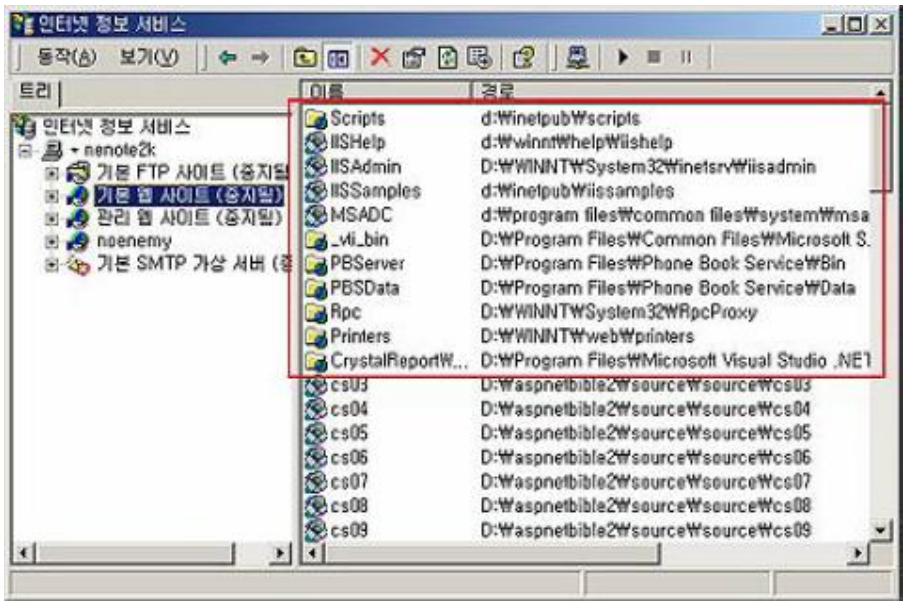
IIS 웹 서버 보호를 위한 방법

1. 필요한 구성요소만 설치한다.

대다수의 악의적인 공격은 초기 기본 설정으로 IIS 서버가 구성되어 있다고 가정하고 취약점을 노리는 경우가 많으므로 FTP나 NNTP, SMTP, Server Extensions 등의 서비스들은 사용하지 않는 경우에는 설치하지 않는 것이 보안 및 관리적인 측면에서 좋다.

IIS 를 설치한 후에 [관리도구] - [인터넷 서비스 관리자]를 실행하여 확인해 보면 다음과 같이 '기본 웹 사이트'와 그 하위에 IISHelp, MSADC, Printers, Scripts 와 같은 가상 디렉토리가 기본적으로 구성되어 있음을 알 수 있다. 그러나 이러한 기본 구성 또한 악의적인 공격의 대상이 된다. 예를 들면 ADSI 스크립트를 이용해서 기본 웹 사이트에 대한 설정을 변경한다든지 MSADC 가상 디렉토리를 통한 서버 자원 접근 등이 가능하다.



물론 이러한 문제점들은 최신 서비스 팩과 보안 패치를 설치함으로써 해결이 되지만, 보안에 관심이 있는 관리자의 경우에는 '기본 웹 사이트'를 중지 또는 제거하고 초기 웹 서버의 루트 경로인 '%system drive% \ inetpub \ wwwroot'가 아닌 다른 위치에 웹 서버를 위한 루트 폴더를 만들어 사용한다. (위 그림을 보면 '기본 웹 사이트'가 중지되어 있고 'noenemy'라는 새로운 웹 사이트를 만들어 운영하고 있음을 알 수 있다.)

2. 최신의 패치와 업데이트를 유지하라.

Win2000에서 제공하는 IIS 5.0 버전대신 Win2003에서 IIS 6.0 버전의 사용을 권장한다. 단, OS 자체를 2003으로 변경해야 IIS 6.0 버전을 사용할 수 있다.

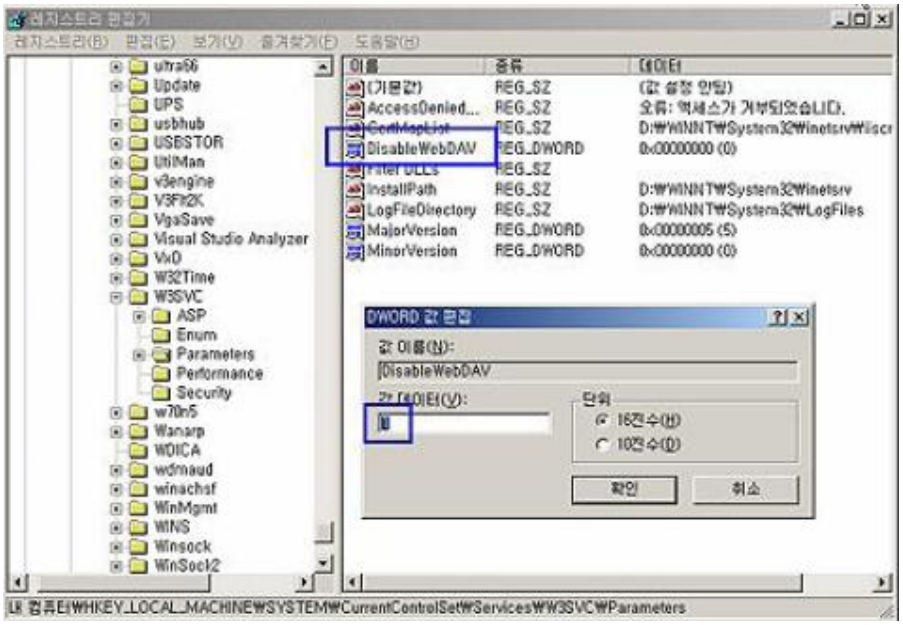
운영체제의 서비스 팩과 보안 패치를 최신 버전으로 유지하는 것은 보안 사고를 예방하기 위한 기본적인 과제이다.

3. 프로토콜 설정으로 웹 서버를 보호한다.

불필요한 프로토콜을 비활성화시킴으로써 잠재적인 위협요소를 줄일 수 있다. 이러한 프로토콜에는 WebDAV 나 NetBIOS, SMB 이 있고 TCP/IP 스택을 강화하는 것도 도움이 된다.

3.1 WebDAV 비활성화하기

WebDAV(Web Distributed and Versioning)는 웹서버 상에 존재하는 파일들을 공동으로 편집·관리하기 위한 도구로서 HTTP 와 같은 웹 운영프로토콜의 확장된 형태이다. 2003년 3월에 IIS 에서 지원하는 WebDAV에서 버퍼오버플로우 취약점이 발견되면서 주요 공격대상이 되고 있다. IIS 설치시 WebDAV가 기본으로 설치되기 때문에 사용하지 않는 경우 제거하는 것이 좋다. 레지스트리 편집기(Regedit.exe)를 실행하고,
HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W3SVC \ Parameters
레지스트리 키를 찾아 DisableWebDAV라는 DWORD 값을 만들어 '1'로 설정한다. 변경된 값을 적용하기 위해서는 IIS를 재시작하면 된다.



3.2 NetBIOS 비활성화하기

NetBIOS 는 별개의 컴퓨터 상에 있는 애플리케이션들이 근거리통신망 내에서 서로 통신할 수 있게 해주는 프로토콜로서 Windows 에 의해 채택되어 있다. 만약 웹 서버에서 네트워크를 통한 다른 컴퓨터와의 공유가 필요 없다면 NetBIOS를 제거함으로써

DDos(Distributed Denial of Service) 공격이나 호스트 열거(host enumeration)에 대한 위험 요소를 줄일 수 있다. NetBIOS 는 다음과 같은 포트를 사용한다.

◦ TCP 와 UDP 137번 포트 (NetBIOS name service)

◦ TCP 와 UDP 138번 포트 (NetBIOS datagram service)

◦ TCP 와 UDP 139번 포트 (NetBIOS session service)

TCP/IP 에서 NetBIOS 를 비활성화하는 방법은 다음과 같다.

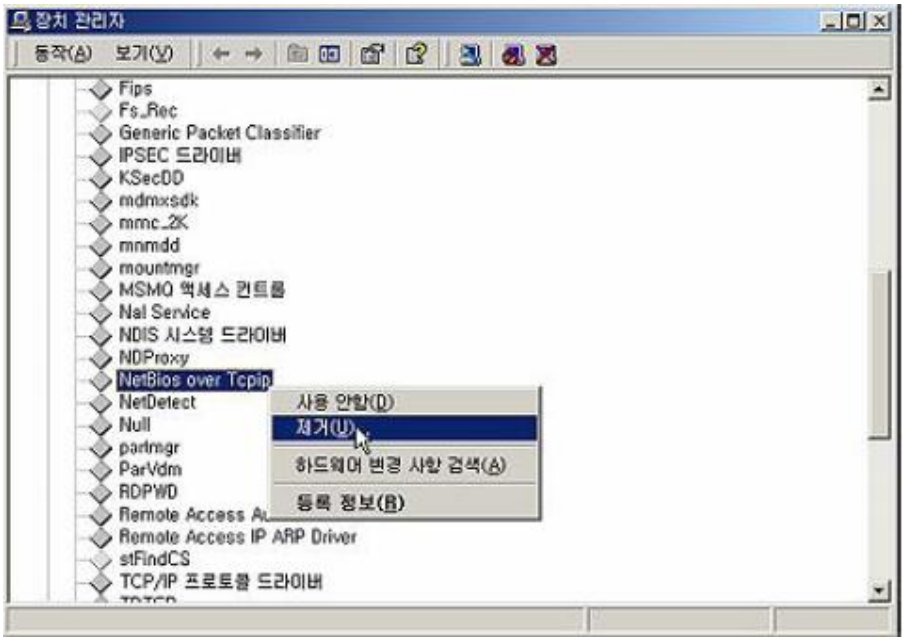
① 바탕화면 또는 제어판에서 [내 컴퓨터]의 등록정보에서 [하드웨어] 탭을 선택한다.

② [장치관리자]를 실행한다.

③ [장치관리자]의 [보기] 메뉴에서 [숨김 장치 표시]를 선택한다.

④ [장치관리자] 목록에서 [비 플러그 앤 플레이 드라이버]를 선택한다.

⑤ 하위 목록에서 [NetBios over Tcpip]를 선택하고 [제거] 한다.



3.3 SMB 비활성화 하기

SMB(Session Message Block) 프로토콜은 Windows에서 디스크와 프린터를 네트워크 상에서 공유하는데 사용된다. SMB 는 다음과 같은 포트를 사용한다.

◦ TCP 139 번 포트

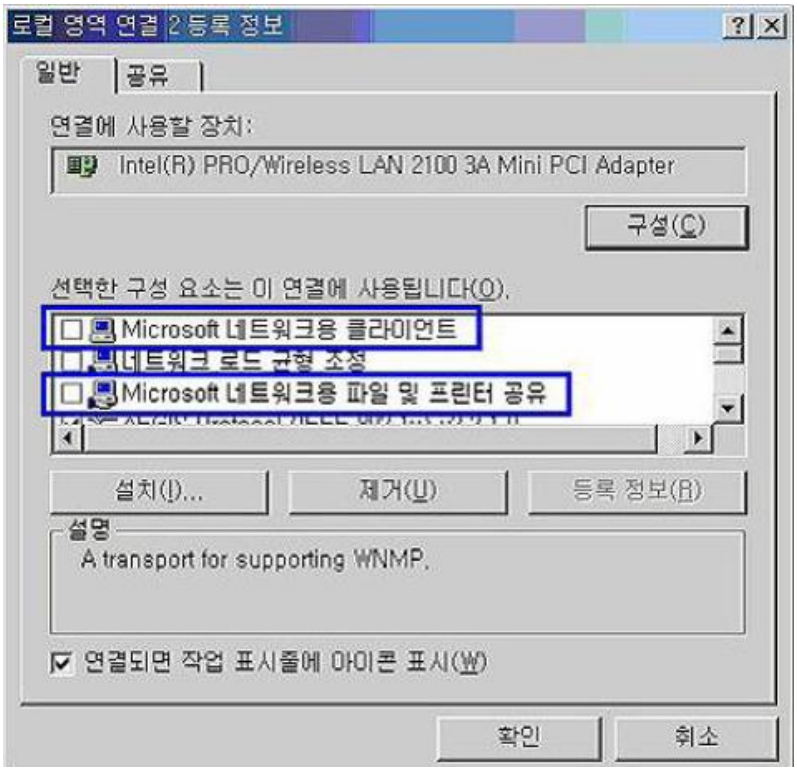
◦ TCP 445 번 포트

SMB를 비활성화하려면 다음과 같은 방법으로 TCP/IP 에서 SMB를 언바인드 시키면 된다.

① 바탕화면 또는 제어판에서 [네트워크 환경]의 [등록정보]를 실행한다.

② 현재 인터넷에 접속된 연결의 [등록정보]를 선택한다.

③ [Microsoft 네트워크용 클라이언트] 항목과 [Microsoft 네트워크용 파일 및 프린터 공유] 항목의 체크를 해제한다.



4. 계정관리를 철저하게 한다.

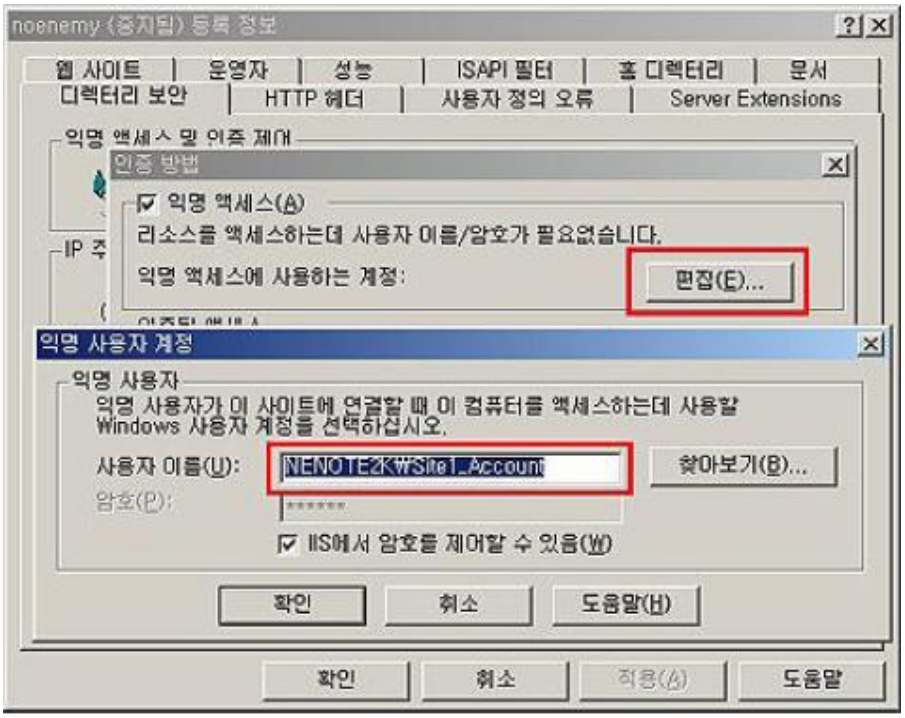
서버에서 사용하지 않는 계정은 제거하고, Guest 계정을 비활성화 시킨다. Guest 계정의 활성화 여부는 [컴퓨터 관리] 도구에서 [로컬 사용자 및 그룹]의 [사용자] 메뉴의 목록에서 확인할 수 있다.

기본적으로 관리자에게 지정되는 Administrator 계정은 컴퓨터에 대한 모든 권한을 가지므로 악의적인 목적으로 사용하기 위한 목표가 된다. 따라서 이 계정의 이름을 다른 이름으로 변경하고 유추하기 어려운 복잡한 패스워드를 사용하는 것이 좋다.

인터넷으로 익명으로 접근하는 사용자들은 IIS 설치시 기본적으로 생성되는 IUSR_Machine(서버의NetBIOS명) 계정으로 접근하게 된다. 예를 들어 'WebSvr'라는 이름의 서버에는 'IUSR_WebSvr'이라는 계정이 생성된다. 이 계정을 비활성화하고 웹 서버의 익명 접속에 사용할 계정을 직접 정의하는 것이 좋다.

웹 애플리케이션의 기능을 제공하는데 필요한 최소한의 권한을 가지는 계정을 만들고, 인터넷관리자에서 웹 애플리케이션 별로 직접 정의한 계정을 지정하면 서버 상에 여러 개의 웹 사이트를 운영하는 경우 로그 분석에도 용이하다.

특정 웹 사이트에 대해서 익명 연결에 사용할 계정을 지정하려면 다음 그림과 같이 [인터넷관리자]에서 해당 사이트의 [등록정보]-[디렉토리 보안]-[익명 액세스 및 인증 제어]- [편집]에서 익명 사용자 계정을 지정하면 된다.



5. **익명 로그온(널 세션)을 비활성화 한다.**

널 세션(Null Session) 접속은 인증을 받지 않은 상태에서 해당 컴퓨터에 접근하는 것을 의미하며 해커들은 이를 이용해서 원격 컴퓨터의 정보를 제공 받을 수 있고, 특정 권한으로 승격하거나 DoS 공격을 수행할 수도 있다. 널 세션 접속을 허용하지 않으려면 레지스트리 편집기를 이용해서 'HKLM \ System \ CurrentControlSet \ Control \ LSA' 키의 RestrictAnonymous 값을 '1'로 설정하면 된다.

6. **불필요한 공유를 제거한다.**

서버에서 사용되지 않는 공유를 제거하고 사용중인 공유 자원에 대해서는 NTFS 권한을 부여함으로써 자원을 보호할 필요가 있다. 특히 기본적으로 공유가 생성될 때 모든 사용자들에게 모든 권한이 부여되므로 NTFS 권한을 적용해서 필요한 사용자에게만 접근을 허용하도록 관리해야 한다.

또한 관리목적에서 사용되는 C$, ADMIN$와 같은 관리 공유를 사용하지 않는다면 제거하는 것이 권장된다. 관리 공유를 사용하지 않으려면 레지스트리 편집기를 이용해서 HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters키에 AutoShareServer와 AutoShareWks 값을 REG_DWORD로 만들고 '0'으로 설정하면 된다.

7. **감사관리**

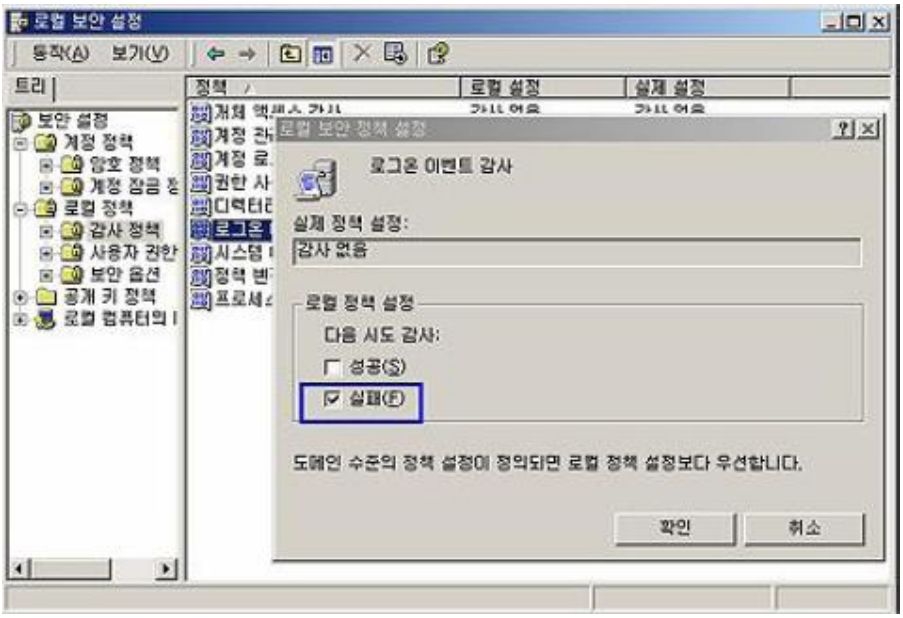
감사관리는 시스템 공격을 막지는 못하지만 진행중인 공격이나 침입자를 인식하고 공격의

흔적을 추적하는데 많은 도움을 준다. 웹 서버의 감사정책 수준을 높이고 NTFS 권한으로 로그 파일을 보호함으로써 공격자가 로그파일을 지우거나 변조하는 것을 방지하는 것도 필요하다.

7.1 로그인 실패 로그를 기록한다.

시스템에 로그인 하는데 실패한 이벤트에 대해서는 반드시 로그를 기록해야 한다. 로그를 통해서 암호에 대한 무차별 대입 공격이나 사전 공격의 흔적을 찾을 수 있으며 공격자가 어떠한 계정으로 접근을 시도했는지도 알 수 있다.

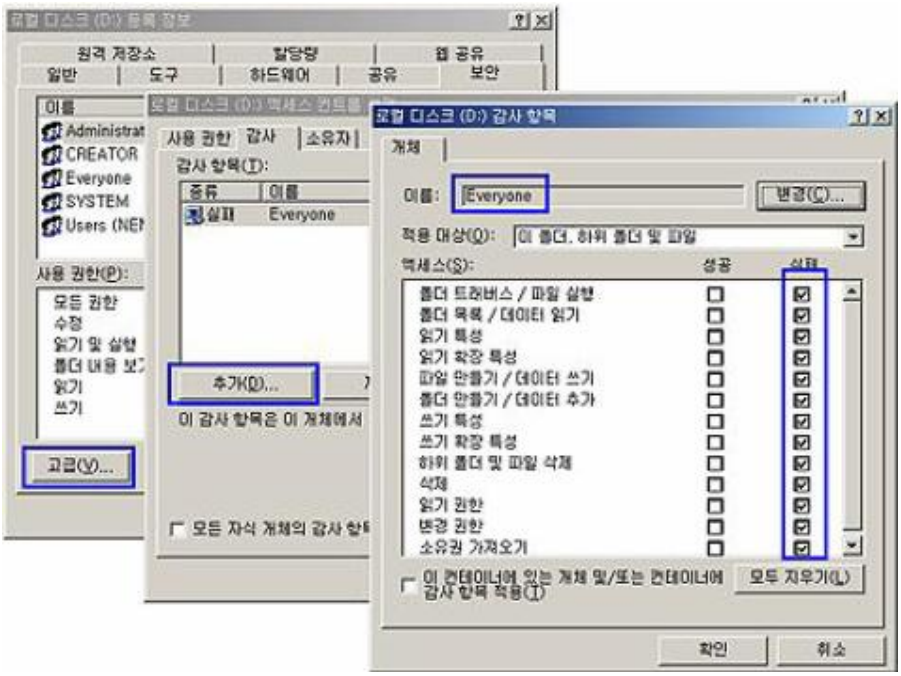
[관리도구]에서 [로컬 보안 설정] 도구를 실행하고 [로컬 정책]-[감사 정책]에서 '로그온 이벤트 감사' 항목에서 '실패' 로그를 기록하도록 설정하면 된다. 이렇게 설정하면 이후에 발생하는 로그인 실패 이벤트에 대한 내역을 [이벤트 뷰어]의 [보안 로그] 목록에서 확인할 수 있게 된다.



7.2 개체 접근 실패에 대한 로그를 기록한다.

파일이나 폴더 등의 개체에 대한 악의적인 접근 시도에 대하여 감사기록을 하는 방법을 알아보자.

먼저 7.1 에서 설명한 것과 동일한 방법으로 감사정책에서 '개체 액세스 감사'에 대하여 '실패'시 로그를 기록하도록 설정한다. 그리고 감사하려는 대상 폴더나 파일을 탐색기에서 선택하고 [등록정보]의 [보안]탭에서 [고급] 버튼을 누른다. 액세스 컨트롤 설정 창에서 [감사]탭을 선택하고 [추가] 버튼을 클릭한 뒤 'Everyone' 그룹에 대한 모든 실패 이벤트를 기록하도록 감사 항목을 설정하면 된다.



7.3 IIS 로그파일의 위치를 변경하고 NTFS 권한을 적용한다.

기본적으로 IIS 로그파일은 '%systemroot% \ system32 \ LogFiles'에 사이트별로 저장되는데 이를 다른 폴더에 저장하거나 이름을 변경함으로써 공격자가 로그 파일을 변경하거나 삭제하는 것을 어느정도 막을 수 있다. 가능하면 이 로그 파일이 저장되는 디렉토리를 웹 사이트가 위치한 디스크와 다른 볼륨을 사용하고 NTFS 권한을 Administrator(모든 권한), System(모든 권한), Backup Operators(읽기)로 지정하여 다른 계정으로 로그 파일에 접근하는 것을 막는 것이 좋다.

8. 사이트와 가상 디렉터리 관리하기

디렉터리 탐색을 통한 공격을 막기 위해 웹 사이트의 루트 디렉터리와 가상 디렉터리를 시스템이 설치된 파티션이 아닌 다른 파티션에 위치시키는 것이 좋다. 공격자들은 경로 탐색을 통해 운영체제의 프로그램이나 유틸리티를 실행시키려는 시도를 하기 때문에 웹 사이트를 시스템 파티션과 분리함으로써 이러한 위협으로부터 보호할 수 있다. 예를 들면 다음과 같은 URL 을 이용하여 시스템 자원에 접근하려는 시도를 할 수 있다.

/scripts/..%5c../winnt/system32/cmd.exe 이러한 디렉터리 탐색에 의한 공격을 막을 수 있는 방법을 알아보도록 하겠다.

8.1 웹 사이트를 시스템 파티션이 아닌 다른 파티션에 위치시킨다.

IIS 설치시에 기본적으로 설정되는 루트 디렉터리인 \ inetpub \ wwwroot 디렉터리를 사용하지 않는다.

만약 운영체제가 C: 드라이브에 설치되어 있다면 웹 사이트를 D: 드라이브와 같은 운영체제가 설치되지 않은 다른 드라이브로 옮긴다. 이로써 디렉터리 탐색 공격에 의한 위험을 줄일 수 있다.

8.2 상위 경로 사용을 제거한다.

스크립트나 어플리케이션에서 MapPath와 같은 함수의 호출시 ".."를 사용해서 상위 경로로 접근하는 것을 거부하도록 설정한다.

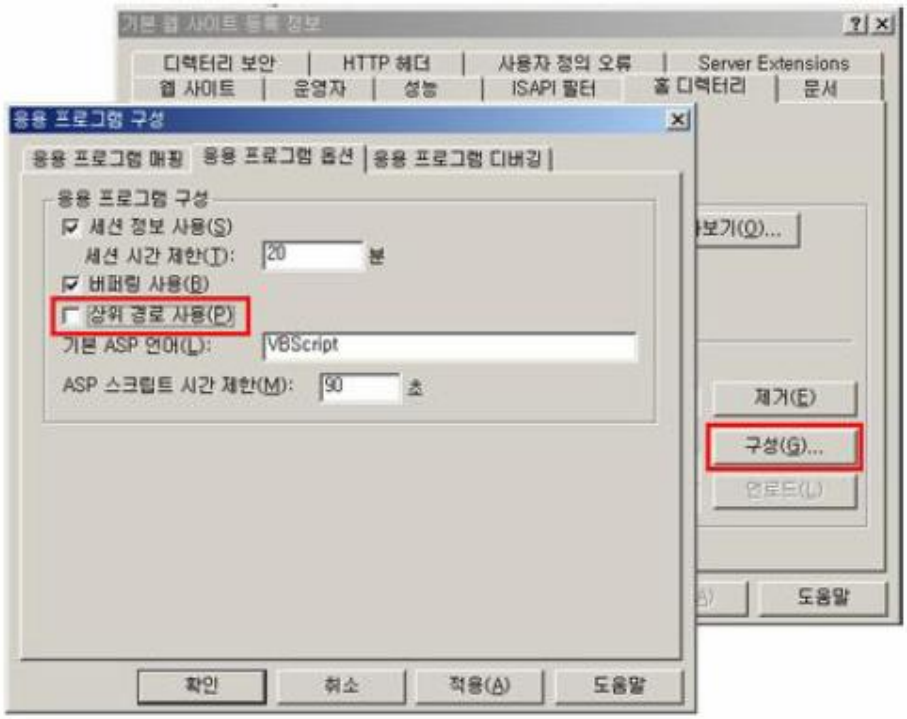
상위 경로 탐색을 거부하는 방법은 다음과 같다.

① 인터넷 정보 서비스(IIS) 관리자를 실행하고 웹 사이트의 [등록정보]를 확인한다.

② [등록정보]에서 [홈 디렉터리] 탭의 [구성] 버튼을 클릭한다.

③ [응용 프로그램 구성] 창에서 [응용 프로그램 옵션] 탭을 선택한다.

④ [상위 경로 사용]의 체크를 해제한다.



8.3 잠재적으로 위험한 가상 디렉터리를 제거한다.

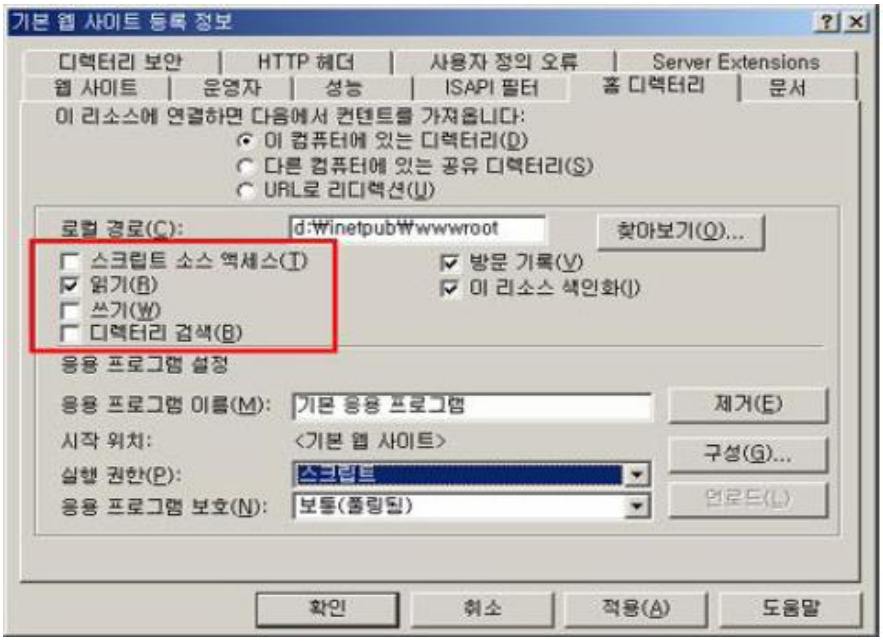
IIS 를 설치하면 기본적으로 몇 가지 샘플 어플리케이션이 가상 디렉터리로 등록되는데 공격 대상이 되기도 한다. 따라서 실제로 운영되는 웹 서버에서는 잠재적인 위험 요소인 IISSamples 나 IISAdmin, IISHelp 와 같은 샘플 어플리케이션의 가상 디렉터리를 제거하는 것이 좋다. IIS 관리자에서 해당 가상 디렉터리를 직접 제거할 수 있다.

8.4 RDS를 제거하거나 보안을 강화한다.

RDS(Remote Data Services)는 IIS를 통해 원격에서 데이터 자원에 접근이 가능하도록 기능을 제공하는 구성요소이다. RDS의 인터페이스는 Program Files \ Common Files \ System \ Msadc 디렉터리에 있는 Msadcs.dll 에 정의되어 있다.
웹 어플리케이션에서 RDS 기능을 사용하지 않는다면 이를 제거하는 것이 좋다. RDS를 제거하는 방법은 다음과 같다.
① '/MSADC' 가상 디렉터리를 IIS에서 제거한다.
② ' \ Program Files \ Common Files \ System \ Msadc' 디렉터리를 삭제한다.
③ 'HKLM \ System \ CurrentControlSet \ Services \ W3SVC \ Parameters \ ADCLaunch' 레지스트리 키를 제거한다.

웹 어플리케이션에서 RDS를 사용한다면 다음과 같은 방법으로 RDS를 안전모드로 실행함으로써 보안을 강화하는 것이 좋다.
① \ Program Files \ Common Files \ System \ Msadc 디렉터리를 삭제한다.
② 'HKLM \ System \ CurrentControlSet \ Services \ W3SVC \ Parameters \ ADCLaunch \ VbBusObj.VbBusObjCls' 레지스트리 키를 삭제한다.
③ IIS 관리자를 이용해서 MSADC 가상 디렉터리에 대한 익명 접속을 거부하도록 설정한다.
④ 'HKLM \ Software \ Microsoft \ DataFactory \ HandlerInfo' 레지스트리 키를 생성하고 DWORD 형으로 handlerRequired라는 값을 생성하고 '1'로 설정한다.

8.5 웹 권한을 설정한다.
웹 권한은 IIS 메타베이스에 의해 관리되는 것으로 NTFS 권한과는 다르므로 혼동하지 않도록 유의해야 한다. Web 권한은 다음과 같이 웹 사이트의 [등록정보] - [홈 디렉터리] 탭을 이용해서 구성할 수 있으며, '읽기'와 '쓰기', '스크립트 소스 액세스', '디렉터리 검색'의 4가지 권한이 제공된다.



9. 스크립트 매핑 설정하기

IIS 는 클라이언트가 요청한 자원의 파일 확장자에 따라서 이를 처리할 ISAPI 확장 핸들러를 지정하게 되어 있는데 이를 스크립트 매핑이라고 한다. 예를 들어 .asp, .shtm, .hdc 등의 확장자를 가진 자원을 요청하면 asp.dll이 처리하고 .aspx 에 대한 요청은 Aspnet_isapi.dll이 처리하게 되어 있다.

9.1 확장 핸들러에 대한 최신 패치를 유지한다.

특정 확장 핸들러의 취약점이 공격 대상이 될 수 있다. 특정 확장 핸들러의 취약점이 발견되고 이를 패치하지 않은 상태에서 서비스를 제공할 경우 공격자는 이를 대상으로 공격할 수 있다. 따라서 항상 최신 보안 패치를 유지해야 한다.

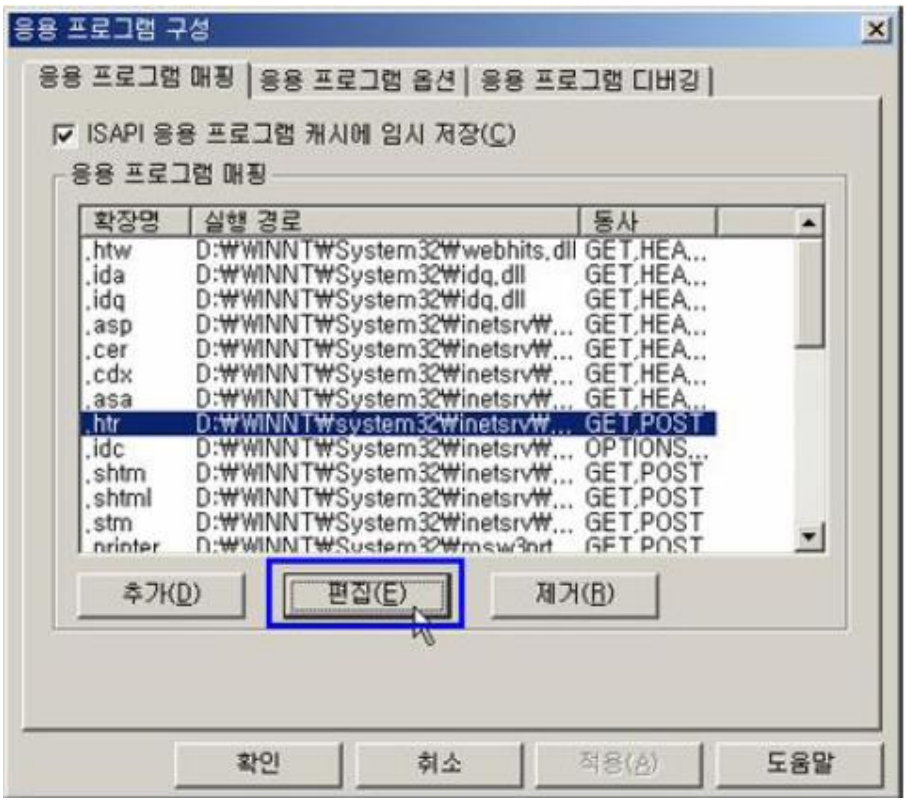
그리고 어플리케이션에서 사용하지 않는 .htr이나 .printer, .idc 와 같은 확장자에 대한 핸들러는 제거하는 것이 좋다. 실제로 이들 특정 확장자에 대한 핸들러의 취약점을 이용하여 서버 자원에 접근할 수 있는 백도어가 여러 가지 발견된 바 있다.

9.2 404.dll 매핑 사용으로 서버 자원을 보호한다.

이는 파일 확장자에 대한 매핑이 정확하게 지정되지 않은 경우 서버상의 파일이나 스크립트가 클라이언트로 다운로드 될 수 있다. 이를 막기 위해 404.dll 파일에 확장자를 매핑함으로써 서버 자원이 다운로드 되는 것을 막을 수 있다. 이 404.dll에 매핑이 되면 해당 확장자에 대한 요청에 대해서 "HTTP 404 - 파일을 찾을 수 없습니다" 오류 페이지를 응답으로 사용자에게 전송하게 된다.

IIS 관리자에서 스크립트 매핑을 설정할 웹 사이트의 [등록정보] - [홈 디렉터리] 탭에서

[구성]버튼을 클릭하면 다음과 같은 응용 프로그램 매핑 정보를 확인할 수 있다. 여기서 사용하지 않을 확장자를 선택하고 [편집]을 누른다.



여기서는 예로서 .htr 확장자에 대한 핸들러를 선택하고 편집하려 한다. .htr 확장자에 대한 처리를 404.dll 에 매핑하려면 다음과 같이 [찾아보기]를 누르고 'System 디렉터리\inetsrv'에 위치하고 있는 '404.dll'을 지정하면 된다.