한국인터넷진흥원 침해사고 분석 절차 안내서

챕터 1. 서론

BoB7기 취약점분석 정성조

최근 인터넷 침해사고는 금전적 이익이 목적이며 복잡해지고 있다.

국내 홈페이지 해킹 후 악성코드 은닉을 통해 개인정보를 유출시키고, 웹서버를 해킹하여 피싱 사이트로 악용한다. 또한 좀비 컴퓨터를 만들어 DDoS, 스팸, 와레즈 사이트 등에 악용된다.

침해사고 탐지가 어려워짐에 따라 침해사고에 대한 적절한 대응이 부족하여 피해가 확산되거나 반복적으로 피해를 입고 있다

본 안내서에서는 이에 대응하기 위한 분석절차와 기술로 좀비PC 분석 및 대응, 홈페이지 악성코드 은닉 사고를 중심적으로 소개한다.

2장에서는 단계별 침해사고 분석 절차를, 3장에서는 운영체제, 네트워크, 데이터베이스 각각의 사고분석 기술을, 4장에서는 홈페이지 악성코드 은닉 사고와 좀비PC의 분석절차를 소개한다.