QnA형식으로 알아보는 WannaCry 랜섬웨어 대응 가이드

2017. 05

미래창조과학부
Ministry of Science, ICT and Future Planning

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

- 목 차 -

Microsoft SMB 취약점을 이용한 랜섬웨어 관련 FAQ

Q1. 어떤 Windows 운영체제가 취약점에 영향을 받나요?

○ 공개 된 공격 도구 별 영향 받는 소프트웨어는 아래와 같습니다.

- 대부분의 Windows 운영체제

  * 최신 보안패치를 적용하여 사용하고 있으시다면 해당 취약점의 영향을 받지 않습니다.

  **** WannaCry 변종이 존재할 가능성이 있어 지속적인 주의 필요**

Q2. 해당 랜섬웨어를 예방하기 위해서는 어떻게 해야 하나요?

○ WannaCry 랜섬웨어는 패치가 되지 않은 파일공유기능(SMB가 사용하는 TCP 445포트)을 이용하여 감염되므로 해당 서비스를 차단해야합니다.

① 이용자PC가 감염될 우려가 있으니, 컴퓨터 부팅전 인터넷 차단(랜선 연결 제거)

② SMB 포트를 차단(프로토콜 비활성화)

③ 이후, 인터넷에 연결하여 윈도우 보안패치 및 백신 업데이트 등의 순서로 진행

* SMB 포트를 차단할 경우 파일 공유 기능을 사용할 수 없으므로 패치가 완료되면, SMB 서비스 필요 시 ② 차단 내용 해제

Q3. SMB 포트는 어떻게 차단하나요?(운영체제 버전별 상세 설명은 붙임 참고)

☐ **SMB 관련 취약점 조치 방안**

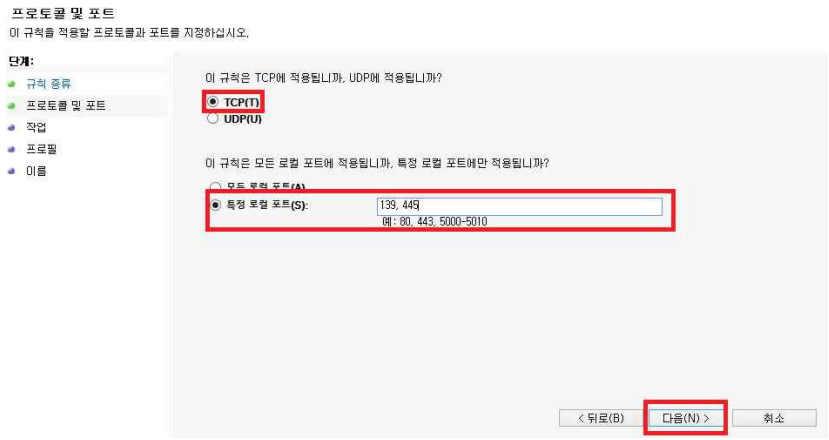
*** 해당 취약점을 해결하기 위해서 아래 3가지 방법 중 한 가지만 수행하면 됩니다.**

① 네트워크 방화벽 또는 운영체제 방화벽으로 SMB에 사용되는 포트 차단

o [제어판] -> [시스템 및 보안] -> [Windows 방화벽] -> [고급 설정] -> [인바운드 규칙] -> [새규칙] -> 포트 -> "TCP", "특정 원격 포트" 선택 -> "139, 445" 입력("UDP"/"137, 138" 입력) -> "연결 차단" 선택 -> "도메인, 개인, 공용" 선택 -> 이름 입력

*** WannaCry 랜섬웨어의 경우 TCP 445번 포트만 해당되나, WannaCry 변종이 존재할 가능성이 있어 SMB 프로토콜 관련 포트인 UDP 137, 138, TCP 139까지 전부 적용하는 것을 권고(상세 내용은 붙임 참고)**

** 해당 서비스를 다시 사용해야 하는 경우 등록된 규칙 삭제



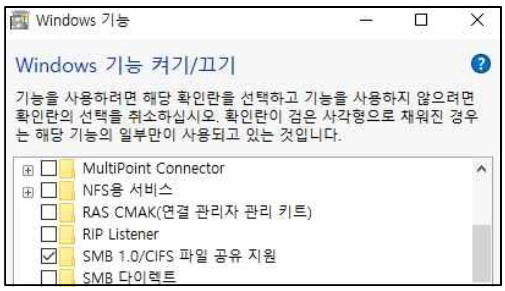
[Windows 방화벽에 포트 차단 적용 화면]

② SMB 기능 해제(Windows 8.1 또는 Windows Server 2012 R2 이상인 경우에만 해당)

[클라이언트 운영 체제의 경우]

o [제어판] -> [프로그램] -> [Windows 기능 설정 또는 해제] -> "SMB1.0/CIFS 파일 공유 지원" 체크해제 -> "시스템 재시작"

* 해당 서비스를 다시 사용해야 하는 경우 [제어판] -> [프로그램] -> [Windows 기능 설정 또는 해제] -> "SMB1.0/CIFS 파일 공유 지원" 체크 -> "시스템 재시작"



[Windows 10 기능 켜기/끄기 화면]

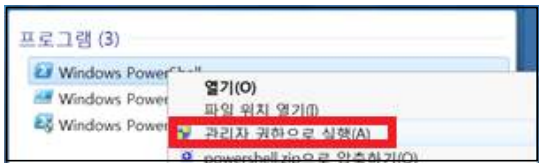
[서버 운영 체제의 경우]

o [서버 관리자] -> [관리] -> [역할 및 기능] -> "SMB1.0/CIFS 파일 공유 지원" 체크 해제 -> "시스템 재시작"

* 해당 서비스를 다시 사용해야 하는 경우 [서버 관리자] -> [관리] -> [역할 및 기능] -> "SMB1.0/CIFS 파일 공유 지원" 체크 -> "시스템 재시작"

③ 레지스트리 등록 방법

o [시작] -> "powershell" 입력 -> 마우스 "우클릭" -> 관리자 권한으로 실행



[Windows 7]

o set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

o set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> _
```

[레지스트리 등록]

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

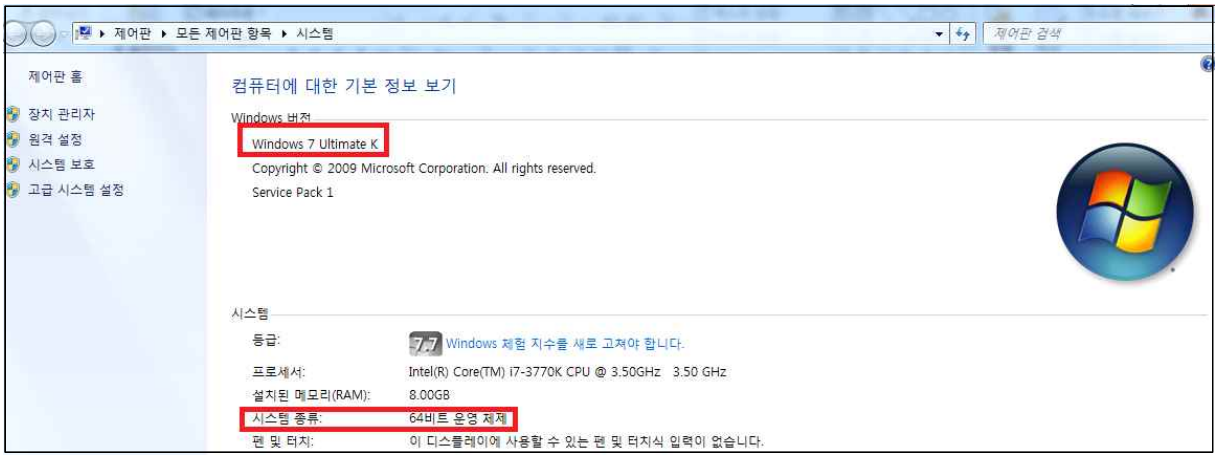
② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키

Q4. 운영체제의 버전확인은 어떻게 확인하나요?

☐ **아래 2가지 방법 중 한 가지를 수행하여 버전 확인을 하면 됩니다.**

① [윈도우 키(⊞) + Pause Break 키(Pause)] 입력

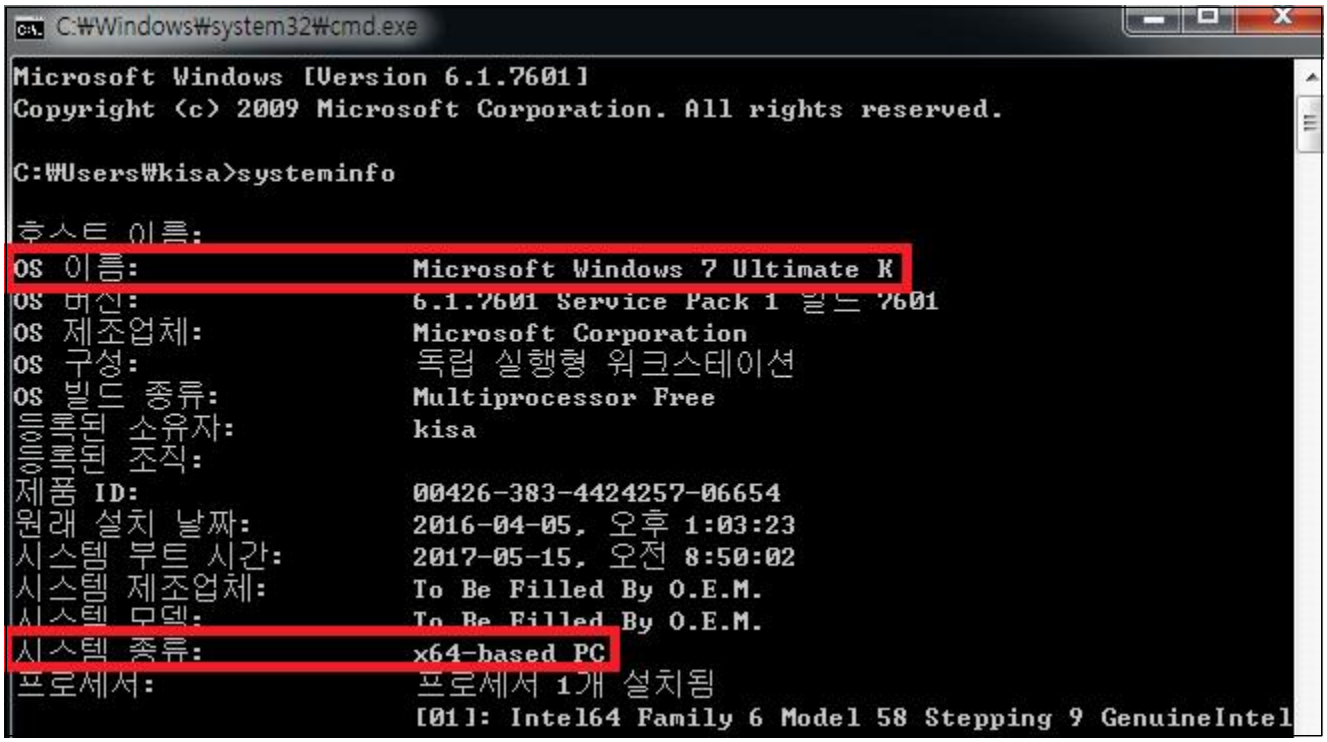
o 시스템 정보화면에서 Windows 버전과 시스템 종류 확인



[Windows 방화벽에 포트 차단 적용 화면]

② CMD 창에서 "systeminfo" 입력 후 엔터

o 입력 결과 중, OS 이름과 시스템 종류 확인



Q5. 보안 패치는 어떻게 하나요?

□ 이번 취약점에 대해서는 Microsoft에서 지원하지 않는 운영체제에서도 긴급 보안 업데이트를 배포하였으며, 아래와 같이 업데이트 권고 드립니다.

o 자동 업데이트가 해제되어 있거나, XP 등 서비스 지원이 종료된 운영체제의 경우 아래 표에서 해당 버전에 맞는 파일 다운로드하여 수동 설치

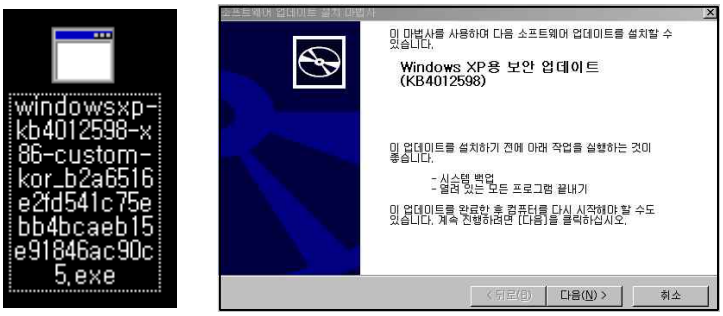
- 버전별 보안패치 파일 다운로드 링크

운영체제	보안 업데이트 파일 링크
Windows XP SP2(64비트 시스템용)	http://www.microsoft.com/downloads/details.aspx?FamilyId=5fbaa61b-15ce-49c7-9361-cb5494f9d6aa
Windows XP SP3 (32비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55245
Windows XP Embedded SP3(32비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55247
Windows 8(32비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55246
Windows 8(64비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55249
Windows 8.1(32비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213
Windows 8.1(64비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213
WindowsVista서비스팩2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598
WindowsVista(64비트 시스템용) 서비스팩2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598
Windows 7(32비트 시스템용) 서비스 팩 1	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012212
Windows 7(64비트 시스템용) 서비스 팩 1	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012212
Windows 10(32비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012606
Windows 10(64비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012606
Windows 10 버전 1511(32비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013198
Windows 10 버전 1511(64비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013198
Windows 10 버전 1607(32비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013429
Windows 10 버전 1607(64비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013429
Windows Server 2003 SP2(32비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55248
Windows Server 2003 SP2(64비트 시스템용)	https://www.microsoft.com/ko-KR/download/details.aspx?id=55244
Windows Server 2008 R2(64비트 시스템용) 서비스 팩 1	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012212
Windows Server 2008 R2(Itanium 기반 시스템용) 서비스 팩 1	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012212
Windows Server 2008(32비트 시스템용) 서비스 팩 2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598
Windows Server 2008(64비트 시스템용) 서비스 팩 2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598
Windows Server 2008(Itanium 기반 시스템용) 서비스 팩 2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598
Windows Server 2012	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012214
Windows Server 2012 R2	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213
Windows Server 2016(64비트 시스템용)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013429

- **보안 업데이트 – 수동 설치**

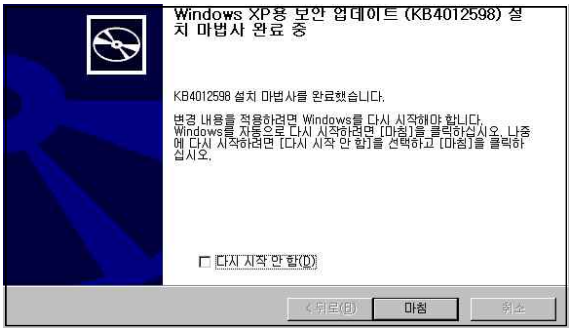
  o Microsoft 보안 업데이트 홈페이지에서 운영체제에 맞는 보안 업데이트 파일 다운로드

  ① 설치 파일 다운로드 및 실행



[다운로드 및 실행 – Windows XP]

  ② 설치 완료 후 재부팅

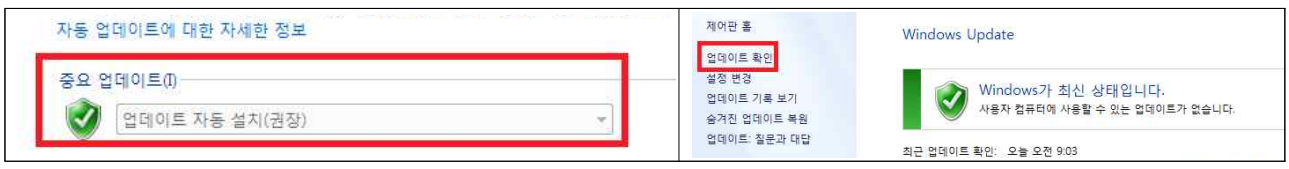


[업데이트 설치 완료]

- **보안 업데이트 – 자동 설치 설정 (설정 이후 자동으로 업데이트 됨)**

  ① [제어판] -> [Windows Update] -> [설정 변경] -> "중요 업데이트에서 업데이트 자동 설치(권장)" 선택 -> [업데이트 확인] -> 자동 업데이트 수행

[제어판 Windows Update]



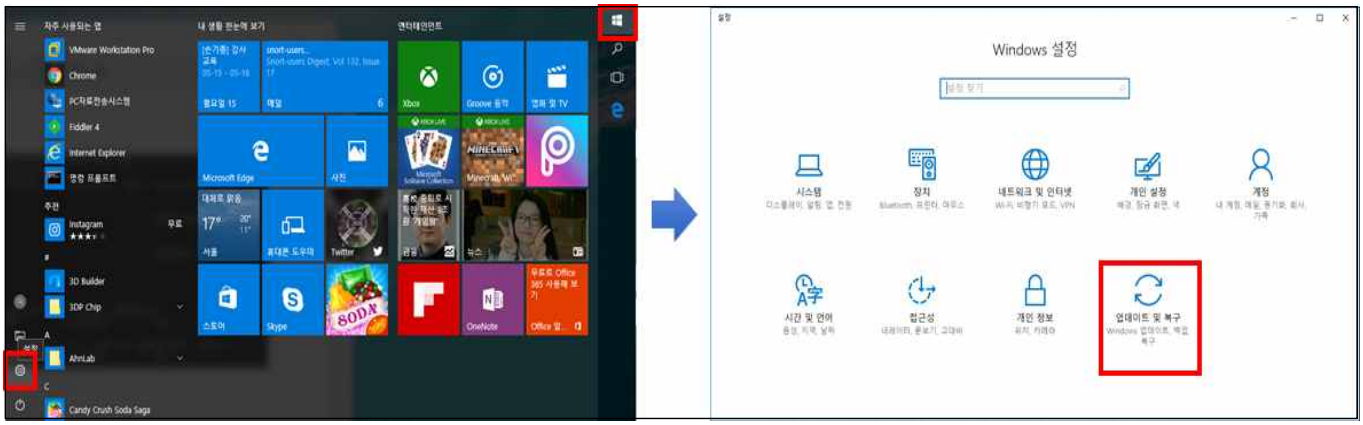
[자동 업데이트 확인 및 설치]

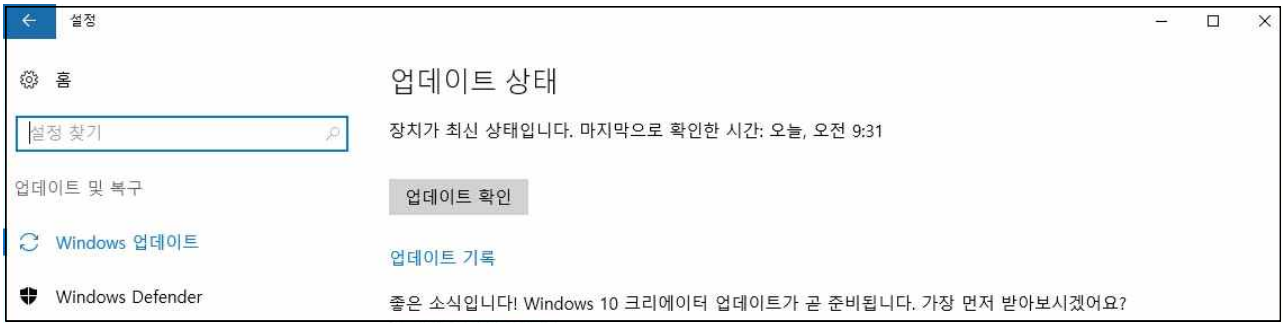
Q6. 보안 패치가 됐는지 어떻게 확인 하나요?

□ Windows 10 사용자

o 최신 버전 사용 유무 확인 방법

- [Windows 설정] -> [업데이트 및 복구] -> [Windows 업데이트] -> 업데이트 확인





o SMB 취약점 패치 여부 확인 방법

- [Windows 설정] -> [업데이트 및 복구] -> [업데이트 기록] -> 설치된 업데이트 목록에서 "KB4012606", "KB4013429", "KB4013198" 중에 하나라도 있으면 패치 적용 상태

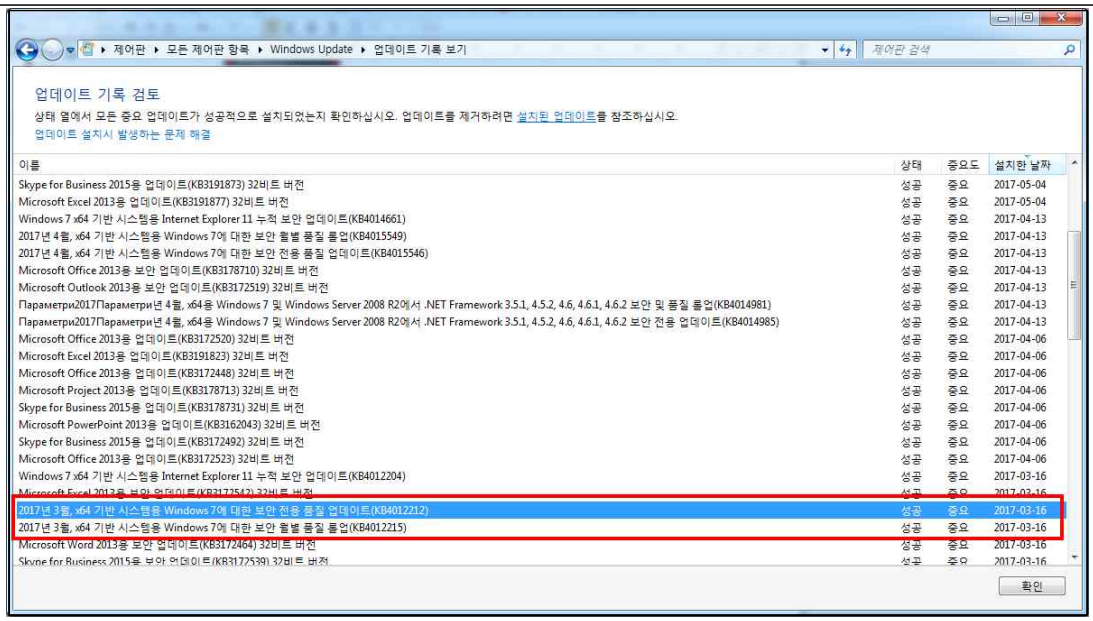
□ Windows 7 사용자

o 최신 버전 사용 유무 확인 방법

- [시작] - [제어판] -> [Windows Update] (안 보이는 경우, 보기 기준을 작은 아이콘으로 변경) -> 업데이트 상태 확인

o SMB 취약점 패치 여부 확인 방법

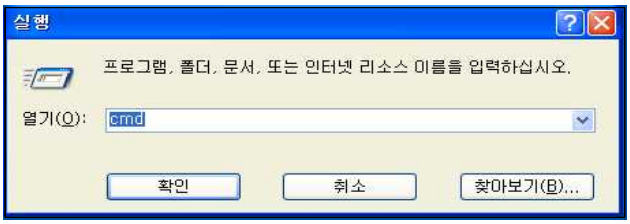
- [시작] - [제어판] -> [Windows Update] (안 보이는 경우, 보기 기준을 작은 아이콘으로 변경) -> [업데이트 기록 보기] -> "KB4012212" 또는 "KB4012215"가 존재하는지 확인



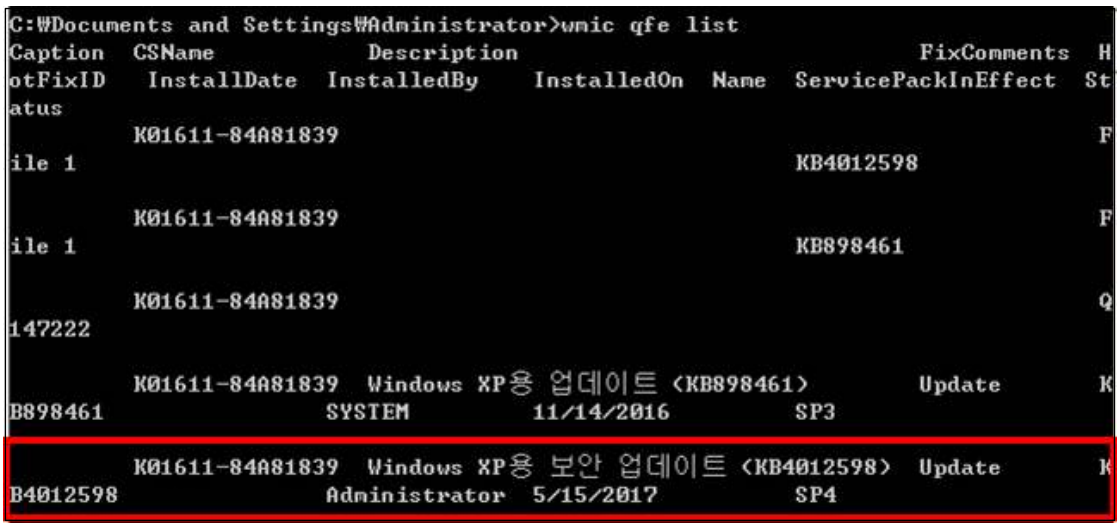
□ Windows XP 사용자

o SMB 취약점 패치 여부 확인 방법

- [Windows 키 + r] 후, "cmd" 입력



- cmd 창에서 "wmic qfe list" 입력 후 엔터



- "KB4012598" 존재 여부 확인

Q7. 스마트폰도 랜섬웨어 감염 위험이 있나요?

○ WannaCry 랜섬웨어의 경우 윈도우 운영체제의 취약점을 악용한 공격이기 때문에 안드로이드, 아이폰, 윈도우 폰과 같은 스마트폰 기종은 공격 대상에서 제외됩니다.
* 단, 변종 출현이 가능

Q8. 무선 인터넷을 이용 중인데 와이파이 연결을 하면 안 되나요?

○ 네트워크 연결의 경우, 랜섬웨어에 감염됐을 때의 가능성을 대비하여 피해 확산을 방지하기 위해 네트워크를 차단하라고 권고 드리는 것입니다. 예방 방법대로 방화벽 포트 설정 및 윈도우 업데이트 버전이 최신인 경우 평소대로 PC 사용하셔도 됩니다.

Q9. 회사 네트워크의 경우, 어떻게 보안 설정을 하면 되나요?

○ 회사의 방화벽 인바운드 정책에 UDP 137번, 138번과 TCP 139번, 445번을 차단하셔야 합니다.
- WannaCry 랜섬웨어의 경우 TCP 445번 포트만 해당되나, WannaCry 변종이 존재할 가능성이 있어 SMB 프로토콜 관련 포트인 UDP 137, 138, TCP 139까지 전부 적용하는 것을 권고

○ 방화벽이 내부망 내에 존재하지 않는 경우, 개별 직원 PC에서 직접 방화벽 설정을 추가 하도록 해야 합니다.

[붙임] Windows 버전별 SMB 상세 차단방법

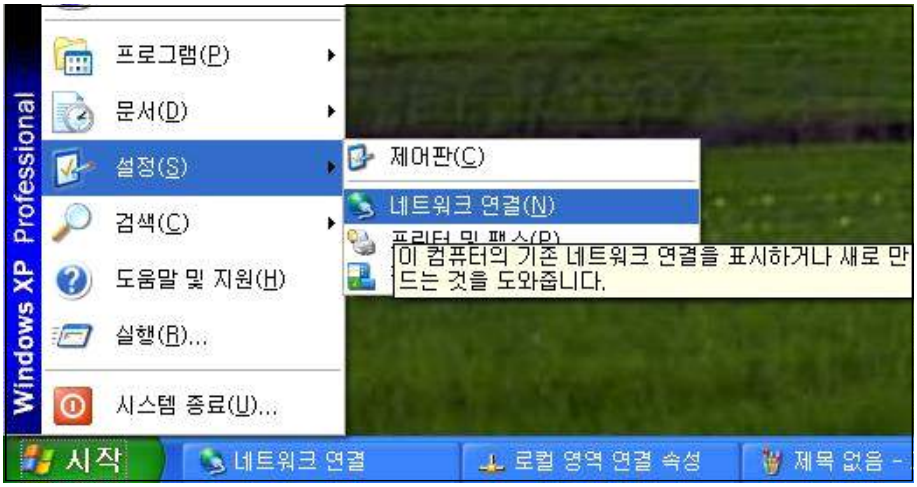
1. Windows XP & Windows Server 2003

* 해당 취약점을 해결하기 위해서 아래 2개 방법 중 한 가지만 수행하면 됩니다.

☐ **SMB 기능 해제 방법**

① 바탕화면에 있는 "시작" 선택 하여 설정에서 [네트워크 및 공유 센터] 실행

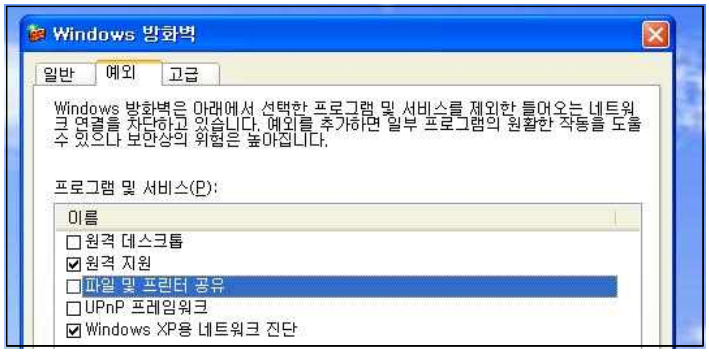
- [시작] -> [설정] -> [네트워크 연결] -> "로컬 영역 연결" 우클릭 -> [속성] -> "Microsoft 네트워크용 파일 및 프린터 공유" 체크 해제 -> 확인



② [네트워크 연결]에서 "로컬 영역 연결" 우클릭 -> [속성] -> "Microsoft 네트워크용 파일 및 프린터 공유" 체크 해제 -> 확인

☐ **방화벽 포트설정 방법**

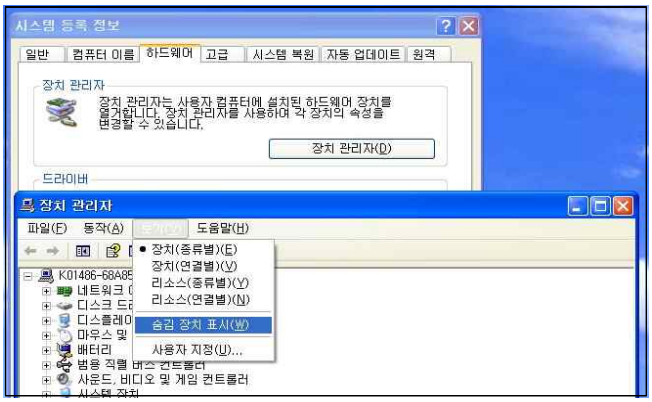
- [시작] -> [설정] -> [제어판] -> [Windows 방화벽] -> "사용(권장)" 체크 -> [예외] 탭 -> "파일 및 프린터 공유" 체크 박스 해제 -> 확인



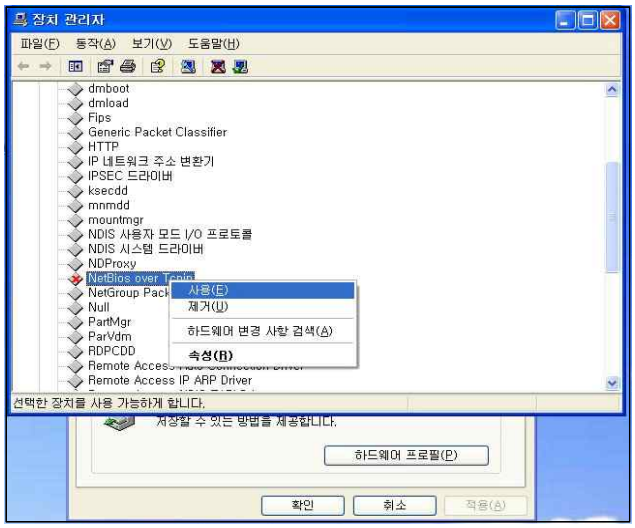
☐ **기존 안내 한 "NetBIOS over TcpIp" 사용안함으로 설정 시 인터넷이 되지 않는 경우**

※ "NetBIOS over TcpIp" 사용안함 설정 시 DHCP 주소를 받아오지 못하는 문제점이 있어 사용함으로 변경

- [내 컴퓨터] 우클릭 -> [속성] -> [하드웨어] -> [장치 관리자] -> [보기] -> [숨김 장치 표시] -> "비 플러그 앤 플레이" 확장 -> [NetBIOS over TcpIp] 사용 -> PC 다시시작



⇓



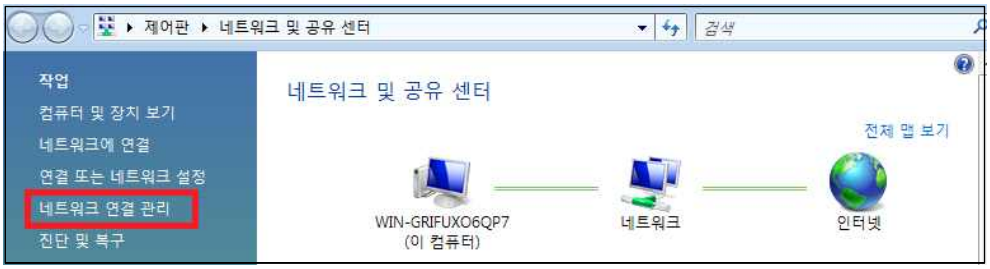
2. Windows Vista

* 해당 취약점을 해결하기 위해서 아래 2개 방법 중 한 가지만 수행하면 됩니다.

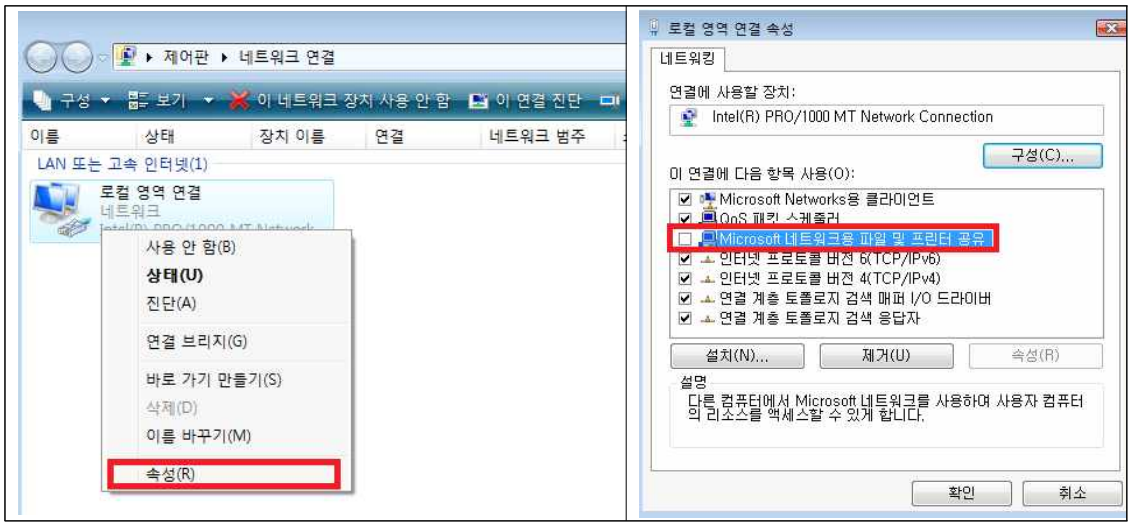
☐ SMB 기능 해제 방법

① 바탕화면에 있는 "시작" 클릭 하여 "네트워크" 검색 후 [네트워크 및 공유 센터] 실행

② "네트워크 연결 관리" 클릭



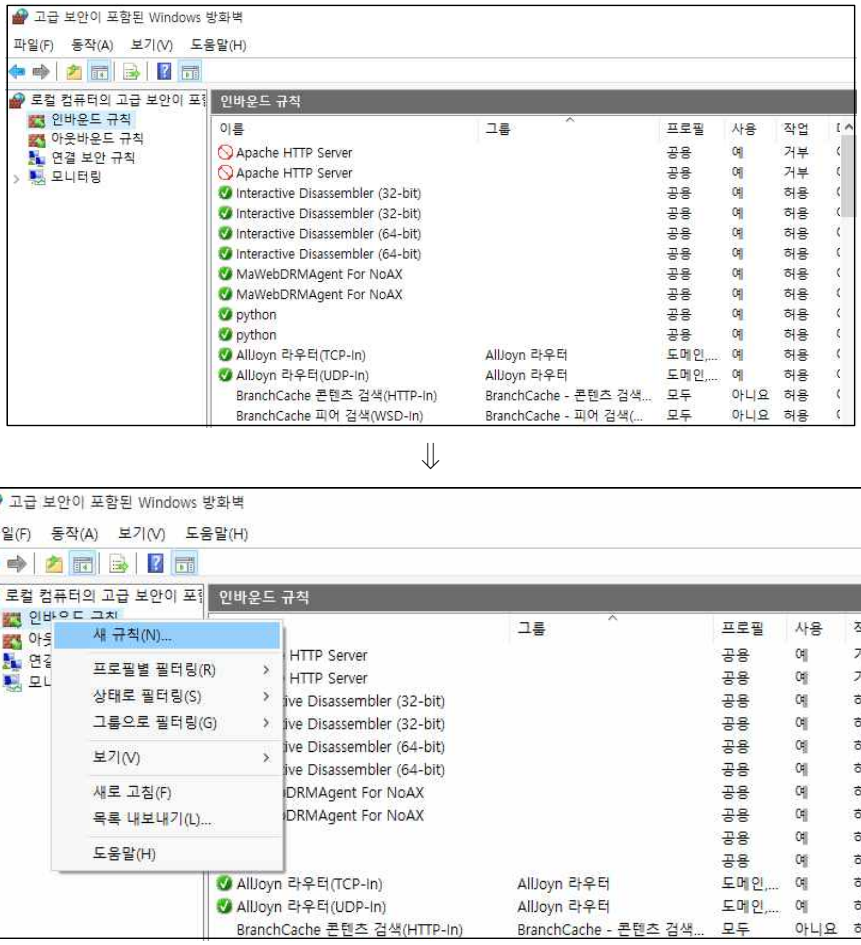
③ "로컬 영역 연결" 우클릭 -> [속성] -> "Microsoft 네트워크용 파일 및 프린터 공유" 체크 해제 -> 확인



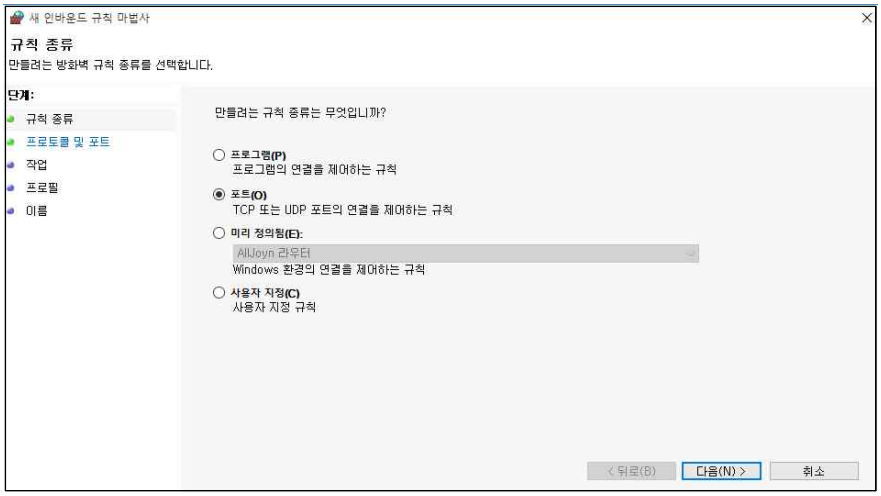
□ **방화벽 포트설정 방법**

① 바탕화면에 있는 "시작" 클릭 하여 "고급 보안" 검색 후 해당 프로그램 실행

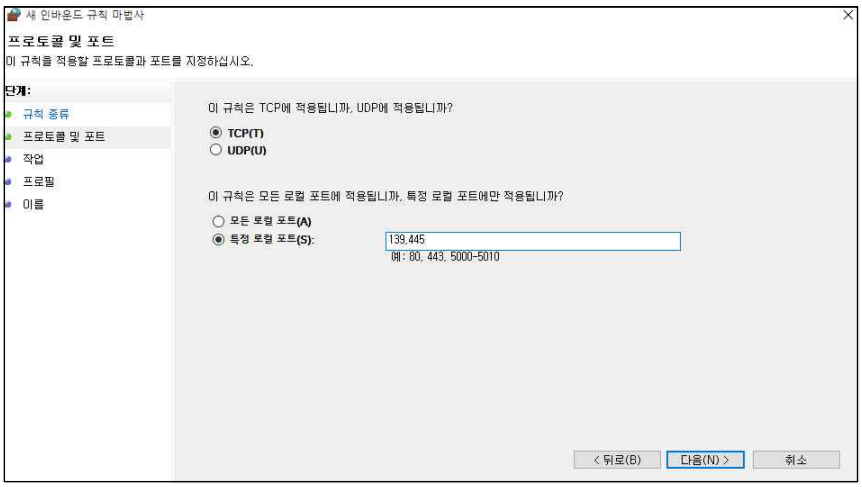
② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



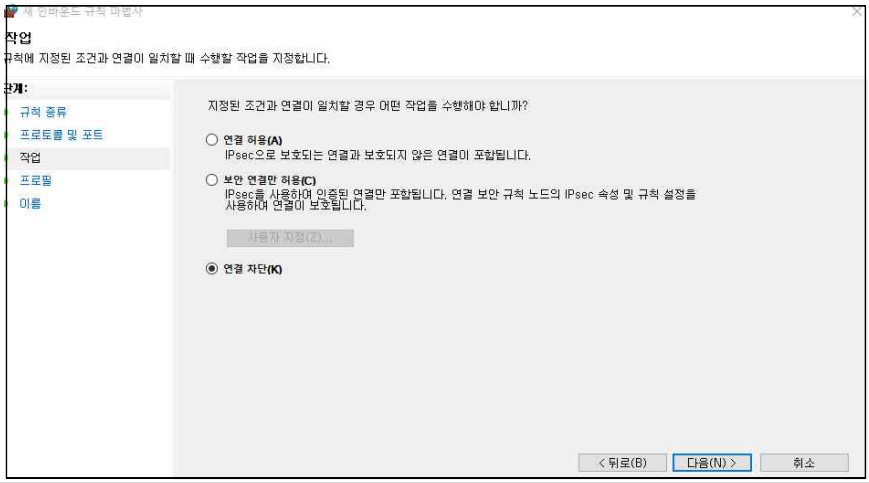
③ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭



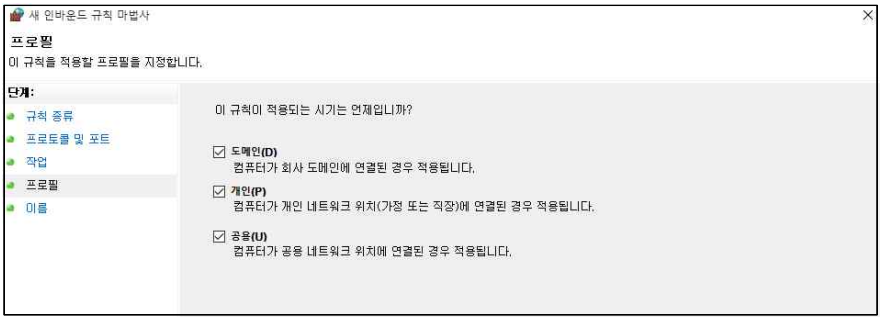
④ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



⑤ "연결 차단" 선택



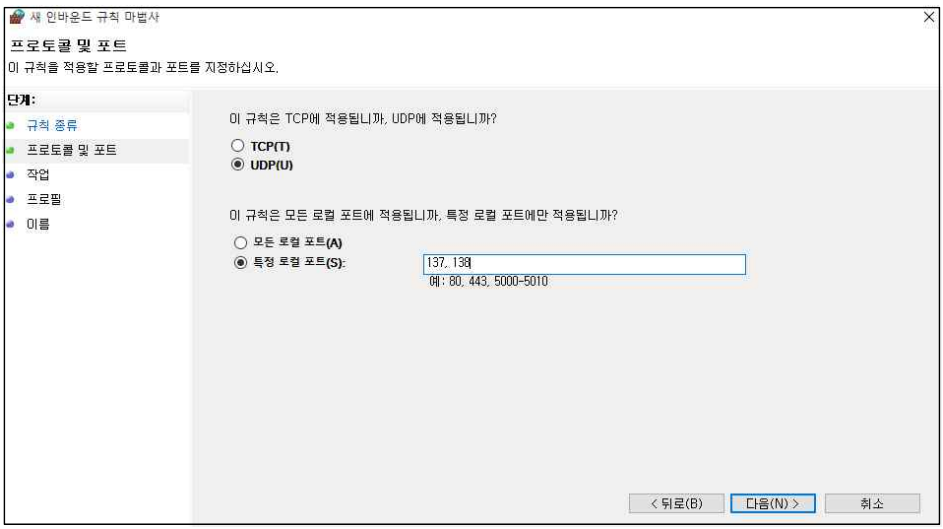
⑥ "도메인", "개인", "공용" 체크 후 "다음" 클릭



⑦ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭

※ 이름의 경우 사용자 임의로 입력 가능

⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단
(④번 화면을 아래의 화면으로 대신하여 설정하면 됨)

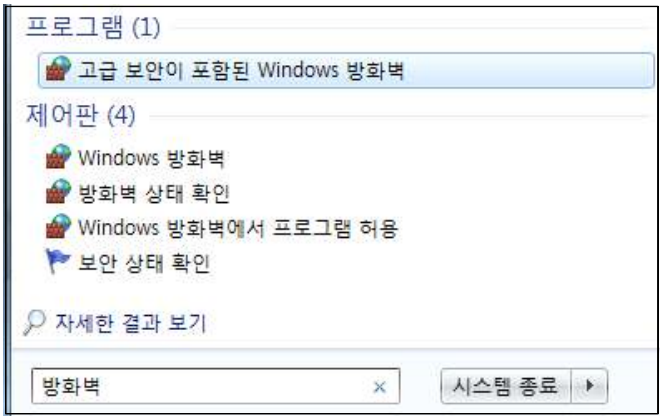


3. Windows 7

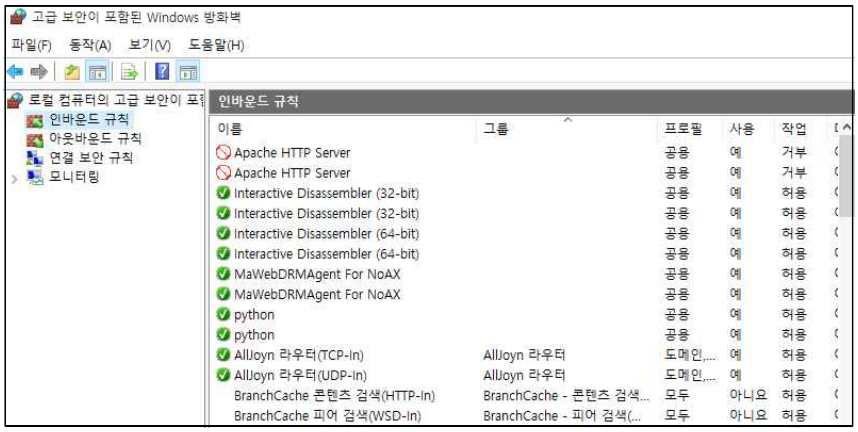
* 해당 취약점을 해결하기 위해서 아래 2개 방법 중 한 가지만 수행하면 됩니다.

□ 방화벽 포트설정 방법

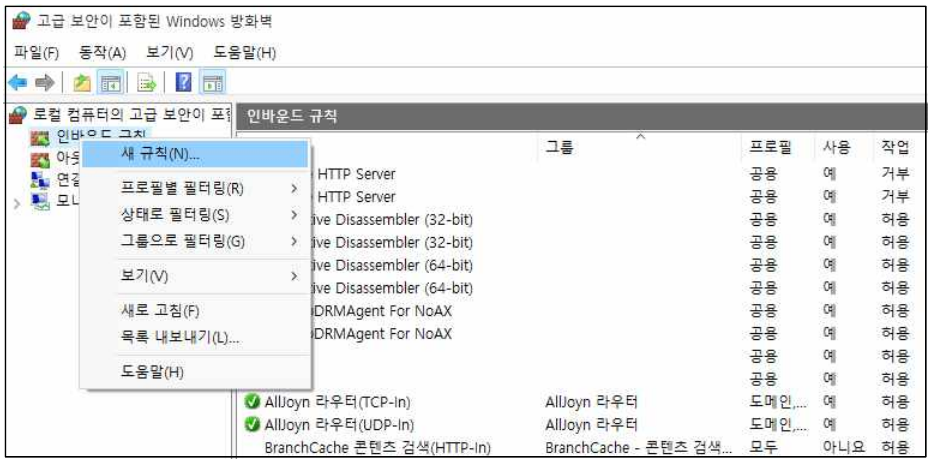
① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "방화벽" 검색 후 해당 프로그램 실행



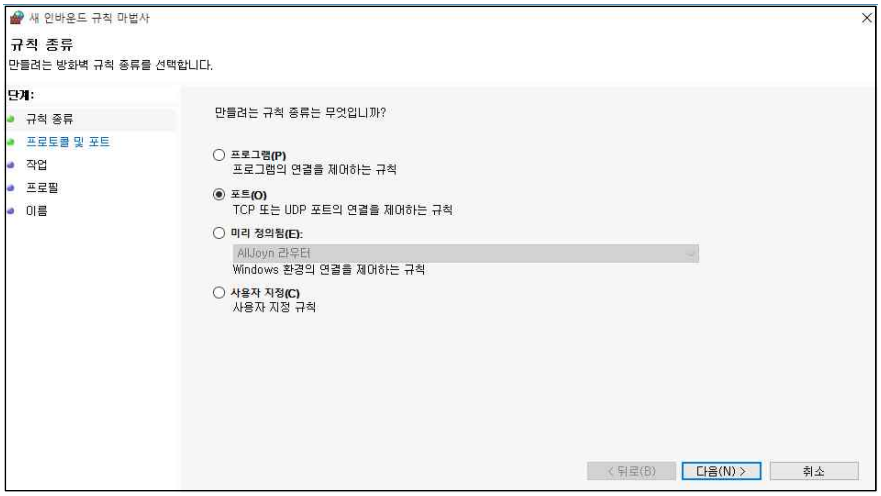
② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



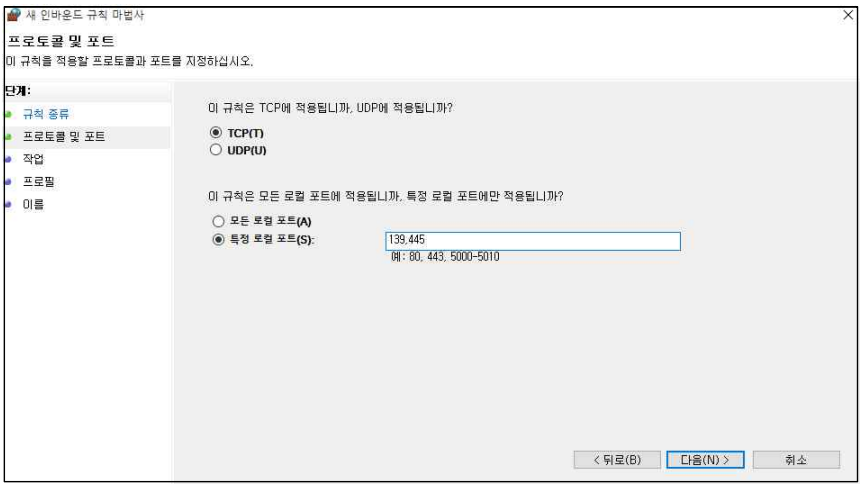
⇓



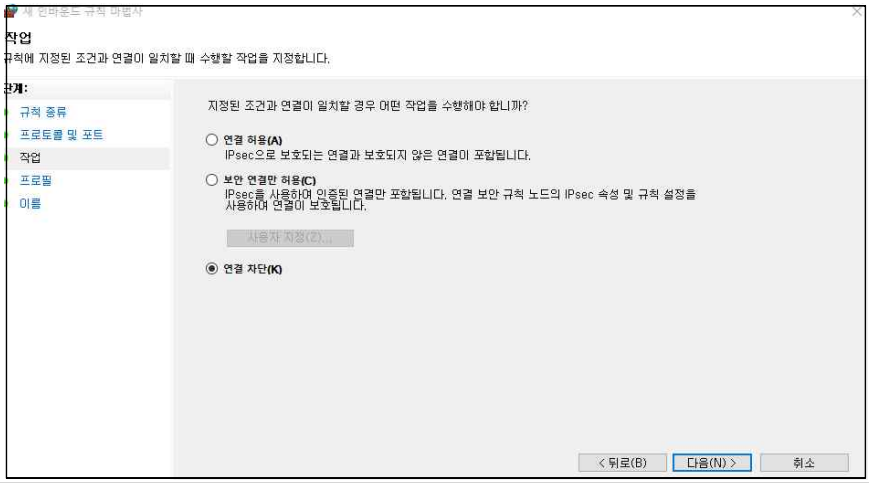
④ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭



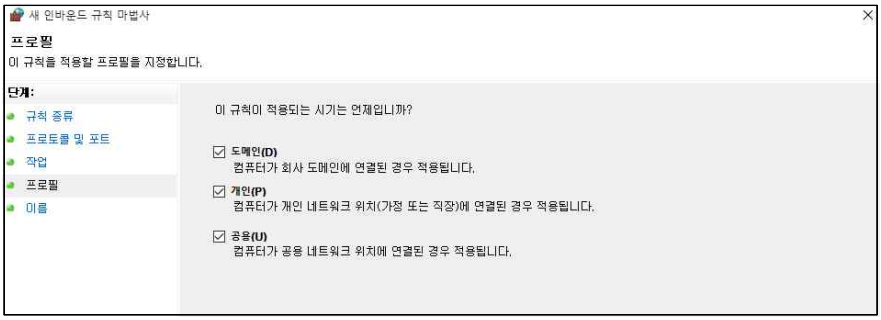
⑤ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



⑥ "연결 차단" 선택



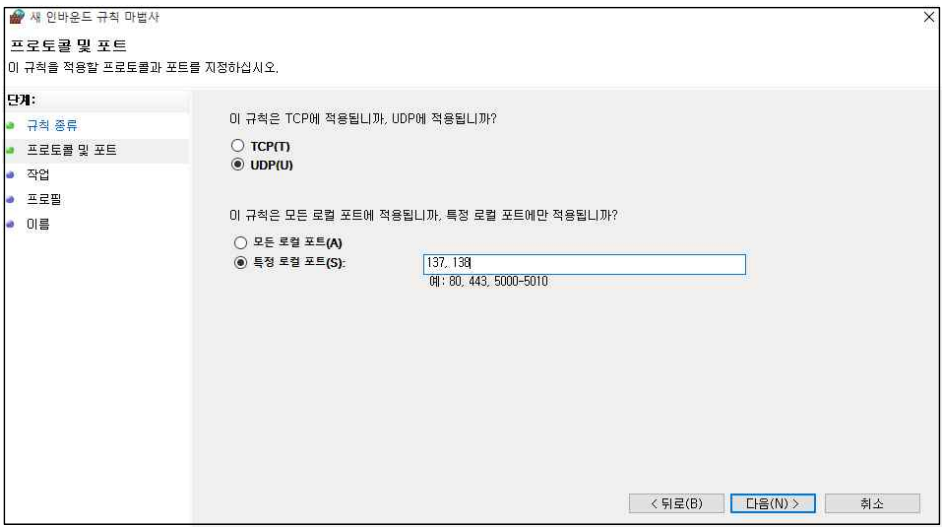
⑦ "도메인", "개인", "공용" 체크 후 "다음" 클릭



⑧ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭

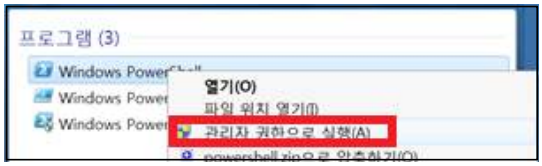
※ 이름의 경우 사용자 임의로 입력 가능

⑨ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단
(⑤번 화면을 아래의 화면으로 대신하여 설정하면 됨)



☐ **레지스트리 등록 방법**

① [시작] -> powershell 검색 -> 관리자 권한으로 실행



② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

③ set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32>
```

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키

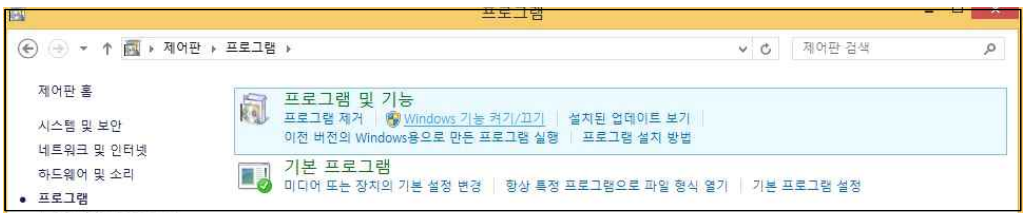
4. Windows 8.1

* 해당 취약점을 해결하기 위해서 아래 3개 방법 중 한 가지만 수행하면 됩니다.

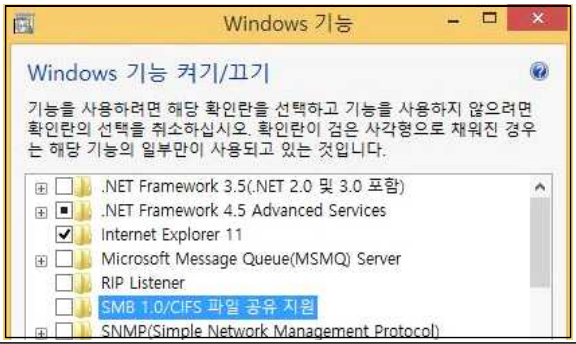
☐ **SMB 기능 해제 방법**

① 제어판 -> 프로그램 -> Windows 기능 설정 또는 해제 -> SMB1.0/CIFS 파일 공유 지원 체크해제 -> 시스템 재시작

* 해당 서비스를 다시 사용해야 하는 경우 제어판 -> 프로그램 -> Windows 기능 설정 또는 해제 -> SMB1.0/CIFS 파일 공유 지원 체크 -> 시스템 재시작



⇓

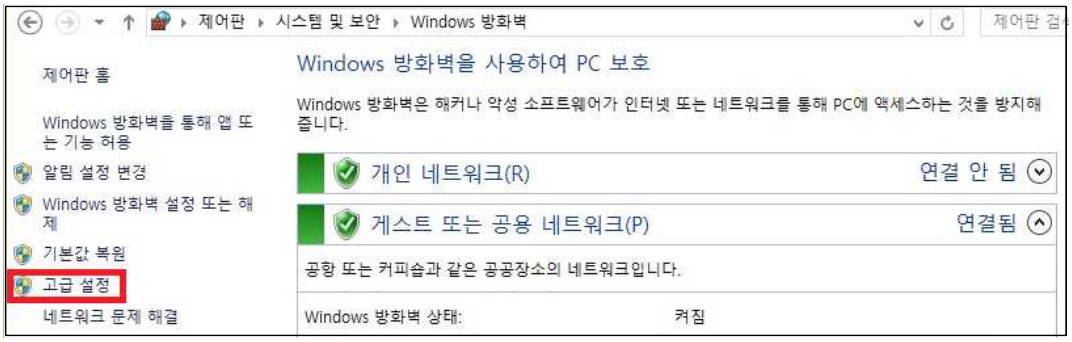


☐ **방화벽 포트설정 방법**

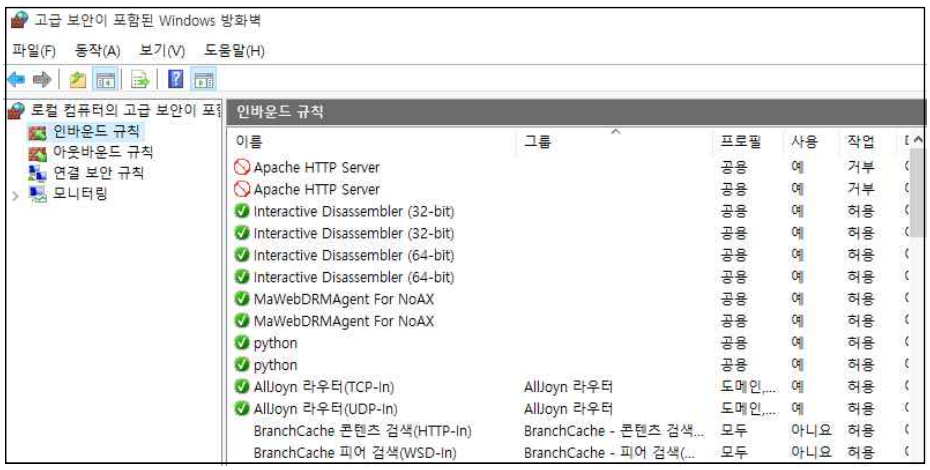
① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "제어판" 검색 후 해당 프로그램 실행

② [제어판] -> [시스템 및 보안] -> [Windows 방화벽] 선택

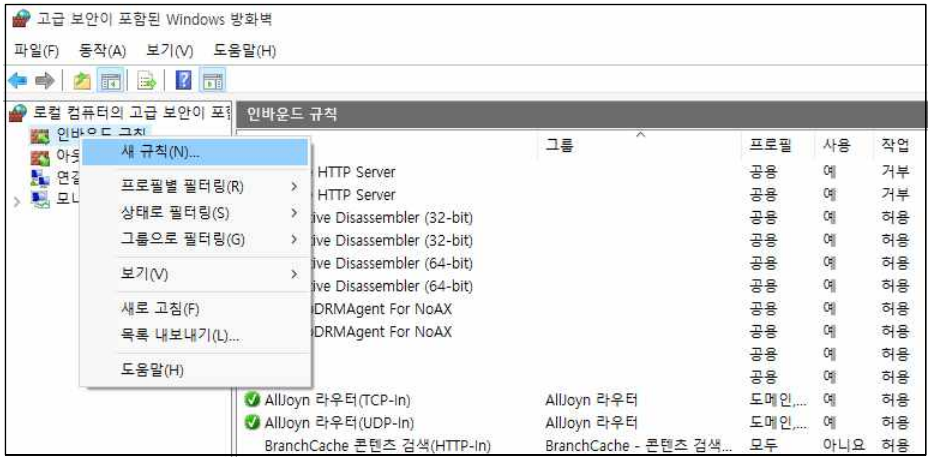
③ [Windows 방화벽] -> [고급 설정] 선택



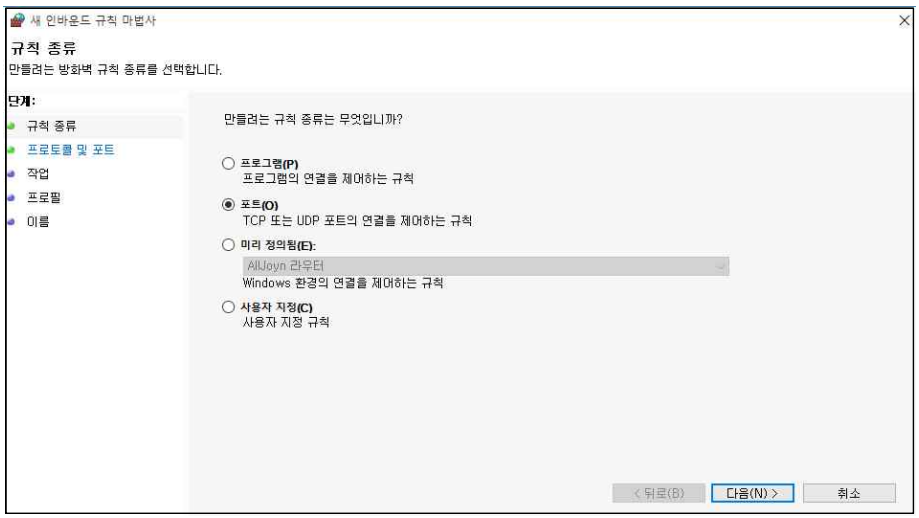
④ 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



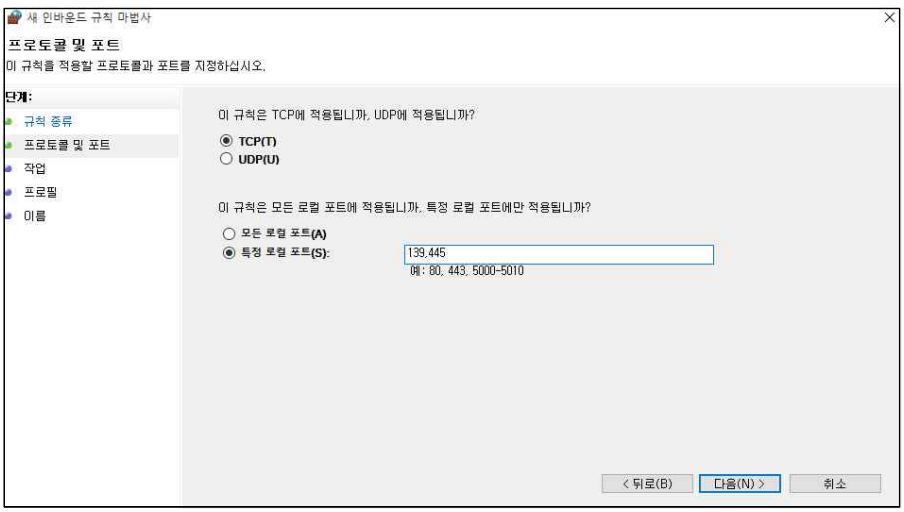
⇓



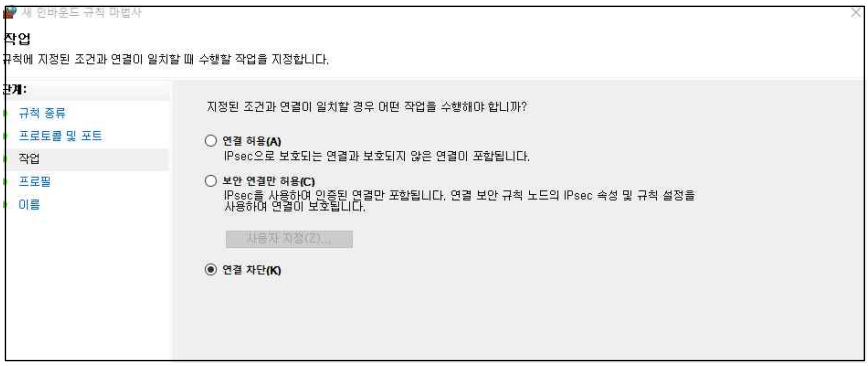
⑤ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭



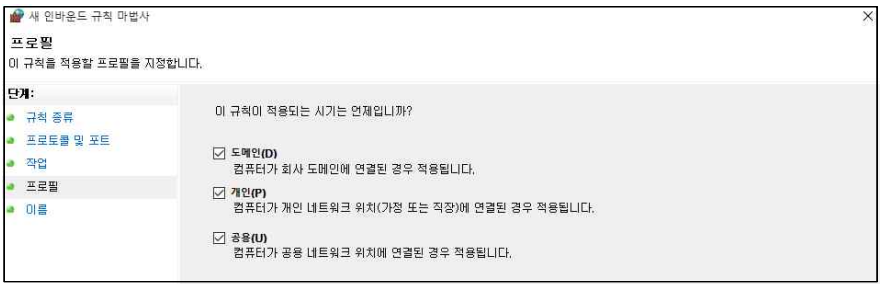
⑥ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



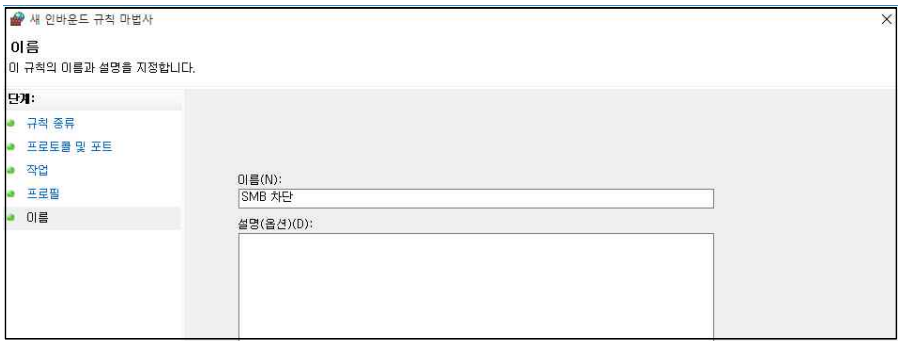
⑦ "연결 차단" 선택



⑧ "도메인", "개인", "공용" 체크 후 "다음" 클릭

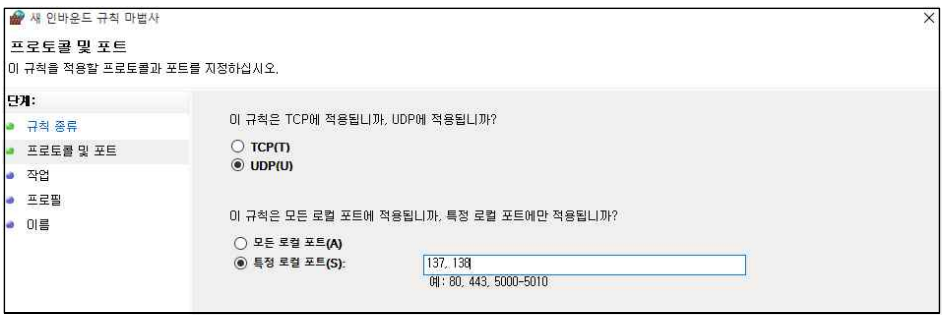


⑨ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭



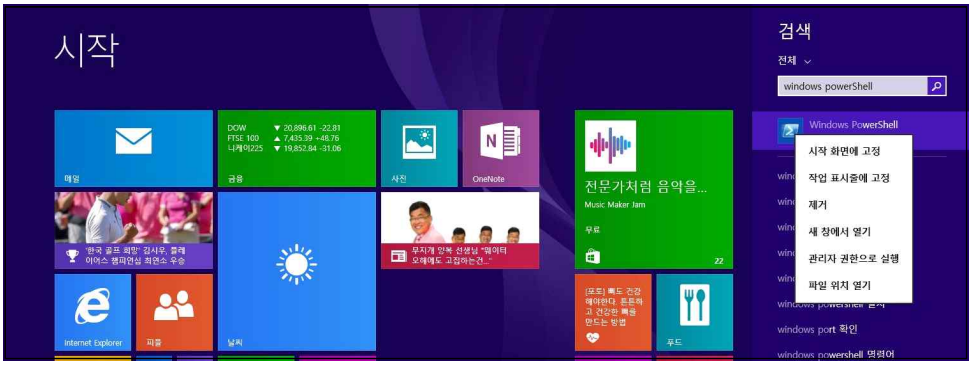
※ 이름의 경우 사용자 임의로 입력 가능

⑩ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단
(⑥번 화면을 아래의 화면으로 대신하여 설정하면 됨)



☐ **레지스트리 등록 방법**

① [시작] -> powershell 검색 -> 관리자 권한으로 실행



② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

③ set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32>
```

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

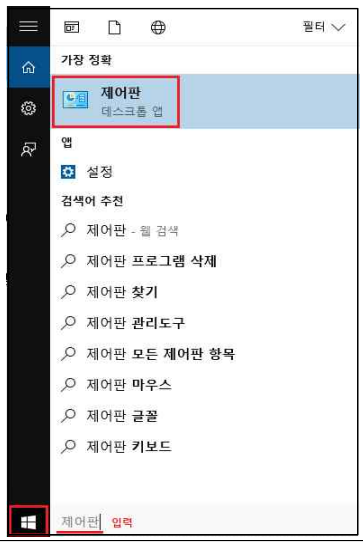
② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키

5. Windows 10

* 해당 취약점을 해결하기 위해서 아래 3개 방법 중 한 가지만 수행하면 됩니다.

☐ **SMB 기능 해제 방법**

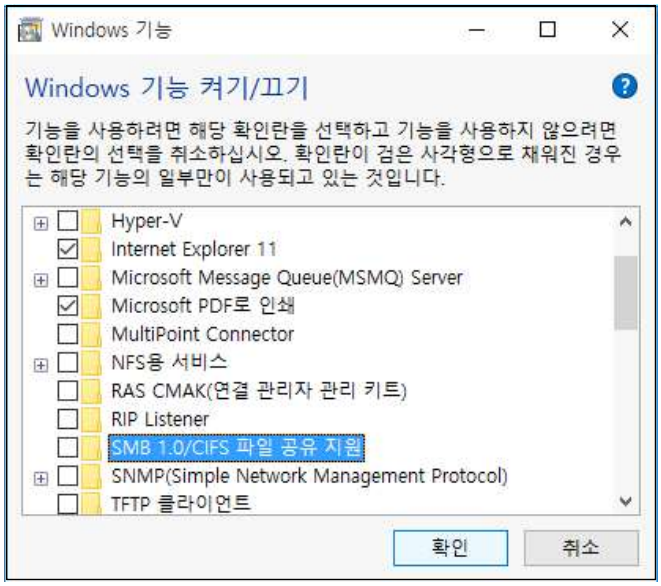
① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "제어판" 검색 후 해당 프로그램 실행



② 제어판 내 "프로그램" 선택

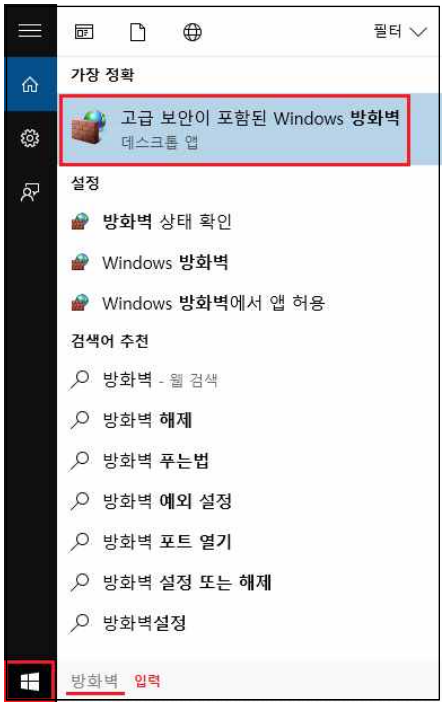
③ 프로그램에서 프로그램 및 기능의 "Windows 기능 켜기/끄기" 선택

④ SMB 기능에서 "SMB 1.0/CIFS 파일 공유 지원" 기능 해제(체크 표시 클릭으로 해제) 후 확인

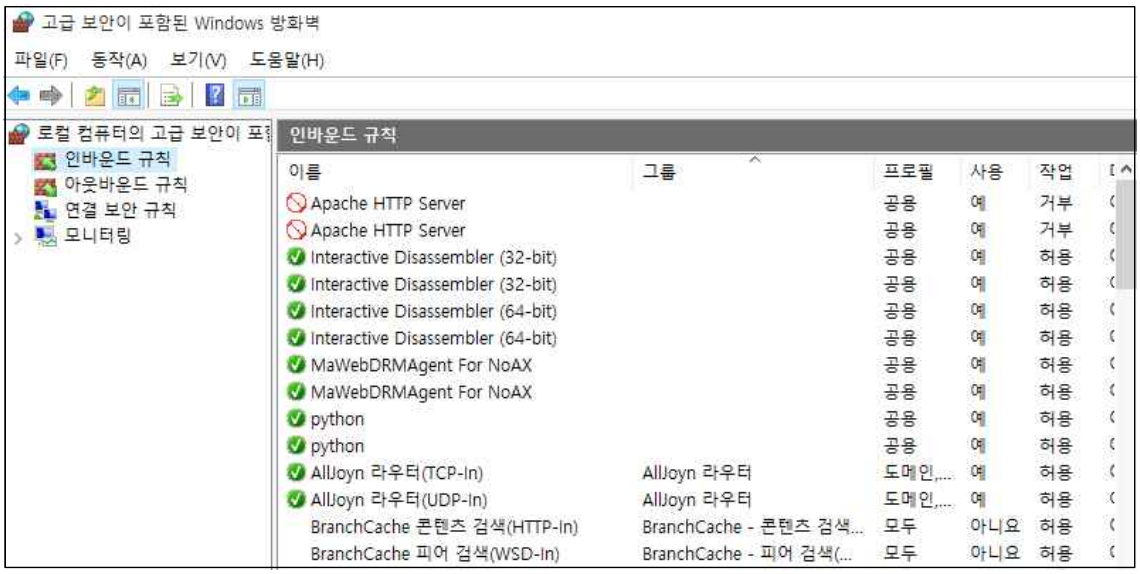


☐ **방화벽 포트설정 방법**

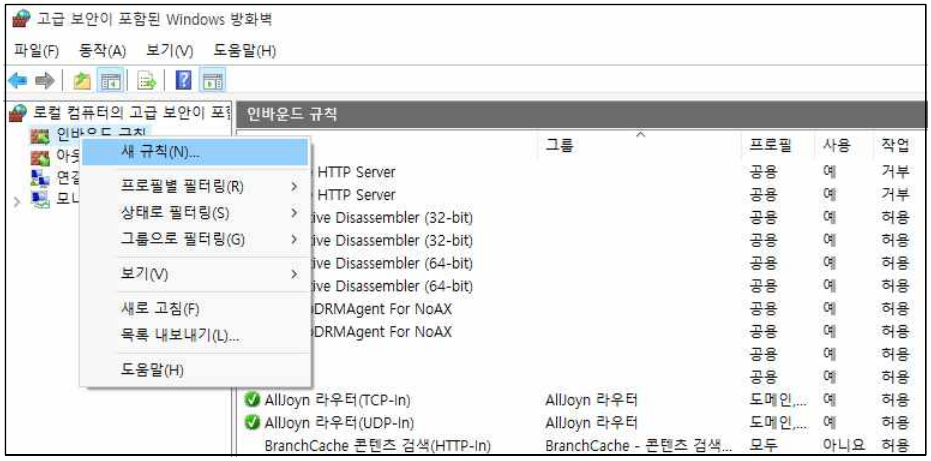
① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "방화벽" 검색 후 해당 프로그램 실행



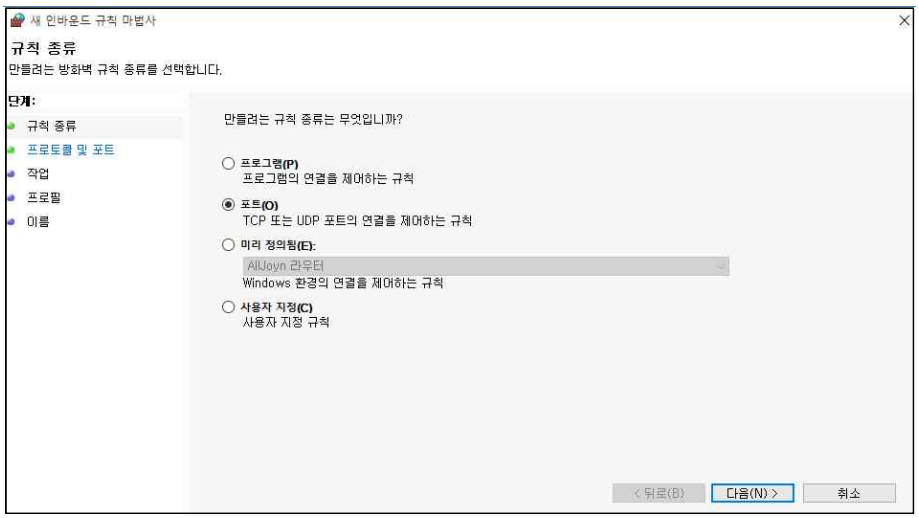
② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



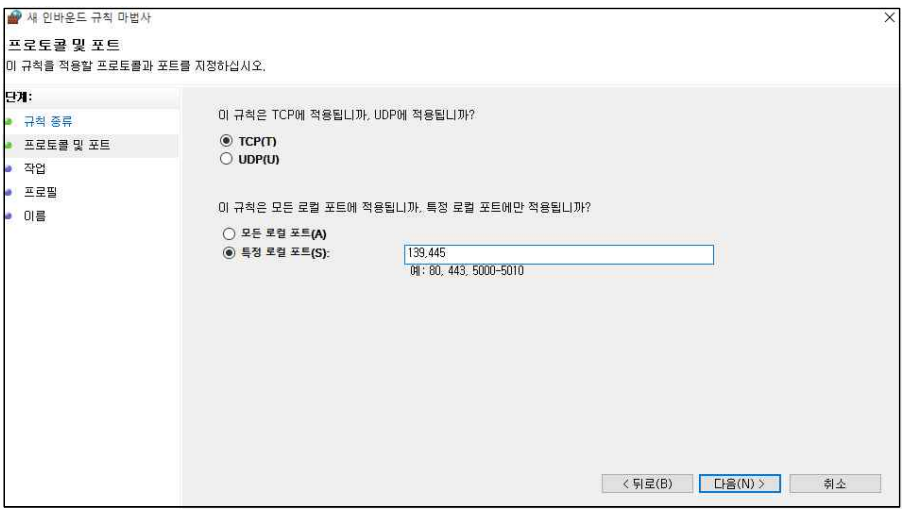
⇓



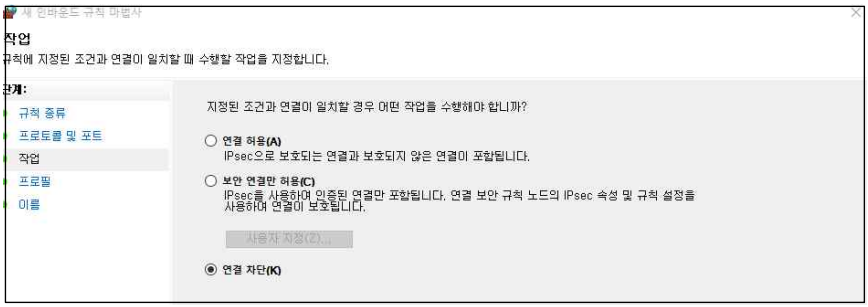
③ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭



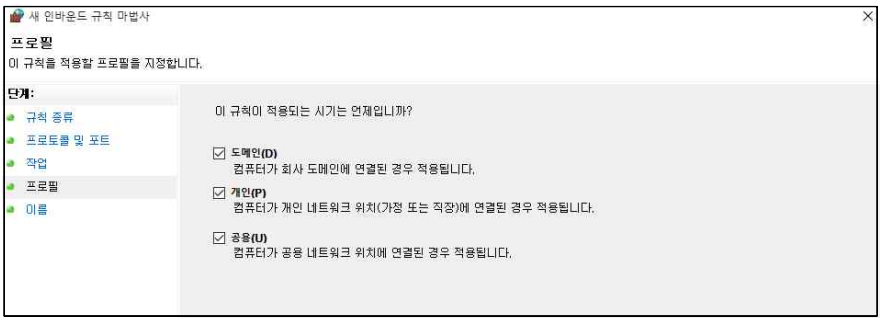
④ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



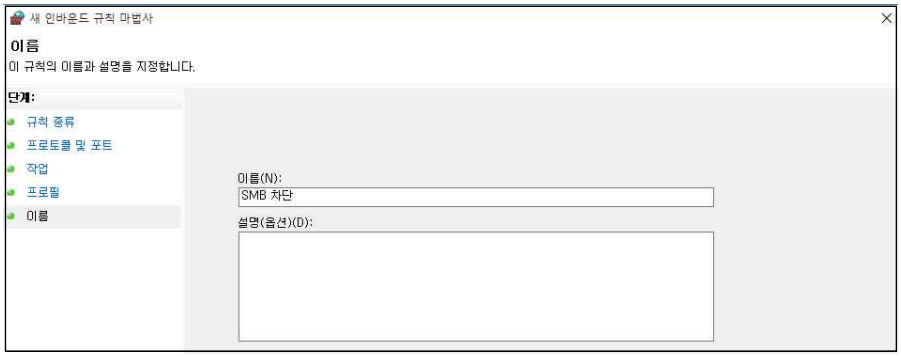
⑤ "연결 차단" 선택



⑥ "도메인", "개인", "공용" 체크 후 "다음" 클릭

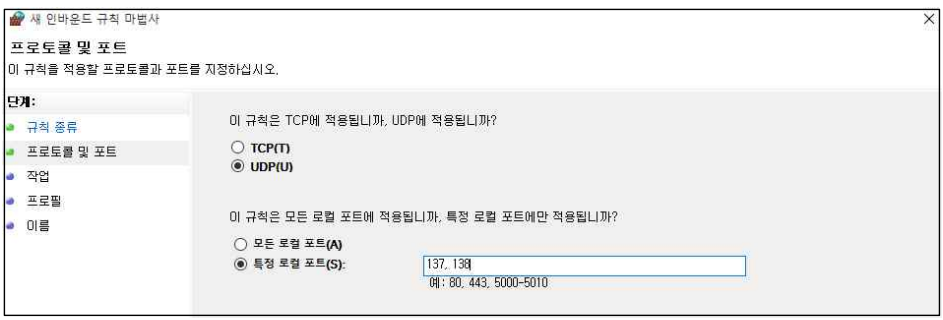


⑦ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭



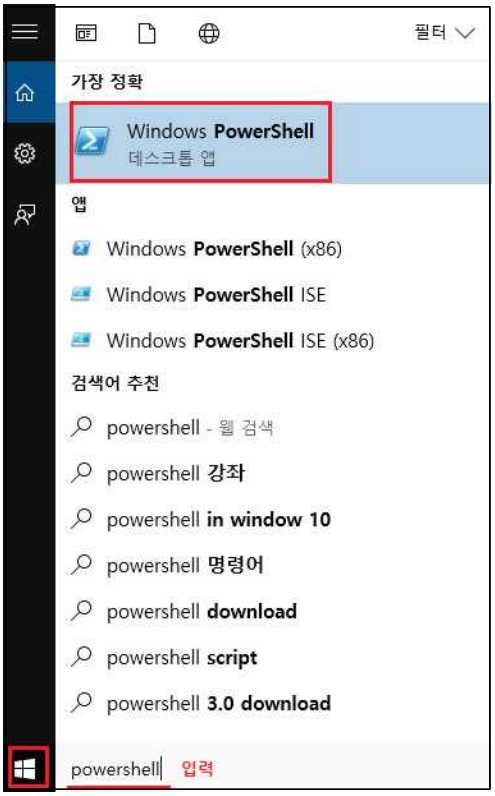
※ 이름의 경우 사용자 임의로 입력 가능

⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단
(④번 화면을 아래의 화면으로 대신하여 설정하면 됨)



☐ **레지스트리 등록 방법**

① [시작] -> powershell 검색 -> 관리자 권한으로 실행



② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

③ set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32>
```

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키

6. Windows Server 2008

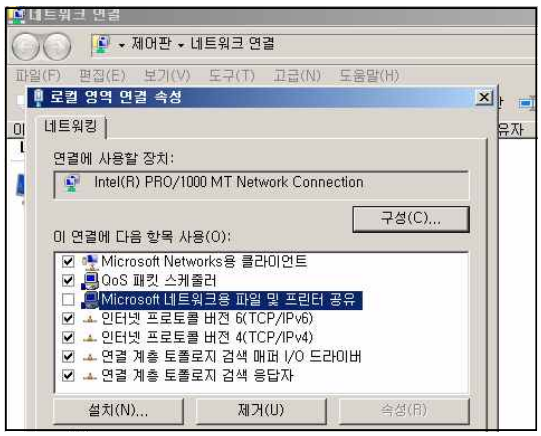
* 해당 취약점을 해결하기 위해서 아래 2개 방법 중 한 가지만 수행하면 됩니다.

☐ SMB 기능 해제 방법(Windows Server 2008의 경우)

① [시작] -> "네트워크" 입력 -> 네트워크 및 공유 센터 클릭

② "네트워크 연결 관리" 클릭 -> 로컬 영역 연결 마우스 "우클릭" -> 속성 클릭

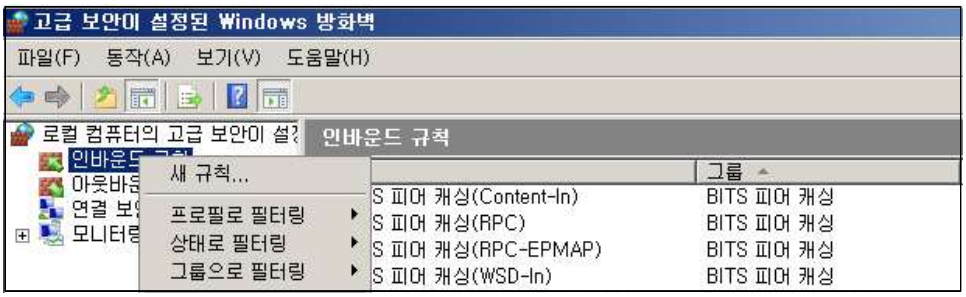
③ "Microsoft 네트워크용 파일 및 프린터 공유" 체크해제 -> 확인



□ **방화벽 포트설정 방법**

① 바탕화면에 있는 "시작" 클릭 하여 "고급 보안" 검색 후 해당 프로그램 실행

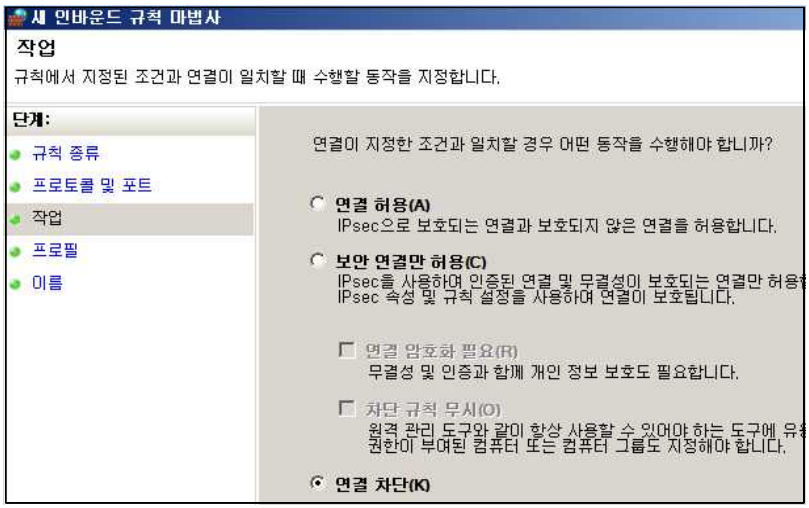
② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭



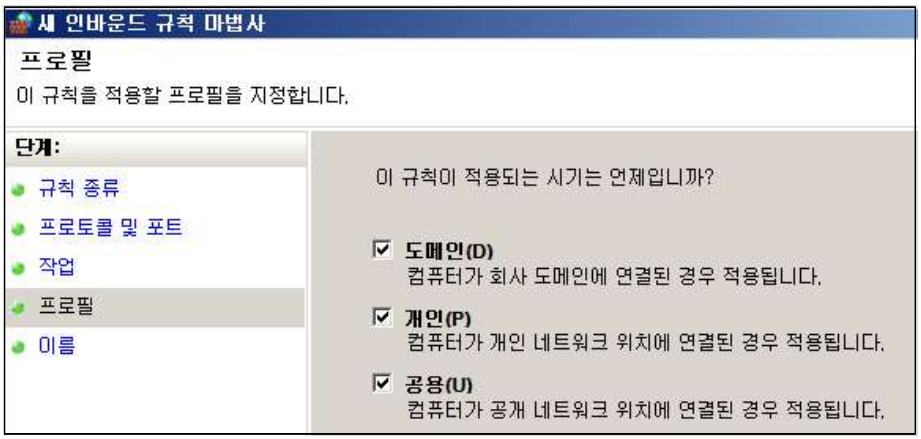
③ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭

④ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭

⑤ "연결 차단" 선택



⑥ "도메인", "개인", "공용" 체크 후 "다음" 클릭

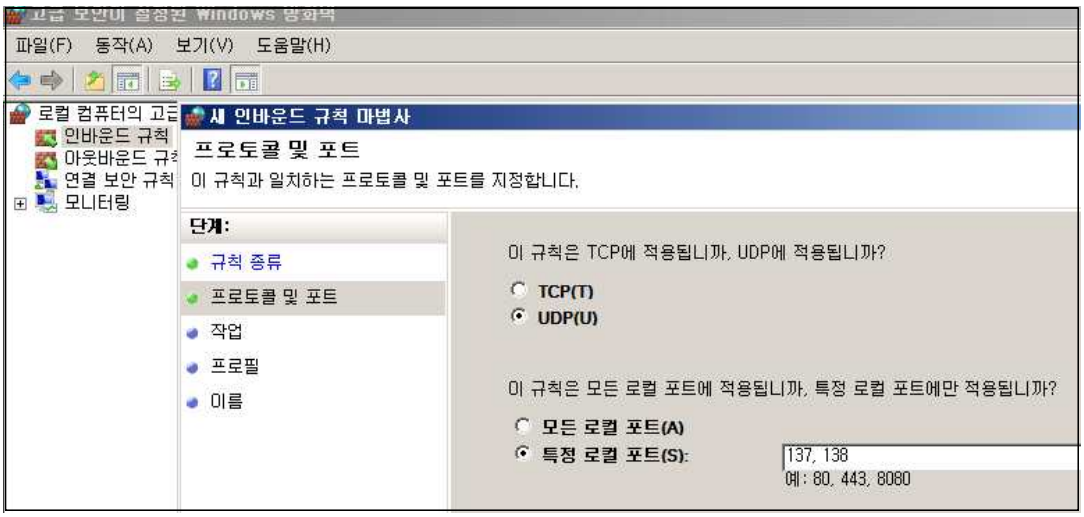


⑦ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭

※ 이름의 경우 사용자 임의로 입력 가능

⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단

(④번 화면을 아래의 화면으로 대신하여 설정하면 됨)



7. Windows Server 2008 R2

* 해당 취약점을 해결하기 위해서 아래 2개 방법 중 한 가지만 수행하면 됩니다.

☐ 방화벽 포트설정 방법

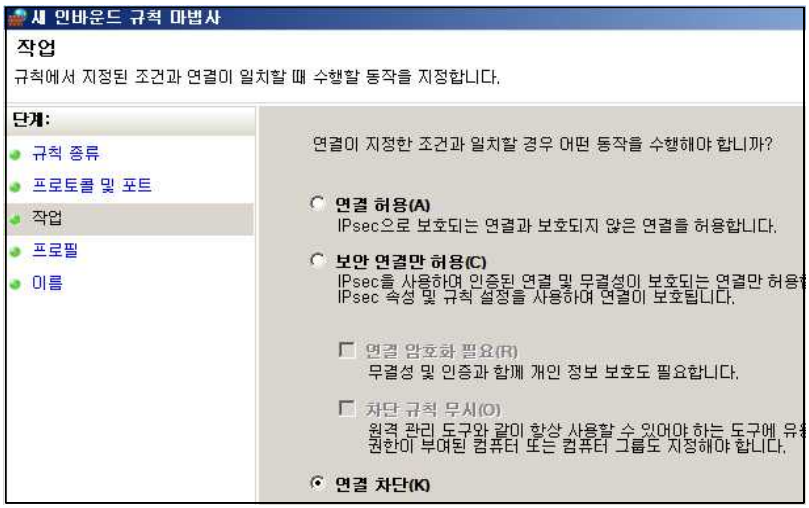
① 바탕화면에 있는 "시작" 클릭 하여 "고급 보안" 검색 후 해당 프로그램 실행

② 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭

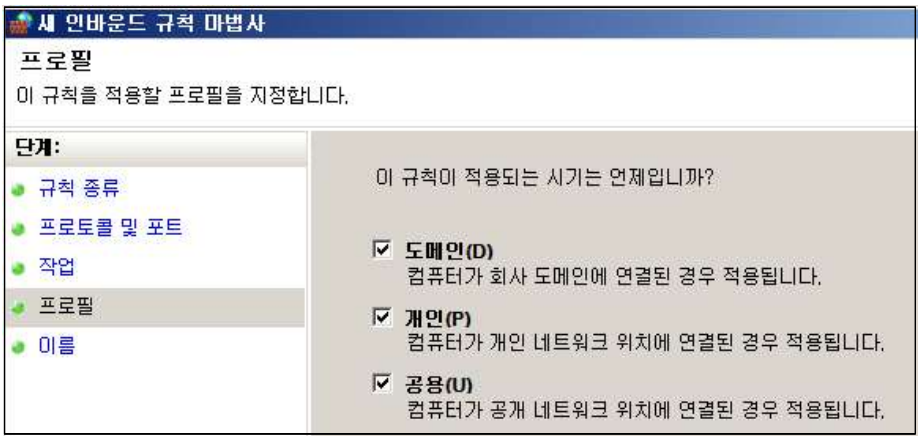
③ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭

④ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭

⑤ "연결 차단" 선택



⑥ "도메인", "개인", "공용" 체크 후 "다음" 클릭

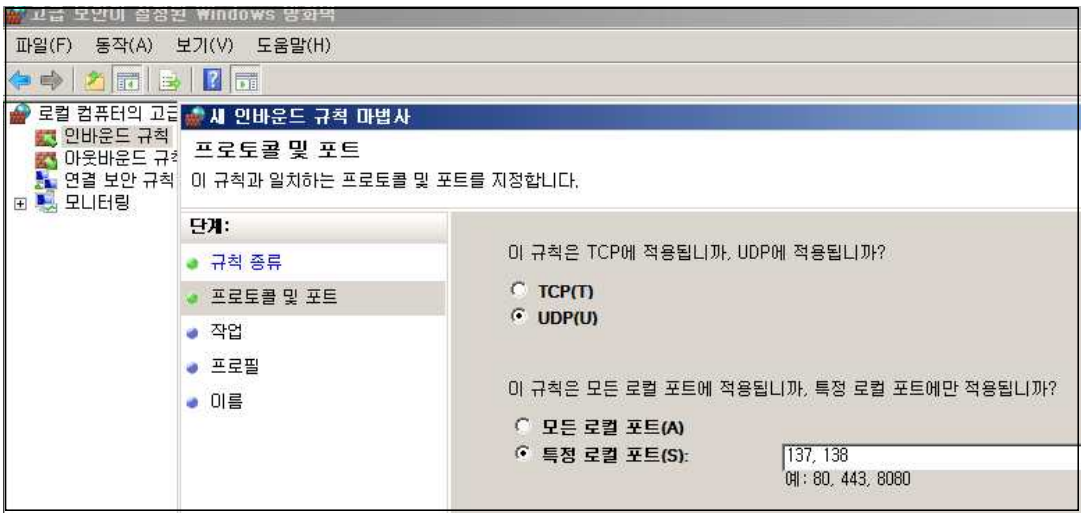


⑦ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭

※ 이름의 경우 사용자 임의로 입력 가능

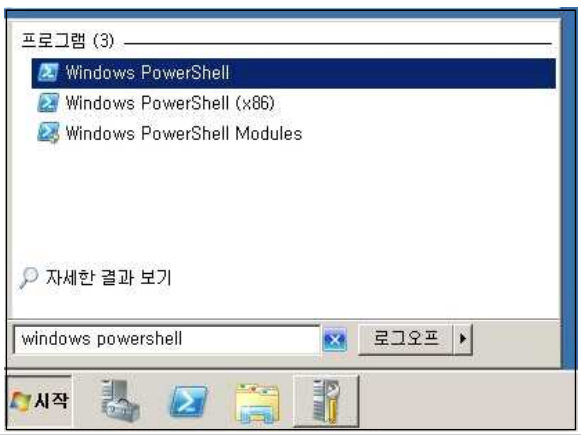
⑧ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단

(④번 화면을 아래의 화면으로 대신하여 설정하면 됨)



□ 레지스트리 등록 방법

① [시작] -> "powershell" 입력 -> 마우스 "우클릭" -> 관리자 권한으로 실행



② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

③ set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> _
```

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키

8. Windows Server 2012 & Windows Server 2012 R2 & Windows Server 2016

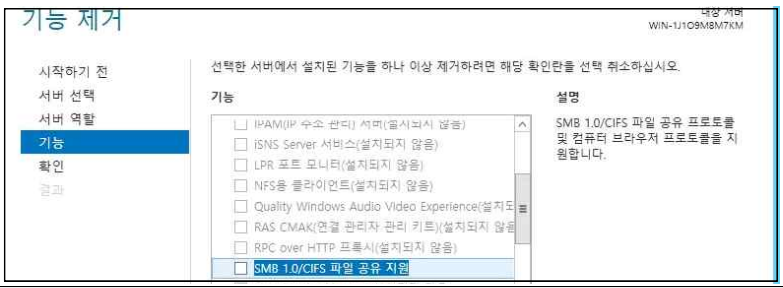
* 해당 취약점을 해결하기 위해서 아래 3개 방법 중 한 가지만 수행하면 됩니다.

☐ **SMB 기능 해제 방법(Windows Server 2012는 해당사항 없음, Windows Server 2012 R2 및 Server 2016만 해당)**

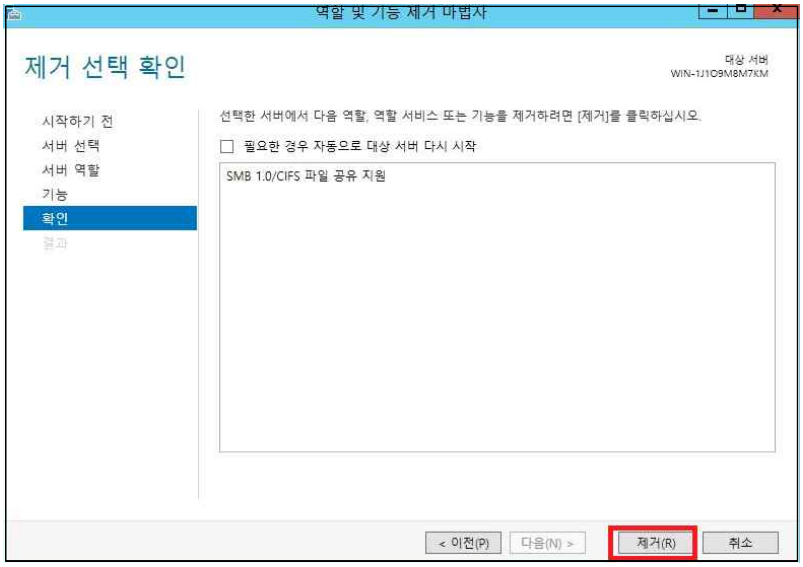
① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "서버 관리자" 실행

② 서버 관리자 내 [관리] -> [역할 및 기능 제거] 선택

③ 역할 및 기능 제거 마법사 실행 후 [다음] -> [기능] -> "SMB 1.0/CIFS 파일 공유 지원" 체크 해제



④ "SMB 1.0/CIFS 파일 공유 지원" 기능 해제된 사항 확인 후 "제거" 클릭 후 재부팅



⇓

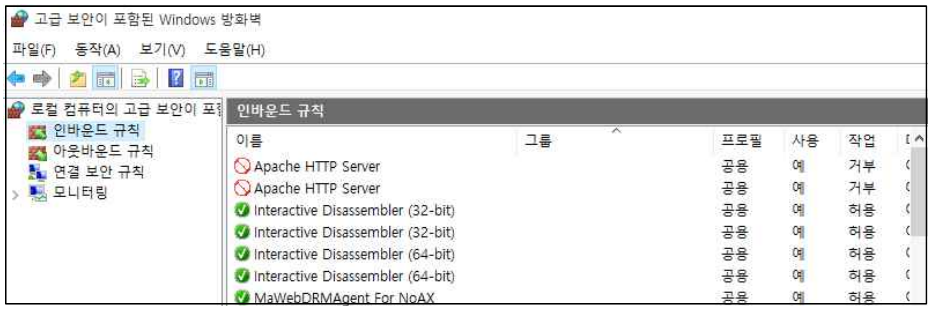
□ 방화벽 포트설정 방법

① [시작] -> [제어판] -> 시스템 및 보안 클릭

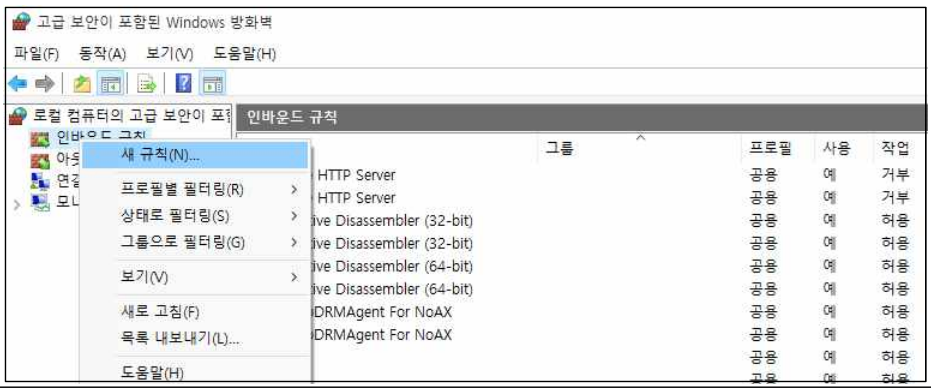
② [Windows 방화벽] 클릭

③ [고급설정] 클릭

④ 방화벽 내에 "인바운드 규칙" 오른쪽 버튼으로 클릭 후 "새규칙" 클릭

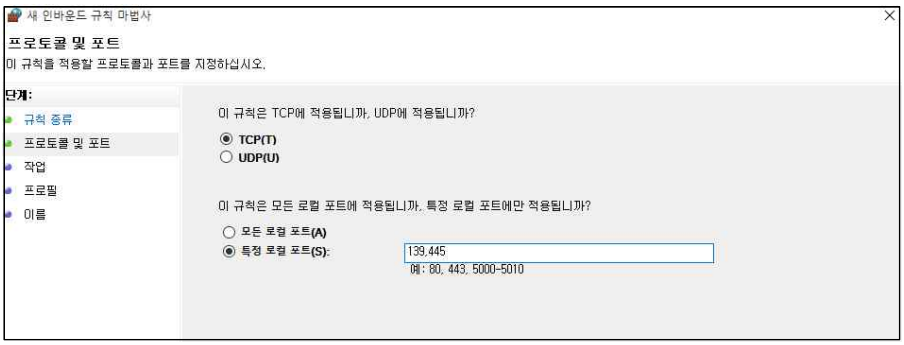


⇓

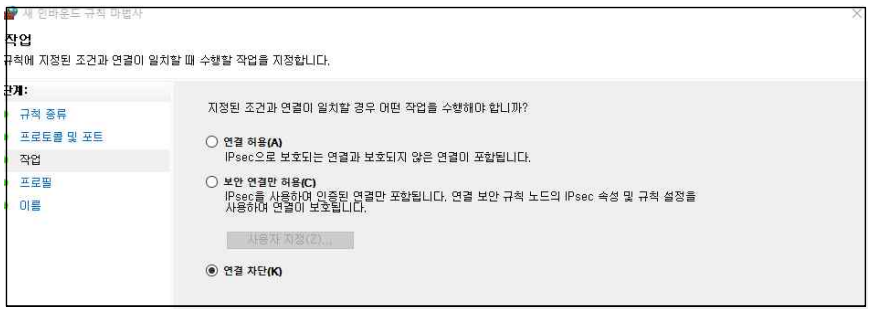


⑤ 새 인바운드 규칙 마법사에서 "포트" 체크 후 "다음" 클릭

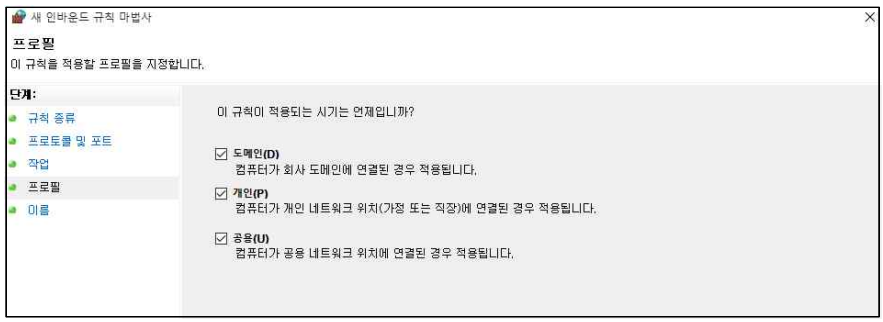
⑥ "TCP", "특정 포털 포트" 체크 후 "139, 445" 입력 후 "다음" 클릭



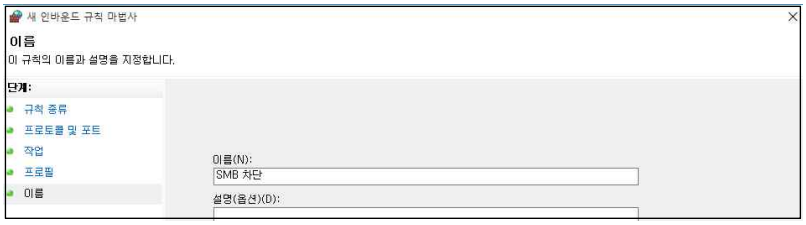
⑦ "연결 차단" 선택



⑧ "도메인", "개인", "공용" 체크 후 "다음" 클릭

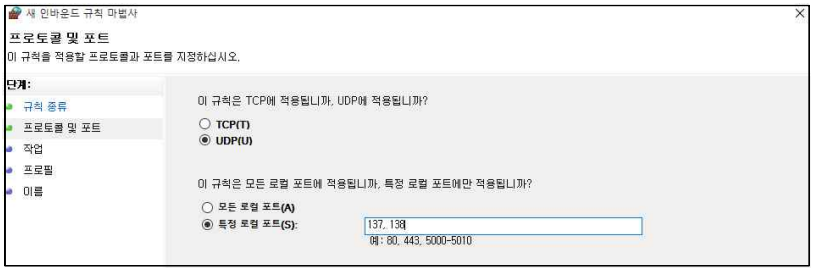


⑨ 이름을 "SMB 차단"으로 입력 후 "확인" 클릭



※ 이름의 경우 사용자 임의로 입력 가능

⑩ 이와 같은 방법으로 동일하게 "UDP", "특정 로컬 포트" 내 137, 138 포트 차단 (⑥번 화면을 아래의 화면으로 대신하여 설정하면 됨)



□ 레지스트리 등록 방법

① 바탕화면에 있는 윈도우 로고(시작 버튼) 클릭 하여 "Windows PowerShell" 마우스 우클릭 후 관리자 권한으로 실행

② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force 입력 -> Enter 키

③ set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -Value 0 -Force 입력 -> Enter 키

```
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32> Set-ItemProperty -Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 -T
ype DWORD -Value 0 -Force
PS C:₩Windows₩system32>
```

* 해당 서비스를 다시 사용해야 하는 경우

① set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB1 –Type DWORD –Value 1 –Force 입력 -> Enter 키

② set-ItemProperty –Path "HKLM:₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters" SMB2 –Type DWORD –Value 1 –Force 입력 -> Enter 키