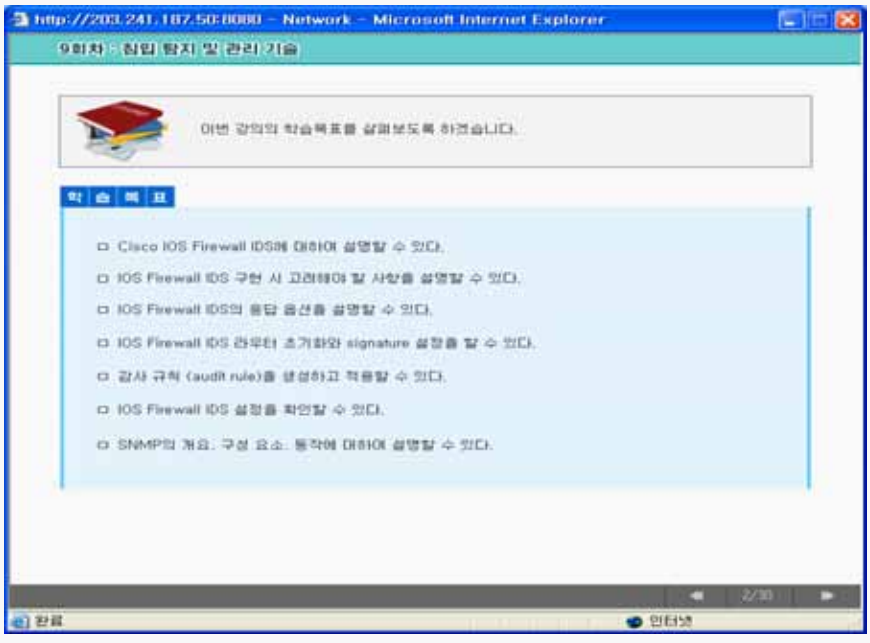
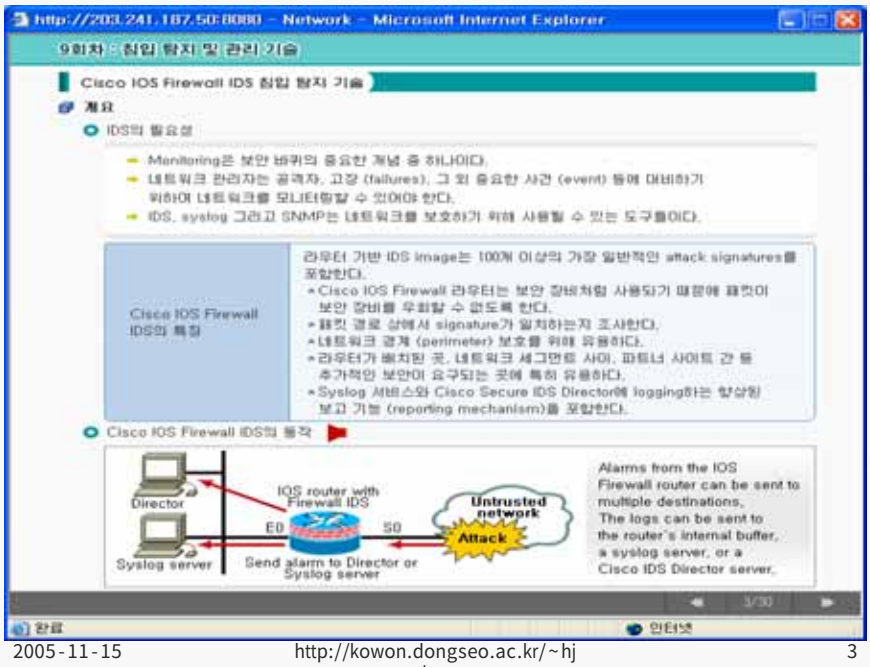
FNS

(Fundamental Network Security)

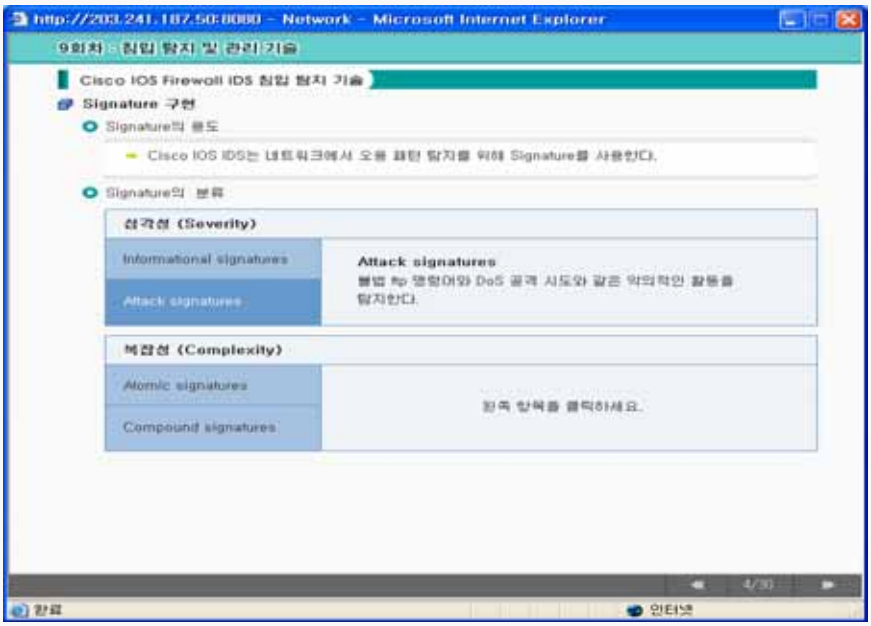
Ch9. 침입탐지 및 관리기술

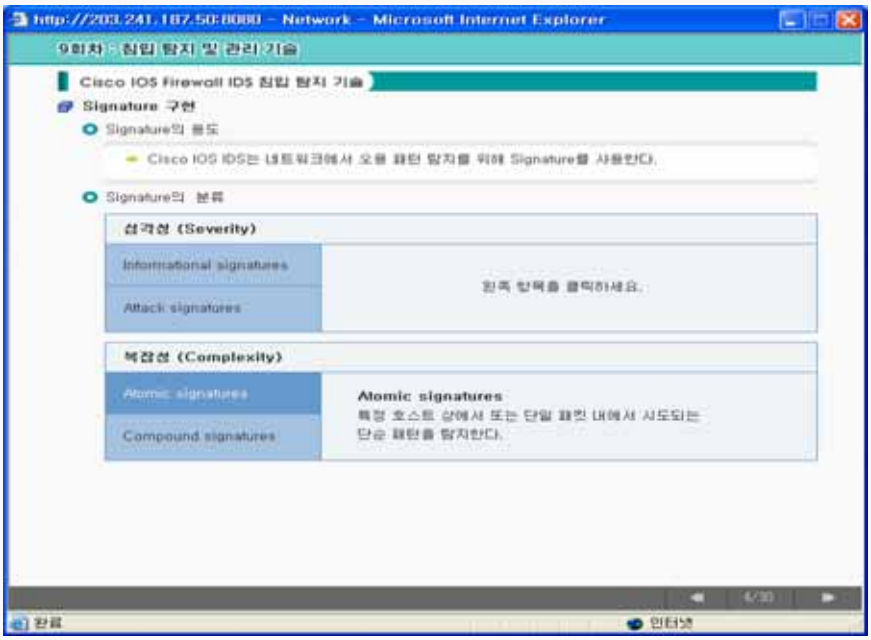
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr

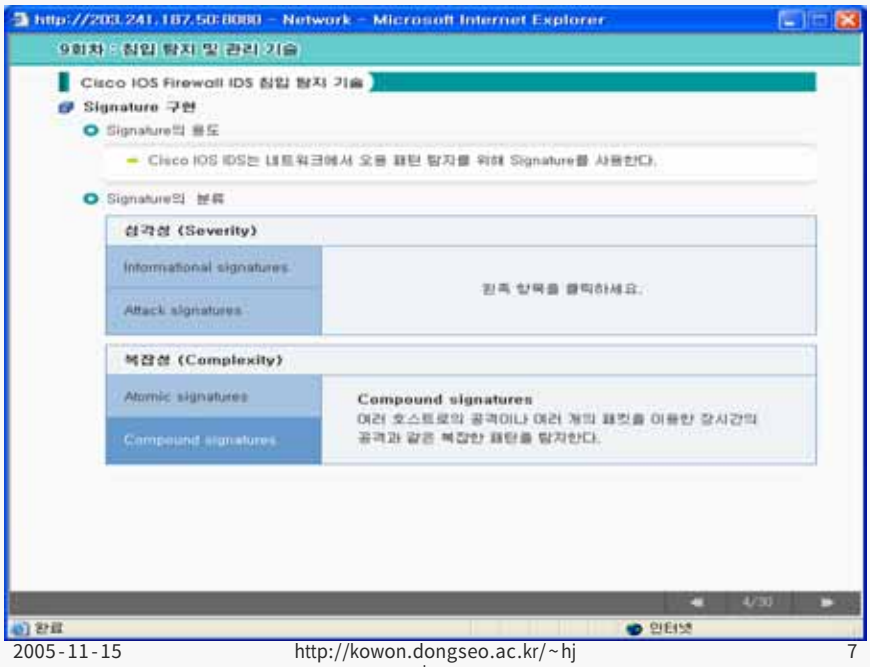


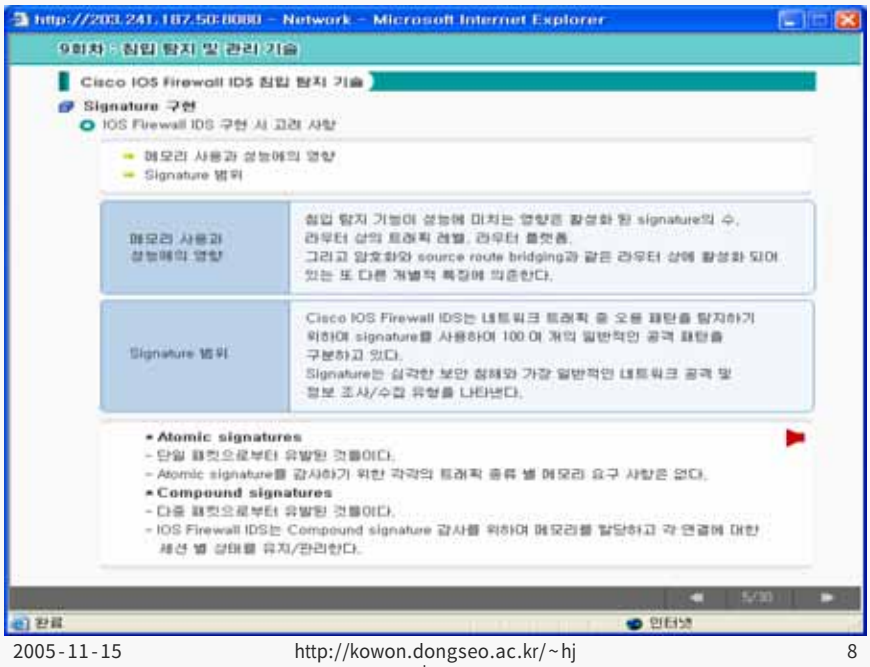

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
개요
IDS의 필요성
Monitoring은 보안 네뷔의 중요한 개념 중 하나이다.
네트워크 관리자는 공격자, 고장 (failures), 그 외 중요한 사건 (event) 등에 대비하기 위하여 네트워크를 모니터링할 수 있어야 한다.
IDS, syslog 그리고 SNMP는 네트워크를 보호하기 위해 사용될 수 있는 도구들이다.
Cisco IOS Firewall IDS의 특징
라우터 기반 IDS Image는 100개 이상의 가장 일반적인 attack signatures를 포함한다.
Cisco IOS Firewall 라우터는 보안 장비처럼 사용되기 때문에 해킹이 보안 장비를 우회할 수 없도록 한다.
패킷 경로 상에서 signature가 일치하는지 조사한다.
네트워크 경계 (perimeter) 보호를 위해 유용하다.
라우터가 배치된 곳, 네트워크 세그먼트 사이, 파트너 사이트 간 등 추가적인 보안이 요구되는 곳에 특히 유용하다.
Syslog 서버스와 Cisco Secure IDS Director에 logging하는 향상된 보고 기능 (reporting mechanism)을 포함한다.
Cisco IOS Firewall IDS의 동작
Director
Syslog server
IOS router with Firewall IDS
E0
S0
Untrusted network
Attack
Send alarm to Director or Syslog server
Alarms from the IOS Firewall router can be sent to multiple destinations. The logs can be sent to the router's internal buffer, a syslog server, or a Cisco IDS Director server.
1/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
Signature 구현
Signature의 용도
Cisco IOS IDS는 네트워크에서 오용 패턴 탐지를 위해 Signature를 사용한다.
Signature의 분류
심각성 (Severity)
Informational signatures
Attack signatures
Informational signatures
port sweep과 같은 정보를 탐지한다.
복잡성 (Complexity)
Atomic signatures
Compound signatures
왼쪽 항목을 클릭하세요.
6/30
완료
인터넷

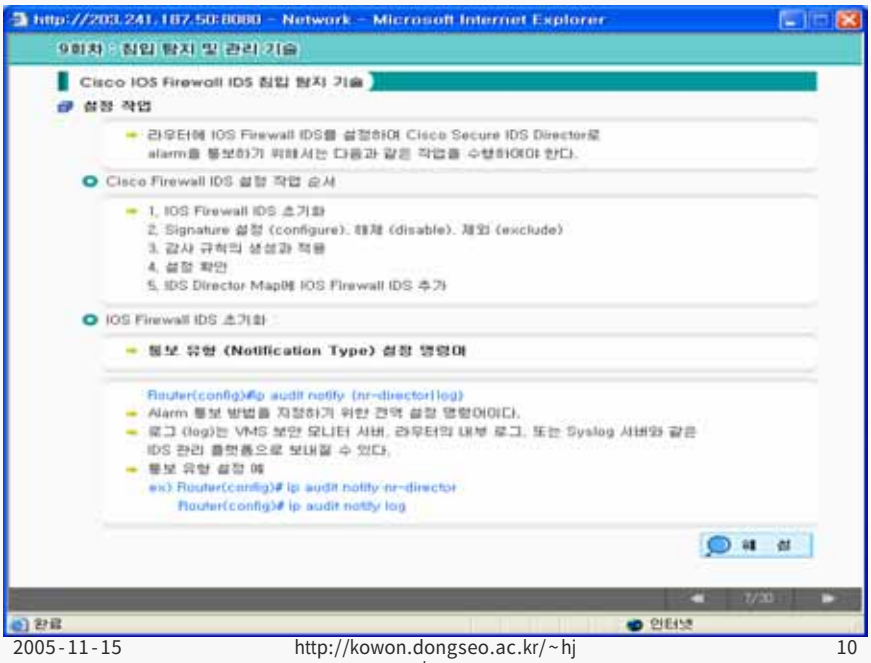

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
Signature 구현
Signature의 용도
Cisco IOS IDS는 네트워크에서 오용 패턴 탐지를 위해 Signature를 사용한다.
Signature의 분류
심각성 (Severity)
Informational signatures
Attack signatures
Attack signatures
불법 ftp 명령어와 DoS 공격 시도와 같은 악의적인 활동을 탐지한다.
복잡성 (Complexity)
Atomic signatures
Compound signatures
왼쪽 항목을 클릭하세요.
4/30
완료
인터넷

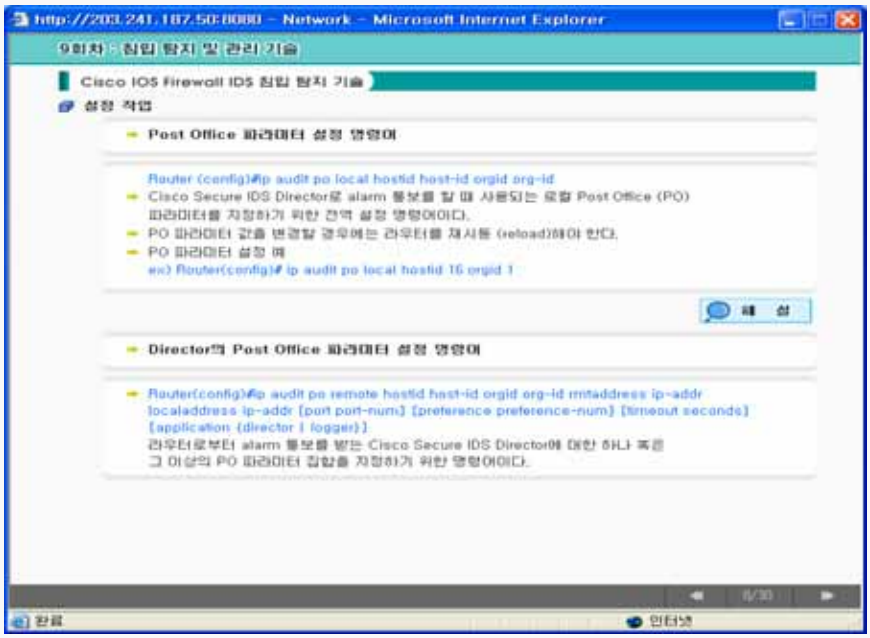

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
Signature 구현
Signature의 용도
Cisco IOS IDS는 네트워크에서 오용 패턴 탐지를 위해 Signature를 사용한다.
Signature의 분류
심각성 (Severity)
Informational signatures
Attack signatures
왼쪽 항목을 클릭하세요.
복잡성 (Complexity)
Atomic signatures
Compound signatures
Atomic signatures
특정 호스트 상에서 또는 단일 패킷 내에서 시도되는 단순 패턴을 탐지한다.
4/30
완료
인터넷

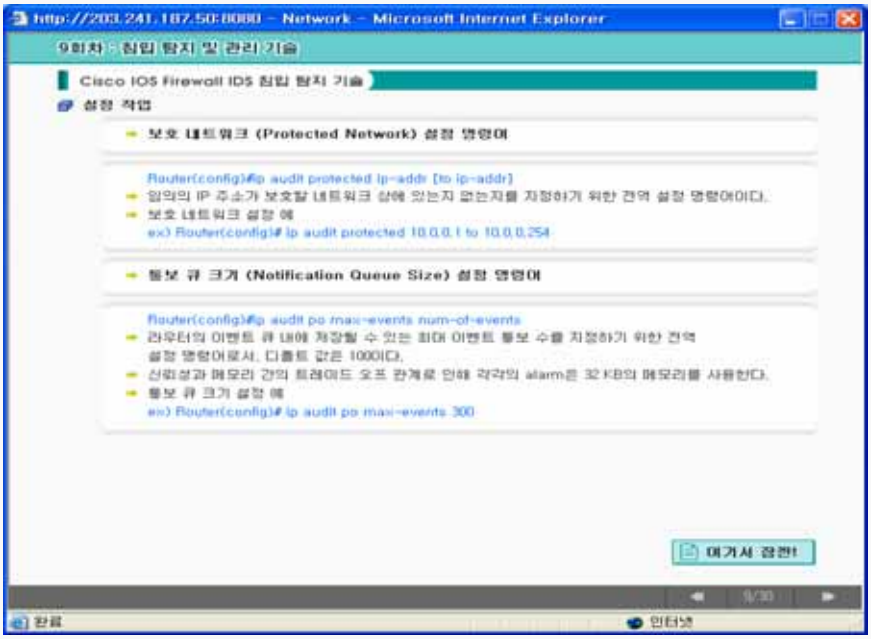

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
Signature 구현
Signature의 용도
Cisco IOS IDS는 네트워크에서 오용 패턴 탐지를 위해 Signature를 사용한다.
Signature의 분류
심각성 (Severity)
Informational signatures
Attack signatures
왼쪽 항목을 클릭하세요.
복잡성 (Complexity)
Atomic signatures
Compound signatures
Compound signatures
여러 호스트로의 공격이나 여러 개의 패킷을 이용한 장시간의 공격과 같은 복잡한 패턴을 탐지한다.
4/30
완료
인터넷

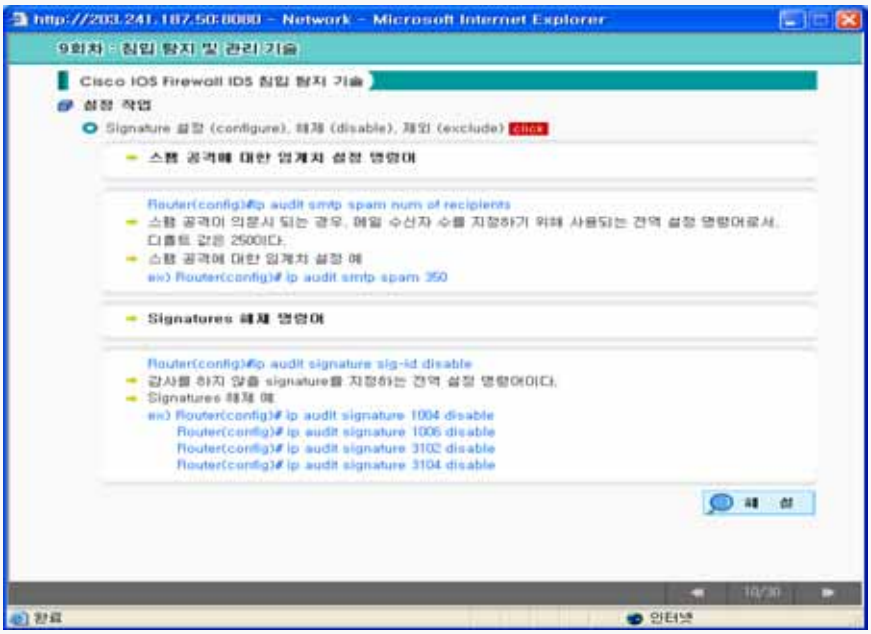

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
Signature 구현
IOS Firewall IDS 구현 시 고려 사항
메모리 사용과 성능에의 영향
Signature 범위
메모리 사용과 성능에의 영향
침입 탐지 기능이 성능에 미치는 영향은 활성화 된 signature의 수, 라우터 상의 트래픽 레벨, 라우터 플랫폼, 그리고 암호화와 source route bridging과 같은 라우터 상에 활성화 되어 있는 또 다른 계별적 특징에 의존한다.
Signature 범위
Cisco IOS Firewall IDS는 네트워크 트래픽 중 오용 패턴을 탐지하기 위하여 signature를 사용하여 100 여 개의 일반적인 공격 패턴을 구분하고 있다.
Signature는 심각한 보안 침해와 가장 일반적인 네트워크 공격 및 정보 조사/수집 유형을 나타낸다.
• Atomic signatures
- 단일 패킷으로부터 유발된 것들이다.
- Atomic signature를 감사하기 위한 각각의 트래픽 종류 별 메모리 요구 사항은 없다.
• Compound signatures
- 다중 패킷으로부터 유발된 것들이다.
- IOS Firewall IDS는 Compound signature 감사를 위하여 메모리를 할당하고 각 연결에 대한 세션 별 상태를 유지/관리한다.
5/30
완료
인터넷

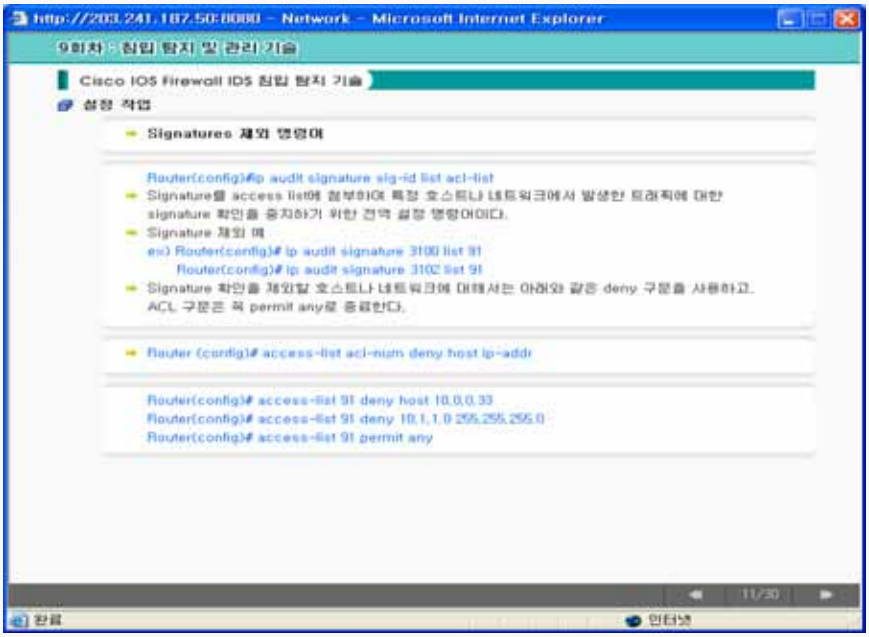

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
응답 옵션
Cisco IOS Firewall IDS는 침입 탐지를 즉각적으로 알아내는 일종의 센서와 같은 기능을 수행하며,
라우터 인터페이스를 통과하는 패킷을 검사하여 미리 정해진 규칙에 따라 동작한다.
단일 세션 내의 한 개 또는 다수의 패킷이 signature와 일치할 때,
IOS Firewall IDS는 다음과 같은 동작을 수행하게 된다.
Alarm
Cisco Secure IDS Director나 Syslog 서버,
또는 라우터 콘솔로 alarm을 보내고, 패킷은 폐기하지 않고 그대로
전달한다.
Reset
해당 패킷이 TCP 세션에 의한 패킷이라면,
양단의 TCP 세션에 reset flag를 설정하여 패킷을 전송한 후,
패킷을 폐기하지 않고 그대로 전달한다.
Drop
패킷을 즉시 폐기한다.
5/30
완료
인터넷

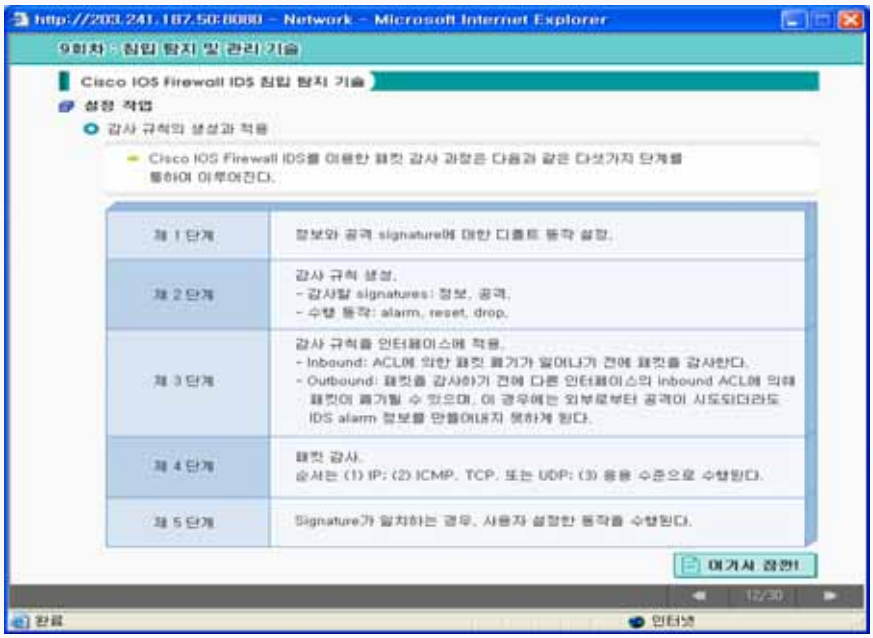

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
라우터에 IOS Firewall IDS를 설정하여 Cisco Secure IDS Director로
alarm을 통보하기 위해서는 다음과 같은 작업을 수행하여야 한다.
Cisco Firewall IDS 설정 작업 순서
1. IOS Firewall IDS 초기화
2. Signature 설정 (configure), 해제 (disable), 제외 (exclude)
3. 감사 규칙의 생성과 적용
4. 설정 확인
5. IDS Director Map에 IOS Firewall IDS 추가
IOS Firewall IDS 초기화
통보 유형 (Notification Type) 설정 명령어
Router(config)#ip audit notify (nr-director|log)
Alarm 통보 방법을 지정하기 위한 전역 설정 명령어이다.
로그 (log)는 VMS 보안 모니터 서버, 라우터의 내부 로그, 또는 Syslog 서버와 같은
IDS 관리 플랫폼으로 보내질 수 있다.
통보 유형 설정 예
ex) Router(config)# ip audit notify nr-director
Router(config)# ip audit notify log
해 설
5/30
완료
인터넷

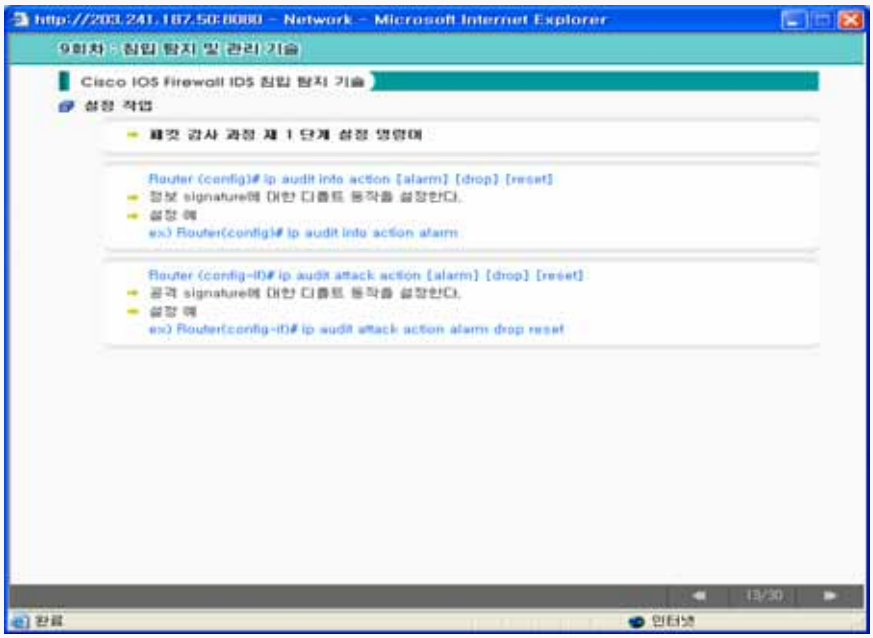

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
Post Office 파라메터 설정 명령어
Router (config)#ip audit po local hostid host-id orgid org-id
Cisco Secure IDS Director로 alarm 통보를 할 때 사용되는 로컬 Post Office (PO)
파라미터를 지정하기 위한 전역 설정 명령어이다.
PO 파라미터 값을 변경할 경우에는 라우터를 재시동 (reload)해야 한다.
PO 파라미터 설정 예
ex) Router(config)# ip audit po local hostid 16 orgid 1
해 설
Director의 Post Office 파라메터 설정 명령어
Router(config)#ip audit po remote hostid host-id orgid org-id rmtaddress ip-addr
localaddress ip-addr [port port-num] [preference preference-num] [timeout seconds]
[application {director | logger}]
라우터로부터 alarm 통보를 받는 Cisco Secure IDS Director에 대한 하나 혹은
그 이상의 PO 파라메터 집합을 지정하기 위한 명령어이다.
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
보호 네트워크 (Protected Network) 설정 명령어
Router(config)#ip audit protected ip-addr [to ip-addr]
임의의 IP 주소가 보호할 네트워크 상에 있는지 없는지를 지정하기 위한 전역 설정 명령어이다.
보호 네트워크 설정 예
ex) Router(config)# ip audit protected 10.0.0.1 to 10.0.0.254
통보 큐 크기 (Notification Queue Size) 설정 명령어
Router(config)#ip audit po max-events num-of-events
라우터의 이벤트 큐 내에 저장될 수 있는 최대 이벤트 통보 수를 지정하기 위한 전역
설정 명령어로서, 디폴트 값은 100이다.
신뢰성과 메모리 간의 트레이드 오프 관계로 인해 각각의 alarm은 32 KB의 메모리를 사용한다.
통보 큐 크기 설정 예
ex) Router(config)# ip audit po max-events 300
여기서 잠깐!
완료
인터넷

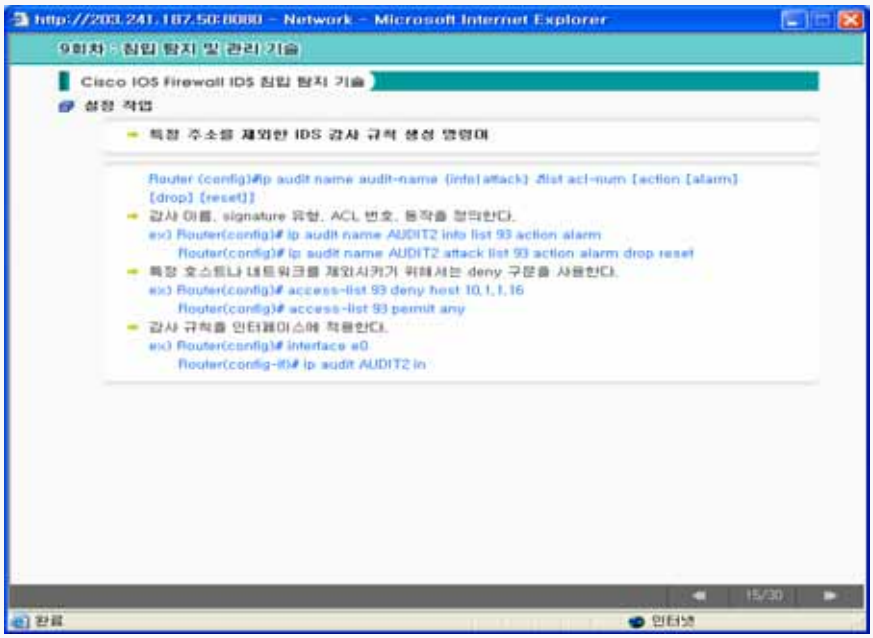

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
Signature 설정 (configure), 해제 (disable), 제외 (exclude)
스팸 공격에 대한 임계치 설정 명령어
Router(config)#ip audit smtp spam num of recipients
스팸 공격이 의문시 되는 경우, 메일 수신자 수를 지정하기 위해 사용되는 전역 설정 명령어로서,
디폴트 값은 2500이다.
스팸 공격에 대한 임계치 설정 예
ex) Router(config)# ip audit smtp spam 350
Signatures 해제 명령어
Router(config)#ip audit signature sig-id disable
감사를 하지 않을 signature를 지정하는 전역 설정 명령어이다.
Signatures 해제 예
ex) Router(config)# ip audit signature 1004 disable
Router(config)# ip audit signature 1006 disable
Router(config)# ip audit signature 3102 disable
Router(config)# ip audit signature 3104 disable
10/30
완료
인터넷

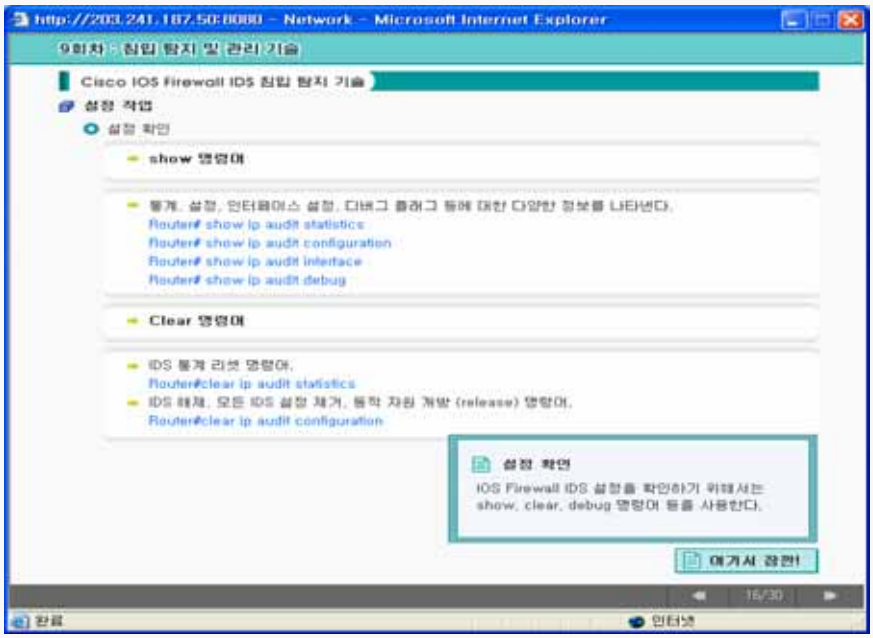

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
Signatures 제외 명령어
Router(config)#ip audit signature sig-id list acl-list
Signature를 access list에 첨부하여 특정 호스트나 네트워크에서 발생한 트래픽에 대한
signature 확인을 중지하기 위한 전역 설정 명령어이다.
Signature 제외 예
ex) Router(config)# ip audit signature 3100 list 91
Router(config)# ip audit signature 3102 list 91
Signature 확인을 제외할 호스트나 네트워크에 대해서는 아래와 같은 deny 구문을 사용하고,
ACL 구문은 꼭 permit any로 종료한다.
Router (config)# access-list acl-num deny host ip-addr
Router(config)# access-list 91 deny host 10.0.0.33
Router(config)# access-list 91 deny 10.1.1.0 255.255.255.0
Router(config)# access-list 91 permit any
11/30
완료
인터넷

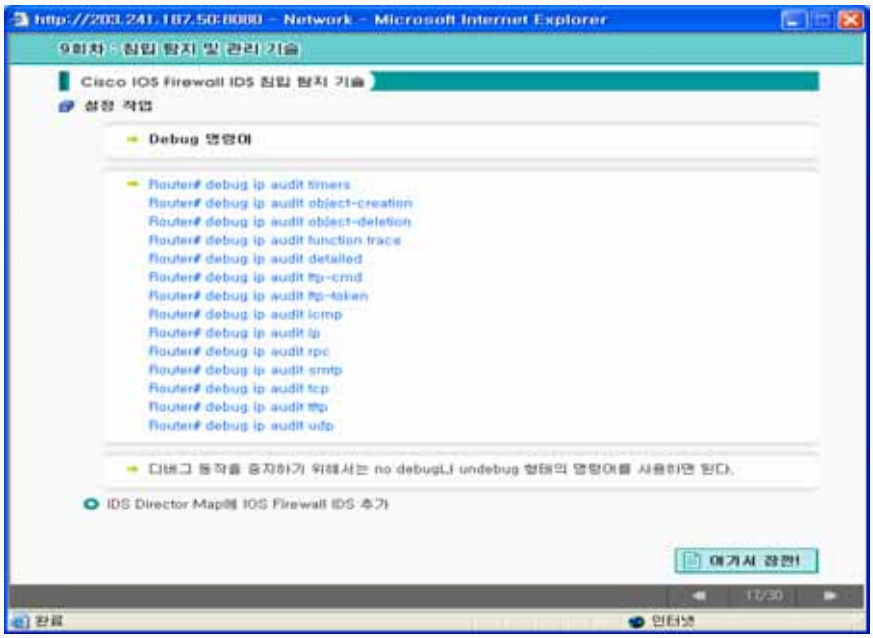

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
감사 규칙의 생성과 적용
Cisco IOS Firewall IDS를 이용한 패킷 감사 과정은 다음과 같은 다섯가지 단계를 통하여 이루어진다.
제 1 단계
정보와 공격 signature에 대한 디폴트 동작 설정.
제 2 단계
감사 규칙 생성.
- 감사할 signatures: 정보, 공격.
- 수행 동작: alarm, reset, drop.
제 3 단계
감사 규칙을 인터페이스에 적용.
- Inbound: ACL에 의한 패킷 필터가 일어나기 전에 패킷을 감사한다.
- Outbound: 패킷을 감사하기 전에 다른 인터페이스의 inbound ACL에 의해 패킷이 폐기될 수 있으며, 이 경우에는 외부로부터 공격이 시도되더라도 IDS alarm 정보를 만들어내지 못하게 된다.
제 4 단계
패킷 감사.
순서는 (1) IP; (2) ICMP, TCP, 또는 UDP; (3) 응용 수준으로 수행된다.
제 5 단계
Signature가 일치하는 경우, 사용자 설정한 동작을 수행한다.
여기서 잠깐!
12/30
완료
인터넷

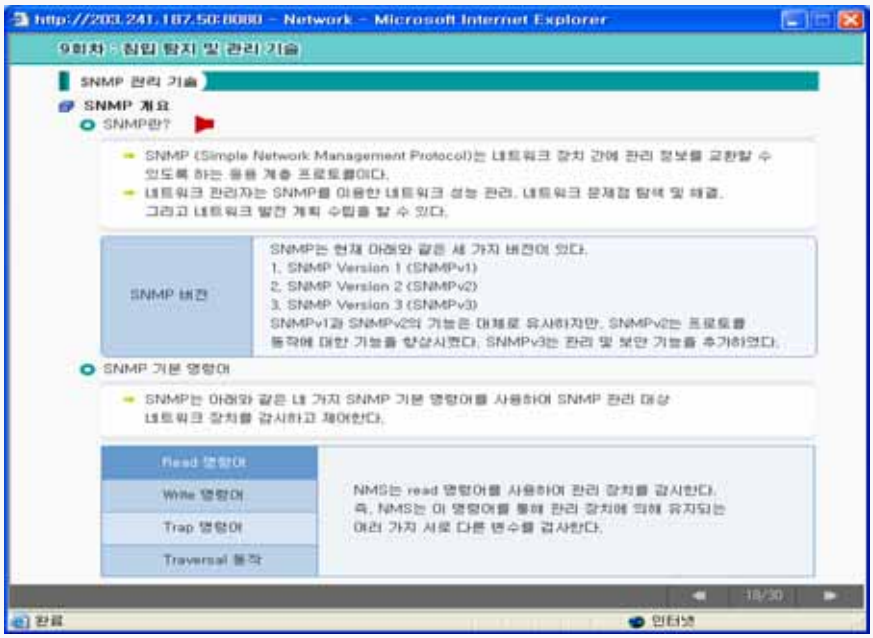

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
패킷 감사 과정 제 1 단계 설정 명령어
Router (config)# ip audit info action [alarm] [drop] [reset]
정보 signature에 대한 디폴트 동작을 설정한다.
설정 예
ex) Router(config)# ip audit info action alarm
Router (config-if)# ip audit attack action [alarm] [drop] [reset]
공격 signature에 대한 디폴트 동작을 설정한다.
설정 예
ex) Router(config-if)# ip audit attack action alarm drop reset
13/30
완료
인터넷

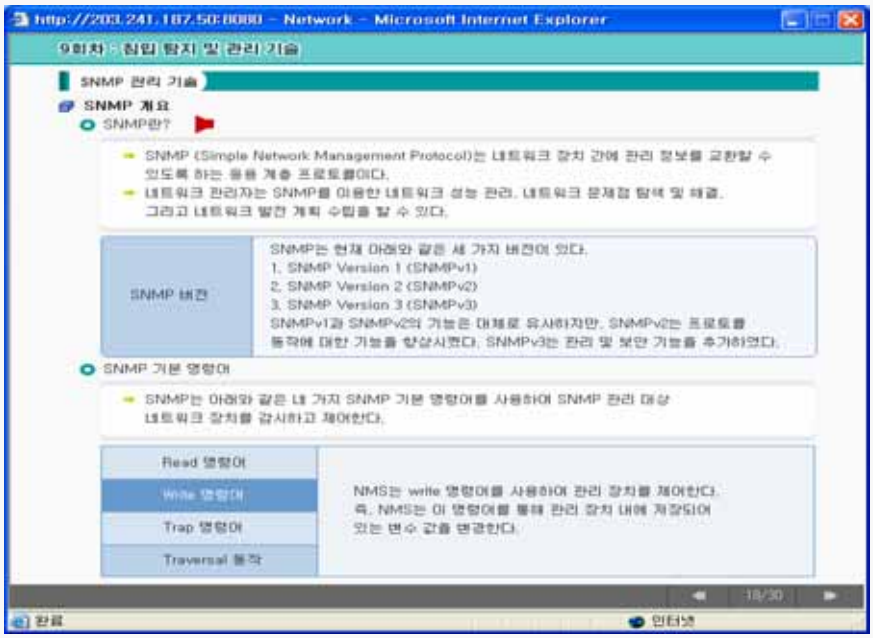

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
패킷 감사 과정 제 2 단계 설정 명령어
Router (config)#ip audit name audit-name {info|attack} [action [alarm] [drop] [reset]]
감사 이름, signature 유형, 동작을 정의한다.
ex) Router(config)# ip audit name AUDIT1 info action alarm
Router(config)# ip audit name AUDIT1 attack action alarm drop reset
패킷 감사 과정 제 3 단계 설정 명령어
Router (config-if)# ip audit audit-name {in|out}
감사 규칙을 인터페이스에 적용한다.
ex) Router(config)# interface e0
Router(config-if)# ip audit AUDIT1 in
14/30
완료
인터넷

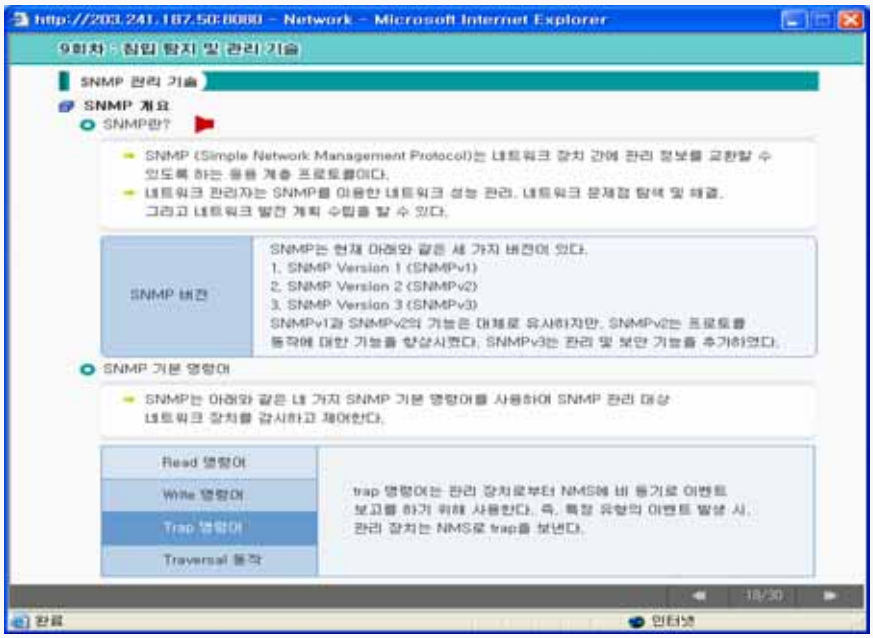

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
특정 주소를 제외한 IDS 감사 규칙 설정 명령어
Router (config)#ip audit name audit-name {info|attack} #list acl-num [action [alarm]
[drop] [reset]]
감사 이름, signature 유형, ACL 번호, 동작을 정의한다.
ex) Router(config)# ip audit name AUDIT2 info list 93 action alarm
Router(config)# ip audit name AUDIT2 attack list 93 action alarm drop reset
특정 호스트나 네트워크를 제외시키기 위해서는 deny 구문을 사용한다.
ex) Router(config)# access-list 93 deny host 10.1.1.16
Router(config)# access-list 93 permit any
감사 규칙을 인터페이스에 적용한다.
ex) Router(config)# interface e0
Router(config-if)# ip audit AUDIT2 in
15/30
완료
인터넷

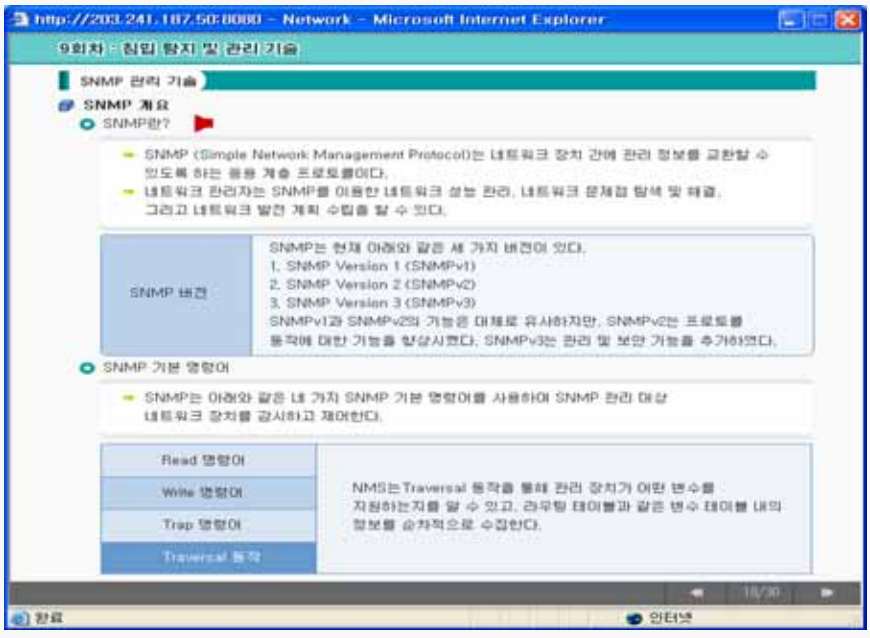

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
설정 확인
show 명령어
통계, 설정, 인터페이스 설정, 디버그 플래그 등에 대한 다양한 정보를 나타낸다.
Router# show ip audit statistics
Router# show ip audit configuration
Router# show ip audit interface
Router# show ip audit debug
Clear 명령어
IDS 통계 리셋 명령어.
Router#clear ip audit statistics
IDS 해제. 모든 IDS 설정 제거, 동작 자원 개방 (release) 명령어.
Router#clear ip audit configuration
설정 확인
IOS Firewall IDS 설정을 확인하기 위해서는
show, clear, debug 명령어 등을 사용한다.
여기서 잠깐!
16/30
완료
인터넷

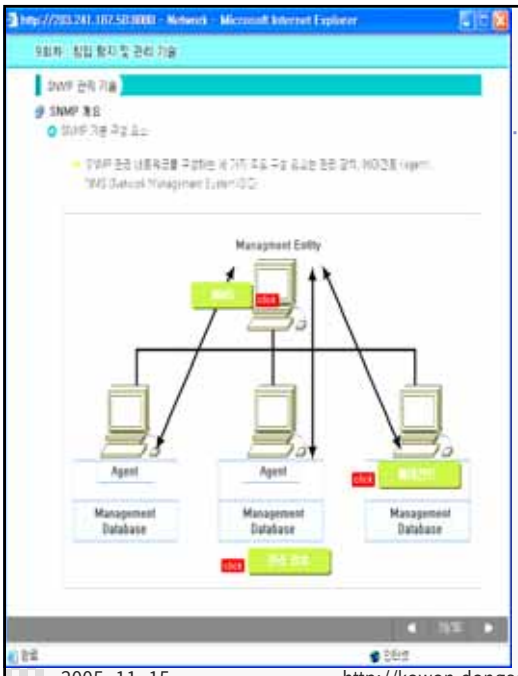

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
Cisco IOS Firewall IDS 침입 탐지 기술
설정 작업
Debug 명령어
Router# debug ip audit timers
Router# debug ip audit object-creation
Router# debug ip audit object-deletion
Router# debug ip audit function trace
Router# debug ip audit detailed
Router# debug ip audit ftp-cmd
Router# debug ip audit ftp-token
Router# debug ip audit icmp
Router# debug ip audit ip
Router# debug ip audit rpc
Router# debug ip audit smtp
Router# debug ip audit tcp
Router# debug ip audit tftp
Router# debug ip audit udp
디버그 동작을 중지하기 위해서는 no debug나 undebug 형태의 명령어를 사용하면 된다.
IDS Director Map에 IOS Firewall IDS 추가
여기서 잠깐!
17/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 개요
SNMP란?
SNMP (Simple Network Management Protocol)는 네트워크 장치 간에 관리 정보를 교환할 수 있도록 하는 응용 계층 프로토콜이다.
네트워크 관리자는 SNMP를 이용한 네트워크 성능 관리, 네트워크 문제점 탐색 및 해결, 그리고 네트워크 발전 계획 수립을 할 수 있다.
SNMP 버전
SNMP는 현재 아래와 같은 세 가지 버전이 있다.
1. SNMP Version 1 (SNMPv1)
2. SNMP Version 2 (SNMPv2)
3. SNMP Version 3 (SNMPv3)
SNMPv1과 SNMPv2의 기능은 대체로 유사하지만, SNMPv2는 프로토콜 동작에 대한 기능을 향상시켰다. SNMPv3는 관리 및 보안 기능을 추가하였다.
SNMP 기본 명령어
SNMP는 아래와 같은 네 가지 SNMP 기본 명령어를 사용하여 SNMP 관리 대상 네트워크 장치를 감시하고 제어한다.
Read 명령어
Write 명령어
Trap 명령어
Traversal 동작
NMS는 read 명령어를 사용하여 관리 장치를 감시한다. 즉, NMS는 이 명령어를 통해 관리 장치에 의해 유지되는 여러 가지 서로 다른 변수를 검사한다.
18/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 개요
SNMP란?
SNMP (Simple Network Management Protocol)는 네트워크 장치 간에 관리 정보를 교환할 수 있도록 하는 응용 계층 프로토콜이다.
네트워크 관리자는 SNMP를 이용한 네트워크 성능 관리, 네트워크 문제점 탐색 및 해결, 그리고 네트워크 발전 계획 수립을 할 수 있다.
SNMP 버전
SNMP는 현재 아래와 같은 세 가지 버전이 있다.
1. SNMP Version 1 (SNMPv1)
2. SNMP Version 2 (SNMPv2)
3. SNMP Version 3 (SNMPv3)
SNMPv1과 SNMPv2의 기능은 대체로 유사하지만, SNMPv2는 프로토콜 동작에 대한 기능을 향상시켰다. SNMPv3는 관리 및 보안 기능을 추가하였다.
SNMP 기본 명령어
SNMP는 아래와 같은 네 가지 SNMP 기본 명령어를 사용하여 SNMP 관리 대상 네트워크 장치를 감시하고 제어한다.
Read 명령어
Write 명령어
Trap 명령어
Traversal 동작
NMS는 write 명령어를 사용하여 관리 장치를 제어한다. 즉, NMS는 이 명령어를 통해 관리 장치 내에 저장되어 있는 변수 값을 변경한다.
18/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 개요
SNMP란?
SNMP (Simple Network Management Protocol)는 네트워크 장치 간에 관리 정보를 교환할 수 있도록 하는 응용 계층 프로토콜이다.
네트워크 관리자는 SNMP를 이용한 네트워크 성능 관리, 네트워크 문제점 탐색 및 해결, 그리고 네트워크 발전 계획 수립을 할 수 있다.
SNMP 버전
SNMP는 현재 아래와 같은 세 가지 버전이 있다.
1. SNMP Version 1 (SNMPv1)
2. SNMP Version 2 (SNMPv2)
3. SNMP Version 3 (SNMPv3)
SNMPv1과 SNMPv2의 기능은 대체로 유사하지만, SNMPv2는 프로토콜 동작에 대한 기능을 향상시켰다. SNMPv3는 관리 및 보안 기능을 추가하였다.
SNMP 기본 명령어
SNMP는 아래와 같은 네 가지 SNMP 기본 명령어를 사용하여 SNMP 관리 대상 네트워크 장치를 감시하고 제어한다.
Read 명령어
Write 명령어
Trap 명령어
Traversal 동작
trap 명령어는 관리 장치로부터 NMS에 비 동기로 이벤트 보고를 하기 위해 사용한다. 즉, 특정 유형의 이벤트 발생 시, 관리 장치는 NMS로 trap을 보낸다.
완료
인터넷

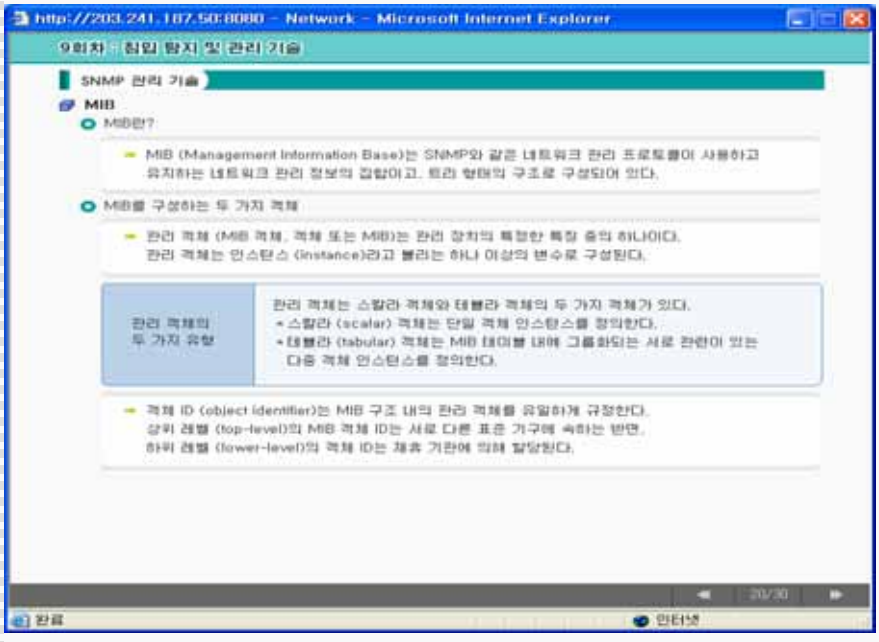

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 - 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 개요
SNMP란?
SNMP (Simple Network Management Protocol)는 네트워크 장치 간에 관리 정보를 교환할 수 있도록 하는 응용 계층 프로토콜이다.
네트워크 관리자는 SNMP를 이용한 네트워크 성능 관리, 네트워크 문제점 탐색 및 해결, 그리고 네트워크 발전 계획 수립을 할 수 있다.
SNMP 버전
SNMP는 현재 아래와 같은 세 가지 버전이 있다.
1. SNMP Version 1 (SNMPv1)
2. SNMP Version 2 (SNMPv2)
3. SNMP Version 3 (SNMPv3)
SNMPv1과 SNMPv2의 기능은 대체로 유사하지만, SNMPv2는 프로토콜 동작에 대한 기능을 향상시켰다. SNMPv3는 관리 및 보안 기능을 추가하였다.
SNMP 기본 명령어
SNMP는 아래와 같은 네 가지 SNMP 기본 명령어를 사용하여 SNMP 관리 대상 네트워크 장치를 감시하고 제어한다.
Read 명령어
Write 명령어
Trap 명령어
Traversal 동작
NMS는 Traversal 동작을 통해 관리 장치가 어떤 변수를 지원하는지를 알 수 있고, 라우팅 테이블과 같은 변수 테이블 내의 정보를 순차적으로 수집한다.
완료
인터넷

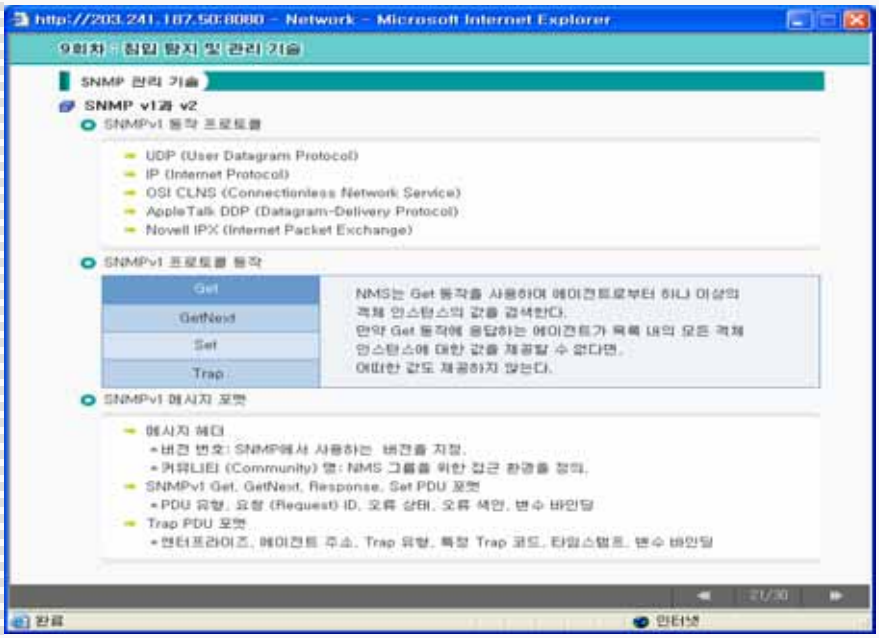


* NMS는 관리 장치를 감시하고 제어하는 응용 프로그램을 실행한다.
* NMS는 네트워크 관리에 필요한 프로세싱 자원과 메모리 자원을 제공한다.
* 임의의 관리 대상 네트워크 상에는 하나 이상의 NMS가 있어야 한다.
* CiscoWorks2000과 같은 SNMP 관리 애플리케이션은 관리 장치로부터의 통계 및 경보 (alert) 정보를 얻기 위하여 에이전트와 통신한다.

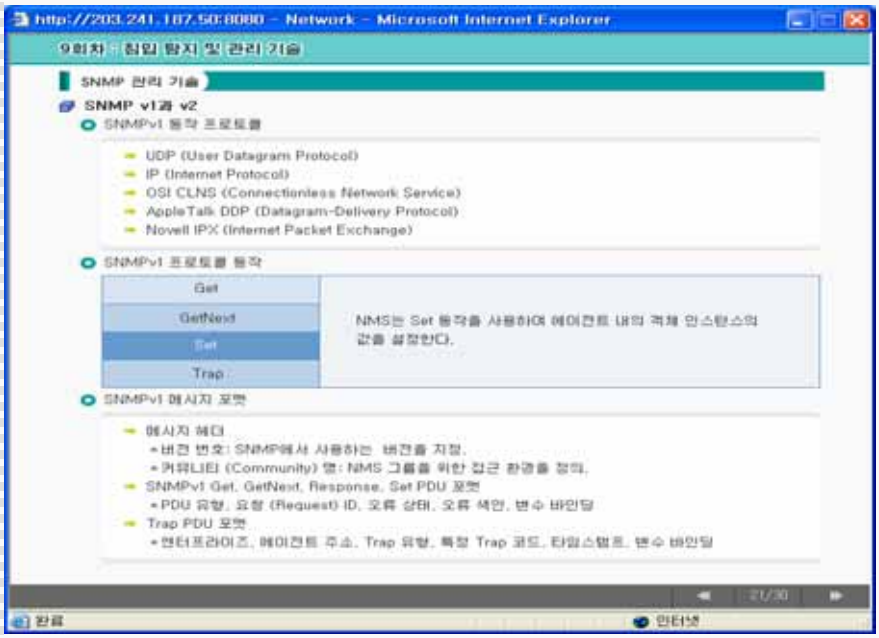
* 에이전트는 관리 장치 내에 있는 네트워크 관리 소프트웨어 모듈이다.
* 에이전트가 가지고 있는 관리 정보는 에이전트에서 만의 지역적 의미를 가지고 있으며, 따라서 이를 SNMP와 호환 가능한 형태의 정보로 변환하고 있다.

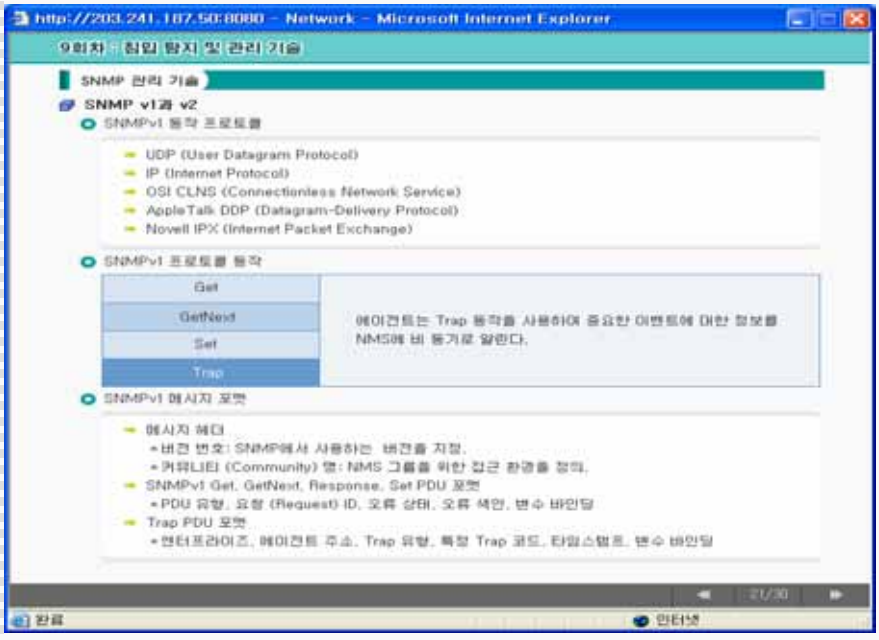
* 관리 장치는 SNMP 에이전트를 가지고 있는 네트워크 노드이며, 관리 네트워크 상에 존재한다.
* 관리 장치는 관리 정보를 수집/저장하고, 이 정보를 SNMP를 사용하여 NMS에 가용한 정보로 만든다.
* 라우터, 액세스 서버, 스위치, 브리지, 허브, 컴퓨터 호스트, 또는 프린터 등이 관리 장치가 될 수 있다.

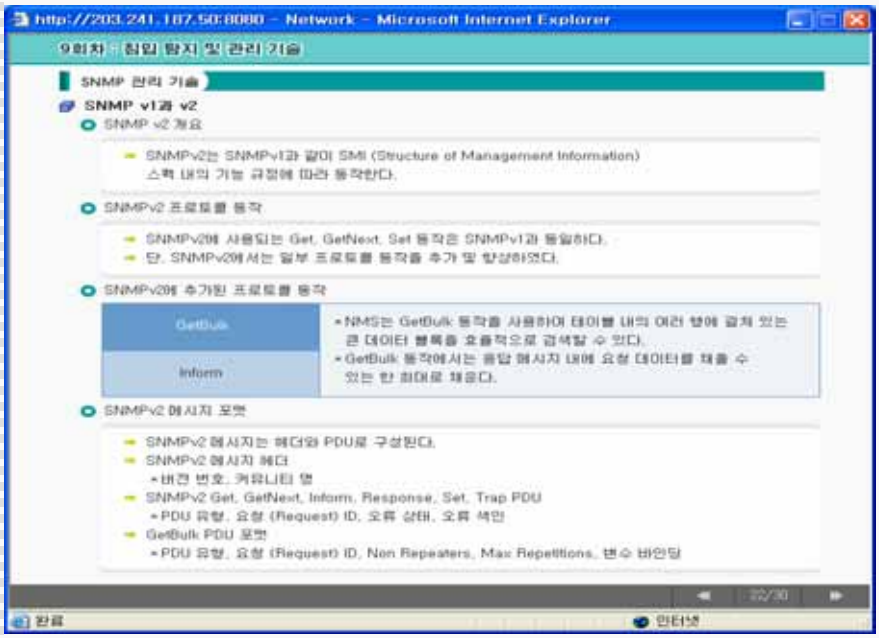



http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMPv1 동작 프로토콜
UDP (User Datagram Protocol)
IP (Internet Protocol)
OSI CLNS (Connectionless Network Service)
AppleTalk DDP (Datagram-Delivery Protocol)
Novell IPX (Internet Packet Exchange)
SNMPv1 프로토콜 동작
Get
GetNext
Set
Trap
NMS는 Get 동작을 사용하여 에이전트로부터 하나 이상의
객체 인스턴스의 값을 검색한다.
만약 Get 동작에 응답하는 에이전트가 목록 내의 모든 객체
인스턴스에 대한 값을 제공할 수 없다면,
에러한 값도 제공하지 않는다.
SNMPv1 메시지 포맷
메시지 헤더
• 버전 번호: SNMP에서 사용하는 버전을 지정.
• 커뮤니티 (Community) 명: NMS 그룹을 위한 접근 환경을 정의.
SNMPv1 Get, GetNext, Response, Set PDU 포맷
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인, 변수 바인딩
Trap PDU 포맷
• 엔터프라이즈, 에이전트 주소, Trap 유형, 특정 Trap 코드, 타임스탬프, 변수 바인딩
21/30
완료
인터넷

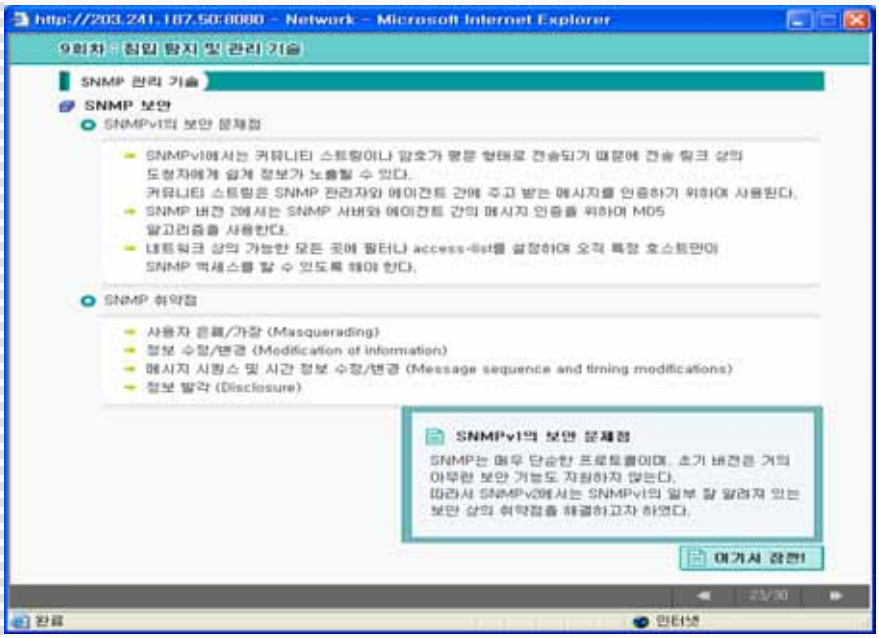

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMPv1 동작 프로토콜
UDP (User Datagram Protocol)
IP (Internet Protocol)
OSI CLNS (Connectionless Network Service)
AppleTalk DDP (Datagram-Delivery Protocol)
Novell IPX (Internet Packet Exchange)
SNMPv1 프로토콜 동작
Get
GetNext
Set
Trap
NMS는 GetNext 동작을 사용하여 에이전트에 있는 테이블이나
목록 내의 다음 번 객체 인스턴스의 값을 검색한다.
SNMPv1 메시지 포맷
메시지 헤더
• 버전 번호: SNMP에서 사용하는 버전을 지정.
• 커뮤니티 (Community) 명: NMS 그룹을 위한 접근 환경을 정의.
SNMPv1 Get, GetNext, Response, Set PDU 포맷
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인, 변수 바인딩
Trap PDU 포맷
• 엔터프라이즈, 에이전트 주소, Trap 유형, 특정 Trap 코드, 타임스탬프, 변수 바인딩
21/30
완료
인터넷

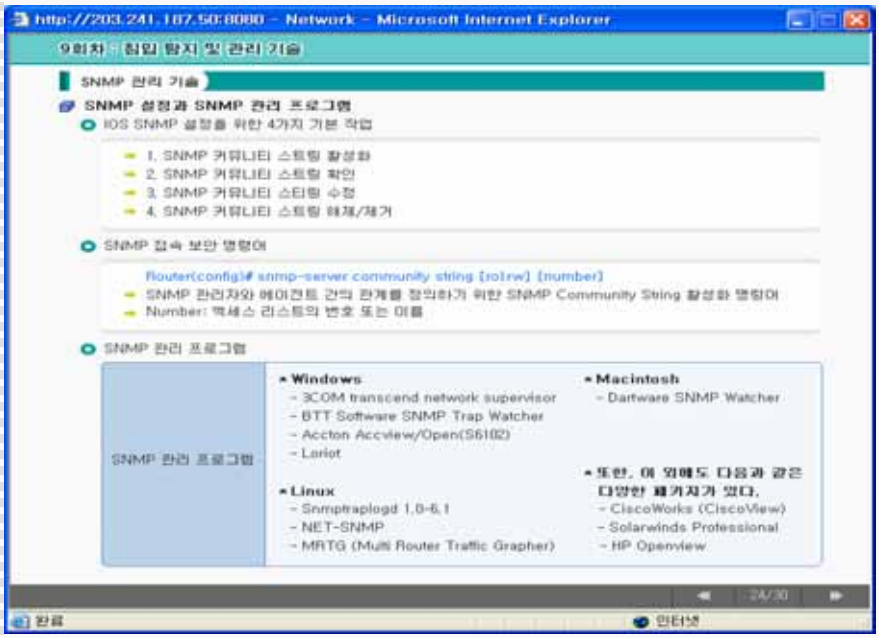

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMPv1 동작 프로토콜
UDP (User Datagram Protocol)
IP (Internet Protocol)
OSI CLNS (Connectionless Network Service)
AppleTalk DDP (Datagram-Delivery Protocol)
Novell IPX (Internet Packet Exchange)
SNMPv1 프로토콜 동작
Get
GetNext
Set
Trap
NMS는 Set 동작을 사용하여 에이전트 내의 객체 인스턴스의 값을 설정한다.
SNMPv1 메시지 포맷
메시지 헤더
• 버전 번호: SNMP에서 사용하는 버전을 지정.
• 커뮤니티 (Community) 명: NMS 그룹을 위한 접근 환경을 정의.
SNMPv1 Get, GetNext, Response, Set PDU 포맷
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인, 변수 바인딩
Trap PDU 포맷
• 엔터프라이즈, 에이전트 주소, Trap 유형, 특정 Trap 코드, 타임스탬프, 변수 바인딩
21/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMPv1 동작 프로토콜
UDP (User Datagram Protocol)
IP (Internet Protocol)
OSI CLNS (Connectionless Network Service)
AppleTalk DDP (Datagram-Delivery Protocol)
Novell IPX (Internet Packet Exchange)
SNMPv1 프로토콜 동작
Get
GetNext
Set
Trap
에이전트는 Trap 동작을 사용하여 중요한 이벤트에 대한 정보를 NMS에 비 동기로 알린다.
SNMPv1 메시지 포맷
메시지 헤더
• 버전 번호: SNMP에서 사용하는 버전을 지정.
• 커뮤니티 (Community) 명: NMS 그룹을 위한 접근 환경을 정의.
SNMPv1 Get, GetNext, Response, Set PDU 포맷
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인, 변수 바인딩
Trap PDU 포맷
• 엔터프라이즈, 에이전트 주소, Trap 유형, 특정 Trap 코드, 타임스탬프, 변수 바인딩
21/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMP v2 개요
SNMPv2는 SNMPv1과 같이 SMI (Structure of Management Information)
스펙 내의 기능 규정에 따라 동작한다.
SNMPv2 프로토콜 동작
SNMPv2에 사용되는 Get, GetNext, Set 동작은 SNMPv1과 동일하다.
단, SNMPv2에서는 일부 프로토콜 동작을 추가 및 향상하였다.
SNMPv2에 추가된 프로토콜 동작
GetBulk
Inform
• NMS는 GetBulk 동작을 사용하여 테이블 내의 여러 행에 걸쳐 있는
큰 데이터 블록을 효율적으로 검색할 수 있다.
• GetBulk 동작에서는 응답 메시지 내에 요청 데이터를 채울 수
있는 한 최대로 채운다.
SNMPv2 메시지 포맷
SNMPv2 메시지는 헤더와 PDU로 구성된다.
SNMPv2 메시지 헤더
• 버전 번호, 커뮤니티 명
SNMPv2 Get, GetNext, Inform, Response, Set, Trap PDU
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인
GetBulk PDU 포맷
• PDU 유형, 요청 (Request) ID, Non Repeaters, Max Repetitions, 변수 바인딩
22/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP v1과 v2
SNMP v2 개요
SNMPv2는 SNMPv1과 같이 SMI (Structure of Management Information)
스펙 내의 기능 규정에 따라 동작한다.
SNMPv2 프로토콜 동작
SNMPv2에 사용되는 Get, GetNext, Set 동작은 SNMPv1과 동일하다.
단, SNMPv2에서는 일부 프로토콜 동작을 추가 및 향상하였다.
SNMPv2에 추가된 프로토콜 동작
GetBulk
Inform
• Inform 동작을 이용하면, 하나의 NMS에서 다른 NMS로 trap 정보를
보내고 또한 이에 대한 응답을 받을 수 있다.
• SNMPv2에서는, GetBulk 동작에 응답하는 에이전트가 목록 내의 모든
변수에 대한 값을 제공할 수 없는 경우, 일부 결과 값만을 제공한다.
SNMPv2 메시지 포맷
SNMPv2 메시지는 헤더와 PDU로 구성된다.
SNMPv2 메시지 헤더
• 버전 번호, 커뮤니티 명
SNMPv2 Get, GetNext, Inform, Response, Set, Trap PDU
• PDU 유형, 요청 (Request) ID, 오류 상태, 오류 색인
GetBulk PDU 포맷
• PDU 유형, 요청 (Request) ID, Non Repeaters, Max Repetitions, 변수 바인딩
22/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 보안
SNMPv1의 보안 문제점
SNMPv1에서는 커뮤니티 스트링이나 암호가 평문 형태로 전송되기 때문에 전송 링크 상의 도청자에게 쉽게 정보가 노출될 수 있다.
커뮤니티 스트링은 SNMP 관리자와 에이전트 간에 주고 받는 메시지를 인증하기 위하여 사용된다.
SNMP 버전 2에서는 SNMP 서버와 에이전트 간의 메시지 인증을 위하여 MD5 알고리즘을 사용한다.
네트워크 상의 가능한 모든 곳에 필터나 access-list를 설정하여 오직 특정 호스트만이 SNMP 액세스를 할 수 있도록 해야 한다.
SNMP 취약점
사용자 은폐/가장 (Masquerading)
정보 수정/변경 (Modification of information)
메시지 시퀀스 및 시간 정보 수정/변경 (Message sequence and timing modifications)
정보 발각 (Disclosure)
SNMPv1의 보안 문제점
SNMP는 매우 단순한 프로토콜이며, 초기 버전은 거의 아무런 보안 기능도 지원하지 않는다.
따라서 SNMPv2에서는 SNMPv1의 일부 잘 알려져 있는 보안 상의 취약점을 해결하고자 하였다.
여기서 잠깐!
24/30
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
9회차 : 침입 탐지 및 관리 기술
SNMP 관리 기술
SNMP 설정과 SNMP 관리 프로그램
IOS SNMP 설정을 위한 4가지 기본 작업
1. SNMP 커뮤니티 스트링 활성화
2. SNMP 커뮤니티 스트링 확인
3. SNMP 커뮤니티 스트링 수정
4. SNMP 커뮤니티 스트링 해제/제거
SNMP 접속 보안 명령어
Router(config)# snmp-server community string [ro|rw] [number]
SNMP 관리자와 에이전트 간의 관계를 정의하기 위한 SNMP Community String 활성화 명령어
Number: 액세스 리스트의 번호 또는 이름
SNMP 관리 프로그램
SNMP 관리 프로그램
• Windows
- 3COM transcend network supervisor
- BTT Software SNMP Trap Watcher
- Accton Accview/Open(S6102)
- Loriot
• Linux
- Snmptraplogd 1.0-6.1
- NET-SNMP
- MRTG (Multi Router Traffic Grapher)
• Macintosh
- Dartware SNMP Watcher
• 또한, 이 외에도 다음과 같은 다양한 패키지가 있다.
- CiscoWorks (CiscoView)
- Solarwinds Professional
- HP Openview
24/30
완료
인터넷

End of Lecture