

목 차

제 1 장 시스템보안	1
1. 운영체제	1
1.1 운영체제 개요	1
1.1.1 운영체제의 주요 기능	1
1.1.2 운영체제의 구조	2
1.1.3 운영체제의 기술 발전 흐름	7
1.2 운영체제의 주요 구성 기술	10
1.2.1 프로세스 관리	10
1.2.2 기억장치 관리	17
1.2.3 파일 시스템 관리	22
1.2.4 분산 시스템	26
1.3 운영체제 사례별 특징과 주요 기능	33
1.3.1 유닉스	33
1.3.2 윈도우	37
1.3.3 리눅스	40
2. 클라이언트 보안	45
2.1 윈도우 보안	45
2.1.1 설치 및 관리	45
2.1.2 공유자료 관리	47
2.1.3 바이러스와 백신	50
2.1.4 레지스트리 활용 [1급]	54
2.2 인터넷 활용 보안	56
2.2.1 웹브라우저 보안	56
2.2.2 메일 S/W 보안	59
2.2.3 기타 인터넷 S/W 보안	62
2.3 공개 해킹도구에 대한 이해와 대응	63
2.3.1 트로이목마 S/W	63
2.3.2 크래킹 S/W	66
2.3.3 포트 스캐닝 S/W	66
2.3.4 키로그 S/W	68
2.3.5 기타 S/W	69
2.4 도구활용 보안관리	70
2.4.1 PC용 보안도구 활용	70
2.4.2 PC용 방화벽 운영 [1급]	71

2.4.3 PC실 관리 및 보안 [1급]	72
------------------------	----

3. 서버보안	74
3.1 인증과 접근 통제	74
3.1.1 계정과 패스워드 보호	74
3.1.2 파일 시스템 보호	76
3.1.3 시스템 파일 설정과 관리	78
3.1.4 시스템 접근통제 기술	80
3.2 보안 측면의 관리	82
3.2.1 시스템 보안 등급 [1급]	82
3.2.2 운영체제 설치 [1급]	85
3.2.3 시스템 최적화 [1급]	86
3.2.4 시스템 로그 설정과 관리 [1급]	87
3.2.5 서버 해킹 원리 이해 [1급]	88
3.2.6 서버 관리자의 의무 [1급]	93
3.3 서버 보안용 S/W 설치 및 운영	95
3.3.1 시스템 취약점 점검 도구	96
3.3.2 시스템 침입 탐지 시스템	97
3.3.3 무결성 점검 도구 [1급]	100
3.3.4 접근통제 및 로깅 도구 [1급]	101
3.3.5 스캔 탐지 도구 [1급]	103
3.3.6 로깅 및 로그 분석 도구 [1급]	104

제 2 장 네트워크보안 109

1. 네트워크 일반	109
1.1 OSI 7 layer	109
1.1.1 각 레이어의 의미와 역할	109
1.1.2 각 계층별 네트워크 장비의 정의 등	113
1.2 TCP/IP 일반	115
1.2.1 IP Addressing	115
1.2.2 서브네팅	119
1.2.3 CIDR 및 VLSM	120
1.2.4 Client-Server Model	122
1.2.5 데이터 캡슐화	123
1.2.6 포트주소의 의미와 할당원칙	125
1.2.7 IP, ARP, IGMP, UDP, TCP 등 각 프로토콜의 원리 및 이해	126

1.2.8 Broadcast 및 Multicast의 이해	129
1.3 Unix/Windows 네트워크 서비스	130
1.3.1 DNS, DHCP, SNMP, telnet, ftp, smtp 등 각종 서비스의 원리 및 이해	130
1.3.2 Workgroup과 DOMAIN	137
1.3.3 터미널서비스 등 각종 원격관리 서비스	139
1.3.4 인터넷 공유 및 NAT 원리, 활용	140
2. 네트워크 활용	142
2.1 IP Routing	142
2.1.1 IP 라우팅의 종류 [1급]	142
2.2 네트워크 장비 이해	144
2.2.1 랜카드	144
2.2.2 허브, 스위치 및 브리지	146
2.2.3 VLAN [1급]	148
2.2.4 라우터 구성 명령어의 이해	149
2.2.5 네트워크 장비를 이용한 네트워크 구성 [1급]	153
2.2.6 네트워크 토폴로지 이해 [1급]	155
2.2.7 각종 네트워크 응용 프로그램의 작동 원리와 활용 [1급]	157
2.3 무선통신	158
2.3.1 이동통신(PDA, WAP) 등	158
2.3.2 이동/무선통신 보안 [1급]	160
2.4 네트워크 기반 프로그램 이해 및 활용	164
2.4.1 Ping, Traceroute 등 네트워크 기반 프로그램의 활용	164
2.4.2 Netstat, Tcpdump 등 활용	165
2.4.3 네트워크 패킷/로그분석 및 이해 [1급]	167
2.4.4. 네트워크 문제의 원인분석과 장애처리 방안 [1급]	168
3. 네트워크 기반 공격의 이해	169
3.1 서비스 거부(DoS)공격	169
3.1.1 Land Attack 등 각종 DoS의 원리와 대처요령	169
3.1.2 Syn Flooding, Smurf 등 각종 Flooding 공격의 원리와 대응 방안	171
3.2 분산 서비스 거부 공격	172
3.2.1 Trinoo, TFN, Stacheldraht 등	172
3.3 네트워크 스캐닝	175
3.3.1 Remote Finger Printing	175
3.3.2 IP 스캔, 포트스캔	176
3.3.3 Third Party Effect 등 [1급]	176
3.4 IP Spoofing, Session Hijacking	177
3.4.1 IP Spoofing과 Session Hijacking의 원리 및 실제	177
3.5 스니핑 및 암호화 프로토콜	182

3.5.1 스니핑 공격의 이해	182
3.6 각종 Remote Attack	184
3.6.1 각종 공격의 인지 및 이해	184
3.7 각종 Trojan 및 Exploit 이해	186
3.7.1 Trojan, Exploit 등	186

4. 각종 네트워크 장비를 이용한 보안기술 188

4.1 침입탐지시스템(IDS)의 이해	188
4.1.1 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등 [1급]	188
4.1.2 False Positive, False Negative 등 [1급]	190
4.2 침입차단시스템(Firewall)의 이해	191
4.2.1 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등	191
4.3 가상사설망(VPN)의 이해	194
4.3.1 원리, 작동방식, 특징, 구성, 실제 활용 등 [1급]	194
4.4 라우터의 이해	196
4.4.1 라우터 자체 보안설정	196
4.4.2 라우터를 이용한 네트워크 보안설정	197
4.4.3 Reflexive Access-list, NBAR를 통한 보안설정 [1급]	200
4.4.4 라우터의 리소스 점검 [1급]	203
4.4.5 인증 서버를 통한 보안 [1급]	203
4.4.6 CAR를 이용한 보안설정 [1급]	204
4.4.7 각종 응용 프로그램을 이용한 라우터 보안 [1급]	206
4.5 각종 네트워크 기반 보안 프로그램 활용 방안 이외 다른 네트워크 보안 관련 프로그램을 활용하여 어떻게 보안을 강화할 수 있는지에 대해 평가한다.	206
4.5.1 기타 네트워크 기반 보안 프로그램의 활용 각 프로그램의 작동원리 및 활용방안에 대해 이해한다.	206
4.6 각 장비의 로그 및 패킷 분석을 통한 공격방식의 이해 및 대처요령 로그 및 패킷분석은 문제 확인과 해결 등에 반드시 필요하다. 로그와 패킷 분석을 통해 공격을 인지하는 방법과 이러한 공격에 대해 어떻게 대처할 지에 대해 평가	207
4.6.1 호스트 및 IDS, 방화벽, 라우터등 각종 네트워크장비의 로그 및 패킷분석 [1급]	207

5. 최근 경향 및 추세 210

5.1 최근 네트워크 기반 침해사고에 대한 이해	210
5.1.1 분산반사 서비스 거부 공격(DRDOS), 기타 새로운 공격방식 [1급]	210
5.2 최근 보안솔루션에 대한 이해	211
5.2.1 역추적 시스템, 보안관계, 취약성 점검, ESM 등 [1급]	211

제 3 장 어플리케이션 보안 217

1. 인터넷 응용 보안	217
1.1 FTP 보안	217
1.1.1 FTP 개념	217
1.1.2 FTP 서비스 운영	222
1.1.3 FTP 공격 유형	224
1.1.4 FTP 보안 대책	226
1.2 MAIL 보안	227
1.2.1 mail 개념	227
1.2.2 mail 서비스 운영	229
1.2.3 mail 서비스 공격 유형	230
1.2.4 spam 대책[1급]	231
1.2.5 악성 mail 및 워밍 대책[1급]	233
1.2.6 mail 보안 기술[1급]	234
1.3 Web 보안	236
1.3.1 Web 개념	236
1.3.2 Web 서비스 운영	238
1.3.3 Web 로그 보안	244
1.3.4 web 서비스 공격 유형[1급]	246
1.3.5 웹보안 개발[1급]	253
1.3.6 XML 기반 Web 보안[1급]	253
1.4 DB 보안	255
1.4.1 DB 데이터 보안	256
1.4.2 DB 관리자 권한 보안	262
1.4.3 DBMS 운영	262
1.4.4 DB 보안 개발[1급]	271
2. 전자상거래 보안	271
2.1 전자상거래 기술	272
2.1.1 암호시스템	272
2.1.2 전자서명	272
2.2 전자상거래 프로토콜	273
2.2.1 전자 지불/화폐 프로토콜	273
2.2.2 전자 입찰 프로토콜	278
2.2.3 전자 투표 프로토콜	280
2.3 무선 플랫폼에서의 전자상거래 보안	281
2.3.1 무선플랫폼에서의 전자상거래 보안[1급]	284
2.4 전자상거래 응용 보안	285

3. 기타 어플리케이션 보안	292
3.1 응용프로그램 보안개발 방법	292
3.1.1 취약점 및 버그방지 개발방법[1급]	292
3.2 보안 신기술	306
3.2.1 암호 알고리즘의 성능향상과 새로운 암호 알고리즘[1급]	307
3.2.2 새로운 인증기술[1급]	310
3.2.3 DRM[1급]	314

제 4 장 정보보호론 **320**

1. 암호학	320
1.1 암호 알고리즘	320
1.1.1 암호 관련 용어	320
1.1.2 암호 공격 방식	322
1.1.3 정보이론 [1급]	323
1.1.4 스트림 암호	324
1.1.5 블록 암호	329
1.1.6 블록 암호 공격 [1급]	337
1.1.7 인수분해 기반 공개키 암호	338
1.1.8 확률적 공개키 암호 [1급]	342
1.1.9 이산대수 기반 공개키 암호	344
1.2 해쉬함수와 전자서명	348
1.2.1 해쉬함수 일반	348
1.2.2 블록암호 이용 방식	349
1.2.3 전용 해쉬 함수	350
1.2.4 해쉬 함수 설계 원리 [1급]	352
1.2.5 전자서명 일반	354
1.2.6 전자서명 예	361
1.2.7 특수서명 [1급]	365
1.3 인증 및 키분배	366
1.3.1 사용자 인증	366
1.3.2 메시지 인증	370
1.3.3 키 분배 프로토콜 [1급]	372
1.3.4 영지식 증명 [1급]	374
1.4 최근동향 [1급]	376
1.4.1 워터마킹	376
1.4.2 스테가노그래피(Steganography)	377

2. 정보보호 관리	378
2.1 정보보호 관리 개념	378
2.1.1 정보보호의 목적 및 특성	378
2.1.2 정보보호와 비즈니스	379
2.1.3 정보보호 관리의 개념	379
2.1.4 정보보호 관리와 타 관리 기능간의 관계 [1급]	380
2.2 정보보호 정책 및 조직	380
2.2.1 정보보호 정책의 의미 및 유형	380
2.2.2 정보보호정책 수립과정 및 내용 [1급]	381
2.2.3 조직 체계와 역할/책임	382
2.2.4 예산 수립 및 정당화 방법 [1급]	385
2.3 위험관리	386
2.3.1 위험관리 전략 및 계획수립	386
2.3.2 위험분석	388
2.3.3 정보보호 대책 선정 및 계획서 작성	392
2.4 대책구현 및 운영	393
2.4.1 정보보호 대책구현, 정보보호 대책유형, 대책 구현 시 고려사항	393
2.4.2 정보보호교육 및 훈련교육/훈련 프로그램 작성방법 인식제고 방법	398
2.4.3 운영, 컴퓨터 운영, 네트워크운영, 매체관리	400
2.4.4 사후관리, 모니터링, 변경관리, 내부감사	403
2.5 업무연속성관리	406
2.5.1 업무연속성관리 체계, 업무연속성관리 과정, 프레임워크 [1급]	406
2.5.2 업무연속성 계획수립, 응급조치, 백업계획, 정상복구 [1급]	407
2.5.3 업무연속성계획 유지보수 시험, 변경관리 [1급]	412
2.6 관련 표준/지침	419
2.6.1 국제/국가 표준 국제 협약 및 지침, OECD보안지침, 사이버공간 국가전략, 관리과정관련 표준/지침, GMITS, ISO17799등 정보보호제품 관련 표준 CC [1급]	419
2.6.2 인증체계, 정보보호 관리체계 인증, 정보보호제품 인증 [1급]	424
3. 관련법규	429
3.1 정보화촉진 기본법	429
3.1.1 정보보호의 정의 [1급]	429
3.1.2 정보화시책의 기본원칙 [1급]	429
3.1.3 정보화촉진기본계획 [1급]	429
3.1.4 정보보호시책 강구 [1급]	430
3.1.5 정보보호시스템 평가, 인증 [1급]	430
3.2 정보통신망 이용촉진 및 정보보호 등에 관한 법률	430
3.2.1 용어의 정의	430
3.2.2 정보통신망이용촉진 및 정보보호 등 시책강구	430
3.2.3 타 법률과의 관계	431

3.2.4 개인정보보호	431
3.2.5 정보통신망의 안정성 확보	432
3.2.6 정보통신망 침해행위 등의 금지	433
3.2.7 한국정보보호진흥원	433
3.2.8 벌칙	434
3.3 정보통신기반 보호법	434
3.3.1 용어의 정의	434
3.3.2 주요정보통신 기반시설 보호체계	435
3.3.3 주요정보통신기반시설의 지정과 취약점 분석	435
3.3.4 주요정보통신기반시설의 보호 및 침해사고 대응	435
3.3.5 정보보호컨설팅 전문업체	436
3.3.6 비밀유지의무	437
3.3.7 벌칙	437
3.4 전자서명법	437
3.4.1 용어의 정의	437
3.4.2 전자서명의 효력	438
3.4.3 공인인증기관	438
3.4.4 공인인증서	438
3.4.5 인증업무의 안전성 및 신뢰성 확보	439
3.4.6 이용자의 준수사항, 특정 공인인증서 요구금지, 배상책임	440
3.4.7 전자서명인증정책 추진 등	440
3.4.8 벌칙	441
3.5 전자거래 기본법	441
3.5.1 전자서명 [1급]	441
3.5.2 정보보호 [1급]	441
3.5.3 암호제품의 사용 [1급]	442