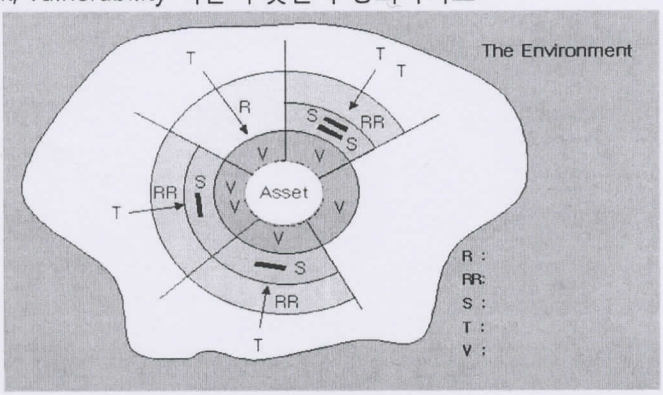
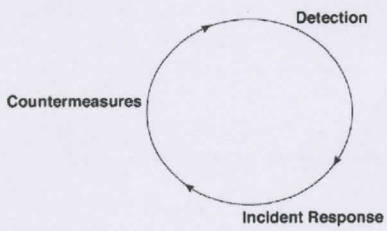
Incident Response Exam

1. threat, risk, vulnerability 이란 무엇인지 정의하시오.



2. 아래 life cycle 모델에서 countermeasures, detection, incident response 에 대해 각각 정의하시오.

Figure 1.1. The computer/information security life cycle.



3. web defacement 가 발생하였을 때 조직에 발생할 수 있는 피해는 어떤 것이 있을지 기술하시오.
4. Incident response methodology 중에서 PDCERF의 각 6단계에 대해 약어를 풀어 쓰고, 각 단계의 주요 목표는 무엇인지 기술하시오.
    a. P ( ) : 목표
    b. D ( ) : 목표
    c. C ( ) : 목표
    d. E ( ) : 목표
    e. R ( ) : 목표
    f. F ( ) : 목표
5. Incident response 에 있어서 외부 contractor 또는 consultancy 를 outsourcing 할 때와 내부 역량 (in-house capability)을 이용하여 대응할 때의 각 장단점을 기술하시오.
    a. In-house: 장점
    b. In-house: 단점
    c. Outsourcing: 장점
    d. Outsourcing: 단점

정보보호 이론 종합시험

2013년 6월 22일

♠ 문제지에도 학과, 학번, 이름을 기입하여 답안지와 같이 제출하시오. 문제지가 없으면 0점 처리됩니다

학번: 이름:

1. 공개키 암호와 비밀키 암호의 장단점에 대하여 표로 만들어 설명하시오.(20점)
2. RSA 공개키 암호에서 $n = 33$, $e = 7$이고 암호문이 26일 때 평문을 구하시오(15점)
3. 디피-헬만 키 공유 방식을 설명하고, 이 방식의 취약점과 이를 보완할 수 있는 방법에 대하여 설명하시오.(20점)
4. 전자서명에 해쉬함수가 사용되는 이유를 설명하시오.(15점)
5. A가 자기의 인증서를 B에게 줄 경우 인증서로부터 B가 얻을 수 있는 정보와 B가 얻은 정보의 진위 여부를 어떻게 확인하는 지 설명하시오. (15점)
6. PGP에서 데이터를 암호화할때 압축을 먼저한 후 암호화를 실행한다. 그 이유를 설명하시오.(15점)

디지털 포렌식 기술

1. A와 B가 관련된 사건을 조사하기 위해 B의 스마트폰에 대한 영장을 받아 압수하여 조사하던 중 B와 C 사이에 발생한 범죄의 단서가 포착되었다. 이후 진행해야 하는 수사 절차를 간략히 설명하라.

2. 피의자가 작성한 디지털 데이터가 전문 증거인 경우에 성립의 진정을 다투는데 이에 대한 문제점을 언급하고 올바른 방향을 제시하라.

3. 윈도우 7을 사용하던 직원이 기술 유출을 하였다. 이를 조사하기 위한 기술적 절차를 설명하라.

4. 압수한 HDD를 법정에서 검증하기 위해 해쉬 값을 계산하였는데 보관 중이던 해쉬 값과 달랐으며, 분석용으로 가지고 있던 이미지 파일은 해쉬 값이 일치하였다. 이러한 경우, 최선의 해결책을 제시하라.

5. Gmail처럼 외국에 데이터가 존재하는 경우가 많이 있으며, 이를 압수 수색할 필요성도 있다. 한편 수사 사실이 알려지게 되면 대상자는 원격에서 해당 데이터를 쉽게 삭제할 수 있다. 이를 해결하면서 원격지 데이터를 압수 수색할 수 있는 기술적, 절차적, 법률적 대책을 제시하고 실현 가능성을 설명하라.