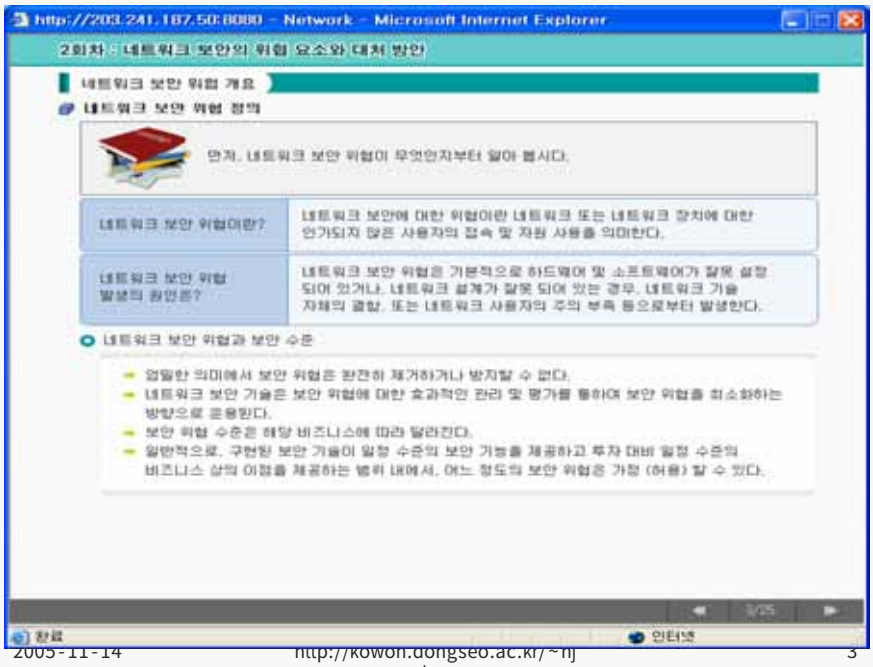
FNS

(Fundamental Network Security)

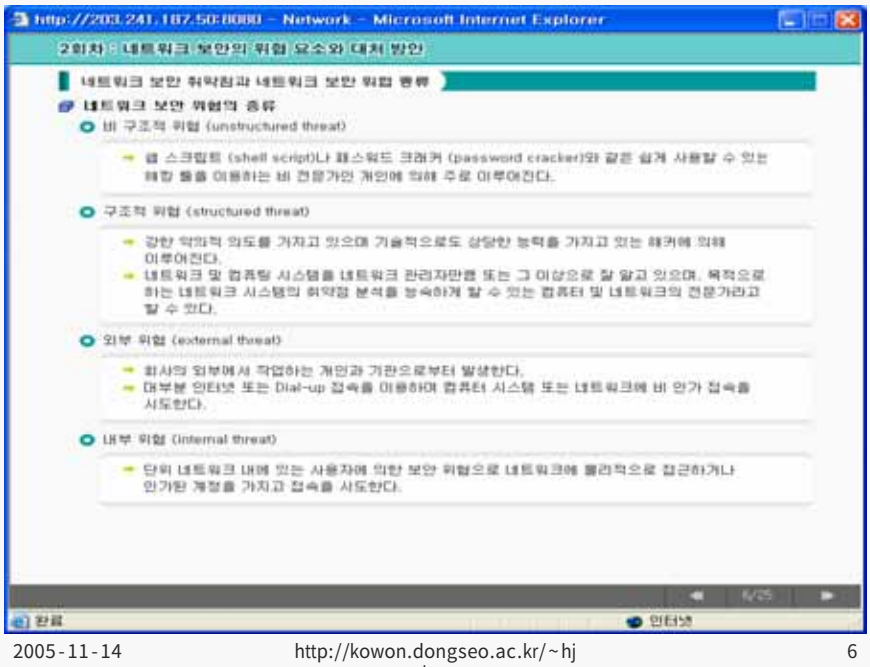
Ch2. 네트워크보안의 위협요소와 대처방안

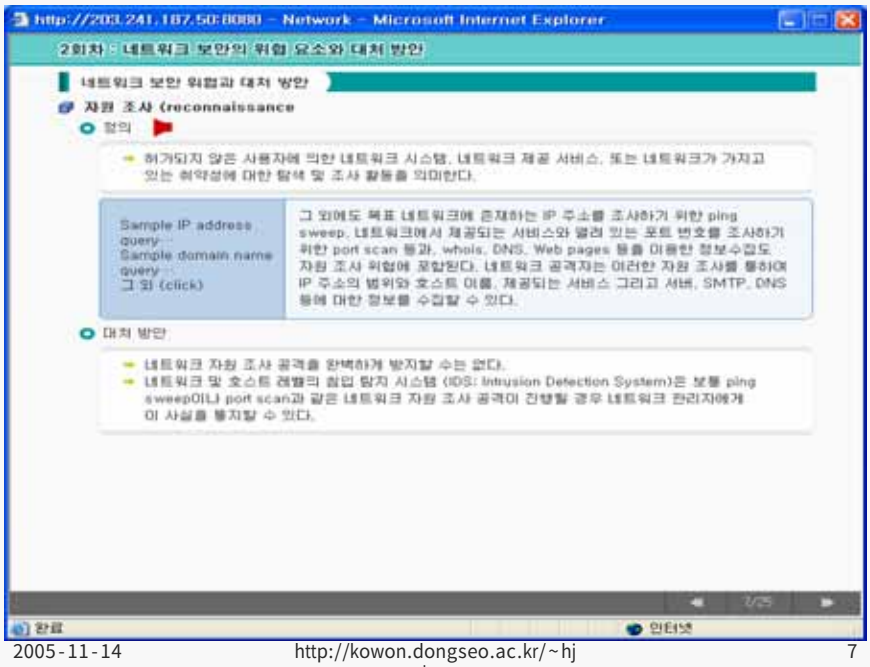
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

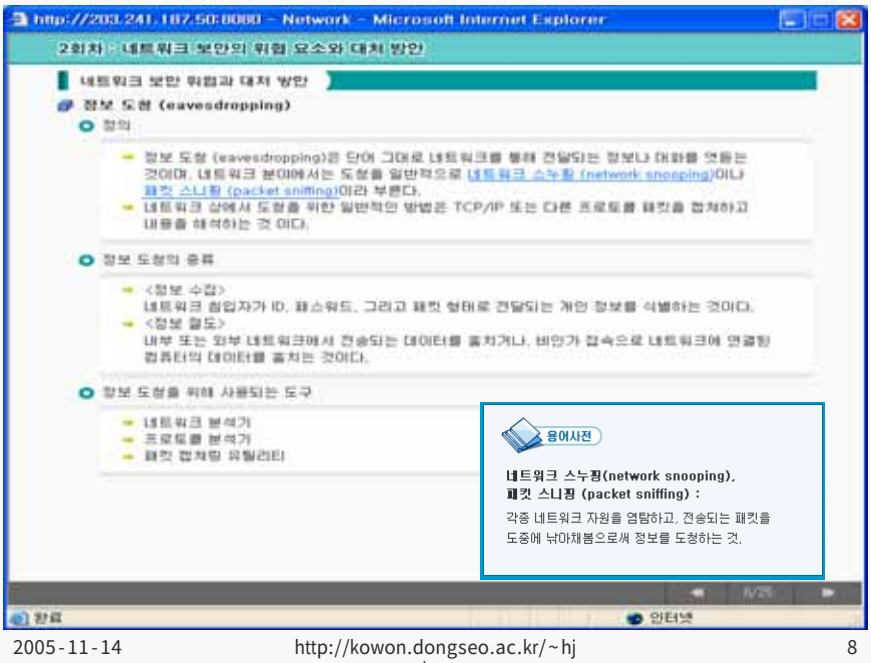

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협 개요
네트워크 보안 위협 정의
먼저, 네트워크 보안 위협이 무엇인지부터 알아 봅시다.
네트워크 보안 위협이란?
네트워크 보안에 대한 위협이란 네트워크 또는 네트워크 장치에 대한 인가되지 않은 사용자의 접속 및 자원 사용을 의미한다.
네트워크 보안 위협 발생의 원인은?
네트워크 보안 위협은 기본적으로 하드웨어 및 소프트웨어가 잘못 설정 되어 있거나, 네트워크 설계가 잘못 되어 있는 경우, 네트워크 기술 자체의 결함, 또는 네트워크 사용자의 주의 부족 등으로부터 발생한다.
네트워크 보안 위협과 보안 수준
업밀한 의미에서 보안 위협은 완전히 제거하거나 방지할 수 없다.
네트워크 보안 기술은 보안 위협에 대한 효과적인 관리 및 평가를 통하여 보안 위협을 최소화하는 방향으로 운용된다.
보안 위협 수준은 해당 비즈니스에 따라 달라진다.
일반적으로, 구현된 보안 기술이 일정 수준의 보안 기능을 제공하고 투자 대비 일정 수준의 비즈니스 상의 이점을 제공하는 범위 내에서, 어느 정도의 보안 위협은 가정 (허용) 할 수 있다.
3/25
완료
인터넷

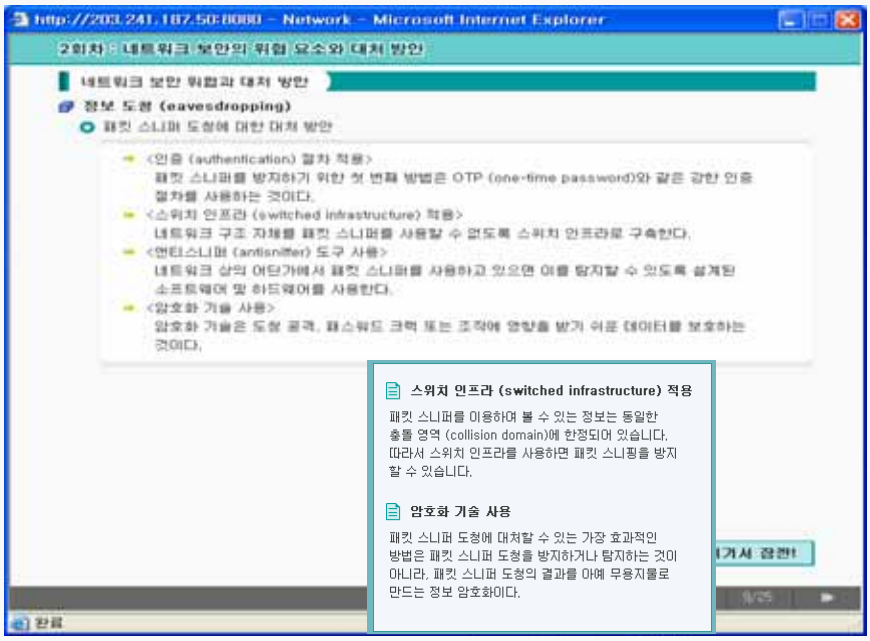

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협 개요
네트워크 보안 기초
네트워크 보안은 우선 보안에 대한 사용자의 인식에서부터 시작되어야 합니다.
모든 네트워크 사용자가 알아야 할 보안 기술
네트워크 시스템을 설계/구현하고 관리하는 모든 사람을 대상으로 보안 기술 트레이닝을 실시해야 한다.
간단하게는 네트워크 자원 이용 시 필요한 암호 관리에서, 네트워크 시스템 개발/운용/관리와 관련된 보안 기술의 종류와 트레픽 관리 방안에 이르기까지 보안에 대한 전반적인 개념을 숙지해야 한다.
네트워크 보안 책임자가 알아야 할 보안 기술
각종 보안 기술
보안 위협과 네트워크 취약점 분석 방법
네트워크 트레픽 제어 기술의 구현 방법
각각의 보안 기능 부재 시 발생 가능한 보안 위협
4/25
완료
인터넷

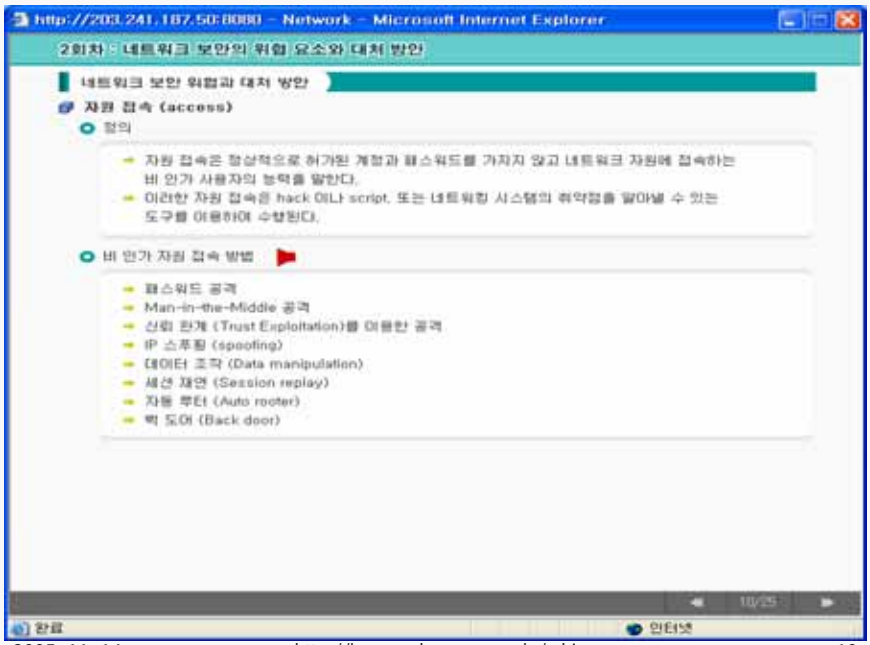

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 취약점과 네트워크 보안 위협 종류
네트워크 보안 상의 취약점
기술 상의 취약점
컴퓨터와 네트워크 기술 자체의 근본적인 취약점이 있다.
예를 들면, TCP/IP 프로토콜 자체의 취약점과 운영 시스템 및 네트워크 장치 상의 취약점 등이다.
구성/설정 상의 취약점
네트워크 관리자나 기술자가 컴퓨팅 및 네트워크 장치의 설정을 올바로 하지 못해서 발생하는 보안 결점이다.
예를 들면, 보안 기능이 적용되지 않은 사용자 ID와 패스워드가 네트워크를 통해 전송될 때 스누퍼(snooper)에 의해 노출될 수 있다. 또한 잘못 설정된 access-list, 라우팅 프로토콜 등이 포함된다.
보안 정책 상의 취약점
보안 정책이 잘못되어 예기치 못한 보안 위협이 발생할 수 있으며, 사용자가 보안 정책을 준수하지 않을 경우에도 네트워크 보안 상의 위협을 초래할 수 있다.
예를 들면, 디폴트 (default) 패스워드를 사용하거나, 쉽게 크랙될 수 있는 패스워드의 사용, 그리고 인가되지 않은 네트워크 토폴로지 변경과 응용 프로그램의 설치 등이다.
5/25
완료
인터넷

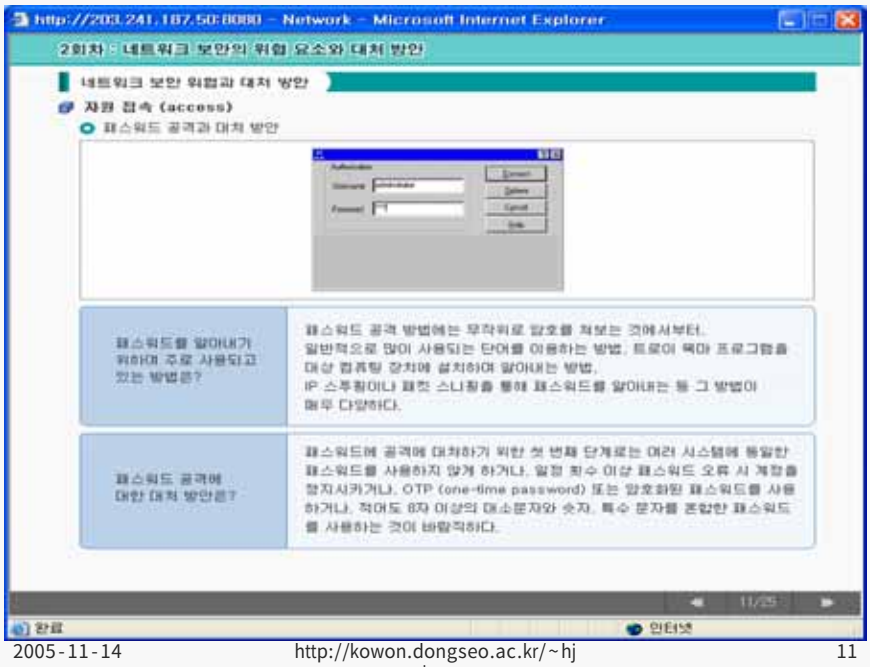

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 취약점과 네트워크 보안 위협 종류
네트워크 보안 위협의 종류
비 구조적 위협 (unstructured threat)
쉘 스크립트 (shell script)나 패스워드 크래커 (password cracker)와 같은 쉽게 사용할 수 있는 해킹 툴을 이용하는 비 전문가인 개인에 의해 주로 이루어진다.
구조적 위협 (structured threat)
강한 악의적 의도를 가지고 있으며 기술적으로도 상당한 능력을 가지고 있는 해커에 의해 이루어진다.
네트워크 및 컴퓨팅 시스템을 네트워크 관리자만큼 또는 그 이상으로 잘 알고 있으며, 목적으로 하는 네트워크 시스템의 취약점 분석을 능숙하게 할 수 있는 컴퓨터 및 네트워크의 전문가라고 할 수 있다.
외부 위협 (external threat)
회사의 외부에서 작업하는 개인과 기관으로부터 발생한다.
대부분 인터넷 또는 Dial-up 접속을 이용하여 컴퓨터 시스템 또는 네트워크에 비 인가 접속을 시도한다.
내부 위협 (internal threat)
단위 네트워크 내에 있는 사용자에 의한 보안 위협으로 네트워크에 물리적으로 접근하거나 인가된 계정을 가지고 접속을 시도한다.
5/25
완료
인터넷

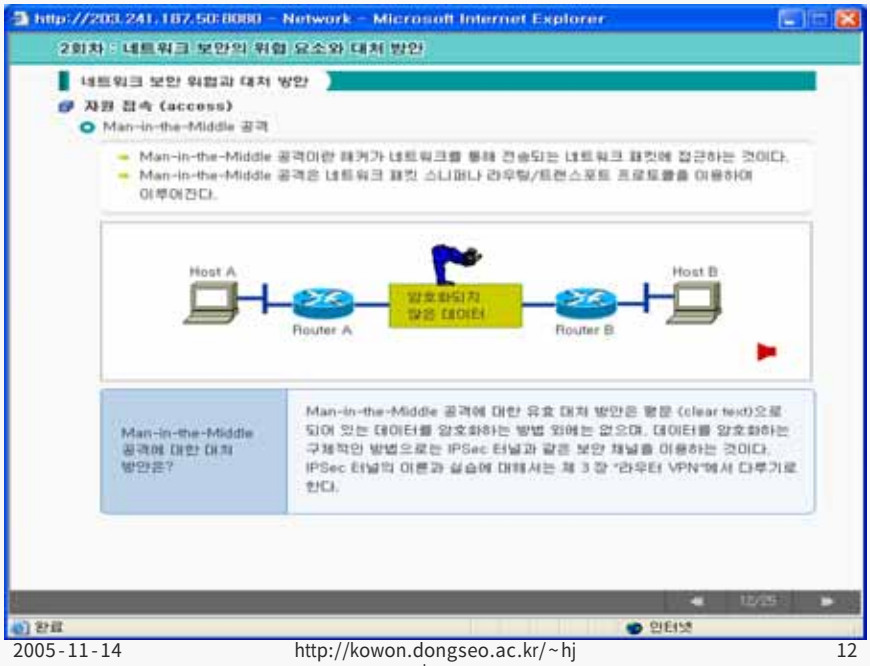

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 - 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 조사 (reconnaissance
정의
허가되지 않은 사용자에 의한 네트워크 시스템, 네트워크 제공 서비스, 또는 네트워크가 가지고 있는 취약성에 대한 탐색 및 조사 활동을 의미한다.
Sample IP address query
Sample domain name query
그 외 (click)
그 외에도 목표 네트워크에 존재하는 IP 주소를 조사하기 위한 ping sweep, 네트워크에서 제공되는 서비스와 열려 있는 포트 번호를 조사하기 위한 port scan 등과, whois, DNS, Web pages 등을 이용한 정보수집도 자원 조사 위협에 포함된다. 네트워크 공격자는 이러한 자원 조사를 통하여 IP 주소의 범위와 호스트 이름, 제공되는 서비스 그리고 서버, SMTP, DNS 등에 대한 정보를 수집할 수 있다.
대처 방안
네트워크 자원 조사 공격을 완벽하게 방지할 수는 없다.
네트워크 및 호스트 레벨의 침입 탐지 시스템 (IDS: Intrusion Detection System)은 보통 ping sweep이나 port scan과 같은 네트워크 자원 조사 공격이 진행될 경우 네트워크 관리자에게 이 사실을 통지할 수 있다.
2/25
완료
인터넷

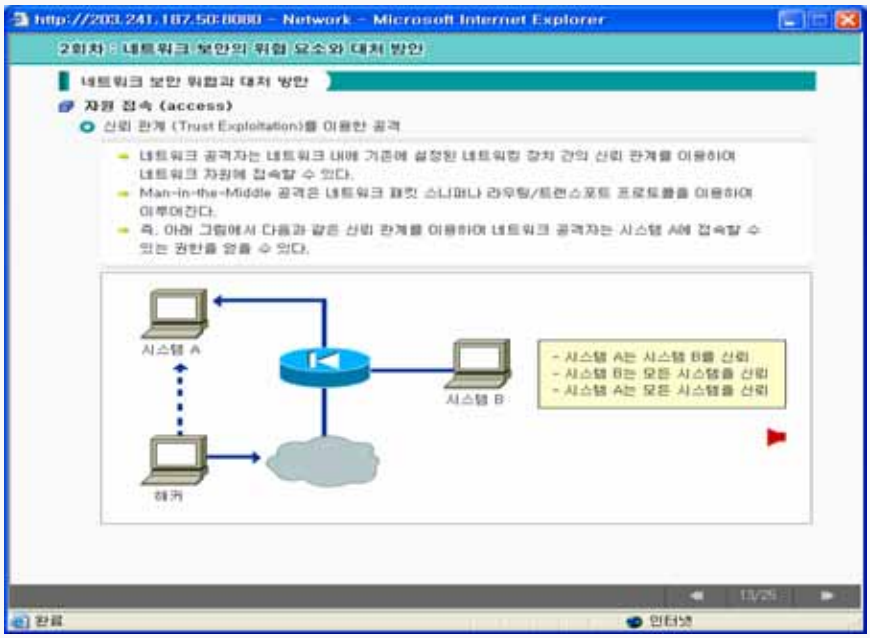

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 - 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
정보 도청 (eavesdropping)
정의
정보 도청 (eavesdropping)은 단어 그대로 네트워크를 통해 전달되는 정보나 대화를 엿듣는 것이며, 네트워크 분야에서는 도청을 일반적으로 네트워크 스누핑 (network snooping)이나 패킷 스니핑 (packet sniffing)이라 부른다.
네트워크 상에서 도청을 위한 일반적인 방법은 TCP/IP 또는 다른 프로토콜 패킷을 캡처하고 내용을 해석하는 것 이다.
정보 도청의 종류
<정보 수집>
네트워크 침입자가 ID, 패스워드, 그리고 패킷 형태로 전달되는 개인 정보를 식별하는 것이다.
<정보 절도>
내부 또는 외부 네트워크에서 전송되는 데이터를 훔치거나, 비인가 접속으로 네트워크에 연결된 컴퓨터의 데이터를 훔치는 것이다.
정보 도청을 위해 사용되는 도구
네트워크 분석기
프로토콜 분석기
패킷 캡처링 유틸리티
용어사전
네트워크 스누핑(network snooping), 패킷 스니핑 (packet sniffing) :
각종 네트워크 자원을 염탐하고, 전송되는 패킷을 도중에 낚아채봄으로써 정보를 도청하는 것.
8/25
완료
인터넷

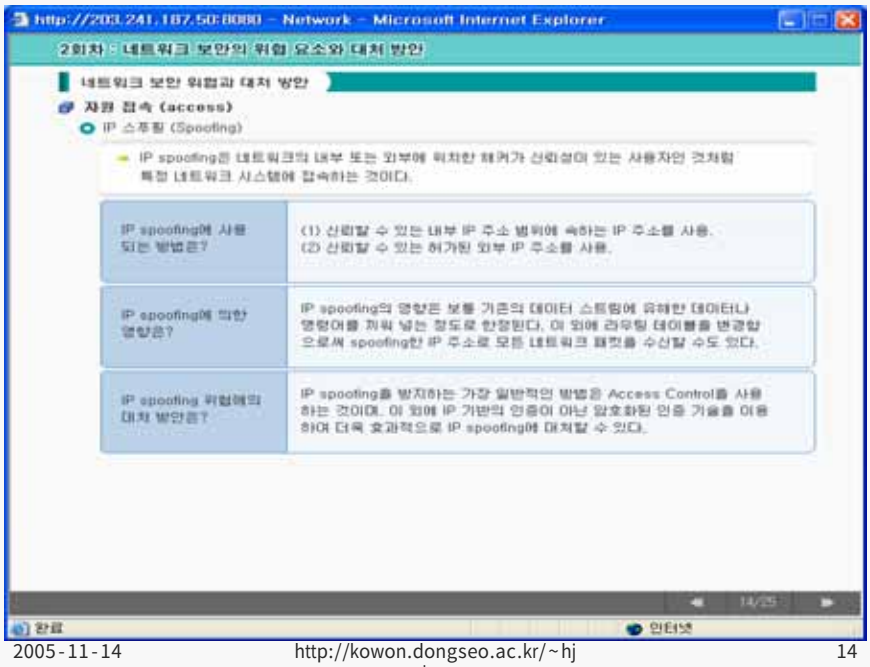

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
정보 도청 (eavesdropping)
패킷 스니퍼 도청에 대한 대처 방안
<인증 (authentication) 절차 적용>
패킷 스니퍼를 방지하기 위한 첫 번째 방법은 OTP (one-time password)와 같은 강한 인증 절차를 사용하는 것이다.
<스위치 인프라 (switched infrastructure) 적용>
네트워크 구조 자체를 패킷 스니퍼를 사용할 수 없도록 스위치 인프라로 구축한다.
<안티스니퍼 (antisniffer) 도구 사용>
네트워크 상의 어딘가에서 패킷 스니퍼를 사용하고 있으면 이를 탐지할 수 있도록 설계된 소프트웨어 및 하드웨어를 사용한다.
<암호화 기술 사용>
암호화 기술은 도청 공격, 패스워드 크랙 또는 조작에 영향을 받기 쉬운 데이터를 보호하는 것이다.
스위치 인프라 (switched infrastructure) 적용
패킷 스니퍼를 이용하여 볼 수 있는 정보는 동일한 충돌 영역 (collision domain)에 한정되어 있습니다. 따라서 스위치 인프라를 사용하면 패킷 스니핑을 방지할 수 있습니다.
암호화 기술 사용
패킷 스니퍼 도청에 대처할 수 있는 가장 효과적인 방법은 패킷 스니퍼 도청을 방지하거나 탐지하는 것이 아니라, 패킷 스니퍼 도청의 결과를 아예 무용지물로 만드는 정보 암호화이다.
완료


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
정의
자원 접속은 정상적으로 허가된 계정과 패스워드를 가지지 않고 네트워크 자원에 접속하는 비 인가 사용자의 능력을 말한다.
이러한 자원 접속은 hack 이나 script, 또는 네트워킹 시스템의 취약점을 알아낼 수 있는 도구를 이용하여 수행된다.
비 인가 자원 접속 방법
패스워드 공격
Man-in-the-Middle 공격
신뢰 관계 (Trust Exploitation)를 이용한 공격
IP 스푸핑 (spoofing)
데이터 조작 (Data manipulation)
세션 재연 (Session replay)
자동 루터 (Auto rooter)
백 도어 (Back door)
완료
인터넷

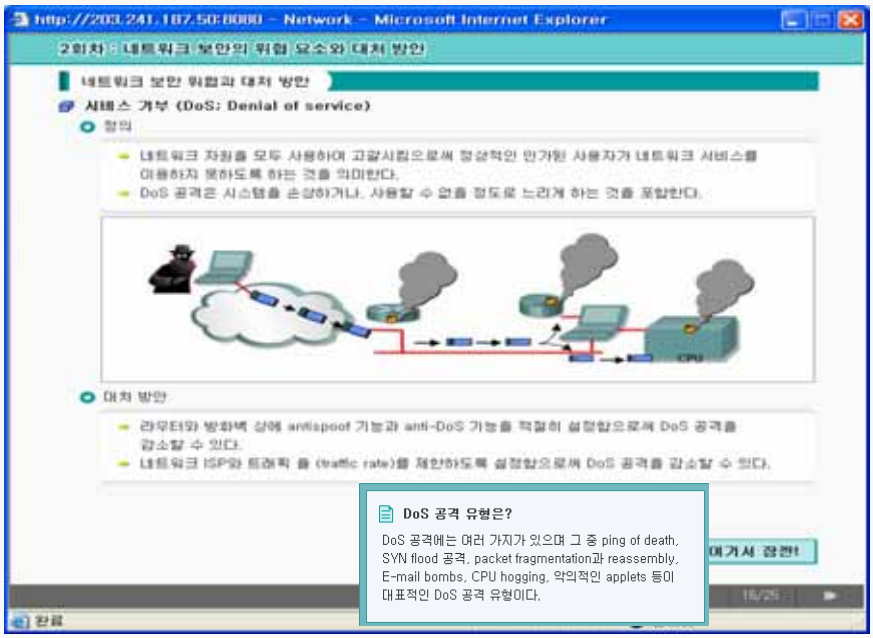

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
패스워드 공격과 대처 방안
패스워드를 알아내기 위하여 주로 사용되고 있는 방법은?
패스워드 공격 방법에는 무작위로 암호를 적보는 것에서부터, 일반적으로 많이 사용되는 단어를 이용하는 방법, 트로이 목마 프로그램을 대상 컴퓨팅 장치에 설치하여 알아내는 방법, IP 스푸핑이나 패킷 스니핑을 통해 패스워드를 알아내는 등 그 방법이 매우 다양하다.
패스워드 공격에 대한 대처 방안은?
패스워드에 공격에 대처하기 위한 첫 번째 단계로는 여러 시스템에 동일한 패스워드를 사용하지 않게 하거나, 일정 회수 이상 패스워드 오류 시 계정을 잠지시키거나, OTP (one-time password) 또는 암호화된 패스워드를 사용하거나, 적어도 8자 이상의 대소문자와 숫자, 특수 문자를 혼합한 패스워드를 사용하는 것이 바람직하다.
11/25
완료
인터넷

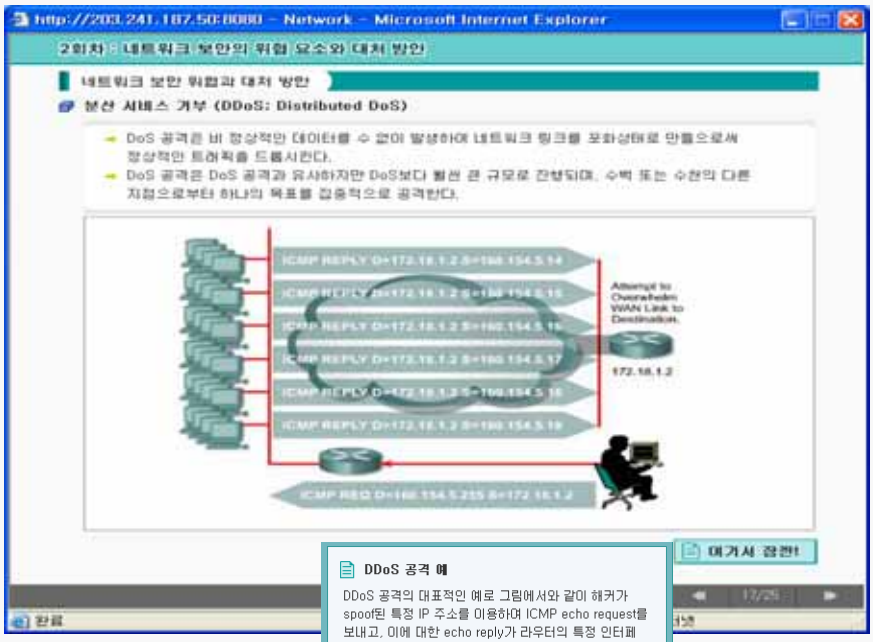

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
Man-in-the-Middle 공격
Man-in-the-Middle 공격이란 해커가 네트워크를 통해 전송되는 네트워크 패킷에 접근하는 것이다.
Man-in-the-Middle 공격은 네트워크 패킷 스니퍼나 라우팅/트랜스포트 프로토콜을 이용하여 이루어진다.
Host A
Router A
암호화되지 않은 데이터
Router B
Host B
Man-in-the-Middle 공격에 대한 대처 방안은?
Man-in-the-Middle 공격에 대한 유효 대처 방안은 평문 (clear text)으로 되어 있는 데이터를 암호화하는 방법 외에는 없으며, 데이터를 암호화하는 구체적인 방법으로는 IPSec 터널과 같은 보안 채널을 이용하는 것이다. IPSec 터널의 이론과 실습에 대해서는 제 3 장 "라우터 VPN"에서 다루기로 한다.
12/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
신뢰 관계 (Trust Exploitation)를 이용한 공격
네트워크 공격자는 네트워크 내에 기존에 설정된 네트워킹 장치 간의 신뢰 관계를 이용하여 네트워크 자원에 접속할 수 있다.
Man-in-the-Middle 공격은 네트워크 패킷 스니퍼나 라우팅/트랜스포트 프로토콜을 이용하여 이루어진다.
즉, 아래 그림에서 다음과 같은 신뢰 관계를 이용하여 네트워크 공격자는 시스템 A에 접속할 수 있는 권한을 얻을 수 있다.
시스템 A
시스템 B
해커
- 시스템 A는 시스템 B를 신뢰
- 시스템 B는 모든 시스템을 신뢰
- 시스템 A는 모든 시스템을 신뢰
13/25
완료
인터넷

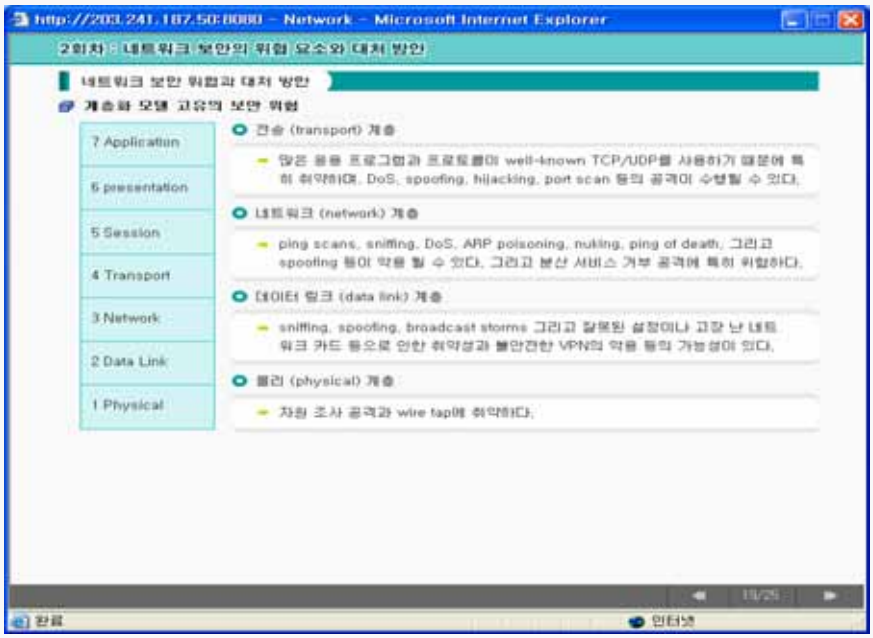

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
IP 스푸핑 (Spoofing)
IP spoofing은 네트워크의 내부 또는 외부에 위치한 해커가 신뢰성이 있는 사용자인 것처럼 특정 네트워크 시스템에 접속하는 것이다.
IP spoofing에 사용되는 방법은?
(1) 신뢰할 수 있는 내부 IP 주소 범위에 속하는 IP 주소를 사용.
(2) 신뢰할 수 있는 허가된 외부 IP 주소를 사용.
IP spoofing에 의한 영향은?
IP spoofing의 영향은 보통 기존의 데이터 스트림에 유해한 데이터나 명령어를 처워 넣는 정도로 한정된다. 이 외에 라우팅 테이블을 변경함으로써 spoofing한 IP 주소로 모든 네트워크 패킷을 수신할 수도 있다.
IP spoofing 위협에의 대처 방안은?
IP spoofing을 방지하는 가장 일반적인 방법은 Access Control을 사용하는 것이며, 이 외에 IP 기반의 인증이 아닌 암호화된 인증 기술을 이용하여 더욱 효과적으로 IP spoofing에 대처할 수 있다.
14/25
완료
인터넷

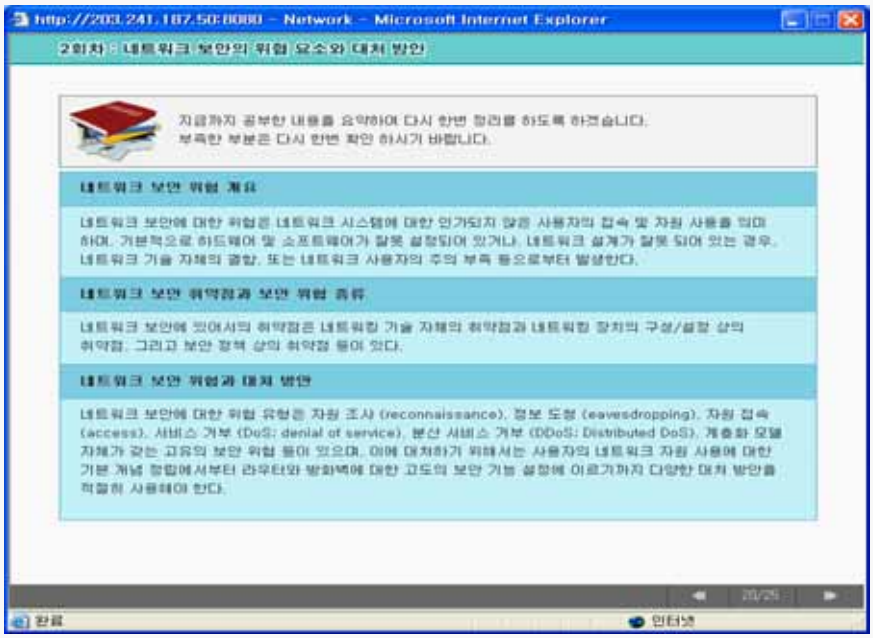

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
자원 접속 (access)
데이터 조작 (Data manipulation)
데이터 조작으로 네트워크 침입자는 통신 채널 상으로 보내진 데이터를 캡쳐하고 조작하고, 재연(rerplay)할 수 있다. 데이터 조작 공격을 수행하기 위해 사용되는 도구로는 프로토콜 분석기, 패스워드 크래커 등이 있다.
세션 재연 (Session replay)
비 인가된 활동을 발생하기 위해 패킷의 순서나 애플리케이션 명령어를 캡쳐하고 조작하고, 재연(replay)하는 것으로 세션 재연 공격에는 Cookies, JavaScript 또는 Active X scripts 등을 사용한다.
자동 루터 (Auto rooter)
자동 루터는 연속적으로 컴퓨터를 스캔/조사/캡쳐하는 전체 해킹 과정을 자동으로 수행하는 프로그램으로서, 네트워크 침입자는 짧은 시간 내에 수백에서 수천 개의 시스템을 스캔할 수 있다.
백 도어 (Back door)
백 도어는 침입이 이루어지는 동안 생성될 수 있는 시스템에의 진입 경로로서, 백 도어는 다른 시스템으로 침입하기 위한 경유지 또는 서비스 부인 공격을 하기 위해 사용될 수 있다.
15/25
완료
인터넷

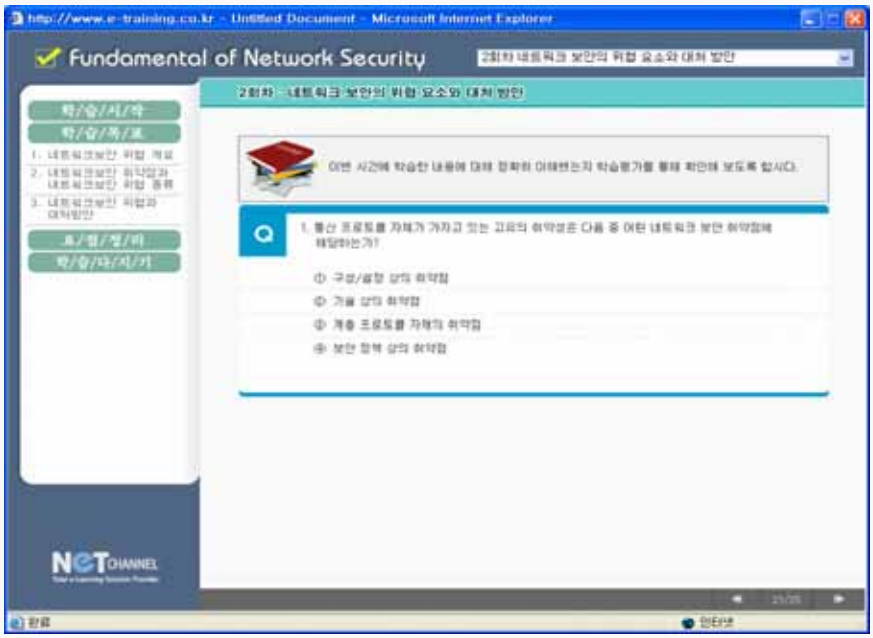

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
서비스 거부 (DoS: Denial of service)
정의
네트워크 자원을 모두 사용하여 고갈시킴으로써 정상적인 인가된 사용자가 네트워크 서비스를 이용하지 못하도록 하는 것을 의미한다.
DoS 공격은 시스템을 손상하거나, 사용할 수 없을 정도로 느리게 하는 것을 포함한다.
CPU
대처 방안
라우터와 방화벽 상에 antispoof 기능과 anti-DoS 기능을 적절히 설정함으로써 DoS 공격을 감소할 수 있다.
네트워크 ISP와 트래픽 률 (traffic rate)를 제한하도록 설정함으로써 DoS 공격을 감소할 수 있다.
DoS 공격 유형은?
DoS 공격에는 여러 가지가 있으며 그 중 ping of death, SYN flood 공격, packet fragmentation과 reassembly, E-mail bombs, CPU hogging, 악의적인 applets 등이 대표적인 DoS 공격 유형이다.
여기서 잠깐!
15/25
완료

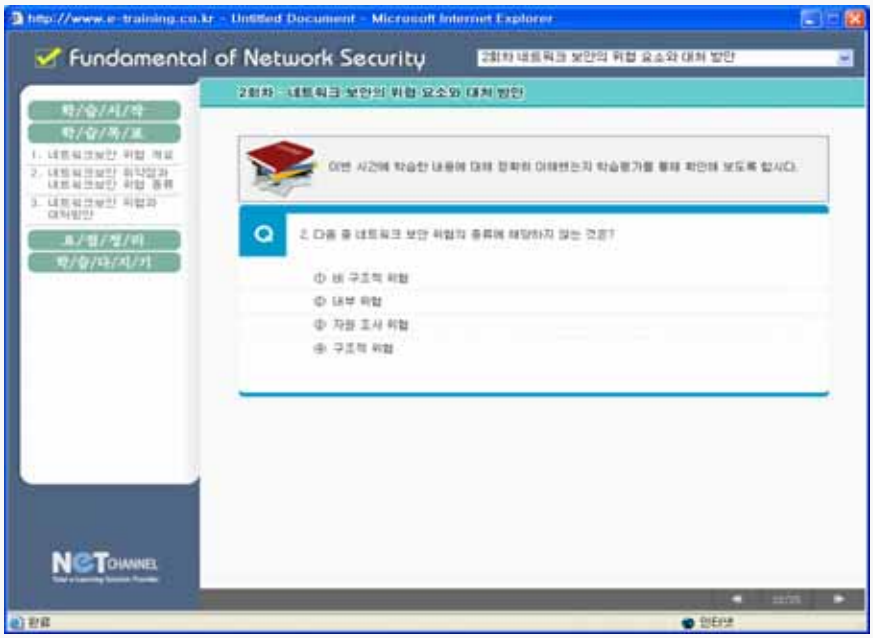

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
분산 서비스 거부 (DDoS: Distributed DoS)
DoS 공격은 비 정상적인 데이터를 수 없이 발생하여 네트워크 링크를 포화상태로 만들으로써 정상적인 트래픽을 드롭시킨다.
DoS 공격은 DoS 공격과 유사하지만 DoS보다 훨씬 큰 규모로 진행되며, 수백 또는 수천의 다른 지점으로부터 하나의 목표를 집중적으로 공격한다.
ICMP REPLY
Attempt to Overwhelm WAN Link to Destination.
172.16.1.2
DDoS 공격 예
DDoS 공격의 대표적인 예로 그림에서와 같이 해커가 spoof된 특정 IP 주소를 이용하여 ICMP echo request를 보내고, 이에 대한 echo reply가 라우터의 특정 인터페이스로 집중되는 Smurf 공격이 있다.
여기서 잠깐!
완료

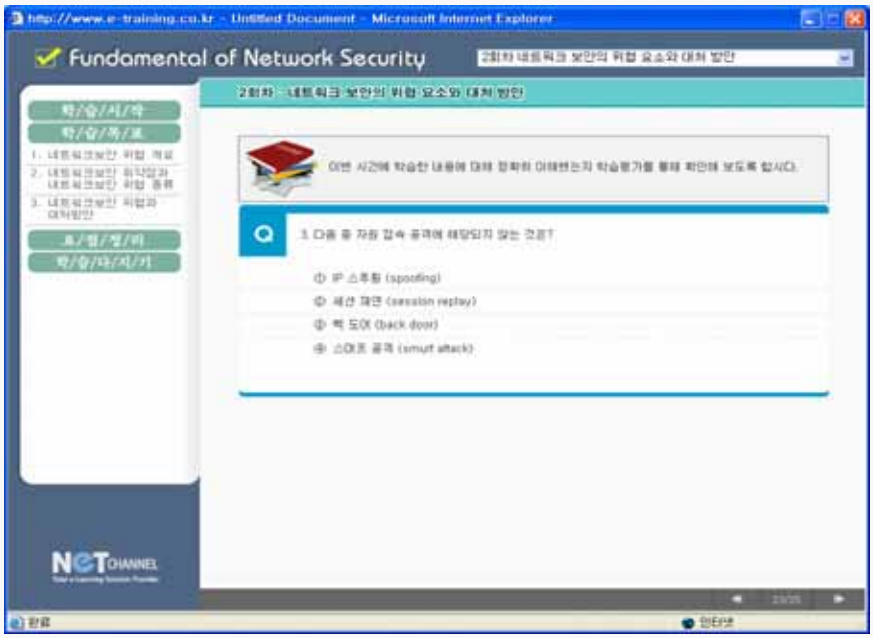

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
계층화 모델 고유의 보안 위협
OSI 참조 모델의 각 계층은 근본적으로 여는 정도의 취약점을 내포하고 있다.
7 Application
6 presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
응용 (application) 계층
Application은 방화벽을 통과하는 port를 사용한다.
예를 들어, 웹 서버가 사용하는 80번 port를 이용하여 공격할 수 있다.
표현 (presentation) 계층
데이터를 보호하기 위해 암호화 기술을 사용하지만 대다수의 일반적인 암호화 기술은 현재 해독될 수 있다.
또한 압축 기술에 의해 압축된 바이러스나 트로이 목마 프로그램들은 대부분의 방화벽을 그대로 통과 할 수 있다.
세션 (session) 계층
NFS, SQL, SMB 그리고 X-windows와 같은 세션 계층에서 수행되는 프로토콜들은 자원에의 비인가 접속을 위해 악용될 수 있다.
완료
인터넷

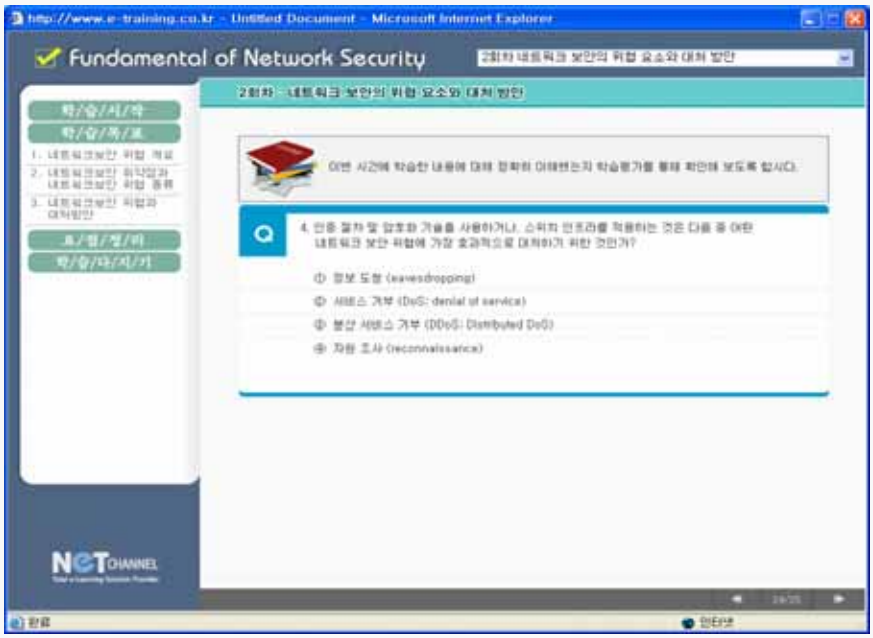

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
네트워크 보안 위협과 대처 방안
계층화 모델 고유의 보안 위협
7 Application
6 presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
전송 (transport) 계층
일부 응용 프로그램과 프로토콜이 well-known TCP/UDP를 사용하기 때문에 특히 취약하며, DoS, spoofing, hijacking, port scan 등의 공격이 수행될 수 있다.
네트워크 (network) 계층
ping scans, sniffing, DoS, ARP poisoning, nuking, ping of death, 그리고 spoofing 등이 악용 될 수 있다. 그리고 분산 서비스 거부 공격에 특히 취약하다.
데이터 링크 (data link) 계층
sniffing, spoofing, broadcast storms 그리고 잘못된 설정이나 고장 난 네트워크 카드 등으로 인한 취약성과 불안전한 VPN의 악용 등의 가능성이 있다.
물리 (physical) 계층
자원 조사 공격과 wire tap에 취약하다.
13/25
완료
인터넷

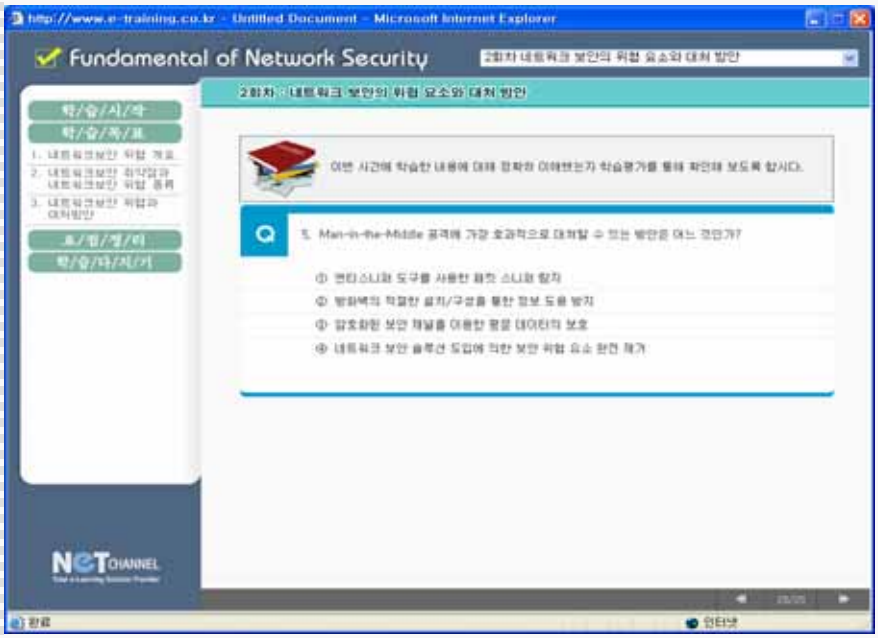

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
2회차 : 네트워크 보안의 위협 요소와 대처 방안
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
네트워크 보안 위협 개요
네트워크 보안에 대한 위협은 네트워크 시스템에 대한 인가되지 않은 사용자의 접속 및 자원 사용을 의미하며, 기본적으로 하드웨어 및 소프트웨어가 잘못 설정되어 있거나, 네트워크 설계가 잘못 되어 있는 경우, 네트워크 기술 자체의 결함, 또는 네트워크 사용자의 주의 부족 등으로부터 발생한다.
네트워크 보안 취약점과 보안 위협 종류
네트워크 보안에 있어서의 취약점은 네트워킹 기술 자체의 취약점과 네트워킹 장치의 구성/설정 상의 취약점, 그리고 보안 정책 상의 취약점 등이 있다.
네트워크 보안 위협과 대처 방안
네트워크 보안에 대한 위협 유형은 자원 조사 (reconnaissance), 정보 도청 (eavesdropping), 자원 접속 (access), 서비스 거부 (DoS: denial of service), 분산 서비스 거부 (DDoS: Distributed DoS), 계층화 모델 자체가 갖는 고유의 보안 위협 등이 있으며, 이에 대처하기 위해서는 사용자의 네트워크 자원 사용에 대한 기본 개념 정립에서부터 라우터와 방화벽에 대한 고도의 보안 기능 설정에 이르기까지 다양한 대처 방안을 적절히 사용해야 한다.
20/25
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
NETCHANNEL


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
NETCHANNEL



End of Lecture