|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:문관필 | | |  | |
|  | <Security Misconfiguration> | | | | | | |  |
|  | | Denial of Service(Slow HTTP Dos) | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| Security Misconfiguration   * OWASP TOP 10 A5(잘못된 보안 구성) * 서버 / 시스템 / DB / 네트워크 장비 / 웹 설정 오류로 인하여 발생하는 취약점   EX) Directory listing, Error Page, Web Page 주석, Web Server 기본 설정, Adobe Flash 취약점  Dos / DDos 공격, 특정 서비스에 대한 Reverse\_TCP 공격, 로컬 권한 취약점, 백업 / 임시 / Robot 파일     * 설정 오류 / 미비 항목들 중 대표적인 예   EX) 클라우드 서비스 접근 권한 설정이 올바르지 않음  필요하지 않거나 감춰야 할 서비스 / 기능을 설치했거나 활성화함(서버 포트 외 다른 포트 개방, 불필요한 슈퍼계정 / 권한, 불필요한 HTTP Method, Debug 모드 등등)  애플리케이션 서버(Tomcat, Apache) / 프레임워크(Spring, ASP.Net)의 보안 설정을 세팅하지 않음  Application Stack 내에서 오래되거나 취약점이 있는 버전을 사용함.  유저들에게 서버의 디렉토리 구조를 모두 혹은 일부 노출시킴.  웹 서버의 프로그램 혹은 버전을 노출시킴  기타 등등..  Dos/DDos 공격   * 대량 패킷들을 전송하여 시스템/서버/네트워크 리소스를 고갈시켜 부하 발생, 요청 방해 및 연결 거부를 발생하는 공격 * DDos는 악성 코드에 감염된 시스템들을 이용하여 Dos 공격을 실시하는 방법   Slow HTTP Dos   * 메시지 헤더의 마지막을 알리는 ‘empty line’을 포함시키지 않고 HTTP 요청을 조금씩/천천히 전송하여 웹 – 서버 대기 현상을 발생시키는 공격 * HTTP 헤더에 Carrige Return을 보내지 않음으로써 서버에게 더 보낼 데이터가 있는 것처럼 만들어서 연결 상태를 유지하는 공격 -> 서버에서 TCP 세선 개수가 계속 늘어나기 때문에 다른 연결을 실시 할 수 없게 된다. * 즉 , 웹 서버가 수신한 HTTP 헤더의 CRLF(0d 0a)가 두 번 들어간 정보를 보고 Body 부분을 인식하는데 이것을 한번만 인식하게 되면 Body 내용이 아직 도착을 안한 것으로 인식하여 대기하게 된다. |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| |  |  |  | | --- | --- | --- | | 실습 환경 | IP Address | OS | | 공격자 | 192.168.1.102/24 | Kali Linux | | 희생자 | 192.168.1.205/24 | Ubuntu(Bee-box) |  1. 환경 구성   **WEB SERVER**  **HACKER**  192.168.1.102 192.168.1.205 |
| 1. 공격  * 보안 레벨 선택 및 시나리오 선택      * bWAPP를 타겟으로 하여 공격 실시      * Wireshark 실행 후 ip.addr==[beebox\_ip] && ip.addr==[kali\_ip]로 필터링 |
| * Kali에서 Metasploit 실행      * Slow HTTP Dos 공격을 위한 Exploit Code를 검색, 사용      * 옵션을 확인하고 공격 대상(beebox)의 IP를 설정해준 뒤 공격 수행 |

|  |
| --- |
|  |
| 3. 공격 결과 |
| * Wireshark에서 패킷 확인     위와 같이 패킷의 마지막 부분에 0d 0a를 확인할 수 있다. 이는 정상적인 HTTP 헤더의 끝이 아니므로, 서버는 계속 연결을 유지한다.   * BeeBox에서 연결 상태 확인     공격이 어느 정도 수행이 되면 Beebox에서 연결을 수용할 수 있는 한계치에 도달하게 되고, 다른 시스템에서 Beebox로 접속을 하게 되면 굉장히 느린 것을 확인 할 수 있다. |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |
|  |
|  |
|  |
|  |
|  |

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