|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:고준혁 | | |  | |
|  | <ICMP Scanning> | | | | | | |  |
|  | | Ping을 이용한 간단한 스캔 | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요 |
| Scan(스캔)은 방화벽과 IDS(침입탐지시스템)을 우회하기 위하여 발전했으며, 종류가 매우 다양하다.  서버의 동작 여부를 알아보는 가장 기본적인 스캔은 ping을 이용하는 것이다.  검사하고자 하는 네트워크에서 동작하는 서버를 찾아내는 일은  공격 대상 네트워크에서 공격대상의 IP주소를 결정하는 데 매우 중요하다.  ping은 네트워크와 시스템이 정상적으로 작동하는지 확인하기 위한 간단한 유틸리티이다.  ping은 ICMP(Internet Control Message Protocol)을 사용하며, 기본적으로 TCP/IP 네트워크에서 사용된다.  넷웨어(Netware)같이 다른 프로토콜 체제를 쓰는 네트워크에서는 ping 유틸리티도 다르다.  따라서 모든 네트워크에 ping이 있는 것은 아니다.  ICMP를 이용해 공격대상 시스템의 활성화 여부를 알아보는 방법은 아래 네 가지이다.  **1. Echo Request와 Echo Reply를 이용한 방법**  **2. Timestamp Request와 Timestamp Reply를 이용한 방법**  **3. Information Request와 Information Reply를 이용한 방법**  **4. ICMP Address Mask Request와 ICMP Address Mask Reply를 이용한 방법** |

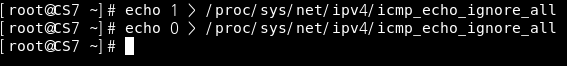
|  |
| --- |
|  |
| 2. 공격 과정 |
| **1.** **Echo Request와 Echo Reply를 이용한 방법**  가장 일반적인 방법으로 옵션 없이 ping을 사용하면 된다     1. **ICMP 패킷의 길이를 나타내는 것으로 운영체제마다 보내는 바이트의 길이가 다르다. 유닉스와 리눅스와 같은 시스템은 위 그림처럼 대부분 56바이트 ICMP Echo Request 패킷을 생성하여 보낸다. 윈도우 시스템은 32바이트이다. 각 바이트의 내용은 의미 없는 알파벳으로 채워진다.** 2. **공격 대상에서 보내온 ICMP Echo Reply 패킷의 크기** 3. **Echo Request 패킷을 보낸 후 Reply 패킷을 받기까지의 시간이다.** 4. **TTL( Time To Live ) 값으로, 라우팅 정보가 잘못되어 패킷이 네트워크를 무한대로 돌아다니지 않도록 최초 라우터를 제외한 라우터를 지날 때마다 값이 1씩 줄어든다. TTL 값도 운영체제에 따라 조금씩 다르다.**  |  |  |  | | --- | --- | --- | | **운영체제** | **ICMP Request 패킷 TTL** | **ICMP Reply 패킷 TTL** | | **리눅스 커널 2.6** | **64** | **64** | | **리눅스 커널 2.2 – 2.4** | **255** | **64** | | **리눅스 커널 2.0** | **64** | **64** | | **우분투** | **128** | **128** | | **FreeBSD** | **255** | **255** | | **솔라리스** | **255** | **255** | | **HP-UX** | **255** | **255** | | **윈도우 95** | **32** | **32** | | **윈도우 98** | **128** | **128** | | **윈도우 NT** | **128** | **128** | | **윈도우 서버 2003, 2008, 2012** | **128** | **128** | | **윈도우 10** | **64** | **64** |  1. **Request 패킷의 개수, Reply 패킷의 개수, 손실된 패킷의 개수.** 2. **Request 패킷을 보낸 후 Reply 패킷이 오기까지의 시간 정보.**   **2**. **Timestamp Request와 Timestamp Reply를 이용한 방법**  Timestamp Request패킷을 이용하는 것으로, Timestamp Request패킷은 원격지 시스템의 현재 시각을 알아보기 위한 패킷이다. Timestamp Request패킷은 송신자가 패킷을 보낸 시각과 수신자가 패킷을 받은 시각, 송신자가 수신자에게 전송하는 동안 걸린 시간으로 공격대상의 현재 시스템 시각을 알 수 있게 해 준다.  상대시스템의 Reply패킷이 돌아온다는 것은 상대시스템이 활성화 되어있음도 알려주는 것이다.  **3**. **Information Request와 Information Reply를 이용한 방법**  Information Request패킷을 이용하는 것으로 원래 Information Request와 Reply는 메인 프레임의 단말기처럼 부팅할 때 자신의 디스크가 없는 시스템이 스스로 IP를 설정할 수 있도록 하는 패킷으로, 자신의 네트워크를 찾기 위해 개발되었다. 기본목적은 RARP, Bootp, DHCP같은 프로토콜과 같으나 다른 프로토콜을 이용한 방법에 비해 원시적이라고 할 수 있다.  이 방법에서도 위 Timestamp Request 패킷처럼 죽은 시스템은 Reply패킷을 보내지 않을 것이다.  **4**. **ICMP Address Mask Request와 ICMP Address Mask Reply를 이용한 방법**  ICMP Address Mask Request 와 Reply패킷을 이용하는 것이다.  이 패킷 역시 두 번째 방법처럼 단말기가 부팅될 때 자신이 속한 네트워크의 서브넷마스크를 알기 위해 보낸다.  앞의 두 방법과 마찬가지로 Reply패킷이 돌아오는지 확인함으로써 상대 시스템의 활성화 여부를 파악할 수 있다.  ▶ 2, 3, 4 방법은 모든 운영체제에서 작동하지는 않는다. 운영체제에 따라 세 가지 중 일부만 지원하며, 지원 여부에 따라 운영체제를 짐작할 수 있다.   |  |  |  |  | | --- | --- | --- | --- | | **운영체제** | **Information** | **Timestamp** | **Address mask** | | **리눅스 커널 2.2 – 2.4** | **X** | **O** | **X** | | **FreeBSD** | **X** | **O** | **X** | | **솔라리스** | **X** | **O** | **O** | | **HP-UX** | **O** | **O** | **X** | | **AIX v4** | **O** | **O** | **X** | | **윈도우 98** | **X** | **O** | **O** | | **윈도우 NT sp4** | **X** | **X** | **X** | | **윈도우 2000** | **X** | **O** | **X** | |

|  |
| --- |
| 3. 보안 대책 및 적용 결과 |
| **ICMP를 차단한다.** |

**-리눅스에서 PING 허용과 차단 방법**

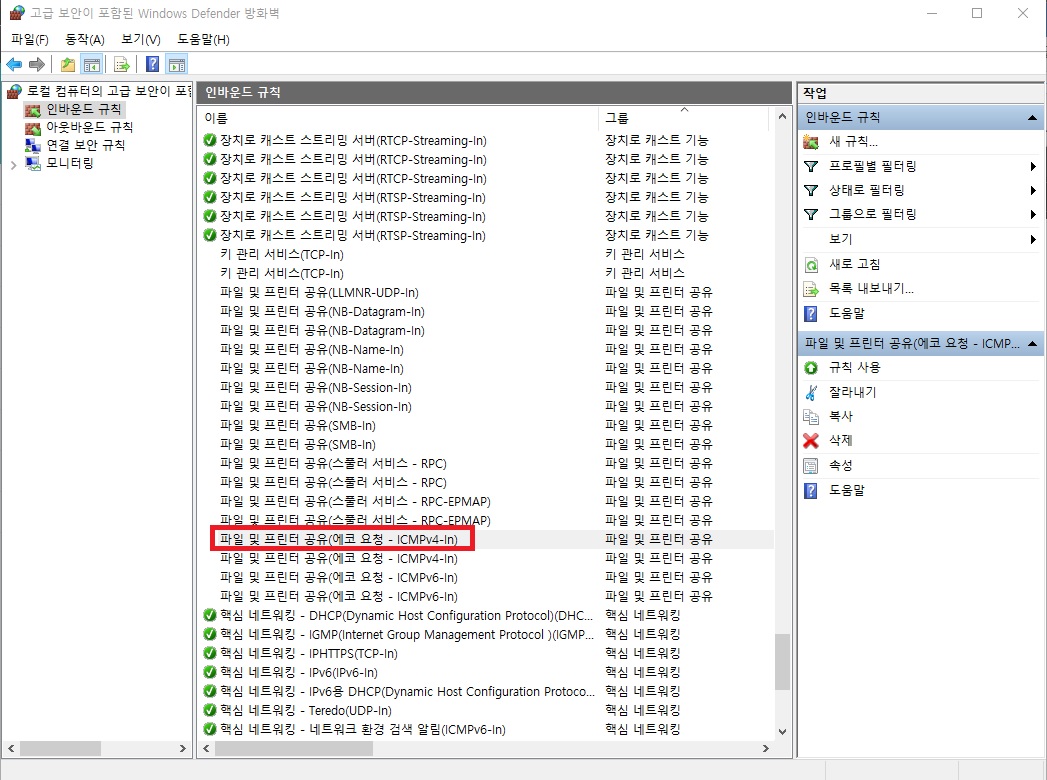
#echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all // 값을 1로 설정하여 ping을 차단

#echo 0 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all // 값을 0로 설정하여 ping을 허용



**-윈도우에서 PING 허용과 차단 방법**

1. 실행창 ▷ firewall.cpl ▷ 고급 설정 ▷ 인바운드 규칙 ▷ 파일 및 프린터 공유(에코 요청 – ICMPv4-in) 항목을 클릭한 후 사용함을 체크하거나 해제하여 설정.



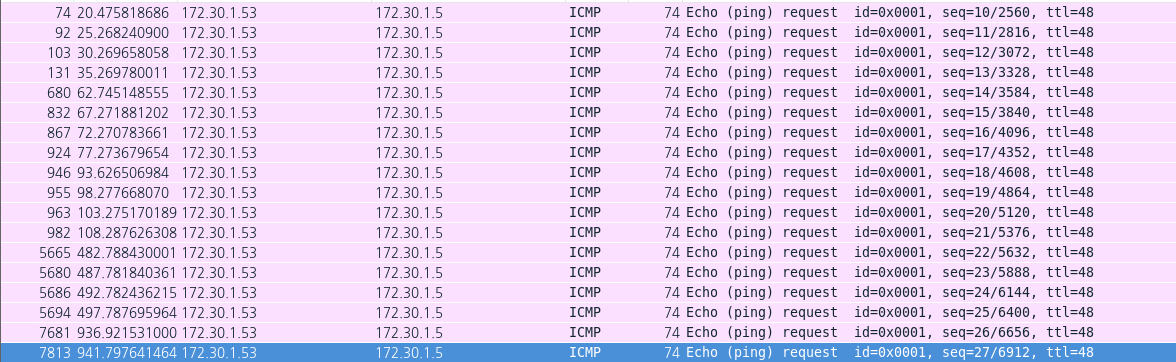
2. cmd 명령으로 설정하는 방법.

시작 ▷ 실행 ▷ cmd를 입력 후 cmd 창에 아래의 명령어를 입력하여 실행

**>netsh advFirewall firewall add rule name=”ICMP Block incoming V4 echo request” protocol=icmpv4:8,any dir=in action=block**

차단한 상태를 다시 허용하려면 차단한 명령어를 제거.

**>netsh advfirewall firewall delete rule name="ICMP Block"**



리눅스에서 icmp 차단 정책 설정 후 wireshark로 패킷 캡처 화면이다.

ICMP Echo request 패킷만 계속 전송되고 응답이 가지 않고 있다는 사실을 확인할 수 있다