[정보보호개론]

Chapter 01 정보 보안의 세계

01 정보 보안의 역사

02 정보 보안의 이해

Chapter 02 시스템 보안

01 시스템 보안의 이해

02 계정 관리

- 운영체제의 계정 관리
- 데이터베이스의 계정 관리
- 응용 프로그램의 계정 관리
- 네트워크 장비의 계정 관리

03 세션 관리

04 접근 제어

- 운영체제의 접근 제어
- 데이터베이스의 접근 제어
- 응용 프로그램의 접근 제어
- 네트워크 장비의 접근 제어

05 권한 관리

- 운영체제의 권한 관리
- 데이터베이스의 권한 관리
- 응용 프로그램의 권한 관리

06 로그 관리

- 운영체제의 로그 관리
- 데이터베이스의 로그 관리
- 네트워크 장비의 로그 관리

07 취약점 관리

- 패치 관리
- 응용 프로그램별 고유 위험 관리
- 응용 프로그램의 정보 수집 제한

08 모바일 보안

- 모바일 운영체제 보안
- 모바일 기기 보안

Chapter 03 네트워크 보안

01 네트워크의 이해

02 서비스 거부 공격: DoS와 DDoS

- 서비스 거부 공격(Dos)
- 분산 서비스 거부 공격(DDoS)

03 스니핑 공격

- 스니핑 공격의 원인
- 스니핑 공격의 종류
- 스니핑 공격의 탐지

04 스푸핑 공격

- ARP 스푸핑 공격
- IP 스푸핑 공격
- ICMP 스푸핑 공격
- DNS 스푸핑 공격

05 세션 하이재킹 공격

06 무선 네트워크 공격과 보안

- AP보안
- 무선 랜 통신과 암호화

[정보보호개론]

Chapter 01 정보 보안의 세계

01 정보 보안의 역사

02 정보 보안의 이해

Chapter 02 시스템 보안

01 시스템 보안의 이해

02 계정 관리

- 운영체제의 계정 관리
- 데이터베이스의 계정 관리
- 응용 프로그램의 계정 관리
- 네트워크 장비의 계정 관리

03 세션 관리

04 접근 제어

- 운영체제의 접근 제어
- 데이터베이스의 접근 제어
- 응용 프로그램의 접근 제어
- 네트워크 장비의 접근 제어

05 권한 관리

- 운영체제의 권한 관리
- 데이터베이스의 권한 관리
- 응용 프로그램의 권한 관리

06 로그 관리

- 운영체제의 로그 관리
- 데이터베이스의 로그 관리
- 네트워크 장비의 로그 관리

07 취약점 관리

- 패치 관리
- 응용 프로그램별 고유 위험 관리
- 응용 프로그램의 정보 수집 제한

08 모바일 보안

- 모바일 운영체제 보안
- 모바일 기기 보안

Chapter 03 네트워크 보안

01 네트워크의 이해

02 서비스 거부 공격: DoS와 DDoS

- 서비스 거부 공격(Dos)
- 분산 서비스 거부 공격(DDoS)

03 스니핑 공격

- 스니핑 공격의 원인
- 스니핑 공격의 종류
- 스니핑 공격의 탐지

04 스푸핑 공격

- ARP 스푸핑 공격
- IP 스푸핑 공격
- ICMP 스푸핑 공격
- DNS 스푸핑 공격

05 세션 하이재킹 공격

06 무선 네트워크 공격과 보안

- AP보안
- 무선 랜 통신과 암호화

Chapter01 정보보안의 세계

01 정보보안의 역사

1950년대 이전

'- 애니그마: Enigma, 제 2차 세계대전에서 독일군의 군사통신보안용 암호장치
최초의 컴퓨터인 콜로셔스(Colossus)가 해독했으며, 이를 개발한 앨런 튜링은 최초의 해커이자 인공지능의 개념을 가장 처음 생각해낸 인물이다.

1960~1970년대(해킹의 태동기)

- APPA : 최초의 컴퓨터 연동망. IMPS네트워크라고 불린 이 연동망은 오늘날 인터넷의 뿌리.
- 유닉스(UNIX) 개발 : 해커 친화적(Hacker-Friendly) – 접근이 쉽고 여러 사용자가 동시에 사용 가능 '인류 역사상 가장 아름다운 해킹'으로 여겨짐
- 최초의 이메일 전송 : 1971년, 레이머드 톰린슨. (내용 : qwertyuiop)
- 마이크로소프트 설립 : 1975, 빌 게이츠, 폴 앨런
- 애플 컴퓨터 탄생 : 1979, 스티브 워즈니악, 스티브 잡스 (666달러 66센트)

1980~1990년대 (해킹이 컴퓨터와 직접적 연관, 해킹사건 증가, 다양화)

- 네트워크 해킹 : '네트워크 해커'라는 개념의 등장
  -414gang : 로널드 마크 오스틴 외 6명의 10대, 컴퓨터 시스템에 침입해 파일삭제
  -이언 머피(캡틴 잽) : 전화요금 조작, 실형을 산 최초의 크래커, 영화<스니커즈>
- 정보 권리 논쟁 : 카오스 컴퓨터 클럽(CCC)에서 정보에 대한 자유로운 접근 권리를 주장한 것이 최초
- 해킹 문화 : 영화- <위험한 게임>(1983)
  소설 - <뉴로맨서>(1984)
  잡지 - <프랙>, <2600:>

  +) 1986년 미 의회는 컴퓨터 범죄와 관련된 최초의 처벌 규정인 '컴퓨터 사기와 오용에 관한 조항'을 만듦
- 해커 : 1986 – 서독 해커들의 해킹 사건 -> 책 <뻐꾸기 알>(1989) 출간
  1987 – 케빈 미트닉의 사회공학 기법 해킹(기술자를 통해)
  1988 - 로버트 모리스의 '모리스 웜'이 정부와 대학의 시스템 마비
  1989 – 로이드 블랭켄십(<해커 선언문>의 저자) 체포
- 데프콘 해킹 대회: 최초의 해킹 대회, 1990 년 라스베이거스에서 개최.
- 해킹 도구의 개발 : 해커들은 다양한 해킹 정보나 해킹 툴을 웹에서 공개하기 시작함.
  이에 따라 '해커'라는 '용어가 시스템 내부를 연구하는 컴퓨터광'을 지칭하지 않게 됨
- AOHell : 아메리카 온라인 침입만을 목적으로 1997년 고안된 무료 해킹 툴, 메일 폭탄 공격
- 백 오리피스 : 1998년 CDC라는 해킹그룹이 데프콘 해킹대회에서 발표한 트로이 목마 프로그램

2000년대 이후 (컴퓨터 대중화, 보안 전문가의 필요성 대두)

- DDoS : (분산 서비스 거부)2000년 2월, 야후 CNN, 아마존 등이 ICMP패킷을 이용한 스머프 공격으로 마비

- 웜, 바이러스 : 바이러스 : 2000년 러브 버그 바이러스 – 메일을 사용, 87억 5000만 달러의 경제적 손실
웜 : 2003년 슬래머 웜, 2004년 베이글 웜, 마이둠 웜, 넷스카이 웜(웜 삼총사)

- 개인정보 유출과 도용 : 주민등록번호, 금융 정보 등

- 전자 상거래 교란 : 인터넷상 신용카드 결제 방식의 취약점 이용한 범죄, 포털사이트 검색 클릭 수 자동 증가, 공인인증서 유출로 인한 불법 인출, 은행 해킹 등

- APT공격 : 지능형 지속 공격, 오랜 시간을 들여 사이트를 분석하고 취약점을 찾아내어 해킹하는 공격

- 농협 사이버 테러 : 북한의 사이버 테러로 발표됨, 국내 기업의 보안 인식을 바꾸는 계기

- 스마트폰 해킹 : 상당히 긴 시간 전원공급이 가능하며 와이파이, 3G, LTE가 가능한 최고의 해킹 도구
스마트폰 내의 정보유출부터 원격으로 스마트폰을 조종하는 등 범위가 확대되고 있음

- 가상 화폐 해킹 : 가상화폐의 가치가 높아져 관련 해킹 사건이 증가함. 해킹 초기의 은행 해킹 형태

02 정보 보안의 이해

보안의 3대 요소

- 기밀성(Confidentiality) : 인가된 사용자만 정보자산에 접근할 수 있음
- 무결성(Integrity) : 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있음
- 가용성(Availability) : 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것

+)국방부에서는 인증(authentication), 부인방지(nonrepudiation)까지 보장하는 '방어적 정보작전'으로 정의

보안전문가의 자격요건

- 윤리 의식 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률
  - 정보통신망법
  - 정보통신기반보호법
  - 개인정보보호법
  - 클라우드컴퓨팅법
  - 헌법 10조 17조
  - 전자정부법

- 다양한 분야의 지식

-운영체제 : 가장 많이 쓰이는 윈도우를 비롯한 유닉스, 리눅스, 맥OS 등이 있음
금융권, 공공기관에서는 유닉스를 사용하며 최근 오픈소스 기반의 서비스에는 리눅스를 사용
리눅스는 유닉스와 비슷한 환경, 쉽게 구할 수 있으며 소스가 공개되어 자유롭게 배우기 좋음

-네트워크 : 하나의 시스템에서 데이터를 처리한 뒤 다른 시스템으로 전달하는 길과 같은 역할
1973년에 만들어진 TCP/IP는 지금도 네트워크의 기본이 되는 프로토콜

-프로그래밍 : C프로그래밍과 객체지향 프로그램에 대한 이해, HTML에 대한 이해 필요.

-서버 : 기업이 안전하고 신뢰할 수 있는 서비스를 제공는 서버를 운용하기 위해 서버에 대한 이해가 필요
기본적인 SQL지식이 필요

-보안시스템 : 기본 보안 통제와 적용 원리, 네트워크 상의 구성과 목적 등을 이해

-모니터링시스템 : 모니터링 시스템의 기본 개념 인지- 네트워크 관리 시스템, 네트워크 트래픽 모니터링 시스템

-암호 : 암호와 해시의 차이, 대칭 키 알고리즘 및 비대칭 키 알고리즘의 종류와 강도, 공개 키 기반 구조

-정책과 절차 : 보안 정책과 해당 기업의 핵심적인 업무 프로세스를 잘 이해하고 있어야 함
보안 거버넌스 : '조직의 보안을 달성하기 위한 구성원 간의 지배 구조'

무결성.

Chapter 02 시스템 보안

기밀성 - 인가된 사용자만 데이터에 접근.

01 시스템 보안의 이해 : - 권한이 없는 사용자가 파일이나 폴더 등을 사용하지 못하게 제한, 시스템을 보호
- 계정 관리, 세션 관리, 접근 제어, 권한 관리, 로그 관리, 취약점 관리로 정리할 수 있음

02 계정 관리

식별(Identification) – 아이디라는 문자열을 통해 자신이 누구인지 확인

인증(Authentication) – 아이디만으론 정확한 식별이 어려워 패스워드를 통해 인증

-인증방법 : – 알고 있는 것(Something you know) : 패스워드
– 가지고 있는 것(Something you have) : 신분증, OTP
– 자신의 모습(Something you are) : 지문인식
– 위치하는 곳(Somewhere you are) : 콜백

03 세션 관리

세션 : 사용자와 시스템 사이 또는 두 시스템 간의 활성화된 접속 세

세션유지를 위한 보안사항 : - 세션 하이재킹, 네트워크 패킷 스니핑에 대응하기 위해 암호화
- 지속적인 인증 : 타임아웃 설정, 재설정 요구

04 접근 제어

접근 제어 : 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것 시스템의 보안 수준을 갖추는 데 가장 기본적인 수단
IP, 서비스 포트를 기본적인 수단으로 함

05 권한 관리

06 로그 관리

AAA : Authentication(인증) : 자신의 신원을 증명하는 과정 (아이디와 패스워드를 입력)
Authorization(인가) : 로그인이 허락된 사용자로 판명되어 로그인하는 과정
Accounting : 로그인했을 때 시스템에 이에 대한 기록을 남기는 활동

07 취약점 관리

패치 관리 : 제작사가 배포하는 패치 또는 서비스 팩을 적용하여 시스템 취약점 보안
윈도우가 사용률이 높고 접근이 쉬워 공격을 더 많이 받음.
업데이트를 통해 자동으로 보안 패치 확인, 적용 가능

- 패치관리 솔루션(PMS) : 시스템의 보안취약점 보완을 위해 배포하는 패치 또는 기타 패치파일에 대해 원격에서 자동으로 관리해주는 솔루션

응용 프로그램별 고유 위험 관리 : 응용프로그램 중 운영체제의 파일, 명령 실행가능한 프로그램이 있음. Ex) MS-SQL의 xp_cmdshell : '확장 저장 프러시저', 데이터베이스를 통함. 이러한 프로그램은 적절성을 검토한 뒤 사용해야 함.

응용 프로그램의 정보 수집 제한 : 응용 프로그램의 특정 기능이 운영체제의 정보를 노출시키기도 함
유닉스에서는 vrfy, expn명령으로, 일반사용자는 텔넷을 이용해 확인 가능
이러한 응용프로그램의 기능은 제한하는 것이 바람직

		계정 관리		접근 제어	권한 관리	로그 관리
운영체제	윈도우	- 관리자 권한을 가진 계정 : Administor - 기본그룹을 정의함.	- 관리자 계정 외의 그룹은 임의로 생성, 고유의 권한이 없음	터미널 서비스 GUI 관리용 툴	권한 종류 : 모든 권한, 수정, 읽기 및 실행, 디렉터리 내용 보기, 읽기, 쓰기 규칙 : 접근권한 누적, 파일접근권한>디렉터리접근권한 허용<거부	- '이벤트'라는 중앙 집중화된 형태로 로그 수집 - 편하지만 위험도가 높음. - 이벤트 뷰어에서 확인가능 레지스트리 키 → USB 이력 확인
	유닉스	- 기본 관리자 계정 : root		텔넷(Telnet), SSH, XDMCP, FTP는 TCPWrapper을 통해 접근 가능 (데몬과 클라이언트의 요청 연결)	읽기 :r , 4 쓰기 : w, 2 실행 : x, 1 ->숫자 치환 방식	- 여러 곳에 산발적으로 저장 - 찾거나 삭제하기 어려움 secure(sulog), history, syslog 등.
데이터베이스		-MSSQL의 관리자 계정은 sa이고 오라클의 관리자 계정은 sys, system (system은 데이터베이스 생성 X)		-오라클 : 일정수준 이상의 데이터베이스 적용가능 - MS-SQL은 IP에 대한 접근제어를 기본으로 하지 않으므로 방화벽을 통해야 함	DDL : 데이터 구조를 정의하는 질의문 DML : 운영 및 사용. 검색/수정 처리 DCL : 권한 관리를 위한 질의문	- MS-SQL : Error, general, slow Query, Binary, Relay 로그 제공 - 오라클 : 감사 - 문장, 권한, 객체 - 모니터링 가능한 '패킷'을 설치해 로그로 남김
응용프로그램		-취약한 응용 프로그램을 통해 정보를 습득한 뒤 운영체제 공격할 수가 있음 -TFTP같이 인증이 필요하지 않은 응용프로그램의 경우 더욱 세심한 주의 필요		-응용 프로그램의 목적, 역할에 따라 접근제어를 적용하거나 그렇지 않음 -IIS, NGINX : IP에대하여 -SSL : 클라이언트, 서버인증서 이용	취약한 응용 프로그램의 경우 해당 프로그램을 실행한 계정의 권한이 악용되는 문제가 발생--> 윈도우 ISS – 실행 프로세스 권한 유닉스 – nobody등 제한된 계정 권한	IIS : '로깅'항목으로 알 수 있음 기본 W3C형식. 다른것도댐 아파치 : 기본 access_log에 'combined'형식으로 저장
네트워크장비		-계정이라는 개념 없이 패스워드로 접속 - 계정 관리에 어려움 때문에 대규모 네트워크에서는 TATACS+ 등의 솔루션을 적용하기도 함		-관리 인터페이스에 대한 접근 제어, ACL을 통한 네트워크 트래픽 접근 제어 ACL어쩌구 : 방화벽에서의 접근제어와 기본적으로 같음	뷰 뷰 : 각 열에 대한 사용자의 권한 설정이 가능한 가상 테이블 뷰에 대해 권한 할당 가능	보안 : 침입 차단 시스템, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS)가 있음 관리, 장비 인증 시스템도 있음

08 모바일 보안

역사 : – 팜OS : 1996년 개발, 주소, 달력, 계산기 등과 간단한 보안 툴 포함
– 윈도우 CE : 1996년 출시, PDA, 모바일 장치 등에 사용하기 위함. 1MB 이하의 메모리에서도 동작
– 블랙베리OS : 2000년에 처음 사용된 명칭, RIM이 만듦, 메시지와 이메일 전송 기능에 초점.
– iOS : 2007년 시작된 애플에서 사용되는 모바일 운영체제
– 안드로이드 : 2007년 시초, 구글과 이동 통신 관련 회사 연합체가 개발한 개방형 모바일 운영체제

iOS vs 안드로이드

	iOS	안드로이드
운영체제	UNIX에서 파생, 발전한 OS X 모바일버전	리눅스 커널을 기반으로 함
보안통제권	애플	개발자, 또는 사용자
프로그램 실행 권한	관리자(root)	일반 사용자
응용 프로그램 서명	애플이 CA를 통해 각각에 서명하여 배포	개발자가 서명
샌드박스	프로그램 간 데이터 통신을 엄격히 통제	상대적으로 자유롭게 애플리케이션 실행
부팅절차	암호화된 로직으로 서명된 방식에 의해 안전한 부팅 절차 확보	
소프트웨어 관리	단말 기기별 고유 소프트웨어 설치 키 관리	
취약점	대부분 '탈옥'한 iOS기기에서 발생	사용자가 보안수준 선택. 악성코드 유포, 그에 따른 백신 보급됨

모바일 기기 문제점

– 워드라이빙 : 노트북에 안테나를 연결하고 차에 탄 채 보안이 취약한 무선 랜을 탐색하며 해킹을 시도하는 것
- 모바일 기기는 이동성이 뛰어나 공격을 받을 때보다 공격에 사용될 때가 문제가 됨
- 좀 더 넓은 영역이나 쉽게 접근하기 어려운 곳의 무선 랜까지 공격당할 수 있음

– 블루투스 : 선을 사용하지 않고 휴대용 장치를 연결하는 기술.
높은 수준의 암호화와 인증 구현이 어려워 다양한 위험에 노출될 수 있음

– 블루프린팅 : 블루투스 공격 장치의 검색 활동. 서비스 발견 프로토콜을 이용해 공격가능한 장치 검색 가능

– 블루스나프 : 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근, OPP기능을 통함

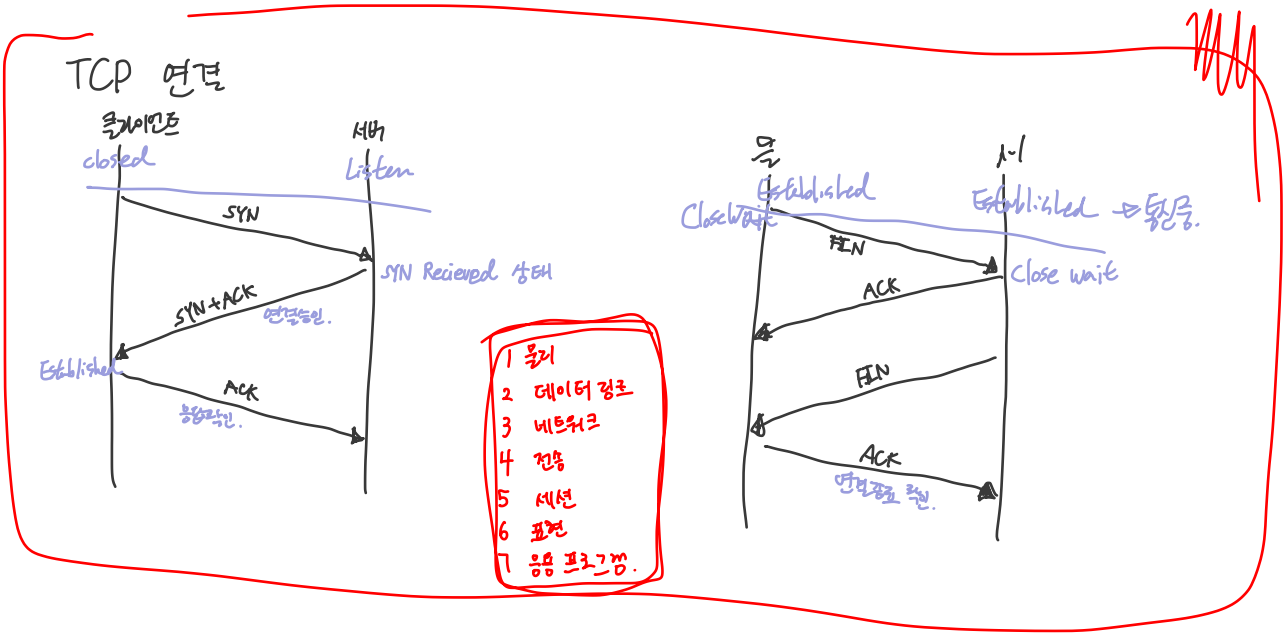
– 블루버그 : 블루투스 장비 간의 취약한 연결관리 활용. (한 번 연결되면 이후에는 바로 서로 연결됨)

Chapter 03 네트워크 보안

01 네트워크의 이해

- OSI 7계층

<table>
<tr><td>7계층</td><td>응용 프로그램 계층</td><td>응용 프로세스와 관계하여 일반적인 응용 서비스 수행</td></tr>
<tr><td>6계층</td><td>표현 계층</td><td>코드 간의 번역 담당, 데이터 구조 통일해 데이터 형식 차이로 발생하는 부담을 덜어줌</td></tr>
<tr><td>5계층</td><td>세션 계층</td><td>양 끝단의 응용 프로세스가 통신을 관리하는 방법 제공</td></tr>
<tr><td>4계층</td><td>전송 계층</td><td>양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌
<table>
<tr><th></th><th>TCP</th><th>UDP</th></tr>
<tr><td>연결방식</td><td>연결형서비스</td><td>비 연결형 서비스</td></tr>
<tr><td>패킷 교환 방식</td><td>가상 회선 방식</td><td>데이터그램 방식</td></tr>
<tr><td>전송 순서</td><td>전송 순서 보장</td><td>전송 순서가 바뀔 수 있음</td></tr>
<tr><td>수신 여부 확인</td><td>수신 여부를 확인함</td><td>수신 여부를 확인하지 않음</td></tr>
<tr><td>통신 방식</td><td>1:1 통신만 가능</td><td>1:1 / 1:N / N:N 통신 모두 가능</td></tr>
<tr><td>신뢰성</td><td>높음</td><td>낮음</td></tr>
<tr><td>속도</td><td>느림</td><td>빠름</td></tr>
</table>
</td></tr>
<tr><td>3계층</td><td>네트워크 계층</td><td>경로를 찾아주는 역할을 하는 계층, 데이터를 네트워크를 통해 전달하고, 서비스 품질을 위해 수단 제공
- 라우팅, 흐름 제어, 세그먼테이션, 오류 제어 등을 수행
- 주소 : IP, 장비 : 라우터와 스위치</td></tr>
<tr><td>2계층</td><td>데이터 링크 계층</td><td>두 지점 간 신뢰성있는 전송을 보장하기 위한 계층
- 12개의 16진수로 구성된 MAC주소를 할당받음
- 스위치를 통해 메모리를 전달함</td></tr>
<tr><td>1계층</td><td>물리 계층</td><td>실제 장치 연결을 위한 전기적, 물리적 세부 사항 정의</td></tr>
</table>



02 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격, DoS(Denial of Service)

: 일종의 '훼방'이라고 볼 수 있음

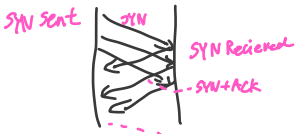
취약점 공격형

- 보잉크/봉크/티어드롭 공격 : TCP 프로토콜이 패킷 전송 시 문제가 있으면 반복적으로 재요청, 수정을 하는 오류 제어 기능을 이용해 패킷 재전송, 재조합에 과부하가 걸리도록 시퀀스 넘버를 속임
->과부하가 걸리거나 반복되는 패킷을 무시하고 버리도록 처리함.

- 랜드 공격 : Land : (나쁜 상태에) 빠지게 하다
패킷을 전송할 때 출발지와 목적지 주소를 같게 하여 과부화 상태를 만듦
->운영체제의 패치관리, 네트워크 보안 솔루션 – 출발지/목적지 주소 적절성 검증.

- 죽음의 핑 공격 : 시스템 파괴에 흔히 쓰인 초기의 DoS 공격 방법
ping 명령을 보낼 때 공격 대상에게 긴 패킷을 보내 대상이 대량의 작은 패킷을 수신하게 함
->방화벽에서 ping를 사용하는 프로토콜인 ICMP를 차단해야 함

- SYN 플러딩 공격 : '동시 사용자 수 제한'을 이용해 존재하지 않는 클라이언트가 접속한 것처럼 속여 사용자가 서비스를 제공받을 수 없게 함
SYN+ACK패킷에서 서버로 ACK패킷을 보내지 않아 모든 접속자를 SYN Received로 만듦
->SNY Received의 대기 시간을 줄이거나 침입방지시스템(IPS)-snort, iptable 사용



ACK를 안보내면 → SYN Recieved 상태로 대기

- HTTP공격 : -GET 플러딩
-CC
-슬로리스트 플러딩
-슬로헤더 DoS (슬로로리스)
-슬로POST

- 스머프 공격
↳ 공격자 IP를 위조 → 다이렉트 브로드캐스트 막기

- 메일 폭탄 공격 —디스크공간을 가득 채움

분산 서비스 거부 공격,DDoS(Distributed Denial of Service)

- 공격자 → 마스터 → 에이전트
⋮ ⋮
핸들러프로그램 데몬프로그램

스니핑 공격

Passive 공격·수동적공격 → 데이터를 '찾는 것'

ex) 도청

탐지 → 스니퍼가 프러미스큐어스 모드에서 작동함을 이용!

- Ping → MAC주소로 위장해 전송, 이에 대해 응답하면 해당 호스트가 스니핑하고있는 것.
- ARP
- DNS
- 유인 → 가짜 ID, Password 복림 → 이걸로 접속하면 OO
- APR Watch