Analyzing 0-day Hacker Tools (For Dummies)

Dynamic Analysis of Windows Binaries

Johnny Long
johnny@ihackstuff.com

The Problem

- Not everyone's a programmer
- Not all tools have been categorized
- The 'establishment' takes too long in some cases…
  - "We need to know what this thing is… ASAP! Oh, and we don't want to spend any money outsourcing…"
- Even YOU could get a 0-day
- Some pros insist that this analysis is 'geek magic'… it doesn't have to be.

Requirements

- **It helps if you know:**
  - **Windows concepts: files, registry**
  - **Network concepts: Ports, subnets, connections**
  - **Hacker tools: Backdoors, Trojans, Rootkits, Exploits**
    - **Know the difference between tool types so you can spot trends and similarities when doing your analysis.**

Tools of the trade

- **There are many tools that do the things we need, but here's a few "must-haves" in my opinion:**
  - **VMWare / Virtual PC**
  - **Regmon, Filemon, Process Explorer, PsList, TcpView / TcpVcon, DebugView, TDIMon**
  - **ListDLLs**
  - **FPORT**
  - **Anti-Virus, optional (yes, optional!)**
  - **Ethereal / tcpdump**

The Process

- **First, set the stage:**
  - **Build an analysis environment (VMWare / VPC)**
  - **Create a *closed* monitoring network**
- **Run the hacker tool through it's paces:**
  - **Run some monitoring tools**
  - **Launch the 0-day**
  - **Check monitoring tools for activity (variable duration)**
  - **Shutdown 0-day (optional)**
  - **Pause monitor tools**
  - **Analyze results of monitors and hacker tool**
  - **Repeat if needed**

Build The Environment

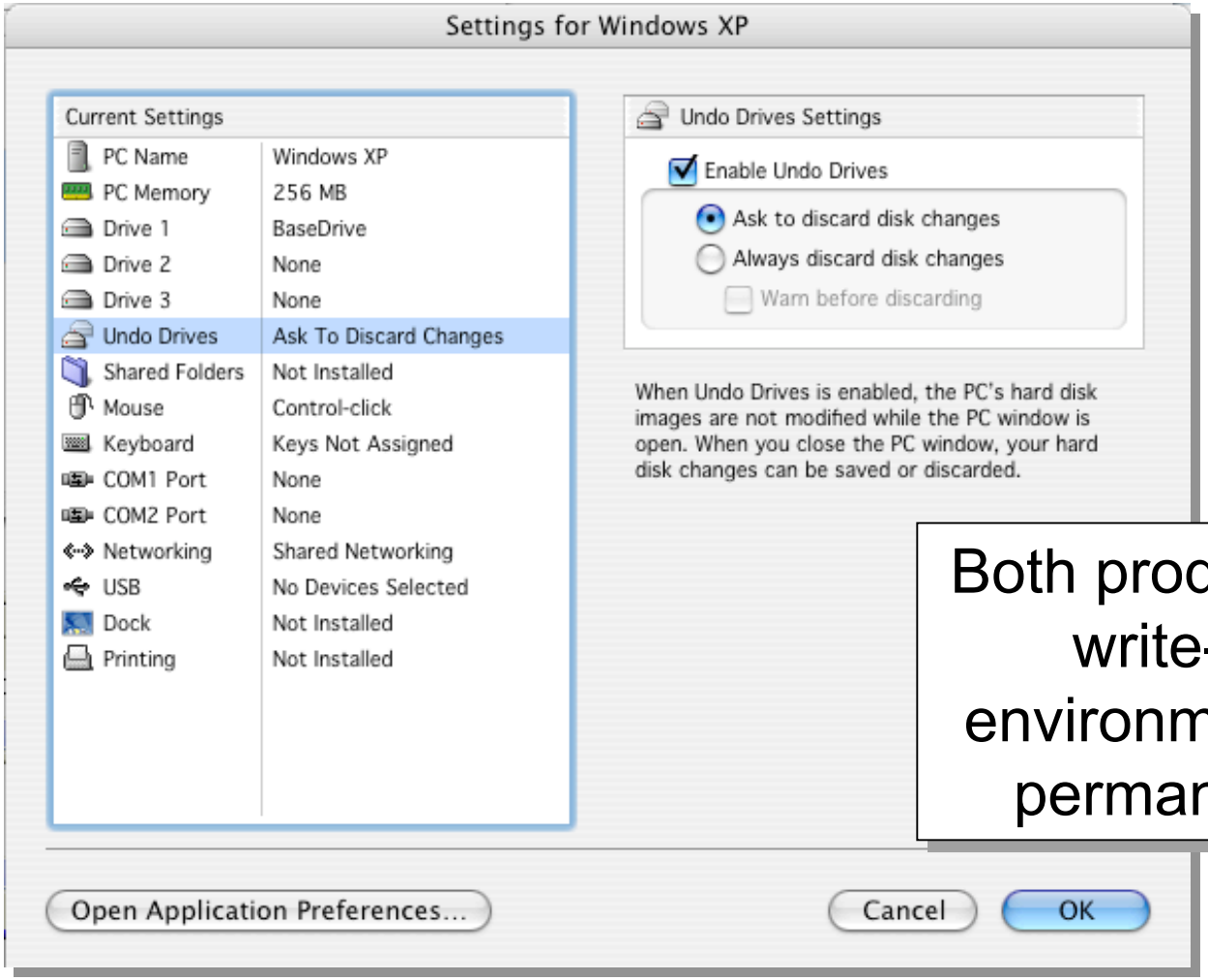
- **We need to create a safe environment for our dangerous dissection.**
- **VirtualPC for Windows or Mac**
  - **www.apple.com/macosx/applications/virtualpc/**
  - **www.microsoft.com/windows/virtualpc/default.mspx**
- **Vmware for Windows or Linux**
  - **www.vmware.com**

Build The Environment

- **Both products allow for the installation of a virtual machine we can work inside of (in this case Windows XP)**
- **Both products allow for a “write protected” environment to prevent permanent system changes.**

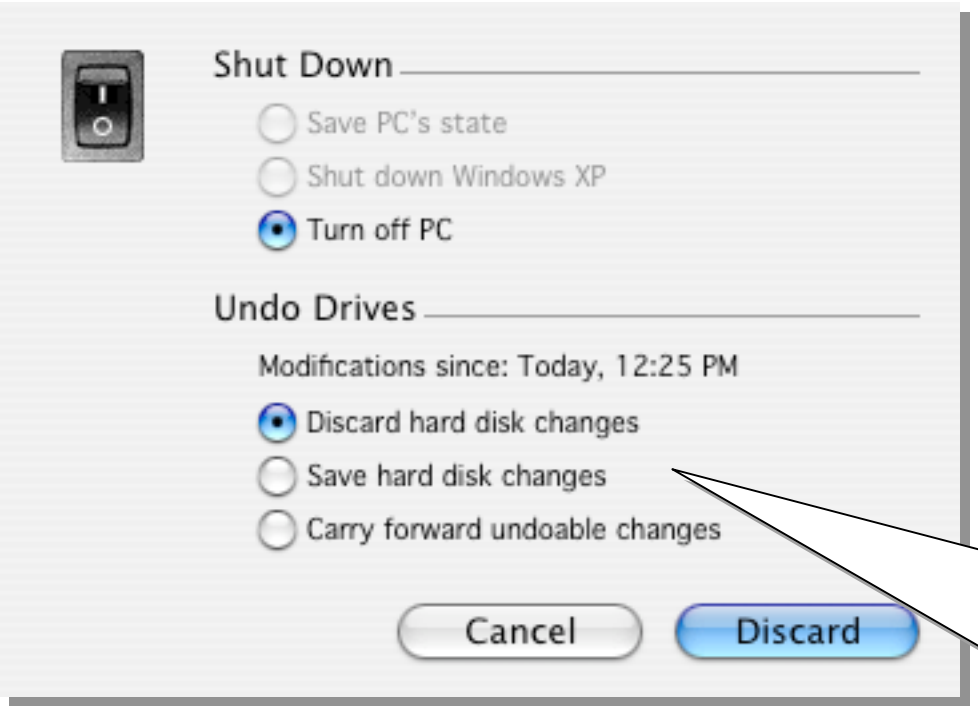
Virtual Windows XP

Write-Protect



Both products allow us to write-protect our environment, preventing permanent changes.

Write-Protect



Changes can be discarded when the VirtualPC is powered down. Vmware calls this *nonpersistent* mode.

Write-Protect

- Even though we can undo changes, we should still approach this box with standard forensic good sense.
- Keep all trusted tools on write-blocked medium (like a CD).
- Don’t trust any system tools after mucking with malicious code…
- Am I preaching to the choir yet?

Create Closed Network

- You'll most likely need a network connection when monitoring the tool.
- If the tool connects to the network, you'll want to know about it. Without a network connection, you'll miss this activity.
- The network should not connect to the Internet. If the tool attacks someone from you're machine, guess who may be liable?
- You may need to make changes to your network (host addresses, names, default routes) if the tool fails to perform a network function correctly.
- "Phantom" services, like netcat listening on a port, can be handy if you want to "fake" a listening service.
  - Example: If the tool wants to connect to a specific mail server, change the IP of a test server to the mail server's address, run netcat listening on port 25, and "play the role" of a mail server to see what the tool does.

A note on virus software

- **Since we're working with malicious code, you may not want to run a virus scanner / spyware detector in the VirtualPC.**
- **Even though our code is zero-day, a stray signature could still keep us from getting any work done, blocking access to our hacker tool.**

The Cast

- **The hacker tool…**

C:\WINDOWS\System32\cmd.exe

```
Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-63C1

 Directory of Z:\die

12/08/2004  12:30 PM    <DIR>          .
12/08/2004  12:30 PM    <DIR>          ..
07/10/2004  12:14 PM           127,184 dnconfig.dll
06/09/2004  01:02 PM                80 dnconfig.ini
06/09/2004  10:55 AM             7,936 dnconfig.sys
               3 File(s)        135,200 bytes
               2 Dir(s)  26,778,767,360 bytes free

Z:\die>
```

Our evil code consists of three files. Notice there is no EXE file.

The Cast

- **The INI file…**

C:\WINDOWS\System32\cmd.exe

```
Z:\die>type dnconfig.ini
[FS]
dnconfig

[SVC]
dnconfig

[REGISTRY]
dnconfig

[PROCESS]
dnconfig
Z:\die>
```

The INI file isn't much to write home about, yet…

A note on the strings command

- **Linux / UNIX commands like *strings* is often used to 'analyze' binaries.**
- **Don't believe the hype.**
- **Use cautiously anything found with *strings…* a hacker could *plant* information in the binary to "bait" you.**
- **Never connect to sites found in the binary unless you're properly proxied. The attacker could be watching for this…**

Strings

```
Terminal — more — 80x24
SeDebugPrivilege
I: IeDEnter  called
winlogon.exe
services.exe
I: [%d]WSARecv backdoor ident in %d !!!!!!!!!!
kikasdikikdkkdnv3i8pmu7290adii8b
I: Connected in Accept %d
I: IeDConfigData: %d, %d, %s, %d, %s, %s
I: Create process [%s], code %d
command.com
get <RemoteFilePath> [LocalDir]   - download file
put <LocalFilePath> [RemoteDir]   - upload file [default dir is %tmp%]
cmd [RemoteAppFileName]           - run console program [default cmd.exe]
ps                                - list process
pskill [ProcessName or ProcessID] - kill process
reboot                            - reboot remote host
halt                              - shutdown remote host
clean                             - clean spi hook and run flag
host                              - show host process
showconfig                        - show ixd config info
?                                 - show this
E: Read file failture, code: %d
E: Open file failture, code: %d
byte 5066
```

Running **strings -8** on our DLL file reveals *possible* functions. Remember: text could be faked. File this away for later…

Strings

```
Terminal — more — 80x24
E: Write file failture, code: %d
I: Put File,  %d bytes saved to %s
E: Create file failture, code: %d
E: Write pipe error
E: Read pipe error
E: Create process failture
E: Idle 60s timeout, disconnected
E: reboot failture errno: %d
IeD.Ident.N
KeyLogFile
NetLogFile
showconfig
I: command %s
NC, http://www.sunx.org
I: socket connect handle %06x
E: Read file failture, code: %d
E: Open file failture, code: %d
E: Write file failture, code: %d
I: Get file, %d bytes saved to %s
E: Create file failture, code: %d
E: Data format error, bad magic
E: Data recv error
I: Input "%s"
byte 5640
```

Certain strings can lead to a wild goose chase. Be careful what you connect to….

Strings

```
Terminal — more — 80x24
E: Tcp connect failture
E: ConnectTo (Auth by inside masterkey) only support tcp
E: Connect failture
E: Shell exited
I: Incoming ixd 0x%08x:%d
cli: direct %d, proto %d, host %s, port %d, magickey %d, localport %d
E: bad local port
Usage: rundll32 ixd.dll cli <direct> <proto> <host> <port> [localport]
  rundll32 ied.dll cli 1 6 10.0.0.1 999 99
E: bad port
Usage: rundll32 ixd.dll cli <direct> <proto> <host> <port> [localport]
  rundll32 ied.dll cli 1 6 10.0.0.1 999 99
E: bad host
Usage: rundll32 ixd.dll cli <direct> <proto> <host> <port> [localport]
  rundll32 ied.dll cli 1 6 10.0.0.1 999 99
E: bad proto
Usage: rundll32 ixd.dll cli <direct> <proto> <host> <port> [localport
  rundll32 ied.dll cli 1 6 10.0.0.1 999 99
E: bad direct
Usage: rundll32 ixd.dll cli <direct> <proto> <host> <port> [localport
  rundll32 ied.dll cli 1 6 10.0.0.1 999 99
          # for server side Auth by inside masterkey
          # will connect to 10.0.0.1 80
byte 7093
```

Usage information about the tool is often found with strings….

Dependency Walker

- **Since all we have is a DLL, we'll be running that, but first we need to know what functions the tool is capable of performing.**
- **Strings sucks at this.**
- **Dependency Walker (http://www.dependencywalker.com/) is great for getting inside Windows binaries, but it's not for the feint of heart.**
- **Relax…Simply opening a program in this tool *does not* launch the malicious program.**

Dependency Walker

Simply loading the DLL file reveals available functions and external DLL's that are loaded.

Dependency Walker - [dnconfig.dll]

File Edit View Options Profile Window Help

DNCONFIG.DLL
KERNEL32.DLL
USER32.DLL
PSAPI.DLL
RPCRT4.DLL
WS2_32.DLL
ADVAPI32.DLL

PI	Ordinal ^	Hint	Function	Entry Point

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	Inj	0x0000593E
C	2 (0x0002)	1 (0x0001)	WSPStartup	0x000014F4
C	3 (0x0003)	2 (0x0002)	clean	0x
C	4 (0x0004)	3 (0x0003)	cli	
C	5 (0x0005)	4 (0x0004)	inst	
C	6 (0x0006)	5 (0x0005)	reload	

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.
	MPR.DLL	08/18/2001 7:00p	08/18/2001 12:33a	55,808	A
	ADVAPI32.DLL	08/18/2001 7:00p	08/18/2001 12:33a	549,888	A

Warning: At least one module has an unresolved import due to a missing export function in a delay-load

For Help, press F1

These function names are important. We'll need these when it comes time to run the hacker tool…

Google

- **Google is your friend.**
- **Don’t forget to run any ‘interesting’ strings through Google.**
- **Since this is (was) a zero-day, Google won’t be much help, especially if the code is original.**
- **Again, remember not to connect to sites (even sites found with Google) without being proxied… Google’s cache is *NOT* anonymous.**

The monitors

- The program's we'll look at now are designed to monitor your system for changes.
- Remember, this is a process:
  - Run the monitoring tools
  - Launch the 0-day
  - Check monitoring tools for activity (variable duration)
  - Shutdown 0-day (optional)
  - Pause monitor tools
  - Analyze results of monitors and hacker tool
  - Repeat if needed

Filemon

File Monitor - Sysinternals: www.sysinternals.com

File Edit Options Volumes Help

#	Time	Process	Requ...	Path	Result	Othe
24	1:20:54 PM	cmd.exe:176	DIRECT...	C:\WINDOWS\System32\	SUCCESS	FileBc
25	1:20:54 PM	cmd.exe:176	CLOSE	C:\WINDOWS\System32\	SUCCESS	
26	1:20:54 PM	cmd.exe:176	OPEN	C:\WINDOWS\system32\rundll32.exe...	FILE NOT F...	Optio
27	1:20:54 PM	cmd.exe:176	CLOSE	C:\WINDOWS\system32\rundll32.exe	SUCCESS	
28	1:20:54 PM	rundll32.exe:1448	QUERY...	C:\WINDOWS\System32\rundll32.exe	SUCCESS	FileN
29	1:20:54 PM	rundll32.exe:1448	OPEN	C:\WINDOWS\Prefetch\RUNDLL32....	SUCCESS	Optio
30	1:20:54 PM	rundll32.exe:1448	QUERY...	C:\WINDOWS\Prefetch\RUNDLL32....	SUCCESS	Lengt
31	1:20:54 PM	rundll32.exe:1448	READ	C:\WINDOWS\Prefetch\RUNDLL32....	SUCCESS	Offse
32	1:20:54 PM	rundll32.exe:1448	OPEN	C:	SUCCESS	Optio
33	1:20:54 PM	rundll32.exe:1448	QUERY...	C:	SUCCESS	FileFs
34	1:20:54 PM	rundll32.exe:1448	OPEN	C:\	SUCCESS	Optio
35	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\	SUCCESS	FileN
36	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\	NO MORE ...	FileN
37	1:20:54 PM	rundll32.exe:1448	OPEN	C:\WINDOWS\		Optio
38	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\		
39	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\		
40	1:20:54 PM	rundll32.exe:1448	OPEN	C:\WINDOWS\SYSTEM32\		
41	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\SYSTEM32\		
42	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\SYSTEM32\		
43	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\SYSTEM32\		
44	1:20:54 PM	rundll32.exe:1448	DIRECT...	C:\WINDOWS\SYSTEM32\		

Filemon, available from www.sysinternals.com shows all file activity on a Windows system.

Filemon

- **Filemon is designed to be run while a process you want to monitor is being run.**
- **Filemon, like the other monitors we'll look at, should be run before launching our malicious code.**
- **Let's look at filemon's output..**

Filemon

Entry Number. Sequential.

Request: Open, Close, Directory, Write, etc

Details of file access result (if available)

#	Time	Process	Requ...	Path	Result	Othe
24	1:20:54 PM	cmd.exe:176	DIRECT...	C:\WINDOWS\System32\	SUCCESS	FileBo
25	1:20:54 PM	cmd.exe:176	CLOSE	C:\WINDOWS\System32\	SUCCESS	
26	1:20:54 PM	cmd.exe:176	OPEN	C:\WINDOWS\system32\rundll32.exe...	FILE NOT F...	Optio
27	1:20:54 PM	cmd.exe:176	CLOSE	C:\WINDOWS\system32\rundll32.exe	SUCCESS	

Time captured (or delta)

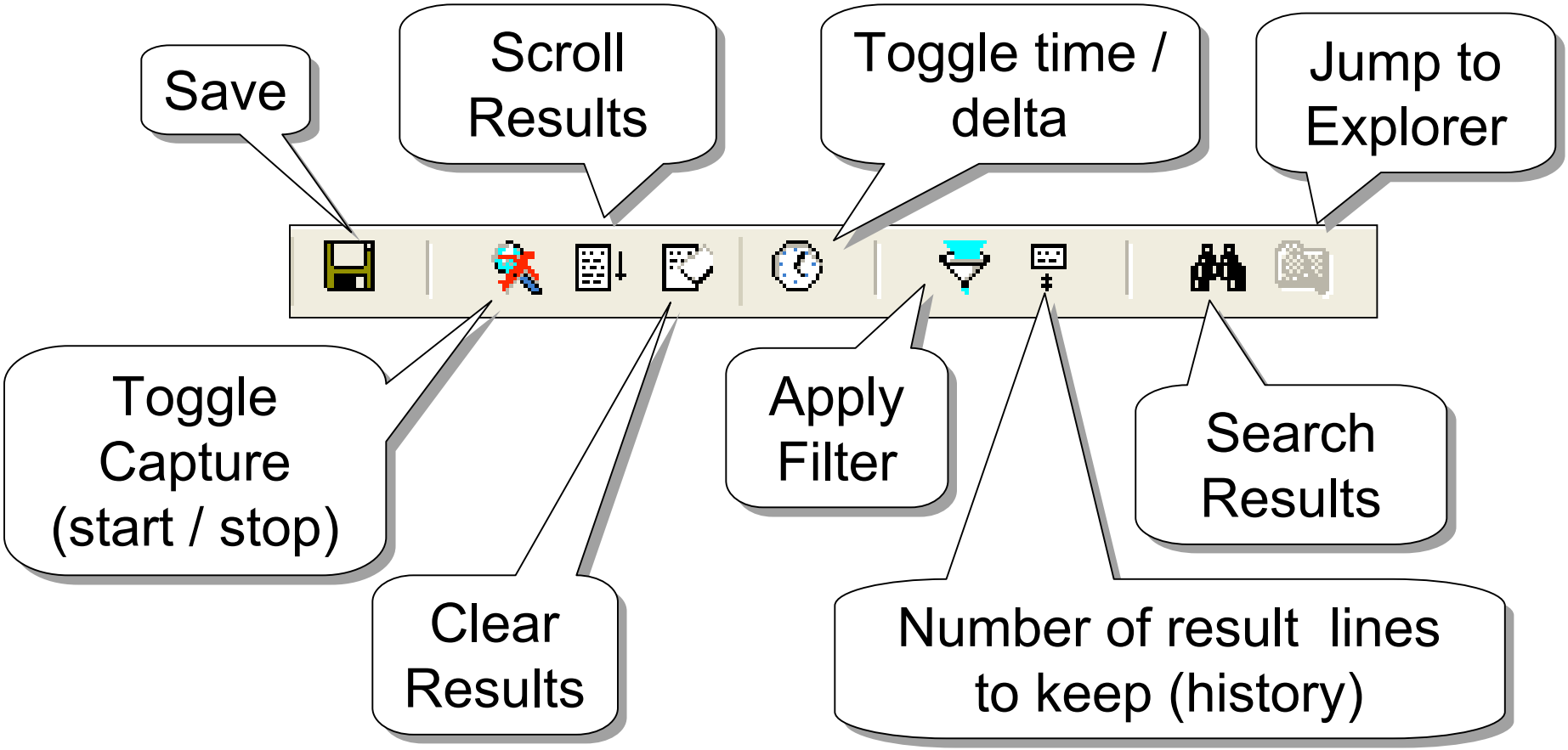
Process name and ID

Path of file accessed

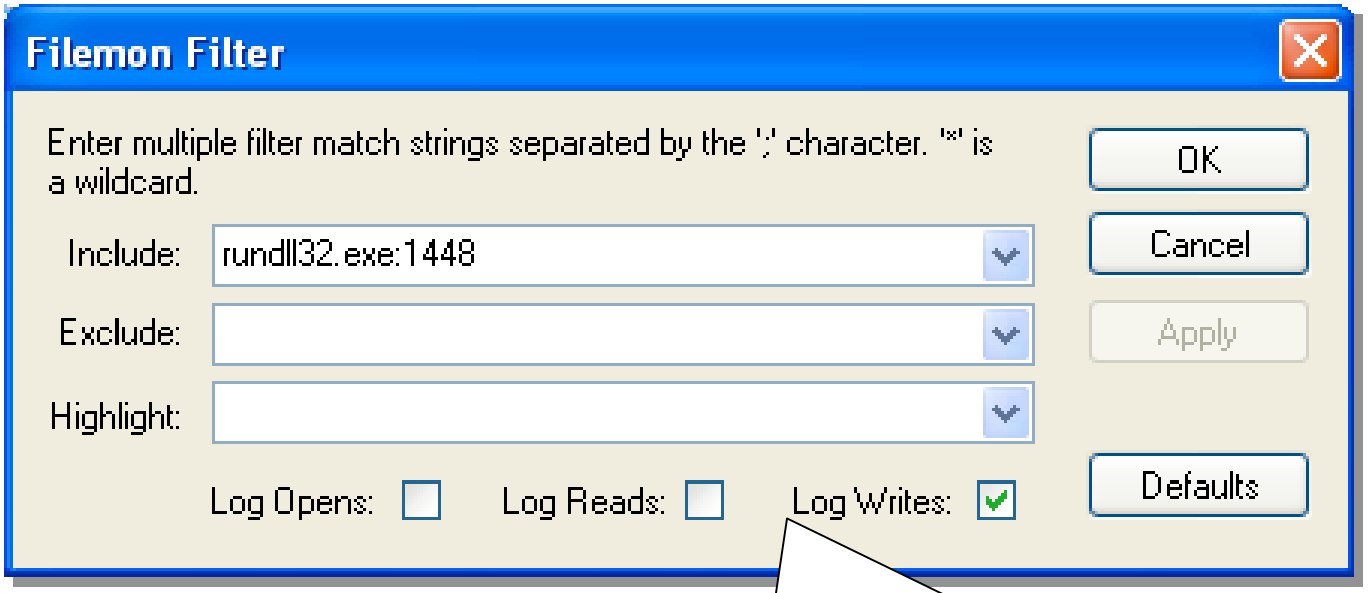
Result of file or directory access or error description

Filemon

- **Filemon and Regmon have similar controls:**

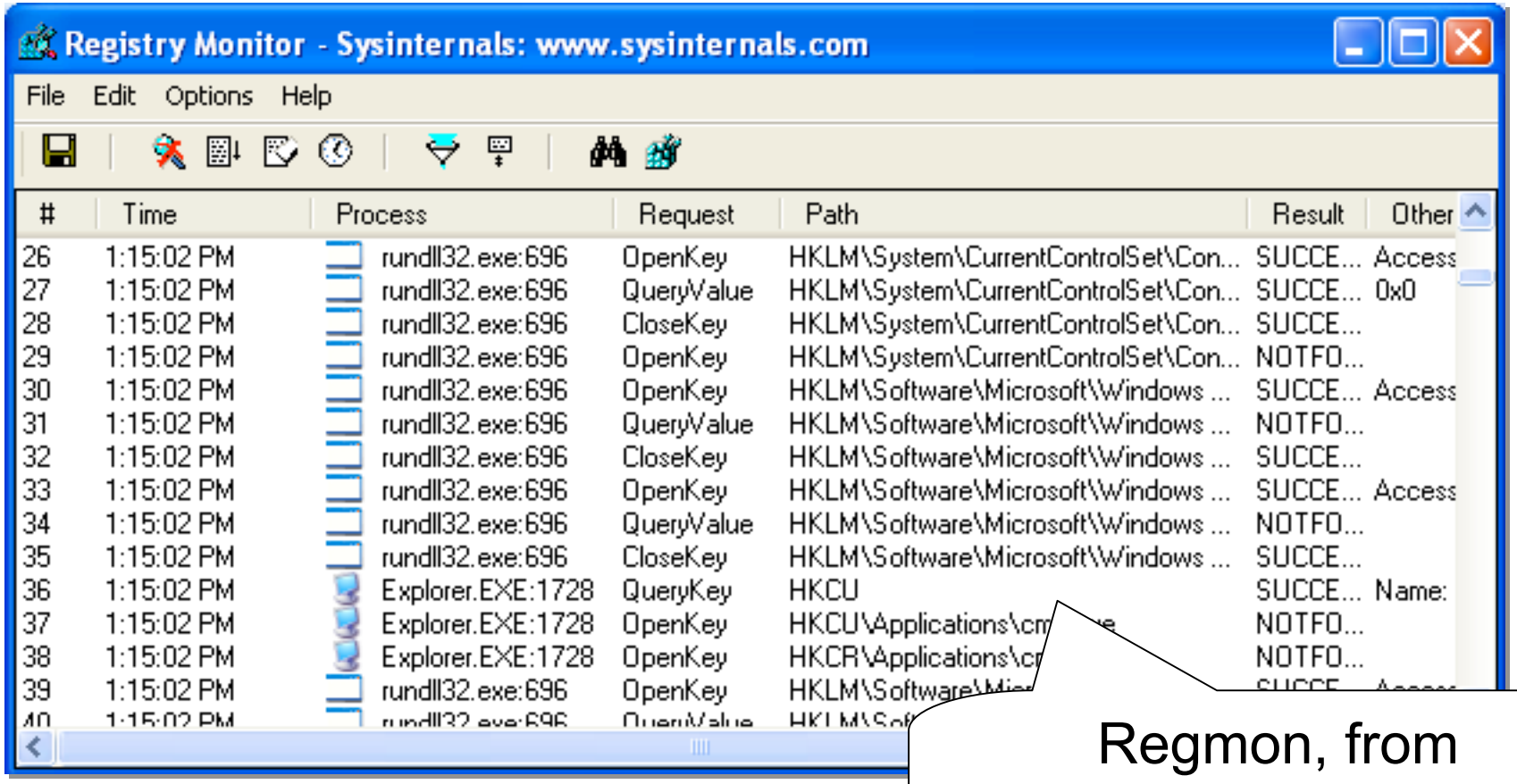


Filemon



Filemon and regmon allow filters to narrow the ‘signal’ from the ‘noise’.

Regmon

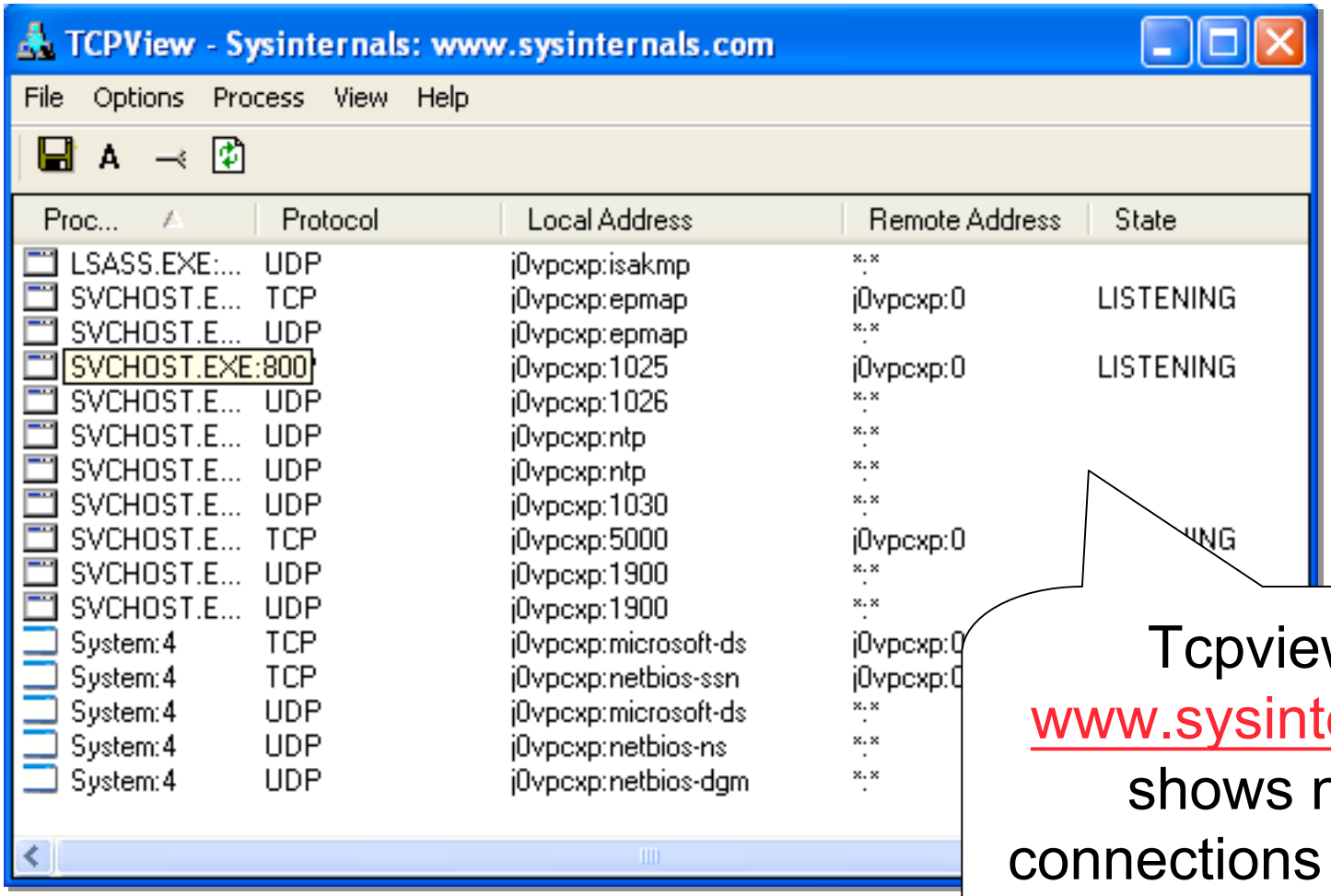


Regmon, from www.sysinternals.com, monitors registry access

Sniffing

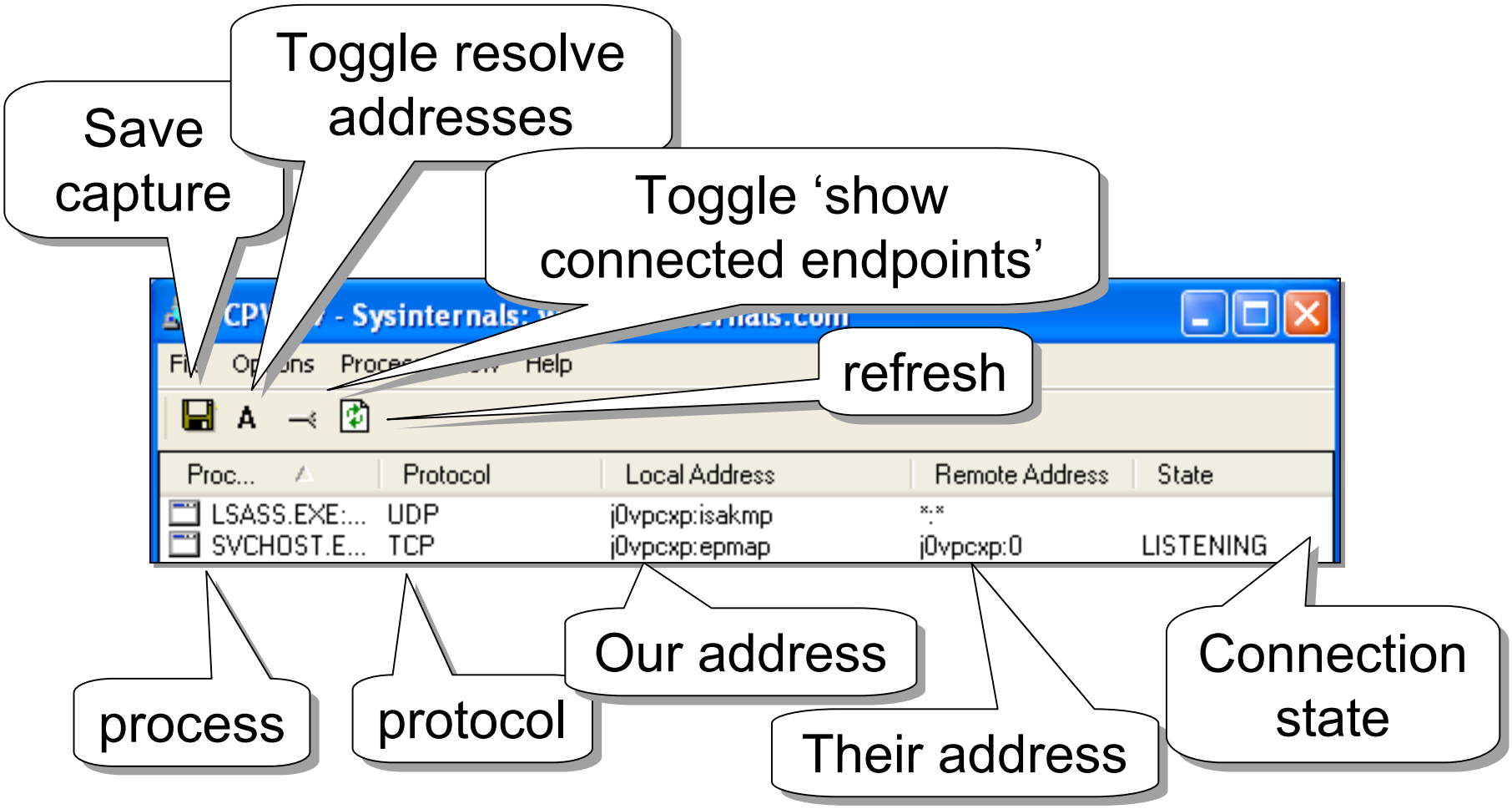
- **There are too many sniffers to list, but a network sniffer should also be run to watch for network activity.**
- **Ethereal, from www.ethereal.com or TCPView from www.sysinternals.com could be used for this task.**

TCPView



Tcpview from www.sysinternals.com shows network connections to and from your machine

TCPView


Save capture
Toggle resolve addresses
Toggle 'show connected endpoints'
refresh
Help
Proc...
Protocol
Local Address
Remote Address
State
LSASS.EXE:...
UDP
j0vpcxp:isakmp
:
SVCHOST.E...
TCP
j0vpcxp:epmap
j0vpcxp:0
LISTENING
process
protocol
Our address
Their address
Connection state

TCPView

- **TCPView is great, especially if you're not a network-head**
- **TCPView won't show details, which a tool like Ethereal can.**

Time to run the tool…

Rundll32

- **There is no executable, so we're forced to analyze the SYS and DLL files.**
  - **The DLL file is our "executable".**
- **We can test out our DLL by running it with the windows command *rundll32.***
  - **(If we were investigating an EXE, we could launch the program by just running it.)**

Warning!!!

- **At this point, we're about to launch the malicious code!**
- **Be forewarned that EVERYTHING on this VirtualPC should be considered suspect after this point!**
- **Ensure the VPC is set up to prevent saving of data at shutdown.**

Rundll32

C:\WINDOWS\System32\cmd.exe

```
Z:\die>rundll32 dnconfig.dll

Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-58F0

 Directory of Z:\die

12/08/2004  10:57 AM    <DIR>          .
12/08/2004  10:57 AM    <DIR>          ..
07/10/2004  12:14 PM           127,184 dnconfig.dll
06/09/2004  01:02 PM                80 dnconfig.ini
06/09/2004  10:55 AM             7,936 dnconfig.sys
               3 File(s)        135,200 bytes
               2 Dir(s)  27,075,190,784 bytes free

Z:\die>_
```

Rundll32 expects the name of a DLL. However, we don't get much response running it this way. We're missing something…

Brute Force

```
Z:\die>rundll32 dnconfig.dll blargle
```

Let's try some random option to the program….

Hey! It didn't do much, but the program "spoke" to us with this dialog box! =)

rundll32

Function
Inj
WSPStartup
clean
cli
inst
reload

Instead of brute forcing options to the program, think back to Dependency Walker. Let's try these function names as parameters to our tool run through rundll32…

Rundll32

C:\WINDOWS\System32\cmd.exe

```
Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-63C1

 Directory of Z:\die

12/08/2004  12:30 PM    <DIR>          .
12/08/2004  12:30 PM    <DIR>          ..
07/10/2004  12:14 PM           127,184 dnconfig.dll
06/09/2004  01:02 PM                80 dnconfig.ini
06/09/2004  10:55 AM             7,936 dnconfig.sys
               3 File(s)        135,200 bytes
               2 Dir(s)  26,809,192,448 bytes free

Z:\die>rundll32 dnconfig.dll Inj

Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-63C1

 Directory of Z:\die

12/08/2004  12:30 PM    <DIR>          .
12/08/2004  12:30 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  26,809,192,448 bytes free

Z:\die>_
```

A simple directory listing…

Let's run the program with Inj (the first function)… What happens?

Files Disappear!

Rundll32 / TCPView

SVCHOST.E...	TCP	j0vpcxp:1031	j0vpcxp:0	LISTENING
SVCHOST.E...	TCP	j0vpcxp:1031	localhost:pop3	SYN SENT

That last function also caused a packet to be sent to a POP email port…
TCPView let us down and didn't capture more data…

Rundll32

C:\WINDOWS\System32\cmd.exe

```
Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-63C1

 Directory of Z:\die

12/08/2004  12:30 PM    <DIR>          .
12/08/2004  12:30 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  26,808,012,800 bytes free

Z:\die>rundll32 dnconfig.dll clean

Z:\die>dir
 Volume in drive Z is XP Transfer
 Volume Serial Number is 3188-63C1

 Directory of Z:\die

12/08/2004  12:30 PM    <DIR>          .
12/08/2004  12:30 PM    <DIR>          ..
07/10/2004  12:14 PM           127,184 dnconfig.dll
06/09/2004  01:02 PM                80 dnconfig.ini
06/09/2004  10:55 AM             7,936 dnconfig.sys
               3 File(s)        135,200 bytes
               2 Dir(s)  26,808,012,800 bytes free

Z:\die>_
```

Files are hidden…

Run with “clean” option…

Files Re-Appear. This is the opposite of the hiding function… We’re getting somewhere…

Option test

```
Z:\die>rundll32 dnconfig.dll cli
```

This option creates some interesting results….

IeD console client

```
Usage: rundll32 ixd.dll cli <Direct> <Proto> <IP/DnsName> <Port> <MagicKey> [
alPort]

    Direct:
        0:    ListenOnPort
        1:    ConnectTo (Auth by ip/port
        2:    ConnectTo (Auth by inside masterkey
    Proto:
        6:    TCP
        17:   UDP
    MagicKey:
        :     A integer for ident ixdbackdoor
    LocalPort:
        :     Used while reusing connect


\Exp: rundll32 ied.dll cli 1 6 10.0.0.1 80 99
          # will connect to 10.0.0.1 80 localport 99
          # for server side Auth by ip/port
\Exp: rundll32 ied.dll cli 2 6 10.0.0.1 80 #
          # will connect to 10.0.0.1 80
          # for server side Auth by inside masterkey
```

Our first real usage statement, and a cool pop-up window! Lots of options to explore…

Server run…

C:\WINDOWS\System32\cmd.exe

```
Z:\die>rundll32 dnconfig.dll cli 0 6 127.0.0.1 12321 99

Z:\die>
```

This run…

leD console client

```
cli: direct 0, proto 6, host 127.0.0.1, port 12321, magickey 99, localport 0
```

Creates another pop-up window, and launches a ***listening server*** on our machine!

Client run

C:\WINDOWS\System32\cmd.exe

```
Z:\die>rundll32 dnconfig.dll cli 0 6 127.0.0.1 12321 99
Z:\die>rundll32 dnconfig.dll cli 1 6 127.0.0.1 12321 99
Z:\die>
```

This run…

IeD console client

```
cli: direct 1, proto 6, host 127.0.0.1, port 12321, magickey 99, localport 0
I: Incoming ixd 0x7f000001:12321
```

Creates another pop-up window, and launches a ***client*** that connects to our listening server!

Client to Server

leD console client

```
cli: direct 1, proto 6, host 127.0.0.1, port 12321, magickey 99, localport 0

I: Incoming ixd 0x7f000001:12321
help
?
```

Typing in our client window…

leD console client

```
cli: direct 0, proto 6, host 127.0.0.1, port 12321, magickey 99, localport 0

I: Incoming ixd 0x7f000001:1053
help
?
```

…echoes in the server window!

What next?

- **Each time a new feature or function of the tool is uncovered, we need to go back to our monitoring tools to see what happened…**
  - **Take notes of each thing that changed, flagging it for later research.**
  - **Wait to research specific details until you've exercised to tool a bit. This will give you the "big picture" about what is the best path for investigation.**
- **Once the monitoring tools are checked, restart them all, and run the tool again, using a different feature or function. Record, reset, repeat.**

Some Functions Revealed

- **After running this tool through several iterations of this process, we eventually discover some of the features of the tool.**

Tool Capabilities

- **General Features**
  - **Windows 2000 and XP capable (at least)**
  - **One file could be used as a client or server**
  - **Not an exploit, a backdoor only (where's the exploit?)**
- **Backdoor Functions**
  - **Remote command shell**
  - **File transfer**
  - **Process control**
- **Network Features**
  - **IP-based or Key-based authentication**
  - **Encoded network communication**
  - **Phone-home capability**
- **Rootkit Capabilities**
  - **Basic File, Registry, and Process Hiding**

Conclusion

- **This ended up being a fairly advanced tool with tons of features.**
- **Even so, this process can be run by an amateur, but it takes time, patience and organization to keep track of *what* happened *when*.**
- **Keeping track of the data the tools generates takes practice.**
- **The more you do this, the better you'll get at it.**
- **More technical tools (ethereal instead of tcpview for example) often yields better results. Improve your tools as you improve your skills.**

Analysis Tips

- **Don’t get too myopic. Keep your eye on the prize.**
- **Don’t believe everything you hear (or read). The pros screw up. A lot.**
- **Realize your limitations. The pros get things right. A lot.**
- **Outline your objectives, stick to them.**
- **Don’t get tool crazy. Stick with what works, only upgrade if a tool is specifically lacking something you *need*.**

References

- VMWare: www.vmware.com
- Tons of tools: www.sysinternals.com
- Virtual PC: Google "virtual PC"
- Fport: Google “Fport”
- Ethereal: Google “Ethereal”
- Tcpdump: Google... You get the idea =)
- My site: http://johnny.ihackstuff.com