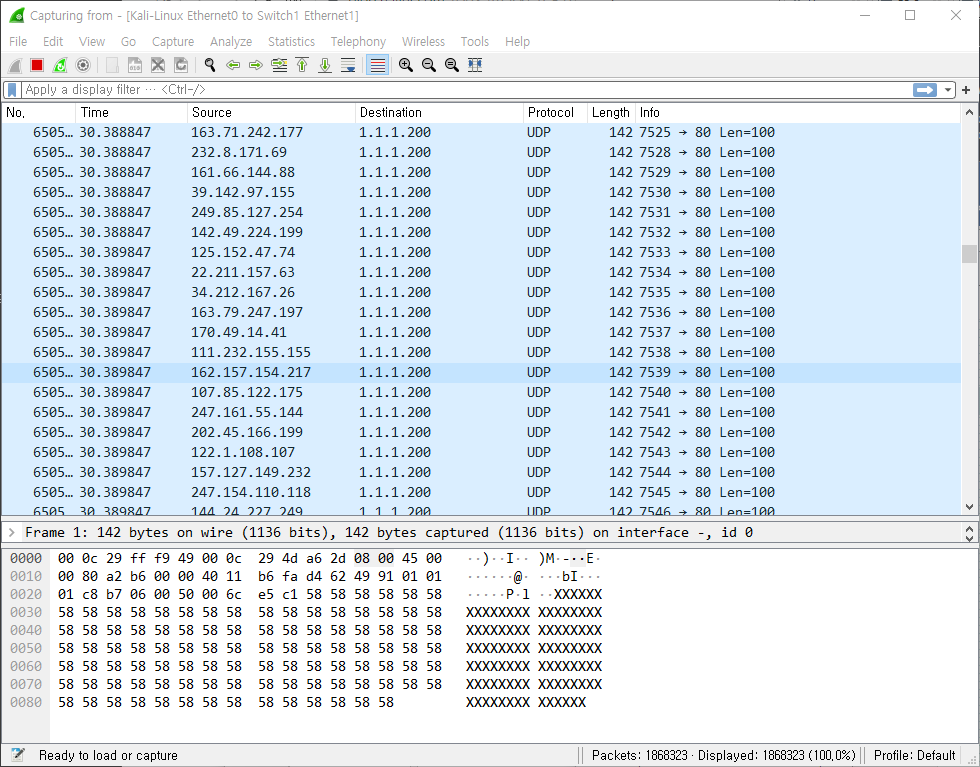
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:김홍규 | | |  | |
|  | UDP Flooding | | | | | | |  |
|  | | -네트워크 보안- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. UDP Flooding 개요 |
|  |
|  |
| 1. UDP Floodings 이란? |
| UDP Flood 공격은 비연결형 컴퓨터 네트워크 프로토콜인 User Datagram Protocol(UDP)을 이용한 Denial of Service(DoS) 공격의 일종으로 SYN Flooding과 유사하지만 비교적 쉬운 공격 방법. 대량의 UDP 패킷을 만들어 보내 상대방이 정상적인 서비스를 하지 못하도록 시스템을 공격 |
| 1. 공격 절차 |
| 1. 출발지와 목적지가 같은 패킷을 공격 대상에 보내면 시스템은 공격자가 처음 보낸 SYN 패킷의 출발지 주소 값을 참조하여 응답 패킷의 목적지 주소를 SYN 패킷의 출발지 주소로 설정해서 보내게 된다. 2. 패킷은 네트워크 밖으로 나가지 않고 자신에게 돌아온다. 3. 돌아온 패킷의 출발지 IP 주소에는 또 다시 자신의 IP 주소가 기록된다. 4. Land 공격이 실행되면 출발지 주소와 목적지 주소가 희생자 IP 주소로 설정되며 희생자는 답신을 자기 자신에게 계속 보내게 되어 패킷은 무한루프에 빠지게 된다. |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정  as |
| 실습 환경  공격자 PC(kali linux): 1.1.1.201/25  타겟 PC(cent os7) : 1.1.1.200 /25 |
| 1. 공격 수행 |
| **-# hping3 [Target IP] -2 --flood- --rand-source -d 100 -p 80**     |  |  | | --- | --- | | hping3 | Flood 공격을 위해 사용하는 패키지 | | 200.200.200.119 | 타겟 IP 주소 | | -2 | UDP 패킷을 사용 | | -flood | 최대한 빠른 속도로 패킷을 전송 | | -rand-source | Client(Source)IP를 랜덤으로 변조 | | -d 100 | 패킷의 데이터 크기를 100Byte로 설정 | | -p 80 | 표적의 80번 포트로 패킷을 전송하라는 옵션값 | |
|  |
| 1. 공격자 PC 패킷 분석 |

* 출발지 IP 주소를 랜덤으로 변조하여 공격대상에 응답이 전달되게 하는 것을 확인 할 수 있다.



|  |
| --- |
| 3. 공격 결과 |
|  |
| 1. 패킷 분석(wireshark) |
|  |
| 1. 트래픽 과부화 |
| * 공격 직후 타겟 PC 에서 과도한 트래팩이 발생된 것을 확인 할 수 있었고, 속도도 저하된 것을 확인 할 수 있다. |
|  |
|  |
| 4. 보안진단 및 대책 |

1) ACL을 이용한 차단 : 웹 서버 혹은 운영 장비에 대한 접근 제어 목록 차단

2) Inbound 패킷 임계치 설정

- 운영 장비로 유입되는 inbound 패킷을 기준으로 PPS 수치를 유입되는 수치보다 낮게 설정

- 임계치 이상의 ICMP 및 UDP 차단

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