

# 원격 레지스트리 접근 취약점 및 대응기법 분석 보고서

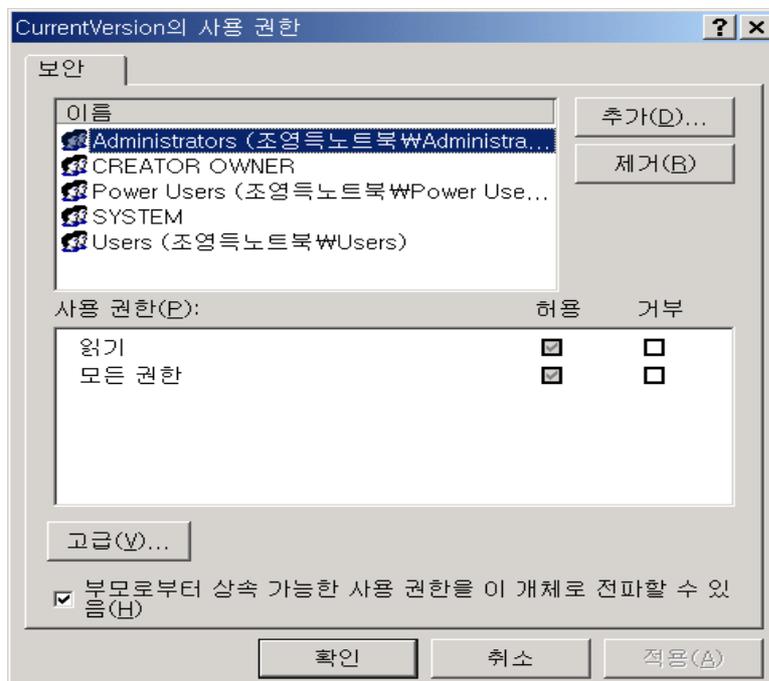
2003. 5



※ 본 문서는 관리기관의 취약점 보호대책 수립을 위해 작성된 것이므로 타 용도로 배포 및 사용을 금지합니다.

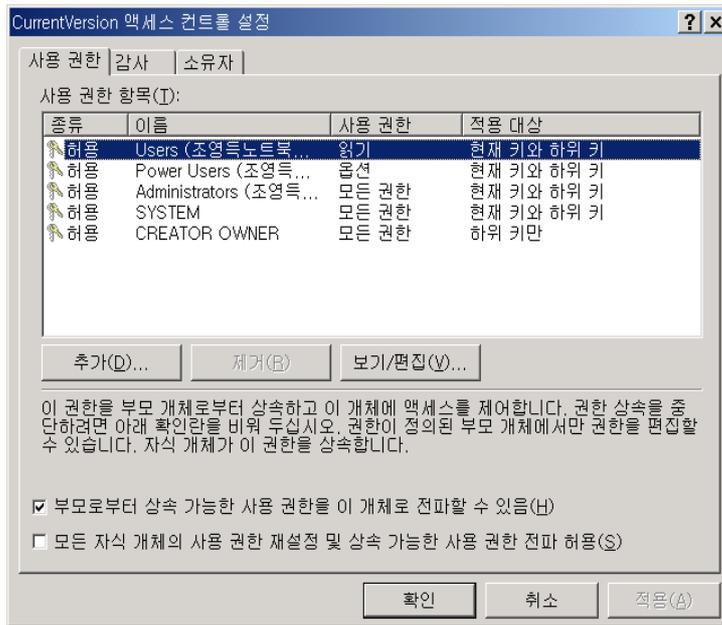
## 원격 레지스트리 접근 보호 방법

1. 레지스트리 보안을 위해서는 레지스트리에 적절한 ACL 을 설정한다.  
먼저 레지스트리 ACL 을 설정하기 위해서 regedt32 를 실행한다.
2. 해당 레지스트리키에 대하여 보안을 설정하기 위하여 regedt32 창>보안>사용권한을 실행하면 다음과 같은 대화상자가 열리며 이 곳에서 사용자를 추가하거나 삭제한다.



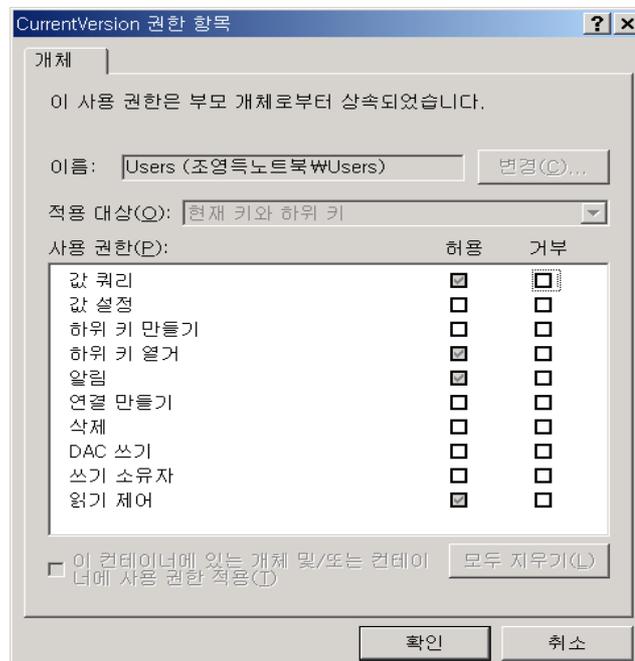
[레지스트리 사용권한 설정]

3. 해당 레지스트리 키에 대한 사용자의 액세스를 컨트롤 하기 위해서는 대화상자의 고급버튼을 클릭하면 액세스 컨트롤을 설정할 수 있는 대화창이 열린다. 이 대화창에서 각 사용자에 대한 레지스트리의 접근 권한을 상세히 적용할 수 있다.



[레지스트리 액세스 컨트롤 설정]

4. 위 액세스 컨트롤 설정 대화창에서 사용자를 선택하여 클릭하면 아래와 같이 사용권한을 설정할 수 있다.



[그림 1-8] 레지스트리 사용권한 항목

5. 원격에서 레지스트리의 접근을 통제하기 위하여 Winreg 를 이용하여 레지스트리에 대한 네트워크 액세스를 제한한다. 먼저 레지스트리에 winreg 를 추가한다.

하이브	HKEY_LOCAL_MACHINE \SYSTEM
키	\CurrentControlSet\Control\SecurePipeServers
값 이름	\winreg

6. 다음에 윈도우 시작>실행에서 regedt32 를 실행한다. Regedt32 화면에서 winreg 를 선택하고, "보안" 메뉴를 선택한 다음, "사용 권한"을 선택한다.
7. 적용하려는 ACL 을 추가하거나 삭제한다. 이 키에 적용되는 사용권한은 네트워크를 통하여 레지스트리에 접근할 수 있는 사용자와 그룹을 결정한다. 기본적으로 administrators 그룹은 모든 권한을 가진다. 새로운 사용자나 그룹에 대해서는 이 목록에 추가하여 원하는 대로 사용 권한을 설정 할 수 있다.

# 목 차

<b>1. 개요</b> .....	<b>8</b>
1.1 관련 용어.....	8
1.2 관련 설명.....	9
1.3 관련 시스템.....	18
<b>2. 취약점 유형 및 보호대책</b> .....	<b>19</b>
2.1 원격 레지스트리 접근 인증 취약점.....	19
2.2 Exchange 2000 System Attendant의 부정확한 원격 레지스트리 권한 설정 취약점 ....	26
2.3 상대 셸 경로 취약점.....	30
2.4 패스워드 취약점 및 퍼미션 설정 취약점.....	32
2.5 컴퓨터관리콘솔에 의한 원격 접근 취약점.....	42
2.6 백오리피스 등 트로이목마를 이용한 원격 레지스트리 접근 취약점.....	46
<b>3. 참고자료</b> .....	<b>50</b>

## 그림 목차

[그림 1-1] HKEY_CLASSES_ROOT 예시 .....	12
[그림 1-2] HKEY_CURRENT_USER 예시 .....	12
[그림 1-3] HKEY_LOCAL_MACHINE 예시 .....	13
[그림 1-4] HKEY_USERS 예시 .....	13
[그림 1-5] HKEY_CURRENT_CONFIG 예시 .....	14
[그림 1-6] 레지스트리 사용권한 설정 .....	15
[그림 1-7] 레지스트리 액세스 컨트롤 설정 .....	16
[그림 1-8] 레지스트리 사용권한 항목 .....	16
[그림 1-9] reg를 이용한 실행중인 서비스 검색 .....	18
[그림 2-1] reg를 이용한 원격 레지스트리 내용 조회 .....	19
[그림 2-2] winfingerprint를 이용한 사용자 액세스 권한 조회 .....	20
[그림 2-3] winfingerprint를 이용한 조회 결과 .....	21
[그림 2-4] reg를 이용한 레지스트리 내용 추가 결과 .....	25
[그림 2-5] winreg 사용권한 점검 .....	27
[그림 2-6] winreg 액세스 컨트롤 설정 .....	27
[그림 2-7] 공격대상 호스트의 레지스트리값 추가 결과 .....	28
[그림 2-8] 원격지에서 텔넷 접속 .....	29
[그림 2-9] shell 레지스트리 엔트리 .....	30
[그림 2-10] 패스워드 목록 .....	33
[그림 2-11] for를 이용한 세션 연결 .....	34
[그림 2-12] for를 이용한 세션 연결 결과 .....	34
[그림 2-13] LC3를 이용한 취약한 패스워드 점검 .....	35
[그림 2-14] dumpsec을 이용한 계정정책 등의 각종 정책 점검 .....	35
[그림 2-15] 원격지에서 NAT을 이용한 취약한 패스워드 점검 .....	35
[그림 2-16] DumpSecdmf 이용한 파일 퍼미션 설정 점검 .....	36
[그림 2-17] NAT를 이용한 사용자 계정 및 패스워드 크랙 .....	39
[그림 2-18] NAT를 이용한 사용자 계정 및 패스워드 크랙 결과 .....	40
[그림 2-19] DumpSec을 이용한 레지스트리 dump .....	40
[그림 2-20] 공유디렉토리에 대한 퍼미션 DUMP .....	41
[그림 2-21] 파일시스템에 대한 퍼미션 DUMP .....	41
[그림 2-22] 레지스트리에 대한 퍼미션 DUMP .....	41

[그림 2-23]	컴퓨터 관리 콘솔을 이용한 원격 컴퓨터 연결 .....	42
[그림 2-24]	원격 컴퓨터 연결 결과 .....	43
[그림 2-25]	컴퓨터 관리콘솔에서 원격컴퓨터 시스템 종료 .....	43
[그림 2-26]	백오리피스를 이용하여 공격대상서버 레지스트리 열람 .....	47
[그림 2-27]	백오리피스를 이용하여 공격대상서버 레지스트리값 변경 ....	47
[그림 2-28]	백오리피스 서버 환경설정 .....	49
[그림 2-29]	백오리피스를 이용한 레지스트리 생성 .....	49

## 1. 개요

### 1.1 관련 용어

- 레지스트리

레지스트리는 윈도우를 실행하는데 필요한 모든 환경설정 데이터를 모아 두는 중앙 저장소를 말한다. 시스템에 설치되어 있는 랜카드나 디스플레이 어댑터등에 대한 정보나 응용프로그램에 대한 정보, 디바이스, 사용자 설정, 윈도우 자체적인 설정, 인터넷 익스플로러 설정등 윈도우의 모든 설정이 담겨져 있다. 윈도우를 설치하면 윈도우관련 설정값들이 레지스트리에 저장되며 추가적으로 설치하는 장치나 프로그램이 있을 때마다 그 정보가 추가된다. 그래서 장치와 프로그램이 많아질수록 레지스트리 덩치가 커지고 복잡해지게 된다. 또한 그런 장치나 프로그램들을 제거할 때에는 레지스트리에서 삭제되게 되어 있다. 그러나 사용자의 실수나 시스템 환경에 따라 레지스트리에서 제거되지 못하고 잔존함으로써 시스템 오류나 문제를 일으킨다.

- 컴퓨터 관리 콘솔

컴퓨터 관리 콘솔은 Microsoft Management Console (MMC)의 snap-in 몇 개를 묶어놓은 것으로 한번에 여러가지를 살펴볼 수 있어 편리하다. 컴퓨터 관리 콘솔은 이벤트 뷰어를 살펴보고, 공유 폴더를 다루고, 장치 관리자를 열어볼 수 있고, 사용자 계정을 새로 만들 수 있고, 디스크 파티션을 만들어 포맷할 수 있고, NT 서비스를 멈추거나 시작할 수 있는 등 여러가지 시스템 관리 도구가 모여 있다. 또한 컴퓨터 관리 콘솔로 로컬 컴퓨터 뿐만 아니라 같은 peer-to-peer network 에 있는 다른 Windows 2000 컴퓨터도 원격으로 다룰 수 있다. 예를 들면 사무실에서 컴퓨터를 잘 다루지 못하는 동료 직원이 공유 폴더 만들기를 어려워 하거나 무슨 서비스를 시작하라고 해도 알아듣지 못할 때 앉은 자리에서 바로 도와줄 수 있고 필요하면 원격으로 로그오프하거나 컴퓨터를 셧다운할 수도 있다.

- 원격 레지스트리 접근

원격에서 레지스트리를 접근하는 것은 원격지에 있는 컴퓨터를 한곳에서 집중관리하기 위한 목적이었다. 이를 위해서 관리자는 컴퓨터관리 콘솔을 이용하거나 reg.exe 와 같은 도구를 이용한다. 원격 컴퓨터를 관리하기 위해서는 먼저 원격 컴퓨터에 로컬 로그인 할 수 있는 사용자 계정이 있어야 한다. 윈도우 NT 3.5.1 이전 버전에서는 누구나 원격 레지스트리에 접근할 수 있었지만 윈도우

NT4 이후에는 보안을 위하여 administrators 그룹에 속한 사용자만이 원격 레지스트리에 접근할 수 있도록 되어 있다.

현재 로컬 컴퓨터에 로그인한 계정이 Administrators 그룹에 속하더라도 원격 컴퓨터에 있는 같은 이름의 계정이 Power Users 나 Users 그룹에 속한다면 Administrator 권한이 없으므로 원격 컴퓨터에 Administrators 그룹에 속한 사용자 계정을 만들고 로컬 컴퓨터에 같은 이름의 사용자로 로그인 해야 한다. 이러한 원리를 이용하여 해킹, 또는 패스워드 크랙 등의 방법으로 원격 컴퓨터의 관리자 계정을 알아내어 원격에서 다른 컴퓨터를 통제할 수 있다.

- 하이브(hive)

레지스트리에서 하이브는 루트 키 아래에 있는 하위 키부터 그 아래의 모든 하위키를 포함하는 레지스트리 트리 구조를 가리킨다. 예를 들면 Software 하이브는 HKEY\_LOCAL\_MACHINESoftware 와 그 밑의 모든 하위 키, 그리고 그 모든 하위키의 가장 아래쪽 하위 키의 값에 이르는 모든 것을 말한다.

## 1.2 관련 설명

레지스트리는 윈도우를 실행하는데 필요한 환경설정 데이터를 말한다. 윈도우의 모든 설정이 이 레지스트리에 담겨있다. 시스템에 설치되어 있는 랜카드나 디스플레이 어댑터등에 대한 정보나 응용프로그램에 대한 정보 그리고 윈도우 자체적인 설정, 인터넷 익스플로러 설정등이 모두 담겨져 있다.

윈도우를 설치하면 윈도우관련 설정값들이 레지스트리에 저장되고 추가적으로 설치하는 장치나 프로그램이 있을 때마다 그 정보가 추가된다. 그래서 장치와 프로그램이 많아질수록 레지스트리 덩치가 커지고 복잡해지게 된다. 또한 그런 장치나 프로그램들을 제거할 때에는 레지스트리에서 삭제되게 되어 있다. 그러나 사용자의 실수나 시스템 환경에 따라 레지스트리에서 제거되지 못하고 잔존함으로써 시스템 오류나 문제를 일으킨다. 따라서 이러한 문제점을 해결하기 위해서 레지스트리를 수동으로 편집해야 하는 경우가 가끔씩 발생한다.

다음은 윈도우 버전별 레지스트리와 관련된 파일들이다.

■ 윈도우 버전별 레지스트리 관련 파일

① win95 레지스트리

저장위치	파일이름	내용
c:\windows	user.dat, system.dat	부팅할 때마다 저장된다. 또한 작업중 갱신된다
c:\windows	user.da0, system.da0	자동백업파일
c:\windows	system.ini, win.ini	win3.1 호환프로그램용

② win98 레지스트리

저장위치	파일이름	내용
c:\windows	user.dat, system.dat	부팅할 때마다 저장된다. 또한 작업중 갱신된다
c:\windows	system.ini, win.ini	win3.1 호환프로그램용
c:\windows\sysbackup	rb000.cab~rb005.cab	백업파일로서 5일분 저장

③ win 2000 레지스트리

저장위치	파일이름	내용
C:\WINNT\system32\config	system, software 등	다수의 파일로 존재
C:\WINNT\repair	system, software 등	Windows 2000 최초 설치시 생성
C:\WINNT\repair\RegBack	system, software 등	백업파일로서 응급복구디스크 작성할 때마다 생성
C:\WINNT\	system.ini, win.ini	win3.1 호환프로그램용

## ■ 레지스트리 구조

레지스트리를 이용하면 레지스트리를 통해 시스템을 관리하는데 있어서 집중화관리가 가능하고 다중 사용자의 경우 각각 사용자에게 대한 설정과 권리에 대한 관리가 가능하다. 또한 Multiple Device 에 대한 환경설정이 가능하다. 이렇게 시스템의 정보가 담겨져 있는 레지스트리는 아래와 같이 구성된다.

- HKEY\_CLASSES\_ROOT
- HKEY\_CURRENT\_USER
- HKEY\_LOCAL\_MACHINE
- HKEY\_USERS
- HKEY\_CURRENT\_CONFIG

먼저 HKEY\_CLASSES\_ROOT 는 파일 확장자와 그 파일에 맞는 애플리케이션에 대한 정보를 가지고 있다. 그리고 HKEY\_CURRENT\_USER 는 현재 로그인해 있는 사용자에게 대한 정보를 가지고 있고, HKEY\_LOCAL\_MACHINE 은 시스템 하드웨어 와 소프트웨어 환경에 대한 전반적인 정보들을 가지고 있으며, HKEY\_USERS 는 각각의 사용자들에 대한 정보들을, 마지막으로 HKEY\_CURRENT\_CONFIG 는 하드웨어 환경설정에 대한 정보들을 가지고 있다. 이렇게 5 가지 종류의 레지스트리가 있으나 실제로는 모두 2 가지의 레지스트리들이 존재할 뿐이다. 그것은 아래와 같은 alias 가 존재하기 때문이다.

- HKEY\_LOCAL\_MACHINE

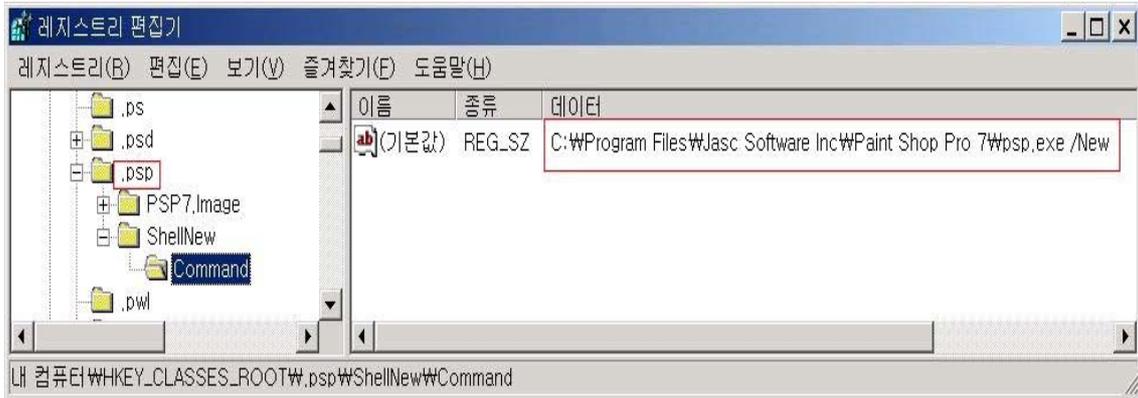
- ◆ HKEY\_CLASSES\_ROOT
  - HKEY\_LOCAL\_MACHINE\Software\Classes
- ◆ HKEY\_CURRENT\_CONFIG
  - HKEY\_LOCAL\_MACHINE 아래의 일부 keys

- HKEY\_USERS

- ◆ HKEY\_CURRENT\_USER
  - ( HKEY\_CURRENT\_USER 의 SID로 표시됨)

### ① HKEY\_CLASSES\_ROOT

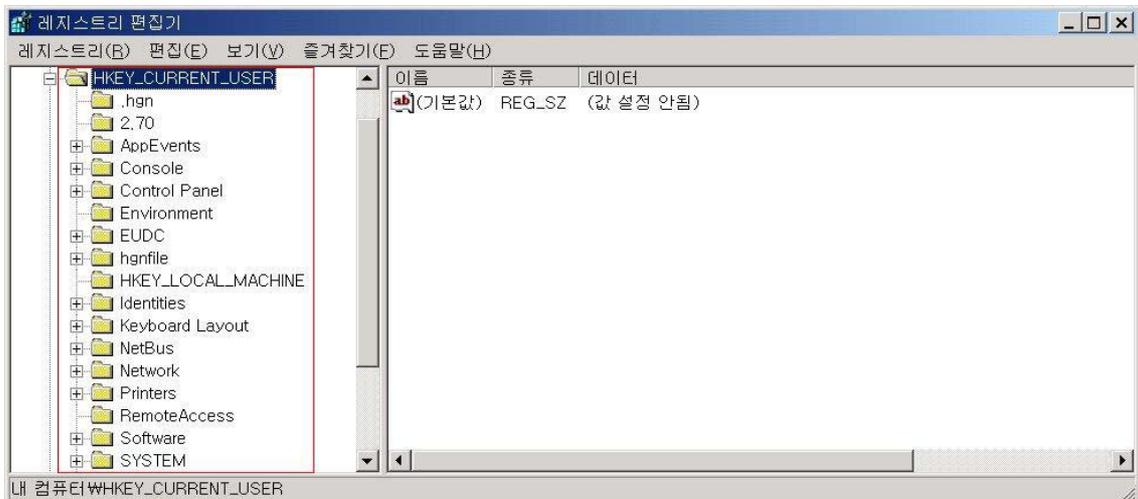
파일 확장자에 대한 정보, 각 프로그램간의 연결 정보, 마우스 오른쪽 단추의 등록정보 등이 담겨 있다. 윈도우에서 사용되는 모든 형식의 파일 확장자가 sub key의 형태 (디렉토리 형태)로 구성되어 있는데 예를 들어 paint shop pro를 설치하게 되면 psp 확장자를 가지는 파일은 psp.exe와 연결된다는 정보가 레지스트리에 새로 저장된다.



[그림 1-1] HKEY\_CLASSES\_ROOT 예시

② HKEY\_CURRENT\_USER

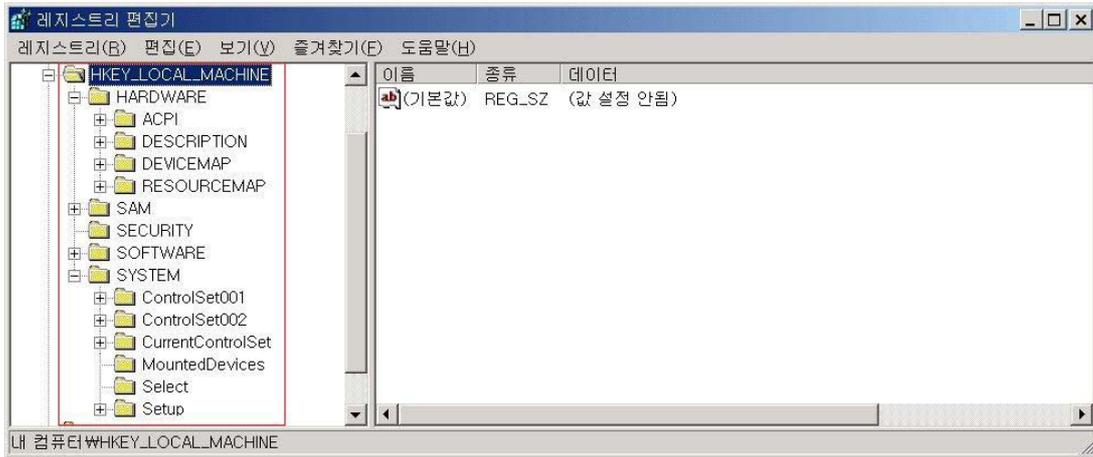
현재 로그인된 사용자의 사용자 초기화 파일에 대한 구성정보를 갖고 있다. 사용자의 배경화면, 디스플레이 설정이나 단축아이콘의 정보가 담겨 있다. 한대의 컴퓨터로 여러명의 사용자가 사용할 경우 각 사용자에 대한 정보는 HKEY\_USERS에 저장되고 HKEY\_CURRENT\_USER에는 현재 로그인한 사용자의 환경이 저장된다. 컴퓨터의 사용자가 한명이라면 HKEY\_USERS/.Default에 있는 내용과 거의 동일하다.



[그림 1-2] HKEY\_CURRENT\_USER 예시

### ③ HKEY\_LOCAL\_MACHINE

윈도우의 실행에 필요한 모든 하드웨어 설정에서부터 그 하드웨어가 사용하고 있는 드라이버 정보가 저장되어 있다. 제어판의 장치관리자 내용등 가장 중요한 부분을 차지하고 있다. 로그인한 사용자와 관계없이 컴퓨터에 등록된 모든사용자에게 동일하게 나타난다.



[그림 1-3] HKEY\_LOCAL\_MACHINE 예시

### ④ HKEY\_USERS

컴퓨터를 공유하는 사용자 각각의 윈도우 환경에 관한 여러 가지 설정을 저장한다. HKEY\_CURRENT\_USER 서브 트리에 대한 포인터와 .default 프로파일을 갖고 있으며 계정이 하나인 경우 .default 프로파일만 존재한다. 여러명이 사용하는 경우 사용자의 정보는 SID 명으로 존재하며 SID 하위 디렉토리의 내용은 HKEY\_CURRENT\_USER 설정과 같다.



[그림 1-4] HKEY\_USERS 예시

### ⑤ HKEY\_CURRENT\_CONFIG

디스플레이나 프린터에 대한 설정 내용이 저장되어 있다.



[그림 1-5] HKEY\_CURRENT\_CONFIG 예시

다섯개의 루트키 각각에는 하위키가 존재하는데 하위키는 자신의 값을 가지거나 실제 값을 갖는 다른 하위키를 포함하는 용도로 사용될 수 있다. 이는 디스크의 하위 디렉토리와 같은 의미를 가진다. 최하위키는 레지스트리 값을 가지는데 레지스트리 값은 보통 세 부분으로 구성되어 있다.

- 이름(name) : 값의 이름으로 같은 레지스트리 키에 속해 있는 값은 모두 다른 이름을 가져야 한다.
- 종류(type) : 그 값에 포함되어 있는 데이터의 종류를 레지스트리와 레지스트리를 사용하는 프로그램에 알려준다. 다음은 많이 쓰이는 데이터 종류이다.
  - reg\_dword : reg\_dword 는 더블 워드를 의미한다. 한 워드는 16 비트 숫자이므로 더블워드는 32 비트 값을 말하여 레지스트리 안에서 가장 일반적으로 쓰이는 데이터 형이다.
  - Reg\_sz : 문자열값을 말하며 reg\_dword 다음으로 많이 쓰이는 데이터형이다. 문자열은 사람이 읽을 수 있는 이름이나, 파일 경로명, 버전 숫자, 또는 다른 많은 유용한 것을 저장한다.
  - Reg\_multi\_sz : 서로 관계있는 문자열 그룹을 한 블록으로 저장할 때 사용되는 데이터 형이다.
  - Reg\_expand\_sz : 시스템 스크립트 언어에 넘겨주기 위해 제공되는 시스템 정의 변수이다. 이러한 변수들은 제어판>시스템>고급>환경변수 단추에서 보여지는 시스템 변수들과 같은 의미를 지닌다.

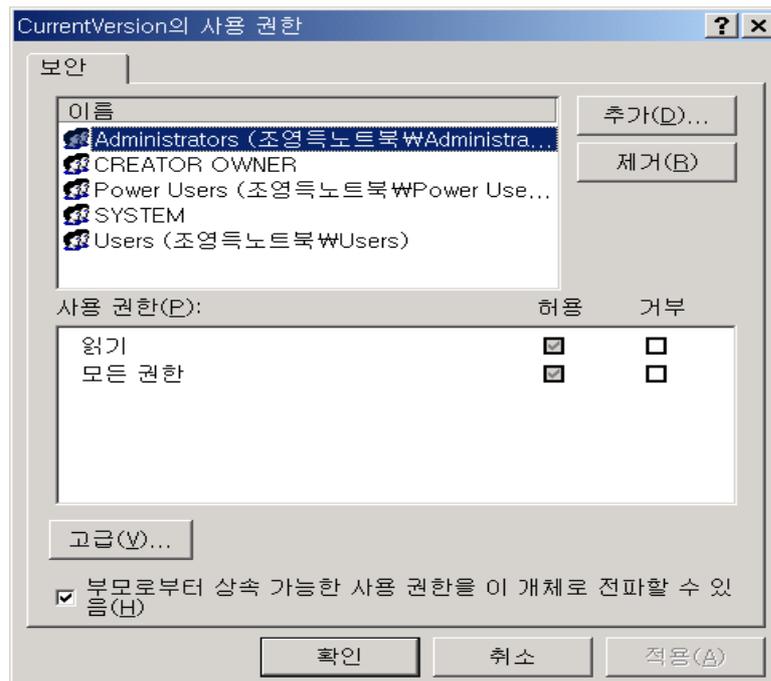
- Reg\_binary : 이진수 값을 그대로 사용하기 위해 이용되며 레지스트리 에디터를 통해 이 값을 볼 때 이 유형의 데이터는 의미가 없다.

- 데이터(data) : 데이터는 그 값의 데이터 형에 따라 제약을 받는데 윈도우 2000 에서의 값의 내용은 크기가 6KB 이하여야 한다.

## ■ 레지스트리 보안

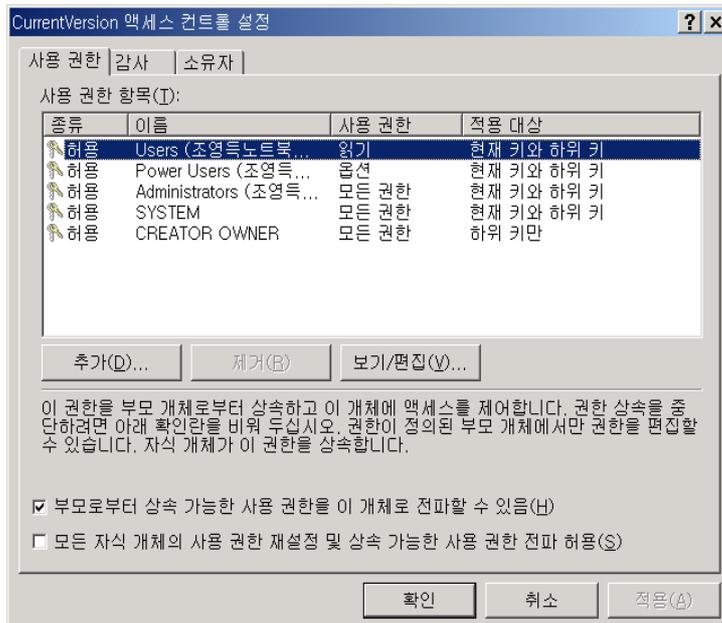
레지스트리 보안을 위해서는 레지스트리에 적절한 ACL 이 설정이 되어야 한다.

먼저 레지스트리 ACL 을 설정하기 위해서 regedt32 를 실행한다(windows 2000). 해당 레지스트리키에 대하여 보안을 설정하기 위하여 regedt32 창> 보안>사용권한을 실행하면 다음과 같은 대화상자가 열리며 이 곳에서 사용자를 추가하거나 삭제한다.



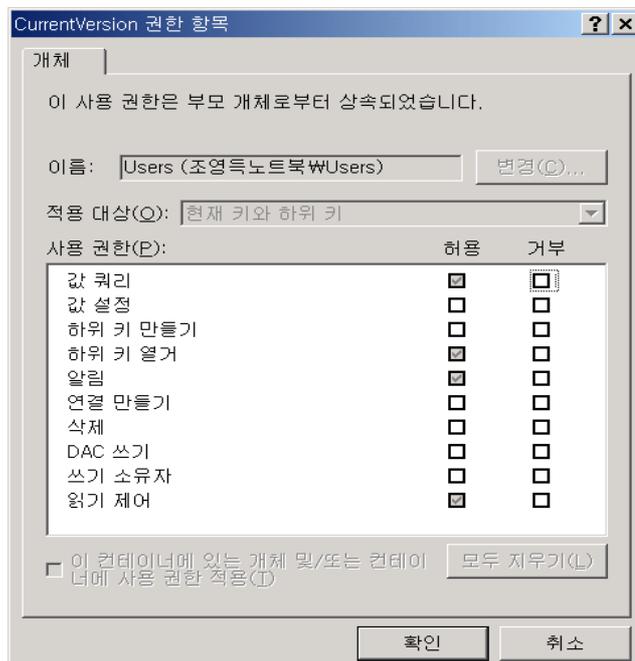
[그림 1-6] 레지스트리 사용권한 설정

해당 레지스트리 키에 대한 사용자의 액세스를 컨트롤 하기 위해서는 대화상자의 고급버튼을 클릭하면 액세스 컨트롤을 설정할 수 있는 대화창이 열린다. 이 대화창에서 각 사용자에게 대한 레지스트리의 접근 권한을 상세히 적용할 수 있다.



[그림 1-7] 레지스트리 액세스 컨트롤 설정

위 액세스 컨트롤 설정 대화창에서 사용자를 선택하여 클릭하면 아래와 같이 사용권한을 설정할 수 있다.



[그림 1-8] 레지스트리 사용권한 항목

### ■ 원격 레지스트리의 접근 제한

레지스트리는 local의 경우 그 접근이 자유로운 편이다. 일반 user들 또한 쉽게 레지스트리를

읽을 수 있다. 하지만 레지스트리를 수정하기 위해서는 HKEY\_CURRENT\_USER를 제외하고는 관리자의 권한이 필요하다. 원격에서 레지스트리로의 접근을 위해서도 관리자의 권한 또는 원격에서 접근을 하기 위한 특별한 계정이 필요하다. 일반적으로 바이러스가 침투해서 권한을 바꾸거나 폴더를 공유하는 경우에는 먼저 root(administrator)의 권한을 획득한 이후에 가능하다. 윈도우 2000에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는 데 이 서비스를 셧다운 시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있다. 중요 서버로서 콘솔에서만 관리할 경우 서버보안을 위해 이와 같이 원격 레지스트리 서비스를 셧다운시키는 것도 주요 보호대책이라 할 수 있다. 그러나 이러한 경우 관리자가 원격지에서 서버 관리를 할 수 없는 문제점이 발생한다.

원격 레지스트리 서비스를 셧다운 시키지 않고 레지스트리에 대한 원격 접근을 제어하기 위해 윈도우 NT 4.0과 윈도우 2000에서는 winreg라는 키를 생성하여 레지스트리 접근에 대한 사용자, 그룹, 서비스를 제어한다. Winreg를 레지스트리에 대한 네트워크 액세스를 제한하는 방법은 다음과 같다.

1. 레지스트리에 아래 키를 추가한다.

하이브	HKEY_LOCAL_MACHINE \SYSTEM
키	\CurrentControlSet\Control\SecurePipeServers
값 이름	\winreg

2. 다음에 윈도우 시작>실행에서 regedt32를 실행한다. Regedt32화면에서 winreg를 선택하고, "보안" 메뉴를 선택한 다음, "사용 권한"을 선택한다.
3. 적용하려는 ACL을 추가하거나 삭제한다. (앞 페이지의 레지스트리 키 보안의 그림 참조) 이 키에 적용되는 사용권한은 네트워크를 통하여 레지스트리에 접근할 수 있는 사용자와 그룹을 결정한다. 기본적으로 administrators 그룹은 모든 권한을 가진다. 새로운 사용자나 그룹에 대해서는 이 목록에 추가하여 원하는 대로 사용 권한을 설정 할 수 있다.

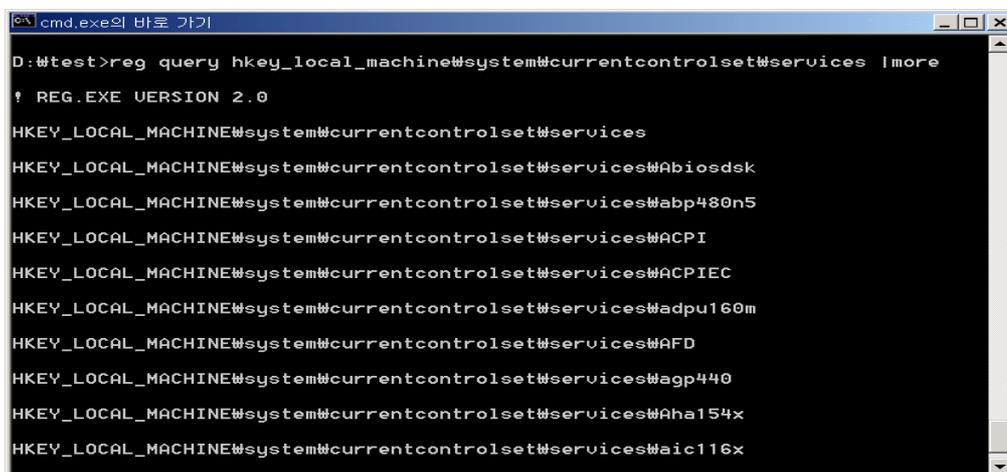
#### ■ 레지스트리 검색을 통한 불법서비스 점검

일반적으로 불법사용자가 불법프로그램을 설치하는 경우 지속적으로 사용하기 위하여 레지스트리에 프로그램을 등록하여 프로그램이 실행시마다 자동으로 실행될 수 있도록 한다. 따

라서 불법서비스가 실행되고 있는지를 점검하기 위해 이러한 레지스트리 리스트를 이용할 수 있다. 검색할 레지스트리 리스트는 다음과 같다.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\AeDebug
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\WinLogon
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" line)
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" value)
```

또는 윈도우 리소스킷에 있는 reg.exe 를 사용하여 현재 실행중인 서비스정보를 볼 수 있다.



[그림 1-9] reg를 이용한 실행중인 서비스 검색

### 1.3 관련 시스템 win2000, winNT

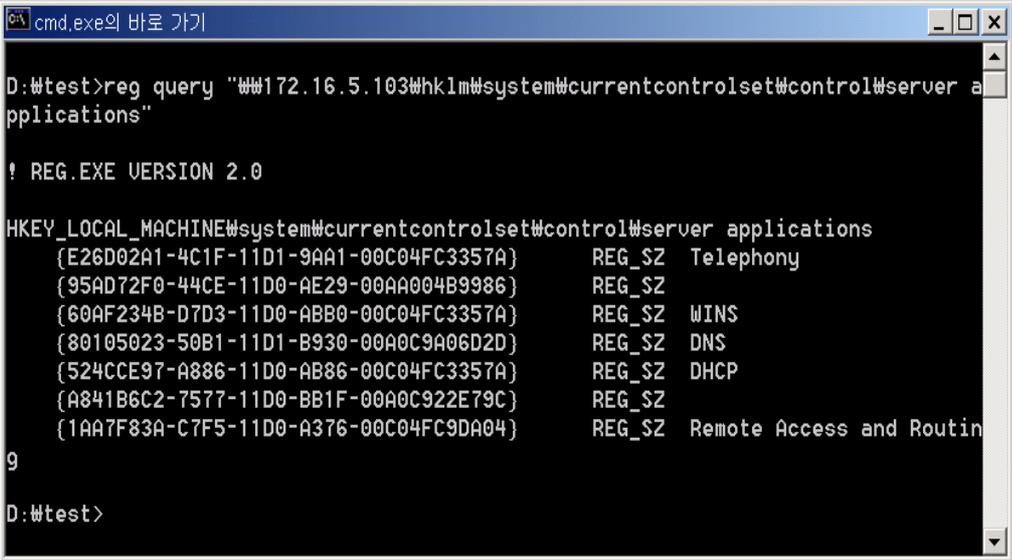
## 2. 취약점 유형 및 보호대책

### 2.1 원격 레지스트리 접근 인증 취약점(CVE-2000-0377, MS00-040)

#### (1) 취약점 설명

원격서버의 레지스트리에 접근을 하기 위해서는 먼저 원격 레지스트리 서버로부터 인증을 받아야 한다. 그런데 인증을 위해 보내는 메시지가 특정한 방식의 잘못된 형식일 경우 원격 레지스트리 서버가 이를 잘못 해석할 수 있고 이로 인하여 원격 레지스트리 서버에 장애가 발생할 수 있다. 그런데 원격 레지스트리 서버는 Windows NT 4.0의 winlogon.exe 시스템 프로세스에 포함되기 때문에, 이 프로세스에서의 장애는 전체 시스템의 장애를 초래할 수 있다. 이러한 취약점은 서비스거부공격에 이용될 수 있는데 영향을 받은 시스템은 재부팅을 통해 정상으로 복구될 수 있다.

그리고 원격 레지스트리 액세스에 대한 인증이 취약한 경우, 즉 관리자 계정의 다른 계정들에게도 원격 레지스트리 액세스가 허용되는 경우 다음과 같이 reg.exe와 같은 도구를 사용하여 원격으로 레지스트리의 내용을 query하거나 의도적인 실행명령어를 레지스트리에 입력하여 실행하도록 할 수 있다.



```
cmd.exe의 바로 가기
D:\wtest>reg query "\\172.16.5.103\hklm\system\currentcontrolset\control\server applications"

! REG.EXE VERSION 2.0

HKEY_LOCAL_MACHINE\system\currentcontrolset\control\server applications
    {E26D02A1-4C1F-11D1-9AA1-00C04FC3357A}    REG_SZ    Telephony
    {95AD72F0-44CE-11D0-AE29-00AA004B9986}    REG_SZ
    {60AF234B-D7D3-11D0-ABB0-00C04FC3357A}    REG_SZ    WINS
    {80105023-50B1-11D1-B930-00A0C9A06D2D}    REG_SZ    DNS
    {524CCE97-A886-11D0-AB86-00C04FC3357A}    REG_SZ    DHCP
    {A841B6C2-7577-11D0-BB1F-00A0C922E79C}    REG_SZ
    {1AA7F83A-C7F5-11D0-A376-00C04FC9DA04}    REG_SZ    Remote Access and Routin
9
D:\wtest>
```

[그림 2-1] reg를 이용한 원격 레지스트리 내용 조회

※ Winlogon: Winlogon.exe는 Windows NT에서 보안과 관련해 사용자 작업을 관리하는 프로세스이다. 이 프로세스는 로그인과 로그오프 요청, 시스템의 잠금이나 잠금 해제, 암호 변경과 기타 요청을 제어하는데 Windows NT 4.0의 Winlogon은 원격 레지스트리 서비스를 포함하고 있다.

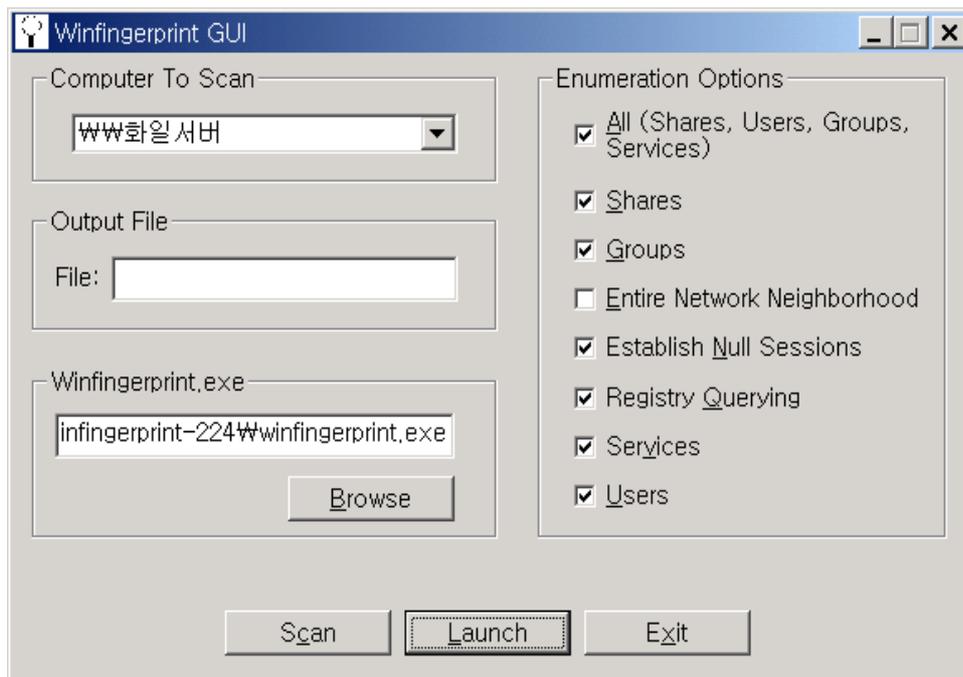
(2) 취약한 시스템

- Microsoft Windows NT 4.0
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Workstation 4.0

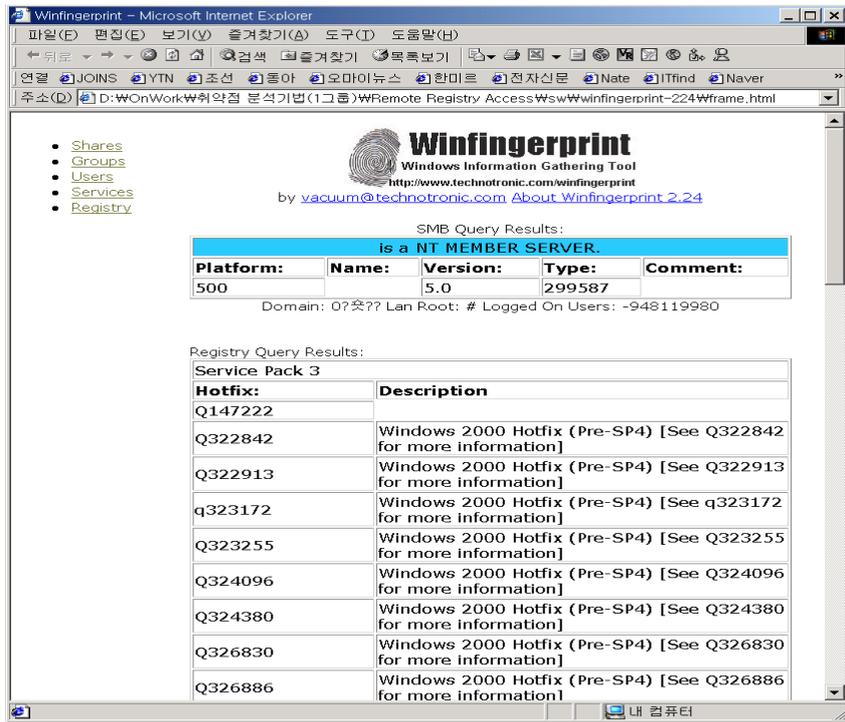
(3) 점검 방법

특별한 점검방법은 없고 취약한 시스템을 사용하고 있는 경우 보호대책에서 제시하는  
바와 같이 winreg 레지스트리키를 사용하여 액세스 권한을 설정하거나 해당 사이트에서  
패치를 한다.

일반적인 정보를 검색하기 위해 winfingerprint를 사용하여 레지스트리 목록, 공유 디  
렉토리, 그룹, 사용자, 서비스 등을 볼 수 있다.



[그림 2-2] winfingerprint를 이용한 사용자 액세스 권한 조회



[그림 2-3] winfingerprint를 이용한 조회 결과

(4) 보호대책

가. winreg 라는 레지스트키를 통한 액세스 권한 설정

Windows NT 4.0 서비스 팩은 Winreg 키라고 불리는 레지스트리 키를 제공하는 데 이 키는 레지스트리를 원격 액세스할 수 있는 대상을 규정할 수 있다. 즉 이 키에 설정된 보안 권한은 레지스트리에 원격으로 액세스하기 위해 어떤 사용자나 그룹이 시스템에 연결할 수 있는지를 규정하고 있다. 기본 상태에서는 administrators 는 모든 권한, backup operators 는 읽기 권한으로 접근할 수 있다. 그러나 이 권한을 수정하면 원격에서 일반사용자가 접속하게 할 수도 있고 administrators조차도 원격에서 접속하지 못하게 할 수 있다.

다음은 네트워크 액세스를 제한하기 위하여 레지스트리 키를 만드는 과정이다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

설명: REG\_SZ

값: Registry Server

1. 레지스트리 편집기(Regedt32.exe)를 시작하고 다음 하위 키로 이동한다.

## HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control

2. 편집 메뉴에서 키 추가를 누른다.

3. 다음 값을 입력한다.

키 이름: SecurePipeServers

클래스: REG\_SZ

4. 다음 하위 키로 이동한다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers

5. 편집 메뉴에서 키 추가를 누른다.

6. 다음 값을 입력한다.

키 이름: winreg

클래스: REG\_SZ

7. 다음 하위 키로 이동한다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

8. 편집 메뉴에서 값 추가를 누른다.

9. 다음 값을 입력한다.

값 이름: Description

데이터 형식: REG\_SZ

문자열: Registry Server

10. 다음 하위 키로 이동한다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg

11. "winreg"를 선택한다. 보안을 누른 다음 사용 권한을 누른다. 액세스를 부여할 사용자나 그룹을 추가한다. 보안을 위하여 관리자의 원격 액세스만 허용하도록 한다.

12. 레지스트리 편집기를 종료하고 Windows NT를 다시 시작한다.

13. 나중에 레지스트리에 액세스할 수 있는 사용자 목록을 변경하려면 10-12단계를 반복한다.

그러나 Winreg 키가 기본값으로 이 취약점으로부터 시스템을 보호하지 않는다. 키를 질의하는 한은 악의적인 사용자가 이 취약점을 악용할 수 있다. 따라서 인증 받은 사용자(Authenticated Users 그룹)가 소수의 레지스트리 키를 질의할 수 있도록 winreg 에 대한 액세스를 설정한다. 이를 위하여 아래의 키에 해당 서비스를 실행할 때 사용할 계정 이름을 추가하거나, AllowedPaths 키의 Machine 또는 Users 값에 특정 키에 대한 액세스를 나열한다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths 키

값: Machine

값 종류: REG\_MULTI\_SZ - 다중 문자열

기본 데이터: System\CurrentControlSet\Control\ProductOptions  
System\CurrentControlSet\Control\Print\Printers  
System\CurrentControlSet\Services\Eventlog  
Software\Microsoft\Windows NT\CurrentVersion  
System\CurrentControlSet\Services\Replicator

유효 범위: 레지스트리 내에 있는 한 위치의 유효한 경로.

설명: 해당 위치에 대한 명시적 액세스 제한이 없을 경우 레지스트리의  
나열된 위치에 대한 컴퓨터의 액세스를 허용

값: Users

값 종류: REG\_MULTI\_SZ - 다중 문자열

기본 데이터: (없음)

유효 범위: 레지스트리 내에 있는 한 위치의 유효한 경로.

설명: 해당 위치에 대한 명시적 액세스 제한이 없을 경우 레지스트리의  
나열된 위치에 대한 사용자 액세스를 허용

Windows 2000 이상에서는 약간만 변경한다.

값: Machine

값 종류: REG\_MULTI\_SZ - 다중 문자열

기본 데이터: System\CurrentControlSet\Control\ProductOptions  
System\CurrentControlSet\Control\Print\Printers  
system\CurrentControlSet\control\Server Applications  
System\CurrentControlSet\Services\Eventlog  
Software\Microsoft\Windows NT\CurrentVersion

나. RestrictAnonymous 레지스트리 값을 추가하고 값을 수정한다.(Windows 2000)

위치 :HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

값 이름: RestrictAnonymous

값 종류: REG\_DWORD

값 데이터: 0x2(16진수)

※ 데이터값 0 : 기본사용권한에 의존,

1 : SAM계정 및 공유 열거 허용안함

2 : 명백한 익명의 사용권한이 없으면 액세스 못함

그런데 주의할 점은 RestrictAnonymous 레지스트리 값을 2로 설정하면 인증되지 않은 사용자에게 대해 작성된 액세스 토큰은 모든 사용자 그룹을 포함하지 않으므로 모든 사용자 그룹에 사용 권한을 부여하는 리소스를 더 이상 액세스할 수 없다. 따라서 하위 수준 클라이언트가 포함되어 있는 혼합 모드 환경에서는 RestrictAnonymous 레지스트리 값을 2로 설정하지 않는 것이 좋다..

다. 다음 사이트에서 패치를 한다.

Microsoft Windows NT 4.0:

<http://download.microsoft.com/download/winntsp/Patch/Q264684/NT4/EN-US/Q264684i.EXE>

#### (5) 공격방법

원격 레지스트리 액세스에 대한 인증이 취약하여 관리자 계정의 다른 계정들에게도 원격 레지스트리 액세스가 허용되거나 레지스트리에 대한 권한설정이 잘못되어 있는 경우 reg.exe를 이용하여 원격에서 공격대상서버의 레지스트리에 임의의 파일에 대한 실행명령어를 입력함으로써 특정화일을 실행시킬 수 있다. 다음은 Internet Explorer의 시작 페이지를 공격자가 원하는 실행화일이 있는 페이지로 변경함으로써 이를 실행할 경우 공격자의 프로그램이 실행되는 예이다.

가. 먼저 공격자는 원격레지스트리에 접근할 수 있는 권한을 획득하고 있어야 한다.

나. 권한을 획득한 후 reg.exe를 이용하여 공격대상PC의 레지스트리 값을 변경시킨다.

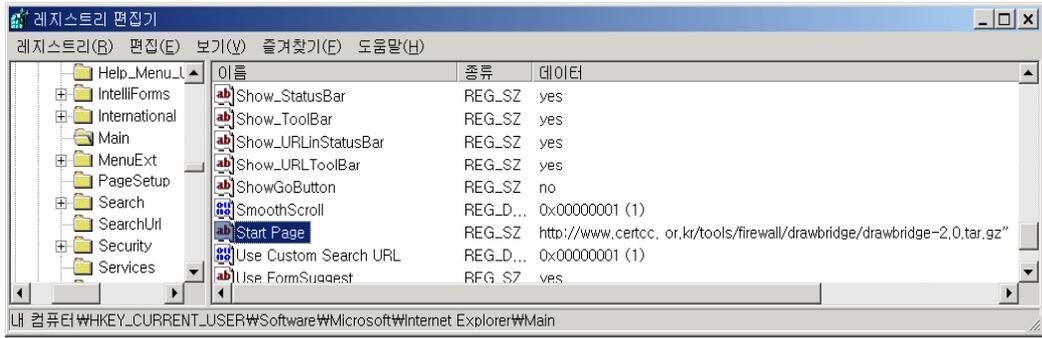
변경할 레지스트리는 Internet Explorer를 실행할 때 제일 처음 열리는 웹페이지인 시작페이지의 값이 입력되는 레지스트리이다. 시작페이지의 레지스트리 키는 다음과 같다.

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
\Start Page
```

이 레지스트리를 변경시키기 위하여 다음과 같이 실행한다.

※ 실행명령은 비공개함

다. 레지스트리 키 값이 성공이 되면 다음 화면과 같이 레지스트리값이 변경된다.



[그림 2-4] reg를 이용한 레지스트리 내용 추가 결과

라. 레지스트리 값 변경후에는 Internet Explorer 실행시 해당 파일을 다운받는 팝업창이 뜨게 되고 무심코 확인을 선택하면 공격자의 프로그램이 실행된다.

## 2.2 Exchange 2000 System Attendant의 부정확한 원격 레지스트리 권한 설정 취약점(CVE-2002-0049, MS02-003)

### (1) 취약점 설명

Exchange 2000은 여러 개의 메시지 데이터베이스를 지원하여, 조직의 내부 및 외부 수신자에게 안전한 메시징 기능을 제공하기 위한 안정적이고 확장 가능한 메시징 환경과 공동 작업 환경을 제공한다. Exchange 2000은 다음과 같이 3가지 제품이 있다.

- Exchange 2000 Server : 중소 규모 기업의 메시징 및 공동 작업 필요
- Exchange 2000 Server Enterprise Edition : 대규모 엔터프라이즈 기업을 위해 설계되었으며 다중 스토리지 그룹과 다중 데이터베이스를 만들 수 있도록 지원한다. 이 제품은 데이터 수량과 관련해 단일 서버가 관리할 수 있는 한계를 극복할 수 있는 무제한의 메시지 저장 능력을 제공한다.
- Exchange 2000 Conferencing Server : 모든 규모의 조직들이 멀티 캐스트 비디오 회의와 응용 프로그램을 공유하면서 데이터 회의를 제공할 수 있도록 Exchange 2000의 기능을 확장한다.

또한 Exchange 2000의 주요한 기능은 다음과 같다.

- 유연한 데이터관리를 위한 데이터 베이스 확장 기능
- 음성과 데이터의 통합된 메시징 환경 제공
- 많은 사용자들에게 안정적적이고 빠른 메시지 제공
- 데이터, 비디오, 오디오 회의기능
- 콘테츠 저장 및 빠른 문서 검색 등 공동작업환경제공

그런데 Microsoft Exchange System Attendant는 Microsoft Exchange의 핵심 서비스들 중의 하나로, Exchange 시스템의 지속적인 유지보수와 관련된 다양한 기능들을 수행한다. Exchange System Manager의 MMC (Microsoft Management Console) 스냅인 기능을 이용한 Exchange Server의 원격 관리를 허용하기 위해, System Attendant는 Exchange 관리자가 레지스트리에 저장된 구성 설정값들을 원격지에서 업데이트 할 수 있도록 Windows 레지스트리에 관한 권한을 변경한다. 이로 인해 권한이 없는 사용자가 원격지에서 서버상의 구성 정보를 액세스할 수 있다. 이때 WingReg 키에 대해 "Everyone" 그룹 권한을 부적절하게 부여하는데, 이 키는 원격지에서 레지스트리로 접속하려는 사용자 및 그룹의 능력을 제어한다. 즉 Exchange 2000 System Attendant가 "Everyone 그룹"을 레지스트리 내의 HKEY\_LOCAL\_MACHINE \SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg의 보안 권한에 부정확하게 추가하기 때문에 취약점이 나타난다.

이 취약점은 자체적으로 침입자에게 레지스트리 설정값들을 변경할 수 있는 능력을 제공하지 않는 반면에, 시스템 레지스트리에 대한 액세스 취득 및 변경을 위해 부적절하

게 권한이 부여된 레지스트리 설정값과 연계하여 이용될 수 있다.

(2) 취약한 시스템

Microsoft Exchange Server 2000

(3) 점검 방법

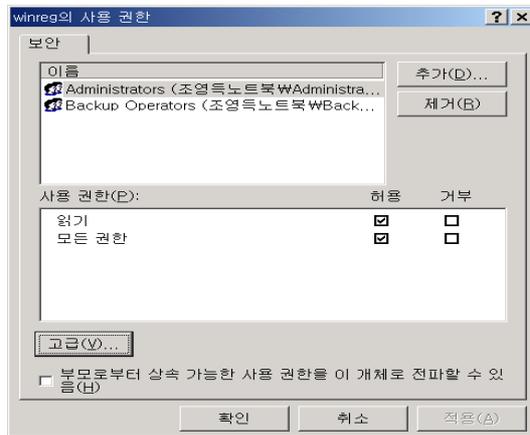
특별한 증상은 없으며 해당 시스템을 사용하고 있는 경우 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 의 보안 권한을 점검한다.

가. 윈도우 시작메뉴의 실행에서 regedt32를 실행한다.

나. winreg 레지스트리 키를 선택한다.

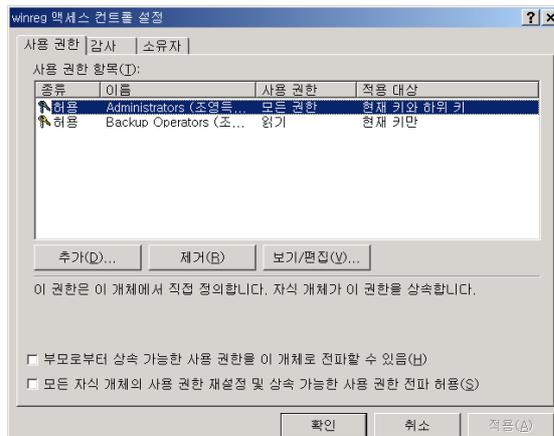
다. 메뉴에서 보안>사용권한을 클릭한다.

라. 다음 그림과 같이 사용권한을 점검한다.



[그림 2-5] winreg 사용권한 점검

마. 상세한 사용권한을 점검하기 위해 고급버튼을 클릭한다.



[그림 2-6] winreg 액세스 컨트롤 설정

(4) 보호대책

[해당 패치]

Microsoft Exchange Server 2000:

<http://www.microsoft.com/downloads/release.asp?ReleaseID=35462>

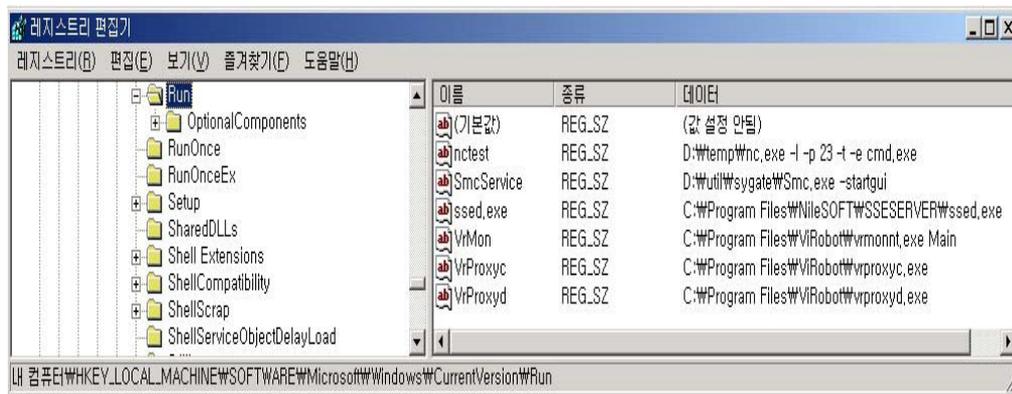
(5) 공격방법

WinReg 키에 대해 "Everyone" 그룹 권한을 부적절하게 부여될 경우 이를 이용하여 공격 대상PC의 레지스트리에 특정 프로그램(nc.exe)을 실행시킬 수 있는 명령을 입력하여 시스템 시작시 이 프로그램이 실행되도록 한다. 이 프로그램이 실행되면 원격지에서 Telnet으로 이 대상PC에 접근이 가능하게 된다. 다음은 실제 공격방법이다.

공격자PC : 172.16.5.104      공격대상PC : 172.16.5.103 로 하고 다음의 절차에 따라 공격을 한다.

가. 먼저 nc.exe를 공격대상 호스트의 temp 디렉토리에 설치한다. 이 작업은 로컬에서 실행하여야 한다.

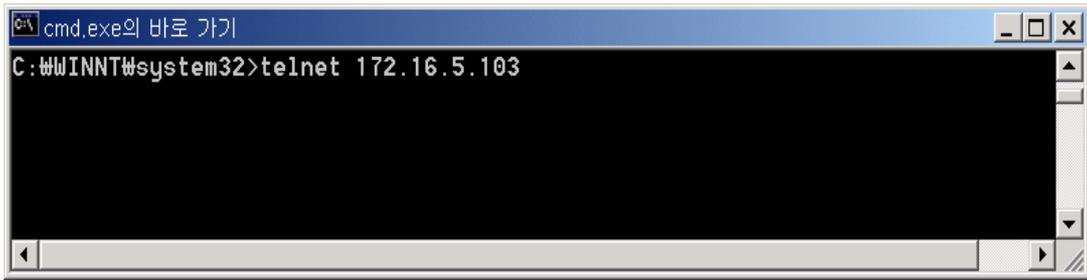
나. 윈도우 2000 또는 NT에서 제공하는 resource kit 중에서 reg.exe를 이용하여 공격 대상PC에 레지스트리 값을 변경시킨다. 이때 시스템 시작시 nc.exe가 항상 실행될 수 있도록 하기 위하여 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run에 레지스트리 값을 추가 시킨다.



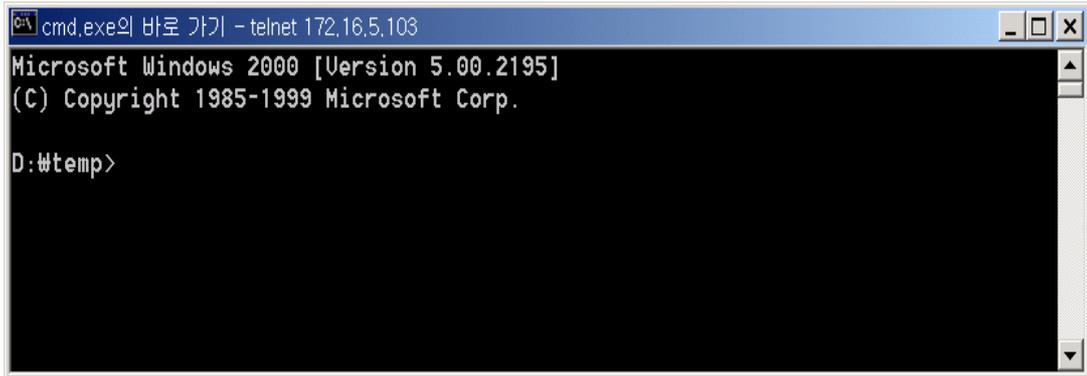
[그림 2-7] 공격대상 호스트의 레지스트리값 추가 결과

다. 이와 같이 입력하면 매번 부팅시에 nc.exe가 실행된다.

라. 공격자는 아래 그림과 같이 원격지에서 telnet으로 공격대상PC에 접속한다.



```
cmd.exe의 바로 가기
C:\WINNT\system32>telnet 172.16.5.103
```



```
cmd.exe의 바로 가기 - telnet 172.16.5.103
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

D:\temp>
```

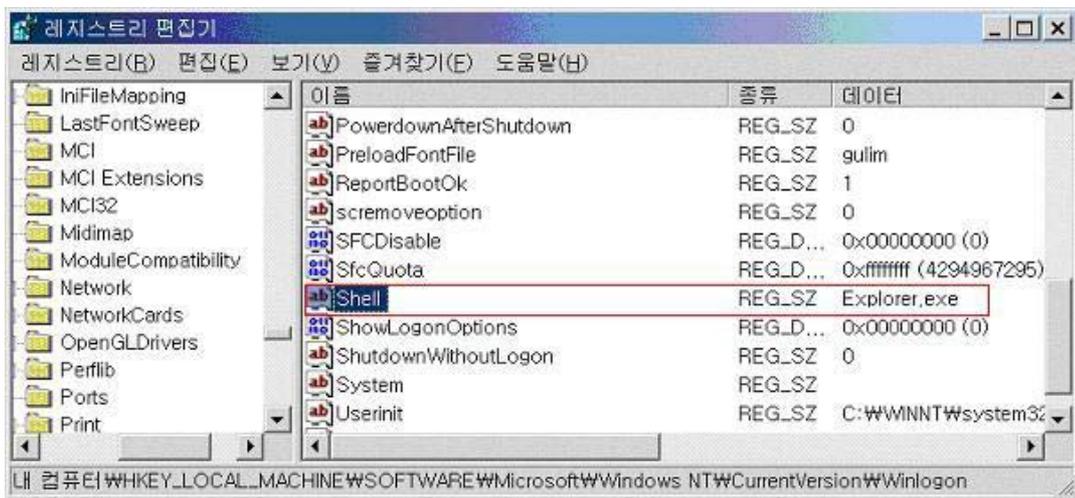
[그림 2-8] 원격지에서 텔넷 접속 (현재 접속호스트는 172.16.5.103 PC임)

마. 공격대상 PC에 접속한 후 주요문서를 가져오거나 다른 작업을 수행할 수 있다.

## 2.3 상대 쉘 경로 취약점(CVE-2000-0663, MS00-052)

### (1) 취약점 설명

윈도우즈 쉘은 윈도우즈와 상호 작용하기 위해 사용되는 프로그램으로 윈도우즈가 부팅될 때 자동으로 시작되어 사용자의 명령을 실행시켜준다. 시스템이 시작되는 동안 Windows NT 4.0과 Windows 2000은 쉘 프로그램으로 로드되어야 할 실행 파일명을 결정하기 위해 "쉘" 레지스트리 엔트리인 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell을 참조하는데, 기본값으로 Explorer.exe가 지정되어 있다.



[그림 2-9] shell 레지스트리 엔트리

그런데 윈도우즈 쉘 프로그램 실행 파일 (Explorer.exe)을 지정하는 레지스트리 엔트리는 절대 경로명이 아닌 상대 경로명을 제공한다. shell path가 절대경로로 지정되어 있지 않기 때문에 시스템이 시작할 때 윈도우 shell(explorer.exe)을 찾기 위하여 경로 우선순위에 따라 shell을 검색한다.

레지스트리 엔트리가 상대 경로를 통해 코드 모듈 이름을 지정할 때마다 Windows는 해당 코드를 찾기 위해 검색 프로세스를 초기화하는데 검색 순서는 다음과 같다

가. 현재 디렉터리를 검색한다.

나. 코드가 발견되지 않는 경우,

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session

Manager\Environment\Path에 지정된 순서대로 디렉터리를 검색한다.

다. 나에서도 코드가 발견되지 않는 경우, HKEY\_CURRENT\_USER\Environment\Path에 지정

된 순서대로 디렉터리를 검색한다.

경로우선순위가 다음과 같을 경우

%SystemDrive%; (예: c:₩)

%SystemRoot%₩system32; (예: c:₩winnt₩system32)

%SystemRoot%;(예: c:₩winnt)

우선순위대로 윈도우 셸을 검색한다. 그런데 위와 같이 우선순위가 지정되어 있는 경우 공격자가 위조된 explorer.exe를 c:₩에 copy를 하면 다른 사용자가 동일한 시스템에 로그 온할 때 우선순위에 따라 위조된 explorer.exe를 실행하게 된다. 이때 위조된 explorer.exe는 트로이목마 프로그램으로서 작동하여 해당 사용자 권한으로 실행되게 된다.

## (2) 취약한 시스템

Microsoft Windows NT 4.0 Workstation

Microsoft Windows NT 4.0 Server

Microsoft Windows NT 4.0 Server, Enterprise Edition

Microsoft Windows NT 4.0 Server, Terminal Server Edition

Microsoft Windows 2000 Professional

Microsoft Windows 2000 Server

Microsoft Windows 2000 Advanced Server

## (3) 점검 방법

### 가. 증상

위조된 explorer.exe는 사용자에게 인증된 모든 작업을 수행할 수 있다. 미약한 권한을 가진 사용자가 로그 온할 경우, 이 코드는 미약한 작업만을 수행할 수 있는 반면 시스템이나 도메인에 주요 권한을 갖고 있는 사용자가 로그 온할 경우에는 심각한 손상을 야기할 수 있다. 위조된 explorer.exe는 트로이목마 프로그램으로 동작한다.

### 나. 점검방법

1. CD-ROM 이나 기타 설치매체에서 설치된 초기 시스템 바이너리 정보를 복사한 후 중요한 파일들에 대해 주기적으로 비교한다.
2. 트로이목마 프로그램을 정상 프로그램과 같은 파일 사이즈, timestamp 로 조작이 가능하므로 Tripwire 나 기타 무결성 점검도구를 이용하여 트로이목마 프로그램을 탐지한다.

3. 백신프로그램을 이용하여 바이러스, 백도어, 트로이목마 프로그램을 점검한다.  
이러한 경우 변종 프로그램이 지속적으로 나오기 때문에 백신 프로그램은  
최신버전으로 지속적으로 업데이트 하여야 한다.

(4) 보호대책

가. c:#\ 디렉토리에 explorer.exe 란 이름의 파일이 존재한다면 위조된 explorer.exe  
일 가능성이 매우 높으므로 이를 제거하여야 한다.

나. 다음 사이트에서 해당하는 패치를 적용한다.

Microsoft Windows NT 4.0 Workstation, Windows NT 4.0 Server, 그리고 Windows NT  
4.0 Server, Enterprise Edition:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23360>

Microsoft Windows NT 4.0 Server, Terminal Server Edition:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23421>

Microsoft Windows 2000 Professional, Server, Advanced Server:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23359>

나. Tripwire나 기타 무결성 점검도구를 이용하여 주기적으로 트로이목마 프로그램을  
탐지한다.

다. 백신프로그램을 이용하여 주기적으로 점검한다.

백신프로그램은 매일 온라인으로 자동 업데이트하도록 설정하고 항상 구동되어 있도  
록 한다. 또한 주기적으로 모든 파일에 대한 백신검사를 수행하도록 한다.

(5) 공격방법

※ 공격방법은 비공개함

## 2.4 패스워드 취약점 및 퍼미션 설정 취약점

### (1) 취약점 설명

윈도우즈 NT, 윈도우 2000 등 윈도우 계열의 OS에서 일반사용자 및 관리자 계정의 패스워드가 취약함으로 인하여 원격에서 쉽게 패스워드를 알아낼 수 있다. Windows의 패스워드 해시방식인 LanMan(LM) 해시는 패스워드가 7문자로 분리되어 구성되므로 자릿수가 10자리가 넘더라도 결국에는 7문자의 패스워드와 유사하다고 할 수 있다.

이러한 취약점 등에 의해 패스워드가 노출될 경우 관리자 또는 일반사용자 계정으로 원격에서 레지스트리에 접속이 가능하게 되므로 중요한 계정정보 또는 기타 정보를 읽거나 변경을 할 수 있다. 이것은 원격 레지스트리 서비스가 윈도우 NT, 윈도우 2000에서 디폴트로 설정되어 있기 때문에 계정정보를 알면 원격지에서 접속이 가능하다. 또한 각 파일시스템에 대한 퍼미션 설정이 잘못 되어 있을 경우 일반사용자의 권한으로 원격에서 접속하여 파일시스템을 읽어서 중요한 정보를 알아 낼 수 있다.

### (2) 취약한 시스템

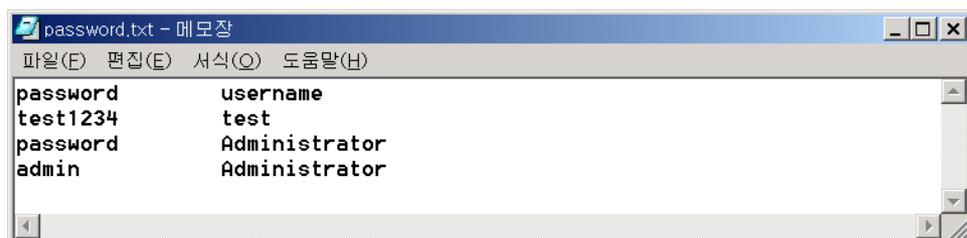
윈도우 계열 시스템(Windows NT, Windows 2000)

### (3) 점검 방법

가. 패스워드 취약점을 조사하기 위하여 cmd.exe에서 For 명령어를 이용하여 패스워드 취약점을 점검한다. For 명령어는 반복되는 명령어의 수행을 batch로 처리하기 위해서 윈도우에서 제공하는 명령어이다.

다음은 for명령어를 이용하여 password.txt에서 user id와 password를 읽어서 원격지에 있는 서버에 접속하는 방법이다.

- 1) for문에 사용하기 위한 패스워드 및 계정 목록(password.txt)을 만든다. 일반적으로 추측하기 쉬운 단어를 선택하여 만들거나 디폴트값으로 많이 사용하는 패스워드 또는 신상정보와 관련되는 패스워드를 넣어서 만든다.



[그림 2-10] 패스워드 목록

- 2) 위의 패스워드 파일의 패스워드 및 계정목록에 대해 for 명령어를 사용하여 반복적인 사용자 계정 및 패스워드 크랙을 한다. 다음 화면에서 사용자명 : test 패스워드:test1234가 잘 수행되었음을 보여준다.

```

cmd.exe의 바로 가기
D:\test>for /F "tokens=1,2*" %i in (password.txt) do net use \\172.16.5.104\IPC$ %i /u:%j

D:\test>net use \\172.16.5.104\IPC$ password /u:username
시스템 오류 1326이(가) 생겼습니다.

로그온 실패: 알 수 없는 사용자 이름이거나 암호가 틀립니다.

D:\test>net use \\172.16.5.104\IPC$ test1234 /u:test
명령을 잘 실행했습니다.
  
```

[그림 2-11] for를 이용한 세션 연결

- 3) 다음 화면은 원격지호스트(172.16.5.104)에 세션이 연결된 결과 화면이다.

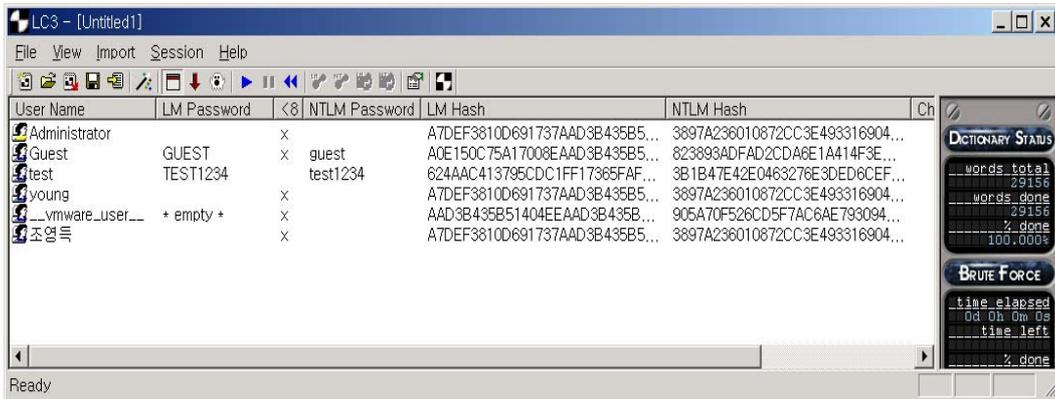
```

cmd.exe의 바로 가기
D:\test>net use
새 연결 정보가 저장되지 않습니다.

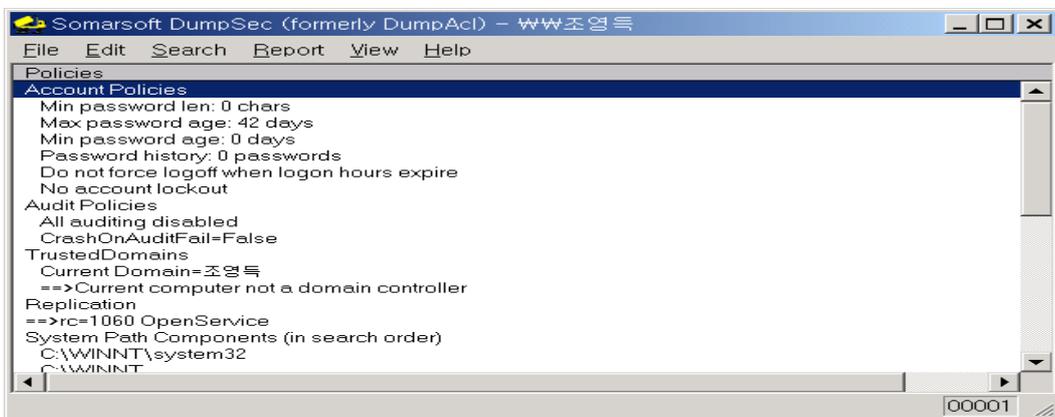
상태      로컬      원격      네트워크
-----
OK        \\172.16.5.104\IPC$  Microsoft Windows 네트워크
명령을 잘 실행했습니다.
  
```

[그림 2-12] for를 이용한 세션 연결 결과

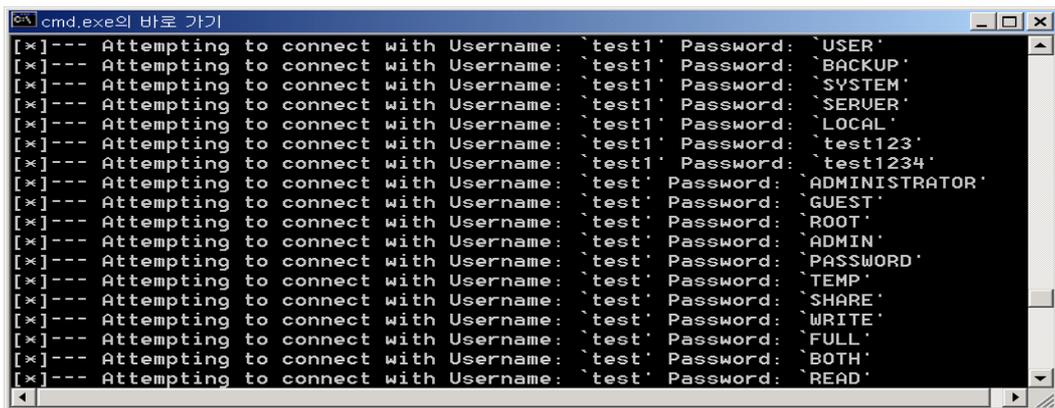
나. LC3, DumpSec과 같은 패스워드 점검 도구 또는 NAT(NetBIOS Auditing Tool)를 이용하여 로컬시스템에서의 패스워드 설정을 점검한다.



[그림 2-13] LC3를 이용한 취약한 패스워드 점검

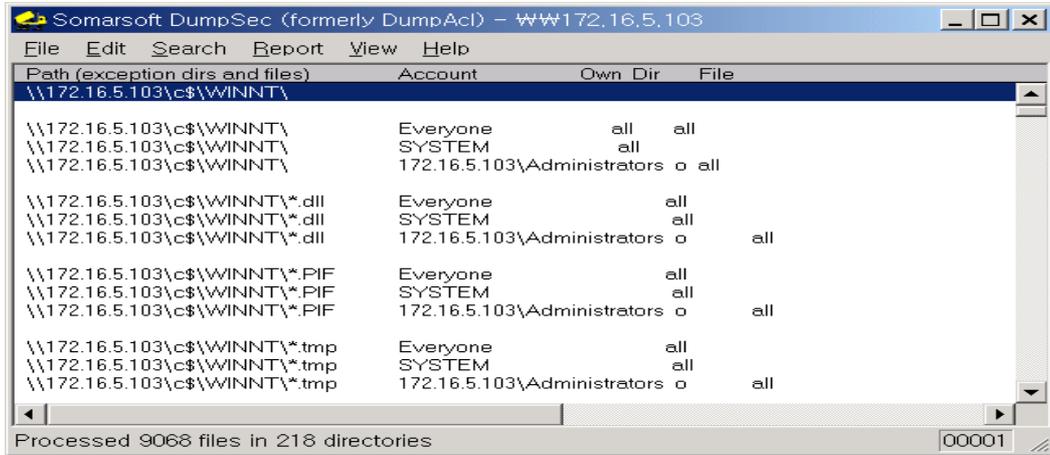


[그림 2-14] dumpsec을 이용한 계정정책 등의 각종 정책 점검



[그림 2-15] 원격지에서 NAT을 이용한 취약한 패스워드 점검

다. 파일시스템에 대한 퍼미션 설정을 점검하기 위하여 DumpSec과 같은 점검도구를 이용하여 잘못 설정된 퍼미션을 점검한다.



[그림 2-16] DumpSecdmf 이용한 파일 퍼미션 설정 점검

#### (4) 보호대책

가. 추측하기 어려운, 강력한 패스워드를 설정한다.

패스워드 정책의 설정은 제어판 > 관리도구 > 로컬보안정책 > 보안설정 > 계정정책 > 암호정책에서 환경에 적합하게 설정한다. 일반적으로 다음과 같이 패스워드 정책을 설정할 것을 권고한다.

- 숫자, 문자 및 특수문자를 혼용하여 암호최소 길이를 8자 이상으로 설정
- 최대 암호 사용기간을 네트워크 환경에 맞게 설정(일반적으로 1달 이내)
- “최근 암호 기억” 옵션을 사용하여 암호사용내역을 최소 6개 이상 유지하도록 설정(최근에 사용했던 패스워드 다시 사용 못하게 함)
- 기억이 쉽고 추측이 어려워야 함
- 특수 권한을 가진 사용자는 패스워드에 NUM-LOCK 등의 ASCII패스워드 사용

또한 다음과 같은 패스워드는 유추하기 쉽기 때문에 사용하지 않도록 한다.

- 개인에 관한 데이터(이름, 생년월일, 주소, 전화번호, FAX번호, 차량번호, 가족·친구 등 아는 사람에 대한 데이터)
- 사전에 있는 단어
- 유명한 고유명사(지명, 인명, 영화·만화·소설·TV·컴퓨터 게임 등에 등장하는 인물 또는 캐릭터명)
- 위와 같은 내용을 역으로 사용하는 것

나. 중요한 파일시스템에 대하여 정확한 퍼미션을 설정한다. 시스템관련파일 및 개인의 중요한 디렉토리는 다른 사용자가 접근하지 못하도록 퍼미션 설정을 한다. 일반적

으로 관리자와 사용자의 기본권한은 다음과 같이 설정된다.

- 관리자, 시스템, 작성자 겸 소유자는 GUI 모드 설치가 시작될 때 존재하는 모든 파일 시스템과 레지스트리 개체에 대한 모든 권한을 가진다.
- 사용자는 아래 위치에 대해서만 쓰기 권한을 허가받는다.

개체	사용 권한	설명
HKEY_Current_User	모든 권한	레지스트리의 사용자 부분
%UserProfile%	모든 권한	사용자 프로파일 디렉터리
All Users\Documents	수정	공유 문서 위치
All Users\Application Data	수정	공유 응용 프로그램 데이터 위치
%Windir%\Temp	동기화, 통과, 파일 추가, 하위 디렉터리 추가	시스템 단위의 임시 디렉터리. 이는 가장된 사용자의 사용자 단위 임시 디렉터리에 액세스하기 위해 프로파일을 로드할 필요가 없도록 서비스 기반 응용 프로그램에 허용되는 위치이다.

다음 표는 Windows 2000 레지스터리에 대한 기본 권한이다.

레지스트리 개체	사용자의 기본 권한
HKEY_LOCAL_MACHINE	
HKLM\Software	읽기
HKLM\Software\Classes\helpfile	읽기
HKLM\Software\Classes\hlp	읽기
HKLM\Software\MICROSOFT\Command Processor	읽기
HKLM\Software\MICROSOFT\Cryptography\OID	읽기
HKLM\Software\MICROSOFT\Cryptography\Providers\Trust	읽기
HKLM\SOFTWARE\MICROSOFT\Cryptography\Services	읽기
HKLM\SOFTWARE\MICROSOFT\Driver Signing	읽기
HKLM\SOFTWARE\MICROSOFT\EnterpriseCertificates	읽기
HKLM\SOFTWARE\MICROSOFT\Non-Driver Signing	읽기
HKLM\SOFTWARE\MICROSOFT\NetDDE	없음
HKLM\SOFTWARE\MICROSOFT\ole	읽기
HKLM\SOFTWARE\MICROSOFT\Rpc	읽기

HKLM\SOFTWARE\MICROSOFT\Secure	읽기
HKLM\SOFTWARE\MICROSOFT\SystemCertificates	읽기
HKLM\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\RunOnce	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DiskQuota	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Drivers32	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Font Drivers	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Font Mapper	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IniFileMapping	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Perflib	읽기(대화형 사용자를 통해)
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SecEdit	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Time Zones	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Windows	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Winlogon	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\AsrCommands	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Classes	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Console	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\EFS	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\ProfileList	읽기
HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Svchost	읽기
HKLM\SOFTWARE\Policies	읽기
<b>HKLM\System</b>	<b>읽기</b>
HKLM\SYSTEM\CURRENTCONTROLSET\Control\SecurePipeServers\winreg	없음
HKLM\SYSTEM\CURRENTCONTROLSET\Control\Session Manager\Executive	읽기
HKLM\SYSTEM\CURRENTCONTROLSET\Control\TimeZoneInformation	읽기
HKLM\SYSTEM\CURRENTCONTROLSET\Control\WMI\Security	없음
<b>HKLM\Hardware</b>	<b>읽기</b>
<b>HKLM\SAM</b>	<b>읽기</b>
<b>HKLM\Security</b>	<b>없음</b>
<b>HKEY_USERS</b>	
USERS\DEFAULT	읽기
USERS\DEFAULT\SOFTWARE\MICROSOFT\NetDDE	없음

HKEY_CURRENT_USER	모든 권한
HKEY_CLASSES_ROOT	= KLM\SOFTWARE\Classes+HKCU\SOFTWARE\Classes
HKEY_CURRENT_CONFIG	HKLM\System\CurrentControlSet\HardwareProfiles\Current

다. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 레지스트리키를 이용하여 허가받지 않은 사용자의 레지스트리의 원격접속을 제어한다.

- 윈도우 시작메뉴의 실행에서 regedt32.exe를 실행한다.
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg를 선택한다.
- 메뉴의 보안>사용권한을 선택한다.
- 실제 원격접속사용자만을 추가하고 필요없는 사용자는 제거한다.
- 상세한 내용은 2.2 원격레지스트리 액세스 인증 취약점의 보호대책 참조

#### (5) 공격방법

가. admin 권한 획득

- 먼저 NAT(NetBIOS Auditing Tool)와 같은 tool을 이용하여 원격지에 있는 공격대상 서버의 사용자 및 패스워드를 알아낸다.

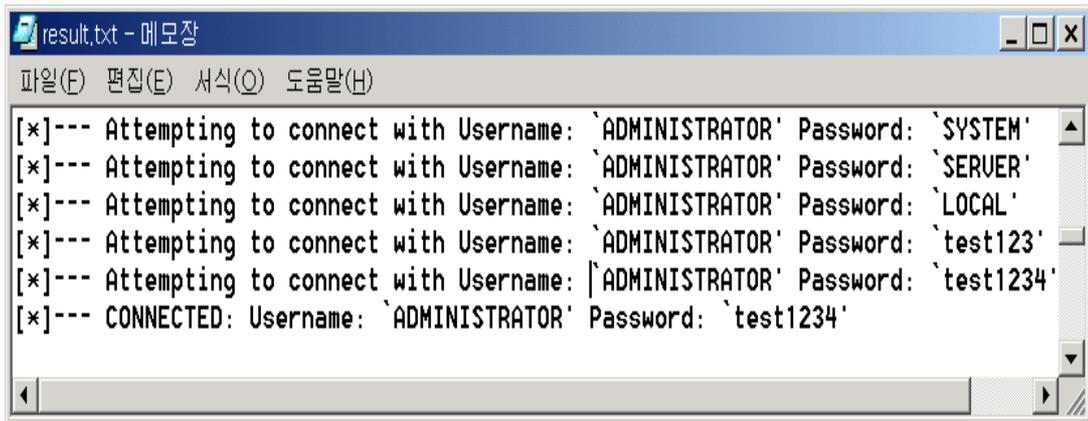
```

cmd.exe의 바로 가기
D:\#test#nat>nat
usage: nat [-o filename] [-u userlist] [-p passlist] <address>
D:\#test#nat>nat -o result.txt -u userlist.txt -p passlist.txt 172.16.5.103
[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt
[*]--- Checking host: 172.16.5.103

```

[그림 2-17] NAT를 이용한 사용자 계정 및 패스워드 크랙

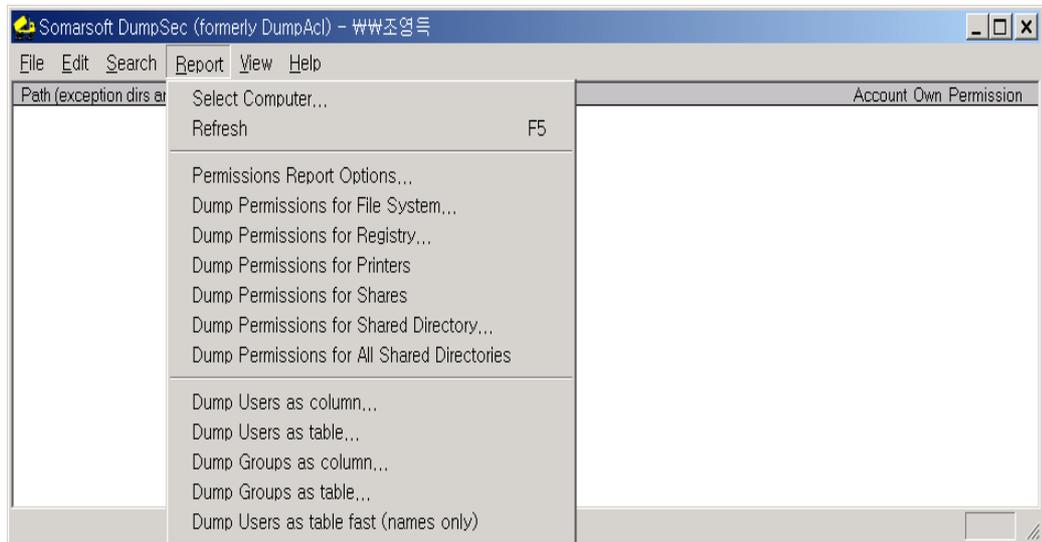
- 아래의 결과 파일(result.txt)를 보면 username : administrator, password : test1234로 연결이 되었음을 알 수 있다.



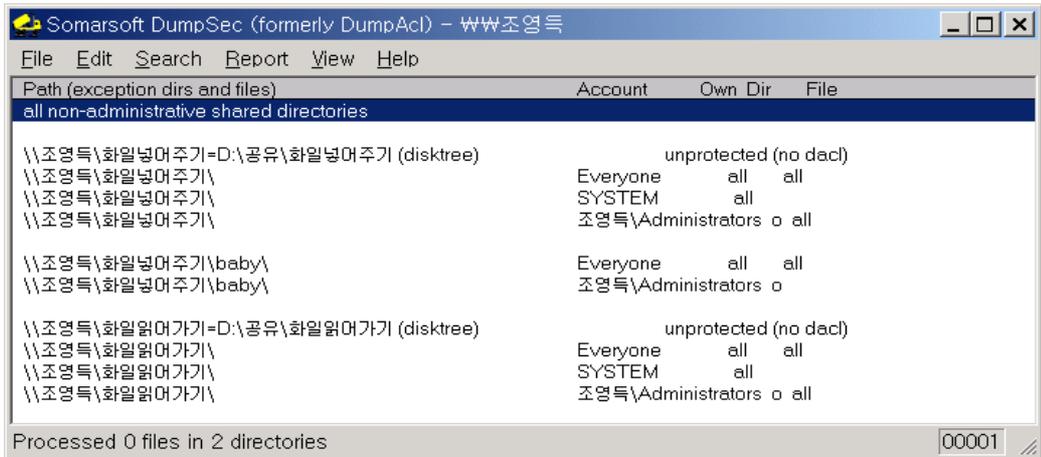
[그림 2-18] NAT를 이용한 사용자 계정 및 패스워드 크랙 결과

나. admin 권한을 획득한 후에는 자신의 PC의 admin에 대하여 공격대상서버의 admin패스워드와 동일하게 설정한다. 이렇게 하면 공격대상서버의 특별한 인증없이 접근이 가능하다. 단 remote registry service가 구동되어야 하는데 대부분 디폴트로 구동되어진다.

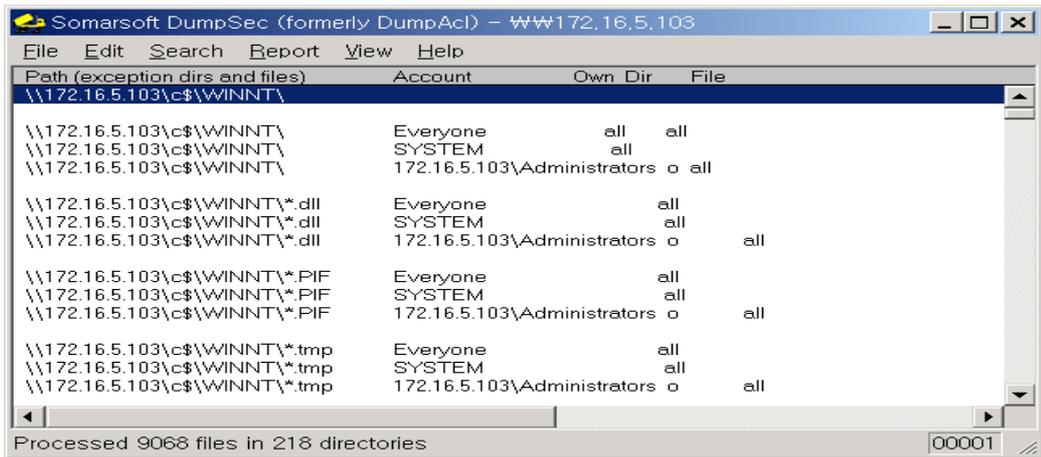
다. 공격대상서버의 레지스트리에 접근이 가능하기 때문에 레지스트리 정보를 dump받는다. 레지스트리 dump를 위해서 regdmp.exe 또는 DumpSec 과 같은 도구를 사용한다. 여기서는 윈도우용 도구인 DumpSec을 사용하여 레지스트리를 dump한다.



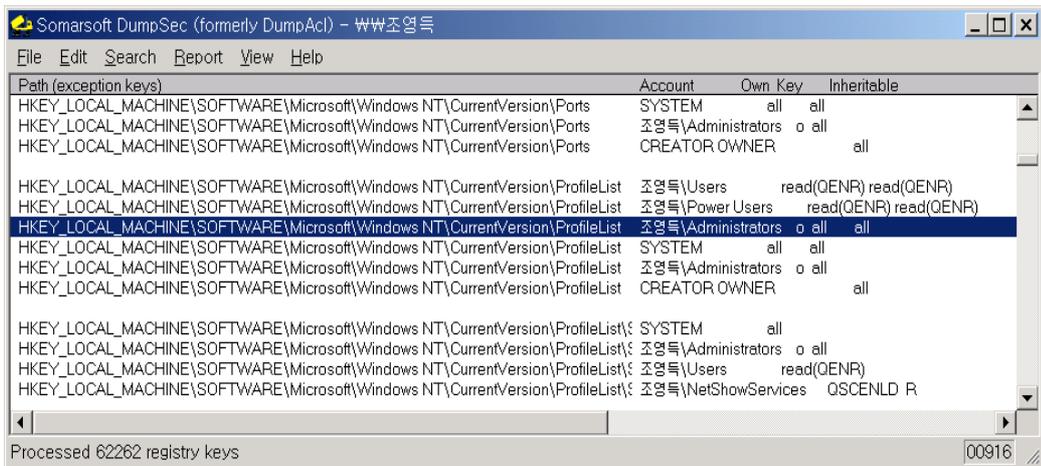
[그림 2-19] DumpSec을 이용한 레지스트리 dump



[그림 2-20] 공유디렉토리에 대한 퍼미션 DUMP



[그림 2-21] 파일시스템에 대한 퍼미션 DUMP



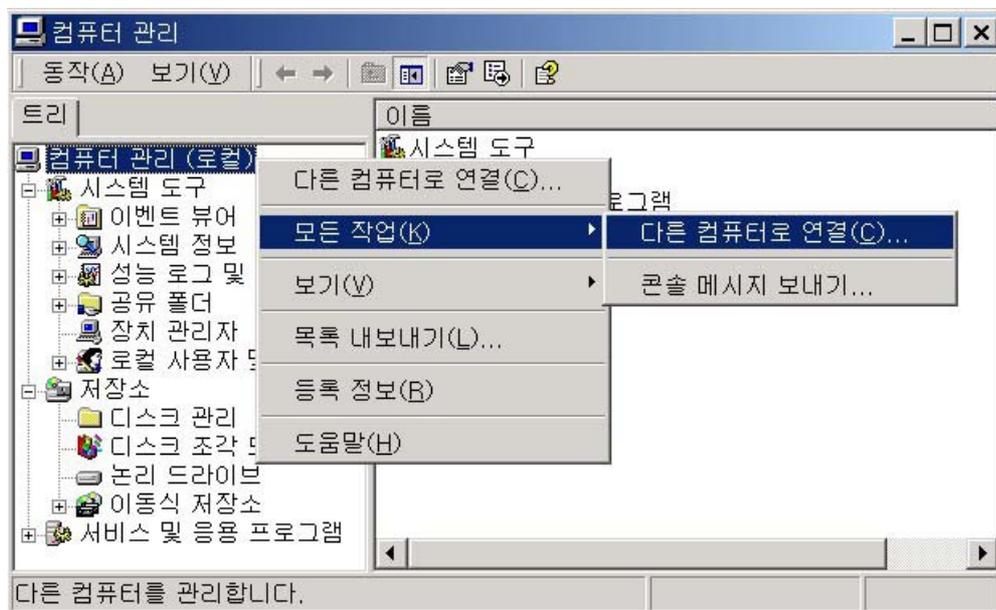
[그림 2-22] 레지스트리에 대한 퍼미션 DUMP

## 2.5 컴퓨터관리콘솔에 의한 원격 접근 취약점

### (1) 취약점 설명

Windows 2000 에서 [내 컴퓨터]를 오른쪽 마우스 버튼으로 클릭하고 관리를 선택하면 컴퓨터 관리 콘솔(The Computer Management console)을 바로 열 수 있다. 컴퓨터 관리 콘솔은 Microsoft Management Console (MMC) snap-in 몇 개를 묶어놓은 것으로 한번에 여러가지를 살펴볼 수 있다. 그런데 컴퓨터 관리 콘솔로 로컬 컴퓨터 뿐만 아니라 같은 peer-to-peer network 에 있는 다른 Windows 2000 컴퓨터도 원격으로 다룰 수 있다. 필요하면 원격으로 로그오프하거나 컴퓨터를 셧다운할 수도 있다. 그런데 관련 권한 획득시 원격에서 시스템을 모두 통제할 수 있는 취약점이 존재한다. 원격지에 있는 PC 의 컴퓨터 관리콘솔에서 할 수 있는 일은 다음과 같다.

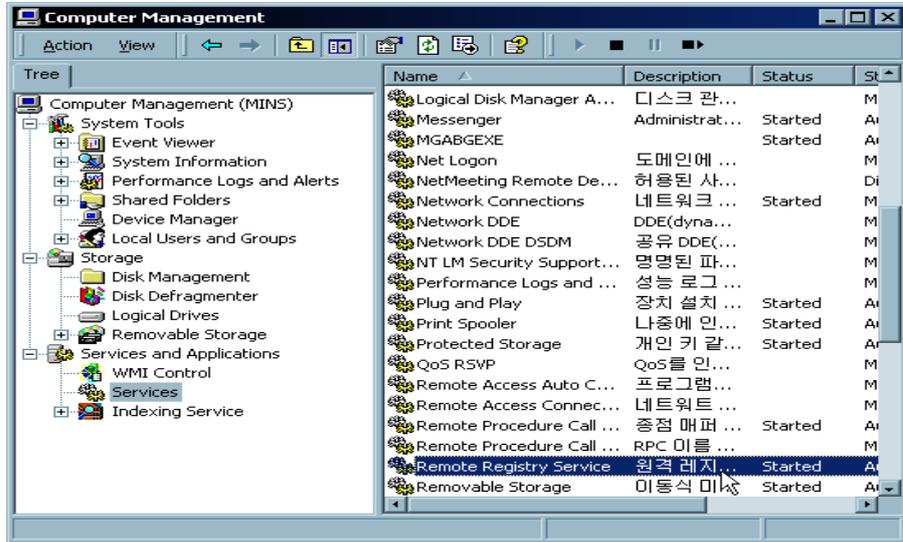
가. 컴퓨터 관리 콘솔에서 맨 위에 있는 "컴퓨터 관리 (로컬)"을 오른쪽 마우스 버튼으로 클릭하고 "다른 컴퓨터로 연결"을 선택하면 컴퓨터 선택 박스가 뜨면서 같은 워크그룹에 있는 다른 컴퓨터가 보인다. 다루고 싶은 컴퓨터를 고르고 확인 버튼을 클릭하면 "컴퓨터 관리 (로컬)"이 아니라 "컴퓨터 관리 (원격 컴퓨터 이름)"으로 바뀐다.



[그림 2-23] 컴퓨터 관리 콘솔을 이용한 원격 컴퓨터 연결

나. 다음 그림은 Windows 2000 Professional 영어 버전 기계에서 Windows 2000 Professional 한국어판을 설치한 컴퓨터를 이어본 것이다. 서비스 설명이

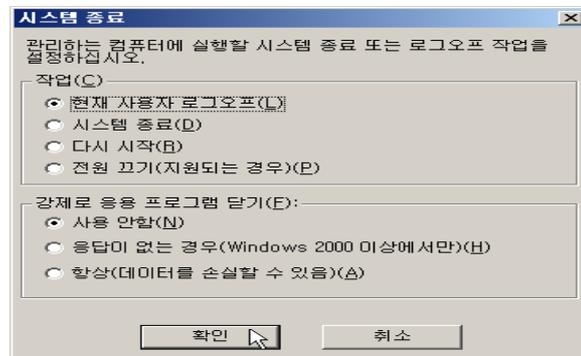
친절하게 한글로 나타난 것을 볼 수 있다. 그리고 원격 컴퓨터도 로컬 컴퓨터와 거의 비슷하게 다룰 수 있는 것을 살펴볼 수 있다.



[그림 2-24] 원격 컴퓨터 연결 결과

다. 컴퓨터 관리 콘솔로 원격 컴퓨터를 연결하였다면 로컬 로그인한 유저를 로그오프 시키거나 컴퓨터를 셧다운할 수 있다.

- 1) [컴퓨터 관리 (원격 컴퓨터 이름)]을 오른쪽 마우스 버튼으로 클릭하고 등록 정보를 선택한다.
- 2) 고급 탭에서 [시작 및 복구] 버튼 클릭한다.
- 3) 시스템 종료 버튼 클릭한다.
- 4) 작업과 강제로 응용 프로그램 닫기에서 어떻게 할 것인지 고르고 확인 버튼 클릭한다.



[그림 2-25] 컴퓨터 관리콘솔에서 원격컴퓨터 시스템 종료

(2) 취약한 시스템

Windows 2000, Windows NT

(3) 보호대책

가. 추측하기 어려운, 강력한 패스워드를 설정한다.

패스워드 정책의 설정은 제어판 > 관리도구 > 로컬보안정책 > 보안설정 > 계정정책 > 암호정책에서 환경에 적합하게 설정한다. 일반적으로 다음과 같이 패스워드 정책을 설정할 것을 권고한다.

- 숫자, 문자 및 특수문자를 혼용하여 암호최소 길이를 8자 이상으로 설정
- 최대 암호 사용기간을 네트워크 환경에 맞게 설정(일반적으로 1달 이내)
- “최근 암호 기억” 옵션을 사용하여 암호사용내역을 최소 6개 이상 유지하도록 설정(최근에 사용했던 패스워드 다시 사용 못하게 함)
- 기억이 쉽고 추측이 어려워야 함
- 특수 권한을 가진 사용자는 패스워드에 NUM-LOCK 등의 ASCII 패스워드 사용

또한 다음과 같은 패스워드는 유추하기 쉽기 때문에 사용하지 않도록 한다.

- 개인에 관한 데이터(이름, 생년월일, 주소, 전화번호, FAX번호, 차량번호, 가족·친구 등 아는 사람에 대한 데이터)
- 사전에 있는 단어
- 유명한 고유명사(지명, 인명, 영화·만화·소설·TV·컴퓨터 게임 등에 등장하는 인물 또는 캐릭터명)
- 위와 같은 내용을 역으로 사용하는 것

나. 중요한 파일시스템에 대하여 정확한 퍼미션을 설정한다. 시스템관련파일 및 개인의 중요한 디렉토리는 다른 사용자가 접근하지 못하도록 퍼미션 설정을 한다. 일반적으로 관리자와 사용자의 기본권한은 다음과 같이 설정된다.

- 관리자, 시스템, 작성자 겸 소유자는 GUI 모드 설치가 시작될 때 존재하는 모든 파일 시스템과 레지스트리 개체에 대한 모든 권한을 가진다.
- 사용자는 아래 위치에 대해서만 쓰기 권한을 허가받는다.

개체	사용 권한	설명
HKEY_Current_User	모든 권한	레지스트리의 사용자 부분
%UserProfile%	모든 권한	사용자 프로파일 디렉터리
All Users\Documents	수정	공유 문서 위치
All Users\Application	수정	공유 응용 프로그램 데이터 위치

Data		
%Windir%\Temp	동기화, 통과, 파일 추가, 하위 디렉터리 추가	시스템 단위의 임시 디렉터리. 이는 가장된 사용자의 사용자 단위 임시 디렉터리에 액세스하기 위해 프로파일을 로드할 필요가 없도록 서비스 기반 응용 프로그램에 허용되는 위치이다.

다. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 레지스트리키를 이용하여 허가받지 않은 사용자의 레지스트리의 원격접속을 제어한다.

- 윈도우 시작메뉴의 실행에서 regedt32.exe를 실행한다.
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg를 선택한다.
- 메뉴의 보안>사용권한을 선택한다.
- 실제 원격접속사용자만을 추가하고 필요없는 사용자는 제거한다.
- 상세한 내용은 2.2 원격레지스트리 액세스 인증 취약점의 보호대책 참조

## 2.6 백오리피스 등 트로이목마를 이용한 원격 레지스트리 접근 취약점

### (1) 취약점 설명

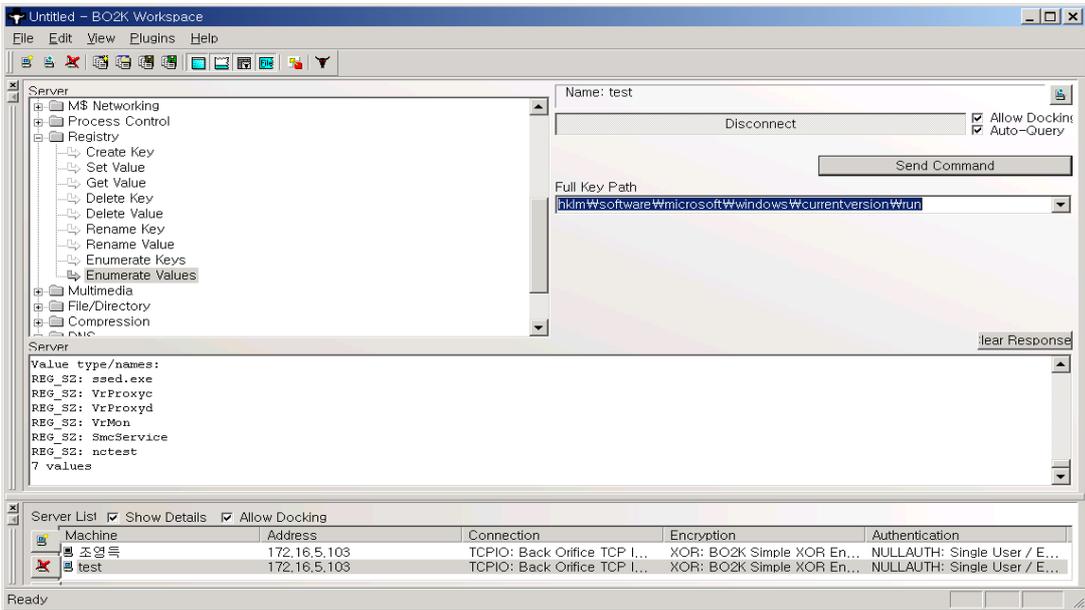
백오리피스, 넷버스와 같은 트로이목마 프로그램은 악의의 목적을 위해 만들어진 백도어 프로그램으로 원격지 네트워크에서 사용자가 모르게 정보 수집, 시스템 명령어 수행, 시스템 재구성, 레지스트리 변경 등 시스템을 통제할 수 있는 클라이언트/서버 프로그램이다. 시스템상에서 백오리피스 서버 프로그램을 수행하기 때문에, 침입자는 특정 IP주소에 원격으로 접속할 수 있다. 트로이목마 프로그램은 간단한 모니터링 툴로 사용될 수 있지만 이것의 주요 목표는 다른 시스템을 재구성하고 데이터를 수집하는 등의 비인가된 통제를 하기 위한것으로 사용자에게 매우 심각한 피해를 끼칠 수 있다.

다음은 많이 사용되는 트로이목마인 백오리피스의 주요기능이다.

- 시스템 제어 : 공격대상 시스템을 재부팅하거나 셧다운 시킬 수 있으며 공격대상시스템의 사용자가 입력하는 키보드 내용을 기록할 수 있다. 또한 사용자 정보, 시스템 정보, 메모리 사용현황, 화면보호기 암호 등과 같은 정보 등도 수집할 수 있다.
- 파일시스템 제어 : 복사, 이름변경, 삭제, 보기, 파일 탐색 등을 할 수 있다.
- 프로세스 제어 : 프로세스 리스팅, 프로세스 제거 등
- 레지스트리 제어 : 레지스트리 리스팅, 생성, 삭제 및 값의 변경
- 네트워크 제어 : 사용가능한 네트워크 자원을 보여주고 모든 연결의 접속, 해제를 알려줌

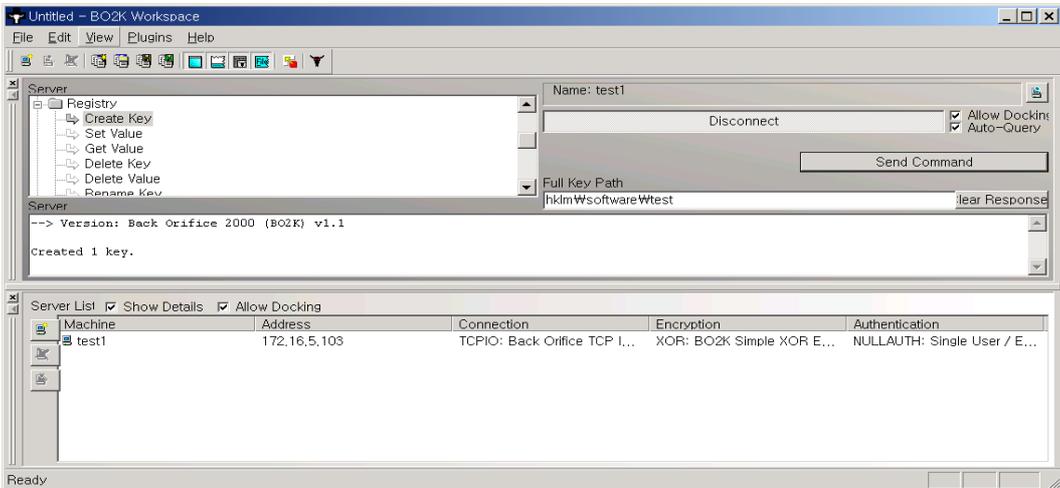
이와 같이 트로이목마 프로그램의 기능은 아주 강력하다. 특히 위험한 것은 파일명을 바꾸거나 또는 레지스트리에 등록된 정보 들을 변조함으로써 시스템에 심각한 손상을 입힐 수 있다는 것이다.

다음은 원격지에서 공격대상서버의 레지스트리를 열람하는 그림이다.



[그림 2-26] 백오리피스를 이용하여 공격대상서버 레지스트리 열람

또는 레지스트리 키를 생성하거나 레지스트리 값을 변경할 수도 있다.



[그림 2-27] 백오리피스를 이용하여 공격대상서버 레지스트리값 변경

(2) 취약한 시스템

Windows 2000, Windows NT 등 모든 Windows 시스템

(3) 점검 방법

가. 트로이 목마 탐지 프로그램(cleaner, BO Detect 등) 또는 바이러스백신 프로그램을 이용하여 트로이목마 설치여부를 탐지한다.

나. HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsServices 레지스트리에 의심스러운 실행파일(.exe)이 있는지 점검한다.

다. 윈도우 탐색기에서 c:\windows\system 디렉토리에 .exe 파일이 있는지 점검한다.(백오리피스경우)

#### (4) 보호대책

가. 시스템에 작동중인 트로이목마 프로그램을 탐지하는 것은 프로그램마다 서로 다른 매우 많은 설정(변수)들이 있기 때문에 매우 어렵다. 따라서 이에 대한 권고책으로 네트워크상에서의 공격을 인식하기 위한 침입탐지 소프트웨어와 항상 새롭게 업데이트된 백신 프로그램을 사용한다.

나. 시스템의 파일 액세스 권한에 제한을 두고 일반작업을 할 때는 관리자 권한이 아닌 일반사용자 권한으로 작업을 할 것을 권고한다. 이러한 경우 트로이목마가 실행되더라도 일반사용자권한을 가짐으로 시스템에 치명적인 결과를 초래할 수 있는 작업을 방지할 수 있다.

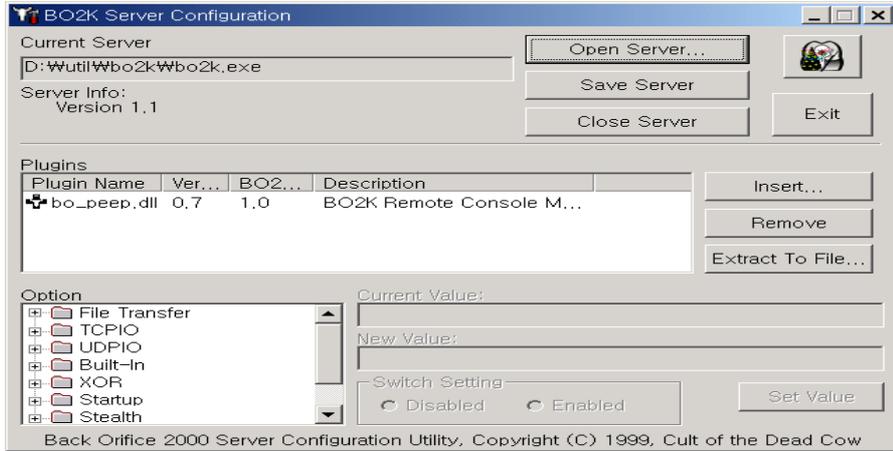
다. 성능이 검증된 트로이목마 제거 툴을 사용하여 트로이목마 프로그램을 제거하고 바이러스 백신 프로그램을 사용하여 방어하도록 한다.

라. 그외 사용자들은 다음과 같은 주의사항을 염두하여 컴퓨터 안전예방책을 취해야 한다.

- 모르는사람으로부터 전송되어온 메일의 첨부물은 함부로 개봉하지 않는다.
- 인터넷 접속시, 보안대책없는 네트워크파일은 공유하지 않도록 유의한다.
- 와레즈사이트에서 다운받은 프로그램에 특히 주의하도록 한다. 백오리피스와 실행파일(\*.exe)을 합치는 툴을 이용하여 일반프로그램 실행파일로 위장하여 제공하기도 한다.

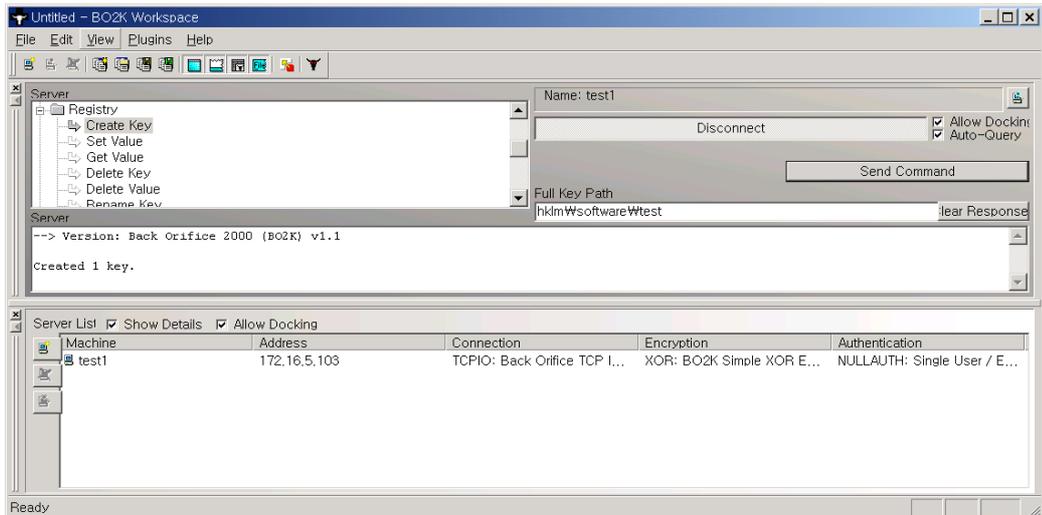
#### (5) 공격방법

가. 백오리피스 또는 넷버스와 같은 트로이목마 프로그램을 설치하고 환경을 적당하게 설정한다.



[그림 2-28] 백오리피스 서버 환경설정

- 나. 위와 같이 환경설정을 한 후 저장된 bo2k.exe 파일을 상대 컴퓨터에서 실행을 시키거나 아니면 다른 파일로 위장하여 전송 후 상대로 하여금 실행 하도록 만든다. 일반적으로 바인딩 툴(joiner 등)을 사용하여 그래픽파일이나 음악파일 속에 bo2k.exe 를 바인딩하여 실행파일의 실행시 bo2k.exe 의 실행 여부를 눈치채지 못하도록 한다. 즉 그래픽 파일과 묶어서 보냈을 경우 상대방은 그래픽 파일만 볼 수 있고 bo2k.exe 가 실행 되는지는 모른다.
- 다. bo2k.exe 가 실행되면 공격자는 원격지에서 다음과 같이 백오리피스 서버에 접속하여 레지스트리를 생성하거나 변경할 수 있다.



[그림 2-29] 백오리피스를 이용한 레지스트리 생성

### 3. 참고자료

- (1) O' Relly, "Windows 2000 Registry", 한빛미디어, 2001
- (2) Joel Scambrary, Stuart McClure 외, "Hacking Exposed Second Edition", 사이버출판사, 2001
- (3) Mark Minasi, Christa Anderson 외, "Mastering Windows 2000 Server", 삼각형프레스, 2001
- (4) Mathrew Strebe, Charles Perkins 외, "NT 네트워크 보안", 삼각형프레스, 1999
- (5) <http://support.microsoft.com/directory/worldwide/ko/kblist/list/winnt.htm?&gssnb=1>
- (6) <http://www.securityfocus.com/archive/88/170715>
- (7) <http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=remote+registry+access&type=archives>
- (8) [http://www.ntfaq.co.kr/search\\_list.asp?category=faq\\_content&keyword=%B7%B9%C1%F6%BD%BA%C6%AE%B8%AE](http://www.ntfaq.co.kr/search_list.asp?category=faq_content&keyword=%B7%B9%C1%F6%BD%BA%C6%AE%B8%AE)
- (9) <http://secinf.net/info/nt/reg/ntreg.html>
- (10) <http://www.somarsoft.com/index.html>
- (11) [http://www.cert.org/tech\\_tips/win\\_intruder\\_detection\\_checklist.html](http://www.cert.org/tech_tips/win_intruder_detection_checklist.html)
- (12) <http://www.microsoft.com/korea/technet/security/current.asp>
- (13) <http://www.jsiinc.com/default.htm?/reghack.htm>
- (14) <http://www.winguides.com/registry/category.php/45/>
- (15) <http://www.cotse.com/tools/netbios.htm>