**Sniffing & Spoofing 실습**

**1. Sniffing 공격 실습**

**[실습 목표] 강의에서 활용된 자료를 기반으로 직접 Sniffing 공격을 따라해보고 공격 원리에 대해 학습한다.**

**[유의사항] 모든 동작 결과 화면은 full screen을 캡쳐하며, 가상 환경 사용자 이름은 학번으로 대체하시오.**

**[제출물] 동작 원리와 각 동작 화면 및 공격 결과를 포함하는 보고서를 제출한다. 또한 동작 화면과 결과에는 분석이 반드시 함께 서술되어야 한다.**

**[실습 1] 강의 자료(3p~10p)를 따라서 TCP Dump를 사용하여 Sniffing 공격 수행**

**[실습 2] 강의 자료(11p~15p)를 따라서 Dsniff를 사용하여 Sniffing 공격 수행**

**2. ARP Spoofing 공격 수행**

**[실습 목표] ARP spoofing 공격을 통해 희생자 노드의 패킷을 sniffing하고 패킷을 변조시켜 전파한다. 또한, 패킷 분석 툴을 이용해 동작 과정을 관찰하고 ARP spoofing 방지 기법에 대해 학습한다.**

**[유의사항] 모든 동작 결과 화면은 full screen을 캡쳐하며, 가상 환경 사용자 이름은 학번으로 대체하시오.**

**[제출물]** 동작 원리와 각 동작 화면 및 공격 결과를 포함하는 보고서를 제출한다.

**[실습 1] 공격 발생 전 서버에 ICMP 패킷 전송**

- **공격 수행 전, 모든 노드의 Network를 “NAT”에서 “Host-only”로 변경하여 고립시킨다.**(Manage - Virtual Machine Settings – Network Adapter)

- 클라이언트에서 **ping**을 통해 서버와 통신한다.

- 서버 노드에서 Wireshark를 통해 **클라이언트 ping packet의 Mac Address**를 확인한다.

**[실습 2] ettercap 툴을 통한 ARP Spoofing 공격 수행**

- 공격자 노드에서 기존에 설치했던 **ettercap graphical 툴**을 실행한다.

- Unified Sniffing 모드에서 공격 대상(Target)을 설정한 후, ARP spoofing 및 sniffing을 실행한다.

- 클라이언트에서 **Mac Address Table**을 확인하고, 서버로 ping을 전송한다.

- 공격자 노드에서 **Wireshark를 통해 수집된 ping packet의 Mac Address 변화를 확인**한다.

**[실습 3] ARP spoofing 방지 기법을 적용한다.**

- 클라이언트 노드에서 네트워크내의 **Mac Address를 정적으로 설정**하고 MAC Address Table을 관찰한다.

- 공격자 노드에서 ARP spoofing 공격을 수행 후, **Wireshark를 통해 클라이언트의 Mac Address를 확인**한다.