2주차 3차시 세션관리, 접근제어

【학습목표】

1. 세션관리의 개념을 설명할 수 있으며, 응용할 수 있다.
2. 접근제어관리의 개념을 설명할 수 있으며, 응용할 수 있다.

학습내용1 : 세션 관리의 개념과 응용

1. 세션의 예

영화관에서 줄을 서고 있다가 콜라를 사오고 싶을 때
차례(세션)를 유지하기 위해 뒷사람이나 친구에게
자리를 맡아 달라고 부탁하고 콜라를 사오는 것과
같은 경우를 클라이언트 측면에서의 세션으로
볼 수 있다.

만약 뒷사람이나 친구가 자신을 기억하고
다시 자리에 넣어주면 세션을 유지하는데
성공 한 것이고, 그들이 자리에 끼워주지 않는다면
클라이언트 측면에서의 사용자의 세션은
실패한 것이다.

2. 세션의 개념

1) 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 접속
- 오두막 집에서 오누이는 일을 나가신 어머니를 기다리는데 호랑이가 어머니와 비슷한 목소리로 문을 열어달라고 할 때 어머니인지 확인하기 위해 문 안으로 손을 넣어보라고 한다.

[그림 2-8] 서버 입장에서 세션을 유지하는 방법

3. 데이터베이스

1) 일반적으로 세션에 대한 타임아웃을 적용하지 않음

2) 데이터베이스는 사람이 접근하는 경우도 있지만 대부분 시스템 간의 세션을 가지고 있기 때문

3) 만약 타임아웃을 적용시키면 시스템 간 통신이 없을 때마다 사람이 다시 연결해야 함

4. 웹 서비스

1) 웹서비스를 이용할 때도 '지속적인 인증'은 적용됨

2) 인터넷뱅킹을 할 때 공인인증서의 패스워드나 보안카드의 숫자를 반복해 물어보는 경우

3) 혹은 시스템에서 패스워드를 변경할 때 원래의 패스워드를 묻는 경우

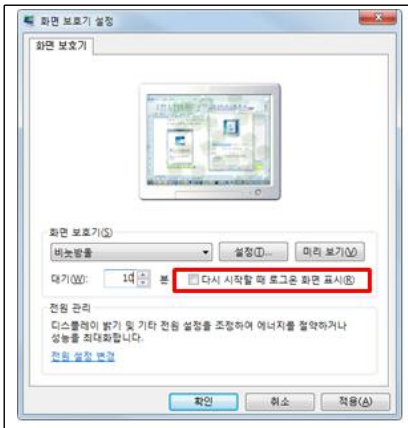
4) 패스워드 기간이 만료되어 재설정을 요구하는 경우가 이에 해당함

5. 세션에 대한 지속적인 인증 (Continuous Authentication)

1) 상황
① 어떤 사용자가 인증 절차를 거쳐 시스템에 접근하는 데 성공함
② 얼마 후 같은 아이디로 시스템에 접근하는 사용자가 처음 인증에 성공한 그 사용자인지 확인하기 위해 지속적으로 재인증을 수행해야 함
③ 그러나 지속적인 인증이라고 해서 명령어 한 줄을 입력할 때마다 패스워드를 입력하게 할 수는 없음
④ 시스템에서는 이러한 문제를 세션에 대한 타임아웃 설정으로 보완함

6. 세션의 의미

1) 세션을 유지하기 위한 보안 사항
① 세션 하이재킹(Session Hijacking)이나 네트워크 패킷 스니핑(Sniffing)에 대응하기 위해 암호화를 하는 것
② 세션에 대한 지속적인 인증(Continuous Authentication)을 하는 것



[그림 2-9] 윈도우 화면 보호기 설정

학습내용2 : 접근제어 관리의 개념과 응용

1. 접근 제어의 의미

1) 접근 제어(Access Control)는 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것

2) 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단

3) 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트이다.

2. 운영체제의 접근 제어

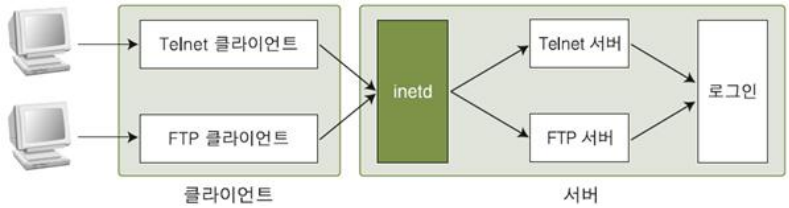
1) 운영체제에 어떤 관리적 인터페이스가 운영되고 있는지 알아보자.

[표 2-2] 일반적으로 사용되는 관리 인터페이스

운영체제	서비스 이름	사용 포트	특징
유닉스 (리눅스 포함)	텔넷(Telnet)	23	암호화되지 않음
	SSH	22	SFTP 가능
	XDMCP	5000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴	-	VNC, Radmin 등

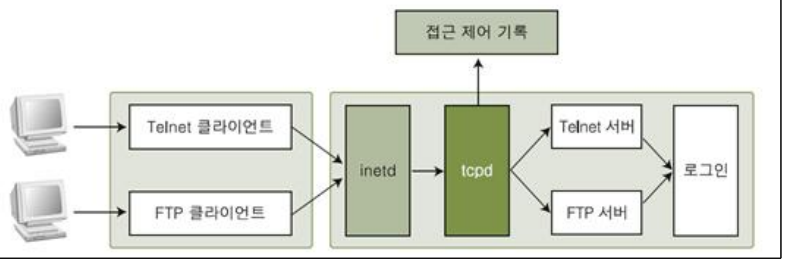
2) Inetd 데몬은 클라이언트로부터 inetd가 관리하고 있는 Telnet이나 SSH, FTP 등에 대한 연결 요청을 받은 후 해당 데몬을 활성화시켜 실제 서비스를 하는, 데몬과 클라이언트의 요청을 연결시켜주는 역할을 함.

[그림 2-10] inetd 데몬을 통한 데몬 동작도



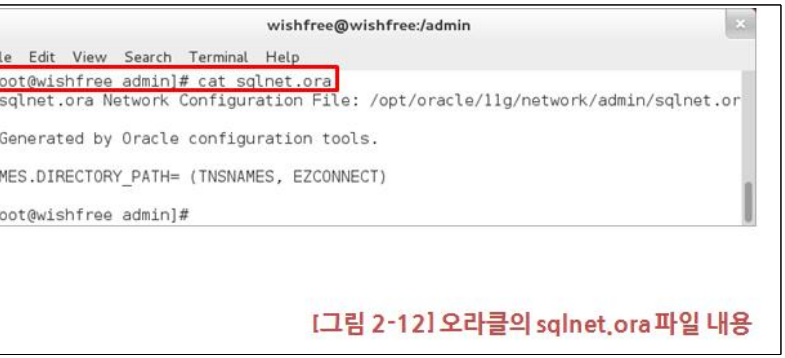
3) TCPWrapper가 설치되면, inetd 데몬은 연결을 TCPWrapper의 tcpd 데몬에 넘겨줌. tcpd 데몬은 접속을 요구한 클라이언트에 적절한 접근 권한이 있는지 확인한 후 해당 데몬에 연결을 넘겨주며, 이때 연결에 대한 로그도 실시할 수 있음.

[그림 2-11] TCP Wrapper를 통한 데몬 동작도



3. 데이터베이스의 접근 제어

1) 오라클은 $ORACLE_HOME/network/admin/sqlnet.ora 파일에서 설정



[그림 2-12] 오라클의 sqlnet.ora 파일 내용

2) 200.200.200.100과 200.200.200.200이라는 두 IP의 접근을 허용하고 싶으면 ①과 같이, 200.200.200.150의 접근을 차단하고 싶으면 ②와 같이 추가

❶ tcp.invited_nodes=(200.200.200.100, 200.200.200.200)
❷ tcp.excluded_nodes=(200.200.200.150)

MS-SQL은 IP에 대한 접근 제어를 기본으로 제공하지 않음.

4. 응용 프로그램의 접근 제어

1) 최근의 상용 응용 프로그램은 IP에 대한 접근 제어를 제공하는 경우가 많음
- 웹 서비스를 제공하는 IIS와 아파치 역시 IP에 대한 접근 제어를 제공

2) SSL(Secure Socket Layer)은 클라이언트와 서버 인증서를 이용하여 접근 제어를 수행할 수도 있다.
- SSL : 우선 보안접속 이라는 것은 ssl을 통해 정보를 전달하는 방식을 말합니다.
- 웹서버 인증, 서버 인증이라고도 합니다.
- 브라우저와 서버간의 통신에서 정보를 암호화 함으로써 도중에 해킹을 통해 정보가 유출 되더라도 정보의 내용을 보호할 수 있게 해 주는 보안 솔루션입니다.
- SSL은 별도의 프로토콜이 아니며. Email, 텔넷, FTP와 같은 다른 응용 프로토콜의 하부 계층 프로토콜로서 사용되고

있습니다.

5. 네트워크 장비의 접근 제어

1) 네트워크 장비에서 수행하는 IP에 대한 접근 제어로는 관리 인터페이스의 접근 제어와 ACL(Access Control List)을 통한 네트워크 트래픽 접근 제어가 있음
- ACL(Access Control List) 개개의 사용자들이 디렉토리나 파일과 같은 특정 시스템 개체에 접근할 수 있는 권한을 컴퓨터의 운영체계에 알리기 위해 설정해 놓은 표라고 할 수 있다. 각 개체는 접근제어목록을 식별할 수 있는 보안 속성을 가지며, 그 목록은 접근권한을 가진 각 시스템 사용자들을 위한 엔트리를 가진다.
- 가장 일반적인 권한은 1개의 파일이나 또는 한 개의 디렉토리 안에 있는 모든 파일들을 읽을 수 있고(Read), 기록할 수 있으며(Write), 그리고 만약 그것이 실행가능한 파일이나 프로그램인 경우라면 실행시킬 수 있는(Execute) 권한 등을 포함한다.

2) 네트워크 장비의 관리 인터페이스에 대한 접근 제어는 유닉스의 접근 제어와 거의 같음.

3) ACL을 통한 네트워크 트래픽에 대한 접근 제어는 방화벽에서의 접근 제어와 기본적으로 같음

【학습정리】

1. 세션은 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 접속을 의미하며 지속적인 인증이 필요하다.

2. 접근 제어(Access Control)는 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것을 의미하며 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단이다.

3. 접근제어의 응용에는 운영체제 접근제어, 데이터베이스 접근제어, 응용프로그램 접근제어, 네트워크장비 접근제어 등이 있다.