작성자 : 기술지원부 홍 종 우 shairin@nextline.net

윈도우 서버에서 서비스 거부 공격에 대비한 TCP/IP 스택 강화

(1) 서비스 거부 공격이란

정보 시스템의 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 행위로 주로 시스템의 cpu나 메모리, 통신대역폭과 같은 자원을 고갈시켜 정보 시스템의 사용을 방해하는 공격 방식 입니다.

(2) Microsoft 홈페이지 참고 주소

Microsoft에서 서비스 거부공격에 대비한 TCP/IP 스택 강화에 관련한 메뉴얼을 제공하고 있습니다.

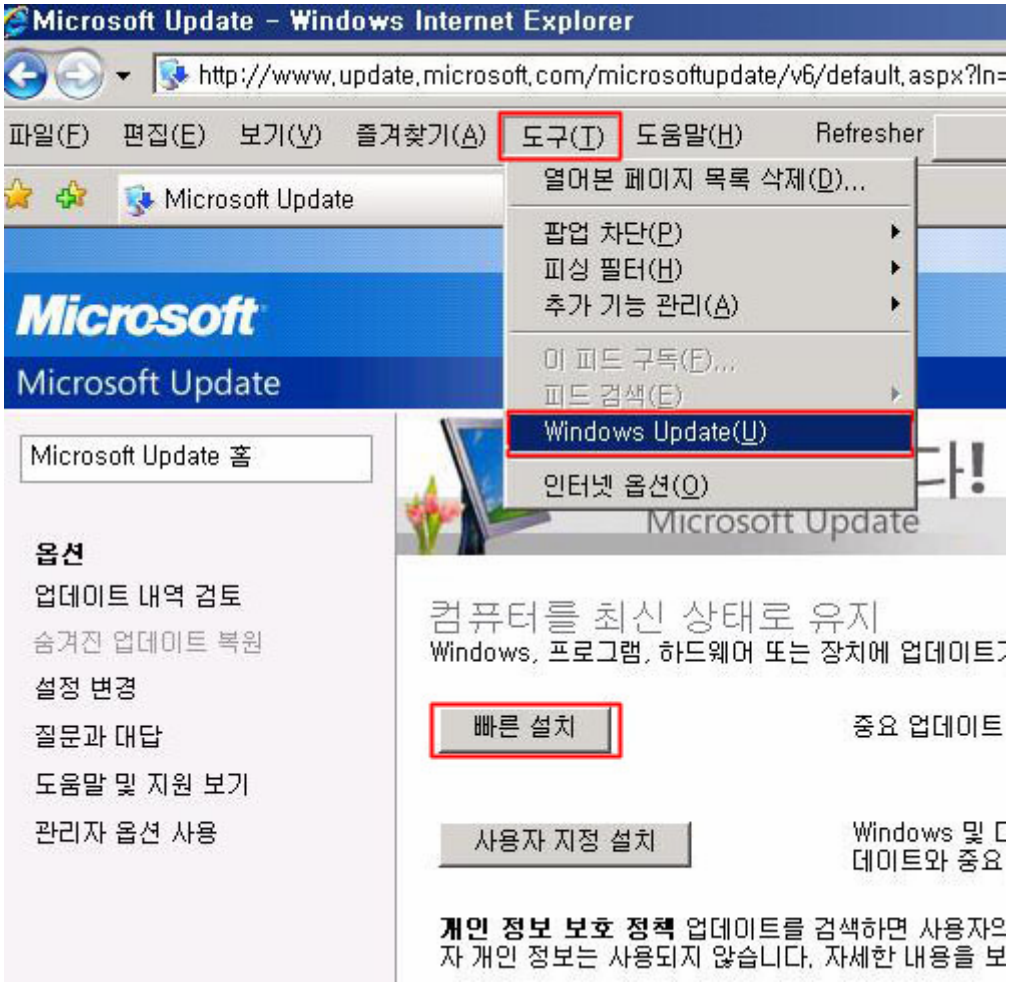
Windows 2000
http://support.microsoft.com/kb/315669/ko

Windows 2003
http://support.microsoft.com/kb/324270/ko

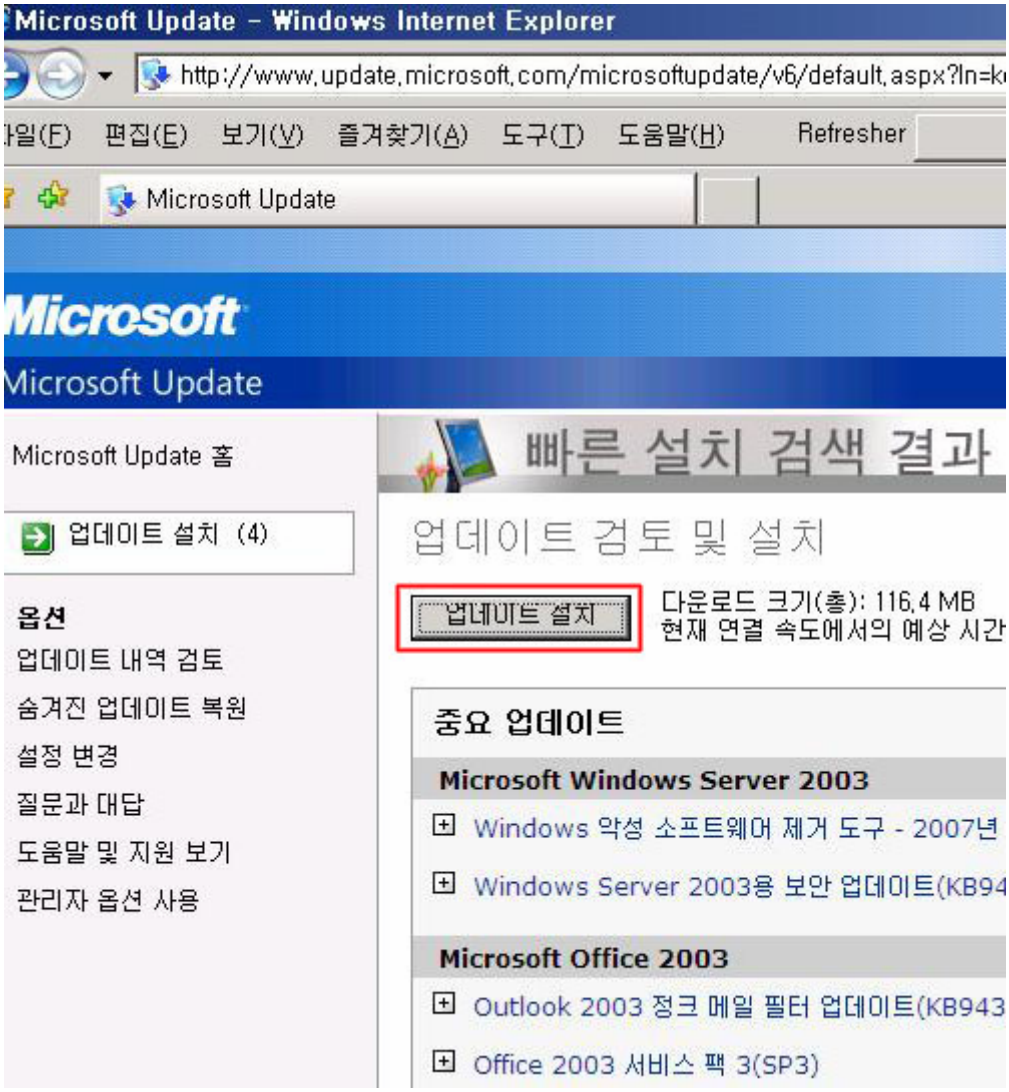
(3) 최신 보안 수정프로그램으로 사용 중인 컴퓨터를 업데이트 (2000/2003 공통)

마이크로 소프트에서는 알려진 Windows의 보안상 취약점이나 버그에 관한 패치를 제공하고 있으며 서비스 거부 공격 외에도 여러 가지 해킹의 위험성을 줄여주기 때문에 주기적으로 업데이트를 실시하는 것이 좋습니다.

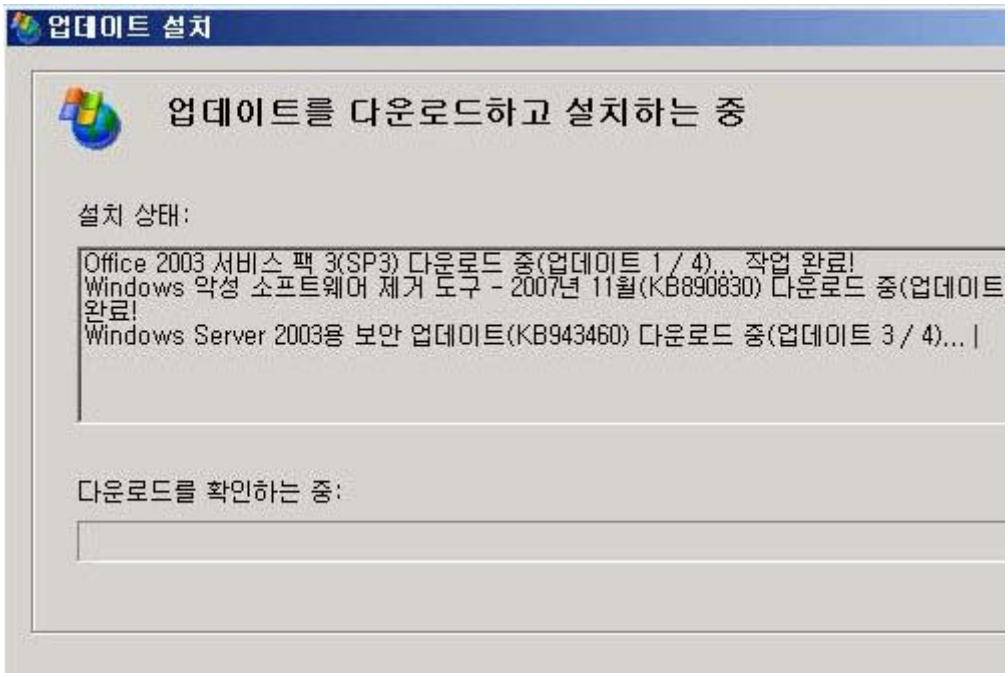
① 윈도우 익스플로러를 실행하여 상단의 도구-Windows Update를 클릭하여 Microsoft Windows Update 페이지에 접속한 후 빠른 설치를 선택



② 자동으로 업데이트할 소프트웨어를 검색한 후 목록이 표시되면 업데이트 설치 선택



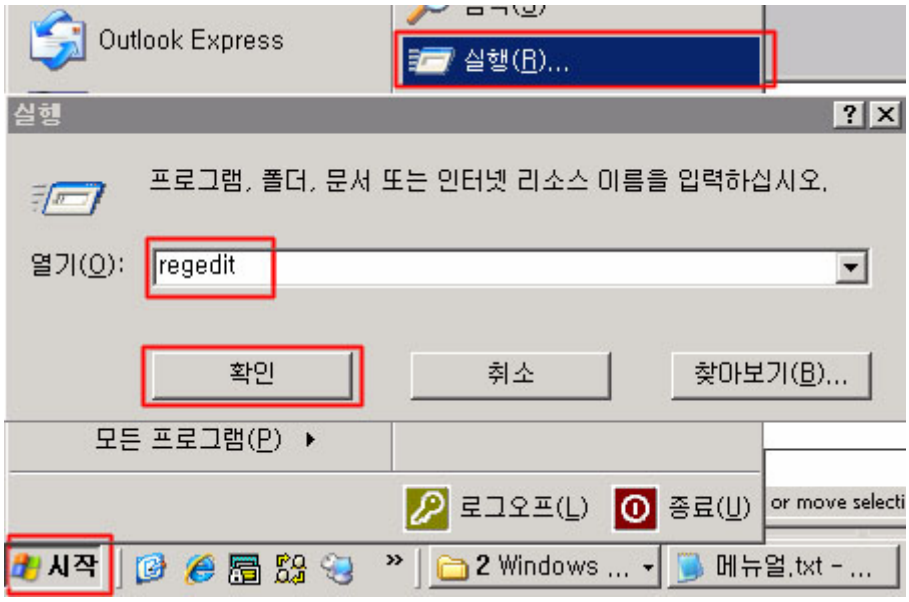
③ 자동으로 업데이트를 다운로드 하고 설치



④ 재부팅 후 목록이 나오지 않을 때 까지 ① 번부터 반복

(4) TCP/IP 스택을 강화하는 TCP/IP 레지스트리 값을 변경
윈도우 서버상의 레지스트리를 수정하여 TCP/IP 프로토콜 스택을 강화합니다.
기본 TCP/IP 스택 구성은 표준 인트라넷 트래픽을 처리하도록 조정되어 있습니다. 컴퓨터를 인터넷에 직접 연결한 경우 서비스 거부 공격에 대비하여 TCP/IP 스택을 강화하는 것이 좋습니다.

① 윈도우 좌측 하단의 시작-실행을 선택하여 regedit를 입력

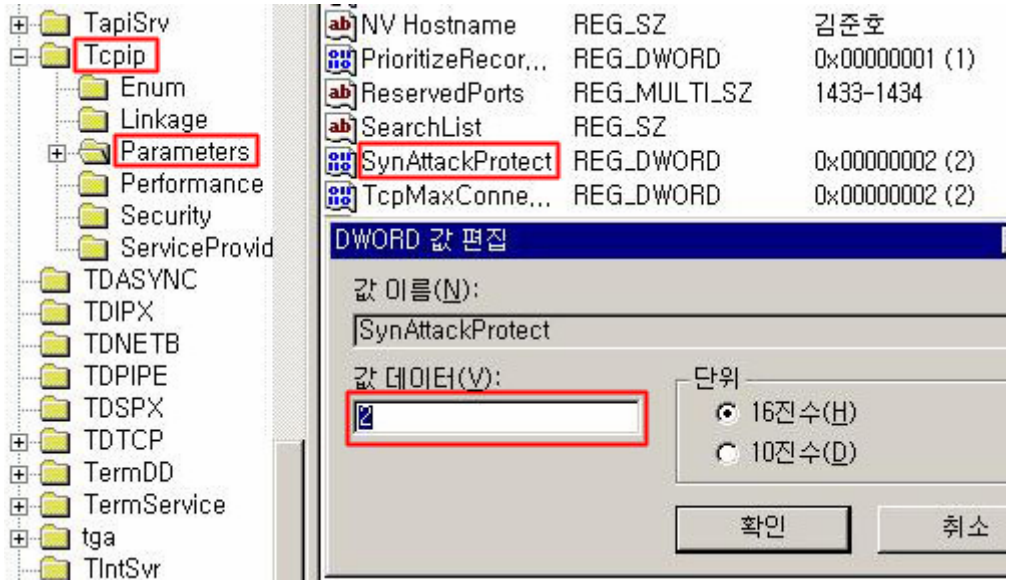


② 좌측에 표시되는 경로에서 다음의 경로를 선택합니다.

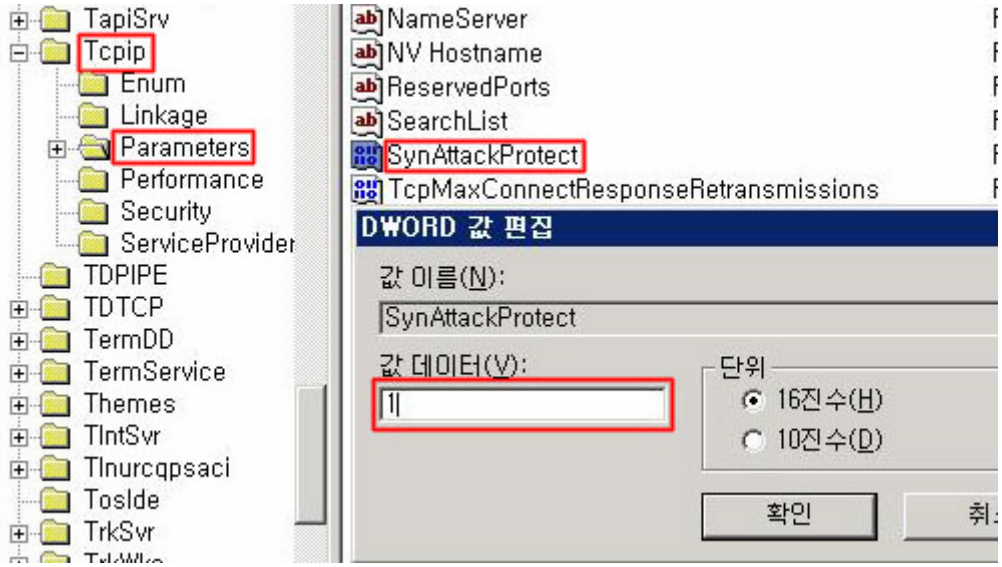
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

우측의 목록에서 SynAttackProtect 를 선택하여 Windows 2000에서는 2를 선택하며 Windows 2003에서는 1을 선택합니다.

Windows 2000



Windows 2003



값 이름: SynAttackProtect

키: TcpipWParameters

값 종류: REG_DWORD

유효 범위: 0,1,(2 : Windows 2000 에서 적용)

기본값: 0

이 레지스트리 값은 TCP(Transmission Control Protocol)가 SYN-ACKS의 재전송을 조정하도록 합니다. 이 값을 구성하면 SYN 공격(서비스 거부 공격의 한 종류) 동안 연결 응답이 더 빨리 시간 초과됩니다.

• 0(기본값): SYN 공격에 대한 일반적인 보호를 하려면 SynAttackProtect를 0으로 설정합니다.

• 1: SYN 공격에 대하여 보다 높은 수준의 보호를 하려면 SynAttackProtect를 1로 설정합니다. 이 매개 변수는 TCP가 SYN-ACKS의 재전송을 조정하도록 합니다. SynAttackProtect를 1로 설정하면 SYN 공격이 이루어지고 있는 경우 연결 응답이 더 빨리 시간 초과됩니다. Windows는 공격이 진행 중인지 확인하기 위하여 다음 값을 사용합니다.• TcpMaxPortsExhausted

• TCPMaxHalfOpen

• TCPMaxHalfOpenRetried

• 2(Windows 2000): SYN 공격에 대하여 최고 수준의 보호를 하려면 SynAttackProtect를 2로 설정합니다. 이 값은 연결 표시가 더 지연되도록 하며, SYN 공격이 진행 중일 때는 TCP 연결 요청이 더 빨리 시간 초과됩니다. 이 값은 권장 설정입니다.

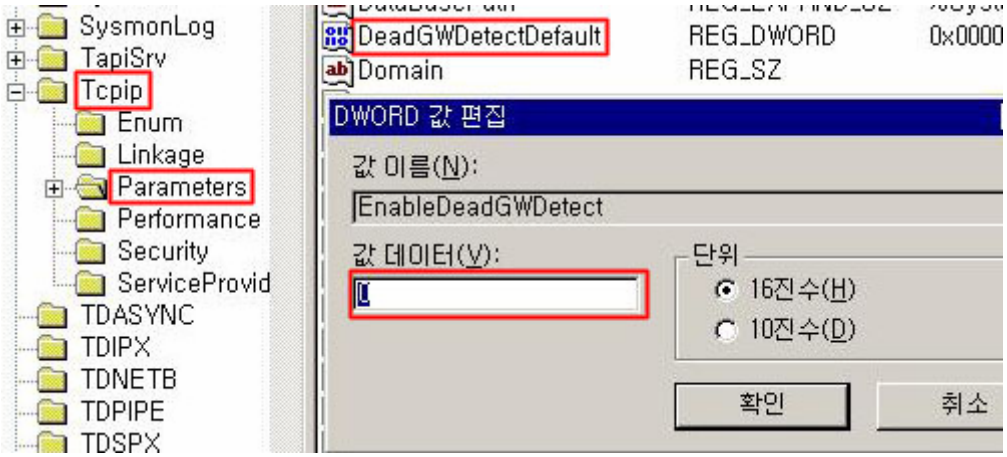
참고: 다음 소켓 옵션은 SynAttackProtect 값을 2로 설정하면 더 이상 작동하지 않습니다.

- 확장 가능한 창
- 각 어댑터에 구성된 TCP 매개 변수(초기 RTT 및 창 크기 포함)

③ 좌측에 표시되는 경로에서 다음의 경로를 선택합니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

우측에 표시되는 목록에서 EnableDeadGWDetect를 선택하여 0 으로 설정합니다.



값 이름: EnableDeadGWDetect

키: TcpipWParameters

값 종류: REG_DWORD

유효 범위: 0, 1(False, True)

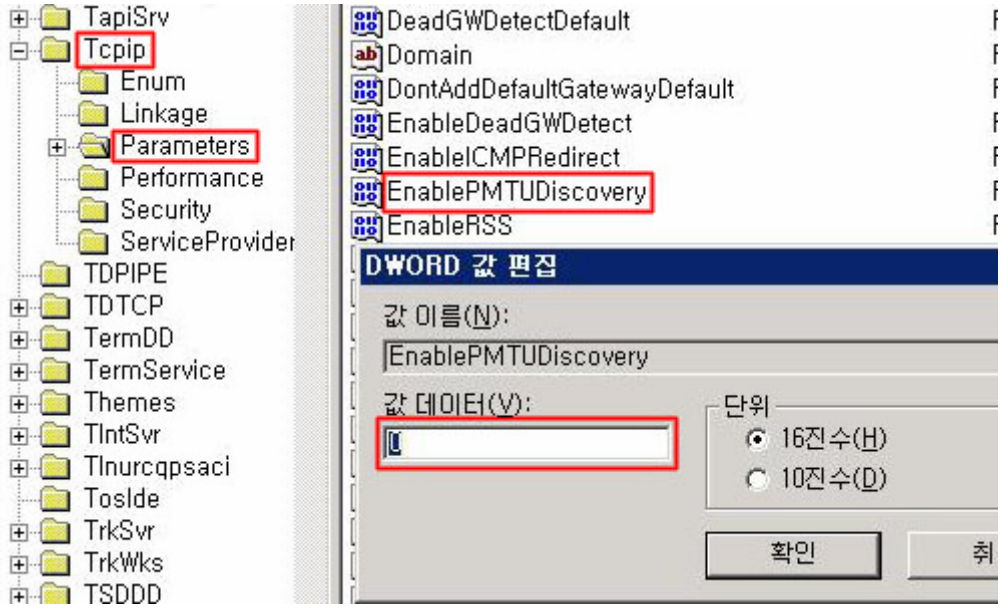
기본값: 1(True)

- 1 : EnableDeadGWDetect를 1로 설정하면 TCP는 더 이상 작동하지 않는 게이트웨이를 검색할 수 있습니다. 더 이상 작동하지 않는 게이트웨이 감지가 사용되면 TCP는 여러 연결에 문제가 발생하는 경우 인터넷 프로토콜(IP)에 백업 게이트웨이를 변경하도록 요청할 수 있습니다. 백업 게이트웨이는 제어판의 네트워크 도구에 있는 TCP/IP 구성 대화 상자의 고급 섹션에서 정의됩니다.
- 0: EnableDeadGWDetect 값은 0으로 설정하는 것이 좋습니다. 0으로 설정하지 않으면 공격으로 인하여 서버가 강제로 원하지 않는 게이트웨이로 전환될 수 있습니다.

④ 좌측에 표시되는 경로에서 다음의 경로를 선택합니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

우측에 표시되는 목록에서 EnablePMTUDiscovery를 선택하여 0으로 설정합니다.



값 이름: EnablePMTUDiscovery

키: TcpipWParameters

값 종류: REG_DWORD

유효 범위: 0, 1(False, True)

기본값: 1(True)

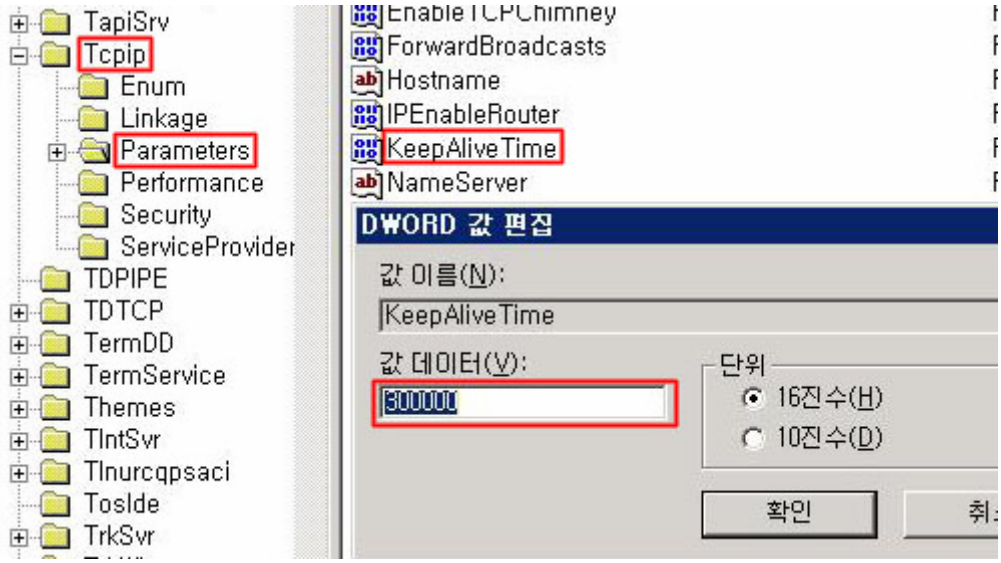
• 1 : EnablePMTUDiscovery를 1로 설정하면 TCP는 최대 전송 단위(MTU)나 원격 호스트 경로에 대한 최대 패킷 크기를 검색하려 합니다. TCP는 경로의 MTU를 검색하고 TCP 세그먼트를 이 크기로 제한하여 경로에 있는 각자 다른 MTU로 네트워크에 연결하는 라우터에서 조각을 제거할 수 있습니다. 조각이 있으면 TCP 처리량에 좋지 않은 영향을 줍니다.

• 0 : EnablePMTUDiscovery는 0으로 설정하는 것이 좋습니다. 이렇게 하면 로컬 서브넷에서 호스트하지 않는 모든 연결에 576바이트의 MTU가 사용됩니다. 이 값을 0으로 설정하지 않으면 공격자가 강제로 MTU를 아주 작은 값으로 설정하여 스택의 부하가 커집니다.

⑤ 좌측에 표시되는 경로에서 다음의 경로를 선택합니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

우측에 표시되는 목록에서 KeepAliveTime을 선택하여 300,000으로 설정합니다.



값 이름: KeepAliveTime

키: TcpipWParameters

값 종류: REG_DWORD - 시간(밀리초)

유효 범위: 1 - 0xFFFFFFFF

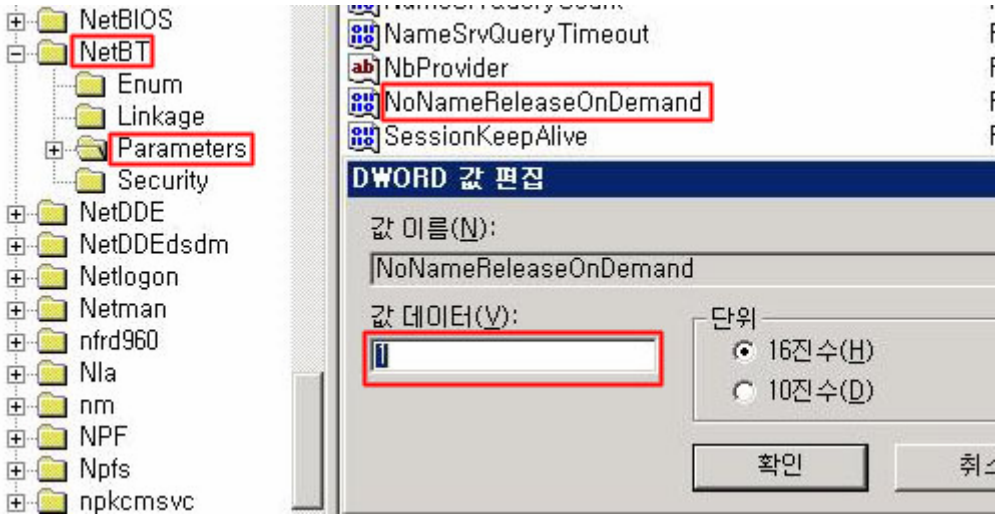
기본값: 7,200,000(2시간)

이 값은 TCP가 Keep Alive 패킷을 보내어 유휴 연결이 열려 있는지 확인하는 빈도를 결정합니다. 연결이 유지되어 있다면 원격 컴퓨터가 Keep-Alive 패킷을 인식합니다. Keep-Alive 패킷은 기본적으로 보내지지 않습니다. 연결에서 이 값을 구성하기 위한 프로그램을 사용할 수 있습니다. 권장값은 300,000(5분)입니다.

⑥ 좌측에 표시되는 경로에서 다음의 경로를 선택합니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Netbt\Parameters

우측에 표시되는 목록에서 NoNameReleaseOnDemand를 선택하여 1로 설정합니다.



값 이름: NoNameReleaseOnDemand

키: NetbtWParameters

값 종류: REG_DWORD

유효 범위: 0, 1(False, True)

기본값: 0(False)

이 값은 컴퓨터가 이름 해제 요청을 받을 때 NetBIOS 이름을 해제할지 여부를 결정합니다. 이 값은 관리자가 악의적인 이름 해제 공격으로부터 컴퓨터를 보호할 수 있도록 추가되었습니다. NoNameReleaseOnDemand 값은 1로 설정하는 것이 좋습니다.

⑦ 레지스트리를 수정을 완료한 이후에 적용을 위해서 재부팅을 실시합니다.