|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:문관필 | | |  | |
|  | <Security Misconfiguration> | | | | | | |  |
|  | | Arbitrary File Access(Samba) | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 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.. |
|  |

|  |
| --- |
|  |
| 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        * Samba 취약점을 이용한 임의적인 파일 접근      * 공격자의 PC에서 Samba 서버에 대해 포트 스캐닝 실시 |
| 139번, 445번 포트가 활성화 되어있는 것을 확인 할 수 있다.   * Metasploit을 이용한 공격 실시     msfdb 생성 및 초기화    Samba 모듈 검색    그 중 exploit/unix/distcc\_exec 복사    exploit/unix/distcc\_exec 사용    show options로 옵션 확인 후 rhost를 Target IP로 설정    cmd/unix/reverse로 payload 설정  lhost를 공격자 IP로 설정 후 run  공격에 성공해 명령어들이 정상적으로 작동하는 것을 확인 |
|  |
|  |
|  |

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
| 공격에 성공 후 명령어들이 정상적으로 작동하는 것을 확인 할 수 있다. |
|  |
|  |
|  |

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

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