<2021 원자력학회 추계학술대회>

사이버보안 사건으로부터 배운 교훈

2021. 10. 22.

이정호

(friend25kr@kinac.re.kr)

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

목 차

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

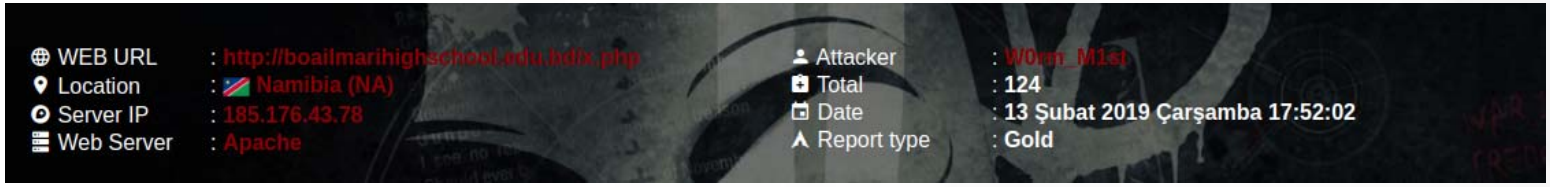
개 요

- **KINAC 정보보안**
  - KINAC 정보보안요령 (G-01-01)
    - **정보보안** 또는 **정보보호**라 함은 **정보시스템 및 정보통신망**을 통해 **수집/가공/저장/검색/송수신** 되는 **정보의 유출/위변조/훼손** 등을 방지하기 이한 **관리적/물리적/기술적 수단**을 강구하는 일체의 행위로서 **사이버보안 포함**
    - **사이버보안**이라 함은 사이버공격으로부터 **정보통신망을 보호**함으로써 **정보통신망**과 **정보의 기밀성/무결성/가용성 등 안전성을 유지**하는 상태를 말한다.

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

사이버보안 사건 개요

- **사건 개시: 일명 불가리아 사건**
  - 2021.1.6. 10:53 사이버보안센터으로부터 통보
  - 통보내용(사건번호: 21-0105221508-025)
    - 2021.1.5. 20:00경 210.119.XX.XXX -> 185.176.43.78 접속시도
- **불가리아 사건 초기 조사**
  - 불가리아 IP(185.176.43.78): Zetta Hosting Solution사 보유
    - 나미비아 소재 W0rm_M1st라는 해커에 의해 악용사례
    - 인도네시아 등에서 유사한 침해사례 보고

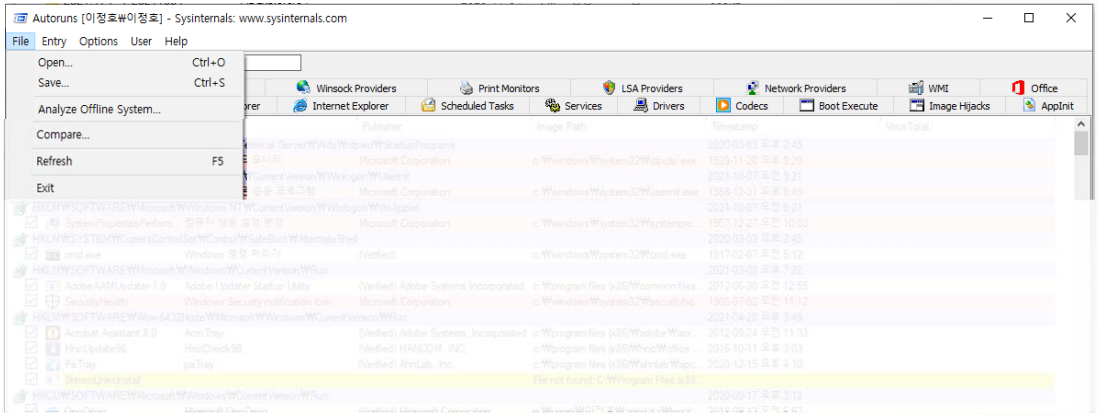


  - 피해시스템: 외부망 NMS(Network Management System) Client
    - 외부망NMS(침해시스템)와 내부망NMS(건전시스템)의 프로세스 비교
    - 내부망NMS에 없으나 외부망NMS에 있는 프로세스 의심

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

사이버보안 사건 조사

- **불가리아 사건 조사**
  - ➢ 내부망NMS와 외부망NMS의 프로세스 비교
    - ➢ Windows 프로세스 분석기(SysInternals)를 이용한 대조
    - ➢ 불가리아IP 접속시도 의심 프로세스 식별



  - ➢ 방화벽 로그 분석
    - ➢ 2020년 7월부터 간헐적으로 불가리아IP에 접속하여 특정 파일을 다운로드 시도
    - ➢ 외부망NMS Client 이외에 원내일부 PC들이 미국,프랑스,중국,이스라엘 등으로 간헐적으로 접속을 시도하는 부가적인 사실 발견

사이버보안 사건 조사

- **피해시스템 조사**
  - 외부망NMS Client를 휴대전화로 테더링하여 인터넷에 연결 (원내 네트워크와 격리)
  - 문제IP들로 접속하는 여부를 네트워크 분석기로 모니터링하여 접속을 시도하는 프로세스를 찾음
  - 악성코드들은 간헐적으로 접속을 시도하므로 찾는데 많은 시간 소요
  - 접속을 시도한 프로세스들을 V3 최신엔진으로 스캔하였으나, 발견되지 않아 안랩에 통보
  - 분석과정에서 침해시스템에서 타 시스템으로 접속을 시도한 이력이 있어, 네트워크에서 격리조치
  - 분석과정에서 유해IP로 접속을 시도하는 일부 직원PC를 발견하고 해당 직원에 통보하고 PC포맷을 권고

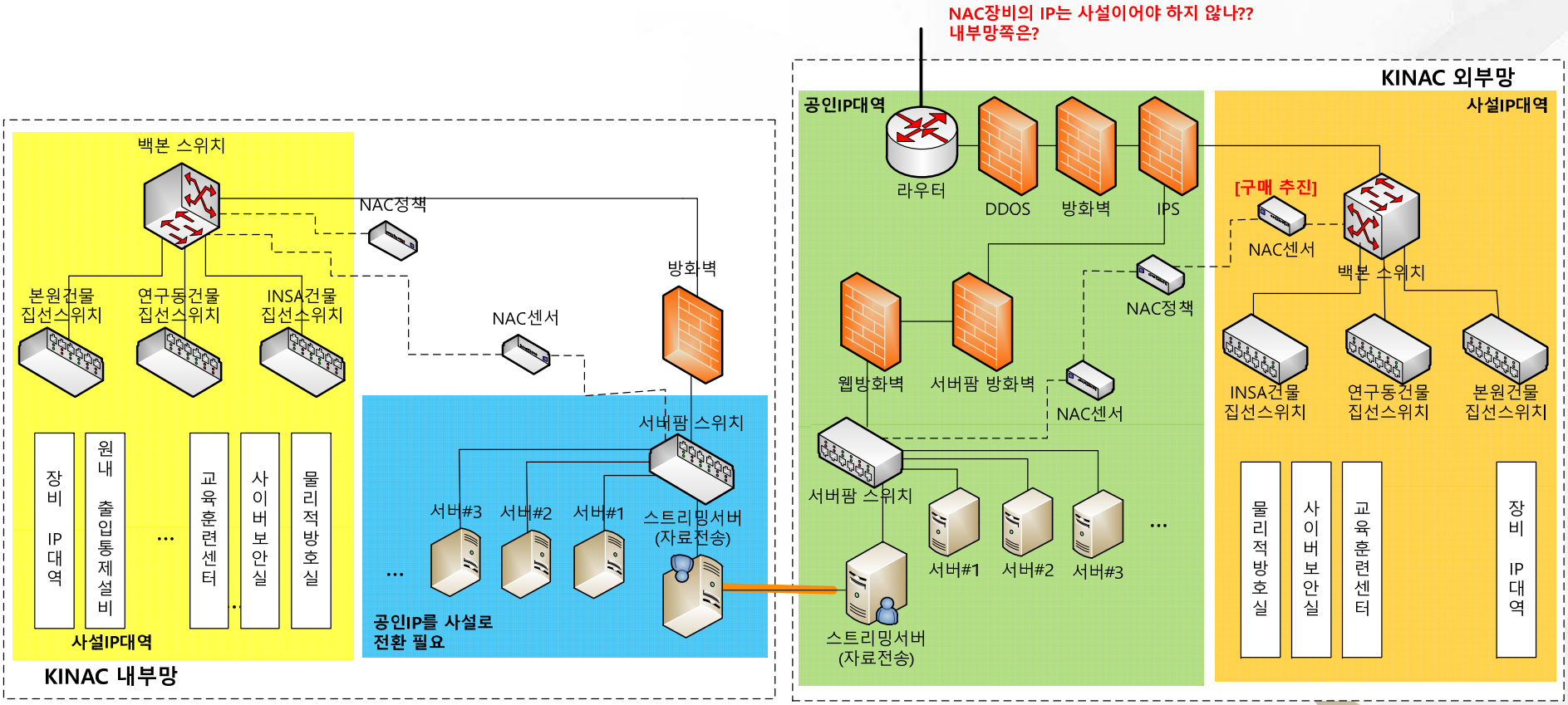
사이버보안 사건 조사

- **피해시스템 조사**
  - 문제가 된 웜바이러스(불가리아IP접속)는 침투한지 6개월 이상 된 것으로 판명 => 방화벽 보안로그를 모니터링 필요
  - 외부망NMS는 기술지원이 종료된 윈도우7을 버젼이 사용하고 있었음 => 관리사각지대 존재 (윈도우7 사용, 필수설치SW를 설치하지 않은 PC를 네트워크에서 격리)
  - 웜바이러스 등 조사를 위한 인적/물적 기반 개선 필요
    - 감염PC 조사를 위한 별도 네트워크, 조사에 필요한 SW, 감염시스템 격리후 대체PC 등 미비
    - Cyber Forensic 능력을 갖춘 인력 필요

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

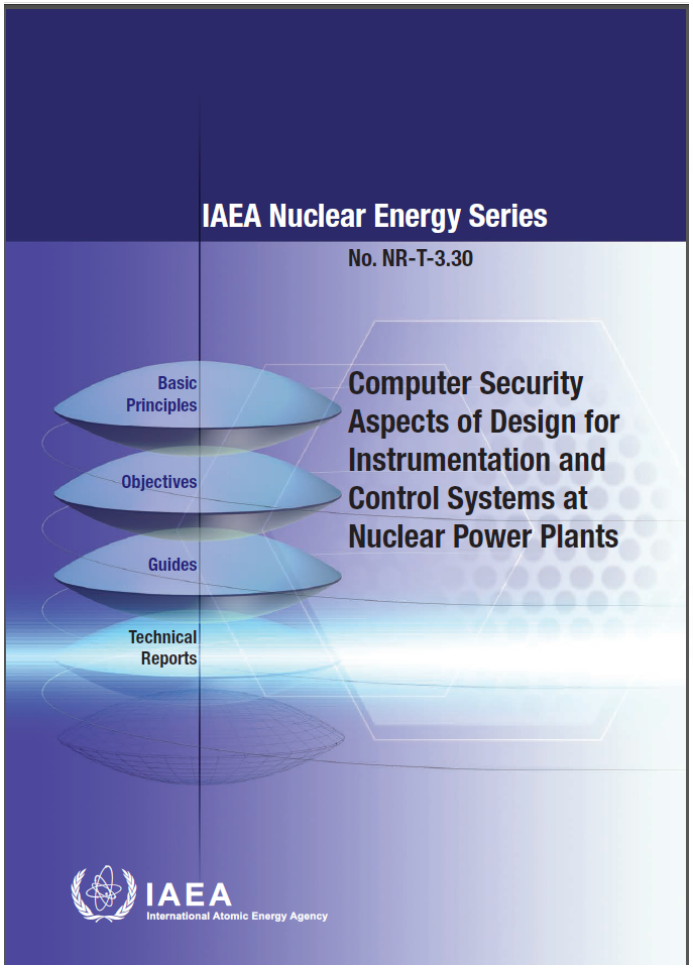
사이버보안 사건 후속조치

- **KINAC 정보통신망 DCSA(Defensive Computer Security Architecture) 적용**
  - ➢ 네트워크를 쓰는 이상 침해를 원천적으로 차단할 수 없음!
  - ➢ 침해를 당하더라도 피해를 최소화하도록 정보통신망 구조변경이 필요



사이버보안 사건 후속조치

- **DCSA(Defensive Computer Security Architecture)란 무엇인가?**



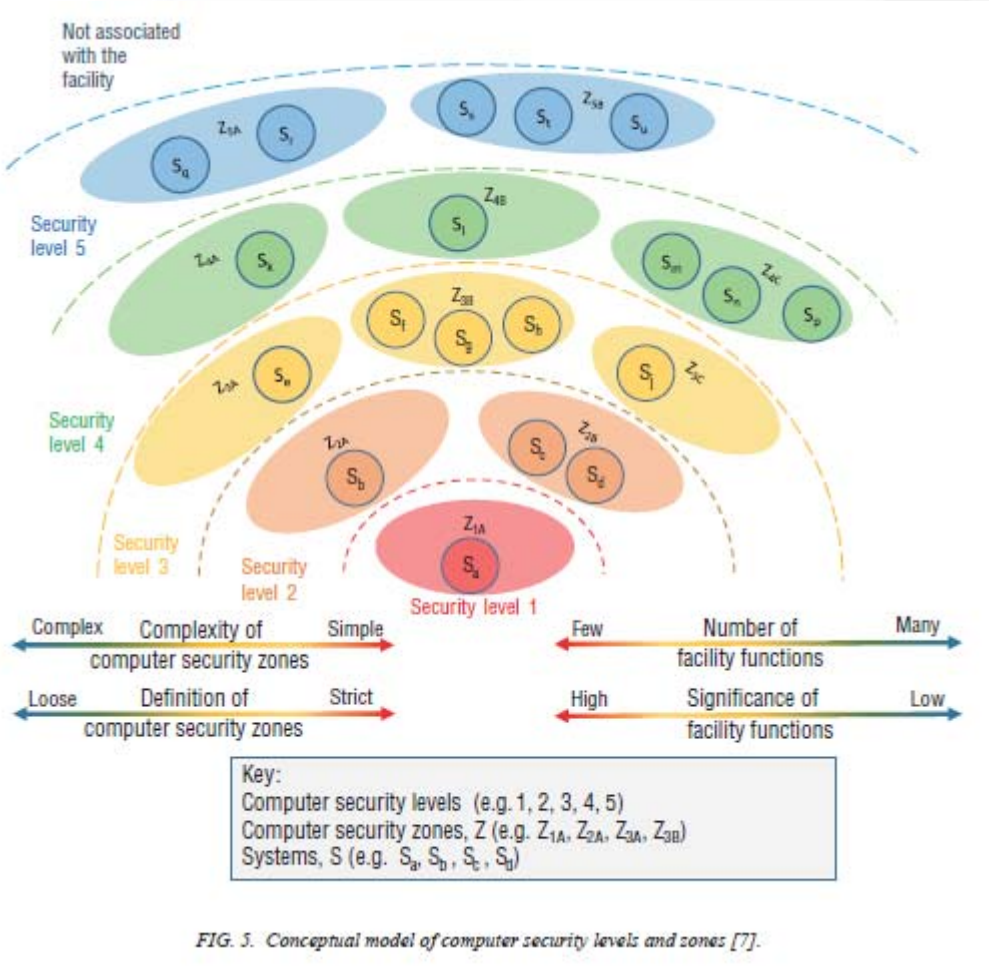


FIG. 5. Conceptual model of computer security levels and zones [7].

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

사이버보안 사건 후속조치

- **KINAC 정보통신망 DCSA(Defensive Computer Security Architecture) 적용**

건물	구분	외부망			내부망		
		vlan	Ipaddress	G/W	vlan	Ipaddress	G/W
연구동	원장실	1711	172.17	172.1	1711	192.17	192.1
	전문위원 및 감사실	1712	172.17	172.1	1712	192.17	192.1
	안전조치실 및 핵비확산본부장	1713	172.17	172.1	1713	192.17	192.1
	수출입통제실	1714	172.17	172.1	1714	192.17	192.1
	비확산기술지원센터	1715	172.17	172.1	1715	192.17	192.1
	물리적방호실 및 핵안보본부장	1716	172.17	172.1	1716	192.17	192.1
	교육훈련센터	1717	172.17	172.1	1717	192.17	192.1
	사이버보안실	1718	172.17	172.1	1718	192.17	192.1
	기획예산실 및 경영부장	1719	172.17	172.1	1719	192.17	192.1
	경영지원실	1720	172.17	172.1	1720	192.17	192.1
	전산실	1721	172.17	172.1	1721	192.17	192.1
	공영시설	1722	172.17	172.1	1722	192.17	192.1
	장비대역	1723	172.17	172.1	1723	192.17	192.1
주재검사팀		1724	172.17	172.1	1724	192.17	192.1
본 원		1611	172.16	172.1	1611	192.16	192.1
INSA 건물	교수/전문위원	1811	172.18	172.1	1811	192.18	192.1
	강의실 등	1812	172.18	172.1	1812	192.18	192.1
	멀티미디어실	1813	172.18	172.1	1813	192.18	192.1
서버		-	210.119 -> 210.119 (subne	210.1	-	(변 192.16 210.119 -> 192.16 (일	192.1 210.11 -> 192.1
개발팀		1814	172.18	172.1	1814	192.18	192.1

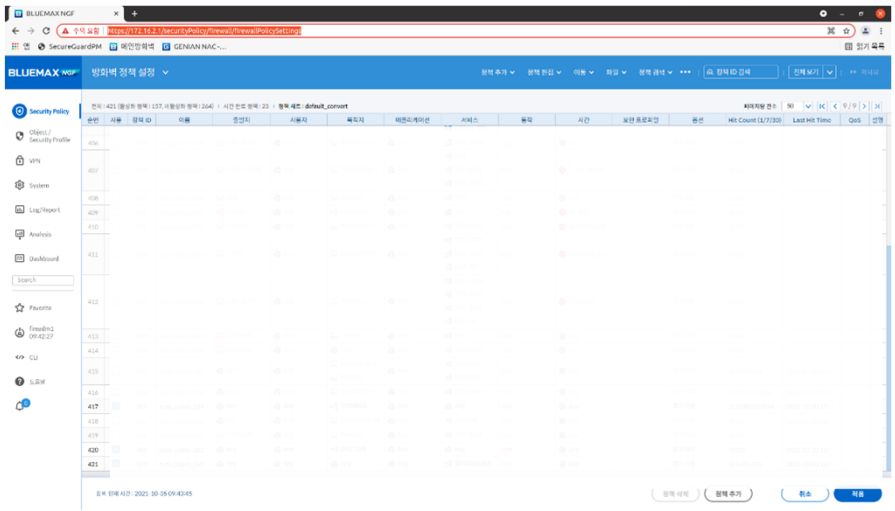
KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

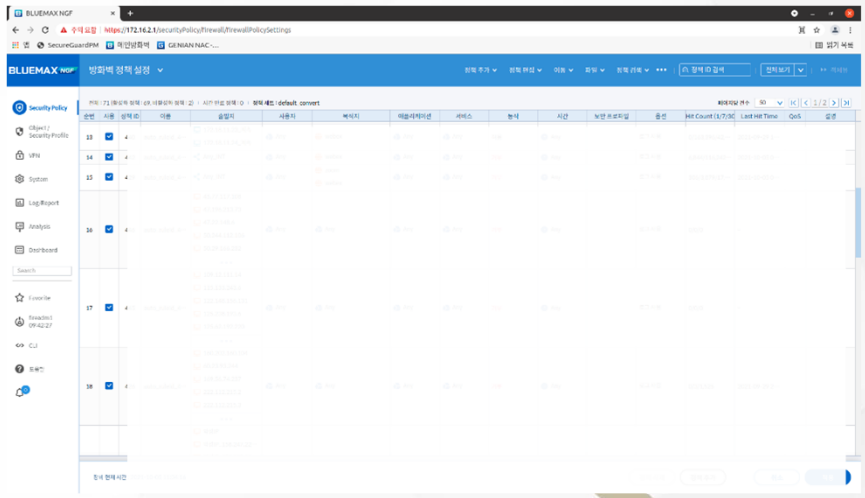
사이버보안 사건 후속조치

- **외부 방화벽 보안로그 주기적 분석(1주일 단위)**
  - ➢ 방화벽 보안정책 위배 현황을 1주일 단위로 분석하여, 해당자에게 통보
  - ➢ 매주 2~5명의 악성코드 감염 의심사례 발견

➢ **외부 방화벽 보안정책 관리체계 개편**

- ➢ 외부망 서버팜으로 접근 기본정책: All Deny & 반드시 필요한 것만 Allow
- ➢ 450여개 보안정책을 70여개로 정리
- ➢ 보안정책의 이력을 관리하기 위한 절차 수립 중

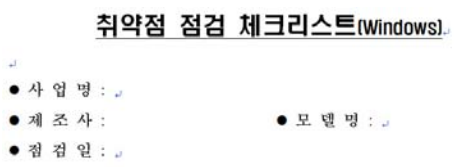




KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

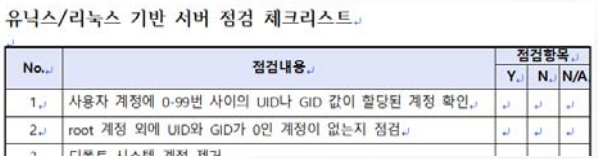
사이버보안 사건 후속조치

- **내외부망 연계정책(스트리밍서버 정책) 관리체계 개편 중**
  - 400여개 연계정책에 대한 소요를 파악하여 정리 추진 중
  - 보안정책의 이력을 관리하기 위한 절차 수립 중
- **전산실 물리적통제 철저**
  - 외부유지보수업체 직원은 담당직원 동행하여 운영서버에 접근
  - 서버유지보수용 전용단말(내부망/외부망 각 1대) 설치
  - 운영환경과 개발환경 분리 (개발업체는 전산실 상주 불가 -> 통신망 보안)
  - 외부매체(유지보수용 노트북 및 USB) 반입통제 절차 준수
- **전산장비 전산실 도입시 요건 제정**
  - 운영체제별(윈도우 및 리눅스계열) 도입전 취약점 점검 체크리스트 제정
  - 불필요한 서비스 및 암호화되지 않은 접속채널 차단 등
  - 복구절차서, 관리자 매뉴얼 등 필수산출물 제출



취약점 점검 체크리스트(Windows)

● 사 업 명 :
● 제 조 사 : ● 모 델 명 :
● 점 검 일 :



유닉스/리눅스 기반 서버 점검 체크리스트

No.	점검내용	점검항목		
		Y	N	N/A
1	사용자 계정에 0-99번 사이의 UID나 GID 값이 할당된 계정 확인			
2	root 계정 외에 UID와 GID가 0인 계정이 없는지 점검			

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
한국원자력통제기술원

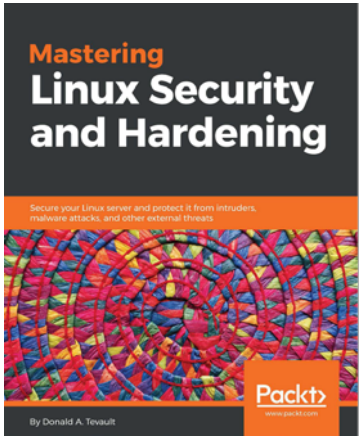
사이버보안 사건 후속조치

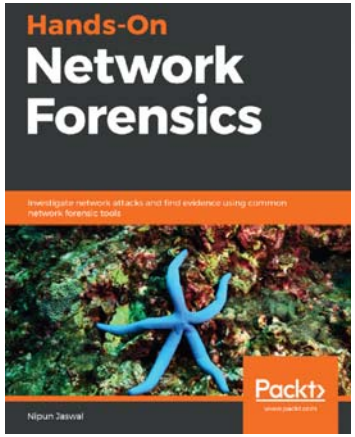
- **통합정보화시스템 개발시 소스코드 보안성 점검 (TrinitySoft사 “Code Ray”)**

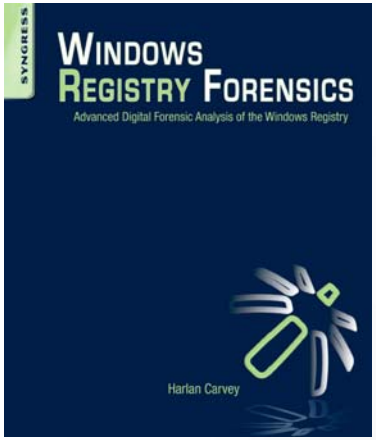
번호	유형	상세 항목	대상시스템					
			안전조치	핵안보 규제	국가계량	홈페이지	원자력 교육	이러닝
1	API 오용	DNS lookup에 의한 보안 결정	-	-	-	-	-	-
2		취약한 API 사용(strcpy) (gethostbyname)	-	-	1	2	-	-
3	코드 오류	널 포인터 역참조	-	-	-	-	-	-
4		부적절한 자원 해제(반환)(IO)	-	-	-	-	-	-
5		해제된 자원 사용	-	-	-	-	-	-
6		초기화되지 않은 변수 사용	-	-	-	-	-	-
7	입력데이터 검증 및 표현	크로스사이트 스크립트	-	-	1	-	4	-
8		OS 명령어 삽입	-	-	-	-	-	-
9		크로스 사이트 요청 위조	-	-	-	-	-	-
10		경로조작 및 자원 삽입	-	-	-	-	-	-
11		SQL 삽입(Mybatis)	-	-	-	4		
12		위험한 형식 파일 업로드	-	-	-	-	-	-
13		정수 오버플로우	-	-	-	-	-	-
14		보안기능 결정에 사용되는 부적절한 입력값	-	-	-	-	-	-
15		메모리 버퍼 오버플로우	-	-	-	-	-	-
16		신뢰되지 않은 URL 주소로 자동 접속	-	-	-	-	-	-

맺음말

- 아는 만큼 보인다.
- 보고 경험한 만큼 안다.







감사합니다

Q&A