제목 : 윈도우 2000 DNS 보안 방법

안녕하세요. 주원아빠입니다. 이 글은 DNS 서버를 구성할 때 주의해야 하는 보안상의 문제점을 짚어 보고 그에 따르는 해결책을 제시하고자 합니다. 이 글은 경험이 부족한 제가 여러 자료를 수집하고 분석하여 작성한 글로 오류가 있을 수도 있습니다. 오류를 발견하시거나, DNS에 대한 좋은 보안 방법을 알려주시면 감사하겠습니다.

주의 : 이 글의 논점은 Windows 2000 Server 한글판 기준으로 되어 있습니다. 간혹 영문화면이 있을 수도 있으니 유념하시기 바랍니다.

서론

현재 Windows 2000 을 사용하는 부류에는 여러가지가 있습니다. 여기에서 알려드릴 DNS 서버, 메일 서버(예:EMWAC, Exchange 서버포함), FTP 서버 등이 있으며, Windows 2000의 새로운 가장 중요한 기능인 액티브 디렉터리(이하 AD)를 이용하여 회사에서 운영하는 경우도 있을 것입니다. 여기서는 AD로 승격하지 않은 독립실행형(standardalone) 및 멤버(member) 서버에서 DNS 서버를 구성할 때, 크래커가 침입을 위한 기본적인 네트워크 구성 정보 파악, 문제점 및 해결방안 등에 대해 다룹니다.

또한, 최근의 DoS 취약점과 더불어 DNS서버의 DoS에 대해서도 많은 관심이 이루어지고 있습니다. 현재 Windows 2000에서 DNS서버의 DoS 공격에 대한 해결책은 완벽하게 제시되지 않았습니다. 다만 Verisign사가 이에 대한 해결책을 일환으로 보조 서버 서비스를 제공한다고 합니다.

이 글에서는 보안 즉 방어가 주 목적이므로 어떻게 공격하는지에 대한 글을 따로 쓰지 않습니다. 저한테 물어보셔도 소용없습니다.

1. NTFS 파티션에 Windows 2000 설치

Windows 2000을 설치하는 방법중에 FAT32(16) 또는 NTFS5에 설치하는 두가지 방법이 있습니다. 하위 운영체제와 듀얼 부팅등을 할 경우에 FAT 파일 시스템으로 설치하는 경우도 있지만, 인터넷상에 DNS서비스를 운영하기 위한 서버에는 반드시 NTFS로 설치하여야 합니

다. 참고로 파일 시스템상에서 DACL을 구현합니다. 즉, 사용자는 액세스하려는 자원에 대해 적절한 권한을 확보해야만 합니다. 크래커가 침입하더라도 적절한 권한이 없다면 별로 할일도 없을 것입니다.

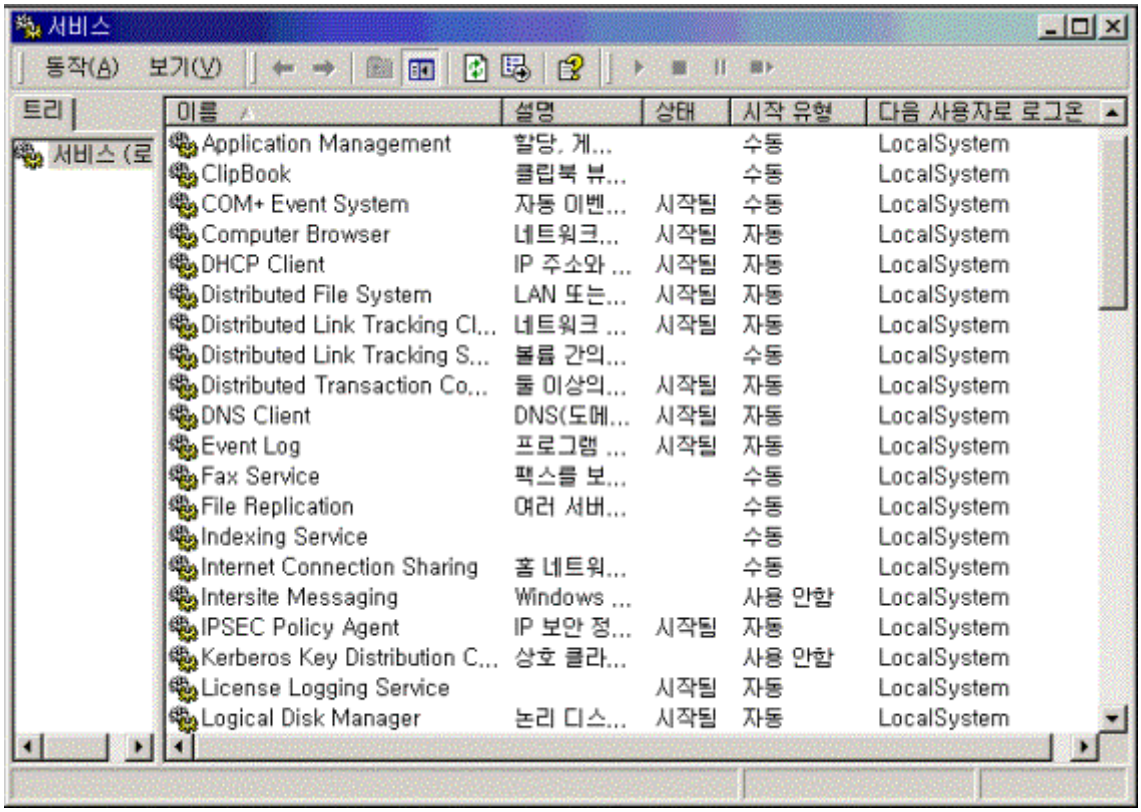
2. 최신의 서비스 팩 설치

현재 Windows 2000에서 제공되는 서비스 팩은 SP1이며 Pre-SP2라고하여 임시용 여러 개의 패치로 구성된 SP2가 제공됩니다. 그리고, SP2가 지금 베타테스팅이라고 하니 조금만 기다리시면 여러분에게 제공될 것입니다.

최신의 서비스팩을 설치함으로써 이전에 발견된 취약점 해결과 개선점을 포함하여 운영체제를 좀더 보안성 있게 해줍니다. 따라서, 모든 보안 상의 패치를 http://windowsupdate.microsoft.com/ 에서 다운로드하여 설치하는 것이 좋습니다. 그리고, www.WindowSecurity.Net에서 최신의 보안 취약점에 대해 자주 방문하여 확인하여 그에 해당하는 패치를 적용하거나 대안책을 적용해야 합니다.

3. 최소한의 서비스로 운영

Windows 2000을 설치한 상태에서 서비스(시작->관리도구->서비스)를 시작합니다. 그 안에 서비스를 보면 아마 수십가지 이상이 현재 동작되고 있을 것입니다. 서비스는 시작유형에 따라 자동/수동 실행방법이 있고, 현재 실행이 되고 있는지에 대한 상태에 대한 정보를 제공해 줍니다. 아래 그림을 보면 여러가지 서비스가 실행되고 있습니다.



제가 지금 사용하는 전용선은 ADSL입니다. 따라서 DHCP Client 서비스가 필요합니다. 하지만 고정 IP를 가지고 있는 경우(DNS서버는 당연하겠지요)에는 이러한 서비스가 필요없습니다. 또한, 오직 DNS 서버로만 운영한다면 IIS, FTP 등에 대한 서비스도 필요가 없을 것입니다.

그래서, 일단 모든 서비스의 목록을 문서로 작성하고 나서 필요없는 서비스를 하나하나 제거해 나갑니다. 일단 알기 쉬운 누가 봐도 뻔한 서비스는 일단 모두 중지를 시켜나갑니다. 한번에 여러 개씩 하는 것이 아니라 한두개씩 합니다. 그러면서 시스템이 DNS서버로 동작하는데 문제점이 발생하는 가에 대해 계속 이벤트 뷰어 등을 통해 확인합니다. 문제가 없을 때까지 최대한 많은 서비스를 중지시키는 것이 좋습니다. 특히, NetBios부분은 보안상 문제가 많은 부분으로 앞으로 많은 취약점이 나올것이라 예상됩니다. 이쪽 부분도 또한 주의해서 없애주시면 됩니다.

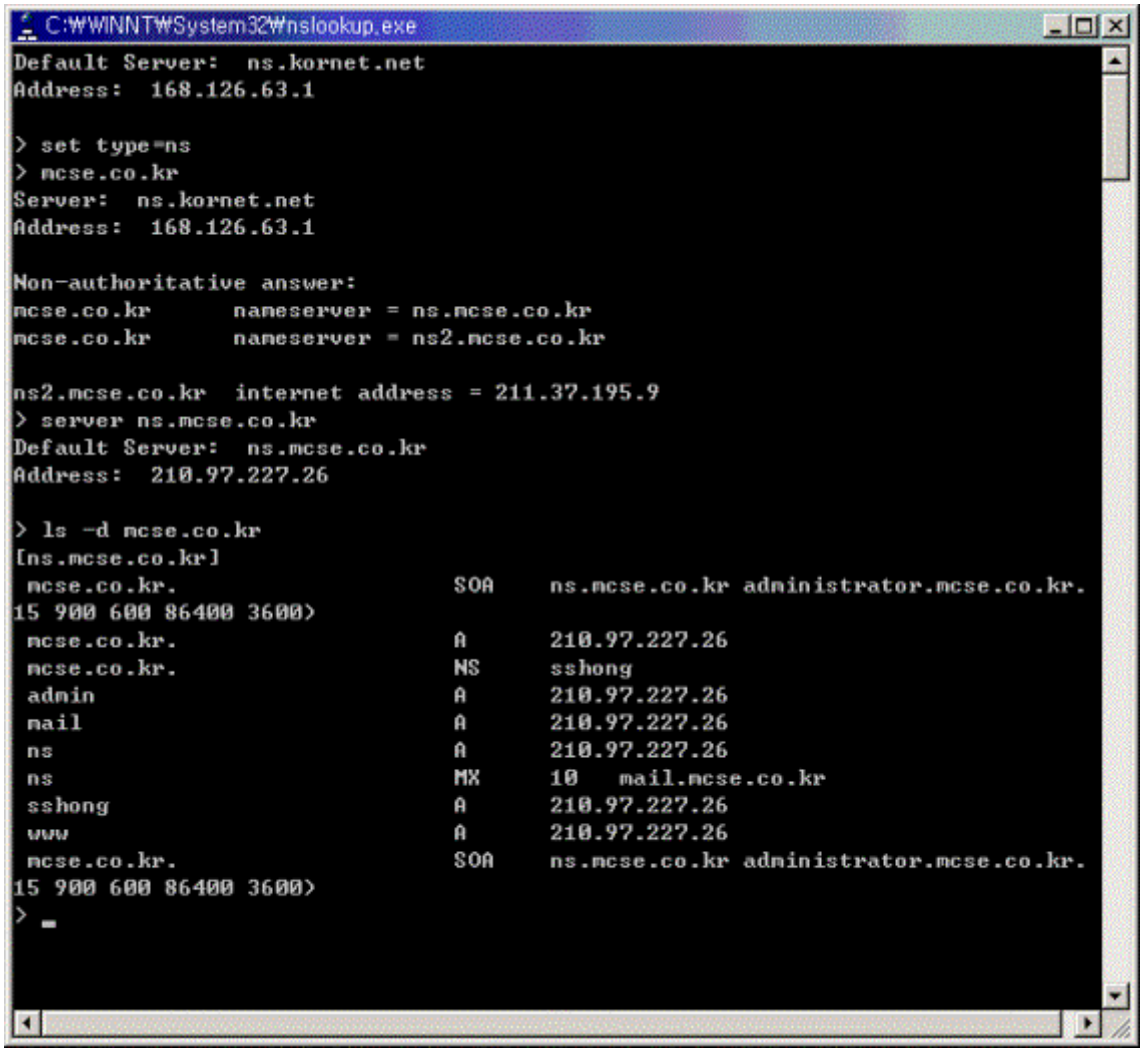
4. 최소한의 사용자 및 관리자 계정 유지 및 암호관리

이 내용은 엄격히 보면 Windows 2000 에 대한 보안 방법이지만 DNS서버를 운영하는데 있

어 필수적으로 적용됩니다. 먼저 DNS 서비스를 유지 및 관리하고자 하는 계정만을 생성하여야 합니다. 필요없는 계정은 모두 삭제 또는 사용중지(계정잠금)을 설정합니다. 관리자 계정 또는 그룹에서만 적절한 권한을 설정해 줍니다. 또한 암호를 복잡하게 입력하도록 로컬 보안 정책에서 " 암호는 복잡성을 만족해야.."를 설정하여 줍니다.

5. 원격에서 nslookup으로 DNS서버의 데이터 확인 막기

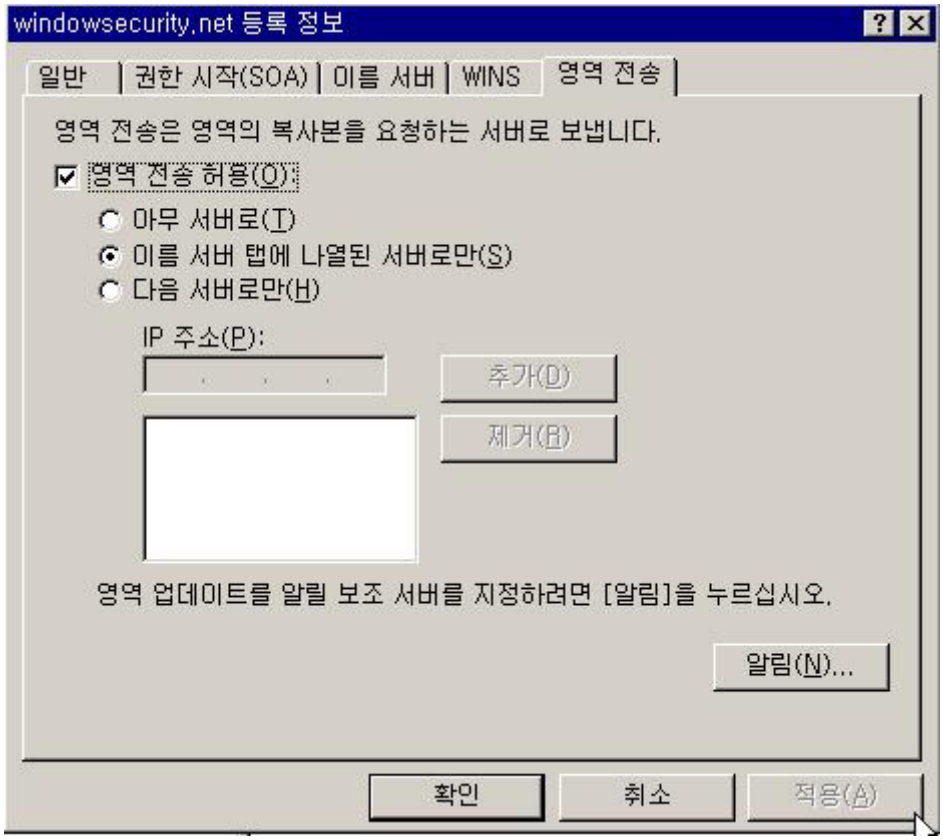
일단 DNS 서버를 구성하고 제대로 동작하는지 확인합니다. 제대로 동작한다고 그대로 놔두어서는 당연히 안됩니다. Nslookup 명령어를 통해 크래커는 DNS서버에 들어있는 모든 레코드를 알아 낼 수 있습니다. 따라서 이것부터 막아보겠습니다. 예를 들어, www.mcse.co.kr 사이트의 내부 DNS 정보를 보도록 하겠습니다. 다음 그림을 천천히 살펴보시면 알 수 있을 겁니다.



nslookup 명령어를 잘 모르시는 분을 위해 간단히 설명드리겠습니다. “set type=ns” 부분은 보고자 하는 DNS정보가 네임서버(이하 NS)라는 것을 알립니다. 즉, 그 다음줄에 “mcse.co.kr“을 입력했을 때에 mcse.co.kr의 NS 정보만을 출력합니다. 그리고 “server ns.mcse.co.kr” 을 입력하여 NS의 위치를 168.126.63.1에서 “ns.mcse.co.kr”로 변경합니다. 마지막 “ls –d mcse.co.kr”은 mcse.co.kr에 있는 모든 레코드 정보를 출력하는 것입니다. 이 정보를 이용하여 크래커는 네트워크에 IP가 어떻게 구성이 되어 있는지 그중 취약한 것이 어느것일지 추측 하는데 사용할 수 있습니다. 따라서, 이 정보를 볼 수 없도록 막을 필요가 있습니다.

막는 방법은 다음과 같습니다.

DNS서버의 웹사이트의 등록정보에 보면 “영역 전송” 탭에서 체크박스를 체크해주고 아래에 영역을 전송할 서버를 입력하여 주면 됩니다.



6. 역방향 조회 영역

역방향 조회 영역은 정방향 조회 영역의 반대 개념으로 IP 주소를 도메인 이름으로 해석하여 줍니다. 일반적인 DNS 서비스나 웹 서비스 등에서는 역방향 조회 영역이 필요하지 않습니다. 따라서, 여기서 말씀드리는 것은 최소한의 역방향 조회 레코드인 PTR을 남겨두고 모두 삭제하는 것입니다. 삭제하지 말하야 할것에는 반드시 NS의 레코드는 남아 있어야 합니다. 없어도 상관은 없지만 매번 관리자가 nslookup을 통해 NS 설정을 체크할 때 불편함이 따릅니다. NS의 레코드가 없는 경우에는 nslookup을 실행했을 때 다음과 같은 에러메시지가 나타납니다.

*** can’t find server name for address xxx.xxx.xxx.xxx : Non-existent /domain

그리고, PTR 레코드는 스팸 메일등의 릴레이를 점검하는데 사용할 수 있습니다. 즉, 메일이 전송되었을 때 서버에서 온건지 아니면 다른 서버를 경유하여 온건지 확인하기 위해 PTR 레코드를 쿼리하게 됩니다. 그러므로, 메일 서버를 운영하는 경우에는 반드시 스팸 방지 유틸을 사용하고, 메일 교환기(MX) 레코드가 연결된 A 레코드를 삭제하지 않고 남겨두어야 합니다.