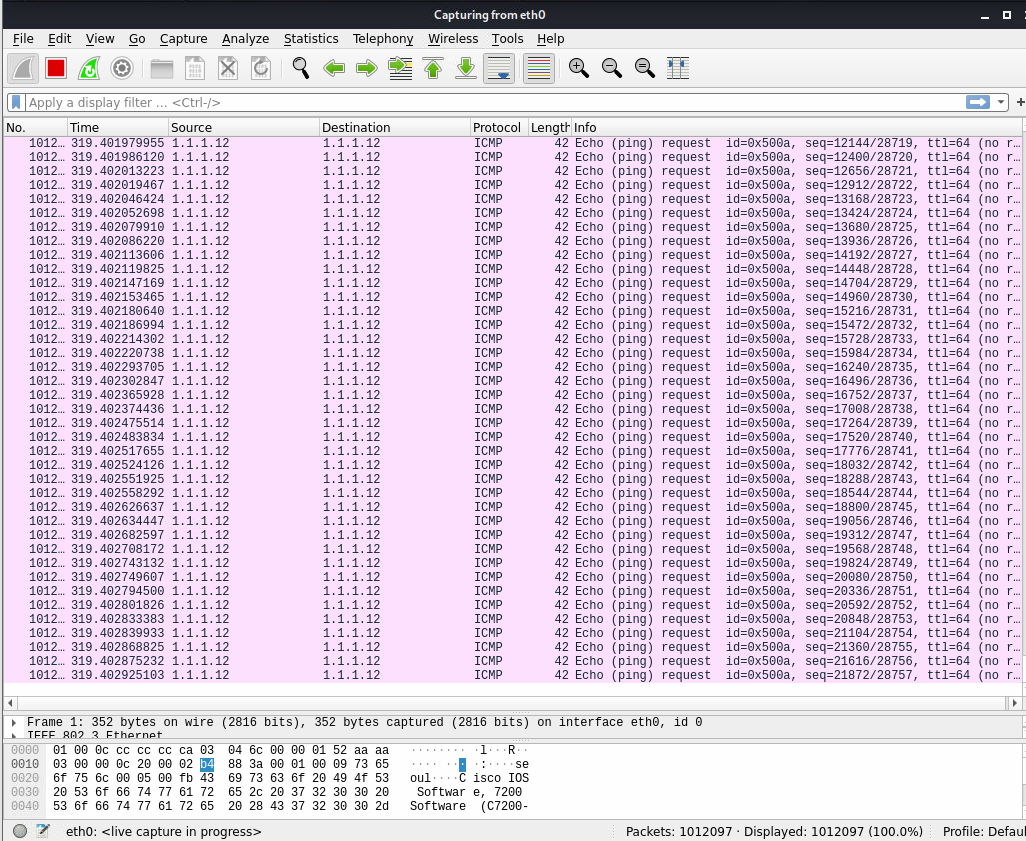
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:신세은 | | |  | |
|  | DOS | | | | | | |  |
|  | | -Land Attack- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. Land Attack 개요 |
| C:\Users\USER\Desktop\1.png |
|  |
| 1. Land Attack 이란? |
| 공격자가 패킷의 출발지 주소(Address) 나 포트(port)를 임의로 변경하여 출발지와 목적지의 주소(또는 포트)를 동일하게 함으로써, 공격 대상 컴퓨터의 실행속도를 느리게 하거나 동작을 마비시켜 서비스 거부 상태에 빠지도록 하는 공격방법이다. |
| 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): 1.1.1.10/25  타겟 PC(cent os7) : 1.1.1.12 /25 |
| 1. 공격 수행 |
| **-# hping3 –a <공격대상IP> <공격대상IP> --icmp –flood**  **-# hping3 –a <공격대상IP> <공격대상IP> -s 80 –k –p 80 –S –flood**     |  |  | | --- | --- | | -a | 출발지와 목적지 IP 타겟 지정 | | -s | 출발지 포트 값을 80번 포트로 지정 | | -p | 목적지 포트 값을 80번으로 지정 | | -k | 포트 고정 | | -S | Syn 패킷을 보냄 | |
|  |
| 1. 공격자 PC 패킷 분석 |

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



|  |
| --- |
| 3. 공격 결과 |
|  |
| 1. 패킷 분석(wireshark) |
| -출발지 주소와 목적지 주소가 같은 것을 확인 할 수 있다.  -Packet을 받은 server는 응답을 보내주지만 목적지 주소가 자기 자신이므로, SYN Packet은 server 내부에서 계속 돌게 된다.    hping3 –a 1.1.1.12 1.1.1.12--icmp –flood    hping3 –a 1.1.1.12 1.1.1.12 -s 80 –k –p 80 –S –flood |
| 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 |
| * 현재는 대부분의 OS에서 해당 취약점이 해결되어 이론적으로만 존재하는 공격이다. |
| 1. 침입차단 시스템 또는 OS 패치를 통해 출발지 주소와 목적지 주소가 동일한 패킷을 차단시킨다. |
| * Watch Mode   C:\Users\USER\Desktop\1.png   * + 1. 타겟 서버의 앞에 있는 라우터/ 방화벽 장비에서 Packet을 감시한다.     2. Packet 중에서 출발지 주소와 목적지 주소, 출발지 포트와 목적지 포트가 동일한 packet이 있는지 감시한다.     3. Land Attack에 해당하는 Packet 인 경우, 라우터/방화벽 장비에서 차단한다. |

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