타나지 않음**



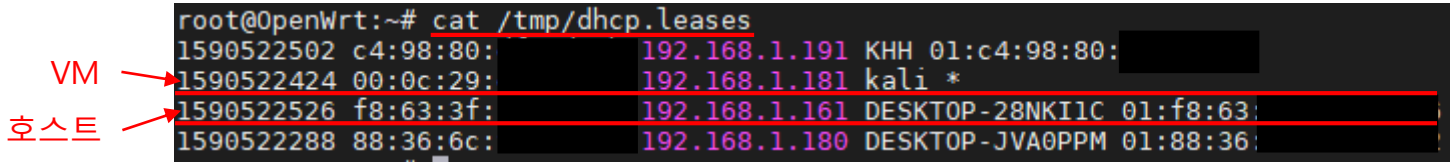
프로젝트 구현

- ARP Table
  - cat /proc/net/arp
  - ARP 통신을 위한 논리적 주소(IP Address)와 물리적 주소(MAC Address)의 정보를 담고 있음
  - **VM 접속 시, VM의 MAC주소가 호스트의 MAC주소로 나타남**



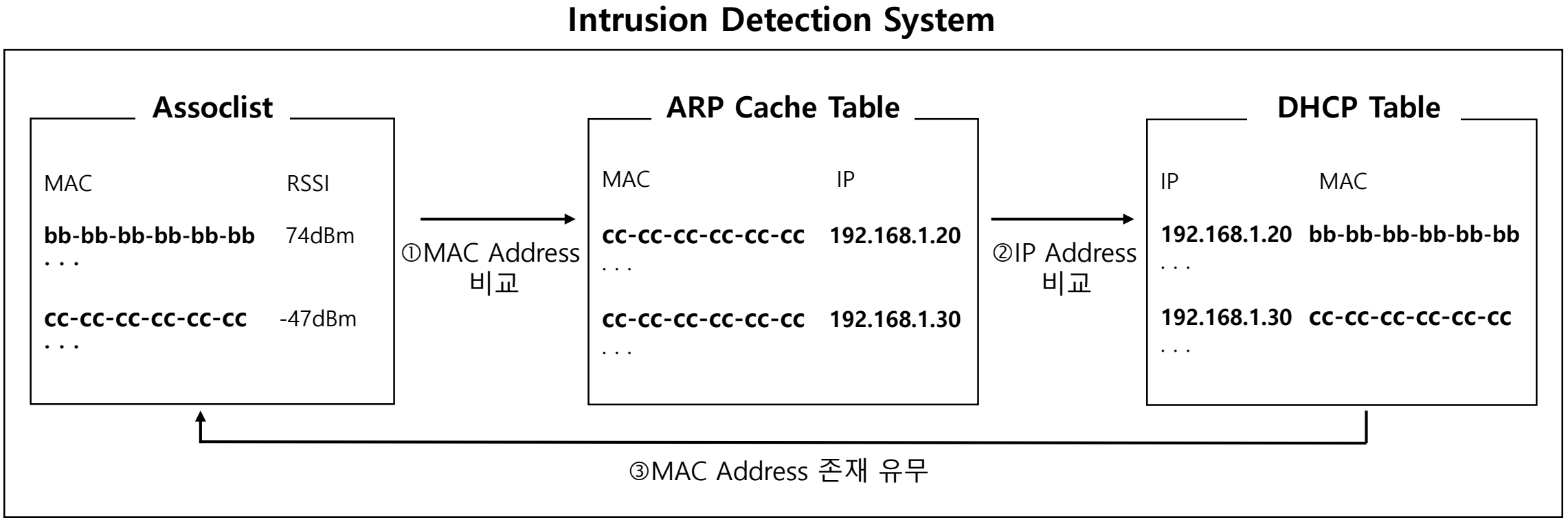
프로젝트 구현

- DHCP Table
  - cat /tmp/dhcp.leases
  - DHCP 서버가 클라이언트에게 IP를 할당한 정보를 저장한 Table
  - IP, MAC, Device Name 등을 알 수 있음
  - **VM 접속 시, VM의 MAC 주소가 정상적으로 나타남**



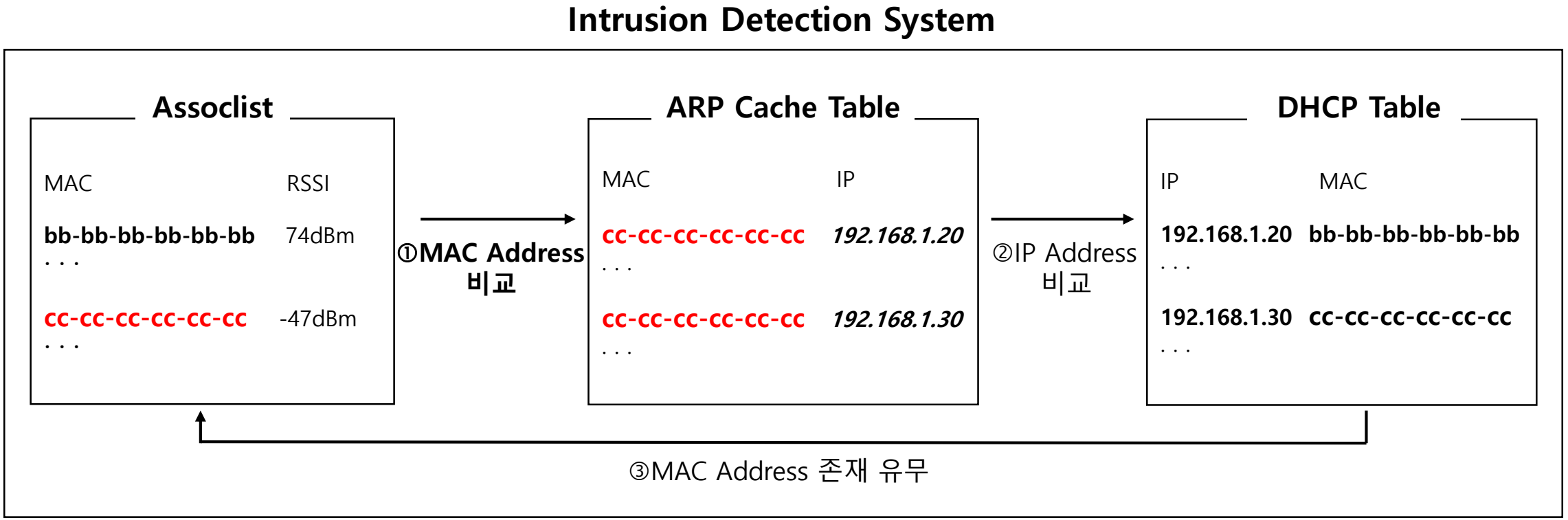
프로젝트 구현

- 시스템 구성도



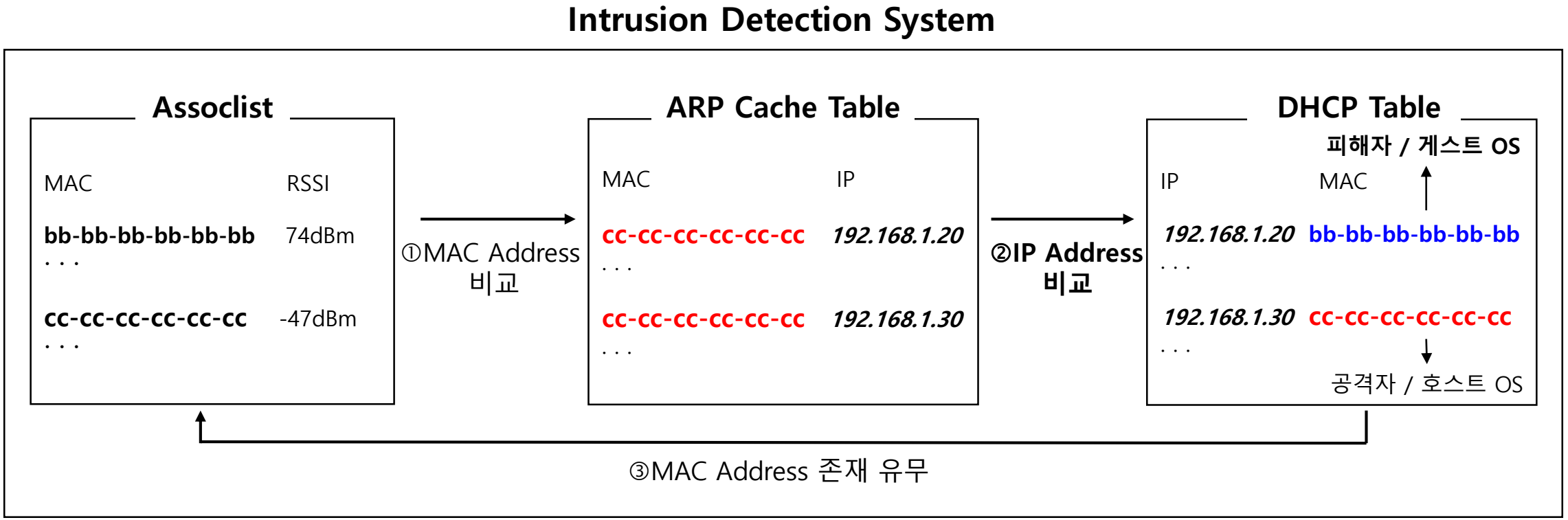
프로젝트 구현

- 시스템 구성도



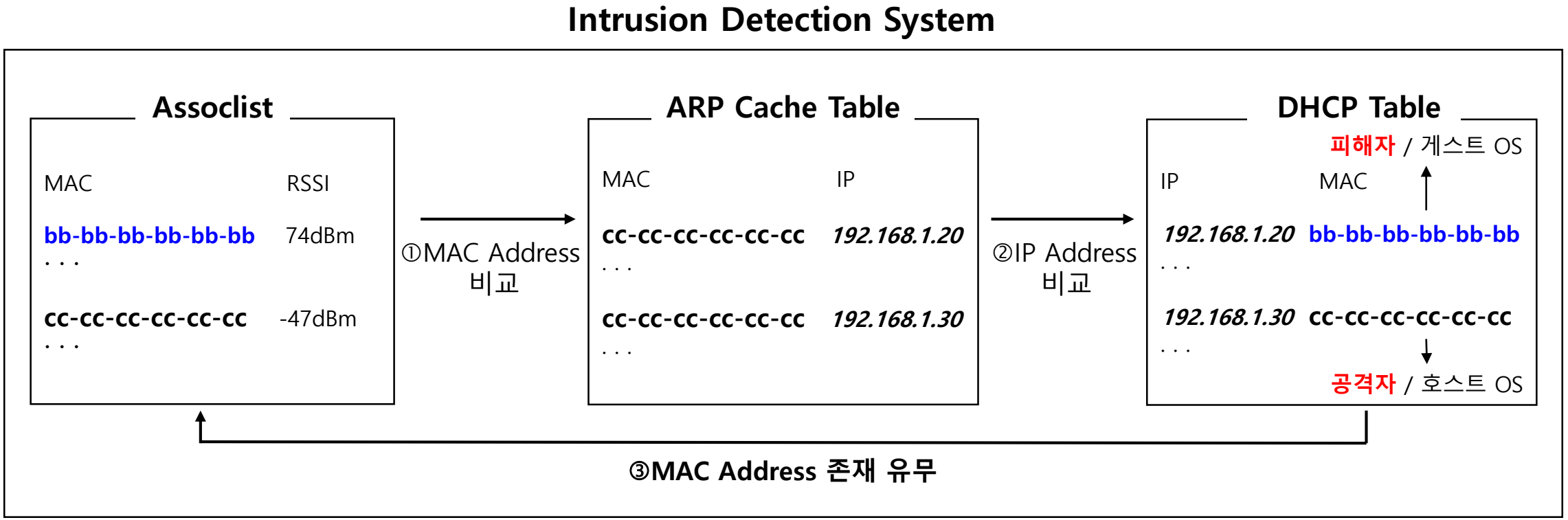
프로젝트 구현

- 시스템 구성도



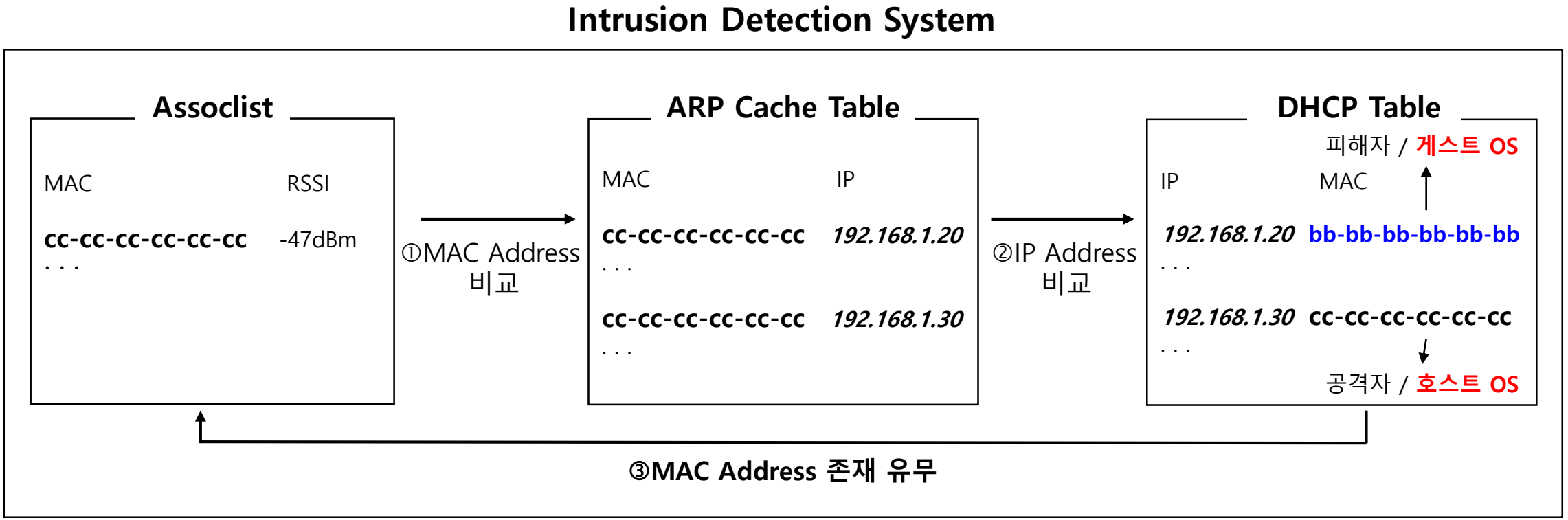
프로젝트 구현

- 시스템 구성도



프로젝트 구현

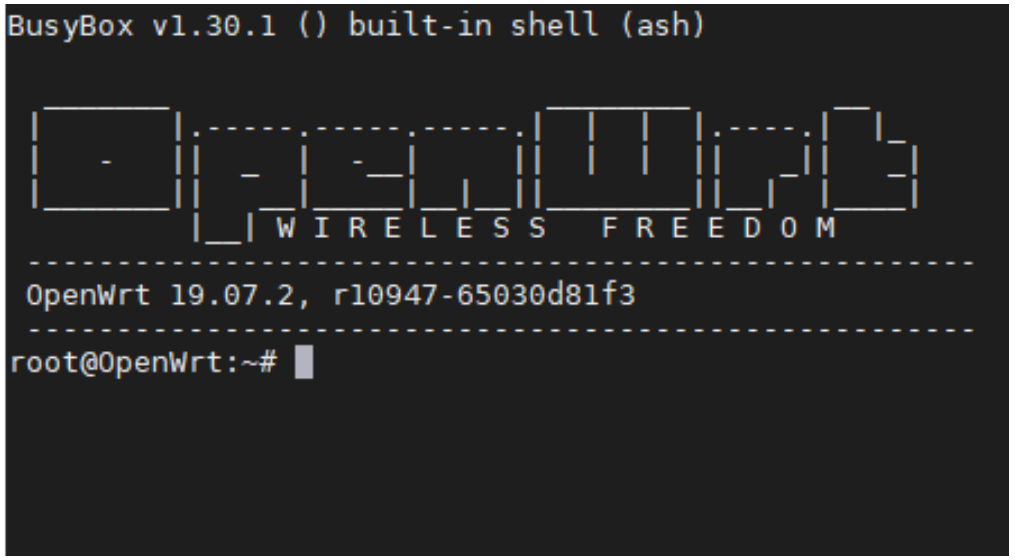
- 시스템 구성도



프로젝트 결과

- 개발환경
  - ❖ 샤오미 공유기2 (Xiaomi Mi Wi-Fi mini)

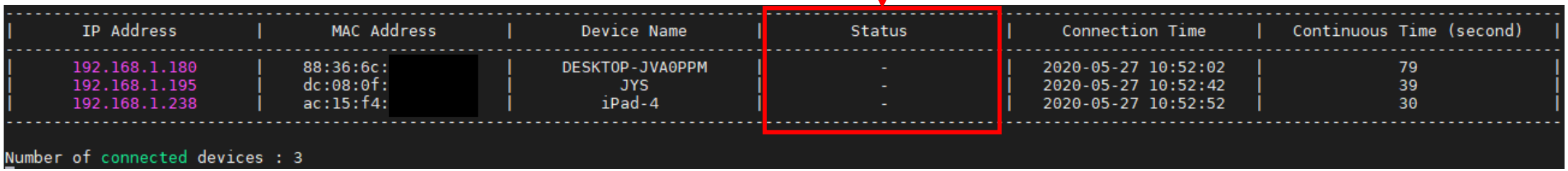
  - ❖ OpenWrt



프로젝트 결과

- 실시간 모니터링 프로그램
  - 정상 상황 시, Status에 아무런 정보가 표기되지 않음

현재 상태 표시



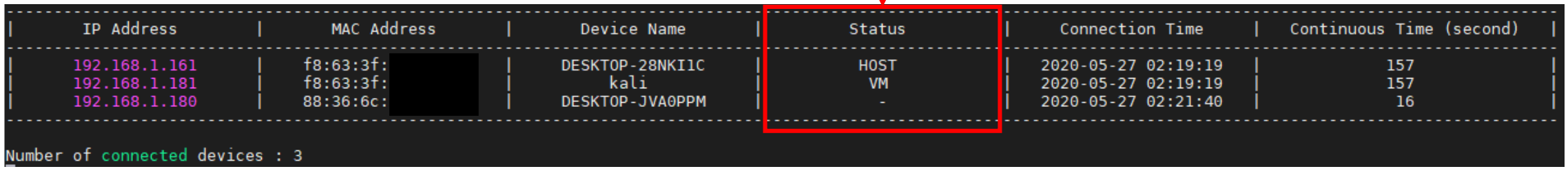
IP Address	MAC Address	Device Name	Status	Connection Time	Continuous Time (second)
192.168.1.180	88:36:6c:	DESKTOP-JVA0PPM	-	2020-05-27 10:52:02	79
192.168.1.195	dc:08:0f:	JYS	-	2020-05-27 10:52:42	39
192.168.1.238	ac:15:f4:	iPad-4	-	2020-05-27 10:52:52	30

Number of connected devices : 3

프로젝트 결과

- 실시간 모니터링 프로그램
  - VM 접속 시, Status에 VM과 호스트의 정보를 표시해 줌

현재 상태 표시



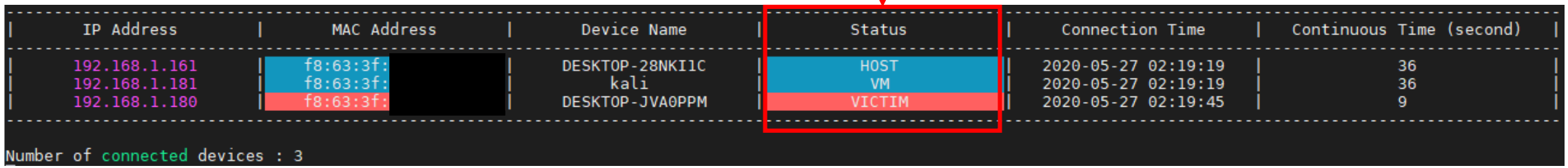
IP Address	MAC Address	Device Name	Status	Connection Time	Continuous Time (second)
192.168.1.161	f8:63:3f:	DESKTOP-28NKI1C	HOST	2020-05-27 02:19:19	157
192.168.1.181	f8:63:3f:	kali	VM	2020-05-27 02:19:19	157
192.168.1.180	88:36:6c:	DESKTOP-JVA0PPM	-	2020-05-27 02:21:40	16

Number of connected devices : 3

프로젝트 결과

- 실시간 모니터링 프로그램
  - ARP Spoofing 공격 발생 시, 피해자는 빨강색, 공격자는 파랑색으로 정보를 나타냄

현재 상태 표시

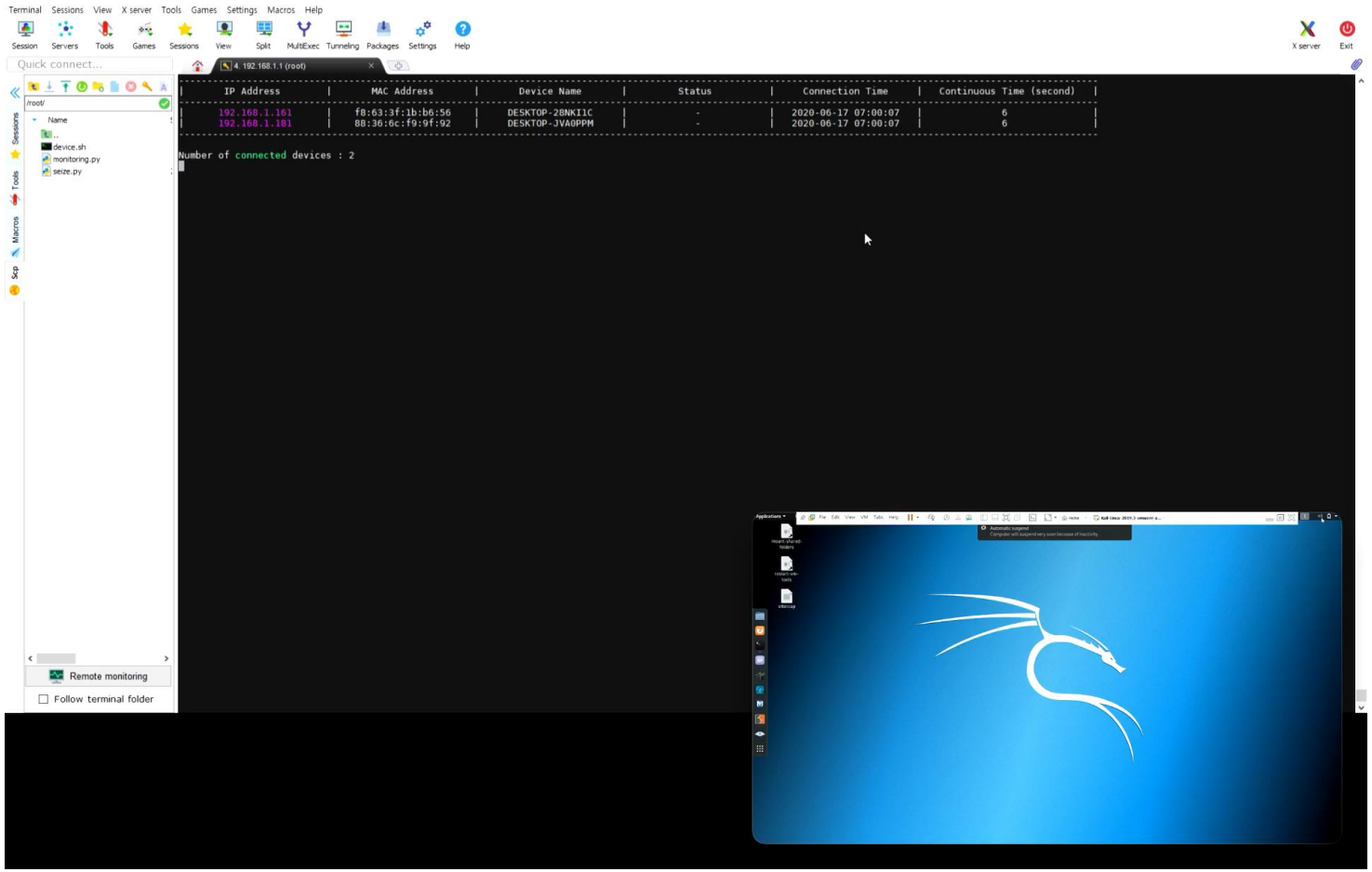


IP Address	MAC Address	Device Name	Status	Connection Time	Continuous Time (second)
192.168.1.161	f8:63:3f:	DESKTOP-28NKI1C	HOST	2020-05-27 02:19:19	36
192.168.1.181	f8:63:3f:	kali	VM	2020-05-27 02:19:19	36
192.168.1.180	f8:63:3f:	DESKTOP-JVA0PPM	VICTIM	2020-05-27 02:19:45	9

Number of connected devices : 3

프로젝트 결과

- 실시간 모니터링 프로그램
  - 동영상 시연



프로젝트 결론

- 하드웨어 추가 및 프로토콜 수정없이 기존의 네트워크 트래픽을 방해하지 않고 실시간으로 ARP Spoofing 공격 상황과 VM 연결 상황을 구별하여 탐지함

- 하지만, ARP Spoofing 공격이 종료됐을 시, 모니터링 프로그램이 멈추는 문제점이 존재함

- 향후 계획으로는 모니터링 프로그램이 정지되는 원인을 파악할 것이며, 탐지된 ARP Spoofing 공격자를 차단하고 일정 시간 동안 재접속을 금지하는 IPS(Intrusion Prevent System)를 구축할 예정임

감사합니다