

**Incident Response Toolkit  
:  
Initial Response**

Sunday, August 24, 2003

**Balwant Rathore, CISSP**  
Founder,  
Open Information System Security Group

[www.oissg.org](http://www.oissg.org)

- **Keep the Toolkit CD Handy**
- **Sample Toolkit for WinNT**
- **Evidence Gathering**

[www.oissg.org](http://www.oissg.org)

## OISSG Keep the Toolkit CD Handy

- Key utilities for different platforms
- Avoids running trojaned binaries on server
- Avoids accessing key files
  - Preserves Last-accessed timestamps

[www.oissg.org](http://www.oissg.org)

### **The purpose of immediate response toolkit are:**

- Helping organization personnel quickly and efficiently recover from security incidents.
- Minimizing loss, theft, or disruption of critical computing services when incidents occur.
- The need to respond systematically. Dealing properly with legal issues.

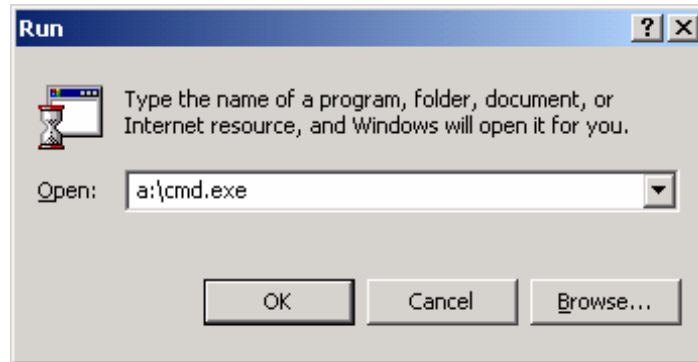
- Cmd.exe
- Loggedon
- Rasusers
- Netstat
- Fport
- Pslist
- listdlls
- Nbtstat
- Arp
- Kill
- Md5sum
- Rmtshare
- Netcat
- doskey

## OISSG Tips on Information Gathering

- Save data to floppy
  - Overwriting data on hard-disk might lose valuable info
- Record the data gathered, in a notebook
- Use netcat / cryptcat to send data to a forensic workstation

[www.oissg.org](http://www.oissg.org)

● Executing a trusted command shell



## OISSG Who have logged on?

- Psloggedon utility from 'sysinternals'

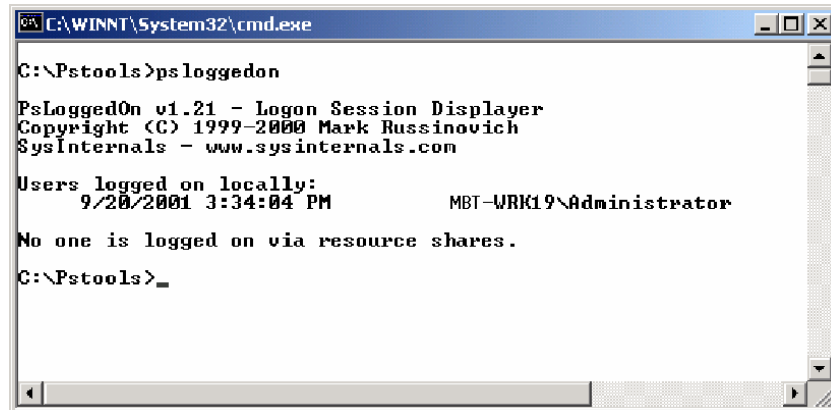
- A utility that shows all users connected locally and remotely

- Rasusers

- To list users logged in via Remote Access Service

[www.oissg.org](http://www.oissg.org)

# OISSG Psloggedon output



```
C:\WINNT\System32\cmd.exe

C:\Pstools>psloggedon

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
    9/20/2001 3:34:04 PM          MBT-WRK19\Administrator

No one is logged on via resource shares.

C:\Pstools>
```

[www.oissg.org](http://www.oissg.org)



## Determine Open Ports Listening

- Open ports indicate server applications
  
- Trojans open new ports to receive commands from attacker
  - Eg Backorifice listens on tcp 31337
  
- Trojan Ports List
  - [www.simovits.com](http://www.simovits.com)

[www.oissg.org](http://www.oissg.org)

Open ports indicates the server applications (running on the server) and using these, Trojans can be executed. The list of Trojan ports can be found in the link given above.

# OISSG Netstat: to list open ports

```
C:\WINNT\System32\cmd.exe
C:\Pstools>netstat -an
Active Connections
Proto Local Address          Foreign Address         State
TCP 0.0.0.0:135             0.0.0.0:0               LISTENING
TCP 0.0.0.0:261             0.0.0.0:0               LISTENING
TCP 0.0.0.0:445             0.0.0.0:0               LISTENING
TCP 0.0.0.0:1028           0.0.0.0:0               LISTENING
TCP 0.0.0.0:1032           0.0.0.0:0               LISTENING
TCP 0.0.0.0:1003           0.0.0.0:0               LISTENING
TCP 0.0.0.0:1111           0.0.0.0:0               LISTENING
TCP 192.168.0.161:139      0.0.0.0:0               LISTENING
TCP 192.168.0.161:139      192.168.0.79:1385      ESTABLISHED
TCP 192.168.0.161:1107    0.0.0.0:0               LISTENING
TCP 192.168.0.161:1107    192.168.0.79:139       ESTABLISHED
TCP 192.168.0.161:1111    192.168.0.1:445        ESTABLISHED
UDP 0.0.0.0:135             *:*
UDP 0.0.0.0:445           *:*
UDP 0.0.0.0:1027          *:*
UDP 0.0.0.0:1033          *:*
UDP 192.168.0.161:137    *:*
UDP 192.168.0.161:138    *:*
UDP 192.168.0.161:500    *:*
C:\Pstools>_
```

[www.oisssg.org](http://www.oisssg.org)

- To identify the trojan binary / service
- Fport from Foundstone
- lsof in Unix

Carbonite from foundstone is a Linux kernel module to aid in RootKit detection, an lsof and ps at the kernel level. Carbonite "freezes" the status of every process in Linux's task\_struct, which is the kernel structure that maintains information on every running process in Linux.

```

C:\WINNT\System32\cmd.exe
C:\>fport
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid  Process          Port  Proto Path
---  -
392  svchost            -> 135  TCP  C:\WINNT\system32\svchost.exe
8    System            -> 139  TCP
916  FwSession         -> 261  TCP  C:\Program Files\CheckPoint\FireWall-1
    Agent\FwSession.exe
8    System            -> 445  TCP
632  MSTask            -> 1028 TCP  C:\WINNT\system32\MSTask.exe
644  alertsvc         -> 1032 TCP  C:\PROGRAM~1\Naunt\alertsvc.exe
8    System            -> 1083 TCP
8    System            -> 1107 TCP
8    System            -> 1111 TCP

392  svchost            -> 135  UDP  C:\WINNT\system32\svchost.exe
8    System            -> 137  UDP
8    System            -> 138  UDP
8    System            -> 445  UDP
220  lsass             -> 500  UDP  C:\WINNT\system32\lsass.exe
208  services          -> 1027 UDP  C:\WINNT\system32\services.exe
644  alertsvc         -> 1033 UDP  C:\PROGRAM~1\Naunt\alertsvc.exe

C:\>

```

## OISSG Recent Connections?

- Use nbtstat
- Recent connections are maintained in the cache
- Depends how lucky you are!

[www.oissg.org](http://www.oissg.org)

```
C:\WINNT\System32\cmd.exe
C:\>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.0.12] Scope Id: []

NetBIOS Remote Cache Name Table

Name                Type                Host Address        Life [sec]
-----
PALADION-PDC        <20> UNIQUE            192.168.0.1         430
PALADION-WRK22     <20> UNIQUE            192.168.0.22        75
PALADION            <1B> UNIQUE            192.168.0.1         57
192.168.0.22       <20> UNIQUE            192.168.0.22       232
192.168.0.19       <20> UNIQUE            192.168.0.19        2
C:\>_
```

## OISSG Listing all running processes

- Pslist from sysinternals
- High Expertise Required to identify rogue processes from normal ones

[www.oissg.org](http://www.oissg.org)

Most UNIX operating systems ship with a command-line tool called "ps" (or something equivalent) that administrators use to view detailed information about process CPU and memory usage. Windows NT/2K comes with no such tool natively, but you can obtain similar tools with the Windows NT Workstation or Server Resource Kits. The tools in the Resource Kits, *pstat* and *pmon*, show you different types of information, and will only display data regarding the processes on the system on which you run the tools. *PsList* is utility that shows you a combination of the information obtainable individually with *pmon* and *pstat*. You can view process CPU and memory information, or thread statistics.

What makes *PsList* more powerful than the Resource Kit tools is that you can view process and thread statistics on a remote computer.

*PsList* uses the Windows NT/2K performance counters to obtain the information it displays. It is a command line tool

```

C:\WINNT\System32\cmd.exe

C:\Pstools>pslist

PsList v1.12 - Process Information Lister
Copyright (C) 1999-2000 Mark Russinovich
Systems Internals - http://www.sysinternals.com

Process information for PALADION-WRK19:

Name           Pid Pri Thd  Hnd  Mem    User Time   Kernel Time   Elapsed Time
Idle            0  0  1    0    16    0:00:00.000  0:52:50.128  1:02:16.484
System          8  8  30  142   84    0:00:00.000  0:00:22.512  1:02:16.484
smss           132 11  6    33   92    0:00:00.050  0:00:01.261  1:02:16.484
csrss          160 13  9   284  1336  0:00:01.311  0:00:28.741  1:01:56.866
winlogon       180 13  14  335   828  0:00:01.121  0:00:03.975  1:01:54.593
services       208  9  33  510  1912  0:00:03.955  0:00:10.004  1:01:52.129
lsass          220  9  15  293   984  0:00:02.022  0:00:02.503  1:01:52.059
suchost        392  8  9   231   900  0:00:00.380  0:00:00.711  1:01:46.431
SFPOOLSU       416  8  11  156  2372  0:00:05.768  0:00:14.050  1:01:45.610
suchost        480  8  12  179   732  0:00:00.741  0:00:02.173  1:01:39.161
navapsc        504  8  8    67   828  0:00:01.161  0:00:03.444  1:01:38.730
npsvc          572  8  5    44   280  0:00:00.040  0:00:00.080  1:01:34.424
regsvc         612  8  2    30   156  0:00:00.010  0:00:00.060  1:01:31.970
mstask         632  8  6    92   608  0:00:00.100  0:00:00.410  1:01:31.330
alertsvc       644  8  13   96   280  0:00:00.160  0:00:00.330  1:01:18.681
explorer       788  8  14  328  5932  0:00:38.285  0:01:32.442  1:00:18.702
loadqm         800  8  5   143   192  0:00:00.240  0:00:01.161  1:00:02.128
msgmgmt        904  8  3    98   472  0:00:00.150  0:00:00.530  1:00:00.005
FMSession     916  8  2    33   480  0:00:00.090  0:00:00.350  0:59:58.923
navapw32       884  4  1    31   484  0:00:00.040  0:00:00.150  0:59:53.785
Vmsgr_tray    976  8  1    23   292  0:00:00.010  0:00:00.040  0:59:41.347
POWERPNT      264  8  6   188  3664  0:01:23.059  0:00:58.704  0:44:02.630
agentsvr       960  8  5    87   416  0:00:00.230  0:00:00.711  0:43:41.449
cmd            528  8  1    24  1332  0:00:00.370  0:00:01.462  0:33:28.182
WINWORD       984  8  4   194  3640  0:00:43.792  0:00:29.021  0:33:05.589
pslist         888  8  2    71  1228  0:00:00.060  0:00:00.190  0:00:00.931

C:\Pstools>_

```



- NTLast from Foundstone
- List successful/failed logons
- List local/remote logons
- Requires Logon/Logoff auditing to be turned on

- Reads saved .evt files - makes it easy to search through your archives
- Allows you to search before, after, and between dates - again to zoom in on something
- Filters logons 'From' a certain host - helps you zoom in on suspected intrusions
- Can save files in a csv format w/ time field formatted for Excel
- Filters out and distinguishes web log usage - cuts down search time

```

C:\WINNT\System32\cmd.exe
C:\>ntlast
Administrator PALADION-WRK19 PALADION-WRK19 Thu Sep 20 03:34:02pm 2001
Administrator PALADION-WRK19 PALADION-WRK19 Thu Sep 20 12:41:51pm 2001
vishal.pranjale PALADION-WRK19 PALADION Wed Sep 19 10:29:39pm 2001
Administrator PALADION-WRK19 PALADION-WRK19 Wed Sep 19 09:16:54pm 2001
Administrator PALADION-WRK19 PALADION-WRK19 Wed Sep 19 09:15:09pm 2001
vishal.pranjale PALADION-WRK19 PALADION Wed Sep 19 09:14:53pm 2001
Administrator PALADION-WRK19 PALADION-WRK19 Wed Sep 19 01:00:39pm 2001
Administrator PALADION-WRK19 PALADION-WRK19 Wed Sep 19 10:28:17am 2001
Administrator PALADION-WRK19 PALADION-WRK19 Tue Sep 18 07:11:48pm 2001
vishal.pranjale PALADION-WRK19 PALADION Mon Sep 17 08:27:58pm 2001

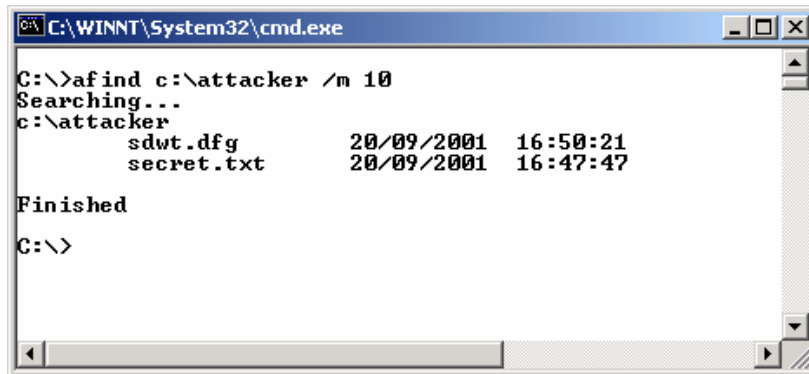
C:\>
    
```

## OISSG Finding Last Access Times

- Find out which files were accessed during the attack
- Afind, from Foundstone
- Specify directories / time range to search

[www.oissg.org](http://www.oissg.org)

AFind is the only tool that lists files by their last access time without tampering the data the way that right-clicking on file properties in Explorer will. AFind allows you to search for access times between certain time frames, coordinating this with logon info provided from ntlast, you can to begin determine user activity even if file logging has not been enabled



```
C:\WINNT\System32\cmd.exe
C:\>afind c:\attacker /m 10
Searching...
c:\attacker
      sdwt.dfg          20/09/2001  16:50:21
      secret.txt       20/09/2001  16:47:47

Finished
C:\>
```

The output of the “afind” command is shown in the figure.

## OISSG Capture Event Log entries

- Dumpevt from Somarsoft
  - Dumps the eventlog in a format suitable for importing into a database
  - Dumps any of the 3 event logs

[www.oissg.org](http://www.oissg.org)

## OISSG A Warning about Event Logs

- By default, NT/2000 event logs restrict each log file to 512 KB and 7 days
- After limit is reached, file is closed and must be cleared.
- Make sure to change the settings for each file, individually

[www.oissg.org](http://www.oissg.org)

In Windows NT/2000 log files size is 512 KB by default and after 7 days it will be closed & must be cleared. Settings for these must be changed individually.

## OISSG Review Key Registry Entries

- Look for specific registry values for clues
- Dumping entire registry is inefficient
- Reg query from NT Resource Kit

[www.oissg.org](http://www.oissg.org)

● Eg. To get recent files used

Reg query

“HKCU\Software\Microsoft\Office  
\9.0\Powerpoint\Recentfilelist”

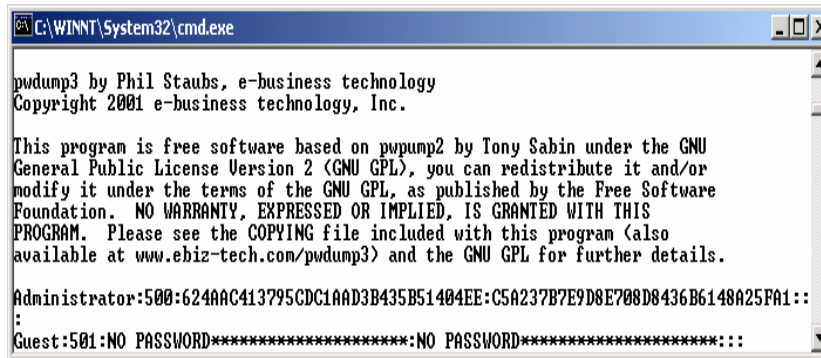


- Need for user passwords, if user is not co-operating
- PWDump by Todd Sabin
- Dumps sam database
- Database can be cracked with John the Ripper, or l0phtcrack

Pwdump: tool to extract password hashes from the registry. By Jeremy Allison.

Pwdump2: tool to extract password hashes from the registry whether or not SYSKEY is enabled on the system.

Samdump: tool to extract password hashes from SAM files.



```
C:\WINNT\System32\cmd.exe

pwdump3 by Phil Staubs, e-business technology
Copyright 2001 e-business technology, Inc.

This program is free software based on pwpump2 by Tony Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Administrator:500:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1::
:
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
```

The output of the “pwdump3” command is shown in the figure.

- Keep a toolkit handy
- Keep a clean set of floppies
- Practice the tools beforehand

Questions?

[www.oissg.org](http://www.oissg.org)

Thanks for your time

...

[www.oissg.org](http://www.oissg.org)