3주차 3차시. 윈도우의 계정과 권한 상승

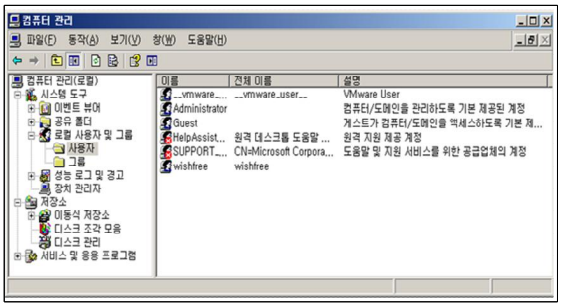
【학습목표】

1. 윈도우 계정 및 권한에 대해 알고, 권한상승과 획득에 대해 설명할 수 있다.

학습내용1 : 윈도우의 계정과 권한 체계

1. 윈도우 사용자 확인

* [제어판]→[컴퓨터 관리]의 [로컬 사용자 및 그룹]



2. 윈도우 기본 사용자

계정 이름	설명
SYSTEM	시스템에서 최고 권한을 가진 계정 로컬에서 관리자보다 상위 권한 원격 접속이 불가능 사용자는 이 계정을 사용하여 시스템에 로그인할 수 없음
Administrator	관리자 권한의 계정 사용자가 사용 가능한 계정 중 가장 강력한 권한
Guest	매우 제한적인 권한을 가진 계정 기본 설정은 사용 불능

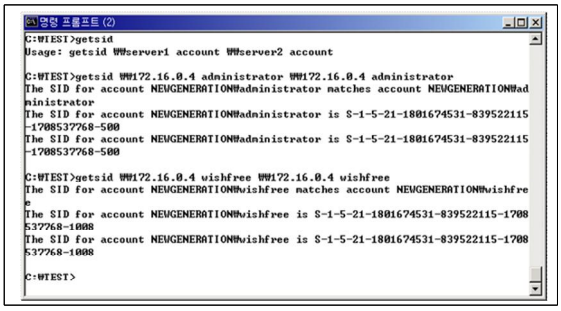
3. 윈도우 기본 그룹

그룹 이름	설명
Administrator	도메인 자원이나 로컬 컴퓨터에 대한 모든 권한
Account Operator	사용자나 그룹 계정을 관리하는 그룹
Backup Operator	시스템 백업을 위해서 모든 시스템의 파일과 디렉터리 접근 가능
Guest	도메인 사용 권한이 제한된 그룹
Print Operator	도메인 프린터에 접근 가능한 그룹

그룹 이름	설명
Power Users	디렉터리나 네트워크 공용, 공용 프로그램 그룹 생성, 컴퓨터의 시계 설정이 가능한 그룹
Replicator	도메인에 있는 파일을 복제할 수 있는 권한을 가진 그룹
Server Operator	도메인의 서버를 관리할 수 있는 권한을 가진 그룹
Users	도메인과 로컬 컴퓨터를 일반적으로 사용하는 그룹

4. SID(Security Identifier)

* 계정을 하나의 코드 값으로 표시



*** 설명**

The SID for account NEWGENERATION₩administrator is

S-1-5-21-1801674531-839522115-1708537768-500

❶ ❷ ❸ ❹

① 해당 시스템이 윈도우 시스템이라는 것을 의미
② 시스템이 도메인 컨트롤러이거나 단독 시스템(Stand alone system)임을 표시
③ 시스템의 고유한 숫자, 시스템을 설치할 때 시스템의 특성을 수집하여 생성
④ 숫자로 표현되는 각 사용자의 고유한 ID
> 관리자(Administrator)는 500번
> Guest 계정은501번
> 일반 사용자는 1000번 이상의 숫자를 가짐

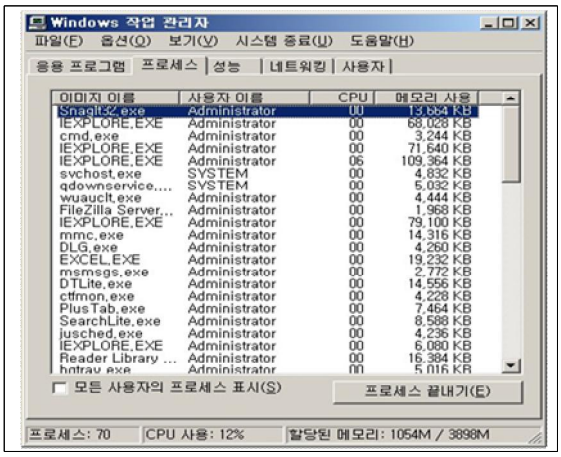
학습내용2 : 윈도우의 권한 상승

1. 정의

SetUID와 같은 기능은 없지만 리눅스/유닉스와 근본적으로 동일
윈도우의 권한 상승은 수행되는 상위의 프로세스 권한을 얻어 타는 것
일반 권한의 사용자가 Administrator와 SYSTEM으로 실행되고 있는 프로세스의 권한을 빼앗는 것

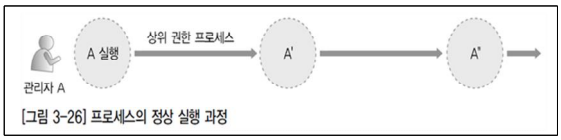
2. 권한 상승을 위한 계정의 프로세스 확인

Administrator와 SYSTEM으로 실행되는 프로세스 확인
Ctrl + Alt + Del 눌러 Windows 작업 관리자 창을 띄워 [프로세스] 탭을 확인



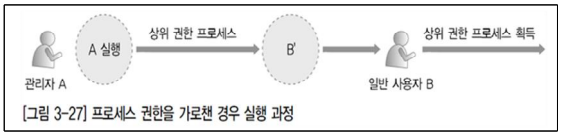
3. 윈도우의 권한 상승 실행 과정

* 수행되고 있는 프로세스의 권한을 빼앗는 방법
① 관리자 A와 일반 사용자 B가 있을 때, 정상적인 경우에 A가 A라는 프로그램을 실행하면 A'와 A"라는 프로그램상의 실행 절차를 거쳐 프로그램이 완료



[그림 3-26] 프로세스의 정상 실행 과정

② 여기에 일반 사용자 B가 A'를 B'로 바꿔 넣고 자신이 A를 실행하여 생성한 상위 권한 프로세스를 가로채는 것



[그림 3-27] 프로세스 권한을 가로챈 경우 실행 과정

학습내용3 : SYSTEM 권한 획득

1. 주제 / 참고

주제
SYSTEM 권한 획득
참고
· 한빛미디어
· 정보 보안 개론과 실습: 시스템 해킹과 보안
· 157페이지
· 실습 3-3. SYSTEM 권한 획득

2. SYSTEM 권한

* 윈도우의 계정 중 최고 권한
* 사용자가 아닌 운영체제가 자체 소유하는 권한
* 윈도우 사용자 해킹

해킹을 통해 윈도우의 SYSTEM 권한 획득
윈도우 XP의 작업 스케줄링 명령 at는 SYSTEM 권한으로 실행되며 이를 통해 SYSTEM 권한 회득 가능

3. at를 통한 프로그램 등록

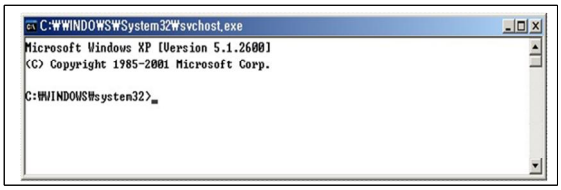
cmd.exe가 21:00에 실행되도록 작업을 등록
> at
> at 21:00 /interactive “cmd.exe”

4. SYSTEM 권한 획득

* 정해진 시간(21:00)에 명령 창이 실행 됨
* 명령창의 라벨 확인

일반적인 명령 창 라벨> C:₩WINDOWS₩system32₩cmd.exe
at를 통한 명령 창 라벨> C:₩WINDOWS₩system32₩svhost.exe

* 명령창의 라벨 확인



* scvhost.exe

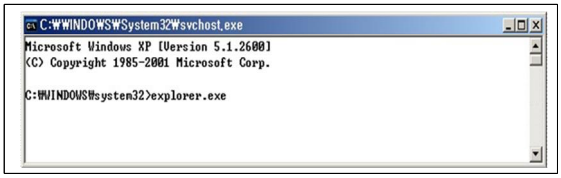
윈도우에서 SYSTEM 계정으로 실행되는 프로세스
at 명령으로 실행한 명령 창이 SYSTEM 권한을 가져온 것

5. SYSTEM 권한의 확장

* Ctrl + Alt + Del 눌러 Windows 작업 관리자 창을 띄워 [프로세스] 탭을 확인
* explorer.exe 프로세스 종료(프로세스 끝내기 버튼)
* explorer.exe 프로세스 종료(프로세스 끝내기 버튼)

* explorer.exe 종료
시스템 화면이 모두 사라짐
at 명령으로 띄운 명령 창만 남게 됨

* SYSTEM 권한으로 explorer.exe 실행
at 명령으로 띄운 명령 창에서 explorer.exe 실행



* SYSTEM 권한 확인
[시작] 버튼을 눌러 현재 계정을 확인

【학습정리】

1. 윈도우의 사용자는 Administrator, SYSTEM, Guest로 나뉜다.

2. 윈도우는 계정의 역할에 따라서 그룹을 Administrator, Account Operators, Backup Operators, Guests, Print Operators, Power Users, Replicator, Server Operators, Users로 나눈다.