Windows NT/2000 시스템 해킹 분석절차

2002.11.07
이완희/CERTCC-KR
lwh@cert.certcc.or.kr

이 문서는 Windows NT/2000 시스템이 해킹을 당했는지 여부를 알 수 있는 분석절차를 기술한다. 특히 서버 시스템을 분석 할 수 있는 일반적인 분석절차이므로 시스템관리자는 운영중인 시스템환경에 맞게 적용하기를 바라며 자세한 내용은
※참고로 링크된 부분을 참조하기를 바란다.

1. 네트워크 상태 및 프로세스 점검

가. 네트워크 상태 확인

▶ [시작] ⇨ [실행] ⇨ [cmd] ⇨ [netstat -na] 로 네트워크 상태확인

Local 시스템에서 열린 포트를 확인한 후 비정상적인 포트나 일반적인 접속이 아닌 접속자의 IP 및 서비스포트를 확인한다.

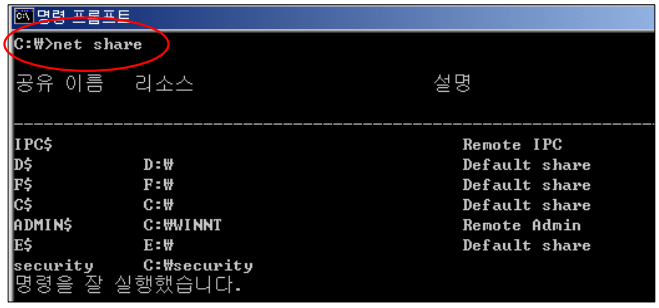
```
C:\>netstat -na
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    172.16.5.51:139        0.0.0.0:0              LISTENING
  TCP    172.16.5.51:1316       211.234.121.32:8002    ESTABLISHED
  TCP    172.16.5.51:445        172.16.5.50:1056       ESTABLISHED
  ...
```

※ 참고 : 서비스 포트 정보 : http://www.iana.org/assignments/port-numbers

윈도우즈 서버에 사용되는 기본적인 포트정보는 아래의 경로에서 확인할 수 있다
" /winnt/system32/drivers/etc/services " => 메모장에서 확인가능

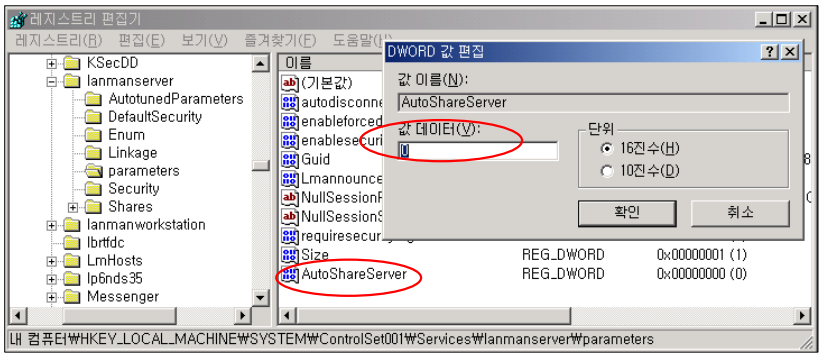
▶ [시작] ⇨ [프로그램]⇨ [관리도구] ⇨ [컴퓨터관리] ⇨ [공유폴더] ⇨ [공유]

특정 바이러스나 침입자가 특정 폴더를 공유하여 외부에서 액세스하는 경우가 있으므로 주기적으로 점검한다. 공유가 되어 있다면 바이러스에 감염되었을 확률이 높다. 명령 프롬프트 창에서 net share 명령어를 사용하여 점검할 수도 있다.



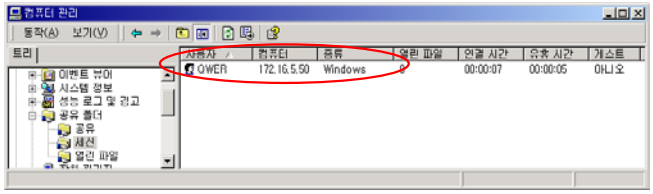
※ 참고 : $표시가 되어 있는 것은 Windows에서 디폴트로 관리를 목적으로 공유되어 있는 것으로 레지스트리값을 추가한 후 재부팅하여 제거해야 한다.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters키에 DWORD값으로 AutoShareSErver 항목을 만든후 0으로 값을 설정한 후 재부팅 한다.



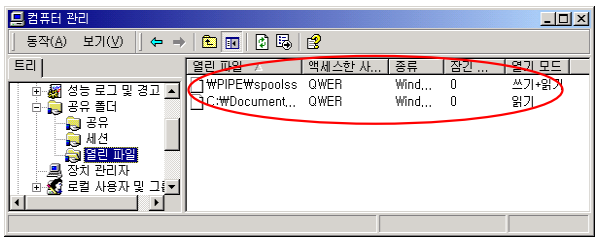
▶ [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [컴퓨터관리] ⇨ [공유폴더] ⇨ [세션]

불법적인 접속을 확인할 수 있으며 접속을 끊을 수 있다.



▶ [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [컴퓨터관리] ⇨ [공유폴더] ⇨ [열린 파일]

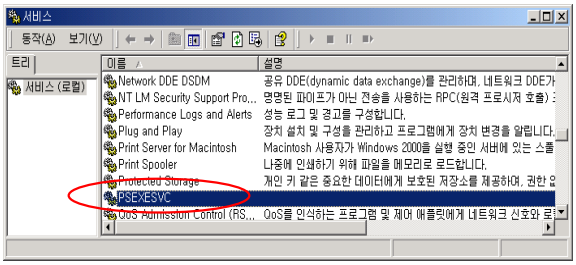
현재 접속중인 불법사용자가 접근하는 파일을 알 수 있다.

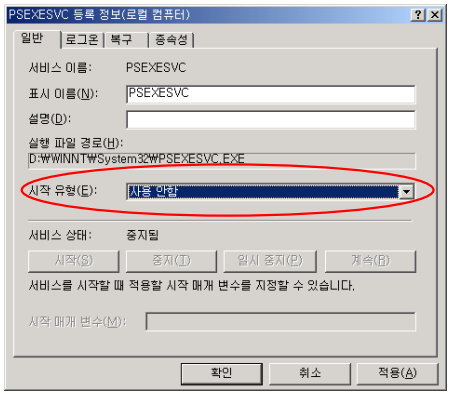


나. 실행중인 서비스 및 프로세스 확인

▶ [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [서비스]

Windows 시스템은 기본적으로 많은 서비스가 열려 있으므로 서버 구축시에 불필요한 서비스는 미리 제거하고 악성프로그램에 감염되었을 때에도 악성프로그램이 서비스에 등록 될 수 있으므로 점검하여 제거한다. 아래의 참조를 참조하여 필요 없는 서비스는 처음 설치시에 제거하기 바란다.



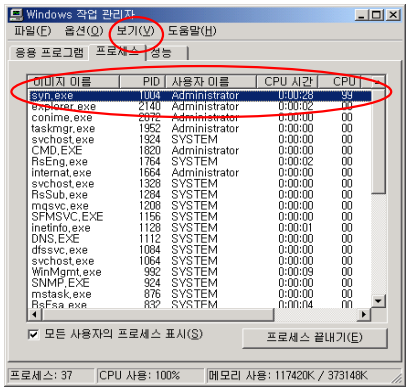


※ 참고 : Windows 서비스 정보

http://www.microsoft.com/korea/technet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp

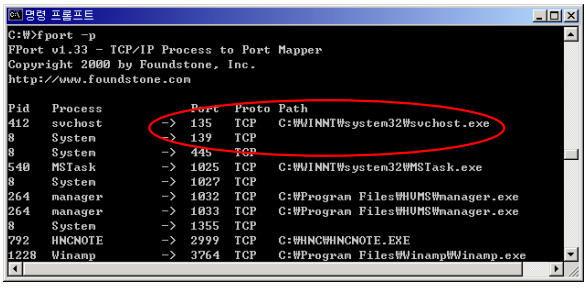
▶ [Ctrl+Alt+Del] ⇨ [작업관리자] ⇨ [프로세스]

의심가는 프로세스의 CPU사용량과 메모리 사용량을 확인하고, 악성프로그램도 일반 프로세스명과 비슷하게 변경되어 실행되므로 주의해서 확인한다. [작업관리자] ⇨ [보기] ⇨ [열선택] ⇨ [사용자 이름]을 체크하면 누가 프로세스를 실행시켰는지 알 수 있다.



▶ Fport프로그램을 이용

Windows 시스템은 winnt/ * .svc.exe 파일들이 여러 서비스를 관리하면서 임의의 포트를 열어서 사용하기 때문에 임의의 포트가 많이 열려 있으므로 Backdoor를 찾기 위해서 Fport 프로그램을 이용하면 쉽게 열린 포트와 그와 매칭되는 실행파일을 확인할 수 있다.



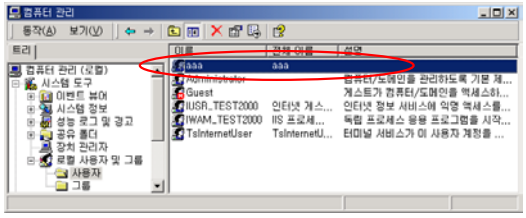
※ 참고 : FPort다운로드 : http://www.foundstone.com/rdlabs/zips/FPortNG.zip

2. 시스템 설정 및 악성프로그램 탐지

가. 계정 및 스케쥴러 점검

▶ [시작] ⇨ [프로그램] ⇨[관리도구] ⇨ [컴퓨터관리] ⇨ [로컬 사용자 및 그룹] ⇨ [사용자],[그룹]

현제 생성되어 있는 계정 및 그룹을 확인하여 불법적인 계정이나 일반사용자의 Administrators 그룹 권한 여부 및 불법 그룹의 생성여부를 점검한다. guest 계정이 사용안함으로 되어 있는지 점검한다.

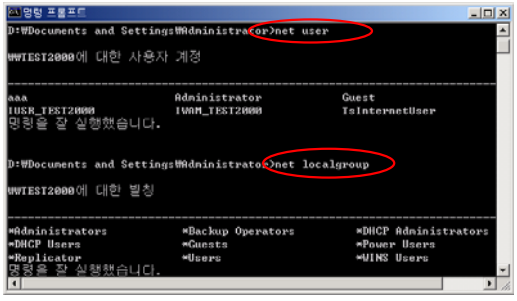


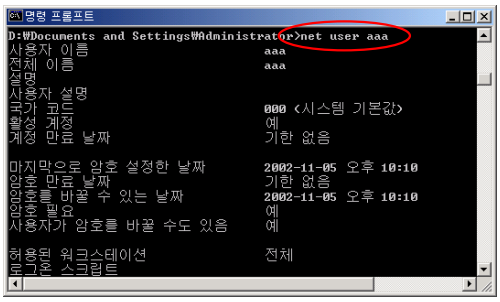
명령 프롬프트 창에서도 아래의 명령어를 이용하여 점검할수도 있다.

net user => 사용자 계정확인

net localgroup => 로컬 그룹 계정 확인

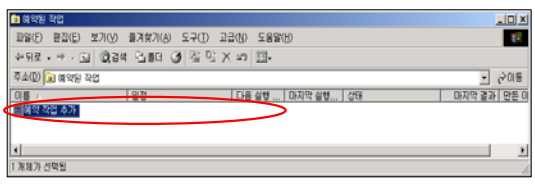
net group => 도메인 컨트롤러 인 경우 그룹 계정확인

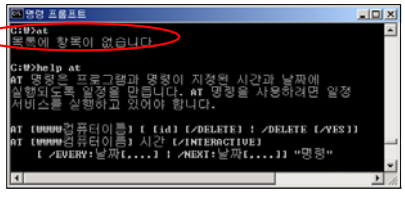




▶ 실행중인 스케줄러를 점검 : [시작] ⇨ [설정] ⇨ [제어판] ⇨ [예약된 작업]

이이를 악성프로그램이 일정시간에 시작되도록 등록할 수 있으므로 예약된 작업을 확인해 보아야 한다. 명령 프롬프트창에서 at 명령으로도 확인가능하다.





나. 악성 프로그램을 점검

▶ win.ini , system.ini 파일에 백도어 관련 실행파일이 설정되어 있지 않은가 검사
▶ 부팅시에 자동으로 실행되게 설정하는 레지스트리를 점검

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce 1
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices 1
```

※ 참고 : 악성 프로그램이 사용하는 자동 실행 설정 및 대응 방법
http://certcc.or.kr/paper/tr2002/tr2002_01/Window_Autostart_setting.pdf

▶ 변경된 시스템 바이너리 파일을 점검 : 탐색기 ⇨ 검색 ⇨ 날짜 ⇨ 수정된파일 ⇨ 기간설정

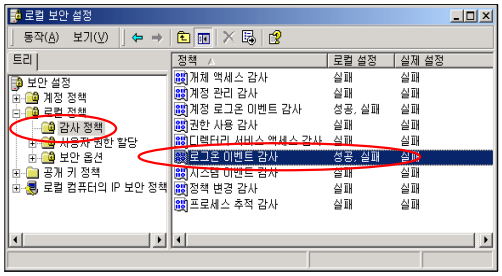
일반적인 파일은 설치된 후 거의 수정되지 않는다. 트로이잔 버전의 파일로 변경되는 경우가 많은데 최근에 이상증상이 나타난 전후로 수정된 파일을 찾아 예전의 시스템의 원본 파일의 크기를 비교해 본다. 특히 패스워드 크래킹 프로그램은 숨김 속성이 있기 때문에 탐색기에서 모든 파일보기를([보기] ⇨ [폴더 옵션] ⇨ [보기] ⇨ [숨김파일 및 폴더 표시])선택한 후 점검한다.

3. 로그 분석

가. 이벤트로그 분석

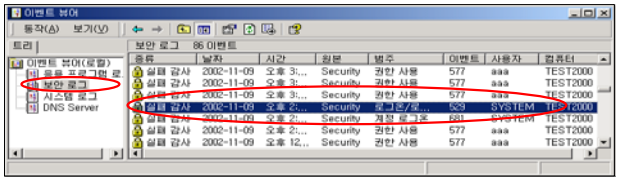
▶ [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [이벤트 뷰어]

Windows 시스템은 최소 설치시에는 시스템 로그온이나 불법적인 접근에 관한 로그는 남기지 않기 때문에 시스템 관리자가 [시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [로컬보안설정] ⇨ [보안설정] ⇨ [보안설정] ⇨ [로컬정책] ⇨ [감사정책]을 직접 설

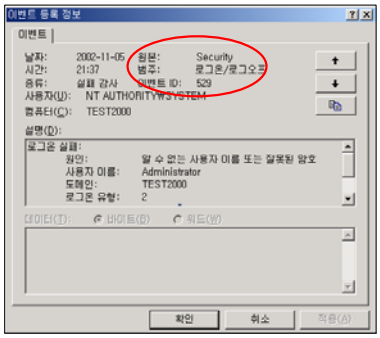


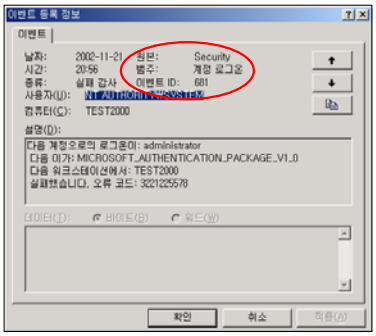
정을 해주어야 보안로그가 남는다.

보안 로그는 로컬보안설정에서 감사정책을 설정한 로그가 남기 때문에 정기적인 점검이 필요하다. 파일 생성, 접근, 삭제 등의 리소스 사용 및 로그온 시도와 같은 접근제어 기록이 보안로그에 기록된다.



특히 이벤트로그에는 다양한 이벤트 ID가 기록되므로 이 ID의 해석을 통해 해킹시도 및 접근 시도를 알 수 있다. 일반적인 로그온(5xx)과 터미널 서버(6xx)를 통한 로그온도 이 이벤트 ID를 통해서 구분할 수 있다.





※ 참고

로컬보안 설정하기

http://www.microsoft.com/korea/technet/security/prodtech/windows/windows2000/staysecure/secops04.asp

이벤트 ID 정보

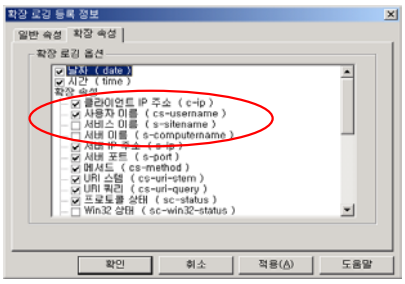
http://www.microsoft.com/korea/technet/security/prodtech/windows/windows2000/staysecure/secops06.asp

나. IIS로그 분석

예전부터 Windows 해킹은 IIS를 통한 해킹이 주를 이루고 있으며 각종한 툴도 취약점이 발견되면 곧바로 만들어질 정도로 취약점이 계속 발견되고 있다. 그러므로 IIS로그를 체크하는 것이 무엇보다도 중요하다. IIS 로그는 단순히 특정 작업이 성공했는지 실패했는지를 알려주는 것만이 아니라, 문제를 해결하는데 필요한 정보도 알려주며 IIS 관련 취약점으로 해킹이 들어 왔을 때에도 로그가 남게 된다. IIS 로그는 Default로 **%SystemRoot%\System32\LogFiles** 디렉토리 아래에 저장되며 로그의 보안을 위해 특정 드라이버로 설정 할 수도 있다.

※ 로그에 기록되는 정보는 **클라이언트 IP주소, 사용자이름, 날짜, 시간, 사용한 서비스,**

서버의 이름, 서버의 IP주소, 처리시간(백만분의 1초), 받은 바이트수, 보낸바이트수, 서비스 상태코드, Win32 에러코드, 작업의 이름, 작업의 대상 또는 목표, 넘겨진 인지 등이며 [웹사이트 등록정보] ⇨ [웹사이트 탭] ⇨ [등록정보] ⇨ [확장속성]에서 관리자가 임의로 제어할 수 있다.



※ 참고

서비스 상태코드 및 작업의 이름

http://lachesis.x-y.net/etc/http10v3.html

Win32 에러코드

http://www.winehq.com/source/include/winerror.h

예제) 2001-09-13 07:41:12 xxx.xxx.136.107 - xxx.xxx.27.107 80 GET /scripts/..%5c..%5c..%5c..%5c../winnt/system32/cmd.exe /c+dir 200 -

xxx.xxx.136.107 시스템(클라이언트)에서 xxx.xxx.27.107(서버)시스템으로 유니코드를 이용하여 dir 명령을 수행하여 성공(200)하였다는 의미이다.

맺음말

한 시스템이 해킹을 당했다면 일반적으로 같은 방법으로 다른 시스템도 해킹을 당했을 경우가 많으므로 해킹방법을 분석하여 로컬 네트워크내의 모든 시스템을 점검하여야 하며 모든 시스템의 패스워드를 변경하여야 한다. 해킹 당한 Windows 시스템을 분석하다 보면 쉬운 패스워드로 인한 패스워드 유추공격 및 이미 예전에 나왔던 취약점을 이용하여 공격을 당한 시스템이 많은데 Windows 보안을 위해서는 최소 8자리이상의 특수문자가 포함된 패스워드 및 패치가 우선이 되어야 할 것이며 최근에 시스템을 다시 설치하였을 경우 우선 최신 서비스팩을 설치한 후 서비스팩에 누락된 핫픽스가 있을수 있으므로 HFNetChk도구를 이용하여 누락된 핫픽스를 추가로 설치하여야 할 것이다.

※ 참고 : **HFNetChk 관련 사이트**

http://support.microsoft.com/default.aspx?scid=http://www.microsoft.com/korea/support/xmlkb/kr303215.asp

또, Windows 시스템 자체적으로는 해킹관련 Forensics를 하기가 어렵기 때문에 보안업체에서 제공하는 IDS나 Firewall을 설치하여 침입탐지 및 대응을 하여야 할 것이며 또한 주기적으로 백신프로그램을 이용하여 웜 바이러스, 트로이잔 프로그램의 감염을 막아야 할 것이다.

[참고자료]

보안 패치 게시판
http://www.microsoft.com/korea/technet/security/current.asp

보안 검사 목록 및 보안도구
http://www.microsoft.com/korea/technet/security/tools/tools.asp

Windows 2000 Server 보안 작업 가이드
http://www.microsoft.com/korea/technet/security/prodtech/windows/windows2000/staysecure/

Windows 2000 Server 구축 및 계획 가이드
http://www.microsoft.com/korea/technet/win2000/dguide/home.asp

Windows 시스템 관련 기술문서 제공
http://www.microsoft.com/korea/windows/server/Technical/default.asp