|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:고준혁 | | |  | |
|  | <ARP Redirect> | | | | | | |  |
|  | |  | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
| \*ARP redirect  ARP redirect란 공격자가 자신을 게이트웨이라고 속이는 것이다. 즉, 희생자들의 패킷이 공격자를 한번 거쳐서 게이트웨이로 가도록하는 공격이다. 이를 통해 공격자는 희생자가 어떤 패킷을 외부망으로 보내는지를 알아낼 수 있다. |

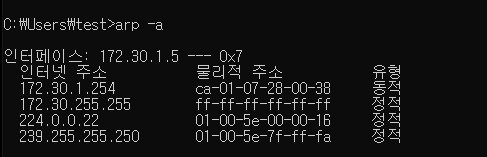
|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |

|  |  |  |
| --- | --- | --- |
| **실습환경** | **주소** | **OS** |
| **공격자 시스템** | **172.30.1.2** | **Kali** |
| **피해자 시스템** | **172.30.1.5** | **Windows 10** |

**(Win10)**

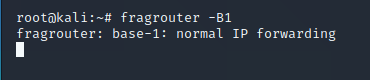
ARP redirect 공격은 위조된 ARP 패킷을 보내 희생자 시스템의 MAC 주소 테이블을 바꾸는 방식이므로 먼저 희생자 시스템의 MAC 주소 테이블을 확인한다.

**# arp -a**



**(Kali)**

희생자 PC로부터 패킷이 전달되어 올 때 세션이 끊어지지 않게 패킷 릴레이를 위해 fragrouter를 실행한다.

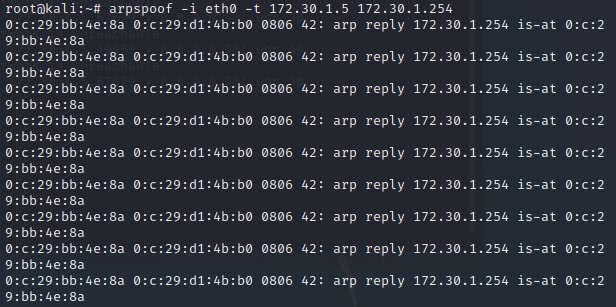


새로운 터미널을 열어 dsniff에서 제공하는 툴 중 하나인 arpsoof를 사용한다.

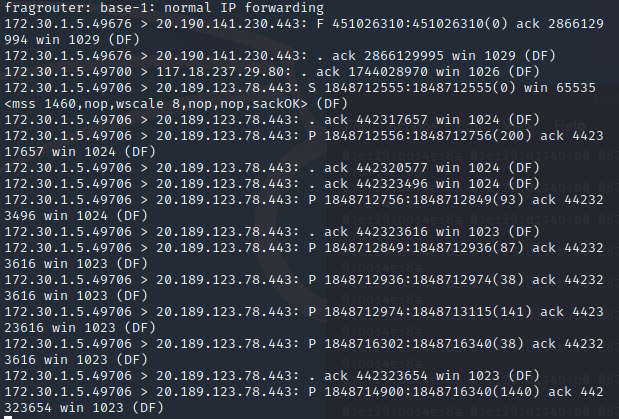
희생자 PC 172.30.1.5에게 공격자의 주소가 172.30.1.254(게이트웨이)라는 것을 알리는 명령으로 다음과 같은 명령어를 사용한다.

**# arpsoof ① -i [interface] ② -t [target] ③ host**

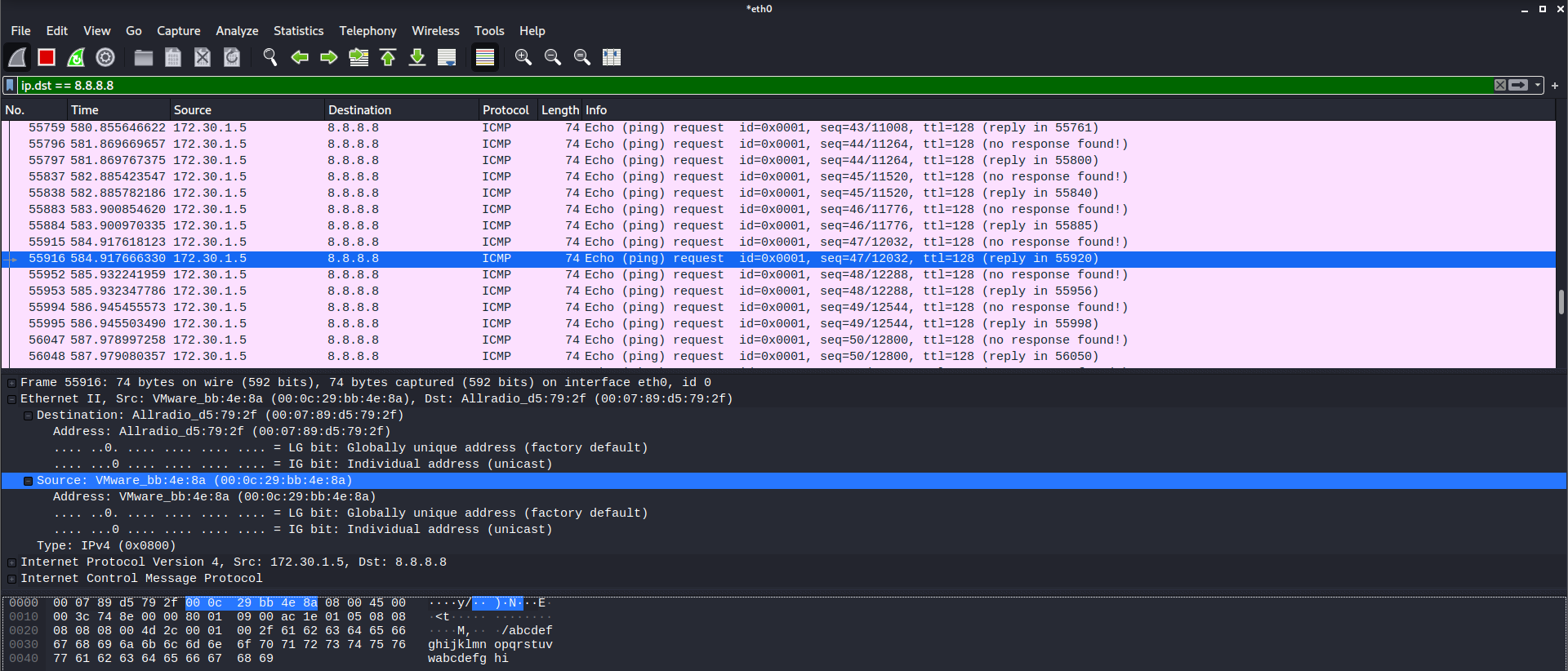
1. **-i: 사용할 인터페이스를 지정**
2. **-t: 타깃이 될 대상의 IP 주소**
3. **host: 속일 IP 주소**

****

다음과 같이 fragrouter를 실행한 화면을 보면 희생자(172.30.1.5) 시스템에서 공격자 시스템을 통과하여 게이트웨이를 통해 외부로 나가는 패킷들을 확인할 수 있다.



|  |
| --- |
| 3. 공격 결과 |
| **(Win10)**  희생자 시스템의 arp 테이블을 확인해 본 결과이다.  게이트웨이인 172.30.1.254의 MAC주소가 공격자 172.30.1.2의 MAC주소와 동일하게 인식된 것을 확인할 수 있다. |
| 패킷의 흐름을 확인해 보기 위해서 공격대상의 PC에서 같은 대역대의 다른 pc로 핑을 날려서 wireshark로 패킷을 잡아보았다.  공격자가 공격 대상의 패킷을 받아서 다시 게이트웨이로 보내기 때문에 보내는 MAC주소는 공격자, 받는 MAC주소는 게이트웨이가 나올 것이다. |



패킷 분석 결과 Source는 공격자의 MAC 주소가 나왔고 Destination는 게이트웨이의 MAC주소가 나온 것을 확인할 수 있다

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
| * + - 1. **타겟 PC의 ARP Cache Table에서 게이트웨이에 해당하는 MAC 주소를 정적으로 바꿔준다.**   **# arp –s [ip 주소] [MAC 주소]**  **# arp –s 172.30.1.5 00-07-89-d5-79-2f** |
| arp- a로 확인 결과 설정해 준 값으로 바뀐 것을 볼 수 있다.  \*\*\*Windows 환경에서 동적 MAC주소 정적으로 설정 변경 방법\*\*\*  **시작 -> 실행 -> cmd -> netsh interface show interface**    인터페이스 이름을 기억해둔다.  netsh interface ip add neighbors “인터페이스 이름” “게이트웨이 주소” “맥주소”    정적으로 바뀐 것을 확인 가능하다  그러나 재시작하면 다시 동적으로 변경되기 때문에 Batch 파일로 만들어 부팅 시마다 실행이 되게 하자   * + - 1. 암호화 및 보안 프로토콜 사용   중요한 정보는 암호화하고 SSL, IPsec, PGP 등과 같은 보안 프로토콜을 사용한다.   * + - 1. Anti-sniffer 도구 사용(antisiff, senitel, ARP watch, Hunt)   안티 스니퍼 도구는 NIC의 promiscuous 모드 유무를 체크하여 스니퍼가 돌고 있는가를 체크하고 DNS test, ICMP time test, Ether ping test, UDP echo test 등 여러 테스트를 지원한다.   * + - 1. ARP / Ping(ICMP) 이용하여 스니핑 탐지   목적지 MAC 주소 값을 네트워크에 없는 값으로 ARP Request를 보냈을 때, ARP Reply를 보낼 수 없음에도 이를 보내는 호스트는 Promiscuous 모드로 동작 중이므로 스니핑하고 있다고 볼 수 있다.  마찬가지로 Ping을 이용하여 해당 네트워크에 없는 MAC주소로 ICMP echo request 메시지를 보냈을 때 ICMP echo reply를 보내는 호스트는 스니핑하고 있다고 볼 수 있다. |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
| **<(4-1 적용) 패킷은 계속 가지만 MAC 주소가 바뀌지 않는 것을 확인할 수 있다>** |