

아이티이지 서비스 운영팀

# [Windows Server 보안 설정 5가지 팁 ]





# - 목 차 -

1. 서버에서 실행되는 서비스 확인
 2. 원격 접속 터미널(RDP) 보안 설정
 3. 사용자 계정보안
 4. Windows 방화벽 설정
 5. 메모리 덤프 분석

#### ⇔ 문서 작성간에 테스트된 환경

- Windows 2003 R2 Stendard 32bit / Windows 2008 R2 Enterprise 64bit

유 **개요** 

- 최근 게임 사이트, 포털 사이트 등 개인정보 유출사고가 빈번하게 일어나는 것을 알 수 있습니
   다. 이와 같은 보안사고는 주요 사이트뿐만 아니라 네트워크가 연결된 모든 서버는 공격 대상
   이 될 수 있습니다. 서버 보안에 각별한 관심이 필요합니다.
- 해당 문서는 OS 상에서 설정 가능한 보안 설정에 대한 내용을 기술하고 있으며, 서버 관리자 분들께서 서버 운영에 참고해 주시기 바랍니다.



#### 1. 서버에서 실행되는 서비스 확인

- 서버에서 실행되는 서비스를 확인하고, 사용하지 않는 서비스는 사용하지 않는 것이 좋습니다.
   서버 자원 소모뿐만 아니라, 사용하지 않는 서비스들을 통해 해킹의 위협에 노출될 수 있기 때 문입니다.
  - ① 서비스 확인

: 아래 명령어를 통해 현재 서버에 Open 되어 있는 Port 확인

시작 > 모든 프로그램 > 보조 프로그램 > 명령 프롬프트 실행



#### 또는

시작 > cmd [엔터]

※ Windows 2003 server 의 경우, 시작 > 실행 > cmd [엔터]



c:₩> netstat -nao

관리자: C:₩₩indows₩system32₩cmd,exe					
Microso Copyrig	ft Windows [Version 6.1 ht (c) 2009 Microsoft C	.7601] orporation. All rights	reserved.		
C:WUser	s\Administrator>netstat	-nao Imore			
활성 연	2				
프로	토콜 로컬 주소	외부 주소	상태	PID	
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING	1400	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	936	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	1728	
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING	1572	
TCP	0.0.0.0:2383	0.0.0.0:0	LISTENING	1760	
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	3044	
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	664	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	192	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	228	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	760	
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	752	
TCP	121.124.127.14:139	0.0.0.0:0	LISTENING	4	
TCP	121.124.127.14:3389	58.74.138.139:51035	<b>ESTABLISHED</b>	3044	
TCP	127.0.0.1:1434	0.0.0.0:0	LISTENING	1728	
TCP	169.254.95.120:139	0.0.0.0:0	LISTENING	4	
TCP	[::]:21	[::]:0	LISTENING	1400	
TCP	[::]:80	[::]:0	LISTENING	4	

※ Open 되어있는 포트가 많을 경우, more를 이용하여 한 페이지씩 출력하여 볼 수 있 습니다.

예시) c:₩> netstat -nao | more

### ※ 서비스 별 포트 목록

서비스명	기본 포트	서비스명	기본 포트
FTP	21	IMAP	143
SSH	22	MMS	554
TELNET	23	MSSQL	1433
SMTP	25 / 587	ORACLE	1521
DNS	53	MYSQL	3306
HTTP	80	RDP	3389
POP3	110	TOMCAT	8080
HTTPS	443		

② 부팅시 불필요 서비스 실행 방지

: 사용하지 않는 서비스가 있으실 경우, 서버가 부팅될 때 실행되지 않도록 하는 것이 좋습니다.

시작 > 모든 프로그램 > 관리 도구 > 서비스



🔍 서비스							
파일(F) 동작(A)	보기(V) 도움말(H)						
	» 🛛 🖬 🕨 🕨 💷 🕕 🕨						
🔍 서비스(로컬)	😋 서비스(로컬)	y a					
	설명이 필요한 항목을 선택하십시오.	OIE       Application Exp         Application Host       Application Host         Application Identity       Application Identity         Application Laye       Application Laye         Application Man       Application Man         Application Man       Application Man         Application Man       Application Man         Application Man       Application Man         Application Man       Background Intel         Background Intel       Background Intel	설명 응용 IIS 응용 추가 인터 그룹 ASP 유휴 BFF	상태 시작됨 시작됨	시작 유형 수동 자동 수동 수동 수동 수동 수동 수동 우동 우동 우동 우동	다음 사용자로 로그온 Local System Local System Local Service Local System Local Service Local System Network Service Local System Local System	



예시) snmp 서비스 중지

N/ 01/0/							
	Q 🛃 🛛 📰 🕨 🔳 II ID						
(비스(로컬)	😋 서비스(로컬)						
	SNMP Service 서비스 중지 서비스 너지 시작 여명: 이 컴퓨터에서 SNMP(Simple Network Management Protocol) 요 경을 처리할 수 있도록 합니다. 이 서 비스를 중지하면 이 컴퓨터에서 SNMP 요청을 처리할 수 있는다. 이 서비스를 사용하지 않도록 설정하 면 관련된 모든 서비스는 사용할 수 없습니다.	OI를 수 Server Shell Hardware Detection Smart Card Smart Card Removal Policy SMTP(Simple Mail Transfer Protocol) SMTP(Service StMMP: Trap Software Protection Software P	<u>실명</u> 이 자동 스마 네트 먼데 로칩 관리 소프 데이 자업 비즈 글라 구조 구조	<u>상태</u> 시작됨 시작됨 시작됨 시작됨 시작됨 시작됨 시작됨	시작 유형 자동 자동 자동 수동 수동 수동 자동(지연 수동 수동 자동(지연 수동 사용 안 합 자동 자용 안 합 자동 자용 안 합 자동	LF음 사용자료 로그온 Local System Local System Local System Local System Local System Local System Local System Local System Local System Network Service Local System Network Service Local System Local System Local System Local System Local System Local System	
		SOL Server Integr 도움말(H)     SOL Server VSS 'mmer     System Event Notification Service     Task Scheduler     TCP/IP NetBIOS Helper     Telephony     Thread Ordering Server     TPM Base Services     UPNP Device Host	SSI Win 시스 사용 Ret 특정 시스 이	시작됨 시작됨 시작됨 시작됨 시작됨	사용 자동 사용 안 함 자동 자동 자동 수동 수동 수동 수동 사용 안 함	Network Service Local System Local System Local System Local System Local Service Network Service Local Service Local Service	

# 서비스 > snmp services [마우스 우클릭] > 속성

## Snmp 서비스 속성 > 일반 > 시작 유형 > "사용 안 함"으로 변경

IMP Service ∉	성(로컬 컴퓨터)				
일반  로그온	복구  에이전트 트랩  보안  종속성				
서비스 이름:	SNMP				
표시 이름:	SNMP Service				
설명: DI 컴퓨터에서 SNMP(Simple Network Management - Protocol) 요청을 처리할 수 있도록 합니다. 이 서비스 -					
실행 파일 경로: C:₩Windows₩	System32₩snmp.exe				
시작 유형(E):	사용 안 함 🔽				
<u>서비스 시작 옵션</u>	<u>1 구성 도움말</u>				
서비스 상태:	시작됨				
시작(S)	중지(T) 입시 중지(P) 계속(R)				
서비스를 시작할	때 적용할 시작 매개 변수를 지정할 수 있습니다.				
지곡 배개 번수()	YU) -				
	화이 최소 적용(A)				



③ 서비스 종료

: 사용하지 않는 프로그램 종료

서비스 > [서비스 명] > 중지

# 예시) 서비스 > snmp services > 중지

🔕 서비스							_ 🗆 🗙
파일(F) 동작(A)	보기(V) 도움말(H)						
	🗟 😼   🛛 📷   🕨 🔳 🕕 🕪						2
🔍 서비스(로컬)	😋 서비스(로컬)	9.					
	SNMP Service	. 이름 🔺	설명	상태	시작 유형	다음 사용자로 로그온	
		🚳 Server	01	시작됨	자동	Local System	
	시비슷 중지 내지?	🖏 Shell Hardware Detection	자동	시작됨	자동	Local System	
		🖏 Smart Card	컴퓨		수동	Local Service	
		🖏 Smart Card Removal Policy	스마		수동	Local System	
	설명: 이 커프터에서 SNMP(Simple	SMTP(Simple Mail Transfer Protocol)	네트		수동	Local System	_
	Network Management Protocol) &	SNMP Service	0	시작됨	사용 안 함	Local System	
	경출 저리할 수 있도록 합니다. 이 서    비스를 중지하면 이 컴퓨터에서	SNMP Trap	로컬		수동	Local Service	





[TIP] 시스템 성능 부하 및 리소스 모니터링

작업 창 [마우스 우클릭] >작업관리자 시작

	도구 모음(T)	۲
	계단식 창 배열(D) 창 가로 정렬 보기(H) 창 세로 정렬 보기(I) <b>바탕 화면 보기(S)</b>	
	작업 관리자 시작(K)	
	작업 표시줄 잠금(L)	

Windows 작업 관리자 > 성능



Windows 작업관리자 > 성능 > 리소스 모니터

🚳리소스 모나티								
파일(F) 모니터(M) 도움말	r(H)							
개요 CPU 메모리 다	스코   네트	워크						
CPU	1% CPU /	사용량		📑 63% 최대 사	용 빈도	<u>م</u>	•	보기 🖌 📤
	PID	설명	상	스레드	CPU	평균 C 🔺	CPU	100% ¬
perfmon,exe	4028	리소스	실행 중	18	0	0,50		
🔲 🗖 svchost,exe(LocalServic,	1224	Host Pr	실행 중	17	0	0,12		
🔲 🗖 svchost,exe(DcomLaunch	h) 860	Host Pr	실행 중	§ 11	0	0,06		
Isass,exe	760	Local S	실행 중	5 7	0	0,02		
svchost,exe(RPCSS)	936	Host Pr	실행 중	8	0	0,02		
System Interrupts	1 <del>2</del> 1222-221	지연된	실행 중	12	0	0,02		
explorer,exe	3788	Windo	실행 술	≩ 16	0	0,02	60초	0% -
System	4	NT Ker	일행 물	225	0	0,00	니스크	IKB/조 ]
Smss,exe	332	WINDO	일행 물	3	U	0,00		
	DID	Client	58.5	; 9	U	0,00 💌		
디스크 🔳	0B/초 디스	:∃ I/0		📕 0% 최고 활성	시간	•		
네트워크 📕	51Kbps U	I트워크 I/O		📕 0% 네트워크	이용률	•		
메모리	0페이지	률트/초		📕 11% 사용된 :	실제 메모리	-	네트워크	1Mbps
<u>.</u>								
							M	
						-		



#### 2. 원격 터미널 접속(RDP) 보안

- RDP(Remote Desktop Protocol) 이란, 마이크로소프트 (Microsoft)에서 Windows NT와 Windows CE가 서로 통신하기 위해 만든 프로토콜 입니다.
  - ① 원격 터미널 포트 변경

: 기본적인 원격 터미널 포트는 3389이지만, 반드시 해당 포트를 사용할 필요는 없습니
 다. 기본 포트로 무차별 대입법 등을 통해 접속 시도가 발생할 수 있기 때문에 포트를
 변경하여 임의 포트로 변경하여, 포트 노출을 예방하는 것이 좋습니다.

: 레지스트리 파일을 변경하는 부분으로 설정 후, 시스템을 재부팅 해야 만 적용됩니다.

#### < Windows Server 2003 >

시작 > 실행 > regedit

실형			?)>
	프로그램, 폴더, 문서, 또	또는 인터넷 리소스 (	이름을 입력하십시오.
열기( <u>0</u> ):	regedit		•
		÷1.1	



레지스트리 편집기에서 아래 경로의 PortNumber값을 3389에서 임의 값을 변경합니다. Windows 2003 Server에서는 두 개의 레지스트리 값을 변경하셔야 합니다.





HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp



## PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.

DWORD 값 편집		? ×
값 이름( <u>N</u> ):  PortNumber		
값데이터(⊻): [1234]	단위 C 16진수( <u>H</u> ) ⓒ 10진수( <u>D</u> )	
	확인	취소



HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

IDE         IDE         SR         IDE           IDE         IDE         SR         IDE           IDE         INTERCE         IDE         IDE           IDE         INTERCE         IDE         SR           IDE         INTERCE         IDE         IDE           IDE         INTERCE         IDE         SR           IDE         INTERCE         IDE         IDE           IDE         SAM         IDE         IDE         IDE           IDE         SECURITY         IDE         IDE         IDE           IDE         SECURITY         IDE         IDE         IDE           IDE         SECURITY
□ = □ + 12 + 12 + 12 + 12 + 12 + 12 + 12 +
□         □
Image: International of the second of the
Image: Instant Cutrine Vision         Im
1         I
Bit And WARE          am the connects are REG_DWORD          bx0000000 (0) connects are REG_DWORD         connects are REG_DWORD
Section Sectio
SOETWARE WITCH WITCH IN THE CONTRACT OF CO
B SVOTEM BEG_SZ
ControlScr001     WinputBufferLen REG_DWORD 0x00000800 (2048)
Control Section Will Interactive Delay REG_DWORD 0x0000032 (50)
ConceptControlSet
Big KeyboardLayout REG_DWORD 0x0000000 (0)
4 GAP BEG_DWORD 0x0000000 (0)
Athiters BEG_DWORD 0x0000000 (0)
MaxDisconne,, REG_DWORD 0x0000000 (0)
생략 0x9 6 0x0000000 (0)
Setup @#MaxInstanceC.,, REG_DWORD 0xfffffff (4294967295)
E Stillmage I MinEncryption, REG_DWORD 0x000002 (2)
SystemResources III NWLogonServer REG_SZ
5 chain Terminal Server I I III OutBufCount REG_DWORD 0x0000006 (6)
B Addins BEG_DWORD 0x0000064 (100)
- Authorized Applications REG_DWORD 0x0000212 (530)
Control Configuration Configuration Configuration Control Cont
Dos BEG_DWORD 0x0000002 (2)
InputDevices     ImputDevices     ImputDevices     ImputDevices     ImputDevices     ImputDevices
E Keyboard Type Mapping     Windows BEG_DWORD     Dx000004e (78)
Licensing Core
SysProcs BEG DWORD Dx00000134 (3389)
B Utilities BEG DWORD Decomposition
TraceEnable BEG DWORD DV0000000 (0)
Contraction in the second seco
- Indate Withama BEG S7 Microsoft BD 52
Production and the second seco
B Video
VirtualDeviceDrivers
Watchdog BEG S7 rdpusy

PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.

D₩ORD 값 편집	? ×
값 이름( <u>N</u> ):  PortNumber	
값데이터(⊻): [1234]	단위 C 16진수( <u>H</u> ) C 10진수( <u>D</u> )
	확인 취소



## **iTEASY**

#### < Windows Server 2008 >

시작 > regedit

regedit			$\mathbf{x}$	로그오프	•
시작	4	$\mathbf{\Sigma}$			

레지스트리 편집기에서 아래 경로의 PortNumber 값을 3389에서 임의 값으로 변경합니다.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp



PortNumber 의 단위를 10진수로 변경한 뒤 임의 값으로 지정합니다.

값 이름( <u>N</u> ):	
PortNumber	
값데이터( <u>V</u> ): [1234]	단위 C 16진수( <u>H</u> ) C 10진수( <u>D</u> )
	 확인 취소

iTEASY

원격 터미널 접속 포트를 임의 값으로 변경하셨을 경우, PC에서 원격 접속 시 아래와 같이 IP 뒤에 임의 포트를 지정하여 연결하셔야 합니다.

예시) 111.111.111.111:1234

😼 원격 데스크톱 연결	
원격 데스크톱 연결	
컴퓨터( <u>C</u> ): 사용자 이름: 지정 안 함 연결할 때 자격 증명을 묻는 메시지가 나티	▼
중 옵션(0)	연결( <u>N</u> ) 도움말( <u>H</u> )

[TIP 레지스트리 백업]

레지스트리 편집기 > 파일 > 내보내기

비지스트리 편집기		
일(F) 편집(E) 보기(V) 즐겨찾기( 가져오기(I) 내보내기(E)	A) 도움말(H)	이름
하이브 로드(L) 하이브 언로드(U)		
<b>네트워크 레지스트리 연결(C)</b> 네트워크 레지스트리 연결 끊기(D)		
인쇄(P)	Ctrl+P	
끝내기(X)		





레지스트리를 백업할 경로 및 파일 명을 지정한 뒤 저장 버튼을 클릭합니다.

AHyper-V Hyper-V SQL Server Management Visual Studio 2005	√ 436 2011- Studio 2011- 2011-	한 날짜   √ 유형 -05-18 오후 파일 -12-15 오후 파일 -12-15 오후 파일	형 <u>↓</u> 발 폴더 발 폴더 발 폴더
이름(N): full_backu	ip		저장(S)
형식(T): 등록 파일	(*,reg)	•	취소
	01름(N): <mark>full_backu</mark> 형식(T): 등록 파일	미름(N): <mark>full_backup </mark> 형식(T): [등록 파일 (*,reg)	이름(N): <mark>full_backup  ▼</mark> 형식(T): 등록 파일 (*,reg) ▼

※ 레지스트리 복구는 반대로 백업된 파일을 "가져오기" 하시면 되십니다.

💣 레지스트리 편집기	
파일(F) 편집(E) 보기(V)	즐겨찾기(A) 도움말(H)
가져오기(I)	
내보내기(E),	
하이브 로드(L) 하이브 언로드(U)	
네트워크 레지스트리 연결(C 네트워크 레지스트리 연결 끊	<b>)</b> 97(D),
인쇄(P)	Ctrl+P
끝내기(X)	

※ 레지스트리 변경 작업의 경우, 잘못 편집 시 시스템에 심각한 손상을 줄 수 있이 때문 에 작업 전 <u>반드시</u> <u>백업</u>을 하셔야 하십니다.

※ 변경된 설정을 적용시키기 위해서는 시스템을 재시작을 하셔야 적용됩니다.

※ 서버 방화벽에서 변경한 임의 포트를 등록하셔야 방화벽에서 차단되지 않습니다.

※ 위 예시의 임의 Port 1234는 임의 값으로 절대 똑같이 설정하시지 마시기 바랍니다.



#### 3. 사용자 계정 보안 설정

- Server 에서는 관리자 계정, FTP 접속을 위한 일반 사용자 계정 등 편의에 따라 각기 계정을 생성하여 사용하게 됩니다. 이렇게 생성한 사용자 계정들에 대한 기본적인 보안 설정을 하지 않을 경우 무차별적인 패스워드 대입 등을 통해 시스템으로 접근할 수 있습니다.
- 또, 일반 사용자 계정이 해킹 등으로 인해 불법적인 접속이 되었다 하더라도 시스템 파일로 접
   속할 수 없도록 해야만 더 큰 피해를 방지할 수 있습니다.
  - Administrator 계정 명 변경
     : Windows에서 기본적으로 제공되는 관리자 계정 명은 "administrator" 입니다. 이 계정 기본적으로 제공되는 계정으로 해당 계정에 패스워드를 계속 대입시키게 되면 아무리 복잡도가 높은 패스워드로 설정하셔도 침해사고가 발생할 수 있습니다.

시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책

		<ul> <li>▶ 원격 데스크톱 서비스</li> <li>▶</li> <li>▶</li> <li>₩yper-V 관리자</li> <li>♥</li> <li< th=""></li<></ul>
명령 프롬프트	- Charles	🛞 Windows Server 백업 🝙 Windows 메모리 진단
🏹 IIS(인터넷 정보 서비스) 관리자		💣 고급 보안이 포함된 Windows 방화벽 📆 공유 및 저장소 관리
lnternet Explorer	Administrator	🍬 구성 요소 서비스 🚍 데이터 원본(ODBC)
🧳 메모장 🔸	문서	🔒 로컬 보안 정책 🗟 보안 구성 마법사
🔒 로컬 보안 정책	컴퓨터	·····································
A SETP	네트워크 	<ul> <li>◎ 성능 모니터</li> </ul>
FileZilla	제어판	시스템 구성 圖 이벤트 뷰어
비S(인터넷 정보 서비스) 6.0 관	장치 및 프린터	④ 작업 스케줄러 ☞ 저장소 탐색기
	관리 도구 🔹 🕨	🌆 컴퓨터 관리
() 성능 모니터	도움말 및 지원	
iscsi 초기자	실행	
▶ 모든 프로그램	Windows 보안	
프로그램 및 파일 검색	로그오프 🕨	
🍂 🗸 🕌		

### ITEASY

로컬 보안 정책 > 로컬 보안 정책 > 보안 옵션 > 계정 : Administrator 계정 이름 바꾸 기 > [마우스 우클릭] > 속성



계정 : Administrator 계정 이름 바꾸기 속성 > administrator 부분을 임의 계정으로 변경

계정: Administrator 계정 이름 바꾸기 속성	? ×
로컬 보안 설정   설명	
계정: Administrator 계정 이름 바꾸기	
ksidc_admin	
	ROW
확인 취소	석용(A)



#### ITEASY

② 일반 사용자 계정 원격 터미널 접속 제한

: 일반적으로 서버로 사용하는 시스템의 경우 일반 사용자 계정을 통해 원격 터미널 접
 속을 하여 작업하는 경우가 매우 적습니다. 일반 사용자 계정을 통해 시스템으로의 직
 접적인 접근을 제한하는 것이 좋습니다.

시작 > 모든 프로그램 > 관리 도구 > 서버 관리자



서버 관리자 > 구성 > 로컬 사용자 및 그룹 > 사용자 > 일반 사용자 계정 [마우스 우 클릭] > 속성

👢 서비 관리자					
파일(F) 동작(A) 보기(V) 도용	움말(H)				
🗢 🔿 🖄 🖬 💥 🖬 🛃	1 🗖				
🔚 서버 관리자(WINDOWS-619TRZ	<b>사용자</b> 3 사용자			작업	
□ ♣ 역할 고 ♣ 기능	이름 전체 이름	설명		사용자	-
표 전단	🔩 Guest Eksido ksido	게스트가 컴퓨터 ETPHISER	1/도메인을 액세	기타 작업	•
<ul> <li>○ 주갑 스케올러</li> <li>② 주갑 스케올러</li> <li>○ 주갑 스케올러</li> <li>○ 주갑 보안이 포함된 Wint</li> <li>○ 서비스</li> <li>○ 제 코럴 사용자 및 그룹</li> <li>○ 사용자</li> <li>그룹</li> </ul>	🖉 ksidc_admin	암호 설정(S)	을 관리하도록 기	ksidc	<b>^</b>
		모든 작업(K) 🔸		기타 작업	) i
		삭제(D) 이름 바꾸기(M)			
		속성(R)			
🗉 🚝 저장소		도움말(H)			



#### ITEASY

일반 사용자 계정의 속성 > 원격 데스크톱 서비스 프로필 > "이 사용자 권한의 원격 데스크톱 세션 호스트 서버 로그온 거부" 체크 > 적용

ksidc 속성 🤶 🕺 🕺
일반 소속 그룹 프로필 환경 세션 원격 제어 원격 데스크톱 서비스 프로필 개인용 가상 데스크톱 전화 접속 로그인
이 탭을 사용하며 원격 데스크톱 서비스 사용자 프로필을 구성하십시오. 이 프 로필의 설정은 원격 데스크톱 서비스에 적용됩니다.
원격 데스크톱 서비스 사용자 프로필 프로필 경로(P):
- 원격 데스크톱 서비스 홈 폴더
○ 로컬 경로(L):
○ 연결(C): 대상(T):
☑ 미 사용자 권한의 원경 데스크통 세션 호스트 서버 로그온 거보(D)
 확인 취소 적용(A) 도움말

※ 원격 접속을 제한한 사용자로 접속을 할 경우 아래와 같이 차단되는 부분은 확인 할 수 있습니다.

원격 데스크	1톱 연결						X
8	사용자 계정어 다.	원격 로그인	권한이	없기 때문 <sup>(</sup>	베 연결이	거부되었습	Ц
					확인	도움	말

③ 계정 잠금 설정

: 계정의 보안을 더욱 강화하기 위해서는 계정 잠금 정책을 활성화 하여 특정 횟수 이 상의 로그인 실패가 발생할 경우 계정을 지정한 시간만큼 접속 차단하여, 외부에서의 Brute force 공격으로부터 방어해야 합니다.





### 시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책

		<ul> <li>▶ 원격 데스크톱 서비스</li> <li>▶</li> <li>▲ Hyper-V 관리자</li> <li>♥ IIS(인터넷 정보 서비스) 6.0 관리자</li> <li>♥ IIS(인터넷 정보 서비스) 관리자</li> <li>♥ IIS(인터넷 정보 서비스) 관리자</li> <li>♥ ISCSI 초기자</li> <li>♥ Microsoft .NET Framework 2.0 Configuration</li> <li>♥ Windows PowerShell Modules</li> </ul>
명령 프롬프트		🛞 Windows Server 백업 🝙 Windows 메모리 진단 🚓 고급 비아이 표창되 Windows 바라비
🏹 IIS(인터넷 정보 서비스) 관리자	<b>≥</b>	📷 공유 및 저장소 관리
Internet Explorer	Administrator	🍬 구성 요소 서비스 🚍 데이터 원본(ODBC)
🧳 메모장 🔸	문서	률 로컬 보안 정책 ➡ 보안 그성 미번 Å
🔒 로컬 보안 정책	컴퓨터	·····································
우리 알FTP	네트워크	(%) 성능 모니터
FileZilla	제어판	시스템 구성 이벤트 뷰어
****	장치 및 프린터	④ 작업 스케줄러 그 저자스 탄생기
김자	관리 도구 🔹 🕨	· 지하고 남아가 • 컴퓨터 관리
()) 성능 모니터	도움말 및 지원	
iscsi 초기자	실행	
▶ 모든 프로그램	Windows 보안	
프로그램 및 파일 검색	로그오프 🔸	
🎮 🛛 🦓 🖉		

로컬 보안 정책 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 계정 잠금 정책 > 계 정 잠금 임계값 [마우스 우클릭] > 속성

🖺 로컬 보안 정책				. 🗆 🗙
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🔿 🖄 📅 💥 🖬 😹 🚺 🖬				
🔒 보안 설정	정책 🔺		보안 설정	
🕞 强 계정 정책	闘 계정 잠금 기간		적용할 수 없음	
🗩 🔂 암호 정책	🎟 계정 잠금 임계값 👘 👘		0 번의 잘못된 로그온	
🗉 🔂 계정 잠금 정책	📓 다음 시간 후 계정 잠금 수를 원래대로	속성(R)	적용할 수 없음	3
🗉 💁 로컬 정책		도운말(비)		
🗉 🧮 고급 보안이 포함된 Windows 방화벽	<u>b</u>			
🛄 네트워크 목록 관리자 정책				
표 🧾 공개 키 경찍				
표 🧾 소프트웨어 세한 성책				
표 🦲 응용 프로그램 세너 상색				
표 🐻 IP 모안 성색(위지; 도갈 컴퓨터)				
비비 🔝 끄급 김사 영역 구영				

### **iTEASY**

계정 잠금 임계값 속성 > 잘못된 로그온 시도 횟수 지정 > 적용

계정 잠금 임계값 속성			? ×
로컬 보안 설정   설명			
계정 잠금 임계값			
· · · · · · · · · · · · · · · · · · ·	로그온 시도		
l.			
-	1	11	1
	확인	취소	적용(A)

해당 로그온 실패 임계 값을 지정하실 경우, 자동적으로 계정 잠금 기간이 30분으로 설 정됩니다.

것 책	정책 설정	제안 설정	
· · · · · · · · · · · · · · · · · · ·	적용할 수 없음	<u> </u>	
다음 시간 후 계정 잠금 수를	원래대로 적용할 수 없음		





위와 같은 계정 잠금 기간은 서버 관리자 분께서 임의로 변경 가능하십니다.

🖺 로컬 보만 정책		
파일(F) 동작(A) 보기(V) 도움말(H)		
🗢 🔿 🞽 🖬 🗶 🖬 🖉 📅		
🔒 보안 설정	정책 🔺	보안 설정
🖃 强 계정 정책	🐻 계정 잠금 기간	30 분
🗉 📴 암호 정책	闘계정 잠금 임계값	5 번의 잘못된 로그온
🗉 🚰 계정 잠금 정책	🐻 다음 시간 후 계정 잠금 수를 원래대로 설정	30 분
🕑 📴 로컬 정책		of and a start of the start of
🗉 🧾 고급 보안이 포함된 Windows 방화벽		
🛄 네트워크 목록 관리자 정책		
🗉 🧮 공개 키 정책		
🗉 🧮 소프트웨어 제한 정책		
田 🧾 응용 프로그램 세어 성책		
田 🌏 IP 보안 성책(위지: 로컬 컴퓨터)		
┃ 표 🔛 고급 감사 성책 구성		

④ 보안 로그 활성화

: 보안 감사 정책을 사용하여 계정의 접속 정보를 이벤트 뷰어에 남기도록 설정합니다.

시작 > 모든 프로그램 > 관리 도구 > 로컬 보안 정책

		<ul> <li>▶ 원격 데스크톱 서비스</li> <li>▶</li> <li>▶</li></ul>
명령 프롬프트	. Con	🛞 Windows Server 백업 💼 Windows 메모리 진단
🏹 IIS(인터넷 정보 서비스) 관리자		☆ 고급 보안이 포함된 Windows 방화벽 중 공유 및 저장소 관리
Internet Explorer	Administrator	🍬 구성 요소 서비스 🚍 데이터 원본(ODBC)
🧳 메모장 🔸	문서 ,	🔒 로컬 보안 정책 🔒 보안 구성 마법사
로컬 보안 정책	컴퓨터	서버 관리자 ④ 서비스
요 <mark>가</mark> 알FTP	네트워크	⑧ 성능 모니터
<b>FZ</b> FileZilla	제어판	및 시스럽 구경 이벤트 뷰어
11S(인터넷 정보 서비스) 6,0 관 리자	경지 및 프린터 과리 도그	· 적립 전개물러 및 저장소 탐색기
() 정능 모니터	도움말 및 지원	🛓 컴퓨터 관리
iscsi 초기자	실행	
▶ 모든 프로그램	Windows 보안	
프로그램 및 파일 검색 📃 😥	로그오프 🕨	
🍂 🗸 🕌 🚺		

## iTEASY

로컬 보안 정책 > 로컬 보안 정책 > 보안 설정 > 로컬 정책 > 감사 정책 > 계정 잠 금 임계값 [마우스 우클릭] > 속성

🖥 로컬 보만 정책				_ 🗆 🗙
파일(F) 동작(A) 보기(V) 도움말(H)				
🗢 🔿 🙍 📅 🗙 🖬 🛃 🖬				
보안 설정         ● ▲ 계정 정책         ● ▲ 로칠 정책         ● ▲ 감사 정책         ● ▲ 감사 정책         ● ▲ 보안 옵션         ● ▲ 고급 보안이 포함된 Windows 방화벽         ● ▲ 대응의 목록 관리자 정책         ● ▲ 공개 키 정책         ● ▲ 소프트웨어 제한 정책         ● ● 용 프로그램 제어 정책         ● ● 요리 감사 정책 우성	정책 · 제정 관리 감사 제정 관리 감사 전한 사용 감사 전한 사용 감사 전 디렉터리 서비스 액세스 감사 로그온 이벤트 감사 제 시스템 이벤트 감사 전 정책 변경 감사 때 프로세스 추적 감사	<b>속성(R)</b> 도움말(H)	보안 설정         감사 안 함         감사 안 함	

계정 로그온 이벤트 감사 속성 > 성공, 실패 체크 > 적용

계정 로그온 이벤트 감사 속성	? ×
로컬 보안 설정   설명	
계정 로그온 이벤트 감사	
다음 시도 감사: ☑ 성공(S) ☑ 실패(F) ▲ 다른 정책이 범주 수준의 감사 정책보다 우선하도록 구성도 이 설정이 적용되지 않을 수 있습니다. 자세한 내용은 <u>계정 로그온 이벤트 감사</u> 을(를) 참고하십시 (Q921468)	리어 있으면 오.
확인 취소	적용(A)



#### 4. Windows 방화벽

① Windows 방화벽 상태 확인

#### < Windows Server 2003 >

#### 시작 > 설정 > 제어판 > Windows 방화벽

S 제어관		
파일(E) 편집	집(E) 보기(Y) 즐겨찾기(A) 도구(I) 도움말(H)	
⊙ 뒤로 + ⊙	) - 🎓 👂 검색 🍃 폴더 🛛 🐼 🗙 🍤 🛄 -	
주소(D) 🕞 제	I어판	- 🛃 이동
》게임 컨트롤 좋관리 도구 알 국가 및 언어 알콜콜 ?? 날짜 및 시긴 네 비위크 연 (니 드워클레이 ♀ 라이센스	원 (武) 휴대용 미디어 장치 (월 Windows 방호택) 배 옵션 (월 Windows CardSpace) 안 안 옵션 [결	
Windows 카탈로그	니오 장치	
🦥 Windows Update	후가. 게근-	
· 프로그램(₽) →	•	
5 📝 문서(D) 🕨 🕨		
월 📝 설정( <u>S</u> )	▶ 제어판(C)	
· 문화 · · · · · · · · · · · · · · · · · ·	<mark>경</mark> Windows 보안(W)	
8 2 도움말 및 지원(H)	<ul> <li>· 미르워크 연결(10)</li> <li>· · · · · · · · · · · · · · · · · · ·</li></ul>	
8 · · · · · · · · · · · · · · · · · · ·	🛃 작업 표시줄 및 시작 메뉴(I)	
[ 출 💋 administrator 로그오프(L)		
호 🔟 시스템 종료( <u>U</u> )		1.
🖉 시작 🛛 🧭 🏉 🖉 제어판		



< Windows Server 2008 >

시작 > 모든 프로그램 > 제어판 > 시스템 및 보안 > Windows 방화벽 > 방화벽 상태 확인



방화벽이 활성화 되어 있을 경우 아래와 같은 화면이 나오며, 고급 설정에서 설정을 추 가합니다.





② 접근 허용할 Port 등록

<	Wind	lows	Server	2003	>
---	------	------	--------	------	---

Windows 방화벽 > 예외 탭 > 포트 추가

🔯 ₩indows 방화벽	×
일반 예외 고급 ]	
Windows 방화벽을 사용하도록 설정되어 있지 않습니다. 사용자의 컴퓨터는 등 외부에서의 공격 및 침입의 위험에 노출되어 있습니다. 일반 탭을 클릭하여 용]을 선택해서 사용자의 컴퓨터를 안전하게 보호하십시오.	인터넷 계 [사
프로그램 및 서비스( <u>P</u> ):	
이름   ☑ 원격 데스크톱	<b>_</b>
확인	취소

접근 허용할 포트를 추가 합니다.

포트 추가				×
이 설정을 사용하여 로토콜을 찾으려면	Windows 방화 사용하려는 프로	벽의 포트를 을 길램 또는 서	열 수 있습니다 비스의 설명서를	포트 번호 및 프 참조하십시오,
이름( <u>N</u> ):	http			
포트 번호( <u>P</u> ):	80			
		€ UDP(U	)	
범위 변경( <u>C</u> )	]	[	확인	취소



< Windows Server 2008 >

접근을 허용할 서비스를 인바운드 규칙에 새로운 규칙을 등록합니다.

🎡 고급 보안이 포함된 Windows	3 방화벽					- 🗆 X
파일(F) 동작(A) 보기(V) 도	:움말(H)					
🗢 🏟 🖄 🖬 🗟 🖬						
💣 로컬 컴퓨터의 고급 보안이 포함	인바운드 규칙				작업	1
🔣 인바운드 규칙 💏 아우바우드 규칙	이름	│그룹 ▲	프로필	사용 🔺	안타	바운드 규칙 🔺
· 연결 보안 규칙			공용 공용	Й M		새 규칙
표 🛃 보니러링	ŏ	BranchCache - 콘텐츠 검	모두	OFLIA	7	프로필로 필터링
	0	BranchCache - 피어 검색	모두	아니요	7	상태로 필터링
	0	BranchCache - 호스트 캐 COM+ 네트의크 액세스	모드	ULLIN		그룹으로 필터링
	0	COM+ 원격 관리	모두	아니요		보기 <b>&gt;</b>
	0	DFS 관리	모두	ଖ		· · · · · · · · · · · · · · · · · · ·
	0	DFS 관리	모두	Й М		세도 끄염
		DFS 관리	모두	И М		목록 내보내기
		DTC(Distributed Transacti	포두	OHLIA	?	도움말
	ŏ	DTC(Distributed Transacti,,,	모두	OFLIA		
	0	DTC(Distributed Transacti,,,	모두	아니요		
	0	FTP 서버	모두	СЯ N		
			보두 ㅁㄷ	и M		
			エテ	베		

사용자 지정 > 다음

💣 🖊 인바운드 규칙 마법사	
규칙 종류 만들려는 방화벽 규칙 종류를 선택	합니다.
단계: • 규칙 종류 • 프로그램 • 프로토를 및 포트 • 범위 • 작업 • 프로필 • 이름	만들려는 규칙 종류는 무엇입니까? - 프로그램의 연결을 제어하는 규칙 - 포트(D) TCP 또는 UDP 포트의 연결을 제어하는 규칙 - 미리 장의됨(E) · DranchCache - 콘텐츠 검색(HTTP 사용) · Windows 환경의 연결을 제어하는 규칙 - 사용자 지장 규칙 - 사용자 지장 규칙 





프로그램	> 다음		
	세 인바운드 규칙 마법사 프로그램 이 규칙과 일치하는 프로그램의 전	체 프로그램 경로 및 실행 파일 이름을 지정합니다.	X
	단기: - 규칙 종류 - 프로그램 - 프로토콜 및 포트 - 범위 - 작업 - 프로플	이 규칙은 모든 프로그램에 적용됩니까, 특정 프로그램에만 적용됩니까? C 모든 프로그램(A) 다른 규칙 속성과 일치하는 컴퓨터의 모든 트래픽에 규칙이 적용됩니다. C 다음 프로그램 경로(T): [ 예계: c:WnathWnngram exe	契아坦기(R)
	• 018	에서···································	사용자 지정(C)
		프로그램 지정에 대해 자세히 알아봅니다.	< 뒤로(B) [[[[음(N] > ]] 취소

률지 한마군도 규칙 마입자		<u> </u>
프로토콜 및 포트		
이 귀약을 약용할 프로토볼과 포트	드늘 A/Gor급시文,	
단계:		
규칙 종류	어떤 프로토콜과 포트베 이 규칙이 석용됩니까?	
● 프로그램		
🎍 프로토콜 및 포트		
<ul> <li>범위</li> </ul>		
• 작업	로컬 포트(L): 특정 포트 💌	
● 프로필	5001-5010	
● 이름	에: 80, 443, 5000-5010 의견 포트/P)· ID도 프트	
	(A): 80, 443, 5000-5010	
	ICMP(Internet Control Message 사용자 지정(C),,,	
	Protocol) 설명:	
	프로토콜 및 포트에 대해 자세히 알아봅니다.	
	< 뒤로(B) 다음(N) >	취소

임위 이 규칙을 적용할 로컬 및 원격	IP 주소를 지정합니다.	
단계:		
<ul> <li>규칙 종류</li> <li>프로그램</li> <li>프로토를 및 포트</li> </ul>	이 규칙이 적용되는 로컬 IP 주소 ⓒ 모든 IP 주소(P)	
· 범위	C 다음 IP 주소(T):	
● 작업	- 年2月35 国際(任)	
● 프로필	1日(日)	
≥ 이름		
	이 규칙에 적용되는 원리페이스 등류를 사용사 시장됩니다. 사용사 시장(U) 이 규칙이 적용되는 원격 IP 주소 ⓒ 모든 IP 주소(Y)	
	이 다음 IP 주소(H):	
	マントロン	
	LINN KIK	
	비외 기저에 대한 지내한 저희	



범위

## iteasy

작업 > 연결 허용 > 다음

🞆 세 인바운드 규칙 바랍사	
<b>작업</b> 규칙에 지정된 조건과 연결이 일	L/치할 때 수행할 작업을 지정합니다.
단계: - 규칙 증류 프로그램 프로토를 및 포트 범위 - 작업 - 프로필 이름	연결이 지정한 조건과 일치할 경우 어떤 작업을 수행해야 합니까?
	작업에 대해 자세히 알아봅니다. 

프로필 >	다음 ● 다음 ● 시 안바운드 규칙 마법사 프로필 이 규칙을 적용할 프로필을 지정함	JCł.	X
	단계:		
	규칙 종류	이 규칙이 적용되는 시기는 언제입니까?	
	<ul> <li>프로그램</li> <li>프로토콜 및 포트</li> <li>범위</li> <li>지역</li> </ul>	<ul> <li>✓ 도매인(D) 컴퓨터가 회사 도메인에 연결된 경우 적용됩니다.</li> <li>✓ 개인(P) 커프인(D) 제 이 네트워크 위치에 여격되 경우 정용됩니다.</li> </ul>	
	• 40 • 770		
		컴퓨터가 공용 네트워크 위치에 연결된 경우 적용됩니다.	
		프로필에 대해 자세히 알아봅니다.	
			< 뒤로(B) 다음(N) > 취소

# 정책 명을 임의로 지정 후 마침

🎻 세 인바운드 규척 마법사	
이름	
이 규칙의 이름과 설명을 지정합니	JCF.
단계:	
<ul> <li>규칙 종류</li> </ul>	
● 프로그램	
프로토콜 및 포트	01=(M)-
<ul> <li>범위</li> </ul>	FTP Passive Mode
<ul> <li>작업</li> </ul>	· 설명(음션)(D):
◎ 프로필	
🖌 이름	



#### 5. 메모리 덤프 분석

- 메모리 덤프란? 시스템 중지 오류(ex. 블루스크린, 시스템 충돌)가 발생하여 윈도우 서버가 예 기치 않게 종료될 경우 시스템에서 파일 형식으로 디버깅 정보를 시스템에 남기게 되는데 이 때 생성되는 파일을 메모리 덤프라고 합니다.
- 메모리 덤프를 분석하기 위해서는 메모리 덤프 파일을 분석하기 위해서는 분석 프로그램인 WinDbg과 i386 폴더가 필요합니다.

※ 메모리 덤프 파일을 개인 PC으로 다운로드 하여 분석하여도 무방합니다.

※ WinDbg 다운로드 경로

- ▶ 32비트 버전 : http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx
- ▶ 64비트 버전 : http://www.microsoft.com/whdc/devtools/debugging/install64bit.mspx

※ Symbols 다운로드 경로

http://msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx

※ 생성 경로 : c:₩windows₩Memory.dmp

① WinDbg 설치

: 다운로드 받은 설치 파일을 실행시킵니다.

4	Some components cannot be installed
•	Some Windows SDK components require the full .NET Framework 4. Setup detected the client .NET Framework 4. If you continue with Setup, these components will not be installed. If you want to install these components, click Cancel, then install the .NET Framework 4 from http://go.microsoft.com/fwlink/?LinkID=187668 and then reru- Setup.
	Click OK to continue.





Net Transwork 4 Windows® 7 and .NET Framework 4	
Detection Progress	Software Development Kit
Status	
Status Setup is now detecting Windows SDK components.	
and the second sec	
Action	
Action 16:48:41: CostFinalize. Computing space requirements	
	Cancel









🐉 Windows® SDK for Windows® 7 and .NET Framework 4	_ <b> ×</b>
Installation Progress	Software Development Kit
Status	
Setup is now installing Windows SDK components.	
Action	
Action 16:49:47: InstallValidate. Validating install	
<u>u</u>	
	Cancel

# 설치된 경로를 확인합니다.

(기본 설치 경로 : C:\Program Files\ Debugging Tools for Windows (x86))

🗸 🗢 😺 🗸 🗸	Files	<b>→</b> 4	Debugging Too	ols for Windows (x86
구성 🔻 라이브러리에	포함 🔻 공유 대상 👻 새 물더			• • •
☆ 즐겨찾기	이름	수정한 날짜	유형	크기
📕 Daum 클라우드	1394	2011-03-25 오후	파일 폴더	
🚺 다운로드	📕 clr10	2011-03-25 오후	파일 폴더	
🔜 바탕 화면	\mu sdk	2011-03-25 오후	파일 폴더	
冠 최근 위치	🍌 srcsrv	2011-06-23 오전	파일 폴더	
	symproxy	2011-03-25 오후	파일 폴더	
🔰 라이브러리	👪 themes	2011-03-25 오후	파일 폴더	
📑 문서	🎉 triage	2011-03-25 오후	파일 폴더	
비디오	\mu usb	2011-03-25 오후	파일 폴더	
🔚 사진	📕 w2kchk	2011-03-25 오후	파일 폴더	
👌 음악	🎩 w2kfre	2011-03-25 오후	파일 폴더	
	winext	2011-03-25 오후	파일 폴더	

- ② Symbols 설치
  - : 다운로드 받은 설치 파일을 실행시킵니다.

Ð	Welcome to the Microsoft Windows Debugging Symbols Setup Wizard
	The Setup Wilzard will install Microsoft Windows Debugging Symbols on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	< Back Next > Cancel



### **iTEASY**

Please read the following license	agreement carefully
MICROSOFT SOF	TWARE LICENSE TERMS
MICROSOFT DEE EXECUTABLES	BUGGING SYMBOLS AND
These license terms are an (or based on where you live them. They apply to the so	agreement between Microsoft Corporation e, one of its affiliates) and you. Please read ftware named above, which includes the
I accept the terms in the Licer	nse Agreement
O I do not accept the terms in t	he License Agreement

beleet the way you want readines to be installed	e
Click on the icons in the tree below to change the v	way features will be installed.
Windows Debugging Symbols	Windows Debugging Symbols (7601, 17514, 101119-1850)
	This feature requires 1605MB on your hard drive.

Ready to Install	
The Setup Wizard is ready to b	egin the Typical installation
Click Install to begin the installa installation settings, click Back.	ation. If you want to review or change any of your Click Cancel to exit the wizard.



### **iTEASY**

	indows Debug	ging Sym		9
Please wait while the This may take several	Setup Wizard ins	talls Microsoft Wi	ndows Debugging	Symbols.
Status:	minuces.			
			-	

### ③ 분석 방법

설치된 경로에서 WinDdg.exe를 실행합니다.

🕎 windbg.exe	2010-02-01 오후	응용 프로그램	521KB
	1.000		
File Edit View Debug Window Help		3 Harsh	
			6
		lin <del>e</del> Arrentoli, Arrentoli	

File > Symbol File Path를 지정해 줍니다.

: Symbols 경로는 SRV\*[설치폴더] \*http://msdl.microsoft.com/download/symbols 으로 지정하시면 되십니다.

ex) SRV\*D:₩Symbols\*http://msdl.microsoft.com/download/symbols





ymbol path:		
SRV*D:\\$Symbols*http://msdl.microsoft.com/download/symbols	*	OK
		Cancel
		Help
	-	Browse

File > Image File Path 에서 i386 경로를 지정해 줍니다.

nage path:		
::₩i386	*	ОК
		Cancel
		Help
	*	Browse

File > Open Crash Dump 를 실행하여 덤프 파일을 가져 옵니다.

1.서 🗶 씨 폰더						8== •	FD	
-6 M 24	A					J *		e
🖌 즐겨찾기 🛛 着	이름	수정한 날짜	유형	크기				
🍶 Daum 클라우드	1394	2011-03-25 오후	파일 폴더					
🚺 다운로드	退 clr10	2011-03-25 오후	파일 폴더					
🔜 바탕 화면	🍶 sdk	2011-03-25 오후	파일 폴더					
💹 최근 위치	🍶 srcsrv	2011-06-23 오전	파일 볼더					
=	🍶 symproxy	2011-03-25 오후	파일 폴더					
라이브러리	🍌 themes	2011-03-25 오후	파일 폴더					
문서	🍶 triage	2011-03-25 오후	파일 볼더					
비디오	🍶 usb	2011-03-25 오후	파일 폴더					
🔄 사진	🍶 w2kchk	2011-03-25 오후	파일 폴더					
음악	🍶 w2kfre	2011-03-25 오후	파일 폴더					
	鷆 winext	2011-03-25 오후	파일 폴더					
🖳 컴퓨터	🍶 winxp	2011-03-25 오후	파일 콜더					
🏭 로컬 디스크 (C:)								
👝 로컬 디스크 (D:)								
👝 로컬 디스크 (E:)								
👝 로컬 디스크 (F:) 🎽								
파일	이름(N): MEMORY DMP			•	Crash Dum	o Files		-



!analyze -v 명령어를 이용하여, Dump 내용 중 오류 내용을 확인하시면 되십니다.

kb> !analyze -v

```
💓 Dump D:₩
                                             HMEMORY.DMP - WinDbg:6.12.0002.633 X86
File Edit View Debug Window Help
 🚰 🛛 🛎 🖻 🗉 💱 📷 🥐 🖓 🖓 🕘 🖉 🖾 🖉 🖉 🖾 🖬 🖗 🖬 🖓 🖓 🖓
Command
Microsoft (R) Windows Debugger Version 6.12.0002.633 X86
Copyright (c) Microsoft Corporation. All rights reserved.
Loading Dump File [D
                                                                      MEMORY . DMP ]
Kernel Complete Dump File: Full address space is available
Symbol search path is: SRV*D:\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows Server 2003 Kernel Version 3790 (Service Pack 2) MP (2 procs) Free x86 compatible
Product: Server, suite: TerminalServer SingleUserTS
Built by: 3790.srv03_sp2_gdr.100216-1301
Machine Name:
Kernel base = 0x80800000 PsLoadedModuleList = 0x808af9c8
Debug session time: Mon Nov 1 05:49:35.140 2010 (UTC + 9:00)
System Uptime: 18 days 16:06:05.407
Loading Kernel Symbols
Loading User Symbols
Loading unloaded module list
    ¥
                          Bugcheck Analysis
Use <u>lanalyze -v</u> to get detailed debugging information.
BugCheck 7A, {c03900d4, c0000185, e4035008, 14747880}
Probably caused by : memory_corruption ( nt!MiWaitForInPageComplete+2cf )
Followup: MachineOwner
1: kd> !avalyze -v
```



#### [Windows 2003 cmd.exe 보안 설정 TIP]

: cmd란 명령 프롬프트으로 도스 창입니다. 즉, "도스(DOS) 명령" 을 실행하는 부분입니다. 일반적으로 서버의 경우 외부에서 cmd를 요청하는 경우가 없기 때문에 외부에서 접근하여 사용하는 부분을 제한 하는 것이 좋습니다.

※ cmd.exe 파일 경로 : C:₩windows₩system32

① cmd.exe [마우스 우클릭] > 속성

😂 C :\WINDO\S\syste	m 32						
파일( <u>F</u> ) 편집( <u>E</u> ) 보기( <u>\</u>	) 즐겨	찾기( <u>A</u> ) 도구(	<u>T</u> ) 도움말( <u>H</u> )				- 100
🔾 뒤로 🗸 🕥 🗸 🎓	검색 📂	폴더 🛄-					
주소(D) 🛅 C:₩WINDOWSt	#system	32					이동
	-	이름 🔺		[ 크기	종류	수정한 날짜	-
시스템 작업	*	cmd, exe	New York Concerns	171KB	으요 표구 기래	12007-02-18 오	전
<ul> <li>한 프로그램 추가/제거</li> <li>과일 또는 폴더 찾기</li> </ul>		Cmdial3 cmdkey cmdl32,1 Cmdl3k cmdlgk cmdlb, v	열기(Q) 다음 계정으로 실행(A) 알집 EXE 만들기(K) 알집으로 압축하기(L) cmd.zip 으로 압축하기(Q)			2007-02-18 오 2007-02-18 오 2007-02-18 오 1998-07-25 오 2005-12-06 오	전 전 전 전 전
		🕐 cmmgr3 📿	cmd.zip 로 압축하여 E-Ma	ail에 첨부하기([)		2005-12-06 오	拿
파일 및 폴더 작업	*	Section:	EditPlus 3			2007-02-18 오	전
📺 파일 이름 변경 😰 파일 이동		S cmpbk3; Cmprops Cmsetac	Microsoft Forefront Endpo UltraEdit-32	int Protection 2010	를 사용하여 검사	2005-12-06 오 2007-02-18 오 2007-02-18 오	후 전 전
📄 파일 복사		🎆 cmstp,e	보내기( <u>N</u> )		•	2007-02-18 오	전
<ul> <li>➡ 파일을 웹에 게시</li> <li>☆ 파일을 전자 메일로</li> </ul>		S cmutil, d cnbjmor cnetcfg,	잘라내기( <u>T</u> ) 복사( <u>C</u> )			2007-02-18 오 2007-02-18 오 2005-12-06 오	전 전 후
🗙 파일 삭제		🛐 cnvfat, dl	바로 가기 만들기( <u>S</u> )			2007-02-18 오	전
		🛐 colbact,	삭제( <u>D</u> )			2007-02-18 오	전
기티 이 귀	^	🔊 comadd	이름 바꾸기( <u>M</u> )			2007-02-18 오	전
711 714	^	S comcat,	소선(B)			2005-12-06 오	拿
<ul> <li>WINDOWS</li> <li>내 문서</li> <li>양 내 컴퓨터</li> <li>당 내 네트워크 환경</li> </ul>		comclus comcti32, d comdig32, d Comdig32, d comdig32, d comm, drv comm, drv	I III Docx	585KB 263KB 127KB 11KB 63KB	응용 프로그램 확장 응용 프로그램 확장 ActiveX 컨트롤 장치 드라이버 응용 프로그램	2007-02-18 오 2010-09-07 오 2007-02-18 오 1997-07-19 오 2005-12-06 오 2005-12-06 오	선 후 후 후 후
77.00.44		🔊 commdig.c	Ш	33KB	응용 프로그램 확장	2005-12-06 오	± +1
사세히	* +	1				1	•
열기(0)							1.

② cmd 속성 > 보안

: 접근이 불필요한 계정들은 모두 삭제하여 내부 관리자가 접속을 한 후에만 사용할 수 있도록 합니다.

Administrators		
M TelnetClients		
	추가( <u>D</u> )	제거( <u>B</u> )
dministrators의 사용 권한( <u>P</u> )	허용	거부
모든 권한	D	D
우성 읽기 및 실행		
읽기		
쓰기		□
특성 권한	- <b>-</b>	
정 권한 및 고급 설정을 보려면	면 [고급]을 클릭하	고급(V)
1110		

