|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:염찬호 | | |  | |
|  | DOS | | | | | | |  |
|  | | -Inconsistent Fragment- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. Inconsistent Fragmentation 이란? |
| * Bonk   패킷을 플래그먼트 하여 전송할 때 패킷을 조작하여 공격대상자의 시스템에 부하를 주는 공격이다.  처음 패킷을 1번으로 보낸 후 다음 패킷을 보낼 때 순서번호를 모두 1번으로 조작하여 전송하는 DoS 공격이다.   * Boink   Bonk를 수정한 DoS 공격도구로, 처음 패킷을 1번으로 보낸 후 다음 패킷을 100번, 다음 패킷을 200번 등 정상적으로 보내다가 20번째 패킷을 2002, 21번째 패킷을 100, 22번째 패킷을 2002등으로 중간에 패킷 시퀀스 번호를 비정상적인 상태로 보내는 공격기술이다. |
| 1. 원리 |
| * 네트워크 TCP의 약점을 이용한 해킹 기법으로, TCP의 데이터 전송에 있어서 신뢰적인 연결 기능을 악용한다.   신뢰적인 연결 기능을 하기 위해 TCP는 패킷의 순서가 올 바른 지, 손실된 패킷은 없는지, 손실된 패킷이 있다면 손실된 패킷의 재전송 여부 등의 기능을 제공한다. 그리고 위와 같은 조건이 충족되지 않은 데이터 패킷에 대해서는 신뢰를 확인하고자 반복해서 재요청과 수정을 하게 되는데, Bonk공격은 이러한 반복적인 작업을 무한적으로 계속 수행하게 함으로써 시스템의 자원을 고갈시키는 것이다. |

|  |
| --- |
|  |
| 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 |
| * [bonk방식 공격]   # hping -a 200.200.200.200 1.1.1.10 –id 3200 -O 12345 -M 34343 -p 21 -d 320 - |
| |  |  | | --- | --- | | -a 200.200.200.200 | 공격자의 IP 주소를 200.200.200.200으로 위조 | | 1.1.1.10 | 공격 대상의 IP 주소 | | --id 3200 | Id를 3200으로 지정 | | -O 1234 | Offset을 12345로 지정 | | -M 34343 | 시퀸스 넘버를 34343으로 지정 | | -p 21 | 21번 포트에 대해 패킷을 전송 | | -d 320 | 전송하는 패킷의 길이를 320바이트로 | | --flood | 시스템이 생성 가능한 만큼 빠른 속도로 패킷을 보냄 |  * [boink방식 공격]   Bonk 방식과 똑같으나 첫 3번의 패킷만 정상적인 시퀸스 넘버로 보내고 이후부터는 일정한 시퀸스 넘버로 보내는 차이만 있다. 이것은 보안장비가 세번째 까지만 패킷을 검사하는 허점을 이용한 것이다. |
| 1. 공격자 PC 패킷 분석 |
| * 출발지 주소 200.200.200.200에서 공격 대상 PC 주소 1.1.1.10으로 21번 포트로 시퀸스 넘버가 1로 고정되어 공격 되어 지고 있는 것을 확인 할 수 있다. |
|  |
| 3. 공격 결과 |
|  |
| 1. 패킷 분석(tcpdump) |
| * 아래 명령어로 패킷 캡처를 실행한다.   # tcpdump -w bonk.log   * 아래 명령어로 패킷 결과를 확인한다.   # tcpdump -r bonk.log   * 출발지 IP 200.200.200.200이고 시퀸스 넘버 34343:34647으로 반복해서 패킷이 오는 것을 확인할 수 있고 이러한 신뢰성이 확인되지 않은 데이터 전송에 대하여 반복적인 재요구와 수정을 하게 되는 과정에서 시스템 자원이 고갈되어 과부하가 오는 것을 확인할 수 있다. |
| 1. 트래픽 과부하 |
| * 공격을 시작하게 되면 다른 PC에서 ping을 보내도 서버 측에서 제대로 응답이 안 되는 것을 볼 수 있다. |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
| * 최근에 나온 시스템을 파괴할 수 있는 경우는 거의 없는 공격이다. |
| 1. 운영체제별 패치를 한다 |
|  |
|  |
|  |
|  |

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