작성자 : 기술지원부 조 태 준 tedcho@nextline.net

서버 내용 분석 스크립트

침해사고를 정확히 분석하기 위해서는 현재 구동중인 프로세스 정보나 네트워크 상태 정보 등 휘발성 증거를 수집해야 됩니다. 그리고 현재 피해시스템의 상황을 빠른 시간 안에 파악할 수 있는 방법이 필요하므로 윈도우 커맨드에서 실행되는 명령어들을 이용해 프로세스. 네트워크, 로그인 정보들을 수집해야 합니다. 이러한 정보들을 이용해 최대한 빨리 시스템의 변경내용이나 공격자의 흔적을 파악해야 합니다.

1. 사용 방법

1.1 해킹관련 프로그램₩서버 내용 분석 스크립트 폴더로 이동합니다
1.2 점검파일.bat 스크립트 파일을 실행합니다.
1.3 결과내용.txt 라는 파일이 생성됩니다.
1.4 결과내용.txt 파일의 내용을 확인하여 시스템의 정보를 확인 한다.

2. 분석 스크립트의 내용 은 아래와 같습니다.

```
@echo KISA INCIDENT FIRST DATA COLLECTION TOOL
@echo -------- Check Data, Start Time ---------
date/T
time/T
@echo -------- Get system information ---------
psinfo -h -s -d
@echo -------- Get Network info ---------------
ipconfig/all
@echo -------- Get Session info ---------------
net sess
netstat -na
nbtstat -c
net user
net share
net localgroup Administrators
@echo -------
fport/i
psloggedon
net start
pslist -t
time/T
```

3. 분석 스크립트의 내용
date /T : 시스템 날짜를 알려주는 명령어
time /T : 시스템 시간을 알려주는 명령어

psinfo –h –s –d : 설치된 핫픽스 및 소프트웨어 목록 정보, 하드디스크 정보

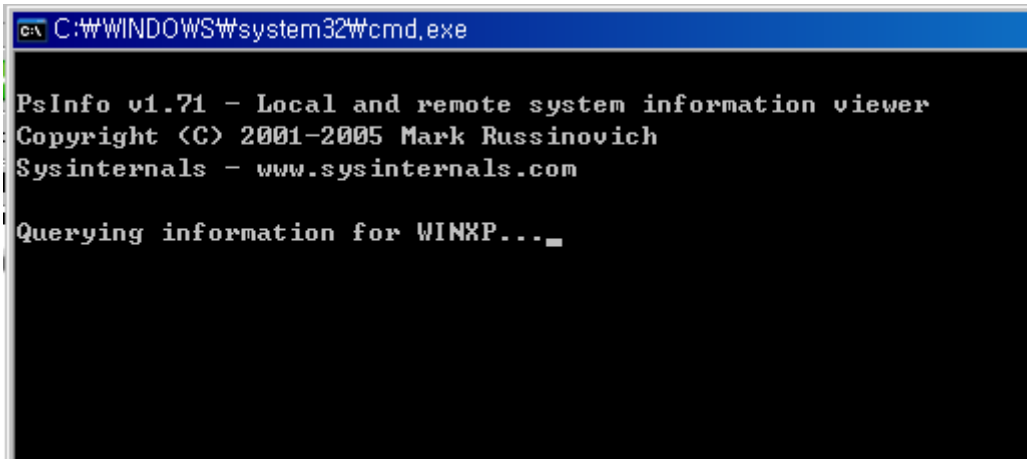
ipconfig/all : 시스템의 아이피 정보 수집

net sess : 공유 자원에 접속한 컴퓨터 정보 출력
netstat –na : 서비스 중인 포트 정보 및 연결된 아이피 정보
nbtstat –c : NBT에 연결된 세션 정보 출력
net user : 시스템에 존재하는 계정정보 출력
net share : 시스템 공유 정보 출력
net localgroup Administrators : 시스템에 존재하는 administrators 그룹정보 출력
fport/i : 서비스 중인 포트를 열고 있는 프로그램 정보
psloggedon : 현재 연결된 세션 정보 확인
net start : 시스템에 가동중인 서비스 리스트
pslist -t : 시스템에 강동중인 프로세스 리스트를 트리 모양으로 출력
time/T : 시스템 시간을 알려주는 명령어

4. 실질적인 예

4.1 점검파일.bat 파일을 실행

4.2. 파일의 실행중인 내용



4.3. 실행 후 결과내용.txt 파일이 생성된 내용

5 결과내용.txt 파일의 내용을 확인

5.1 date/T , time/T 한 내용

```
KISA INCIDENT FIRST DATA COLLECTION TOOL
-------- Check Data, Start Time ---------
2007-09-17
오후 02:16
```

5.2 시스템에 설치된 핫픽스 및 소프트웨어 목록 정보, 하드디스크 정보 출력

```
-------- Get system information ---------
System information for WWWINXP:
Uptime:                    0 days 3 hours 20 minutes 10 seconds
Kernel version:            Microsoft Windows XP, Uniprocessor Fr
Product type:              Professional
Product version:           5.1
Service pack:              2
Kernel build number:       2600
Registered organization:   WinXP
Registered owner:          WinXP
Install date:              2007-04-17, Activation status:
IE version:                6.0000
System root:               C:WWINDOWS
Processors:                1
Processor speed:           1.3 GHz
Processor type:            Intel(R) Celeron(R) M processor
Physical memory:           502 MB
Video driver:              Intel(R) 82852/82855 GM/GME Graphics
Volume Type       Format     Label                        Size
    C: Fixed      NTFS                                40.00 GB   2
    D: Fixed      NTFS                                15.88 GB   1
    E: CD-ROM
    F: CD-ROM
    Y: Remote     NTFS                                50.11 GB   2

Installed     HotFix
2007-04-24    FIX: ASP stops responding when calling Response.Re
2007-08-15    Security update for MSXML4 SP2 (KB936181)
2007-04-17    Windows Media Player 6.4
2007-04-17    Windows Media Player 9
2007-08-15    Windows Media Player 9
2007-04-17    Windows XP
2007-04-17    Windows XP
2007-04-17    Windows XP
```

5.3 시스템의 아이피 정보 수집

```
-------- Get Network info ---------------

Windows IP Configuration

        Host Name . . . . . . . . . . . . : winxp
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : local

Ethernet adapter 무선 네트워크 연결:

        Connection-specific DNS Suffix  . : local
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 2200BG Network Connection
        Physical Address. . . . . . . . . : 00-12-F0-81-5E-21
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.9
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 168.126.63.1
                                            222.122.12.11
        Lease Obtained. . . . . . . . . . : 2007년 9월 17일 월요일 오전 11:04:21
        Lease Expires . . . . . . . . . . : 2007년 9월 27일 목요일 오전 11:04:21
```

5.4 네트워크에 연결된 세션 및 연결된 port 상태

```
-------- Get Session info ---------------
목록에 항목이 없습니다.


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    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    192.168.0.9:139        0.0.0.0:0              LISTENING
  TCP    192.168.0.9:1355       61.100.191.30:445      ESTABLISHED
  TCP    192.168.0.9:1363       61.100.191.30:4829     ESTABLISHED
  TCP    192.168.0.9:2219       211.115.213.200:88     TIME_WAIT
  TCP    192.168.0.9:2220       211.115.213.200:88     TIME_WAIT
  TCP    192.168.0.9:2225       211.115.213.200:88     TIME_WAIT
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1031           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1046         *:*
```

5.5 NBT 연결 세션 및 겨정정보 출력

```
무선 네트워크 연결:
Node IpAddress: [192.168.0.9] Scope Id: []

    No names in cache

\\WINXP에 대한 사용자 계정

-------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
SUPPORT_388945a0         ted
명령을 잘 실행했습니다.
```

5.6 공유 정보 및 그룹정보 출력

```
공유 이름   리소스                         설명

-------------------------------------------------------------------------
D$           D:\                            Default share
print$       C:\WINDOWS\system32\spool\drivers
                                            프린터 드라이버
C$           C:\                            Default share
ADMIN$       C:\WINDOWS                     Remote Admin
IPC$                                        Remote IPC
SharedDocs   C:\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS

명령을 잘 실행했습니다.

별칭 이름     Administrators
설명          컴퓨터/도메인에 모든 액세스 권한을 가진 관리자

구성원

-------------------------------------------------------------------------
Administrator
ted
명령을 잘 실행했습니다.
```

5.7 사용중인 포트 및 프로그램 정보

```
------- Get Port info --------------------
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
0     System         ->  2219  TCP
0     System         ->  2220  TCP
0     System         ->  2225  TCP
4     System         ->  1355  TCP
4     System         ->  139   TCP
4     System         ->  445   TCP
804   svchost        ->  3389  TCP   C:₩WINDOWS₩system32₩svchost.exe
848                  ->  135   TCP
1036                 ->  2869  TCP
1944                 ->  1025  TCP
3448  ClipSock       ->  1363  TCP   C:₩Documents and Settings₩ted₩바탕 화면₩ClipSock.exe

0     System         ->  137   UDP
0     System         ->  138   UDP
0     System         ->  1900  UDP
4     System         ->  1046  UDP
4     System         ->  500   UDP
804   svchost        ->  4500  UDP   C:₩WINDOWS₩system32₩svchost.exe
848                  ->  445   UDP
1036                 ->  1031  UDP
```

5.8 현재 연결된 세션 정보 및 시스템에 가동중인 서비스 리스트

```
PsLoggedOn v1.31 - Logon Session Displayer
Copyright (C) 1999-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     <Unknown> NT AUTHORITY₩LOCAL SERVICE
     <Unknown> NT AUTHORITY₩NETWORK SERVICE
     2007-09-17 WINXP₩ted
     <Unknown> NT AUTHORITY₩SYSTEM

No one is logged on via resource shares.
```

다음과 같은 Windows 서비스가 시작되었습니다.

```
   Ac Profile Manager Service
   Access Connections Main Service
   Application Layer Gateway Service
   Automatic Updates
   COM+ Event System
   Computer Browser
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Error Reporting Service
   Event Log
   EvtEng
   Fast User Switching Compatibility
```

5.9 시스템에 강동중인 프로세스 리스트

```
PsList 1.26 - Process Information Lister
Copyright (C) 1999-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for WINXP:

Name                                Pid Pri Thd  Hnd      VM      WS    Priv
Idle                                  0   0   1    0       0      16       0
  System                              4   8  58  328    1856     280       0
    smss                            444  11   3   21    3780     392     172
      csrss                         492  13  12  484   66212    3044    2488
      winlogon                      516  13  19  504   61324    4108    8236
        services                    560   9  15  291   36344    5016    2108
          ibmpmsvc                  752   8   4   30   18452    1496     512
          svchost                   804   8  19  207   66568    5180    2836
          svchost                   848   8  11  279   39532    4492    1916
          svchost                   952   8  69 1489  144496   26096   16052
          svchost                   988   8   6   81   31816    3420    1356
          svchost                  1036   8  15  217   45872    7516    5632
          spoolsv                  1220   8  11  137   52108    5508    3472
          AcPrfMgrSvc              1460   8   6   82   38544    5056    1708
          EvtEng                   1508   8   8  133  184088    7900    3944
          hsvcmod                  1556   8   2   23   17900    1768     588
          npkcmsvc                 1576   8   3   31   17184    1884     552
          RegSrvc                  1616   8   3   76   24868    2664     776
          vrmonsvc                 1672   8   3   54   77904   33796   31792
          AcSvc                    1760   8  13  195   57568    7256    3472
            SvcGuiHlpr              948   8   2   80   39672    5940    2744
            AcMurocHlpr            1360   8   7  116   47532    7904    4928
          alg                      1944   8   5   99   35872    3688    1240
          svchost                  2188   8   8   92   41012    3584    1656
          svchost                  3028   8   8  127   41436    4344    2588
        lsass                       596   9  21  381   48168    3908    4776
explorer                           1860   8  16  538  189848   31300   19112
  hkcmd                             112   8   2   98   34548    4720    2072
```

5.10 스크립트 종료시간

오후 02:16