윈도우즈 환경에서의
공유폴더 취약점을 이용한 공격 유형 및 취약점 대응 방법

(Ver. 1.0)

CERTCC-KR

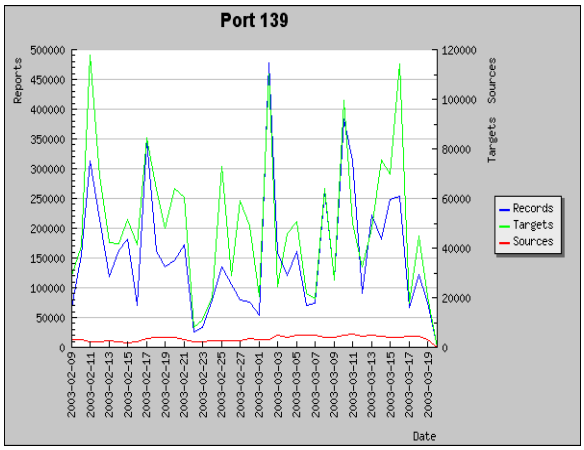
2003.04.23(수)

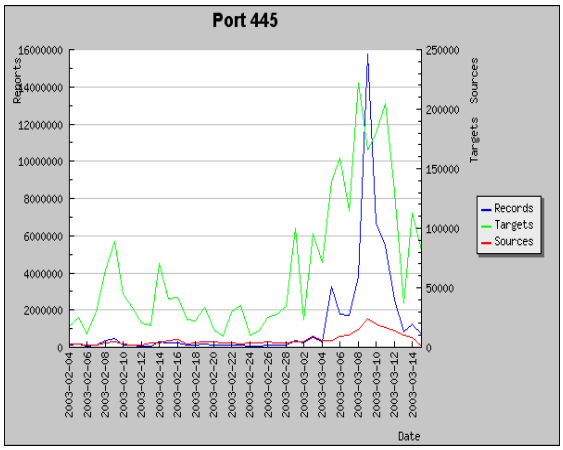
임명현 (mhlim@certcc.or.kr)
강준구 (jgkang@certcc.or.kr)
전완근 (wkjeon@certcc.or.kr)

- 차 례 -

1. 개요

1.25 대란 이후 국내 ISP를 집중적으로 모니터링 한 결과 2003년 3월 7일부터 14일 사이에 445포트의 트래픽이 증가하고 있다는 사실을 CERTCC-KR로 알려왔다. 동 시점에서 해외 트래픽을 모니터링한 결과, 공유폴더 취약점과 관련된 포트에 대한 트랙픽 또한 증가하고 있음이 확인되었다[1].





트래픽이 증가한 포트들에 대해 조사한 결과, 공유폴더 취약점과 관련된 포트들이라고 판단이 되었으며, 이에 사용자 및 관리자에게 공유 폴더 관련 취약점에 대해서 알려야 할 필요성을 느끼게 되었다. 또한, 사이버테러에 대하여 윈도우즈 사용자의 공유폴더 취약점과 관련된 포트들을 대상으로 brute-force 공격[2]과 인터넷 속도로 감소로 인한 일시적인 인터넷 마비 증상으로 이루어질 가능성이 높아, 이에 대한 공격 사례와 해결 방법에 대해서 논의하고자 한다. 본 문서에서 모든 공격방법에 대해서 논의할 수 없어, 대표적인 공격 방법에 대해서만 본 문서에서 다루고자 한다.

본 문서에서는 인터넷 환경의 개선과 함께, 개인 사용자들의 시스템을 보호할 목적으로 만들어졌으며, 국내에 이미 알려진 사례를 통하여 작성되었다. 일부는 CERTCC-KR에서의 자체 실험 결과를 토대로 작성되었다. 본 문서에서 언급한 내용 이외에도 수많은 공격기법과 취약점이 있지만, 일반 사용자 및 시스템 관리자가 꼭 알아두어야 할 내용과 대응방법에 대해서 언급하였다. 본 문서에서 다루어지지 않은 취약점 및 공격기법에 대해서는 CERTCC-KR 홈페이지[3]의 보안권고문을 참조하길 바란다.

---

1) http://isc.incidents.org/port_details.html?port=139
http://isc.incidents.org/port_details.html?port=445

2) 일명 패스워드의 사전(dictionary)공격이라고도 한다.

2. 공유폴더와 관련된 포트의 이해

공유폴더 취약점으로 이용되고 있는 NetBIOS와 관련된 포트와 윈도우즈 XP/2000 시스템에서 파일과 프린터를 공유하기 위한 목적으로 사용되고 있는 SMB와 관련된 포트의 특징은 다음과 같다.

1) 137, 138, 139 포트와 관련된 서비스 : NetBIOS

NetBIOS(Network Basic Input/Output System)는 1983년 Sytek이 IBM을 위해 개발하였으며, 어플리케이션이 네트워크 상에서 통신을 할 수 있도록 한다. NetBIOS는 세션 레벨 인터페이스와 세션 관리/데이터 트랜스포트 프로토콜로 정의된다. NetBIOS 인터페이스는 사용자 어플리케이션이 네트워크 I/O를 사용하고 기반 네트워크 프로토콜을 제어하기 위한 표준 API이다.

NetBIOS는 BIOS가 의미하듯이 네트워크 상의 기본 입출력 시스템을 의미한다. NetBIOS가 TCP/IP나 UDP/IP 전송에 사용된다면 이를 NetBIOS over TCP/IP[4] 또는 NetBIOS over UDP/IP라고 한다. NetBIOS는 TCP/IP나 UDP/IP 보다 상위계층인 세션계층에 위치하며, 이름부여 서비스, 데이터그램 서비스, 세션 서비스, 일반 명령어 서비스를 제공한다. NetBIOS에서 제공하는 기본 서비스와 이와 관련된 포트는 다음과 같다.

NetBIOS에서 제공하는 기본 서비스 및 관련 포트 정보

포트번호	Protocol	Service 명	설명
137	TCP	NetBIOS 이름 관리	네트워크 상의 자원(PC, 응용어플리케이션 등)을 식별하기 위해 사용됨
138	UDP	NetBIOS 데이터그램	호스트, 그룹 또는 LAN 전체로 브로드캐스팅하는데 사용됨
139	TCP	NetBIOS 세션	네트워크 공유 등을 이용한 실제 데이터를 송수신하는데 사용됨

2) 445 포트와 관련된 서비스 : SMB[5]

1980년 초에 Intel, Microsoft, IBM에서 공동으로 개발한 SMB는 파일, 프린터, 비동기식

3) http://www.certcc.or.kr

4) NetBIOS over TCP/IP(NBT) : NetBIOS 응용을 TCP/IP상에서 동작시키기 위해 필요한 통신 규약. TCP/IP를 사용해서 NetBIOS명을 조사하는 단계와 NetBIOS 세션을 확립하는 단계로 구성된다.

5) SMB : 서버 메시지 블록, Server Message Block

포트를 공유하기 위해, 그리고 명명된 파이프 및 메일 슬롯을 이용하는 컴퓨터들 간의 통신을 위해 Microsoft가 이용하는 프로토콜이다.

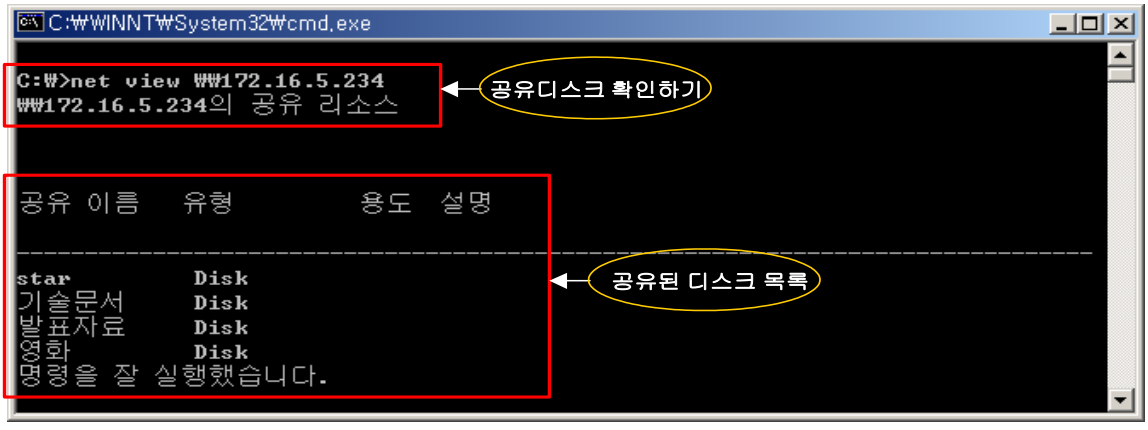
445 포트 정보			
Protocol		Service 명	설명
1	TCP	microsoft-ds	Win2k+ SMB
2	UDP	microsoft-ds	Win2k+ SMB

3. 공유폴더 취약점을 이용한 공격 유형 및 취약점 해결 방법

1) NetBIOS 취약점을 이용한 공격 및 취약점 해결 방법

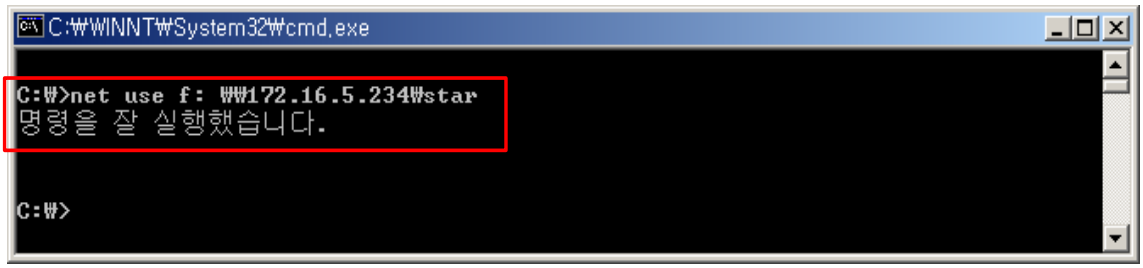
공인 IP Address를 가진 사용자가 윈도우즈 시스템에 "Microsoft 파일/프린터 공유프로그램" 서비스가 등록되어져 있다면 임의의 사용자가 해킹 툴이 아닌 NetBIOS over TCP/IP 기능을 이용하여 원격 PC의 공유된 디스크나 폴더(Directory)로 접근하여 파일을 복사하거나 지우는 등의 해킹 행위로 인하여 선의의 사용자 즉, 정상적인 인터넷 사용자들에게 공유된 디스크와 폴더를 공격함에 따라 네트워크에 과부가 발생하여 정상적인 인터넷 사용에게 피해를 주게 된다. 아래의 방법은 자신의 컴퓨터가 TCP/IP 상에 노출되어 있는지를 검사해주는 반면 공유폴더에 암호가 Null 패스워드로 되어 있거나 공격자가 추측하기 쉬운 암호로 지정되어 있다면 공격 대상이 될 수 있다.

가) 공유된 디스크 목록 확인하기

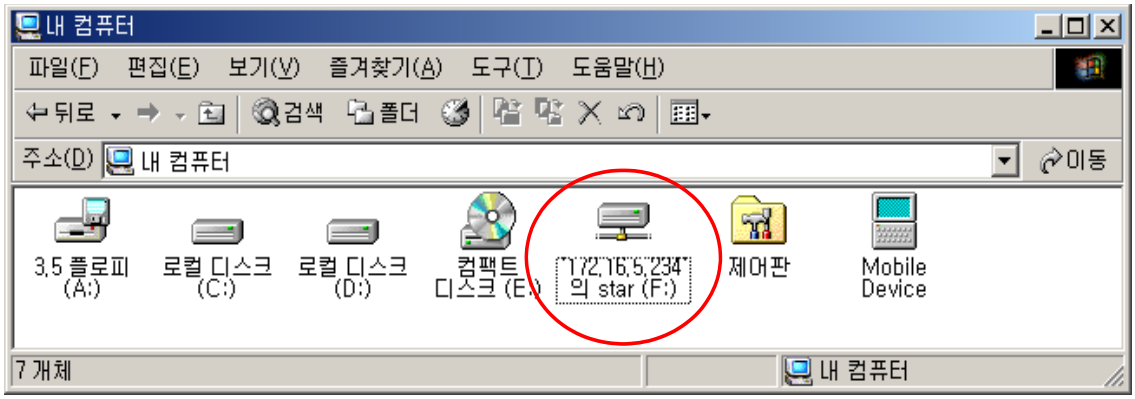


위의 그램에서와 같이 "net view" 명령으로 상대방의 컴퓨터에 공유된 폴더가 있는지를 확인할 수 있다.

나) 공유된 디스크 및 폴더(Diredtory) 네트워크 드라이브로 연결 및 확인하기



"net view"명령으로 디스크가 공유되었는지를 확인한 다음, 위의 그림에서와 같이 "net use"명령을 사용하여 디스크를 지정하여 상대방의 IP와 폴더를 지정하게 되면 네트워크 드라이브가 아래 그림에서와 같이 연결되었음을 확인할 수 있다.



다) NetBIOS 취약점 해결 방법

A. 네트워크 관리자에 의한 라우터에서의 접근 통제 방법

외부에서의 내부로의 모든 NetBIOS 트래픽을 차단하기 위한 방법으로 아래와 같이 라우터에 ACL을 설정한다.

```
RouterA#config terminal

RouterA(config)#access-list 101 deny udp any host HOST_IP eq 135
RouterA(config)#access-list 101 deny udp any host HOST_IP eq 137
RouterA(config)#access-list 101 deny udp any host HOST_IP eq 138
RouterA(config)#access-list 101 deny udp any host HOST_IP eq 139

RouterA(config-if)#ip accesss-group 101 in
```

※ 다음과 같은 설정으로 인해 특정 서비스에 문제가 되는지를 확인한 후에 정책을 세우시기 바랍니다.

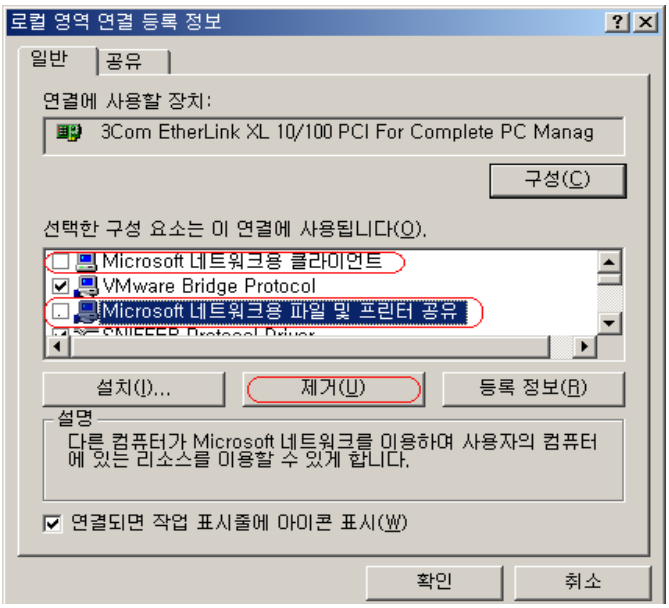
B. 개인 서버 상에서의 접근 통제 방법

윈도우즈 시스템 서버에서는 기본적으로 IP와 포트를 필터링하는 기능을 제공하고 있다. 대표적인 방법이 IPSEC를 이용하여 특정 IP와 트래픽을 제어하는 방법이다. "시작 → 프로그램 → 관리도구 → 로컬보안정책"을 실행하여 로컬 보안 정책을 설정한다. 자세한 설정방법은 아래의 사이트를 통해 참고하길 바란다.

※ http://www.ntfaq.co.kr/download/ipsec-filter.pdf [6]

C. 개인 PC상에서의 취약점 해결 방법

아래 그림에 나타난 **"Microsoft 네트워크용 클라이언트"**와 **"Microsoft 네트워크용 파일 및 프린터 공유"**를 제거하거나 메뉴의 체크표시를 제거한다. 이를 통해 NetBIOS의 고질적인 문제로 인한 보안상의 문제는 해결된다.



※ 체크박스만 없애주시더라도 구성요소를 제거한 것과 동일한 효과가 발생한다.

그러나 꼭 NBNS[7]와 WINS[8] 서비스를 사용해야 한다면 Windows 2000에서 제공하는 IPSec 필터를 통해 UDP 137~139로 송수신되는 트래픽을 인증하도록 설정해 준다. 또한

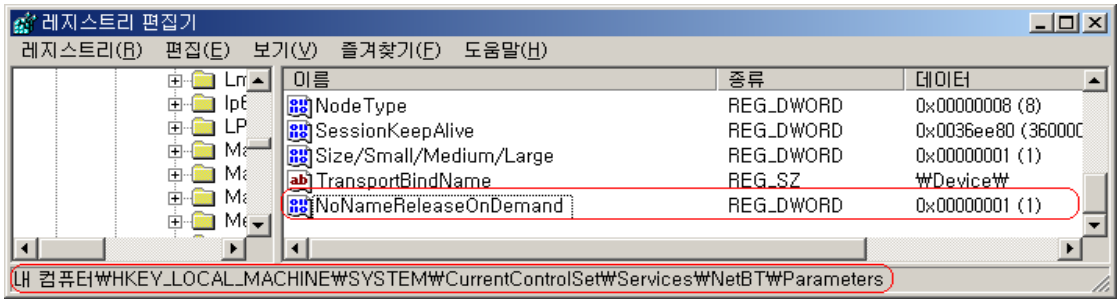
6) 파일을 다운받기 위해서는 회원가입을 요구한다.

7) NetBIOS Name Server : 3page "이름부여 서비스(Naming Service)" 참고

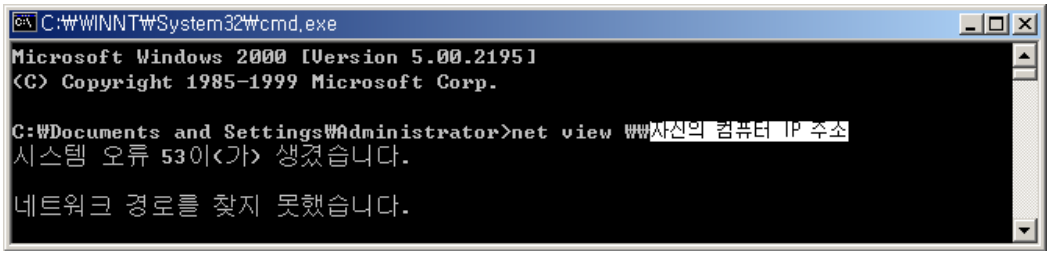
8) WINS(Windows internet Name Service)는 NetBIOS Name를 IP로 해주는 역할을 한다. 이 서비스는 NT4.0에 비하여 Windows 2000 환경에서는 그 역할 많이 줄어들었지만 여전히 필수적인 서비스 중에 하나이다.

호스트 레벨에서 다음과 같이 레지스트리 값을 새로 생성시키거나, 설정을 아래와 같이 바꾼다.

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ NetBT \ Parameters
NoNameReleaseOnDemand Reg_DWORD = 1



라) 취약점 해결 확인하기



위의 그림에서와 같이 "net view"명령을 통해 자신의 컴퓨터 IP를 주소를 입력함으로써 취약점이 해결되었는지를 검사할 수 있다.

2) SMB 취약점을 이용한 공격 및 취약점 해결 방법

가) SMB 취약점을 이용한 공격 방법

위의 방법을 통해 기본적으로 디스크와 폴더가 공유된 문제점에 대해서는 악의적인 행동에 대해서는 해결하였다. 그러나, 해킹 툴에 의한 공격에 대해서는 해결책이 되지 못한다. 그래서, 아래와 같이 공격 툴에 의한 문제점을 살펴보고, 해결방법에 대해서 알아보고자 한다.

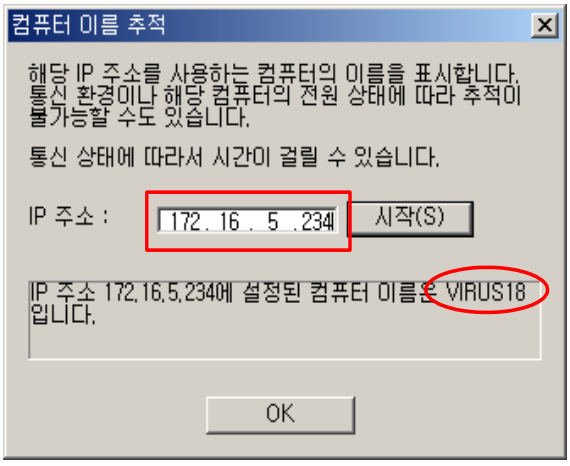
Microsoft Windows는 다른 컴퓨터와 파일과 프린트 자원을 공유하기 위한 목적으로

SMB 프로토콜을 사용한다. Windows의 오래된 버전(즉, 95, 98, Me, 그리고 NT)에서의 SMB 공유는 TCP 포트 137, 139와 UDP 포트 138에서 NetBIOS over TCP/IP를 통해 NetBIOS 상에서 실행된다. 그러나 Windows 2000/XP에서는 TCP 포트 445상에서 TCP/IP를 통해 직접 SMB 운영이 가능하다. 추측이 가능한 패스워드와 패스워드가 설정되지 않은 Windows 파일 공유는 네트워크를 통해 협동 작업을 하는 사용자와 가정 사용자에게 심각한 위협을 가져다 줄 수 있다. 보안에 대한 심각한 위험은 인터넷 환경에 노출된 상태에서 패스워드 유추가 쉽게 구성된 공유 환경에서 종종 일어날 수 있다. 침입자는 특수하게 작성한 패킷 요청을 전송함으로써, 목표로 삼는 서버 기기에 서비스 거부 공격을 일으키고 이를 통해 시스템을 중단시킬 수 있다. 침입자는 이를 위해 사용자 계정과 익명 액세스 모두를 이용할 수 있다.

공격 대상 시스템의 구성
O Windows XP 또는 2000 시스템 O 서비스 팩 1이 설치된 시스템 O NULL 패스워드

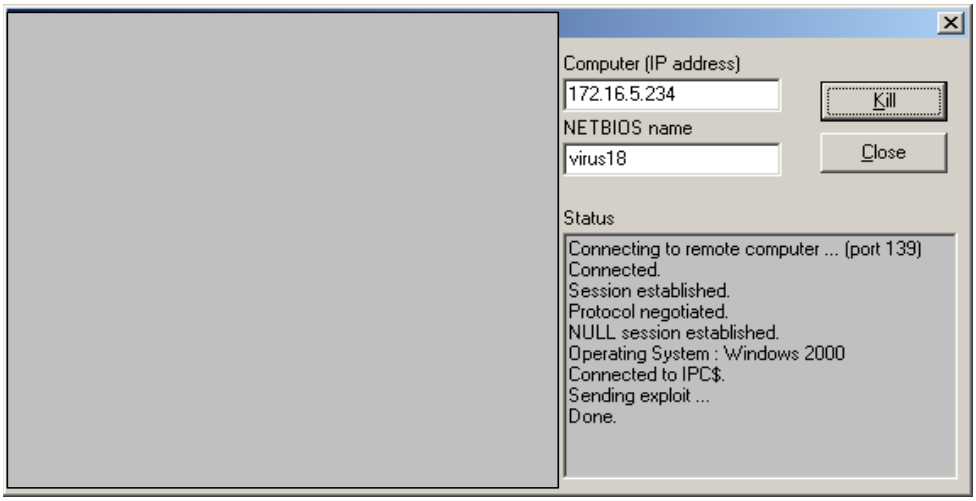
□ 1 단계 : NetBIOS 이름 알아내기

아래 그림에서와 같이 특정 프로그램을 통해 공격 대상 시스템의 NetBIOS 이름(즉, 컴퓨터 이름)을 알아내어야 한다.

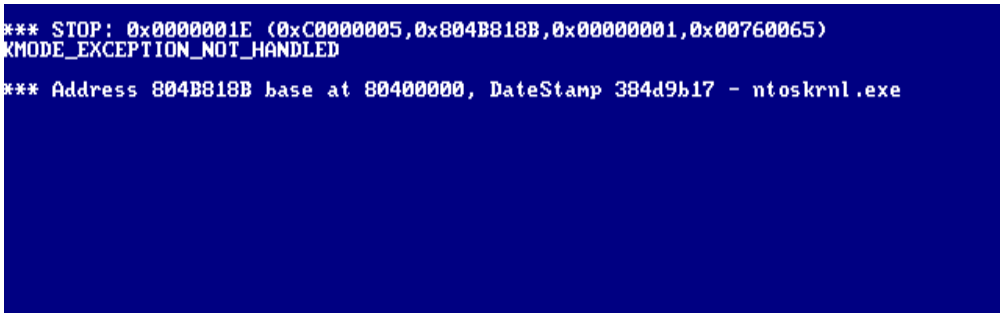


□ 2단계 : 공격도구를 이용한 공격

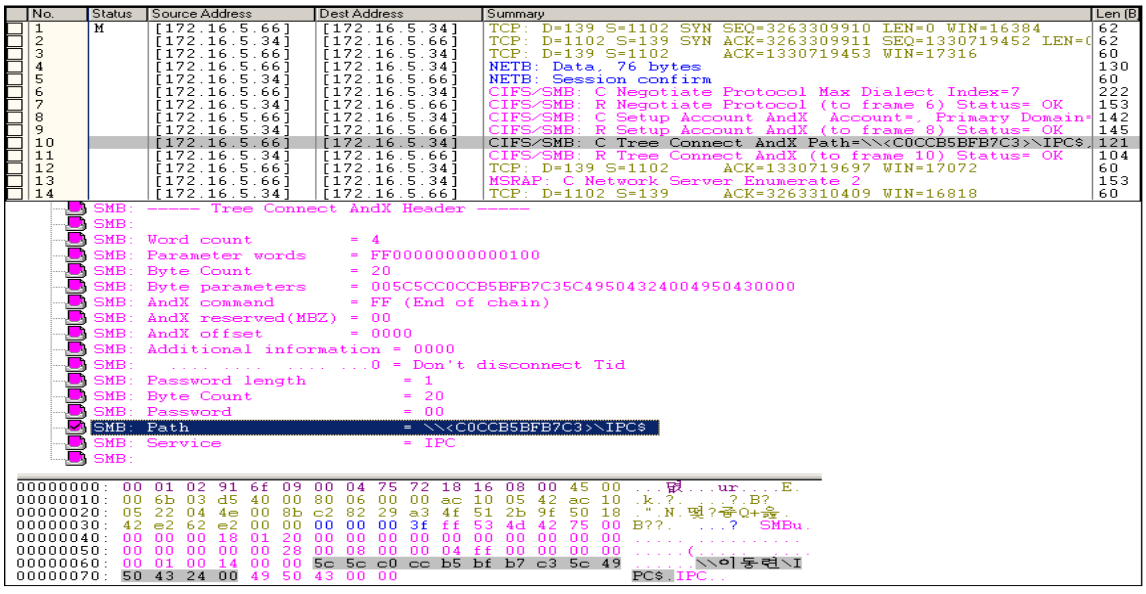
위의 1단계에서 알아낸 NetBIOS 명을 이용하여 2단계에서 IP 주소와 NetBIOS 명을 입력한 다음 "Kill" 버튼을 클릭하여 공격한다. 공격에 성공하면 3단계의 그림에서와 같이 공격 대상시스템이 블루스크린으로 바뀌면서 재부팅을 하게 된다.



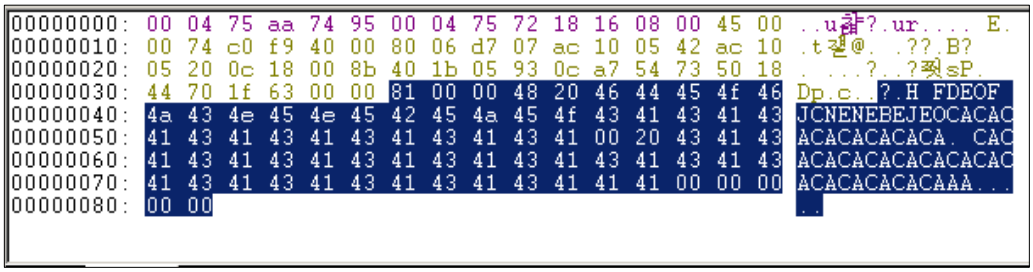
☐ 3단계 : SMB 취약점을 이용한 공격툴에 의한 시스템 다운



☐ 4단계 : 공격 코드 분석



네트워크 분석 툴을 이용하여 공격 패킷을 캡쳐해본 결과 76byte의 아래와 같은 데이터에 의해 원격 컴퓨터가 공격되었다는 것을 알 수 있었다.



2) 취약점 해결 방법

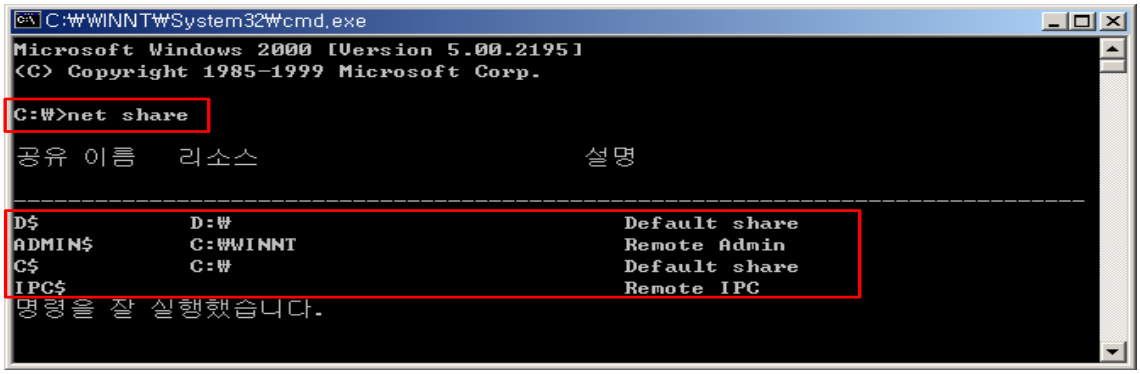
관리자는 신뢰하지 않는 네트워크가 SMB 포트에 액세스하는 것을 TCP 포트 445 및 139를 차단함으로써, 신뢰할 수 없는 집단에 의한 침입을 관리자 수준에서 방지할 수 있다. 그러나 이는 신뢰하지 않는 네트워크로부터의 액세스는 차단하나, 파일 및 프린트 네트워킹 환경에서 합법적인 사용자까지도 차단될 수 있기 때문에 관리자의 판단이 요구된다. 또한 Microsoft 사의 사이트를 통해 취약한 시스템에 대해서 패치를 해야 한다.

해당 시스템 패치 URL
- Microsoft Windows NT 4.0: http://www.microsoft.com/downloads/Release.asp?ReleaseID=41493 - Microsoft Windows NT 4.0 Terminal Server Edition: http://www.microsoft.com/downloads/Release.asp?ReleaseID=41519 - Microsoft Windows 2000: http://www.microsoft.com/downloads/Release.asp?ReleaseID=41468 - Microsoft Windows XP: http://www.microsoft.com/downloads/Release.asp?ReleaseID=41532 - Microsoft Windows XP 64 bit Edition: http://www.microsoft.com/downloads/Release.asp?ReleaseID=41549

패치 설치 확인
• 기기에 설치된 패치를 확인하려면, 다음의 등록키가 기기 상에 생성되어 있음을 확인한다. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\...\Q326830 • 개별 파일을 확인하려면, 다음의 레지스트리 키에서 제공된 날짜/시각 및 버전 정보를 이용한다. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\...\Q326830\Filelist

라) 취약점 해결 확인하기

아래 그림에서와 같이 "net share"명령을 통해서 자신의 컴퓨터에 공유된 폴더를 확인할 수 있지만, 공유 폴더에 대한 취약점을 해결하는 방법은 패치 사이트를 통해 자신의 컴퓨터를 패치하는 것이다. 시스템이 관리하는 C$, IPC$, ADMIN$ 등은 재부팅을 하게 되면 다시 공유되기 때문에 반드시 패치를 통해 업그레이드를 해야만 위와 같은 툴에 의한 공격을 예방할 수 있다.



3) 공유 폴더 취약점을 이용한 웜 · 바이러스

최근 공유 폴더 취약점을 이용한 웜 · 바이러스는 다음과 같다. 이와 같은 웜 · 바이러스를 살펴봄으로써 관리자와 사용자가 주의해할 사항이 무엇인지를 확인할 수 있을 것이다.

바이러스 명	특 징
Delorder	- 네트워크 공유를 통해 전파된다. - 바이러스에 감염되면 445 포트를 스캔하여 administrator 계정으로 접속을 시도한다. - 감염이 되면 원격에서 제어할 수 있는 백도어(5800 or 5900/TCP)를 열어놓고, 동시에 6667/TCP IRC Server에 접속을 시도한다.
LOVEGATE	- 메일 및 암호가 취약한 관리목적 공유폴더로(또한 읽기/쓰기 가능한 폴더 및 네트워크 드라이브 포함) 전파된다. - 20168 포트가 오픈된다.
Opaserv	- 네트워크 환경에서 C 드라이브가 읽기/쓰기 공유된 시스템 - - 137번 포트(NETBIOS Name Service)을 사용하여 동일 네트워크와 인접한 네트워크를 랜덤하게 검색한다.
Mircpack	- 윈도우 2000 시스템에서 'Administrator' 계정을 그대로 사용하고 암호를 설정하지 않거나 또는 누구나 알기 쉬운 계정 및 암호를 사용하는 시스템이
FunLove	- 특별한 파괴동작은 없으나 이 바이러스에 감염되면 시스템이 느려지는 특징이 있다. - 네트웍을 통하여 감염되기 때문에 감염속도가 매우 빠르며 특히 공유폴더를 사용하는 네트웍이 구성되어있는 기업체에 피해가 많다.
Netspree	- 윈도우 2000 의 IPC$ 공유된 시스템들을 대상으로 전파, 설치된다. - 연결 대상은 윈도우 2000 에 기본 ipc$ 공유(Microsoft-DS 서비스, TCP 445번 포트)를 이용한다. - 연결시 배치파일에 포함된 몇개의 계정 및 암호를 이용하여 연결된다.

이 외에도 무수히 많은 웜·바이러스가 있지만, 최근 발생했던 웜·바이러스들을 열거하였다. 위의 특징에서와 같이 목적이 공유폴더 취약점을 이용한 공격이라는 것을 파악할 수 있었을 것이다. 따라서, 특별한 목적으로 사용하지 않는 이상, 취약점을 패치하고, 문제가 되는 공유 폴더 설정을 변경해 주어야 할 것이다. 이에 아래와 같이 좀더 상세한 정보와 해결책을 나열하였다.

위의 웜·바이러스에 대한 해결책은 CERTCC-KR 홈페이지 및 각 백신업체의 홈페이지에 게시되어 있다. 이를 참조하여 취약성에 대한 해결을 해야 할 것이다. 다음은 위의 웜·바이러스에 대한 해결책을 제시한 URL들이다.

바이러스 명	해결책 참고 URL
Delorder	- http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DELODER.A - http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.deloder.html
LOVEGATE	- http://www.certcc.or.kr/cvirc/Alert/warning/2003/WORM_LOVGATE_F.html - http://home.ahnlab.com/smart2u/virus_detail_1135.html - http://www.hauri.co.kr/virus/vir_read.html?code=IWW3000384 - http://vil.nai.com/vil/content/v_100183.htm - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_LOVGATE.F
Opaserv	- http://www.certcc.or.kr/cvirc/Alert/2002/W32_Opaserv_Worm.html - http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.html - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_OPASOFT.A - http://hauri.co.kr/virus/vir_info_detail.html?uid=350 - http://home.ahnlab.com/smart2u/virus_detail_1033.html
Mircpack	- http://www.certcc.or.kr/cvirc/Alert/2003/Win_Trojan.html - http://home.ahnlab.com/smart2u/virus_detail_1066.html - http://hauri.co.kr/virus/vir_read.html?code=TRW3000348
FunLove	- http://home.ahnlab.com/smart2u/virus_detail_710.html - http://www.hauri.co.kr/virus/vir_read.html?code=VRW3000044
Netspree	- http://www.certcc.or.kr/cvirc/Alert/2003/Win32_Netspree.html - http://home.ahnlab.com/smart2u/virus_detail_1093.html - http://www.sophos.com/virusinfo/analyses/w32netspreea.html

앞으로도 위와 비슷한 특성을 가진 바이러스가 기승을 부릴 것이다. 따라서 관리자나 개인 사용자들은 백신업체 및 CERTCC-KR 홈페이지를 통해 관심을 가지고 해킹·바이러스 대응에 앞장서야 할 것이다.

4. 결론

윈도우즈 환경에서 공유 폴더에 대한 취약점으로 인한 피해가 확산되고 있다. 이는 개인 한 사람으로 국한되는 것이 아니라, 인터넷을 사용하는 사람이라면 누구든지 피해를 볼 수 있다는 점에 그 심각성이 한층 더해지고 있다. 예전에는 그 확산 정도나 피해정도가 한 개인의 PC에 피해를 줌으로써 문제의 심각성을 쉽게 인지하였고, 이에 대한 대책을 스스로 해결하였다. 그러나 현재 발생되고 문제는 한 개인의 문제가 인터넷 망을 사용하고 있는 전체에 영향을 미칠 뿐만 아니라, 국가 전체에 영향을 미친다는 점과 개인 사용자는 자신의 시스템의 피해 사실은 인지 못하고 인터넷 망에만 문제가 있다고 생각한다는 점이 더 문제점으로 대두되고 있다.

공유폴더 취약점으로 인해 웜·바이러스가 유포되거나 자신이 시스템이 다른 사용자에게 노출되어 해킹이 이루어진다면, 다음과 같이 인터넷 환경에 영향을 미칠 수 있다.

- 외부에서 전용회선을 통하여 자신의 컴퓨터와 네트워크를 연결하여 파일이나 폴더(디렉토리)를 복사할 경우, 상대적으로 작은 회선을 사용하는 경우 심각한 속도저하 현상을 가져올 수 있다.
- 취약점을 이용해서 개인 정보가 유출 당할 수 있으며, 개인의 시스템에 심각한 피해를 줄 수 있다.
- 취약점을 통해 개인의 PC에 트로이잔을 심어놓고, ID와 패스워드를 가로챌 수 있으며, 원격에서 조정을 당할 수도 있다.
- 바이러스 확산의 근원지가 될 수 있으며, 바이러스에 감염될 위험 높다.

위의 문제점을 해결하기 위해서는 지속적인 패치가 이루어져야 할 것이며, 백신을 이용한 시스템 점검이 필수적으로 뒤따라야 할 것이다. 우리나라 인터넷 사용자 수의 양적인 증가와 더불어 사용자 개개인의 보안 의식과 인터넷 사용에 대한 질적인 향상도 더불어 이루어져야 할 것이다.

5. 참고사이트

1) http://www.microsoft.com/korea
2) http://www.wins21.com
3) http://www.ebora.co.kr
4) http://cncpc.co.kr
5) http://terms.co.kr