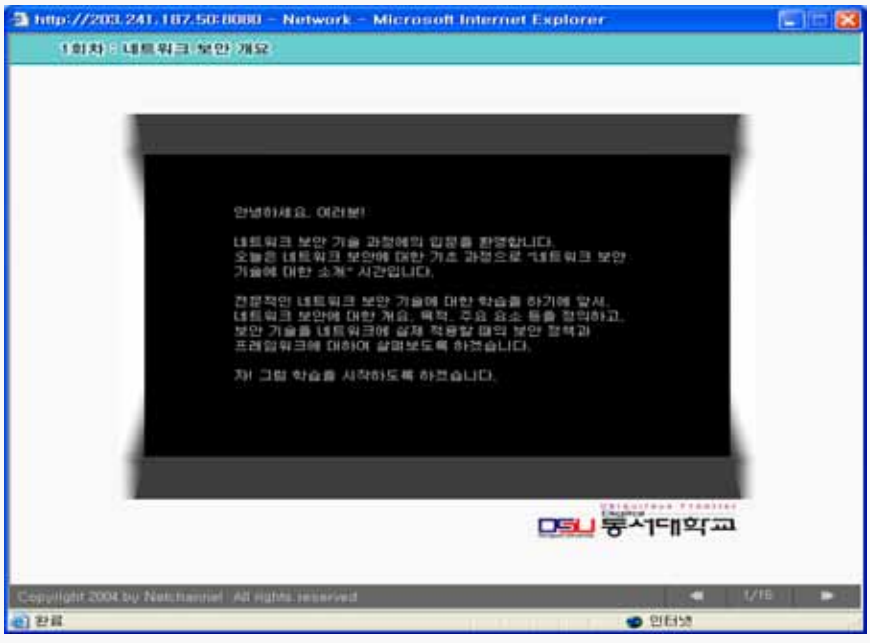
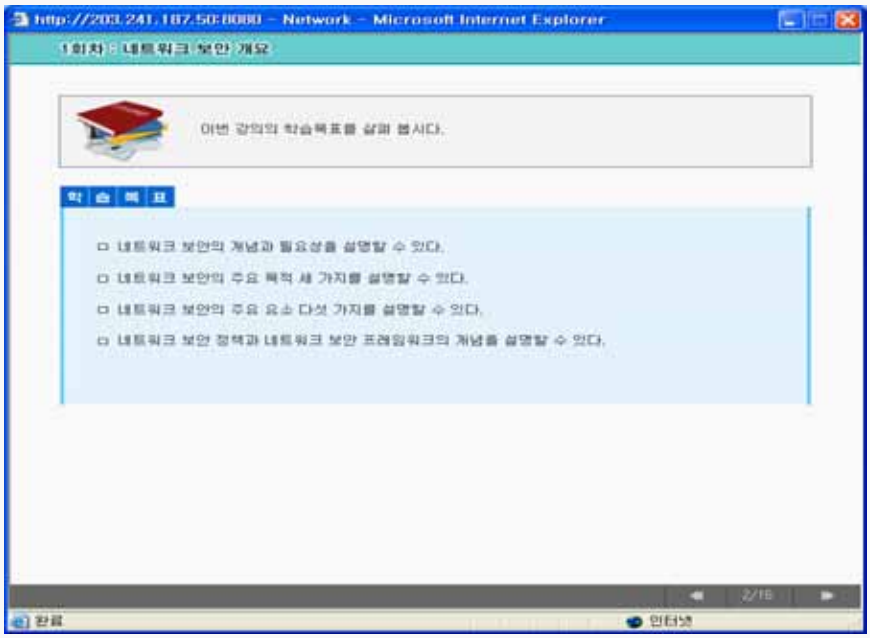
FNS

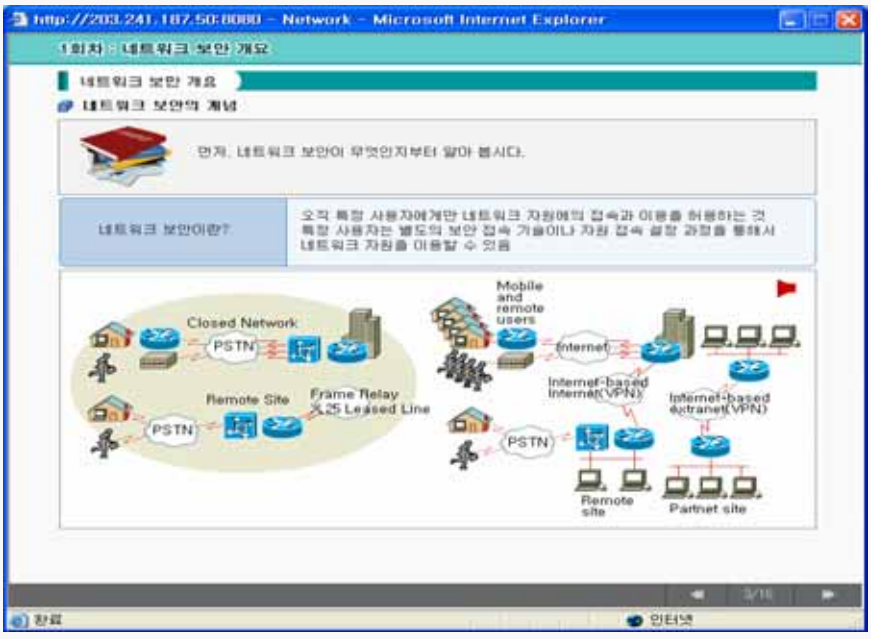
(Fundamental Network Security)

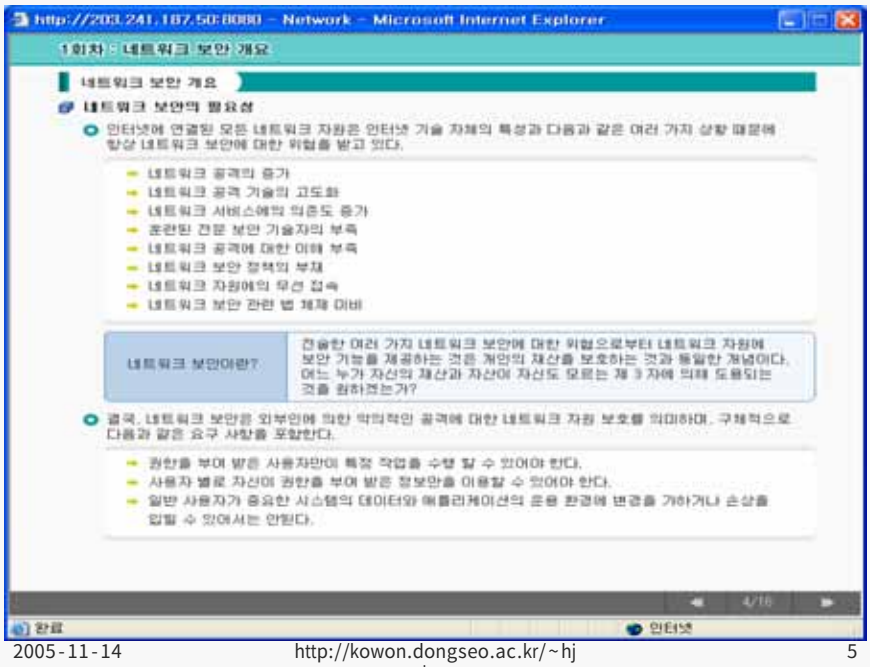
Ch1. 네트워크보안의 개요

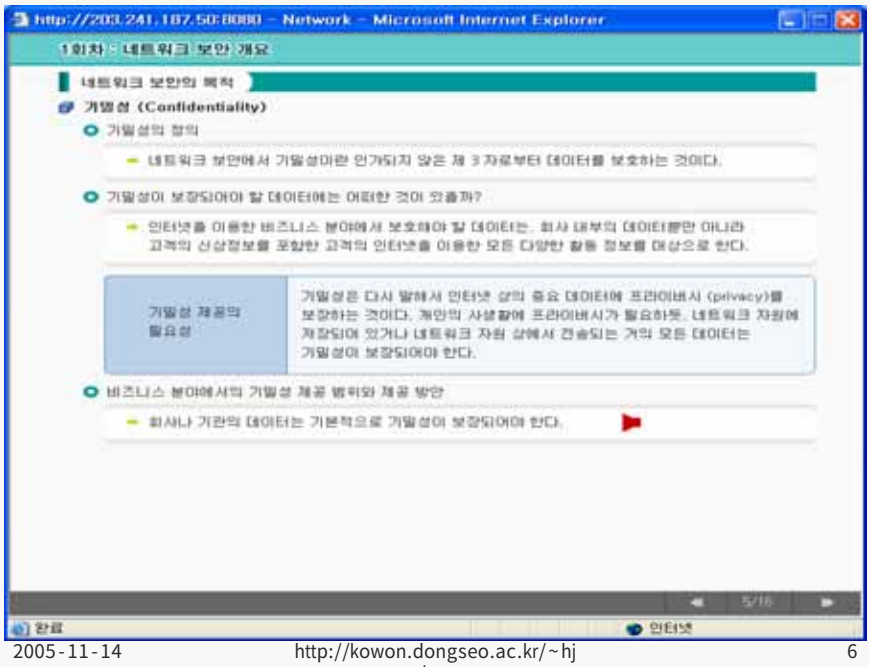
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

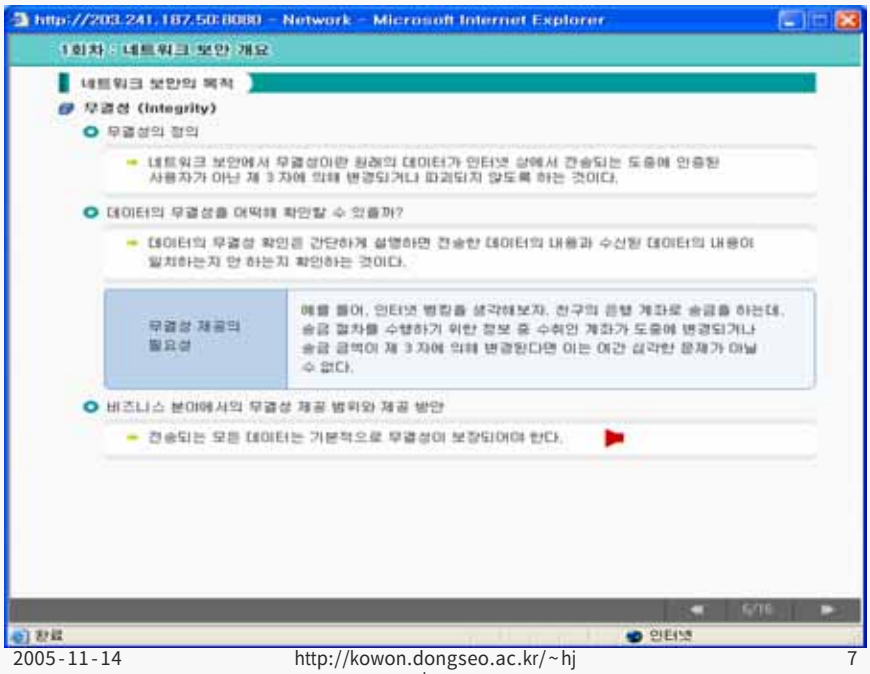



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
이번 강의의 학습목표를 살펴 봅시다.
학 습 목 표
□ 네트워크 보안의 개념과 필요성을 설명할 수 있다.
□ 네트워크 보안의 주요 목적 세 가지를 설명할 수 있다.
□ 네트워크 보안의 주요 요소 다섯 가지를 설명할 수 있다.
□ 네트워크 보안 정책과 네트워크 보안 프레임워크의 개념을 설명할 수 있다.
2/15
완료
인터넷

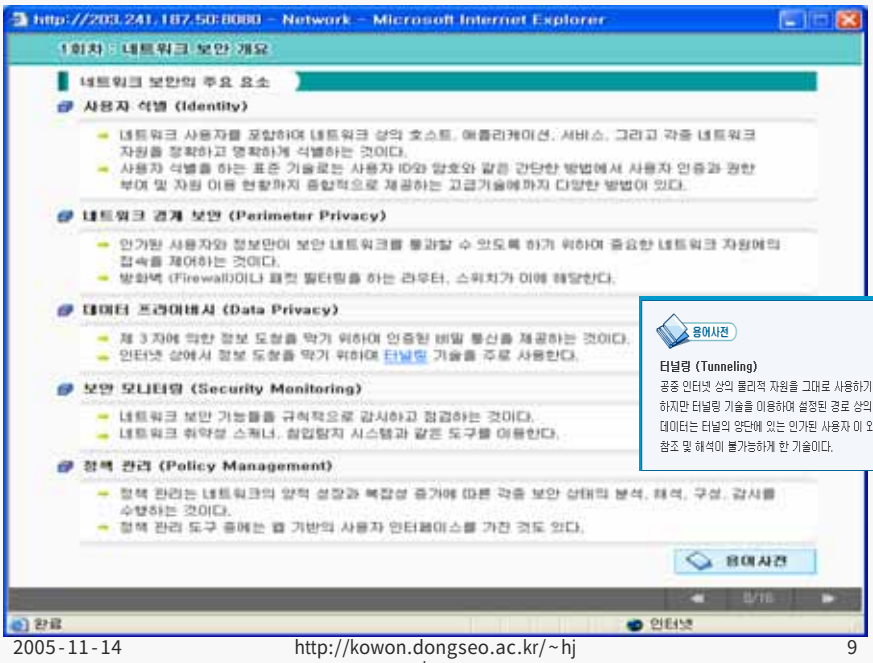

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안 개요
네트워크 보안의 개념
먼저, 네트워크 보안이 무엇인지부터 알아 봅시다.
네트워크 보안이란?
오직 특정 사용자에게만 네트워크 자원에의 접속과 이용을 허용하는 것
특정 사용자는 별도의 보안 접속 기술이나 자원 접속 설정 과정을 통해서
네트워크 자원을 이용할 수 있음
Closed Network
PSTN
Remote Site
Frame Relay
X.25 Leased Line
PSTN
Mobile and remote users
Internet
Internet-based Internet(VPN)
Internet-based extranet(VPN)
PSTN
Remote site
Partnet site
3/15
완료
인터넷

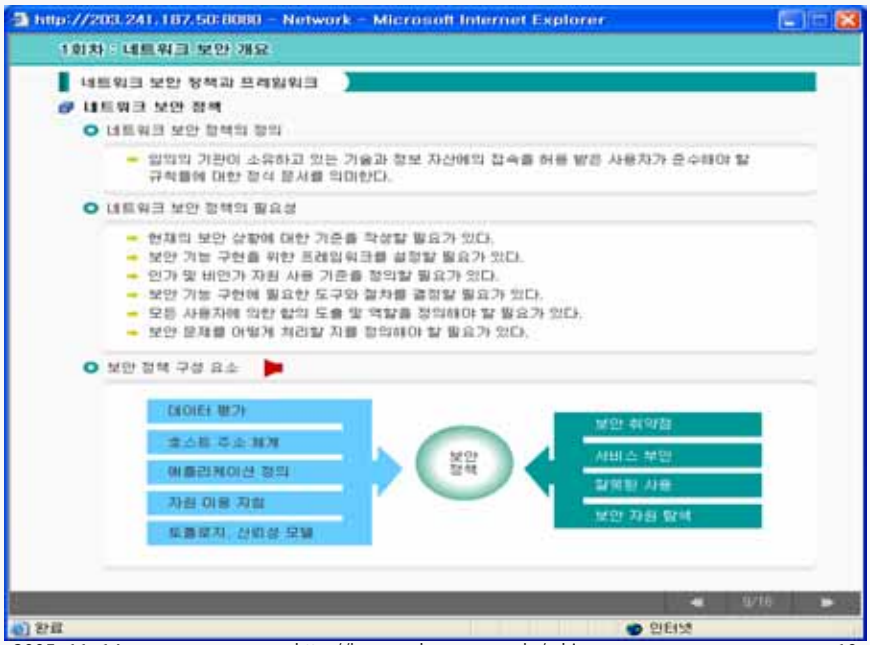

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안 개요
네트워크 보안의 필요성
인터넷에 연결된 모든 네트워크 자원은 인터넷 기술 자체의 특성과 다음과 같은 여러 가지 상황 때문에 항상 네트워크 보안에 대한 위협을 받고 있다.
네트워크 공격의 증가
네트워크 공격 기술의 고도화
네트워크 서비스에의 의존도 증가
숙련된 전문 보안 기술자의 부족
네트워크 공격에 대한 이해 부족
네트워크 보안 정책의 부재
네트워크 자원에의 무선 접속
네트워크 보안 관련 법 체제 미비
네트워크 보안이란?
전술한 여러 가지 네트워크 보안에 대한 위협으로부터 네트워크 자원에 보안 기능을 제공하는 것은 개인의 재산을 보호하는 것과 동일한 개념이다. 여느 누가 자신의 재산과 자산이 자신도 모르는 제 3 자에 의해 도용되는 것을 원하겠는가?
결국, 네트워크 보안은 외부인에 의한 악의적인 공격에 대한 네트워크 자원 보호를 의미하며, 구체적으로 다음과 같은 요구 사항을 포함한다.
권한을 부여 받은 사용자만이 특정 작업을 수행 할 수 있어야 한다.
사용자 별로 자신이 권한을 부여 받은 정보만을 이용할 수 있어야 한다.
일반 사용자가 중요한 시스템의 데이터와 애플리케이션의 운용 환경에 변경을 가하거나 손상을 입힐 수 있어서는 안된다.
4/16
완료
인터넷

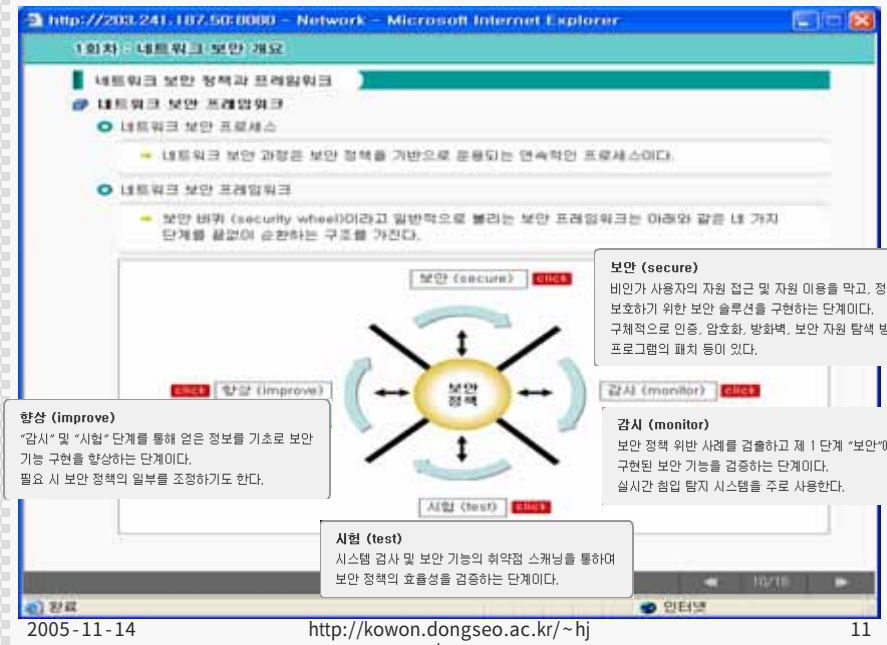

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안의 목적
기밀성 (Confidentiality)
기밀성의 정의
네트워크 보안에서 기밀성이란 인가되지 않은 제 3 자로부터 데이터를 보호하는 것이다.
기밀성이 보장되어야 할 데이터에는 어떠한 것이 있을까?
인터넷을 이용한 비즈니스 분야에서 보호해야 할 데이터는, 회사 내부의 데이터뿐만 아니라 고객의 신상정보를 포함한 고객의 인터넷을 이용한 모든 다양한 활동 정보를 대상으로 한다.
기밀성 제공의 필요성
기밀성은 다시 말해서 인터넷 상의 중요 데이터에 프라이버시 (privacy)를 보장하는 것이다. 개인의 사생활에 프라이버시가 필요하듯, 네트워크 자원에 저장되어 있거나 네트워크 자원 상에서 전송되는 거의 모든 데이터는 기밀성이 보장되어야 한다.
비즈니스 분야에서의 기밀성 제공 범위와 제공 방안
회사나 기관의 데이터는 기본적으로 기밀성이 보장되어야 한다.
5/16
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안의 목적
무결성 (Integrity)
무결성의 정의
네트워크 보안에서 무결성이란 원래의 데이터가 인터넷 상에서 전송되는 도중에 인증된 사용자가 아닌 제 3 자에 의해 변경되거나 파괴되지 않도록 하는 것이다.
데이터의 무결성을 어떻게 확인할 수 있을까?
데이터의 무결성 확인은 간단하게 설명하면 전송한 데이터의 내용과 수신된 데이터의 내용이 일치하는지 안 하는지 확인하는 것이다.
무결성 제공의 필요성
예를 들어, 인터넷 뱅킹을 생각해보자. 친구의 은행 계좌로 송금을 하는데, 송금 절차를 수행하기 위한 정보 중 수취인 계좌가 도중에 변경되거나 송금 금액이 제 3 자에 의해 변경된다면 이는 여간 심각한 문제가 아닐 수 없다.
비즈니스 분야에서의 무결성 제공 범위와 제공 방안
전송되는 모든 데이터는 기본적으로 무결성이 보장되어야 한다.
5/16
완료
인터넷

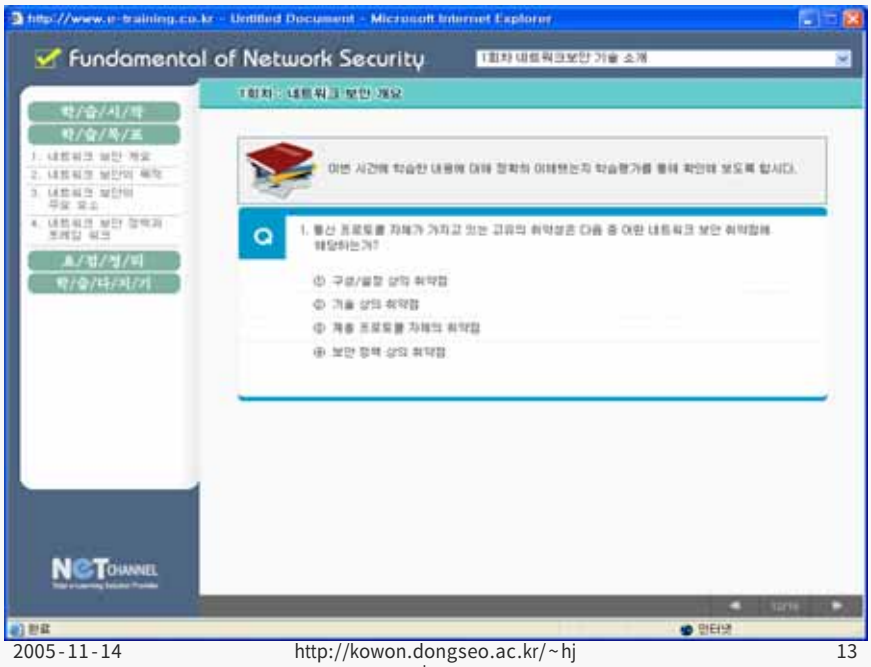

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안의 목적
가용성 (Availability)
가용성의 정의
네트워크 보안에서 가용성이란 컴퓨팅 시스템들이 연속적으로 또한 정상적으로 동작해야 한다는 것이다.
가용성 레벨
인터넷 상의 애플리케이션은 애플리케이션 별로 서로 다른 가용성 레벨을 가지고 있다. 어떤 서비스는 연중 상시 서비스를 제공하기도 하지만 어떤 서비스는 특정 날자 및 시간에는 관리 차원에서 서비스를 중지하기도 한다.
가용성 제공의 필요성
인터넷 사용자는 언제든 원하는 시간에 원하는 정보를 얻고자 한다. 그러나 원하는 정보를 저장하고 있는 컴퓨팅 시스템이 임의의 공격을 받아 정상적인 서비스를 할 수 없거나 이에 해당 시스템에 접속할 수 없는 상황이라면 서비스 제공 자체가 불가한 것이다.
비즈니스 분야에서의 가용성 제공 범위와 가용성 제공 방안
인터넷 상의 애플리케이션을 비롯하여 데이터베이스 서버, 스토리지 장치, 네트워킹 장치는 모든 기본적으로 가용성이 보장되어야 한다.
7/16
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안의 주요 요소
사용자 식별 (Identity)
네트워크 경계 보안 (Perimeter Privacy)
데이터 프라이버시 (Data Privacy)
보안 모니터링 (Security Monitoring)
정책 관리 (Policy Management)
용어사전
터널링 (Tunneling)
공중 인터넷 상의 물리적 자원을 그대로 사용하기는 하지만 터널링 기술을 이용하여 설정된 경로 상의 데이터는 터널의 양단에 있는 인가된 사용자 이 외에는 참조 및 해석이 불가능하게 한 기술이다.
완료
인터넷

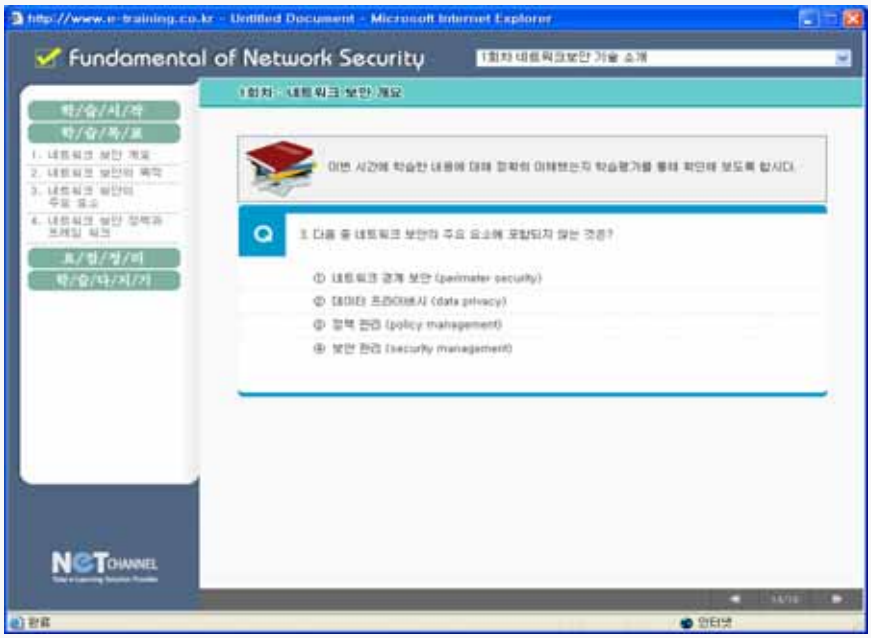

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안 정책과 프레임워크
네트워크 보안 정책
네트워크 보안 정책의 정의
네트워크 보안 정책의 필요성
보안 정책 구성 요소
데이터 평가
호스트 주소 체계
애플리케이션 정의
자원 이용 지침
토폴로지, 신뢰성 모델
보안 정책
보안 취약점
서비스 부인
보안 자원 탐색
완료
인터넷

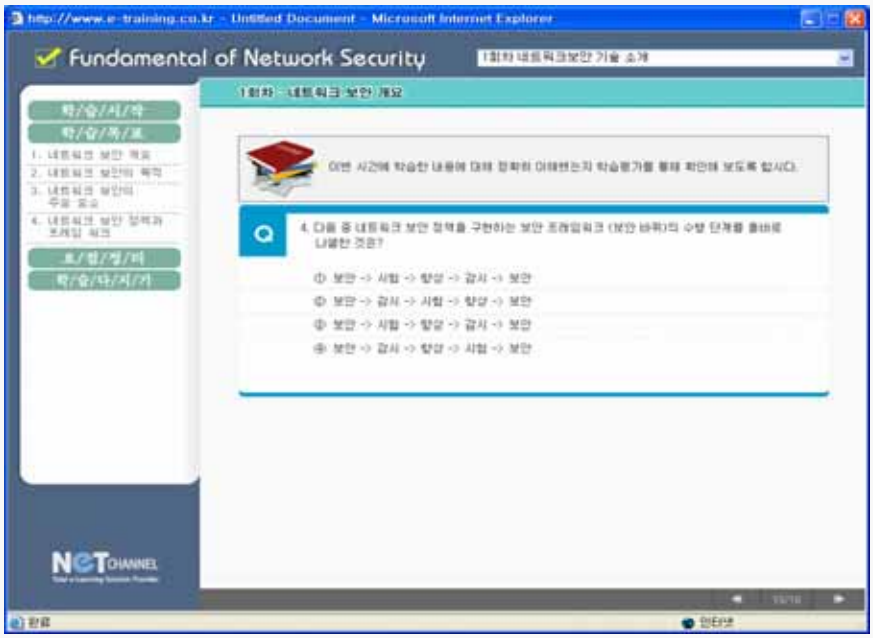

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
네트워크 보안 정책과 프레임워크
네트워크 보안 프레임워크
네트워크 보안 프로세스
네트워크 보안 과정은 보안 정책을 기반으로 운용되는 연속적인 프로세스이다.
네트워크 보안 프레임워크
보안 바퀴 (security wheel)이라고 일반적으로 불리는 보안 프레임워크는 아래와 같은 네 가지 단계를 끊임이 순환하는 구조를 가진다.
보안 (secure)
CLICK
향상 (improve)
CLICK
보안 정책
감시 (monitor)
CLICK
시험 (test)
CLICK
보안 (secure)
비인가 사용자의 자원 접근 및 자원 이용을 막고, 정보를 보호하기 위한 보안 솔루션을 구현하는 단계이다.
구체적으로 인증, 암호화, 방화벽, 보안 자원 탐색 방지 프로그램의 패치 등이 있다.
향상 (improve)
"감시" 및 "시험" 단계를 통해 얻은 정보를 기초로 보안 기능 구현을 향상하는 단계이다.
필요 시 보안 정책의 일부를 조정하기도 한다.
감시 (monitor)
보안 정책 위반 사례를 검출하고 제 1 단계 "보안"에서 구현된 보안 기능을 검증하는 단계이다.
실시간 침입 탐지 시스템을 주로 사용한다.
시험 (test)
시스템 검사 및 보안 기능의 취약점 스캐닝을 통하여 보안 정책의 효율성을 검증하는 단계이다.
10/16
완료
인터넷

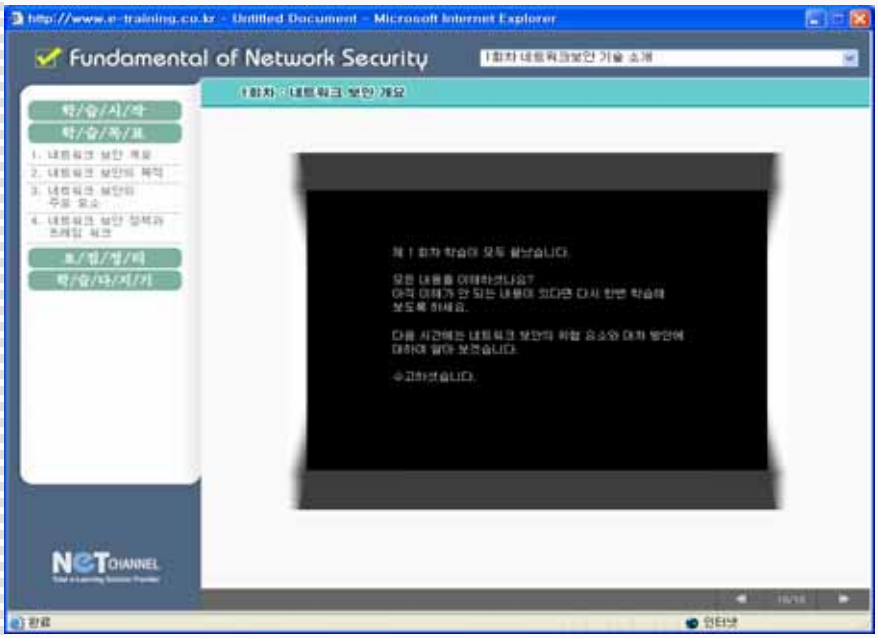

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
1회차 : 네트워크 보안 개요
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
네트워크 보안 개요
특정의 인가된 사용자에게만 네트워크 자원에의 접속과 이용을 허용하는 것이다.
네트워크 보안의 목적
네트워크 보안의 세 가지 주요 목적은 기밀성, 무결성, 가용성이다.
기밀성은 데이터가 비인가 사용자에게 노출되는 것을 보호하는 것이며, 무결성은 데이터가 비인가 사용자에 의해 변경 및 손상되는 것을 막는 것이며, 가용성은 컴퓨팅 시스템의 연속적인 운영으로 정의된다.
네트워크 보안의 주요 요소
네트워크 보안의 다섯 가지 주요 요소로 사용자 식별, 네트워크 경계 보안, 데이터 프라이버시, 보안 모니터링, 정책 관리가 있다.
네트워크 보안 정책과 프레임워크
임의의 기관이 소유하고 있는 기술과 정보 자산에의 접속을 허용 받은 사용자가 준수해야 할 규칙들에 대한 정식 기준을 보안 정책이라 하며, 보안 바퀴를 기반으로 보안 정책을 지속적으로 유지,관리한다.
11/16
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
1회차 네트워크보안 기술 소개
학/습/시/작
학/습/목/표
1. 네트워크 보안 개요
2. 네트워크 보안의 목적
3. 네트워크 보안의 주요 요소
4. 네트워크 보안 정책과 프레임 워크
효/험/정/리
학/습/마/치/기
1회차 : 네트워크보안 개요
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
1. 통신 프로토콜 자체가 가지고 있는 고유의 취약성은 다음 중 어떤 네트워크 보안 취약점에 해당하는가?
① 구성/설정 상의 취약점
② 기술 상의 취약점
③ 제품 프로토콜 자체의 취약점
④ 보안 정책 상의 취약점
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
1회차 네트워크보안 기술 소개
학/습/시/작
학/습/목/표
1. 네트워크 보안 개요
2. 네트워크 보안의 목적
3. 네트워크 보안의 주요 요소
4. 네트워크 보안 정책과 프레임 워크
효/험/정/리
학/습/마/치/기
1회차 : 네트워크보안 개요
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
2. 다음 중 네트워크 보안의 세 가지 목적에 포함되지 않는 것은?
① 사용자 식별 (Identity)
② 기밀성 (confidentiality)
③ 무결성 (Integrity)
④ 가용성 (availability)
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
1회차 네트워크보안 기술 소개
학/습/시/작
학/습/목/표
1. 네트워크 보안 개요
2. 네트워크 보안의 목적
3. 네트워크 보안의 주요 요소
4. 네트워크 보안 정책과 프레임 워크
효/율/성/비
학/습/닥/지/기
1회차 - 네트워크 보안 개요
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
3. 다음 중 네트워크 보안의 주요 요소에 포함되지 않는 것은?
① 네트워크 경계 보안 (perimeter security)
② 데이터 프라이버시 (data privacy)
③ 정책 관리 (policy management)
④ 보안 관리 (security management)
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
1회차 네트워크보안 기술 소개
학/습/시/작
학/습/목/표
1. 네트워크 보안 개요
2. 네트워크 보안의 목적
3. 네트워크 보안의 주요 요소
4. 네트워크 보안 정책과 프레임 워크
효/율/성/비
학/습/닥/지/기
1회차 - 네트워크 보안 개요
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
4. 다음 중 네트워크 보안 정책을 구현하는 보안 프레임워크 (보안 바퀴)의 수행 단계를 올바르게 나열한 것은?
① 보안 -> 사업 -> 향상 -> 감시 -> 보안
② 보안 -> 감시 -> 사업 -> 향상 -> 보안
③ 보안 -> 사업 -> 향상 -> 감시 -> 보안
④ 보안 -> 감시 -> 향상 -> 사업 -> 보안
NETCHANNEL
완료
인터넷



End of Lecture