|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:염찬호 | | |  | |
|  | Scanning | | | | | | |  |
|  | | -tcp ack scan- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. Tcp ack scan 이란? |
| * 포트의 오픈 여부를 판단하는 것이 아니라 방화벽의 룰셋을 테스트하기 위한 스캔이다. * Ack 플래그만 설정해서 보낸다. * 방화벽에서 필터링 된다면 응답이 없거나 ICMP 메시지를 받고 필터링 되지 않으면 RST+ACK를 받는다. * 방화벽이 stateful한 필터인지 아니면 단순히 들어오는 syn패킷을 차단하는 필터링인지를 점검하는 목적으로 사용된다. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| 실습 환경  공격자 PC(kali linux): 1.1.1.12/25  공격 대상 PC(cent OS): 1.1.1.10/25 |
| 1. 공격 수행 |
| * #nmap -sA -P0 -p 20,21,23,25,53,80 1.1.1.10 |
|  |
|  |
|  |

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
| 1. 패킷 분석(wireshark) |
| * 방화벽이 미설정 되어 있어 공격자가 보내온 신호에 대해 RST신호로 응답을 해주는 것을 확인할 수 있다. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |
| 1. 방화벽을 설정한다. |
| * #systemctl start firewalld |
|  |
|  |
|  |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
| 1. 방화벽 설정이 되었을 경우 |
| * 방화벽이 켜져 필터 되고 있음을 알 수 있다. |
| * 방화벽 설정 시 공격자가 보낸 신호에 대해 ICMP프로토콜을 이용해서 Destination unreachable로 응답하고 있다. |
|  |
|  |