**Best of Best 11**

**HORANGI**

**김종현 멘토님 과제 #4 번**

**Best of Best 11기**

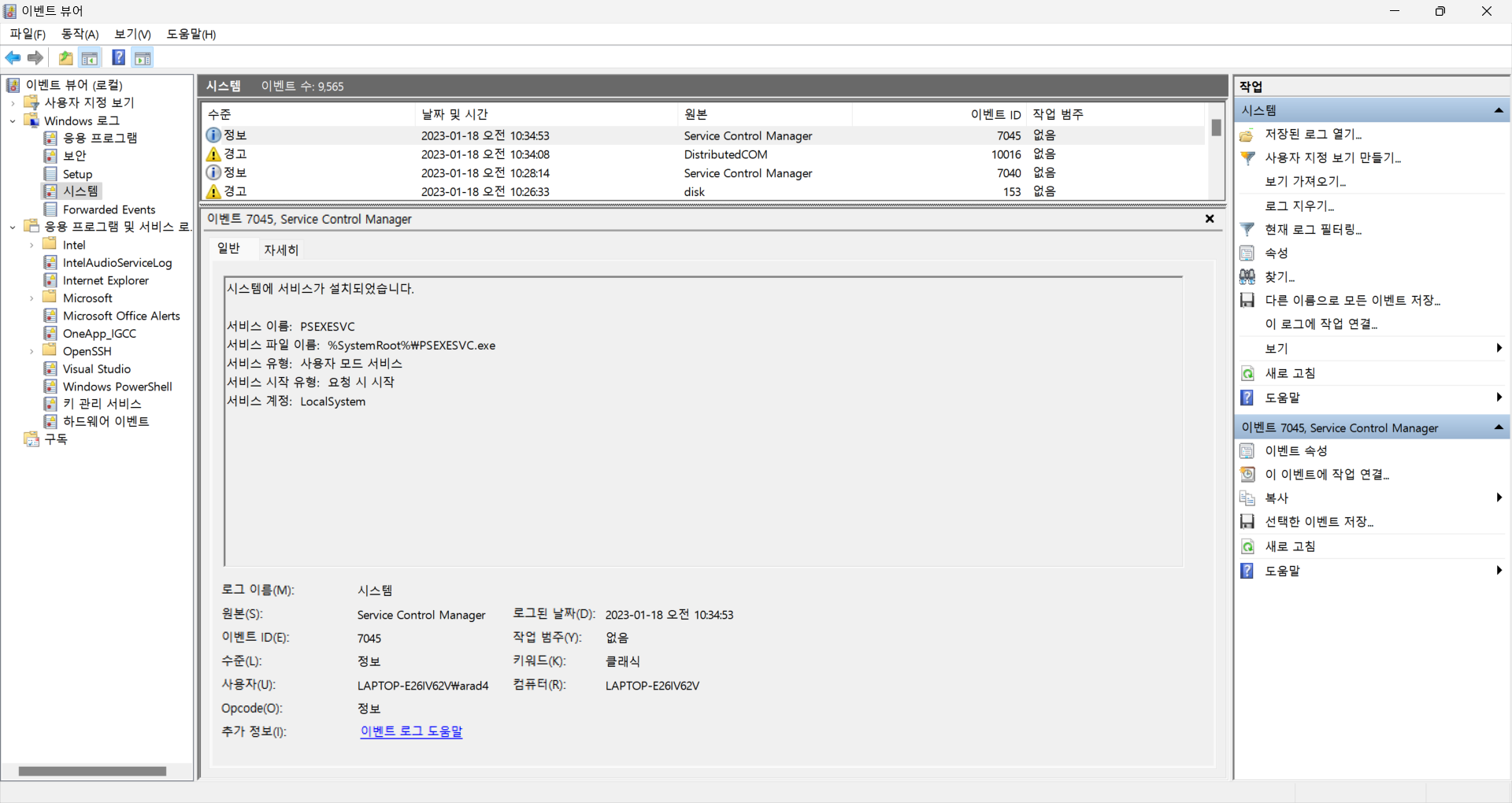
**보안제품 개발 정경재**

**제출날짜:2023-01-12**

1. PsExec 처음 실행 시 라이센스 동의 프롬프트가 발생하게 되는데, 사용자가 동의 버튼을 눌렀을 때 비로소 실행이 됩니다. 그 이후, 어플리케이션을 재 실행하게 되면 더이상 라이센스 프롬프트가 발생하지 않게 됩니다. PC는 어떻게 이를 감지하는 것일까yo?  
   프로세스가 라이선스를 확인하는 방법은 2가지 정도 있는 것 같습니다.  
   그중 첫번째 방식은 간단히 프로세스가 동작하면 프로세스에 해당하는 윈도우 레지스트리에 가서 정보를 확인하는 방법입니다.  
   PsExec, 프로세스 모니터 등 다양한 윈도우 프로그램은 실행 시 프로그램들의 고유한 레지스트리 위치에서 라이선스 동의와 관련된 정보를 얻는 과정을 거칩니다.  
   이때 만약 특정 위치에 레지스트리 값이 없다면 생성 후 사용자에게 라이선스 이용 동의를 얻는 창을 띄우고 동의 여부를 레지스트리에 저장합니다.  
   (아래의 왼쪽은 레지스트리 편집기 오른쪽은 레지스트리 값의 위치입니다.)  
    텍스트이(가) 표시된 사진

   자동 생성된 설명텍스트이(가) 표시된 사진

   자동 생성된 설명[[1]](#footnote-1)위의 자료와 같이 레지스트리에는 프로그렘에서 정한 정보가 담겨 있고 이 저장된 정보를 매번 읽어고 확인해 사용자에게 인증을 진행하지 않는 것입니다.  
   두번째 방식은 txt와 같은 문서 파일을 통해 사용자의 라이선스 동의 정보를 얻는 것 입니다.  
   두번째 방식은 IBM에서 일반 사용자 라이선스 계약인증 메커니즘[[2]](#footnote-2)을 토대로 이야기드리면 사용자가 라이선스 키를 입력을 하고 해당 라이선스를 인증을 합니다.  
   인증된 라이선스의 경우 특정위치에 txt파일로 내용을 저장하고 매번 프로그램이 실행하는 시점에 해당 파일을 읽어 사용자에게 라이선스 동의 창을 띄우지 않습니다.
2. PsExec를 이용해서 진행 할 수 있는 명령어들에 대해 조사해보아yo. 그리고, 명령어를 실행해보고 침해사고 분석가 입장에서 IOC 정보를 Windows event를 통해 식별해 보아yo.  
   - PsExexec를 통해 실행할 수 있는 명령어들은 다음과 같습니다.  
   기본적인 System32 하위에 있는 프로그램들이 가능하며, 추가적으로 Command Line Util들과 Script, Window Service, Batch file, power shell 명령어 등 다양한 프로그램을 실행할 수 있습니다  
   텍스트이(가) 표시된 사진

   자동 생성된 설명[[3]](#footnote-3)  
   - PsExec 명령어를 통해 직접 윈도우 로그를 확인해본 결과입니다.  
   처음에는 VM을 통해 가상환경에서 진행하려고 하였으나 네트워크 및 윈도우 충돌등의 문제로 인해 로컬에서 실습을 진행했습니다.  
   (아래 사진들은 실제 로컬의 PsExec를 통해 나온 윈도우 이벤트 로그들과 실제 실행 명령어 입니다.)  
   텍스트이(가) 표시된 사진

   자동 생성된 설명  
   다음과 같이 PsExec를 통해 Powershell, ipconfig 등 다양한 명령어를 실행한 결과 윈도우 이벤트상에서 시스템에 서비스가 설치 되었다는 로그와 함께 PsExec로 실행한 결과는 나오나, 정확히 무슨 프로그램인지는 나오지 않습니다.
3. Lateral movement 중 Pass-the-ticket에 대해 조사해 보아yo.  
   Microsoft사[[4]](#footnote-4)에서 이야기한 Pass-the-ticket은 공격은 다음과 같이 이야기힙니다.  
   Pass-the-Ticket 공격은 공격자가 한 컴퓨터에서 Kerberos 티켓을 도용하고 이 티켓을 다시 사용하여 다른 컴퓨터에 액세스하는 데 사용하는 측면 확대 기술입니다. 이 검색에서 Kerberos 티켓이 둘 이상의 컴퓨터에서 사용되는 것으로 표시됩니다.   
     
   자세한 방법은 다음과 같이 동작합니다. (NetWrix)[[5]](#footnote-5)  
   첫번째로는 사용자의 티켓을 훔칩니다.  
   다양한 프로그램과 방법을 통해서 티켓을 훔칠 수 있습니다.  
   ex) Mimikatz의 경우   
   mimikatz.exe "privilege::debug" "sekurlsa::tickets /export"  
     
   두번째는 훔친 티켓을 재사용합니다.  
   mimikatz.exe "kerberos::list"  
     
   세번째는 타겟 시스템을 정찰해 정보를 얻습니다.  
   net user joed /domain  
     
   네번째로는 타겟 시스템에 훔친 티켓을 통해 접속을 합니다.  
   .\PsExec.exe \\workstation456 powershell.exe

1. Psexec [License Agreement 창 Skip](https://www.snoopybox.co.kr/1684): <https://www.snoopybox.co.kr/1684> [↑](#footnote-ref-1)
2. IBM 일반 사용자 라이선스 관리: <https://www.ibm.com/docs/ko/sva/10.0.0?topic=authentication-configuring-end-user-license-agreement-mechanism> [↑](#footnote-ref-2)
3. Chat GPT [↑](#footnote-ref-3)
4. Microsoft Document: <https://learn.microsoft.com/ko-kr/defender-for-identity/lateral-movement-alerts> [↑](#footnote-ref-4)
5. NetWrix Pass-the-ticket Attack: https://www.netwrix.com/pass\_the\_ticket.html [↑](#footnote-ref-5)