|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  |  | | |  | |
|  | **IP Spoofing** | | | | | | |  |
|  | | **네트워크 해킹** | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. **ip Spoofing 이란?** |
| * **TCP/IP 약점을 이용한 여러 공격 기법 중 해커가 자신의 인터넷 프로토콜(IP)을 악용하고자 하는 호스트의 IP 주소로 속이거나 바꾸어서 이를 통해 해킹 공격하는 기법. 즉, 자신의 MAC 주소를 다른 컴퓨터의 MAC 주소인 것처럼 속이는 공격입니다.** * **ARP Cache 정보를 임의로 바꾼다 하여 ‘ARP Cache Poisoning 공격이라고도 합니다.** |
| 1. **공격 원리** |
| 1. 신뢰(trust) 관계가 맺어져 있는 두 시스템 사이에서 서버와 클라이언트를 확인 2. 신뢰관계가 있는 클라이언트를 연결 불가능한 상태로 만들고자 클라이언트에 DoS 공격 등을 통하여 연결을 끊는다. 3. 공격자가 클라이언트의 IP 주소를 확보 및 위조(스푸핑)하여 공격자가 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속임으로써 서버에 실제 클라이언트처럼 패스워드 없이 접근 |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 |
| **실습 환경**  00:0C:29:FF:F9:49  **공격 호스트(kali linux): 1.1.1.10 /25**  **타겟 호스트(centos7): 1.1.1.12 /25**  **게이트웨이(라우터): 1.1.1.126** |
| 1. **실습환경** |
| |  |  |  | | --- | --- | --- | |  | IP 주소 | MAC 주소 | | kali | 1.1.1.201 | 00:0c:29:4d:a6:2d | | window server 2019 (dns 서버) | 1.1.1.200 | 00:0C:29:FF:F9:49 | | Windows 10 | 1.1.1.210 | 00:0C:29:EA:A7:1C | | 게이트웨이 | 1.1.1.254 | ca:02:0c:fc:00:1c |   **# hping3 -1 [victim\_ip] : 정상적인 ping**  **# hping3 -1 -a [속일\_ip] [victim\_ip]**  **-1 : ICMP를 사용하겠다**  **-a : spoof 사용하겠다** |
| 1. **시나리오1. 내부망에 없는 IP 사용** |

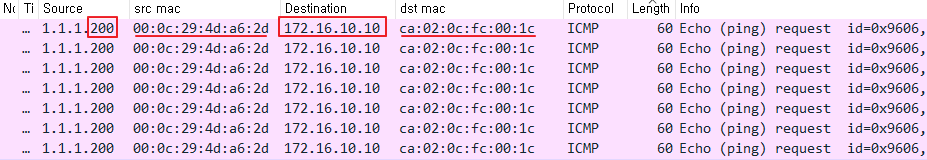
**# hping3 -1 -a 1.1.1.200 172.16.10.10**

Kali의 IP는 1.1.1.201 이지만 Windows server 2019 (DNS서버)의 1.1.1.200으로 속여 172.16.0.0이라는

없는 대역대에게 통신을 시도



**<결과값>**



**내부망에 172.16.0.0 대역대가 없기 때문에 Gateway를 빠져나가지 못함을 확인**

**- 위의 사진을 보면 source IP는 DNS서버의 주소지만 source mac address는 kali인 것을 확인**

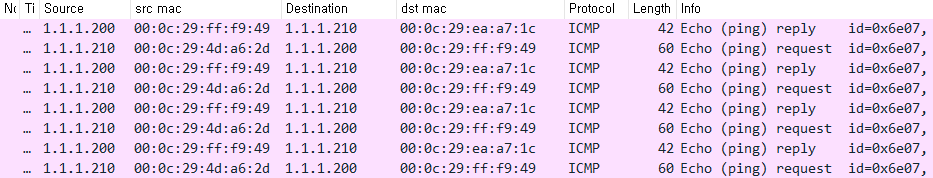
**destination IP는 172.16.10.10이지만 destination mac address는 게이트웨이인 것을 확인**

|  |
| --- |
| 1. **시나리오2. Windows 10을 가장해서 DNS서버(WS-2019)와 통신** |

**# hping3 -1 -a 1.1.1.210 1.1.1.200**



**<결과값>**



1. **Request**

출발지 IP : 1.1.1.210 🡪 Windows 10

src mac : ~:2D 🡪 Kali

출발지는 Windows 10로 출발했지만 고유 MAC 주소는 Kali이다.

도착지는 Windows server 2019에 MAC주소도 맞게 도착

1. **Reply**

출발지 IP : 1.1.1.200 🡪 Windows server 2019 (DNS서버)

src mac : ~:49 🡪 Windows server 2019 (DNS서버)

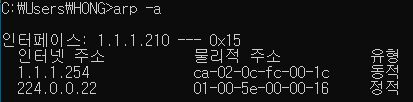
도착지 IP : 1.1.1.210 🡪 Windows 10

dst mac : ~:A7:1C 🡪 Windows 10

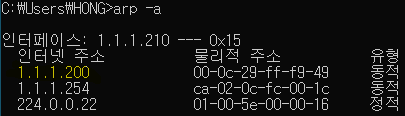
출발지에서는 IP만 스푸핑하여 MAC주소는 kali로 보냈지만 응답할 때는 MAC 주소를 보지않고 IP주소만 보고 보냈기 때문에 MAC 주소 역시 IP주소에 맞게 변환 됨

**<윈도우 10>**

- 스푸핑이 일어나기 전



- 스푸핑이 일어난 후



Windows server 2019의 흔적이 나타남

|  |
| --- |
| 3. 보안진단 및 대책 |
|  |
| 신뢰 관계를 이용한 IP Spoofing에 가장 좋은 대책 방법은 신뢰를 사용하지 않는 것이다.  부득이하게 신뢰(Trusted)를 사용해야 할 경우 신뢰(Trusted)된 클라이언트의 MAC주소를 Static으로  지정해 둔다. 공격자가 연결을 끊을 수는 있으나 클라이언트의 IP로 위장하여 접근하더라도 MAC주소까지  같을 수 없기 때문에 세션을 빼앗기지는 않는다. |