**호남 대학간 침해대응/분석 대회 2022**

Phase 2 두번째 과제

윈도우PC 침해 진단 보고서

|  |  |
| --- | --- |
| 팀 명 |  |
| 팀 원 |  |
| 소속대학 |  |



|  |
| --- |
| **-작성요령-**   1. 주어진 범위 내에서 자유롭게 작성하시면 됩니다. 챕터의 추가나 제거, 변경도 가능합니다. 단, 적절한 가독성은 확보되어야 합니다. 2. 제출시에는 작성요령 및 기타 안내와 주석들은 제거하셔야합니다. 3. **제출은 반드시 PDF로 제출하셔야합니다.** |

|  |
| --- |
| **-출제의도-**   1. 침해사고 준비도(또는 포렌식 준비도)란 침해사고 발생시 관련된 디지털 증거를 법적 증거로써 효력을 갖추기 위하 일련의 과정, 디지털 포렌식에 의한 수집 및 분석에 있어 필요한 계획 및 시스템, 자원 활용 방안 등에 대한 전반적인 준비활동을 말합니다. 2. 잘 구축된 침해사고 준비도는 침해사고 발생 시 신속하게 사고 원인을 파악하게 해주어 시스템의 공백은 물론 관련 비용과 시간을 최소화 해줄 수 있을 뿐만 아니라, 법적 분쟁에서 큰 역할을 하기도 합니다. 3. 따라서 이번 과제에서는 이러한 침해사고 준비도와 그 효과에 대해 파악해 봅시다! |

**1. 침해사고 준비도**

|  |
| --- |
| **-작성요령-**   1. 침해사고 발생 시 적절한 디지털 증거와 현황이 확보되지 않는다면 당연히 그 원인 분석이 쉽지 않겠죠! 2. 실제 사례에서도, 로그나 관련 데이터들이 단기간에 유실되어 사고를 분석하는데 어려운 경우가 많습니다. 3. 따라서 효율적인 대응을 하기 위해서는 분석에 활용가능한 정보를 확보할 수 있는 여러 기술적 준비가 되어야 합니다. 4. 제공된 시나리오 환경(윈도우 PC)에서 기술적으로 적용할 수 있는 준비도에 대해 작성해 보세요.  * 자산, 예상되는 침해 유형, 증거 수집 등 기타 다른 부분은 작성하지 않아도 되지만, 로그 확보, 모니터링 프로그램 설치 등 기술적으로 보완할 수 있는 부분은 반드시 작성해주세요. |

**2. 침해사고 준비도 적용**

|  |
| --- |
| **-작성요령-**   1. 침해사고 준비도의 가장 중요한 덕목은 당연히 ‘실제 활용 할 수 있는’ 입니다. 2. 1에서 작성한 준비도를 Phase 2-1 가상머신에 적용해봅시다. 3. 적절하게 준비도가 작성 되었는지 확인할 수 있겠군요! |

**3. 적용된 머신에서 악성행위 재현**

|  |
| --- |
| **-작성요령-**   1. 침해사고 분석 시 가장 중요한 요소 중 하나는 침입 행위에 대해 정확히 파악하는 것입니다. 2. 우리의 시나리오에서는 악성코드에 의한 감염이었으니, 그 악성 코드를 기반으로 한 각종 행위들을 정확히 파악할 필요가 있겠죠. 3. 지난 바이너리의 타겟 ip와 동일하게 nc -lvp 8080을 열고 있으면, 리버스쉘 이후의 행위를 재현할 수 있습니다. 4. 이를 이용해, 내부망에 다른 PC를 설정한 후 리버스쉘 이후 실행 행위를 재현하여 보세요. |

**4. 준비도 적용 전/후 분석 데이터 비교**

|  |
| --- |
| **-작성요령-**   1. 마지막으로 준비도가 적용 된 것과 적용되지 않은 것에 대한 차이를 파악해봅시다. 2. 준비도 적용으로 인해 확보가능한 추가 분석 데이터를 첫번째 과제의 보고서와 비교하여 작성순으로 작성해주세요 |