

FNS

(Fundamental Network Security)

Ch5. CBAC(Context-based Access Control)

hjlee@dongseo.ac.kr
<http://kowon.dongseo.ac.kr/~hjlee>
<http://crypto.dongseo.ac.kr>

2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

1

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5주차 : CBAC 기술

이번 강의의 학습목표를 살펴본도록 하겠습니다.

학 습 목 표

- ACL의 한계점을 이해하고 설명할 수 있다.
- CBAC의 개념과 동작 방법에 대하여 설명할 수 있다.
- CBAC를 이용하여 DoS 공격을 예방하는 방법을 설명할 수 있다.
- CBAC에 지원하는 프로토콜을 설명할 수 있다.
- CBAC의 구체적인 설정 방법을 설명할 수 있다.

완료 인터넷

2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

2

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC이란?

CBAC의 개요

- ACL의 한계점
 - ACL은 네트워크 보안을 위한 완전한 기능을 제공하지 못한다.

Cisco IOS ACLs 특징

- ACL은 명시적인 거부 문장으로 실행된다.
- 만약 인터페이스에 설정되지 않으면, 모든 연결은 기본적으로 허용된다.
- ACL은 다음의 방법으로 트래픽 필터링을 지원한다.
 - 발신자와 목적지 IP 주소
 - 발신자와 목적지 포트
- 필터링 방법을 구현하는데 사용할 수 있다.
- 포트는 정구히 트래픽을 허용하기 위해 열린다.
- 포트와 동적으로 협상하는 응용 프로그램과 작업하지 않는다.

CBAC의 개요

- CBAC는 방화벽을 통과하는 TCP와 UDP 트래픽을 허용하거나 거부한다.
- CBAC는 방화벽 인터페이스의 ACL에 일시 통로를 생성한다.
- 이러한 일시 통로는 특정 트래픽에 내부 네트워크로부터 방화벽을 통하여 외부로 나갈 때 생성되며, 방화벽을 나갈 때 CBAC를 trigger한 트래픽과 같은 세션에 속하는 트래픽만이 내부 네트워크로 들어올 수 있도록 허용한다.
- CBAC는 네트워크 자원을 DoS 공격으로부터 보호한다.

CBAC가 지원하는 프로토콜

- TCP/UDP (단일 채널)	- RPC
- FTP/TFTP	- UNIX R 명령어 (rlogin, rexec, rsh)
- SMTP	- HTTP (자바 플러그인)
- Java	- SQL*Net
- RTSP (RealNetworks)	- H.323 (NetMeeting, ProShare) 등등

2005-11-15 <http://kowon.dongseo.ac.kr/~hjee> 3

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC

CBAC의 동작

CBAC의 기본 동작

- CBAC는 어떤 프로토콜을 검사할 것인지, 어떤 인터페이스를 검사할 것인지, 그리고 검사를 실행할 인터페이스 방향에 라우터의 입력 방향인지 출력 방향인지 등을 규정한다.
- CBAC는 방화벽을 통해 들어오는 packets이 인터페이스의 inbound ACL을 통과할 경우에만 검사한다. 즉, packets이 ACL에서 거부된다면 해당 packets은 패기되어 CBAC 검사를 수행하지 않는다.
- CBAC는 연결 (connection)의 채 채널만을 검사하고 검사한다.

1 Control traffic is inspected by the CBAC rule.
ip inspect name FWIULE tcp

2 CBAC creates a dynamic ACL allowing return traffic back through the firewall.
access-list 102 permit TCP host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447

3 CBAC continues to inspect control traffic and dynamically creates and removes ACLs as required by the application. It also monitors and protects against application-specific attacks.

4 CBAC detects when an application terminates or times out and removes all dynamic ACLs for that session.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjee> 4

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5화차 : CBAC 기술

CBAC

CBAC의 동작

CBAC의 세션 상태 정보

- CBAC은 세션 상태 정보를 관리하기 위해 timeout과 threshold 값을 사용한다.
- 이 값을 환경하게 설정되지 않은 세션의 drop 여부를 결정하기 위해 사용된다.

Timeout과 DoS 예방

- Timeout 값은 half-open 세션의 수를 제어하여 시스템 자원의 사용량을 제어함으로써 DoS 공격을 예방한다.
- 세션이 drop되면, CBAC은 세션의 말쪽 종단(endpoint)의 발신자/수신자 값으로 reset 메시지를 보낸다.
- DoS 공격을 받고 있는 시스템은 reset 명령을 받을 때, 불완전한 세션과 관련된 프로세스와 자원을 해제 (release/free) 한다.

- CBAC은 DoS공격에 대응하여 3가지 threshold를 제공한다.
 - half-open TCP 또는 UDP 세션의 전체 개수
 - 시간 당 half-open 세션의 수
 - 시간 당 half-open TCP-only 세션의 수

Threshold 초과 시 동작 방법

만약 threshold가 초과되면, CBAC은 2가지 선택(option)을 할 수 있다.

- 가장 오래된 open 세션의 종단(endpoint)으로 reset 메시지를 보내고, 새롭게 도착하는 SYN 패킷에 대한 서비스가 가능한 자원을 생성한다.
- half-open TCP-only 세션의 경우, CBAC은 threshold 값에 의해 설정된 시간동안 모든 SYN 패킷을 일시적으로 막는다. 라우터가 SYN 패킷을 막을 때, TCP three-way handshake는 초기화되지 않는다. 이것은 유효한 연결을 위해 라우터가 메모리를 사용하거나 자원을 처리 (process)하는 것을 방지한다.

참고사항

half-open TCP
클라이언트와 서버에 TCP 연결을 설정하기 위해서는 three-way hand shake를 수행한다. 이 과정의 마지막 단계에서 클라이언트가 서버에게 ACK 메시지를 보내지 않은 상태를 말한다.
서버에서는 TCP 연결을 위해서 자신의 메모리에 (buffer)를 주고 받거나 연결 상태를 유지하기 위한 (buffer) 영역을 확보한다.
그런데, Half-open 상태가 계속 발생하게 된다면 결국 메모리는 부족하게 되고, 서버 시스템에서는 다른 공인버티 오는 모든 TCP 연결 요청을 거부하게 된다.

완료 인터넷

2005-11-15 5

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5화차 : CBAC 기술

CBAC 설정 방법

CBAC 기본 파라미터 설정 (Task 1과 Task 2)

감시 (audit trails) 기능과 경고 (alerts) 기능 설정

- Router(config)#ip inspect audit-trail
Syslog 서버를 활성화 시키고(enable) logging을 켜다 (turn on).

```
Router(config)# logging on
Router(config)# logging 10.0.0.3
Router(config)# ip inspect audit-trail
```

- Router(config)#[no] ip inspect alert-on
경보(Alert)는 켜거나 (turn on) 할 수 있다 (turn off).

완료 인터넷

2005-11-15 http://kowon.dongseo.ac.kr/~hj lee 6

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

CBAC 기본 파라미터 설정 (Task 1과 Task 2)

TCP, SYN, FIN Wait Times 설정

- Router(config)#ip inspect tcp synwait-time seconds
Cisco IOS 방화벽이 확립 상태에 이르기 위해 TCP 세션을 기다리는 시간을 명시한다. 디폴트로 30초이며 설정시간 후에 세션을 drop시킨다.
- Router(config)#ip inspect tcp finwait-time seconds
세션을 끝내기 전에 FIN 교환을 위한 대기 시간을 명시한다. 디폴트로 5초이다.
- Router(config)#ip inspect tcp idle-time seconds
Router(config)#ip inspect udp idle-time seconds
비활성 TCP와 UDP 세션을 위해 허용된 시간을 명시한다. TCP는 디폴트로 3600초이고 UDP는 30초이다.
- Router(config)#ip inspect dns-timeout seconds
비활성 DNS 세션을 위해 허용된 시간을 명시한다. 디폴트로 30초이다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 7

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

CBAC 기본 파라미터 설정 (Task 1과 Task 2)

Global half-open 연결 제한

- Router(config)#ip inspect max-incomplete high number
소프트웨어가 half-open 세션 삭제할 시작하는 half-open 세션 수를 정의한다.(aggressive mode)
디폴트 값은 500임.
- Router(config)#ip inspect max-incomplete low number
소프트웨어가 half-open 세션 삭제할 멈추는 half-open 세션 수를 정의한다.
디폴트 값은 400임.
- Router(config)#ip inspect one-minute high number
1 분당 새로운 half-open 세션 수를 정의하며, 이 수 이상의 세션이 발생할 경우 그 때부터의 세션은 삭제된다.
- Router(config)#ip inspect one-minute low number
1 분당 새로운 half-open 세션 수를 정의하며, 이 수 이하의 세션이 발생할 경우 세션 삭제는 종료된다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 8

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

CBAC 기본 파라미터 설정 (Task 1과 Task 2)

호스트에 의한 Global half-open 연결 제한

- Router(config)# ip inspect tcp max-incomplete host number block-time seconds
Cisco IOS 방화벽이 특정 호스트로의 half-open 세션 삭제 작업을 시작하기 전에, 동시에 존재할 수 있는 동일한 목적지 주소로 갖는 half-open TCP 세션 수를 정의한다.
- 특정 호스트로의 half-open 연결 수가 초과된 이후, 소프트웨어는 다음과 같은 방법에 의해 호스트 상의 half-open 세션을 삭제한다.
 - Block-time이 0 일 경우, 새로운 연결을 허용하기 위해 새로운 연결 요구 차단. 가장 오래된 half-open 세션을 삭제한다.
 - 만약 block-time이 0 이 아닐 경우, 모든 half-open 세션을 삭제하고 호스트로의 새로운 연결은 명시된 block time 동안 허용하지 않는다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjee> 9

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

PAM (Port-to-Application Mapping) (Task 3)

PAM 개요

- 종종 프로토콜에 대한 포트 번호 설정이 가능하다.
- CBAC은 일의의 포트에 설정할 응용 프로그램을 결정하기 위해 PAM을 사용한다.

사용자 정의 포트 매핑

- Router(config)#ip port-map appl_name port port_num
종종 프로그램에 포트 번호를 매핑한다.
- Router(config)#access-list permit acl_num ip_addr
Router(config)#ip port-map appl_name port port_num list acl_num
특정 호스트에 대하여, 응용 프로그램에 포트 번호를 매핑한다.
- Router(config)#access-list permit acl_num ip_addr wildcard_mask
Router(config)#ip port-map appl_name port port_num list acl_num
특정 네트워크에 대하여, 응용 프로그램에 포트 번호를 매핑한다.

해설

CBAC 설정을 위한 앞의 두 가지 작업을 완료한 후에는 PAM을 설정해야 한다. PAM은 네트워크 서비스나 애플리케이션에 대한 TCP/UDP 포트 번호의 커스텀 매핑이 가능하다. 포트 정보를 이용하여 PAM은 피어웨어 애플리케이션 별로 디폴트 포트를 설정하고, 이 정보를 이용하여 CBAC 기능이 지정되는 서비스는 표준 포트 번호가 아닌 포트 상에서 동작할 수가 있다. 즉, CBAC은 원래 잘 알려진 포트 (well-known port) 상의 애플리케이션 만 감시할 수 있는 제한이 있으나, PAM을 사용함으로써 특정 애플리케이션이나 서비스에 대한 제약이 가능해지는 특징을 가지게 된다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjee> 10

5회차 : CBAC 기술

CBAC 설정

PAM (Port-to-Application Mapping) (Task 3)

PAM 설정 작업 설명서

- Router#show ip port-map
모든 포트 매핑 정보를 보여준다.
- Router#show ip port-map appl_name
특정 호스트에 대하여, 응용 프로그램에 포트 번호를 매핑한다.
- Router#show ip port-map port port_num
특정 포트 상의 특정 응용 프로그램에 대한 포트 매핑 정보를 보여준다.
- 예제**
Router# sh ip port-map ftp
Default mapping: ftp port 21 : system defined
Host specific: ftp port 1000 in list 10 user

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 11

5회차 : CBAC 기술

CBAC 설정

검사 규칙 (Inspection Rules) 정의 (Task 4)

응용 프로토콜에 대한 검사 규칙

- 인터페이스에 적용 가능한 프로토콜 : tcp, udp, cuseeme, ftp, http, h323, netshow, rcmd, realaudio, rpc, smtp, sqlnet, streamworks, ftp, vdlive.
- alert, audit-trail, timeout은 프로토콜마다 설정 가능하고 전역 설정 (global settings)에 우선한다 (override).
- Router(config)#ip inspect name inspection-name protocol [alert {on|off}]
[audit-trail {on|off}] [timeout seconds]
검사할 응용 프로토콜을 정의한다.
- 예제**
Router(config)# ip inspect name FWRULE smtp alert on audit-trail on timeout 300
Router(config)# ip inspect name FWRULE ftp alert on audit-trail on timeout 300

해설

FWRULE이라는 이름을 갖는 검사 규칙을 5분의 제한 시간을 가지고 smtp 및 ftp 프로토콜에 적용하여 검사 규칙과 일치할 경우 syslog 서버에 로그 정보를 저장한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 12

5회차 : CBAC 기술

CBAC 설정

검사 규칙 (Inspection Rules) 정의 (Task 4)

RPC 응용에 대한 검사 규칙

```
Router(config)#ip inspect name inspection-name rpc
program-number number [wait-time minutes] [alert {on|off}] [audit-trail {on|off}]
[timeout seconds]
```

- 특정 RPC 프로그램 번호를 허용한다.
- Wait-time은 명시한 시간(분) 동안 해당 연결을 오픈 상태로 유지한다.

예제

```
Router(config)#ip inspect name FWRULE rpc program-number 100022
wait-time 5 alert off audit-trail on
```

해설

FWRULE이라는 이름의 검사 규칙을 100022번의 rpc 프로그램에 적용하되 검사 규칙과 일치할 경우 경고 메시지는 표시하지 않고 syslog 서버에 로그 정보를 저장한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 13

5회차 : CBAC 기술

CBAC 설정

검사 규칙 (Inspection Rules) 정의 (Task 4)

SMTP 응용에 대한 검사 규칙

```
Router(config)#ip inspect name inspection-name smtp [alert {on|off}] [audit-trail {on|off}]
[timeout seconds]
```

- SMTP 응용에서 다음과 같은 합법적인 명령어만을 허용한다
= DATA, EXPN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, VRFY.
- 이 기능이 disable 되어 있으면, 모든 SMTP 애플리케이션이 방화벽을 통과할 수 있게 되고, 이는 잠재적인 메일 서버 취약점 노출로 이어진다.

예제

```
Router(config)#ip inspect name FWRULE smtp
```

해설

FWRULE이라는 이름을 갖는 검사 규칙을 smtp 프로토콜에 적용한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 14

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

검사 규칙 (Inspection Rules) 정의 (Task 4)

IP 패킷 단편화 (fragmentation)에 대한 검사 규칙

- Router(config)#ip inspect name inspection-name fragment max-number timeout seconds
 - 단편화된 (fragmented) IP 패킷을 포함한 일련의 DoS 공격으로부터 호스트를 보호한다.
 - Max-number : 조립되지 않은 단편화된 IP 패킷의 최대 수.
디폴트로 256이고 범위는 50 ~ 10000 이다.
 - Timeout-seconds : 조립되지 않은 단편화된 IP 패킷이 폐기되기 (discarded) 시작하는 시간 (단위: 초).
디폴트로 1초이고 만일 타임아웃 설정값이 적절하다면 조립되지 않은 패킷을 바로 폐기한다.

예제

```
Router(config)# ip inspect name FWRULE fragment max 254 timeout 4
```

해설

FWRULE이라는 이름을 갖는 검사 규칙을 최대 254 개의 조립되지 않은 단편화된 IP 패킷에 적용하되, 검사 규칙에 일치한 순간의 4초 후 부터 조립되지 않은 단편화된 IP 패킷을 폐기한다.

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 15

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)

검사 규칙과 ACL 적용을 위한 일반적인 규칙

- 트래픽 검색이 시작되는 인터페이스
 - 특정 트래픽만을 허용하는 ACL을 라우터 입력 방향에 적용한다.
 - 특정 트래픽을 검사하는 규칙을 라우터 입력 방향에 적용한다.
- 모든 다른 인터페이스
 - 원하지 않는 모든 트래픽을 거부 (deny)하는 ACL을 라우터 입력 방향에 적용한다.

인터페이스에의 검사 규칙 적용 방법

```
Router (config-if)#ip inspect inspection-name {in | out}
```

일련의 인터페이스에 검사 규칙을 적용한다.

예제

```
Router(config)# interface s0/0
Router(config-if)# ip inspect FWRULE in
```

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 16

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

라우터 인터페이스에 검사 규칙과 ACL 적용 (Task 5)

세 개의 인터페이스를 가지고 있는 라우터에 검사 규칙과 ACL 적용 해주세요

Outbound

- Allow all general TCP and UDP traffic
- Allow all ICMP traffic
- Deny everything else

DMZ-Bound

- Allow all ICMP and HTTP traffic only to 172.16.0.2
- Deny everything else

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 17

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

라우터 인터페이스에 검사 규칙과 ACL 적용 (Task 5)

세 개의 인터페이스를 가지고 있는 라우터에 검사 규칙과 ACL 적용 해주세요

➤ Outbound Traffic

➤ Router(config)#ip inspect name OUTBOUND tcp
Router(config)#ip inspect name OUTBOUND udp
TCP와 UDP 트래픽 검사를 위한 CBAC을 설정한다.

➤ Router(config)#access-list 101 permit ip 10.0.0.0 0.0.0.255 any
Router(config)#access-list 101 deny ip any any
10.0.0.0 네트워크 내부에서 발생한 트래픽을 허용한다.

➤ Router(config)#interface e0/0
Router(config-if)#ip inspect OUTBOUND in
Router(config-if)#ip access-group 101 in
10.0.0.0 네트워크 내부에서 발생한 트래픽을 허용한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 18

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)

세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제

➤ Inbound Traffic

```

Router(config)#ip inspect name INBOUND tcp
Router(config)#access-list 102 permit icmp any host 172.16.0.2
Router(config)#access-list 102 permit tcp any host 172.16.0.2 eq www
Router(config)#access-list 102 deny ip any any
Router(config)#interface e0/1
Router(config-if)#ip access-group 102 in
  
```

TCP 트래픽 검사를 위한 CBAC을 설정한다.

호스트 172.16.0.2로 향하는 외부에서 발생한 ICMP와 HTTP 트래픽을 허용한다.

외부 인터페이스의 라우터 입력 방향에 ACL과 검사 규칙을 적용한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 19

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 CBAC 기술

CBAC 설정

라우터 인터페이스에의 검사 규칙과 ACL 적용 (Task 5)

세 개의 인터페이스를 가지고 있는 라우터에의 검사 규칙과 ACL 적용 예제

➤ DMZ-bound Traffic

```

Router(config)# access-list 103 permit icmp host 172.16.0.2 any
Router(config)# access-list 103 deny ip any any
Router(config)# access-list 104 permit icmp any host 172.16.0.2
Router(config)# access-list 104 permit tcp any host 172.16.0.2 eq www
Router(config)# access-list 104 deny ip any any
Router(config)# interface e1/0
Router(config-if)# ip access-group 103 in
Router(config-if)# ip access-group 104 out
  
```

DMZ에서 발생한 ICMP 트래픽만을 허용한다.

호스트 172.16.0.2로 향하는 라우터 출력 방향의 ICMP와 HTTP 트래픽만을 허용한다.

외부 인터페이스의 라우터 입력 방향에 ACL과 검사 규칙을 적용한다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 20

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

CBAC 테스트 및 확인 (Task 6)

- show 명령어
 - Router#show ip inspect name inspection-name
 - Router#show ip inspect config
 - Router#show ip inspect interfaces
 - Router#show ip inspect session [detail]
 - Router#show ip inspect all
 - CBAC 설정, 인터페이스, 인터페이스 설정, 세션을 표시한다.
- debug 명령어
 - Router(config)#debug ip inspect function-trace
 - Router(config)#debug ip inspect object-creation
 - Router(config)#debug ip inspect object-deletion
 - Router(config)#debug ip inspect events
 - Router(config)#debug ip inspect timers
 - 일반적인 debug 명령어들의 입력 형식이다.
 - Router(config)#debug ip inspect protocol
 - 특정 프로토콜에 관련된 debug 명령어 입력 형식이다.

해설
감사 기능 추적, 감사 객체 생성/삭제, 감사 이벤트, 감사 타이머 등의 각종 CBAC 이벤트에 대한 메시지를 화면에 표시하기 위해서는 debug ip inspect 실행 명령어를 사용한다.

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 21

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

CBAC 설정

CBAC 테스트 및 확인 (Task 6)

- CBAC 설정 제거 방법
 - Router(config)#no ip inspect
 - 전체 CBAC 설정을 제거한다.
 - 모든 지역 (global) timeouts과 thresholds 값을 디폴트 값으로 reset 한다.
 - 설정되어 있는 모든 세션을 삭제한다.
 - 연관된 (associated) 모든 dynamic ACL을 제거한다.

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 22

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer

5회차 : CBAC 기술

지금까지 공부한 내용을 요약하여 다시 한번 복습할 부분은 다시 한번 확인 하시기 바랍니다.

CBAC

CBAC은 방화벽을 통과하는 TCP와 UDP 트래픽을 허용하거나 거부하기 때문에 ACL과 유사하다. 그러나 CBAC은 방화벽을 통과하여 내부 네트워크로 들어가는 인터페이스의 ACL 내에 임시적인 통로가 동적으로 생성되거나 삭제된다는 점에서 ACL과 다르다.

CBAC의 동작

CBAC은 방화벽을 통해 들어오는 패킷이 인터페이스의 inbound ACL 테스트를 통과할 경우에만 검사한다. CBAC은 연결의 제어 채널만을 검사하고 검사한다. 응용 프로그램에 의해 요구된 트래픽이 라우터를 통해 다시 들어올 수 있도록 ACL을 동적으로 생성하고 제거한다.

CBAC 설정 단계

- 감사 (audit trails) 기능과 경고 (alerts) 기능 설정
- Global timeouts과 thresholds 설정
- PAM
- 검사 규칙 정의
- 라우터 인터페이스의 검사 규칙과 ACL 적용
- CBAC 테스트 및 확인

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.

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 23

http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer

Fundamental of Network Security

5회차 CBAC(Content-based Access Control) 기술

5회차 : CBAC 기술

이번 시간에 학습한 내용에 대해 정확한 이해했는지 학습평가를 통해 확인해 보도록 합니다.

1. 다음 중 DoS 공격에 대응하기 위해 사용할 수 있는 Cisco IOS의 특성은 것은?

- ⓐ Extended audit
- ⓑ CBAC
- ⓒ RDP
- ⓓ Reactive filtering

2005-11-15 http://kowon.dongseo.ac.kr/~hjlee 24

http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer

Fundamental of Network Security

5회차 CBAC(Context-based Access Control) 기술

학/습/시/작
학/습/목/표
1. CBAC란?
2. CBAC 설정 방법
프/정/정/리
학/습/타/지/기

이런 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합니다.

2. 다음 중 CBAC에 검사할 수 있는 공격의 형태가 아닌 것은?

- ① syn flooding
- ② fragmented IP packet
- ③ port scanning
- ④ buffer overflow

NETCHANNEL
Total e-Learning Solution Provider

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 25

http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer

Fundamental of Network Security

5회차 CBAC(Context-based Access Control) 기술

학/습/시/작
학/습/목/표
1. CBAC란?
2. CBAC 설정 방법
프/정/정/리
학/습/타/지/기

이런 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합니다.

3. 다음 중 CBAC에 의해 차단되지 않는 프로토콜은 어느것인가?

- ① SMTP
- ② RTSP
- ③ SNMP
- ④ FTP

NETCHANNEL
Total e-Learning Solution Provider

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 26

http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer

Fundamental of Network Security

5회차 CBAC(Context-based Access Control) 기술

5회차 : CBAC 기술

이전 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합니다.

4. 다음 중 콘솔에 대한 CBAC alert 메시지를 turn off 하는 명령은 무엇인가?

- ① Router(config)#ip inspect alert-off
- ② Router(config)#no ip inspect alert
- ③ Router(config)#ip inspect alert-off
- ④ Router(config)#ip inspect alert log-only

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 27

http://www.e-training.co.kr - Untitled Document - Microsoft Internet Explorer

Fundamental of Network Security

5회차 CBAC(Context-based Access Control) 기술

5회차 : CBAC 기술

이전 시간에 학습한 내용에 대해 정확히 이해했는지 학습평가를 통해 확인해 보도록 합니다.

5. 다음 중 PAM을 이용하여 네트워크의 관리자 계정을 관리하는 방법은 무엇인가?

- ① 응용 프로그램에 등록한 (well-known) 포트에 자동 접속을 시도할 수 있다.
- ② 응용 프로그램을 등록하지 않은 (non-registered) 포트에 접속할 수 있다.
- ③ 여러 개의 응용 프로그램을 하나의 단일 검사 포트에 접속할 수 있다.
- ④ 임의의 응용 프로그램으로부터의 다음 패킷을 하나의 단일 검사 포트에 접속할 수 있다.

2005-11-15 <http://kowon.dongseo.ac.kr/~hjlee> 28

End of Lecture



2005-11-15

<http://kowon.dongseo.ac.kr/~hjlee>

29