OISSG

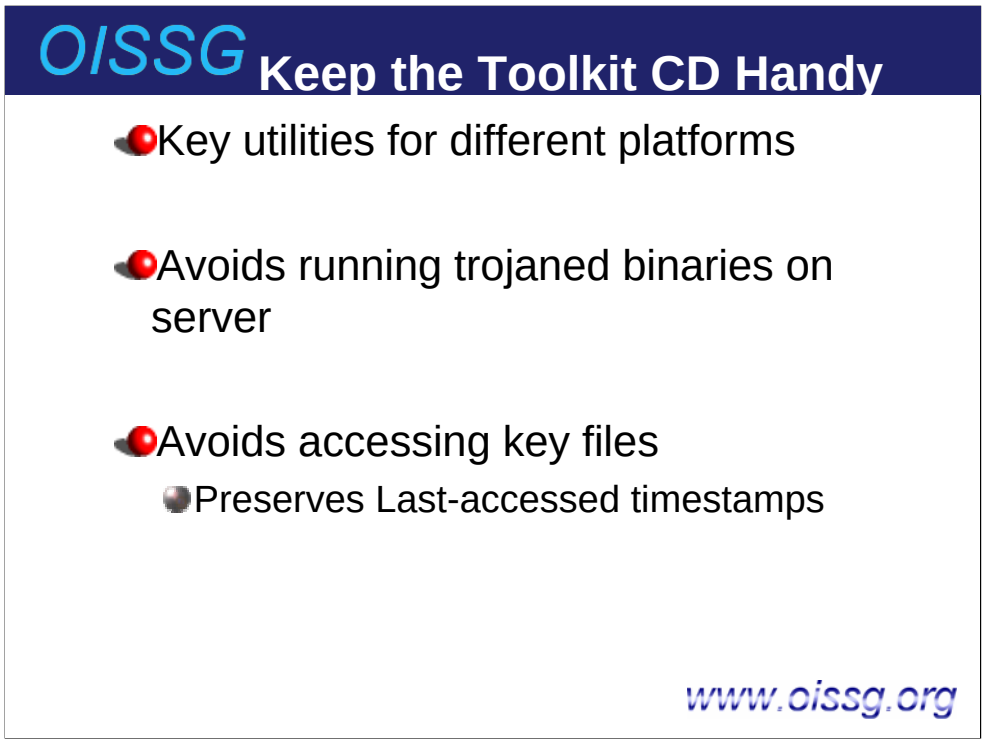
Incident Response Toolkit
:
Initial Response

Sunday, August 24, 2003

Balwant Rathore, CISSP
Founder,
Open Information System Security Group
www.oissg.org

Index

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



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.

OISSG

Sample Toolkit for WinNT

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

www.oissg.org

OISSG Tips on Information Gathering

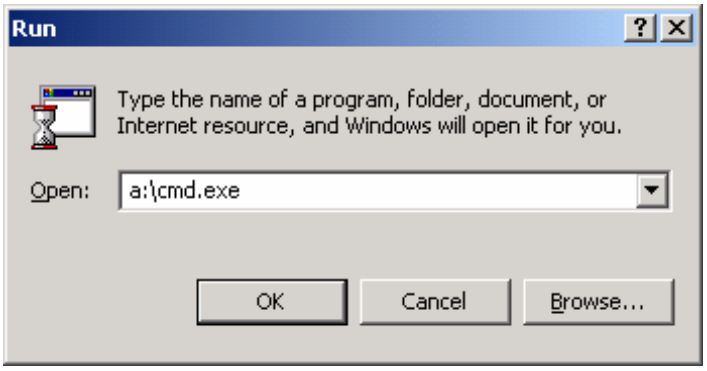
- Save data to floppy
  - Overwriting data on hard-disk might lose valuable info
- Record the data gathered, in a notebook
- Use netcat / cryptcat to send data to a forensic workstation

www.oissg.org

OISSG

The first step…

- Executing a trusted command shell



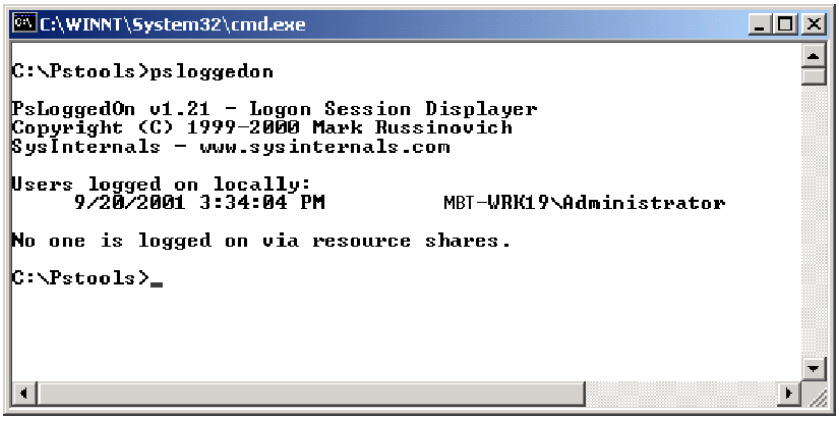
www.oissg.org

OISSG Who have logged on?

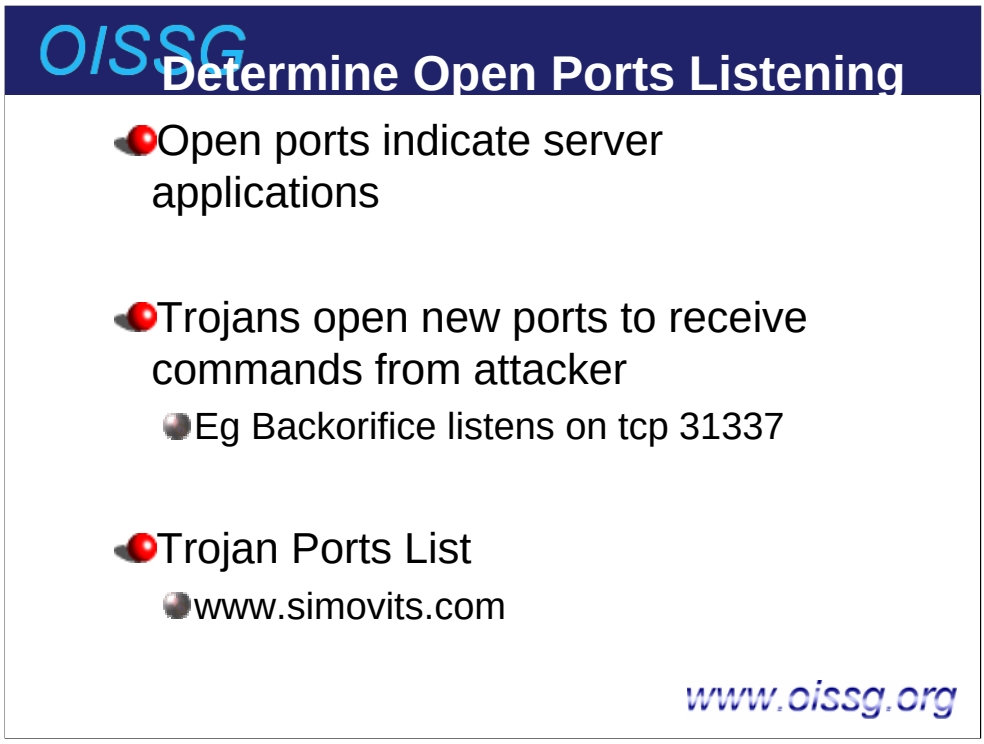
- Psloggedon utility from ‘sysinternals’
  - A utility that shows all users connected locally and remotely
- Rasusers
  - To list users logged in via Remote Access Service

www.oissg.org

OISSG Psloggedon output

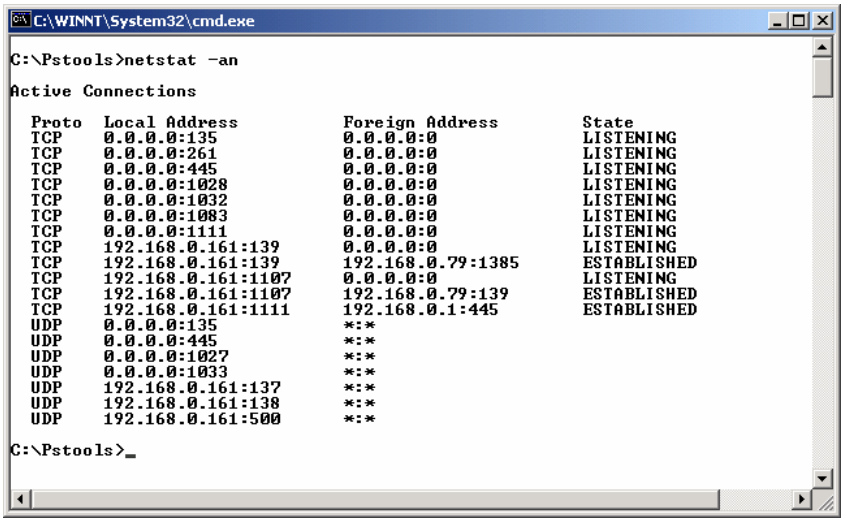


www.oissg.org



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



www.oissg.org

OISSG

Which application is listening on port?

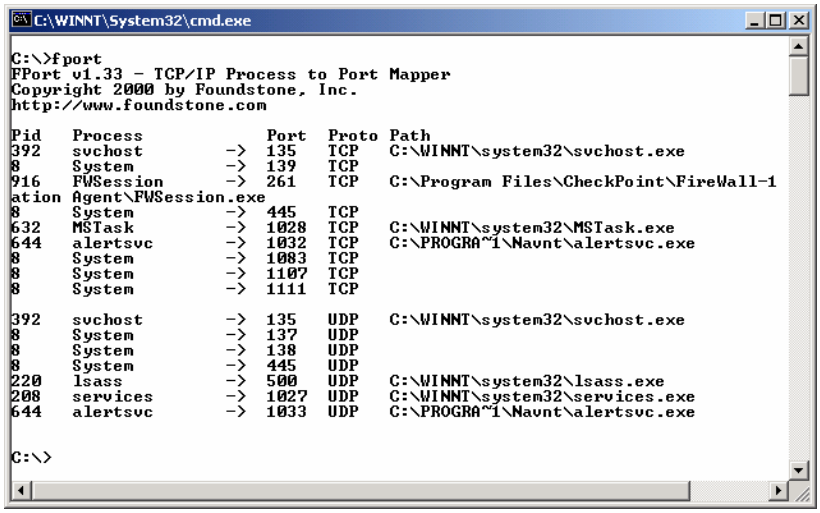
- To identify the trojan binary / service
- Fport from Foundstone
- lsof in Unix

www.oissg.org

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.

OISSG

Fport Output



www.oissg.org

OISSG

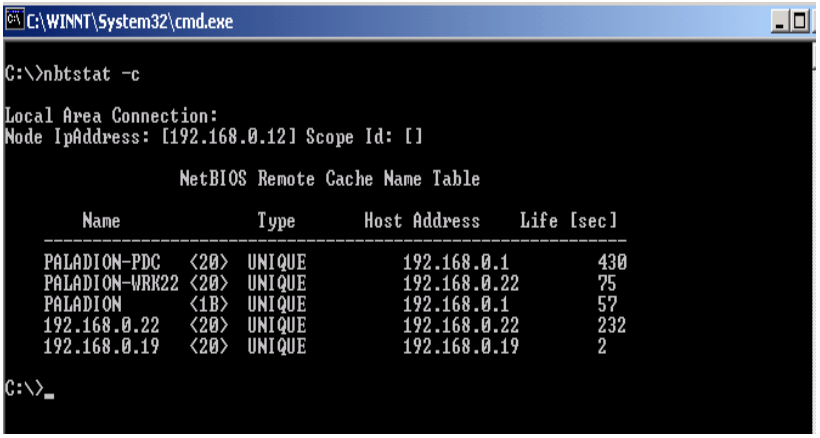
Recent Connections?

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

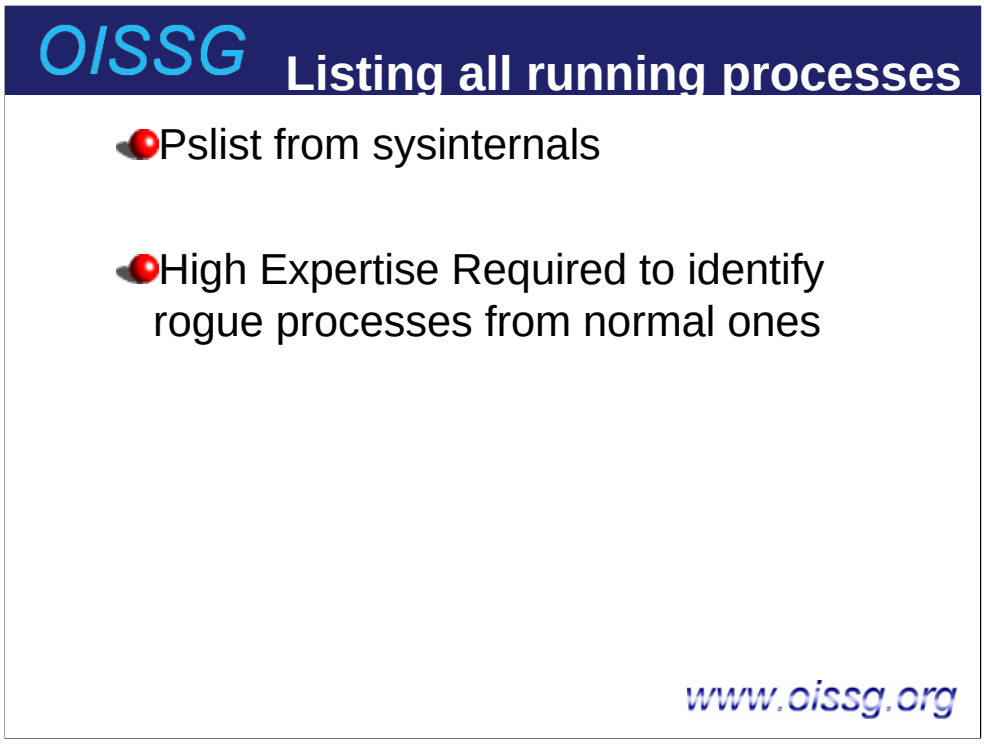
www.oissg.org

OISSG

nbtstat Output



www.oissg.org



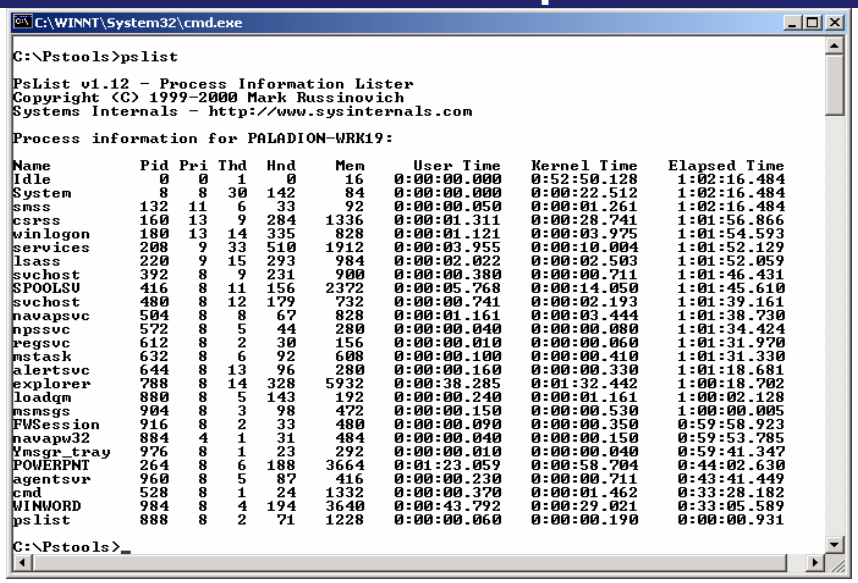
Most UNIX operating systems ship with a command-line tool called "ps" (or something equivalent) that administrators use to view detailed information about process CPU and memory usage. Windows NT/2K comes with no such tool natively, but you can obtain similar tools with the Windows NT Workstation or 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.

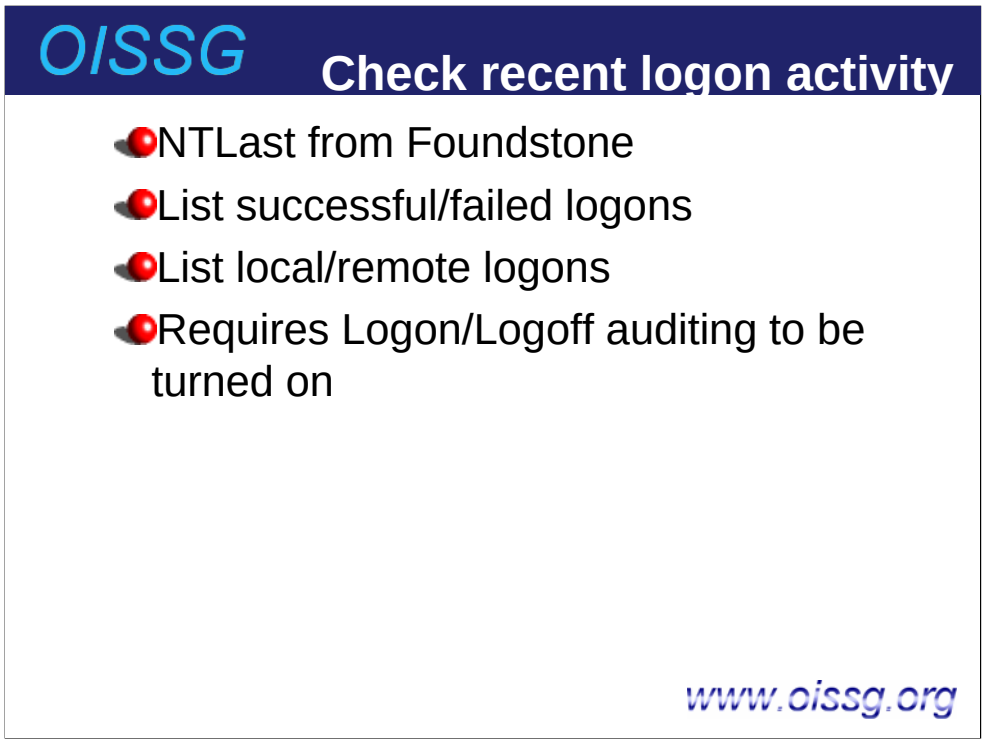
PsList uses the Windows NT/2K performance counters to obtain the information it displays. It is a command line tool

OISSG

PSList output



www.oissg.org



• 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

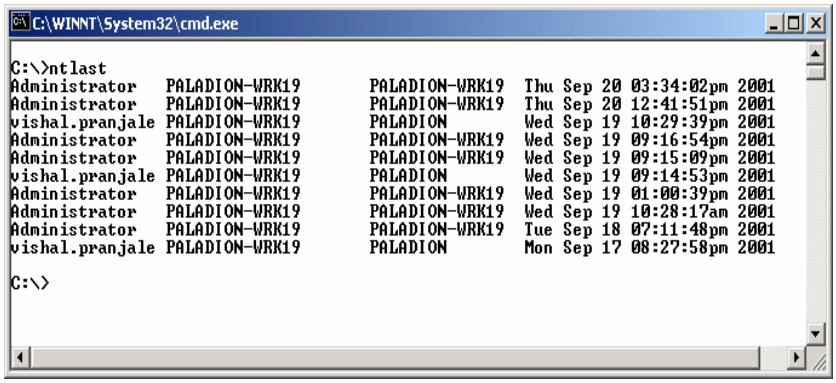
• Filters logons 'From' a certain host - helps you zoom in on suspected intrusions

• Can save files in a csv format w/ time field formatted for Excel

•Filters out and distinguishes web log usage - cuts down search time

OISSG

NTLast Output



www.oissg.org

OISSG Finding Last Access Times

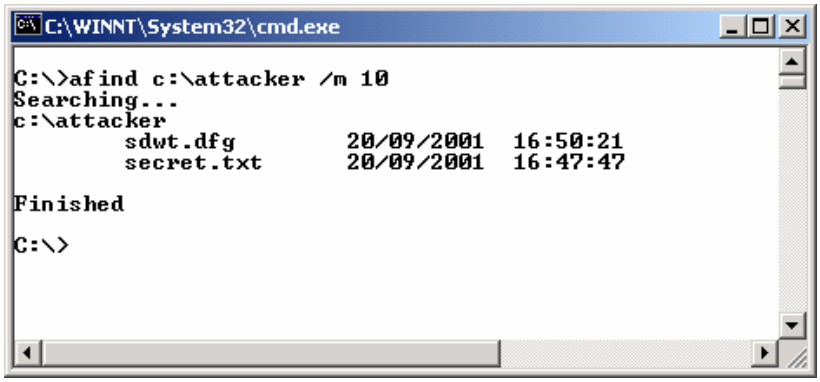
- Find out which files were accessed during the attack
- Afind, from Foundstone
- Specify directories / time range to search

www.oissg.org

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

OISSG

Afind Output



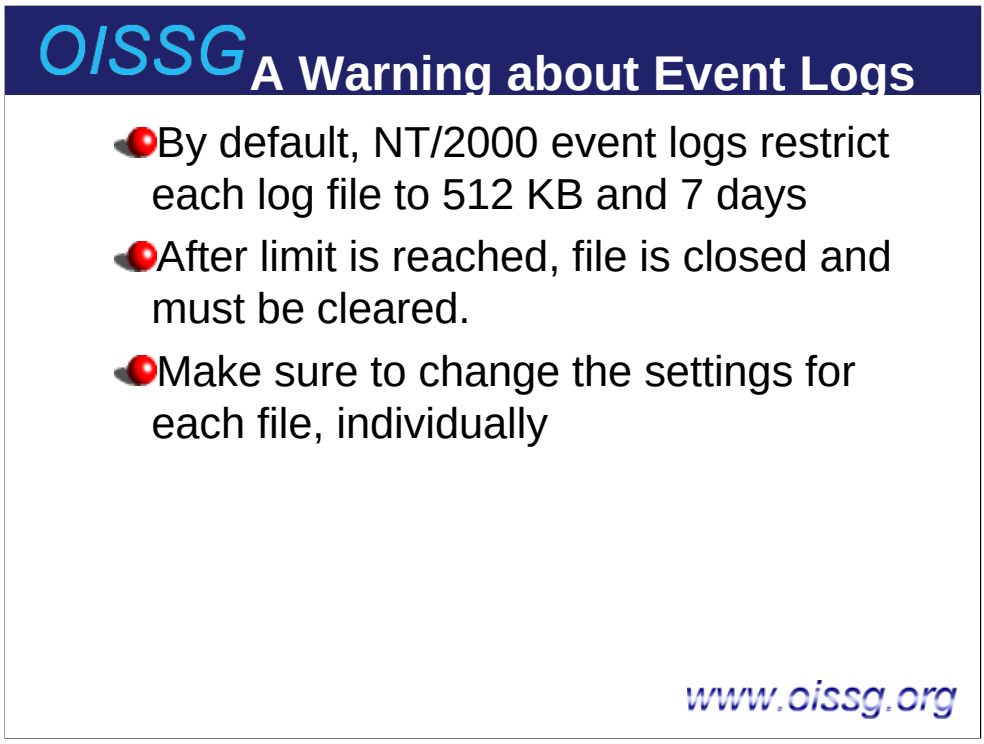
www.oissg.org

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



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

OISSG

Using reg query

- Eg. To get recent files used

Reg query
"HKCU\Software\Microsoft\Office
\9.0\Powerpoint\Recentfilelist"

www.oissg.org

OISSG Obtaining System Passwords

- 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

www.oissg.org

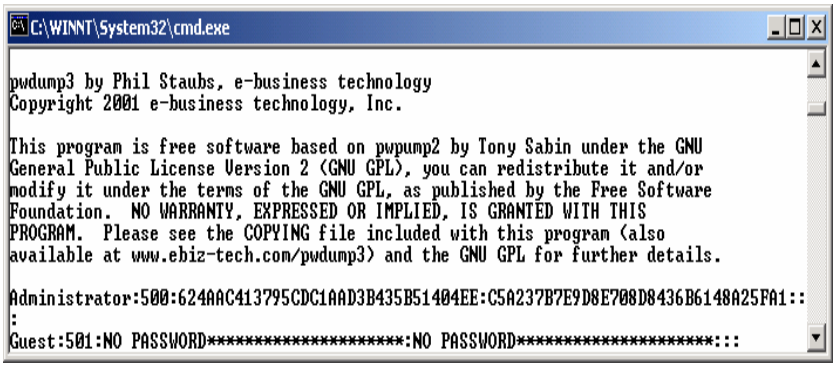
Pwdump: tool to extract password hashes from the registry. By Jeremy Allison.

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.

OISSG

Pwdump3 Output



www.oissg.org

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

OISSG

Summary

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

www.oissg.org

OISSG

Questions?

www.oissg.org

OISSG

Thanks for your time

…

www.oissg.org