|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:문관필 | | |  | |
|  | <SMURF, FRAGGLE Attack> | | | | | | |  |
|  | |  | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| SMURF 공격은 같은 네트워크 상의 사용자들에게 송신지를 Target IP로 속인 뒤 ICMP echo Request 메시지를 Broadcast로 날린다. |
|  |
| 그러면 메시지를 받은 호스트들은 Target IP로 ICMP echo Reply 메시지를 보내게 되는데, 이 과정을 여러 번 반복하여 공격 대상의 서비스를 다운 시키는 DoS 공격의 한 종류이다. |
|  |
|  |
|  |
| FRAAGLE 공격은 Smurf 공격과 비슷하지만 ICMP 대신 UDP를 사용한다는 것이 다른점이다. |
|  |
| 공격자는 브로드캐스트 주소로 포트 7(echo)를 이용해 UDP 패킷을 전송한다. 그렇게 되면 echo가 가능한 네트워크 내의 시스템들은 엄청난 트래픽을 생성하고 희생자에게 응답을 보내게 된다. |
|  |
|  |
|  |
| 이 두 공격은 ICMP, UDP 차이 밖에 없으므로 SMURF 공격으로 실습을 진행한다. |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| |  |  |  | | --- | --- | --- | | 실습 환경 | IP Address | OS | | 공격자 | 1.1.1.3/24 | Kali Linux | | 희생자 | 1.1.1.1/24 | Ubuntu |  1. 토폴로지 구성 |
| 1. 공격   공격자 PC(Kali)에서 hping3를 사용해 공격을 수행 |
| hping3 [희생자 Gateway] -a [Target IP] –-flood --icmp  -a : Source IP 변경  --flood : flood 공격  --icmp : icmp 패킷 |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
|  |
| 공격자의 PC에서 패킷을 보면 공격자가 1.1.1.1의 주소를 출발지로 하고 Gateway에게 무수히 많은 echo Request를 보내는 것을 알 수 있다. |
|  |
| 희생자의 PC에서도 echo Reqly를 계속 받고 있는 것을 확인 할 수 있다. 결국 서비스에 문제가 생긴다. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| <FRAGGLE 공격 패킷> |
|  |
| <희생자 PC에서 패킷 확인> |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |
| 1. 다른 네트워크로부터 자신의 네트워크로 들어오는 IP Broadcast 패킷을 막는다.      * no ip directed-broadcast  1. 호스트들은 IP Broadcast 주소로 전송된 ICMP 패킷에 대해서는 응답을 하지 않도록 설정  * # cat /proc/sys/net/ipv4/tcp\_syncookies 명령으로 확인값이 1 이 아니면,   # sysctl -w net.ipv4.tcp\_syncookies=1 로 값을 수정해주면 된다. |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
|  |
|  |
| 공격자 PC에서 똑같이 공격을 시도해보고 있다. |
|  |
|  |

하지만 희생자의 PC에서는 공격 패킷이 들어오고 있지 않은 것을 확인할 수 있다.