|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:고준혁 | | |  | |
|  | <ICMP redirect> | | | | | | |  |
|  | |  | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
| \*ICMP redirect란?  보통의 네트워크는 라우터나 게이트웨이가 하나다. 하지만 하나의 라우터로 트래픽을 감당할 수 없을 때는 라우터나 게이트웨이를 두 개 이상 운영해서 로드 밸런싱(Load balancing)을 해야 할 것이다. 로드 밸런싱을 하는 방법은 다양하다. 시스템의 라우팅 테이블에 라우팅 엔트리를 하나 더 넣어 주는 방법도 있으나, ICMP redirect를 사용하기도 한다.  ICMP redirect 공격은 이러한 경우를 강제적으로 만들어주게 된다. 공격자가 네트워크에 존재하는 또다른 라우터임을 각 호스트에게 알리게 된다. ARP Spoofing과 다른 점은 ARP Spoofing은 모든 트래픽에 대한 redirect를 가능하게 하지만, ICMP redirect는 특정한 목적지 주소를 가진 패킷만을 리다이렉트하게 된다. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) | | | | |
| **\* ICMP 리다이렉트 작동 원리** | | | | |
| 호스트가 인터넷으로 패킷을 보낼 때 디폴트 라우터로 라우터A가 정해져 있다면 호스트는 일단 패킷을 라우터 A로 보낸다.  라우터 A는 라우팅 테이블을 검색해서 직접 데이터를 처리하는 것 보다 라우터 B가 처리하는 것이 효과적이라면 패킷을 라우터 B로 전송한다.  라우터 A는 동일 목적지로 보내는 패킷이 라우터 B로 전송되도록 호스트에게 ICMP 리다이렉트 패킷을 보낸다.  호스트는 라우팅 테이블에 현재 전송중인 패킷에 대한 정보를 저장하고 동일 목적지로 전송하는 패킷은 라우터 B로 보  낸다.  **[실습 환경]** | | | | |
|  | IP주소 | MAC주소 | OS |
| **공격자** | **172.30.1.2** | **00:0c:29:bb:4e:8a** | **Kali** |
| **피해자** | **172.30.1.35** | **00-0C-29-57-10-99** | **Windows XP** |

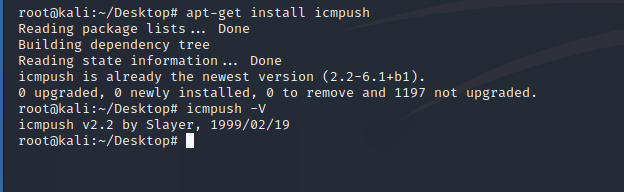
**(Kali)**

1. 사용 툴

1. Fragrouter : 패킷 릴레이를 하기 위해 사용한다. 사용하지
2. Icmpush : 공격자가 ICMP redirect 패킷을 송신하는 것으로 피해자의 라우팅 테이블에 특정 사이트에 접속하면 지정 IP를 게이트웨이로 사용하게 한다.

**# apt-get install icmpush** // icmpush를 설치한다

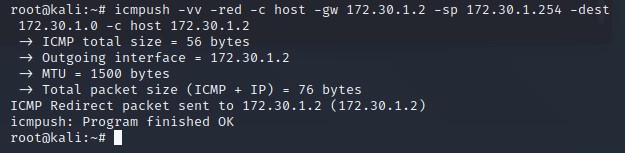
**# icmpush -V //** icmpush 설치 확인



Icmpush로 공격 수행

**# icmpush -vv -red -sp [GW] -gw [redi-GW] -dest [Destination] -c host [Victim]**

|  |  |
| --- | --- |
| **-vv** | **자세히 보기** |
| **-red** | **Icmp redirect attack** |
| **-sp** | **원래 게이트웨이 주소** |
| **-gw** | **재지정할 게이트웨이 주소** |
| **-dest** | **라우팅 테이블에 등록할 목적지 주소** |
| **-c** | **Code(host : 특정 호스트 지정, net: 특정 네트워크 지정** |
| **-host** | **패킷을 받을 host의 주소** |



공격이 진행되면 피해자 시스템에서 라우팅 테이블이 공격자가 지정한 주소로 변경된다.

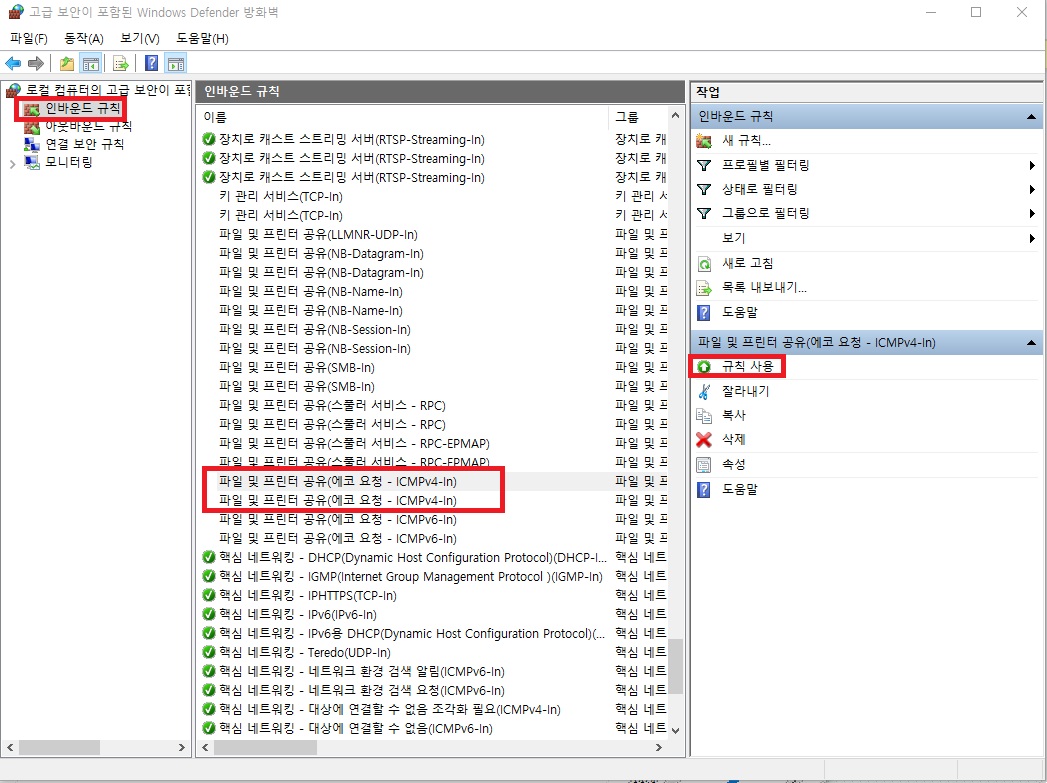
추가로 **# fragrouter -B1** 명령을 통해 패킷을 포워딩 시켜준다.

|  |
| --- |
|  |
| 3. 공격 결과 |
| **공격자 PC에서 Wireshark로 패킷 캡처 결과 게이트웨이의 주소를 바꾸어서 Redirect 메시지를 보낸 것을 확인 할 수 있다.**    **피해자 PC에서 네이버 카페, 네이버 메일 등 웹사이트를 접속한 기록 파악 가능** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
| ICMP redirection 메시지에 의해 라우팅 테이블이 변경되지 않도록 ICMP redirection 옵션을 해제한다.  현재 대부분의 OS에서 보안상의 이유로 ICMP redirect 옵션을 기본적으로 해제하고 있다. |

1. **윈도우에서 ICMP 방화벽 정책 설정**

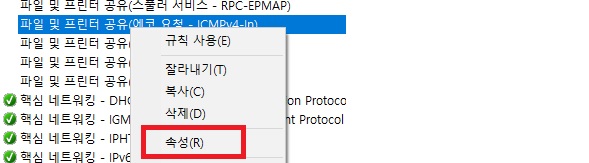
* 윈도우 키 + R 입력하여 firewall.cpl 입력 or 제어판 -> Windows 방화벽 -> 고급설정



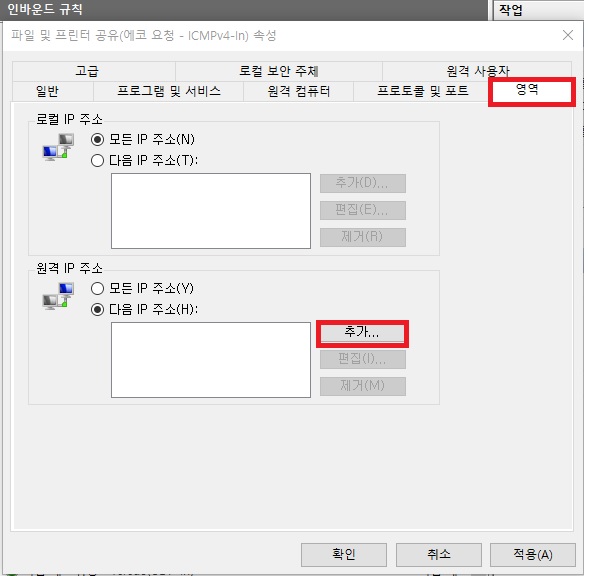
방화벽 정책의 파일 및 프린터 공유(에코 요청 - ICMPv4-in)를 규칙 사용을 선택하면 정책부분의 녹색 체크표시로 체크되어 있는 것을 확인할 수 있다.

**2. 윈도우 ICMP 특정 네트워크 사용자에게만 허용**

모든 네트워크의 ICMP를 모두 허용하면 보안적으로 ICMP 취약점인 Ping Flooding, SYN Flooding, Ping of Death 등 공격의 노출이 되어 위험할 수가 있다 그렇기 때문에 특정 네트워크 사용자(IP)에게만 허용하는 것을 권고한다고 한다.



방화벽 정책의 파일 및 프린터 공유(에코 요청 - ICMPv4-in)를 더블클릭이나 우클릭하여 속성



IP 주소의 창에 허용할 IP 입력하거나 서브넷 형식으로 입력해도 가능

정책 반영 시 다음 IP 주소를 체크한 후 다음 IP주소 안에 있는 IP는 모두 허용된다

**3. 리눅스에서 ICMP 보안 설정**

리눅스 커널 파라미터 중 ICMP Redirect 설정인 accept\_redirects를 0(허용 안 함)으로 설정한다.

**# sysctl -w net.ipv4.conf.all.accept\_redirects=0**

|  |
| --- |
|  |