|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:염찬호 | | |  | |
|  | DOS | | | | | | |  |
|  | | -Ping of Death- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. Ping of Death 이란? |
| * 죽음의 핑(Ping of Death)은 해킹 기법의 하나이다. 규정 크기 이상의 ICMP 패킷으로 시스템을 마비시키는 공격을 말한다. |
| 1. 원리 |
| * Ping을 이용하여 ICMP 패킷을 정상 크기 보다 훨씬 크게 만들어 공격 대상에게 보내는 공격이다. |
| * 크기가 큰 패킷은 네트워크 상에서 분할되어 목적지로 전송 된다.      * 분할 되어진 수 많은 패킷을 받은 공격 대상은 부하가 발생해 시스템이 마비 된다. |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| 실습 환경  공격자 PC(kali linux): 1.1.1.130/25  공격 대상 PC(cent OS7): 1.1.1.10/25 |
| 1. 공격 수행 |
| * # hping –-icmp –rand-source 1.1.1.10 -d 65536 –flood |
| |  |  | | --- | --- | | --icmp | 전송할 패킷의 유형(icmp) | | --rand-source | 공격자의 IP 주소를 랜덤하게 생성(알아 보지 못하게) | | 1.1.1.10 | 공격 대상 시스템 | | -d 65536 | 전송할 패킷의 크기 | | --flood | 패킷 전송 속도(빠르게) | |
|  |
| 1. 공격자 PC 패킷 분석 |
| * 출발지 IP 주소를 랜덤한 주소로 변조 하여 공격 대상에게 패킷을 계속 전달 하는 것을 확인 할 수 있다. |

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
| 1. 패킷 분석(tcpdump) |
| * 아래 명령어로 패킷 캡처를 실행 한다.   # tcpdump -w ping-of-death.log   * 아래 명령어로 패킷 결과를 확인 한다.   # tcpdump -r ping-of-death.log     * 랜덤한 주소로 빠르게 패킷을 전송 받고 있는 것을 확인 할 수 있다. |
| 1. 트패픽 과부하 |
| * 공격을 시작하게 되면 다른 컴퓨터에서 icmp 패킷을 보내도 서버 측에서 제대로 응답이 안 되는 것을 볼 수있다. |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |
| 1. 브로드 캐스트나 멀티캐스트 주소로 들어오는 ICMP Echo Request에 대해서 응답하지 않도록 설정 |
| * conf t -> interface serial 0 -> no ip directed-broadcast * ndd/dev/ip ip\_respond\_to\_echo\_broadcast 0 |
|  |
| 1. ICMP Echo Reply패킷을 차단하거나 rate-limit을 이용하여 QoS 설정한다. |
|  |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
|  |
|  |
|  |
|  |
|  |