# NETWORK 보안 실무

## (사이버보안과 2학년)

양승익(Yang Seung Ik)
KIMPO University
Tel: +82-010-3341-7700
Email: skyang611@gmail.com

# Orientation

1. 담당 교수 : 양 승 익( **Seung Ik Yang)**
   학교소속 : 사이버보안과 겸임교수

2. E-mail : skyang611@gmail.com // skyang611@kimpo.ac.kr

3. 교재 : 자체교재
4. 교육방법

- 산업현장에서 필요로 하는 Human-Resource
- 기초 지식을 바탕으로 한 기술능력 배양
- 핵심 기술 위주의 교육

# Orientation

5. NCS 교육과정의 강의 계획 및 평가계획

- 평가 계획(8주차, 16주차, 평시)

. 서술형, 실무, 평가자 체크리스트, 출석

서술형, 실무, : 60%, 평가자 체크리스트 : 20, 출석 : 20%

평가자 체크리스트는 REPORT, 수업 중 제출자료, 수업태도 등

## Orientation( 과정확인을 위한 질의 / 응답)

**본 시간은 네트워크 보안의 강의진행을 위하여 사전 기술 습득및 강의진행에 참고하기 위하여 시행하는 평가입니다**

**본인의 학번 이름 없이 무기명으로 진행합니다 솔직한 답변을 바랍니다**

❖ 네트워크에 대한 이해도 질의사항

1. TCP/IP Layer 또는 OSI 7 Layer 에 대하여 쓰시오
2. Data Link Layer의 Ethernet 프래임 포멧에 대하여 쓰시오
3. IP Packet의 구조에 대하여 아는 대로 설명하시오

❖ 네트워크 보안 관련

4. NMS(Network Management system)이란?
5. Network 보안 종류에 대하여 아는데로 쓰시오

0. 네트워크 역사

✓ 모스와 전신기
- 1800년경 볼타(Volta)가 최초로 전지를 발명
- 이후 전선을 통해 신호를 보내는 방법을 연구하기 시작 했고, 모스가 처음 실질적인 성과를 냄.
- 1832년 알파벳 문자에 점과 대시를 사용하여 모스 부호를 발명

✓ 벨의 전화기
- 1876년 알렉산더 그레이엄 벨이 전화기를 개발
- 1877년 1월 30일 상자 모양의 첫 전화기가 등장(일대일 통신만 가능)
- 1878년 1월 28일 미국 코네티컷주 뉴헤이븐에서 처음으로 교환기가 설치되어 사용자의 전화가 중앙의 교환수를 거쳐 연결됨.
- 우리나라는 1896년 궁 내부 전화가 전화기의 효시 1902년에는 서울과 인천 사이에 전화가 개설

✓ 전자기파의 발견 및 전파이용
- 1864년 제임스 클럭 맥스웰이 전자기파가 대기중으로 전파된다고 처음 예측
- 1888년 하인리히 루돌프 헤르츠가 실험을 통해 라디오파를 주고받음으로써 전파의 존재가 실제로 입증됨.

0. 네트워크 역사

✓ 모뎀의 개발과 네트워크의 시작

- 벨 텔레폰 연구소가 '모델-K' 기기를 개발했고, 후에 뉴욕의 CNC와 전화선으로 연결해 데이터를 입력하는 과정을 시연, (네트워크 컴퓨팅의 효시)
- 1958년 벨 연구소에서 최초의 상업용 모뎀인 데이터폰을 개발
- 미국 국방부는 군사 작전 수행을 위한 세계 최초의 컴퓨터 네트워크 개발에 착수하여 사상 최초 대단위 컴퓨터 네트워크인 ARPANET의 탄생으로 이어짐.

✓ 장거리 컴퓨터 통신과 인터넷의 시작

- ARPA는 MIT 링컨 연구소의 TX-2와 캘리포니아 산타모니카 SDC의 Q-32 컴퓨터와 전화선으로 직접 통신하는 장거리 데이터 통신을 최초로 시도
- 프로토콜 : 컴퓨터와 컴퓨터 사이에서 메시지를 전달하는 과정(톰 마릴)
- 년 ARPA는 ACM에서 각 호스트를 IMP라는 특정 컴퓨터에 연결하고, IMP를 서로 연결하는 ARPANET을 제안(현재의 라우터와 개념이 유사)
- 1969년 네 개의 노드(UCLA, USCB, SRI, UU)를 네트워크로 구성하고 NCP라는 프로토콜을 호스트 간 통신에 사용
- 1971년 레이 톰린슨이 전자 메일 프로그램을 발명

0. 네트워크 역사

✓ 장거리 컴퓨터 통신과 인터넷의 시작

- 1972년 빈트 서프와 로버트 칸이 게이트웨이를 개발
- 1973년 빈트 서프는 로버트 칸과 함께 TCP/IP 프로토콜과 인터넷 구조를 설계
- 호스트 컴퓨터와 터미널로 구성된 네트워크는 IBM의 SNA 망이 최초
- 1974년 제록스가 이더넷을 개발(오늘날의 클라이언트-서버 구조로 전환)
- 1979년 유즈넷 탄생
- 1981년 유닉스 운영체제에 TCP/IP가 포함되어 배포되었고, TCP/IP가 ARPANET의 공식 프로토콜.
- 1983년 군사용 MILNET과 군사용이 아닌 ARPANET으로 분리
- 1983년 존 포스텔이 도메인이름 시스템 개발
- 1984년 DNS가 구성되어 네트워크가 폭발적으로 확장됨.
- 1990년 ARPANET이 해체되고 NSFNET이 만들어짐.
- 1989년 3월 버너스-리가 웹 개념을 제안
- 1990년 동료 로버트 카이유와 개정된 개념을 소개

  → 서로 다른 컴퓨터끼리 정보를 공유하고 서로 링크하여 찾기 쉬운 하이퍼텍스트 형태의 서비스를 도입하자는 것

0. 네트워크 역사

✓ 국내 인터넷의 역사

- 1982년 서울대학교와 KIET(전자통신연구소의 전신)가 TCP/IP로 SDN 시작
- 1983년 미국으로 UUCP 다이얼 업(Dial-Up) 연결
- 1984년 유럽으로 X.25를 이용한 UUCP 연결
- 1987년 교육 연구 전산망 추진 위원회 구성
- 1988년 연구 전산망 기본 계획 확정, 교육망을 BITNET과 연결
- 1990년 HANA/SDN이 56Kbps로 인터넷에 연결
- 1991년 연구 전산망이 56Kbps로 인터넷에 연결
- 1993년 HANA/SDN이 56Kbps에서 256Kbps로 확충
- 1994년 한국통신, 데이콤에서 인터넷 상용 서비스 시작
- 1995년 INET, 나우콤에서 인터넷 상용 서비스 시작
- 1995년 초고속 정보통신망 구축 사업 시작
- 1996년 7천 대 이상의 호스트 컴퓨터가 연결됨
- 1997년 한국인터넷협회 설립
- 1998년 초고속 정보통신망 구축 사업 1단계 완료
- 2000년 초고속망 구축 기술로 각종 서비스가 이루어짐(하나로, 두루넷, 드림라인, 신비로 등)
- 2001년 초고속 광전송망 구축(155Mbps~40Gbps)
- 2002년 서울대, 한국전자통신연구원ETRI 등이 참여한 IPv6 활성화를 위한 프로젝트 시작
- 2004년 한국 인터넷 이용자 수 3천만 명 돌파
- 2005년 한국 IPv6 주소 보유율 세계 3위로 평가
- 2012년 한국 인터넷 속도 세계 1위로 평가

# 1. 네트워크 보안의 기초

## ○ 네트워크 보안 개념

✓ 조직의 네트워크 및 네트워크 접근 가능한 리소스에 대한 공격을 방지하는 정책, 실행, 기술.

✓ 권한 밖의 네트워크와 네트워크로 접속 가능한 자원에 접근 시, 네트워크 관리자가 사용하는 컴퓨터 네트워크 하부구조에서의 기본적인 설비 또는 방책.

✓ 공격자가 TCP/IP 등 통신 프로토콜의 다양한 취약점을 이용하여 허가 되지 않은 네트워크자원에 접근하거나 그 자원을 파괴하거나 또는 그 자원의 사용을 방해하는 것을 방어하는 것.

1. 네트워크 보안의 기초

○ 네트워크 보안 중요성

✓ 네트워크의 모든 부분이 공격이나 불법행위의 대상이 됨.

✓ 네트워크뿐만 아니라 연결된 리소스를 위협으로부터 방어하는 것이 중요.

✓ 승인 받지 않은 사람이나 프로그램이 네트워크와 네트워크에 연결된 디바이스에 접근하는 것을 막는 데 사용하는 툴과 작업으로 구현.

1. 네트워크 보안의 기초

○정보 보안의 3요소와 추가 요소

- ✓ 기밀성(Confidentiality)
- ✓ 무결성(Integrity)
- ✓ 가용성(Availability)
- ✓ 서버 인증(Server Authentication)
- ✓ 클라이언트 인증(Client Authentication)

- ✓ 기밀성(Confidentiality)

- 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것
- 프라이버시 보호와도 밀접한 관계가 있음.
- 네트워크 보안 측면에서 기밀성은 '시스템 간 안전한 데이터 전송'과 관련이 있음.
- 스니핑(Sniffing)은 기밀성을 해치는 가장 일반적인 공격 형태
- 통신의 암호화가 가장 일반적인 보안 대책

# 1. 네트워크 보안의 기초

## ○ 정보 보안의 3요소와 추가 요소

### ✓ 무결성(Integrity)

- 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것
- 네트워크에서의 무결성은 '클라이언트와 서버 간의 데이터가 변조되지 않고 전송되는가 ' 와 관련이 있음.
- 중간에 유효한 다른 연결을 빼앗는 세션 하이재킹, 두 시스템 간의 데이터를 중간에 변조하는 MITM 공격은 무결성을 해치는 대표적인 공격
- 통신의 암호화가 가장 일반적인 보안 대책(PKI와 밀접한 관련이 있음)

### ✓ 가용성(Availability)

- 허락된 사용자 또는 객체가 정보에 접근하려고 할 때 방해받지 않도록 하는 것
- DoS가 가용성을 해치는 대표적인 공격

1. 네트워크 보안의 기초

○ 정보 보안의 3요소와 추가 요소

✓ 서버 인증(Server Authentication)

- '클라이언트가 올바른 서버로 접속하는가 ' 를 의미
- 서버 인증으로 생기는 문제는 무척 다양하며, 일반적으로 DNS 스푸핑이나 서버 파밍 등이 있음.
- SSL(HTTPS)을 통해 서버 인증을 하지만, 경고를 보여주고 사용자에게 선택을 하게 하는 것이 일반적이며 강제적인 서버 인증은 흔치 않음.

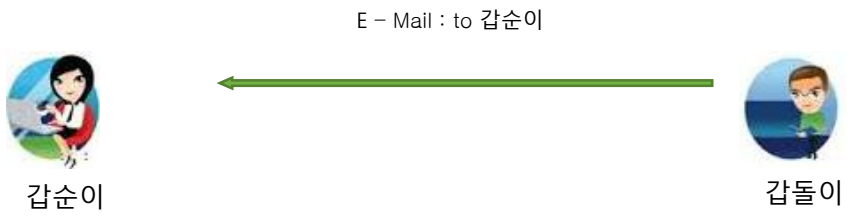
✓ 클라이언트 인증(Client Authentication)

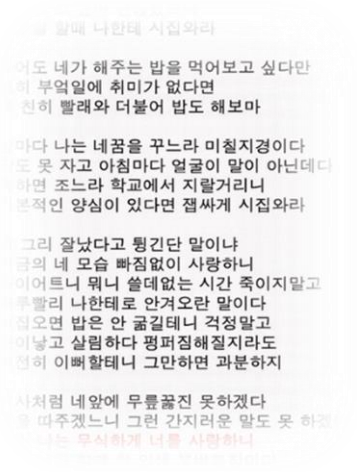
- '올바른 클라이언트가 접속을 시도하는가 ' 를 의미
- 웹 사이트에 접근할 때 사용하는 아이디와 패스워드가 대표적인 클라이언트 인증
- 클라이언트 인증과 관련된 해킹은 스푸핑, 세션 하이재킹, 피싱 등이 있음.

# 1. 네트워크 보안의 기초

○ 정보 보안의 3요소와 추가 요소

- ✓ 제3자가 갑순이에게 보낸 E-mail을 훔쳐보지 않았을까?
  : Confidential (기밀성)
- ✓ 갑돌이가 보낸 E-mail내용이 혹 변경되지는 안았을까?
  : Integrity(무결성) , Message 인증
- ✓ 갑순이 입장 : 갑돌이가 보낸 E-mail 인데 갑돌이가 보냈다는 것과 Mail내용이 나중에 갑돌이가 안 보냈다고 하지는 않을까?
  : 부인방지



# 1. 네트워크 보안의 기초

## ○ 정보보호 기술의 특징

- ✓ 특수성
- ✓ 독자성
- ✓ 기반특성
- ✓ 고부가가치

## ○ 정보보호 위협요소

| 정보보호 위협요소 | 요구되는 보안요소 |
|---|---|
| 비인가 접근 | 인증 |
| 데이터 도청 | 기밀성 |
| 데이터 가로막기 | 가용성 |
| 데이터 변조 / 위조 | 무결성/인증 |
| 부인 | 부인방지 |
| 서비스 거부 | 가용성 / 인증 |

# 1. 네트워크 보안의 기초

## ❖ 해킹(Hacking)이란

- 해킹의 개념
  - ✓ 어떠한 의도에 상관없이 다른 컴퓨터에 침입하는 모든 행위.
  - ✓ 불법적인 시스템 사용, 자료열람, 유출 및 변조 등을 하는 것.
  - ✓ 긍정적의미로써'각종 정보
  - ✓ "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부.
  - ✓ 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태.
  - ✓ 시스템의 보안 취약점을 미리 알아내고 보완하는 데에 필요한 행위'

1. 네트워크 보안의 기초

❖ 해커의 개념

- 긍정적 의미 : 초기 사전적 의미로써 컴퓨터 전반에 걸쳐 깊이 배우기를 즐기는 사람 또는 컴퓨터 프로그래밍을 즐기고 열광하는 사람.
- 부정적 의미(크래커 또는 시스템 침입자) : 보안시스템을 악의적으로 무력화 시키거나 상대 시스템에서 불법으로 정보를 빼내는 사람.
- 현재는 해커와 크래커는 구분 없이 해커로 통칭하며 범죄를 일으키는 블랙해커와 윤리적이고 합법적인 화이트해커로 구분.

1. 네트워크 보안의 기초

- 해커의 수준별 분류
  - 길버트 아라베디언은 해커의 등급을 프로그램 능력, 네트워크 이해도, 시스템의 취약점 분석 능력 등 세가지 능력에 따라 수준을 5가지로 분류.

| 분류 | 설명 |
|---|---|
| Lamer | 해커가 되고 싶지만 경험도 없고 컴퓨터 관련 지식도 많지 않은 해커 |
| Script Kiddie | 네트워크와 운영체제에 대한 약간의 기술적인 지식이 있는 해커 |
| Developed Kiddie | 대부분의 해킹 기법에 대해 알고 있으며, 해킹 수행 코드가 적용될 수 있는 취약점을 발견한 때까지 여러 번 시도해 시스템 침투에 성공할 수 있는 해커 |
| Semi Elite | 컴퓨터에 대한 포괄적인 지식이 있고 운영체제와 네트워크에 대한 지식도 갖추고 있으며, 운영체제에 존재하는 특정 취약점을 알고 이 취약점을 공격할 수 있는 해킹 코드를 만들 수 있는 해커 |
| Elite | 해킹하고자 하는 시스템의 새로운 취약점을 찾아내어 해킹할 수 있고 해킹 시도 후 흔적을 완벽하게 지울 수 있어 추적하기 어려운 최고 수준의 해커 |

# 1. 네트워크 보안의 기초

- 해커의 성격에 따른 분류
  - 화이트 해커 : 모의 해킹이나 취약점 점검 등의 기법을 활용하여 취약점을 알려주고 문제를 해결하도록 도와주는 윤리적이고 합법적인 정보보호 전문가.
  - 블랙 해커 : 악의적 목적의 정보 체계 침입, 컴퓨터 소프트웨어 변조, 컴퓨터 바이러스 유포 등의 행위로 해를 끼치는 해커(크래커).
  - 그레이 해커 : 해커와 크래커의 중간적인 성질을 가짐.
  - 그외 구분
    - ✓ 레드햇(홍커)
    - ✓ 스크립트 키디