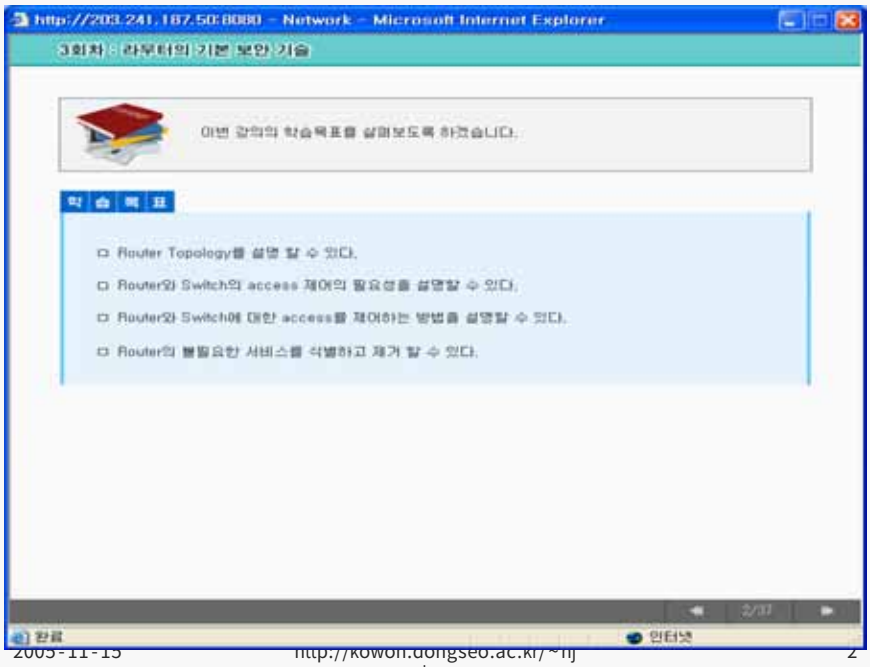
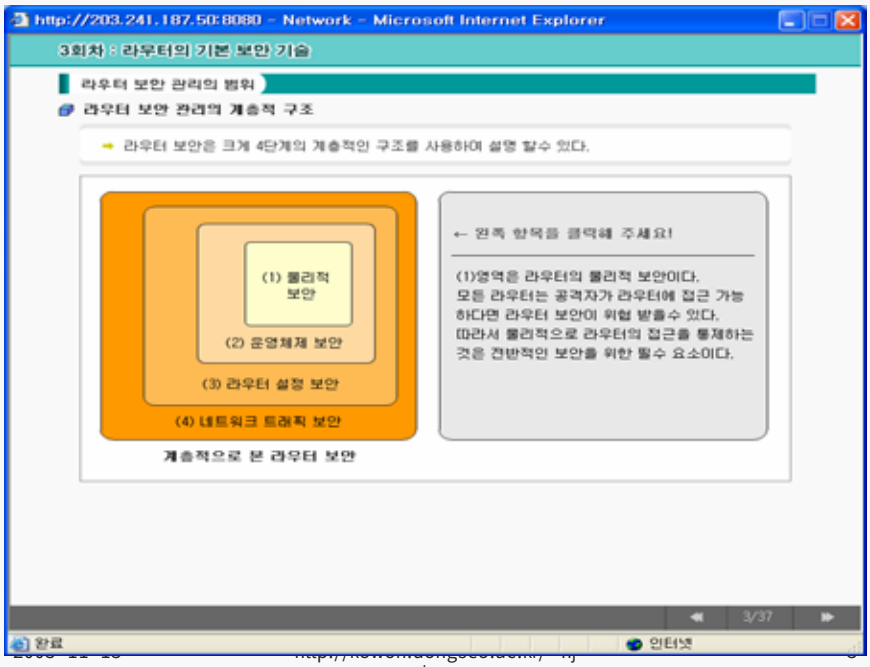
FNS

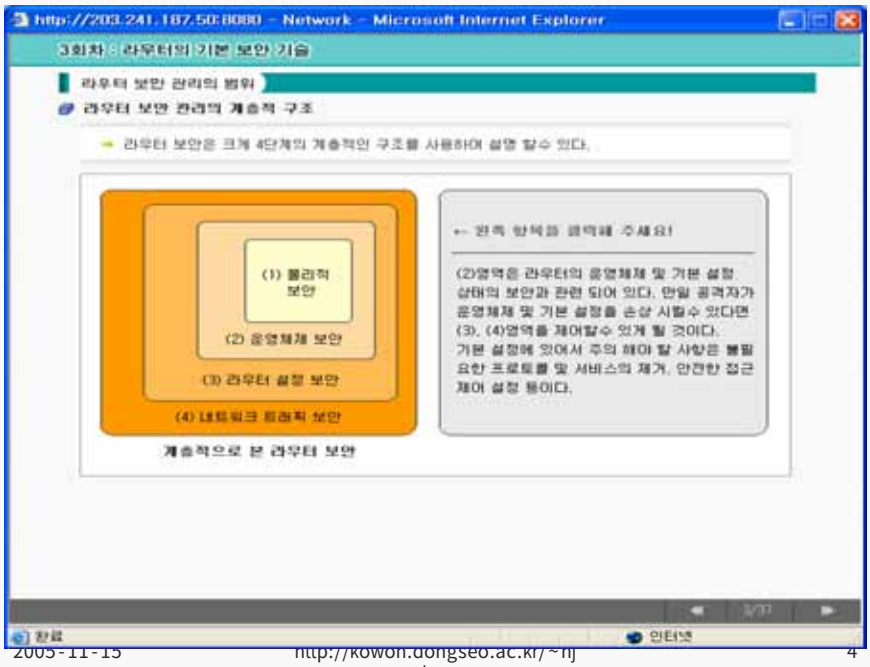
(Fundamental Network Security)

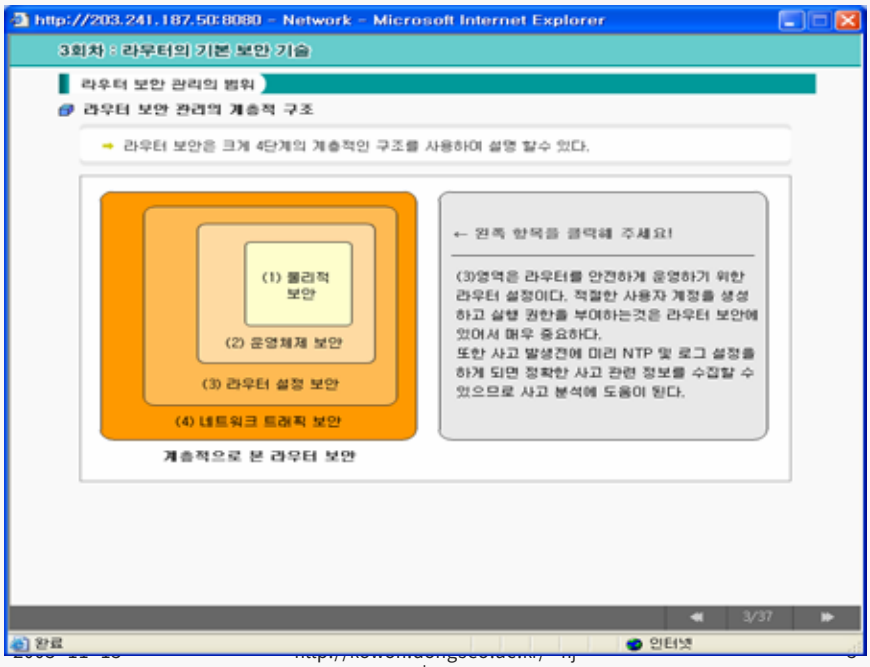
Ch3. 라우터의 기본 보안 기술

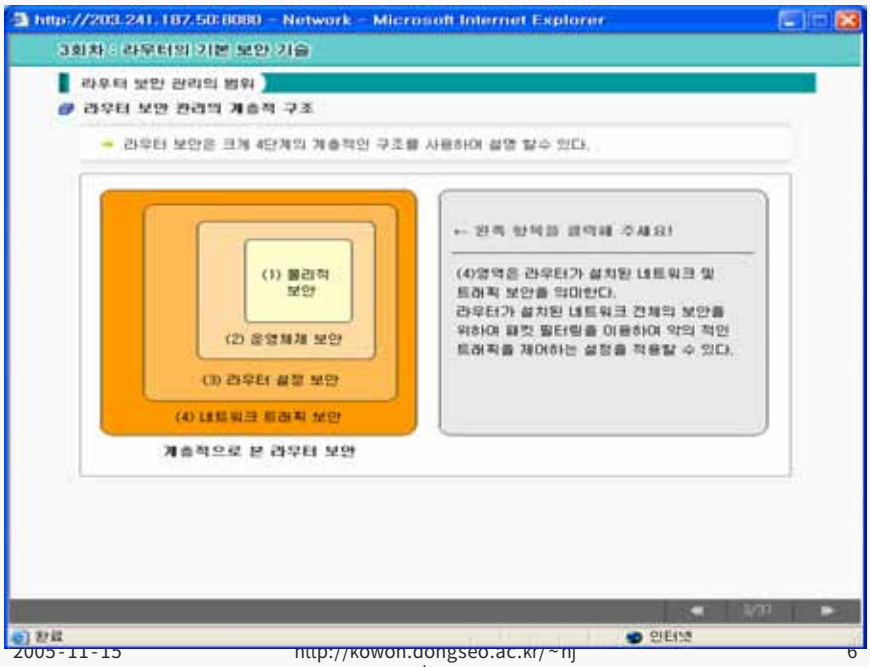
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

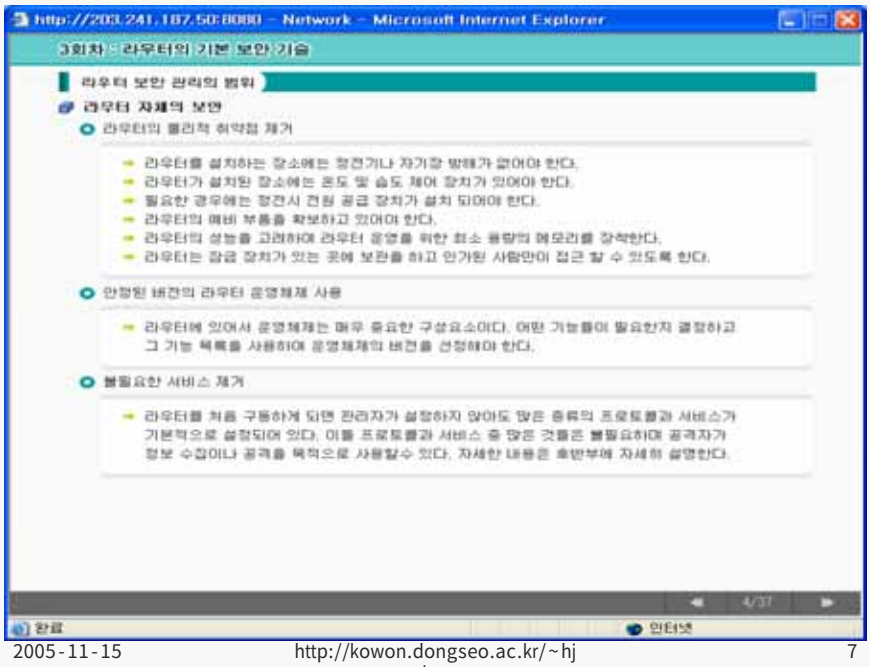


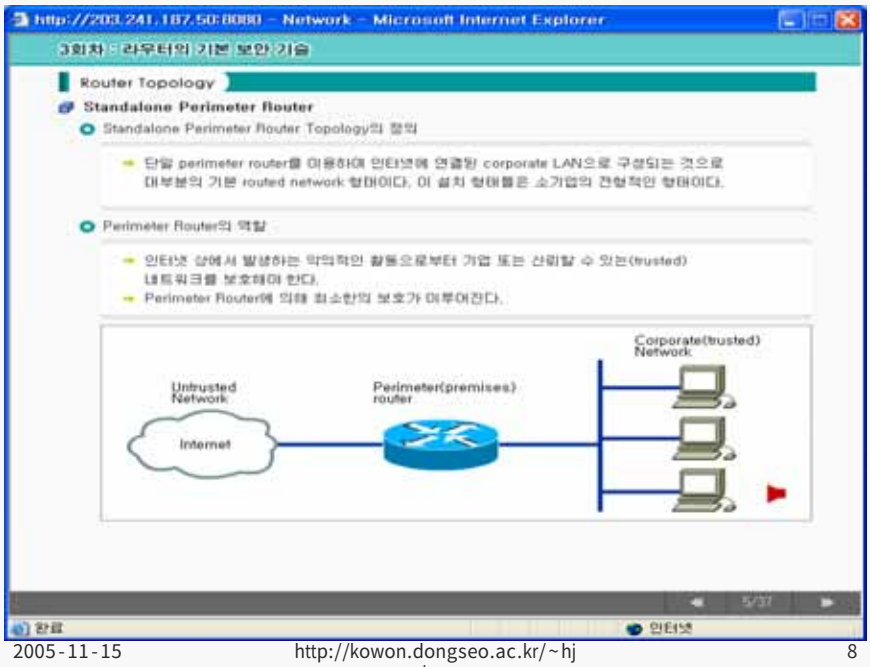

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
라우터 보안 관리의 범위
라우터 보안 관련의 계층적 구조
라우터 보안은 크게 4단계의 계층적인 구조를 사용하여 설명 할수 있다.
(1) 물리적 보안
(2) 운영체제 보안
(3) 라우터 설정 보안
(4) 네트워크 트래픽 보안
계층적으로 본 라우터 보안
← 왼쪽 항목을 클릭해 주세요!
(1)영역은 라우터의 물리적 보안이다.
모든 라우터는 공격자가 라우터에 접근 가능하다면 라우터 보안이 위협 받을수 있다.
따라서 물리적으로 라우터의 접근을 통제하는 것은 전반적인 보안을 위한 필수 요소이다.
3/37
완료
인터넷

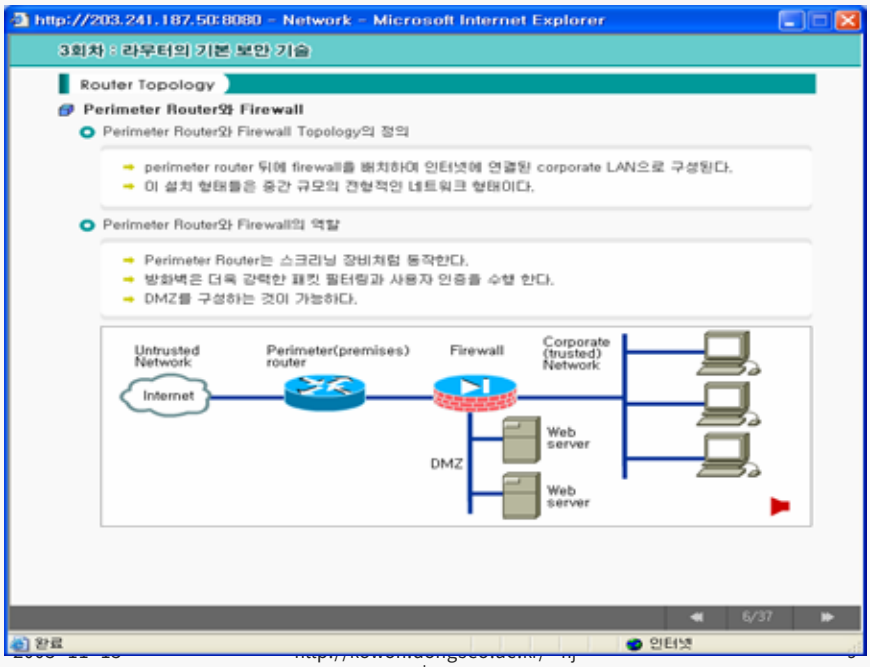

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
라우터 보안 관리의 범위
라우터 보안 관련의 계층적 구조
라우터 보안은 크게 4단계의 계층적인 구조를 사용하여 설명 할수 있다.
(1) 물리적 보안
(2) 운영체제 보안
(3) 라우터 설정 보안
(4) 네트워크 트래픽 보안
계층적으로 본 라우터 보안
← 왼쪽 항목을 클릭해 주세요!
(2)영역은 라우터의 운영체제 및 기본 설정 상태의 보안과 관련 되어 있다. 만일 공격자가 운영체제 및 기본 설정을 손상 시킬수 있다면 (3), (4)영역을 제어할수 없게 될 것이다.
기본 설정에 있어서 주의 해야 할 사항은 불필요한 프로토콜 및 서비스의 제거, 안전한 접근 제어 설정 등이다.
3/37
완료
인터넷

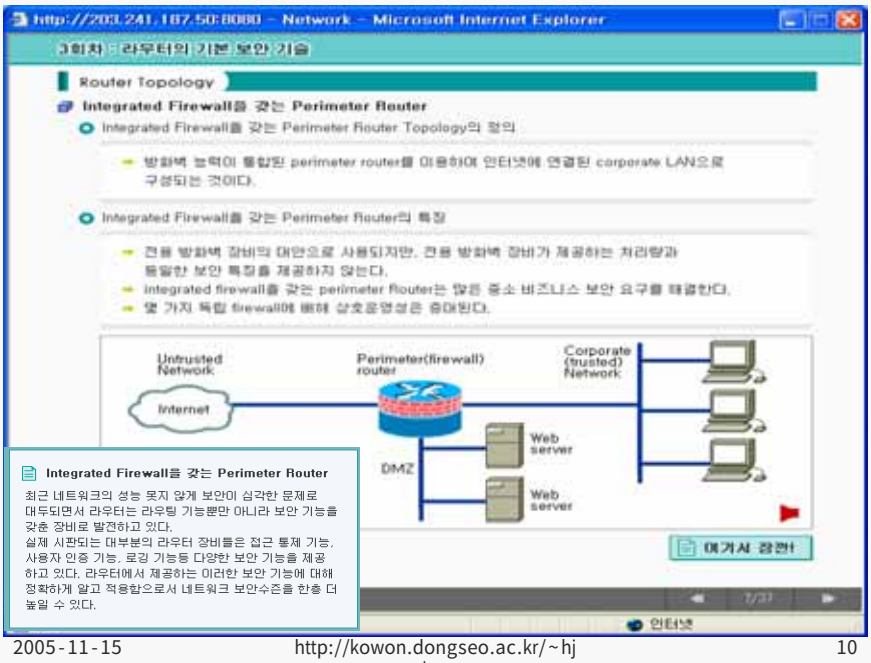

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
라우터 보안 관리의 범위
라우터 보안 관련의 계층적 구조
라우터 보안은 크게 4단계의 계층적인 구조를 사용하여 설명 할수 있다.
(1) 물리적 보안
(2) 운영체제 보안
(3) 라우터 설정 보안
(4) 네트워크 트래픽 보안
계층적으로 본 라우터 보안
← 왼쪽 항목을 클릭해 주세요!
(3)영역은 라우터를 안전하게 운영하기 위한 라우터 설정이다. 적절한 사용자 계정을 생성하고 실행 권한을 부여하는것은 라우터 보안에 있어서 매우 중요하다.
또한 사고 발생건에 미리 NTP 및 로그 설정을 하게 되면 정확한 사고 관련 정보를 수집할 수 있으므로 사고 분석에 도움이 된다.
3/37
완료
인터넷

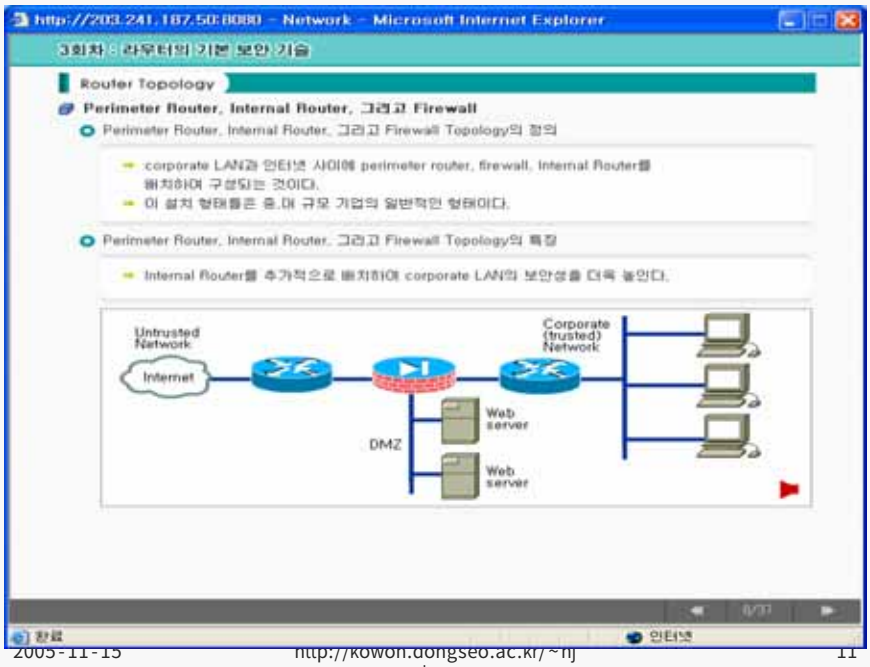

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
라우터 보안 관리의 범위
라우터 보안 관련의 계층적 구조
라우터 보안은 크게 4단계의 계층적인 구조를 사용하여 설명 할수 있다.
(1) 물리적 보안
(2) 운영체제 보안
(3) 라우터 설정 보안
(4) 네트워크 트래픽 보안
계층적으로 본 라우터 보안
← 왼쪽 항목을 클릭해 주세요!
(4)영역은 라우터가 설치된 네트워크 및 트래픽 보안을 의미한다.
라우터가 설치된 네트워크 전체의 보안을 위하여 패킷 필터링을 이용하여 악의 적인 트래픽을 제어하는 설정을 적용할 수 있다.
3/37
완료
인터넷

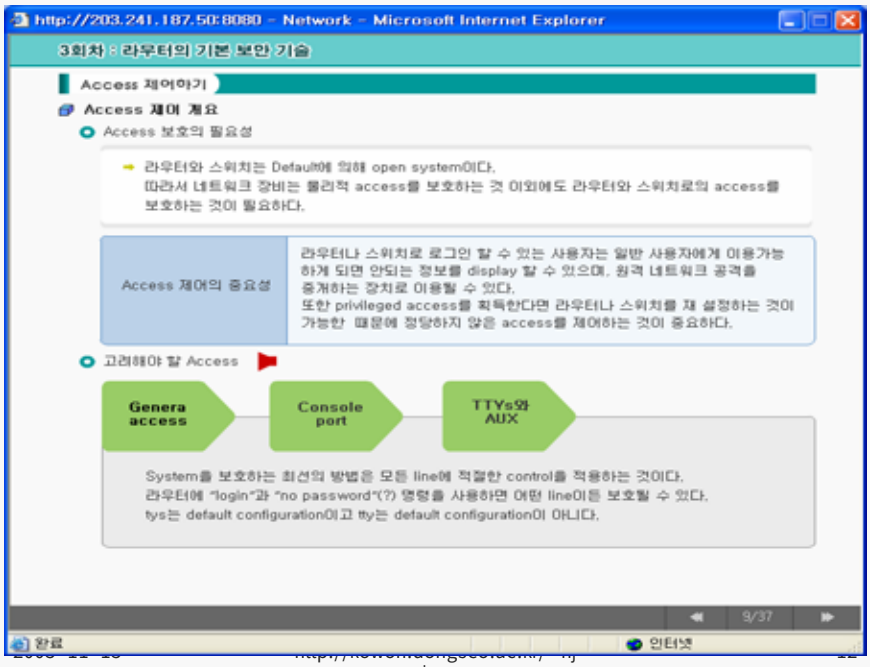

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
라우터 보안 관리의 범위
라우터 자체의 보안
라우터의 물리적 취약점 제거
라우터를 설치하는 장소에는 정전기나 자기장 방해가 없어야 한다.
라우터가 설치된 장소에는 온도 및 습도 제어 장치가 있어야 한다.
필요한 경우에는 정전시 전원 공급 장치가 설치 되어야 한다.
라우터의 예비 부품을 확보하고 있어야 한다.
라우터의 성능을 고려하여 라우터 운영을 위한 최소 용량의 메모리를 장착한다.
라우터는 잠금 장치가 있는 곳에 보관을 하고 인가된 사람만이 접근 할 수 있도록 한다.
안정된 버전의 라우터 운영체제 사용
라우터에 있어서 운영체제는 매우 중요한 구성요소이다. 어떤 기능들이 필요한지 결정하고
그 기능 목록을 사용하여 운영체제의 버전을 선정해야 한다.
불필요한 서비스 제거
라우터를 처음 구동하게 되면 관리자가 설정하지 않아도 많은 종류의 프로토콜과 서비스가
기본적으로 설정되어 있다. 이들 프로토콜과 서비스 중 많은 것들은 불필요하며 공격자가
정보 수집이나 공격을 목적으로 사용할수 있다. 자세한 내용은 후반부에 자세히 설명한다.
4/37
완료
인터넷

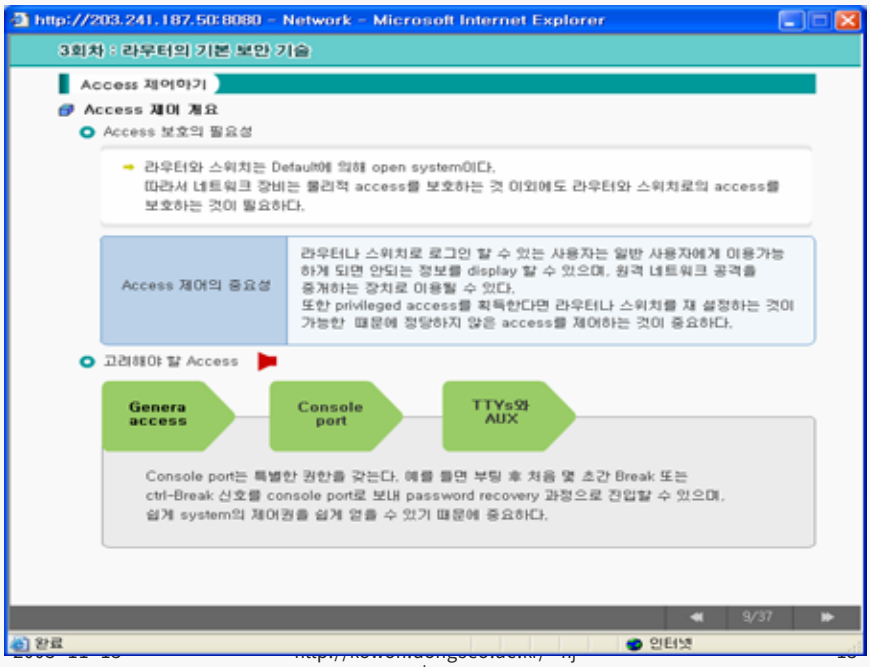

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Router Topology
Standalone Perimeter Router
Standalone Perimeter Router Topology의 장점
단일 perimeter router를 이용하여 인터넷에 연결된 corporate LAN으로 구성되는 것으로
대부분의 기본 routed network 형태이다. 이 설치 형태를 소기업의 전형적인 형태이다.
Perimeter Router의 역할
인터넷 상에서 발생하는 악의적인 활동으로부터 기업 또는 신뢰할 수 있는(trusted)
네트워크를 보호해야 한다.
Perimeter Router에 의해 최소한의 보호가 이루어진다.
Corporate(trusted) Network
Untrusted Network
Perimeter(premises) router
Internet
5/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Router Topology
Perimeter Router와 Firewall
Perimeter Router와 Firewall Topology의 정의
perimeter router 뒤에 firewall를 배치하여 인터넷에 연결된 corporate LAN으로 구성된다.
이 설치 형태를은 중간 규모의 전형적인 네트워크 형태이다.
Perimeter Router와 Firewall의 역할
Perimeter Router는 스크리닝 장비처럼 동작한다.
방화벽은 더욱 강력한 패킷 필터링과 사용자 인증을 수행 한다.
DMZ를 구성하는 것이 가능하다.
Untrusted Network
Internet
Perimeter(premises) router
Firewall
Corporate (trusted) Network
DMZ
Web server
Web server
6/37
완료
인터넷

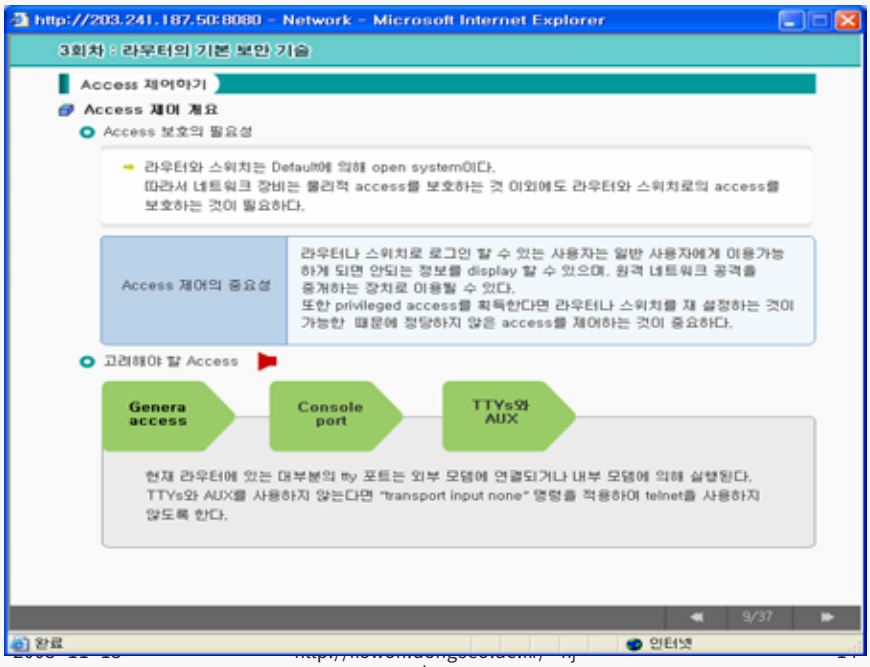

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Router Topology
Integrated Firewall를 갖는 Perimeter Router
Integrated Firewall를 갖는 Perimeter Router Topology의 정의
방화벽 능력이 통합된 perimeter router를 이용하여 인터넷에 연결된 corporate LAN으로 구성되는 것이다.
Integrated Firewall를 갖는 Perimeter Router의 특징
전용 방화벽 장비의 대안으로 사용되지만, 전용 방화벽 장비가 제공하는 처리량과 동일한 보안 특징을 제공하지 않는다.
integrated firewall를 갖는 perimeter Router는 많은 중소 비즈니스 보안 요구를 해결한다.
몇 가지 독립 firewall에 배해 상호운영성은 증대된다.
Untrusted Network
Internet
Perimeter(firewall) router
Corporate (trusted) Network
DMZ
Web server
Web server
여기서 잠깐!
Integrated Firewall를 갖는 Perimeter Router
최근 네트워크의 성능 못지 않게 보안이 심각한 문제로 대두되면서 라우터는 라우팅 기능뿐만 아니라 보안 기능을 갖춘 장비로 발전하고 있다.
실제 시판되는 대부분의 라우터 장비들은 접근 통제 기능, 사용자 인증 기능, 로깅 기능등 다양한 보안 기능을 제공하고 있다. 라우터에서 제공하는 이러한 보안 기능에 대해 정확하게 알고 적용함으로서 네트워크 보안수준을 한층 더 높일 수 있다.
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Router Topology
Perimeter Router, Internal Router, 그리고 Firewall
Perimeter Router, Internal Router, 그리고 Firewall Topology의 정의
corporate LAN과 인터넷 사이에 perimeter router, firewall, Internal Router를 배치하여 구성되는 것이다.
이 설치 형태를 흔 중.대 규모 기업의 일반적인 형태이다.
Perimeter Router, Internal Router, 그리고 Firewall Topology의 특징
Internal Router를 추가적으로 배치하여 corporate LAN의 보안성을 더욱 높인다.
Untrusted Network
Internet
Corporate (trusted) Network
Web server
DMZ
Web server
9/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Access 제어 개요
Access 보호의 필요성
라우터와 스위치는 Default에 의해 open system이다.
따라서 네트워크 장비는 물리적 access를 보호하는 것 이외에도 라우터와 스위치로의 access를 보호하는 것이 필요하다.
Access 제어의 중요성
라우터나 스위치로 로그인 할 수 있는 사용자는 일반 사용자에게 이용가능하게 되면 안되는 정보를 display 할 수 있으며, 원격 네트워크 공격을 중계하는 장치로 이용될 수 있다.
또한 privileged access를 획득한다면 라우터나 스위치를 재 설정하는 것이 가능한 때문에 정당하지 않은 access를 제어하는 것이 중요하다.
고려해야 할 Access
Genera access
Console port
TTYs와 AUX
System을 보호하는 최선의 방법은 모든 line에 적절한 control을 적용하는 것이다.
라우터에 "login"과 "no password"(?) 명령을 사용하면 어떤 line이든 보호될 수 있다.
tys는 default configuration이고 tty는 default configuration이 아니다.
9/37
완료
인터넷

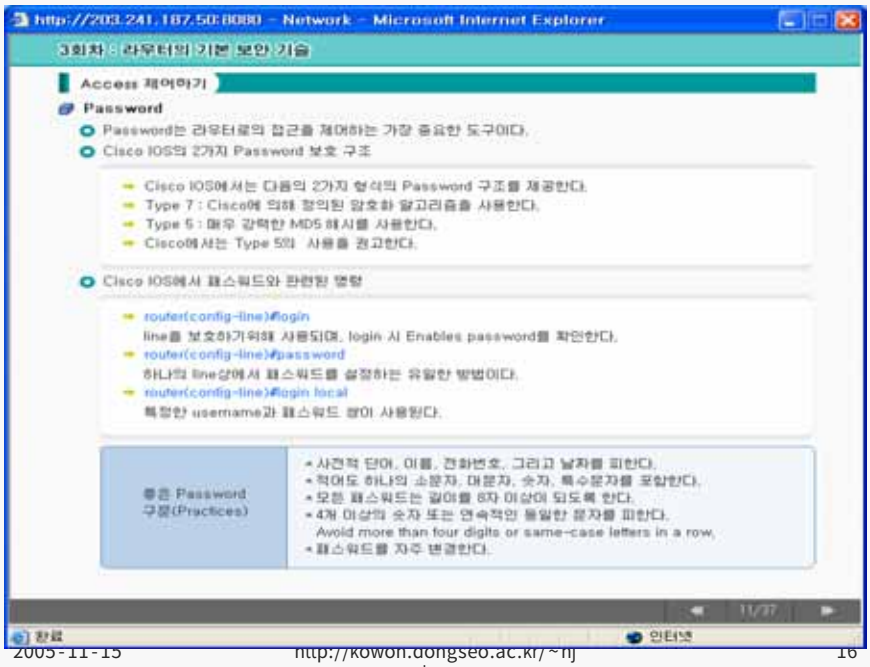

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Access 제어 개요
Access 보호의 필요성
라우터와 스위치는 Default에 의해 open system이다.
따라서 네트워크 장비는 물리적 access를 보호하는 것 이외에도 라우터와 스위치로의 access를 보호하는 것이 필요하다.
Access 제어의 중요성
라우터나 스위치로 로그인 할 수 있는 사용자는 일반 사용자에게 이용가능하게 되면 안되는 정보를 display 할 수 있으며, 원격 네트워크 공격을 중계하는 장치로 이용될 수 있다.
또한 privileged access를 획득한다면 라우터나 스위치를 재 설정하는 것이 가능한 때문에 정당하지 않은 access를 제어하는 것이 중요하다.
고려해야 할 Access
Genera access
Console port
TTYs와 AUX
Console port는 특별한 권한을 갖는다. 예를 들면 부팅 후 처음 몇 초간 Break 또는 ctrl-Break 신호를 console port로 보내 password recovery 과정으로 진입할 수 있으며, 쉽게 system의 제어권을 쉽게 얻을 수 있기 때문에 중요하다.
9/37
완료
인터넷

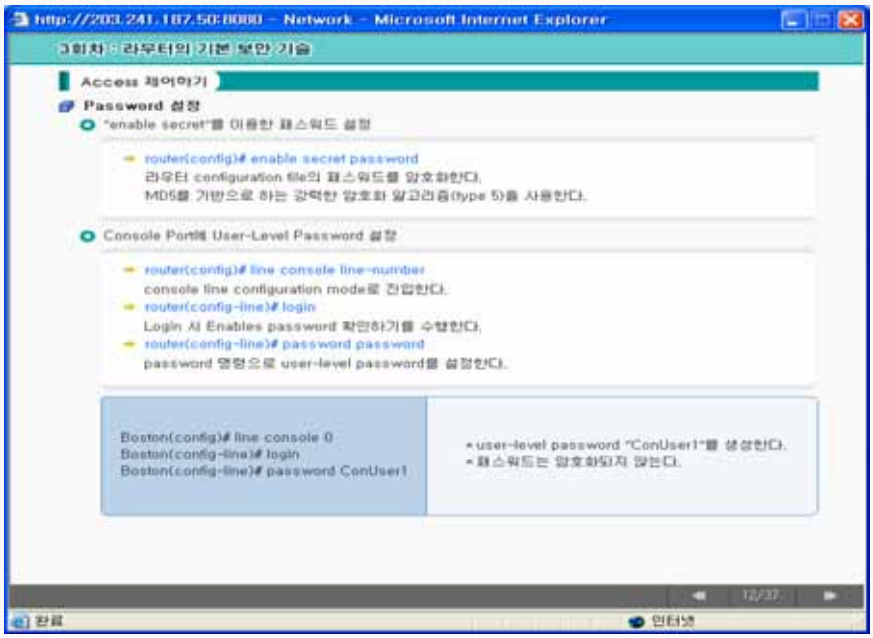
lee

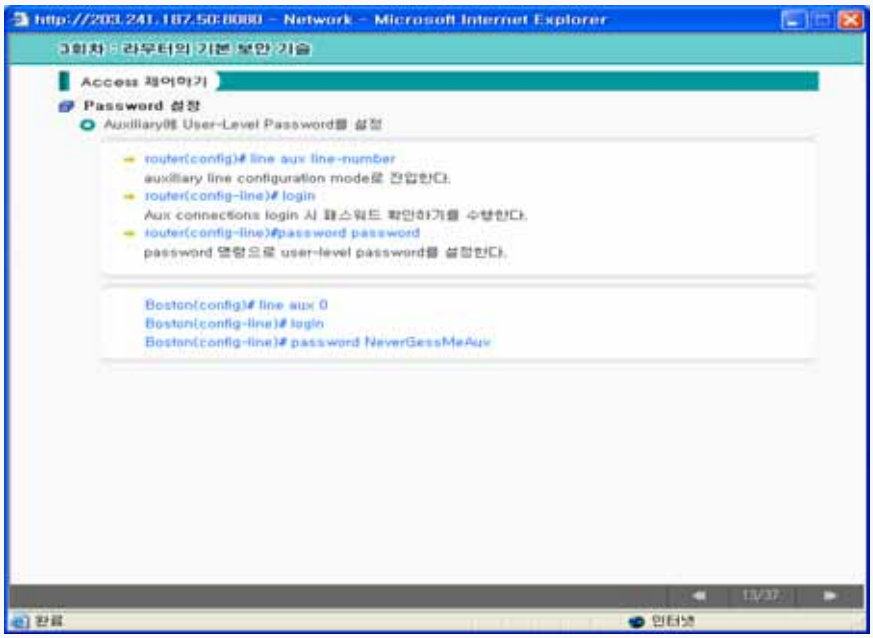

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Access 제어 개요
Access 보호의 필요성
라우터와 스위치는 Default에 의해 open system이다.
따라서 네트워크 장비는 물리적 access를 보호하는 것 이외에도 라우터와 스위치로의 access를 보호하는 것이 필요하다.
Access 제어의 중요성
라우터나 스위치로 로그인 할 수 있는 사용자는 일반 사용자에게 이용가능하게 되면 안되는 정보를 display 할 수 있으며, 원격 네트워크 공격을 중계하는 장치로 이용될 수 있다.
또한 privileged access를 획득한다면 라우터나 스위치를 재 설정하는 것이 가능한 때문에 정당하지 않은 access를 제어하는 것이 중요하다.
고려해야 할 Access
Genera access
Console port
TTYs와 AUX
현재 라우터에 있는 대부분의 tty 포트는 외부 모뎀에 연결되거나 내부 모뎀에 의해 실행된다. TTYs와 AUX를 사용하지 않는다면 "transport input none" 명령을 적용하여 telnet를 사용하지 않도록 한다.
9/37
완료
인터넷

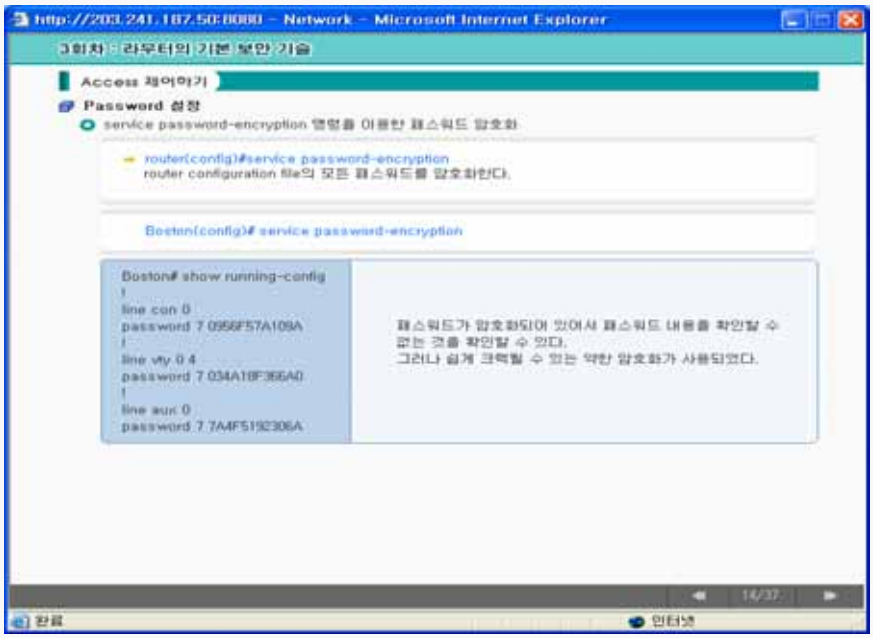
lee

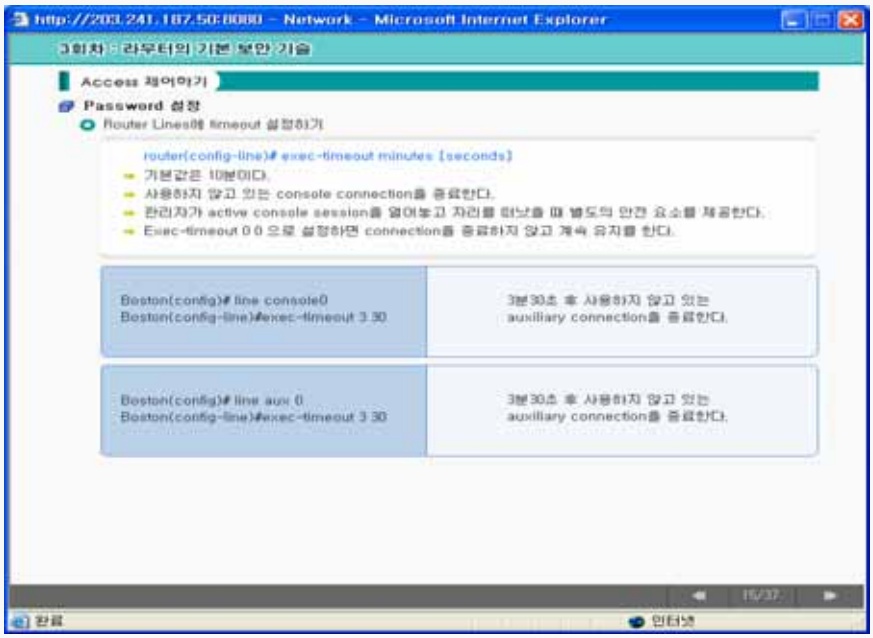

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Access 제어 개요
VTYs 제어하기
라우터에 모든 non-IP 기반 원격접속 프로토콜의 기능을 제거한다.
모든 원격접속에 대해 SSH, SSL 또는 Ipsec 암호화를 사용한다.
관련 명령
router(config-line)#transport input all
모든 session을 허용한다.
router(config-line)#transport input telnet
Telnet session만을 위한 vty를 설정한다.
router(config-line)#transport input telnet ssh
Telnet과 SSH session을 허용하는 vty를 설정한다.
router(config-line)# ip access-class in
vty가 연결을 수락하는 IP 주소를 제한한다.
10/37
완료
인터넷

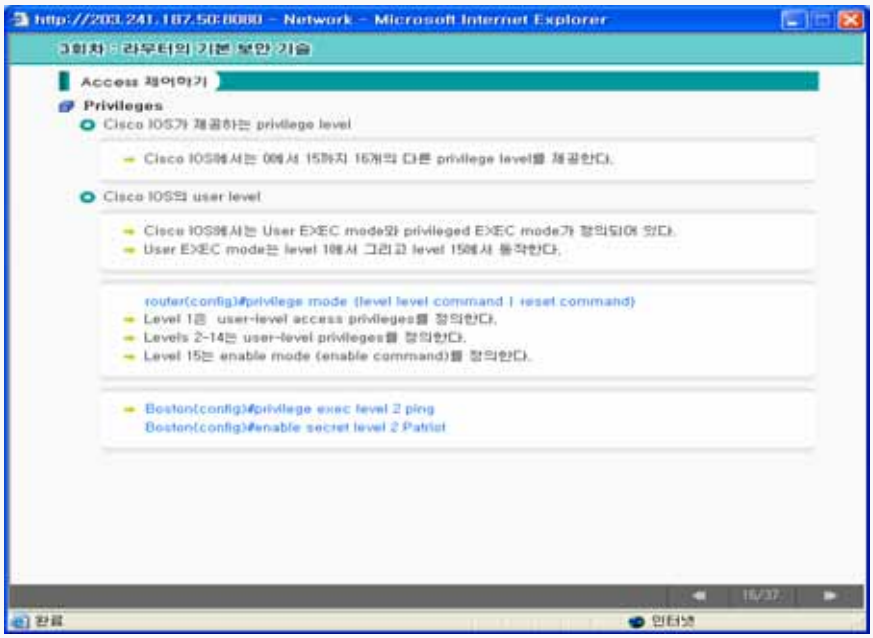

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Password
Password는 라우터로의 접근을 제어하는 가장 중요한 도구이다.
Cisco IOS의 2가지 Password 보호 구조
Cisco IOS에서는 다음의 2가지 형식의 Password 구조를 제공한다.
Type 7 : Cisco에 의해 정의된 암호화 알고리즘을 사용한다.
Type 5 : 매우 강력한 MD5 해시를 사용한다.
Cisco에서는 Type 5의 사용을 권고한다.
Cisco IOS에서 패스워드와 관련된 명령
router(config-line)#login
line을 보호하기위해 사용되며, login 시 Enables password를 확인한다.
router(config-line)#password
하나의 line상에서 패스워드를 설정하는 유일한 방법이다.
router(config-line)#login local
특정한 username과 패스워드 쌍이 사용된다.
좋은 Password 구문(Practices)
사전적 단어, 이름, 전화번호, 그리고 날짜를 피한다.
적어도 하나의 소문자, 대문자, 숫자, 특수문자를 포함한다.
모든 패스워드는 길이를 8자 이상이 되도록 한다.
4개 이상의 숫자 또는 연속적인 동일한 문자를 피한다.
Avoid more than four digits or same-case letters in a row.
패스워드를 자주 변경한다.
11/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Password 설정
"enable secret"를 이용한 패스워드 설정
router(config)# enable secret password
라우터 configuration file의 패스워드를 암호화한다.
MD5를 기반으로 하는 강력한 암호화 알고리즘(type 5)을 사용한다.
Console Port에 User-Level Password 설정
router(config)# line console line-number
console line configuration mode로 진입한다.
router(config-line)# login
Login 시 Enables password 확인하기를 수행한다.
router(config-line)# password password
password 명령으로 user-level password를 설정한다.
Boston(config)# line console 0
Boston(config-line)# login
Boston(config-line)# password ConUser1
• user-level password "ConUser1"를 생성한다.
• 패스워드는 암호화되지 않는다.
12/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Password 설정
Auxiliary에 User-Level Password를 설정
router(config)# line aux line-number
auxiliary line configuration mode로 진입한다.
router(config-line)# login
Aux connections login 시 패스워드 확인하기를 수행한다.
router(config-line)#password password
password 명령으로 user-level password를 설정한다.
Boston(config)# line aux 0
Boston(config-line)# login
Boston(config-line)# password NeverGessMeAux
13/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Password 설정
service password-encryption 명령을 이용한 패스워드 암호화
router(config)#service password-encryption
router configuration file의 모든 패스워드를 암호화한다.
Boston(config)# service password-encryption
Boston# show running-config
!
line con 0
password 7 0956F57A109A
!
line vty 0 4
password 7 034A1F366A0
!
line aux 0
password 7 7A4F5192306A
패스워드가 암호화되어 있어서 패스워드 내용을 확인할 수 없는 것을 확인할 수 있다.
그러나 쉽게 크랙될 수 있는 약한 암호화가 사용되었다.
14/37
완료
인터넷

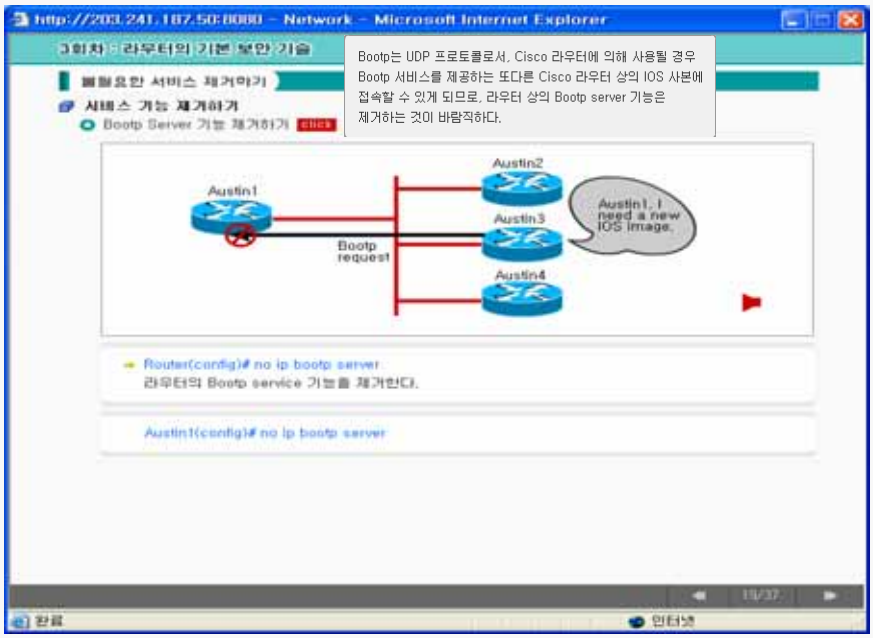

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Password 설정
Router Lines에 timeout 설정하기
router(config-line)# exec-timeout minutes [seconds]
기본값은 10분이다.
사용하지 않고 있는 console connection을 종료한다.
관리자가 active console session을 열어놓고 자리를 비웠을 때 보안의 안전 요소를 제공한다.
Exec-timeout 0 0 으로 설정하면 connection을 종료하지 않고 계속 유지를 한다.
Boston(config)# line console0
Boston(config-line)#exec-timeout 3 30
3분30초 후 사용하지 않고 있는 auxiliary connection을 종료한다.
Boston(config)# line aux 0
Boston(config-line)#exec-timeout 3 30
3분30초 후 사용하지 않고 있는 auxiliary connection을 종료한다.
15/37
완료
인터넷

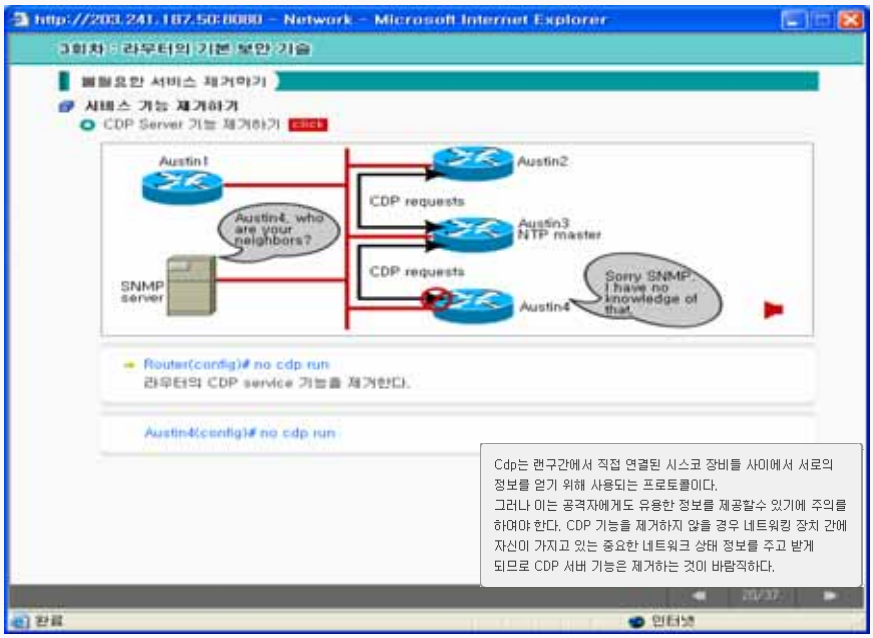

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Privileges
Cisco IOS가 제공하는 privilege level
Cisco IOS에서는 0에서 15까지 16개의 다른 privilege level을 제공한다.
Cisco IOS의 user level
Cisco IOS에서는 User EXEC mode와 privileged EXEC mode가 정의되어 있다.
User EXEC mode는 level 1에서 그리고 level 15에서 동작한다.
router(config)#privilege mode {level level command | reset command}
Level 1은 user-level access privileges를 정의한다.
Levels 2-14는 user-level privileges를 정의한다.
Level 15는 enable mode (enable command)를 정의한다.
Boston(config)#privilege exec level 2 ping
Boston(config)#enable secret level 2 Patriot
16/37
완료
인터넷

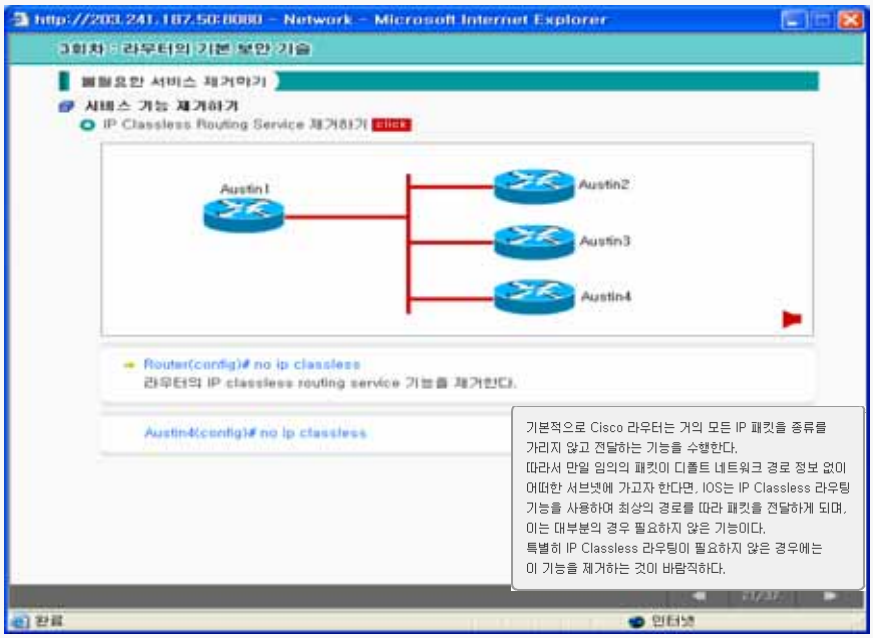

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Banner
Banner의 필요성
Banner는 사용자들에게 메시지를 전달하기 위해 사용된다.
사용자들에게 보안 경고 메시지를 제공하기 위해 모든 네트워크장비에서 이용되어야 한다.
Banner에 포함되어야 할 내용
Banner에 포함되지 않아야 할 내용
누가 사용할 권한이 부여되어야 하는지에 대한 정보와 시스템이 오직 인증된 구성원에 의해서만 접속되고 로그인 된다는 통지
시스템의 비 인가된 사용자는 불법이고 민형사상 처벌의 대상이 될 수 있다는 통지
어떠한 시스템의 사용은 추가적인 통보 없이 기록되고 감사될 수 있다는 것과 기록의 결과물은 법정에서 증거로 사용될 수 있다는 통지
특정한 지방 법률에 의해 요구되는 구체적인 통지
Banner 메시지 설정하기
router(config)# banner {exec | incoming | login | motd | slip-ppp} d message d
Boston(config)# banner motd #
WARNING: You are connected to $(hostname) on the Cisco Systems, Incorporated network.
Unauthorized access and use of this network will be vigorously prosecuted. #
Banner 설정 시 고려 사항
시스템의 적합한 사용이 무엇인지를 명시한다.
시스템이 감시되고 있다는 명시한다.
이 시스템을 사용할 때 privacy가 보호되지 않을 수 있다는 것을 명시한다.
"welcome" 단어를 사용하지 않는다.
메시지의 내용에 대하여 법률적 검토를 한다.
17/37
완료
인터넷

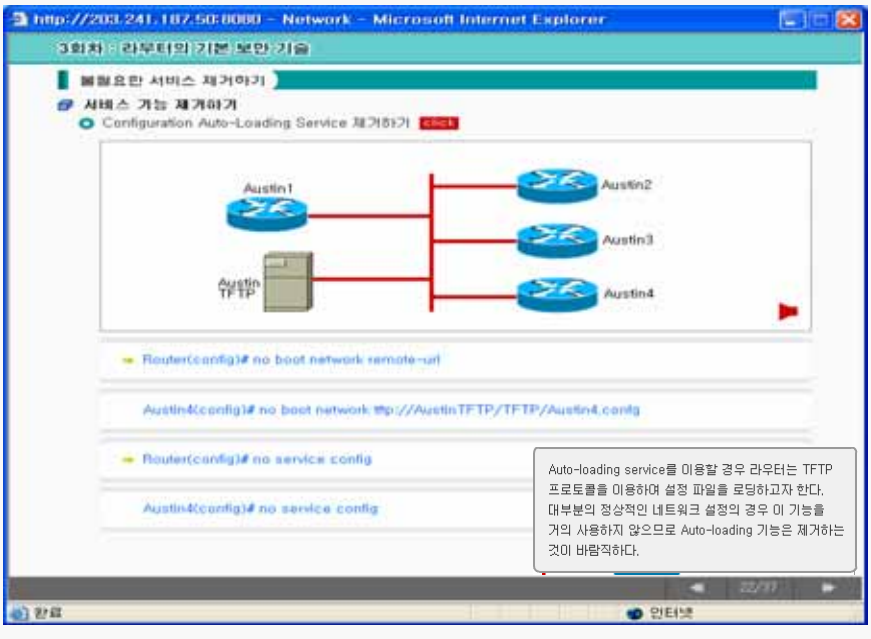

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
Access 제어하기
Banner
Banner의 필요성
Banner는 사용자들에게 메시지를 전달하기 위해 사용된다.
사용자들에게 보안 경고 메시지를 제공하기 위해 모든 네트워크장비에서 이용되어야 한다.
Banner에 포함되어야 할 내용
Banner에 포함되지 않아야 할 내용
login banner는 일반적으로 라우터에 대한 이름, 모델명, 수행되고 있는 소프트웨어 또는 소유자 등 구체적인 정보를 포함하지 않아야 한다.
Banner 메시지 설정하기
router(config)# banner {exec | incoming | login | motd | slip-ppp} d message d
Boston(config)# banner motd #
WARNING: You are connected to $(hostname) on the Cisco Systems, Incorporated network.
Unauthorized access and use of this network will be vigorously prosecuted. #
Banner 설정 시 고려 사항
시스템의 적합한 사용이 무엇인지를 명시한다.
시스템이 감시되고 있다는 명시한다.
이 시스템을 사용할 때 privacy가 보호되지 않을 수 있다는 것을 명시한다.
"welcome" 단어를 사용하지 않는다.
메시지의 내용에 대하여 법률적 검토를 한다.
12/37
완료
인터넷

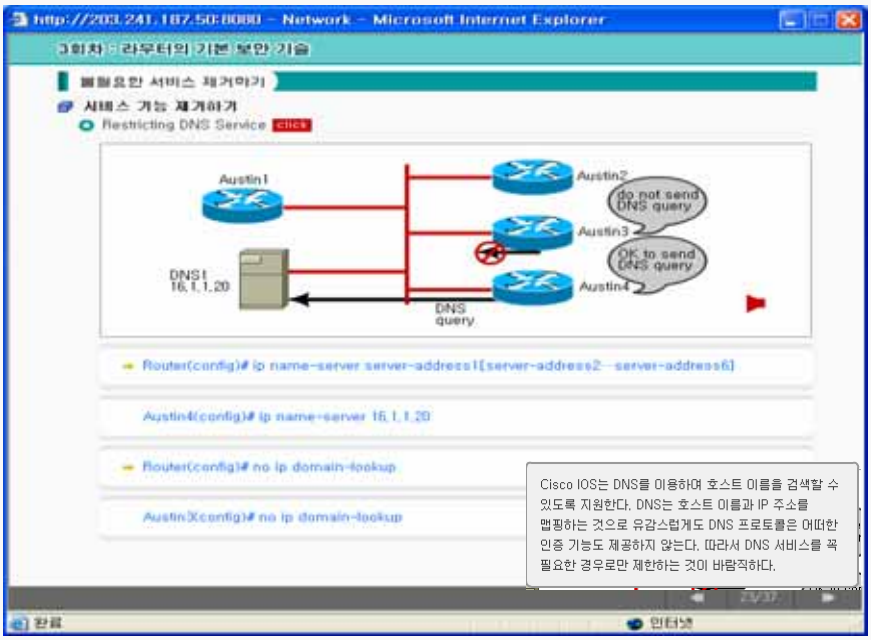

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
네트워크 서비스와 보안
IOS 네트워크 서비스
Cisco 라우터는 많은 수의 네트워크 서비스를 제공한다.
이들 서비스 중 몇몇은 보안에 악영향을 미칠 수 있기 때문에 필요하지 않은 서비스는 turn-off 하거나 disable로 설정하는 것이 필요하다.
보안에 위협이 될 수 있는 서비스의 예
Bootp server
Cisco Discovery Protocol (CDP)
Classless Routing Behavior
Configuration auto-loading
DNS
Finger
HTTP server
IP directed broadcast
IP mask reply
IP redirects
IP source routing
IP unreachable notifications
NTP service
Proxy ARP
SNMP
TCP small servers
UDP small servers
라우터에 대한 일반적인 보안 관례
오직 네트워크가 필요한 트래픽과 프로토콜만 지원하는 것이다.
Cisco 라우터는 제 2, 3, 4, 7 계층에서 여러 가지 네트워크 서비스를 제공한다. 이 중 일부는 사용자와 호스트로 하여금 라우터에 접속할 수 있도록 허용하는 응용 계층 프로토콜이다. 그리고 나머지 서비스들은 특정 라우터 설정 (configuration)을 지원할 수 있도록 되어 있는 자동 프로세스인데 이러한 사항은 네트워크 보안에 이롭지 않다. 따라서 이들 서비스 중 라우터의 동작에 영향을 미치지 않으면서도 보안 수준을 높일 수 있는 서비스들을 제거하는 것이 바람직하다.
16/37
완료
인터넷

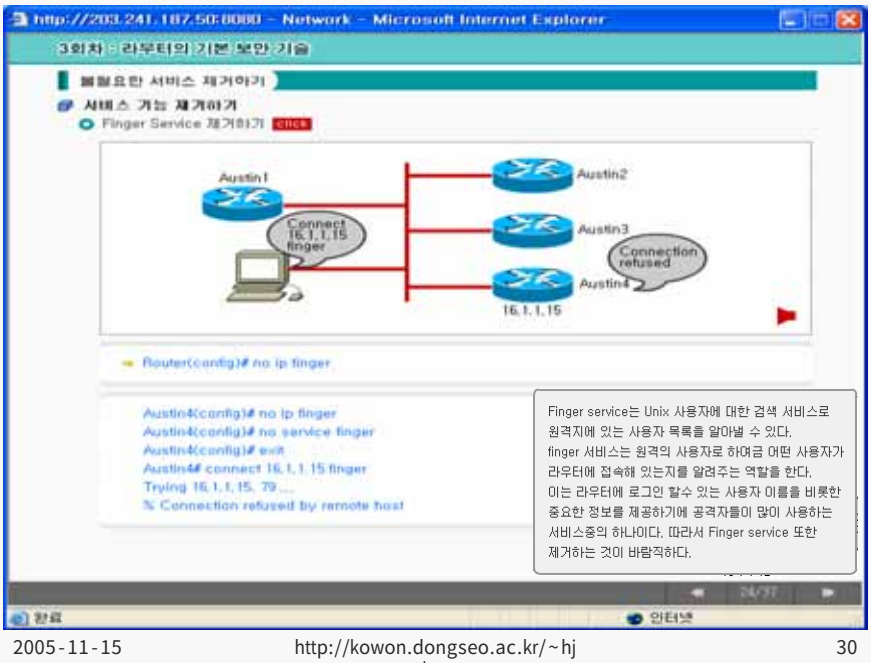

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
Bootp Server 기능 제거하기 click
Bootp는 UDP 프로토콜로서, Cisco 라우터에 의해 사용될 경우 Bootp 서비스를 제공하는 또다른 Cisco 라우터 상의 IOS 사본에 접속할 수 있게 되므로, 라우터 상의 Bootp server 기능은 제거하는 것이 바람직하다.
Austin1
Austin2
Austin3
Austin4
Bootp request
Austin1, I need a new IOS image.
Router(config)# no ip bootp server
라우터의 Bootp service 기능을 제거한다.
Austin1(config)# no ip bootp server
완료
인터넷

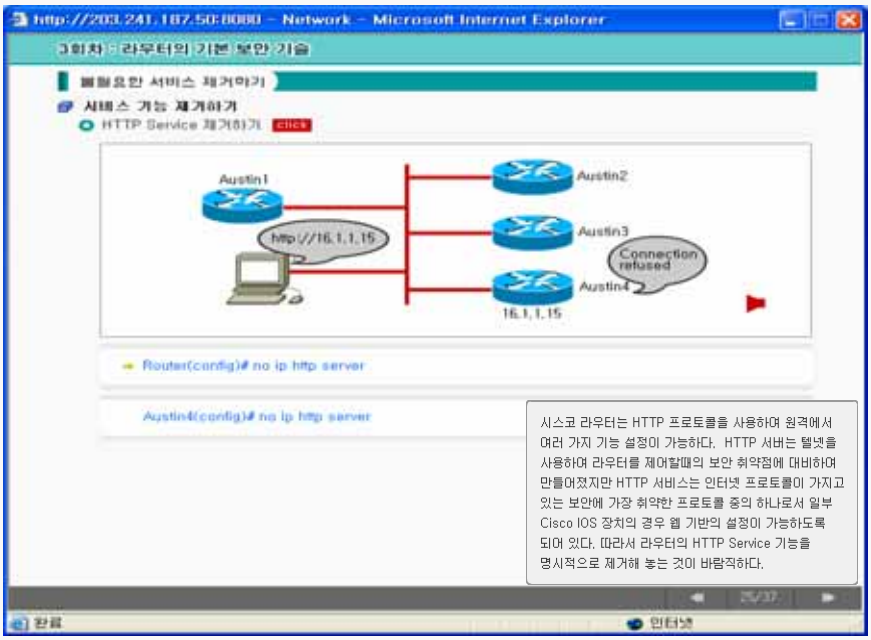

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
CDP Server 기능 제거하기 click
Austin1
Austin2
Austin3
Austin4
CDP requests
Austin4, who are your neighbors?
NTP master
SNMP server
Sorry SNMP, I have no knowledge of that.
Router(config)# no cdp run
라우터의 CDP service 기능을 제거한다.
Austin4(config)# no cdp run
Cdp는 랜구간에서 직접 연결된 시스코 장비들 사이에서 서로의 정보를 얻기 위해 사용되는 프로토콜이다.
그러나 이는 공격자에게도 유용한 정보를 제공할수 있기에 주의를 하여야 한다. CDP 기능을 제거하지 않을 경우 네트워킹 장치 간에 자신이 가지고 있는 중요한 네트워크 상태 정보를 주고 받게 되므로 CDP 서버 기능은 제거하는 것이 바람직하다.
완료
인터넷

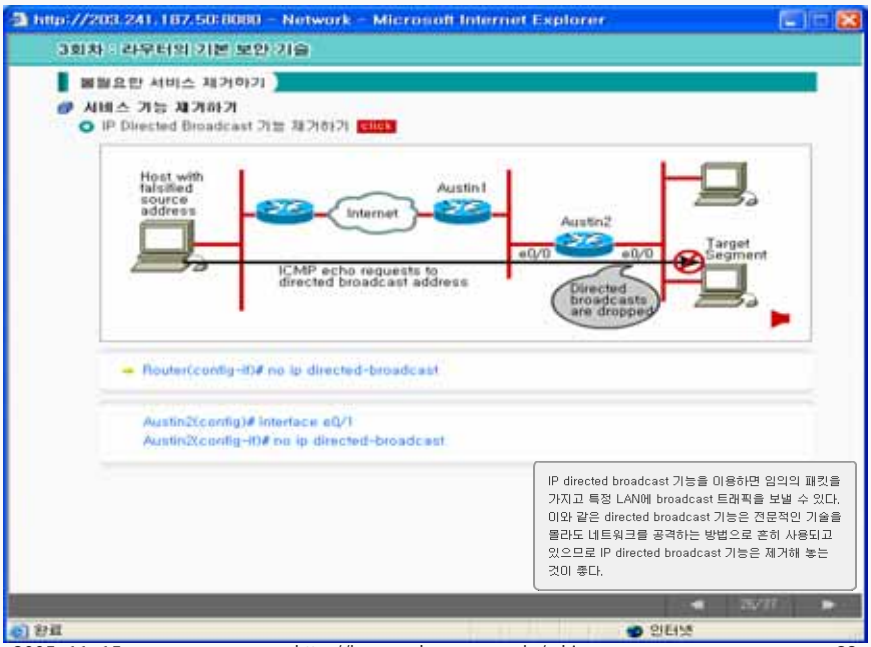

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
IP Classless Routing Service 제거하기
Austin1
Austin2
Austin3
Austin4
Router(config)# no ip classless
라우터의 IP classless routing service 기능을 제거한다.
Austin4(config)# no ip classless
기본적으로 Cisco 라우터는 거의 모든 IP 패킷을 종류를 가리지 않고 전달하는 기능을 수행한다.
따라서 만일 임의의 패킷이 디폴트 네트워크 경로 정보 없이 어떠한 서브넷에 가고자 한다면, IOS는 IP Classless 라우팅 기능을 사용하여 최상의 경로를 따라 패킷을 전달하게 되며, 이는 대부분의 경우 필요하지 않은 기능이다.
특별히 IP Classless 라우팅이 필요하지 않은 경우에는 이 기능을 제거하는 것이 바람직하다.
완료
인터넷

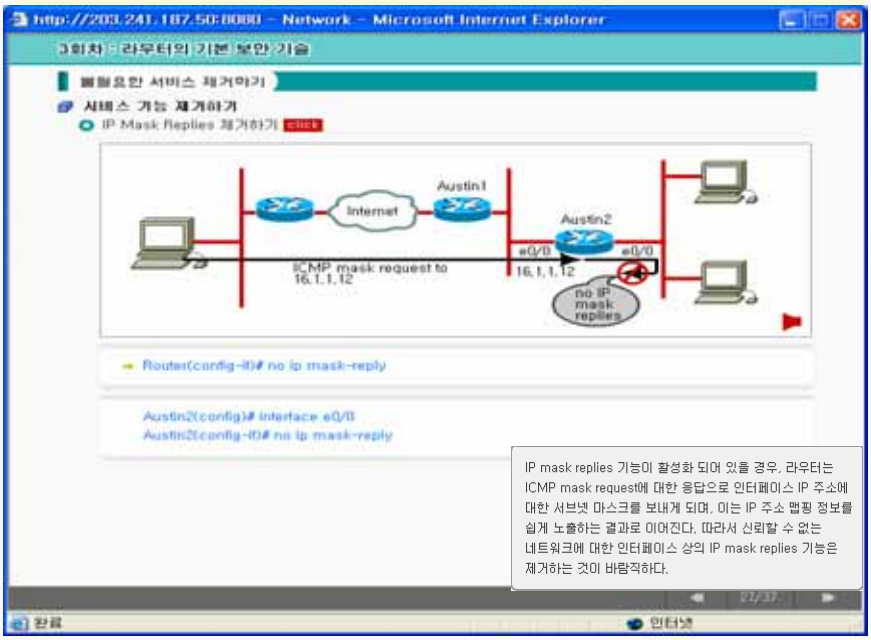

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
Configuration Auto-Loading Service 제거하기
Austin1
Austin2
Austin3
Austin4
Austin TFTP
Router(config)# no boot network remote-url
Austin4(config)# no boot network ftp://AustinTFTP/TFTP/Austin4.config
Router(config)# no service config
Austin4(config)# no service config
Auto-loading service를 이용할 경우 라우터는 TFTP 프로토콜을 이용하여 설정 파일을 로딩하고자 한다.
대부분의 정상적인 네트워크 설정의 경우 이 기능을 거의 사용하지 않으므로 Auto-loading 기능은 제거하는 것이 바람직하다.
완료
인터넷

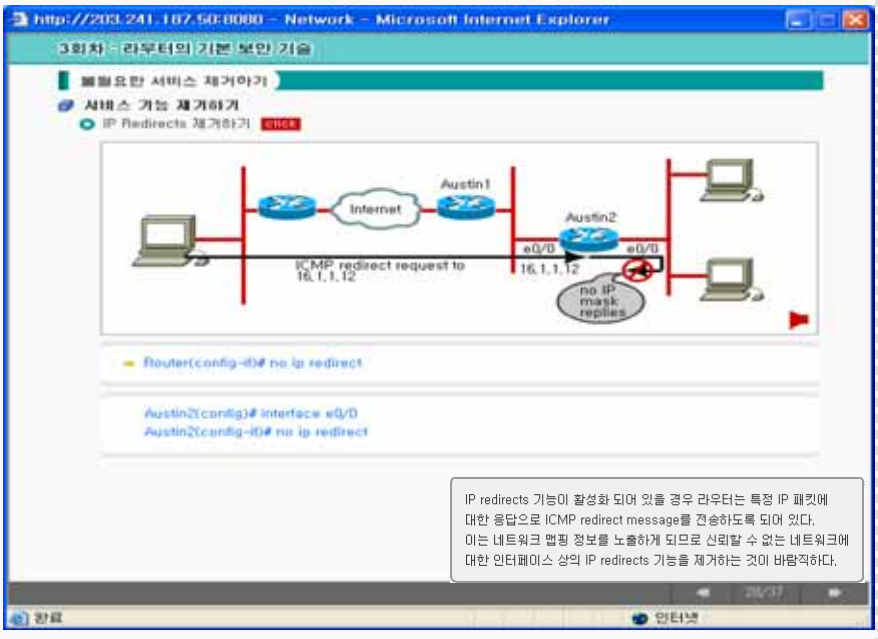

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
Restricting DNS Service
click
Austin1
Austin2
Austin3
Austin4
do not send DNS query
OK to send DNS query
DNS1 16.1.1.20
DNS query
Router(config)# ip name-server server-address1[server-address2 ... server-address6]
Austin4(config)# ip name-server 16.1.1.20
Router(config)# no ip domain-lookup
Austin3(config)# no ip domain-lookup
Cisco IOS는 DNS를 이용하여 호스트 이름을 검색할 수 있도록 지원한다. DNS는 호스트 이름과 IP 주소를 맵핑하는 것으로 유감스럽게도 DNS 프로토콜은 어떠한 인증 기능도 제공하지 않는다. 따라서 DNS 서비스를 꼭 필요한 경우로만 제한하는 것이 바람직하다.
완료
인터넷

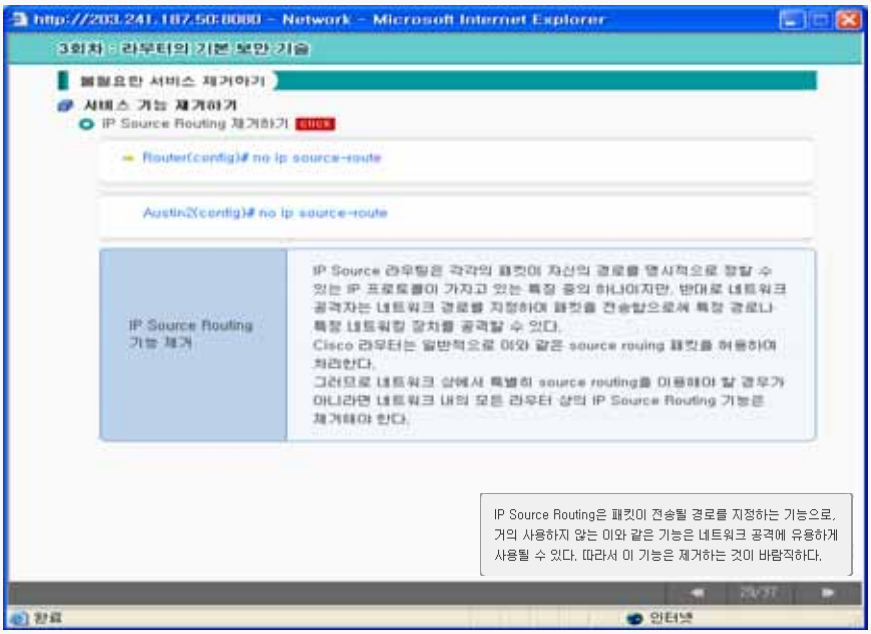

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
Finger Service 제거하기
click
Austin1
Austin2
Austin3
Austin4
Connect 16.1.1.15 finger
Connection refused
16.1.1.15
Router(config)# no ip finger
Austin4(config)# no ip finger
Austin4(config)# no service finger
Austin4(config)# exit
Austin4# connect 16.1.1.15 finger
Trying 16.1.1.15, 79 ...
% Connection refused by remote host
Finger service는 Unix 사용자에 대한 검색 서비스로 원격지에 있는 사용자 목록을 알아낼 수 있다. finger 서비스는 원격의 사용자로 하여금 어떤 사용자가 라우터에 접속해 있는지를 알려주는 역할을 한다. 이는 라우터에 로그인 할수 있는 사용자 이름을 비롯한 중요한 정보를 제공하기에 공격자들이 많이 사용하는 서비스중의 하나이다. 따라서 Finger service 또한 제거하는 것이 바람직하다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
HTTP Service 제거하기
click
Austin1
Austin2
Austin3
Austin4
http://16.1.1.15
Connection refused
16.1.1.15
Router(config)# no ip http server
Austin4(config)# no ip http server
시스코 라우터는 HTTP 프로토콜을 사용하여 원격에서 여러 가지 기능 설정이 가능하다. HTTP 서버는 텔넷을 사용하여 라우터를 제어할때의 보안 취약점에 대비하여 만들어졌지만 HTTP 서비스는 인터넷 프로토콜이 가지고 있는 보안에 가장 취약한 프로토콜 중의 하나로서 일부 Cisco IOS 장치의 경우 웹 기반의 설정이 가능하도록 되어 있다. 따라서 라우터의 HTTP Service 기능을 명시적으로 제거해 놓는 것이 바람직하다.
25/37
완료
인터넷

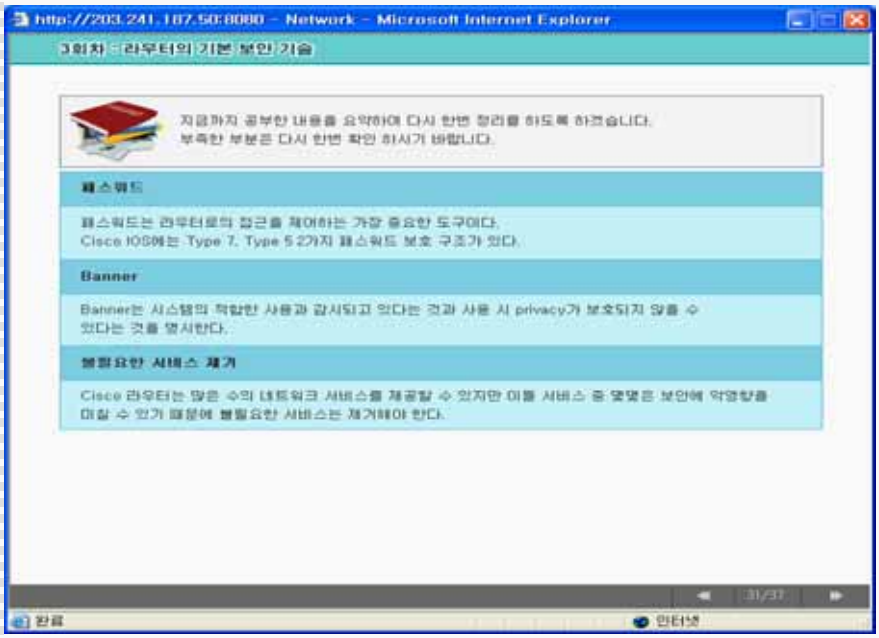

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
IP Directed Broadcast 기능 제거하기
click
Host with falsified source address
Internet
Austin1
Austin2
e0/0
e0/0
Target Segment
ICMP echo requests to directed broadcast address
Directed broadcasts are dropped
Router(config-if)# no ip directed-broadcast
Austin2(config)# interface e0/1
Austin2(config-if)# no ip directed-broadcast
IP directed broadcast 기능을 이용하면 임의의 패킷을 가지고 특정 LAN에 broadcast 트래픽을 보낼 수 있다. 이와 같은 directed broadcast 기능은 전문적인 기술을 몰라도 네트워크를 공격하는 방법으로 흔히 사용되고 있으므로 IP directed broadcast 기능은 제거해 놓는 것이 좋다.
25/37
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 - 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
IP Mask Replies 제거하기 CHECK
Austin1
Internet
Austin2
e0/0
e0/0
ICMP mask request to 16.1.1.12
16.1.1.12
no IP mask replies
Router(config-if)# no ip mask-reply
Austin2(config)# interface e0/0
Austin2(config-if)# no ip mask-reply
IP mask replies 기능이 활성화 되어 있을 경우, 라우터는 ICMP mask request에 대한 응답으로 인터페이스 IP 주소에 대한 서브넷 마스크를 보내게 되며, 이는 IP 주소 맵핑 정보를 쉽게 노출하는 결과로 이어진다. 따라서 신뢰할 수 없는 네트워크에 대한 인터페이스 상의 IP mask replies 기능은 제거하는 것이 바람직하다.
완료
인터넷

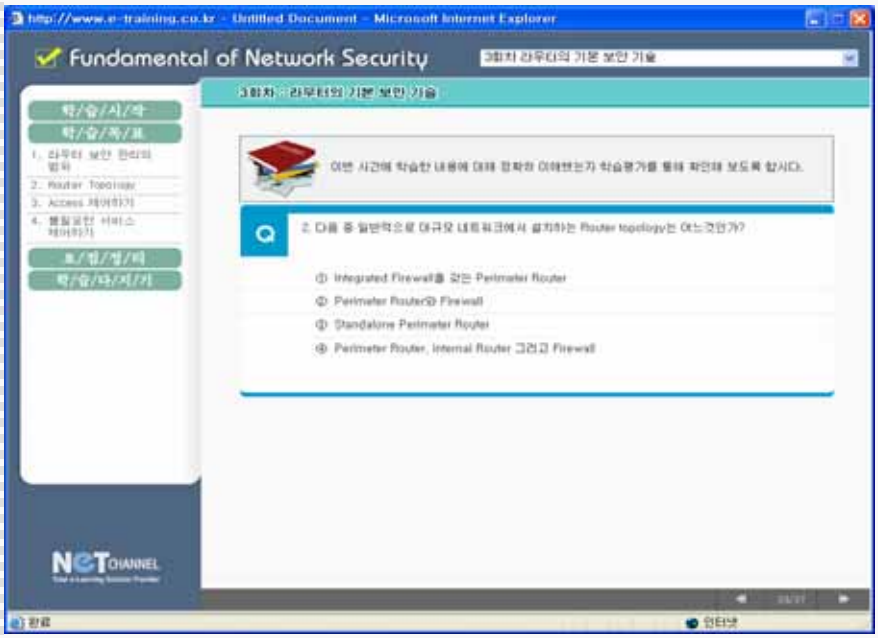

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 - 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
IP Redirects 제거하기 CHECK
Austin1
Internet
Austin2
e0/0
e0/0
ICMP redirect request to 16.1.1.12
16.1.1.12
no IP mask replies
Router(config-if)# no ip redirect
Austin2(config)# interface e0/0
Austin2(config-if)# no ip redirect
IP redirects 기능이 활성화 되어 있을 경우 라우터는 특정 IP 패킷에 대한 응답으로 ICMP redirect message를 전송하도록 되어 있다.
이는 네트워크 맵핑 정보를 노출하게 되므로 신뢰할 수 없는 네트워크에 대한 인터페이스 상의 IP redirects 기능을 제거하는 것이 바람직하다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
불필요한 서비스 제거하기
서비스 기능 제거하기
IP Source Routing 제거하기
Router(config)# no ip source-route
Austin2(config)# no ip source-route
IP Source Routing 기능 제거
IP Source 라우팅은 각각의 패킷이 자신의 경로를 명시적으로 정할 수 있는 IP 프로토콜이 가지고 있는 특징 중의 하나이지만, 반대로 네트워크 공격자는 네트워크 경로를 지정하여 패킷을 전송함으로써 특정 경로나 특정 네트워킹 장치를 공격할 수 있다.
Cisco 라우터는 일반적으로 이와 같은 source routing 패킷을 허용하여 처리한다.
그러므로 네트워크 상에서 특별히 source routing을 이용해야 할 경우가 아니라면 네트워크 내의 모든 라우터 상의 IP Source Routing 기능은 제거해야 한다.
IP Source Routing은 패킷이 전송될 경로를 지정하는 기능으로, 거의 사용하지 않는 이와 같은 기능은 네트워크 공격에 유용하게 사용될 수 있다. 따라서 이 기능은 제거하는 것이 바람직하다.
완료
인터넷

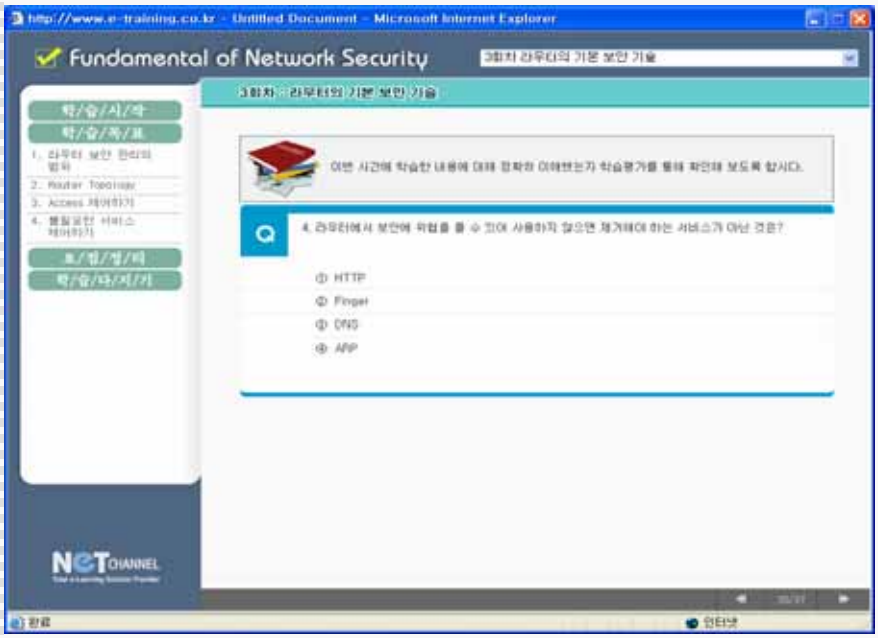

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 : 라우터의 기본 보안 기술
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
네트워크 보안을 위한 topology
"Standalone Perimeter Router"는 최소한의 보호가 이루어지며,
"Perimeter Router와 Firewall"는 DMZ를 구성하는 것이 가능한다. 또한 "Integrated firewall을 갖는 Perimeter Router" 는 통합된 perimeter router로 구성되며, "Perimeter Router, Internal Router, 그리고 Firewall"는 Perimeter 라우터, 방화벽 장비와 함께 내부 라우터를 사용한다.
low-risk 장비와 high-risk 장비
Low-risk 장비는 소형 라우터나 스위치 그리고 케이블링 등 저가 또는SOHO 장비이다.
High-risk 장비는 인터넷 라우터, 스위치, 방화벽, 관리시스템과 같은 대규모 사무실이나 캠퍼스에서 사용되는 중요 장비이다.
라우터와 스위치로의 access 보호
라우터와 스위치는 Console port, TTYs와 AUX, VTYs로의 access를 적절하게 제어하는 것이 필요한다.
완료
인터넷

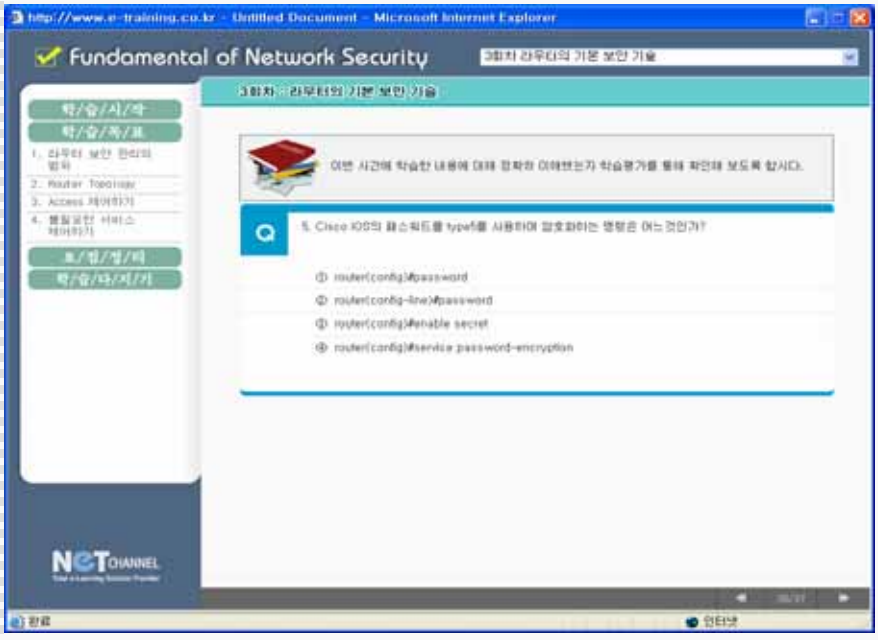

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
3회차 - 라우터의 기본 보안 기술
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
패스워드
패스워드는 라우터로의 접근을 제어하는 가장 중요한 도구이다.
Cisco IOS에는 Type 7, Type 5 2가지 패스워드 보호 구조가 있다.
Banner
Banner는 시스템의 적합한 사용과 감시되고 있다는 것과 사용 시 privacy가 보호되지 않을 수
있다는 것을 명시한다.
불필요한 서비스 제거
Cisco 라우터는 많은 수의 네트워크 서비스를 제공할 수 있지만 이들 서비스 중 몇몇은 보안에 악영향을
미칠 수 있기 때문에 불필요한 서비스는 제거해야 한다.
31/37
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
3회차 라우터의 기본 보안 기술
학/습/시/작
학/습/목/표
1. 라우터 보안 전반의 개요
2. Router Topology
3. Access 제어하기
4. 불필요한 서비스 제어하기
요/점/정/리
학/습/자/기/검
3회차 - 라우터의 기본 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는가 학습평가를 통해 확인해 보도록 합시다.
Q
1. 다음 중 Perimeter Router의 특징에 해당되지 않는 것은 어느 것인가?
① 모든 기능이 탑재된 Firewall 장치로 동작한다.
② 인터넷으로부터 내부 네트워크로의 접근을 막는 첫 번째 장치로 동작한다.
③ DMZ 영역을 정의한다.
④ DMZ 영역 내에 위치한 호스트를 방어한다.
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
3회차 라우터의 기본 보안 기술
학/습/시/작
학/습/목/표
1. 라우터 보안 관리의 필요
2. Router Topology
3. Access 제어하기
4. 불필요한 서비스 제어하기
보/충/설/명
학/습/자/가/점
3회차 : 라우터의 기본 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
2. 다음 중 일반적으로 대규모 네트워크에서 설치하는 Router topology는 어느것인가?
① Integrated Firewall을 갖는 Perimeter Router
② Perimeter Router와 Firewall
③ Standalone Perimeter Router
④ Perimeter Router, Internal Router 그리고 Firewall
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
3회차 라우터의 기본 보안 기술
학/습/시/작
학/습/목/표
1. 라우터 보안 관리의 필요
2. Router Topology
3. Access 제어하기
4. 불필요한 서비스 제어하기
보/충/설/명
학/습/자/가/점
3회차 : 라우터의 기본 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합시다.
Q
3. 아래 설명이 맞으면 O에 체크, 틀리면 X에 체크 하시오.
Cisco IOS에는 표스워드 구조로 Cisco 에서 정의한 알고리즘을 사용하는 type5와 MD5를 사용하는 type 7가 있다. Cisco에서는 Type 7의 사용을 권고하고 있다.
O
X
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
3회차 라우터의 기본 보안 기술
학/습/시/작
학/습/목/표
1. 라우터 보안 관리의 필요
2. Router Topology
3. Access 제어하기
4. 불필요한 서비스 제어하기
요/점/정/리
학/습/마/치/기
3회차 : 라우터의 기본 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는가 학습평가를 통해 확인해 보도록 합시다.
4. 라우터에서 보안에 위협을 줄 수 있어 사용하지 않으면 제거해야 하는 서비스가 아닌 것은?
① HTTP
② Finger
③ DNS
④ ARP
NETCHANNEL
완료
인터넷


http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer
Fundamental of Network Security
3회차 라우터의 기본 보안 기술
학/습/시/작
학/습/목/표
1. 라우터 보안 관리의 필요
2. Router Topology
3. Access 제어하기
4. 불필요한 서비스 제어하기
요/점/정/리
학/습/마/치/기
3회차 : 라우터의 기본 보안 기술
이번 시간에 학습한 내용에 대해 정확히 이해했는가 학습평가를 통해 확인해 보도록 합시다.
5. Cisco IOS의 콘소울포트를 type5를 사용하여 암호화하는 명령은 어느 것인가?
① router(config)#password
② router(config-line)#password
③ router(config)#enable secret
④ router(config)#service password-encryption
NETCHANNEL
완료
인터넷

End of Lecture