

---

# Intro to Incident Response and Forensics



Jim Clausing



# Outline

---

- ◆ Who is this guy?
- ◆ What is Incident Response?
- ◆ What is Forensics?
- ◆ How are they related?
- ◆ The Tools
- ◆ Demo
- ◆ Q & A



# Who is this guy?

---

- ◆ Jim Clausing – [jclausing@isc.sans.org](mailto:jclausing@isc.sans.org)
- ◆ MS (and ABD) in CIS from OSU
- ◆ Been doing this since 1980 or 81
- ◆ Day job
- ◆ SANS Internet Storm Center volunteer handler
- ◆ Instrument-rated private pilot
- ◆ ...



# What is Incident Response?

---

- ◆ Events vs. Incidents
  - ◆ Event – observable occurrence
    - Examples: Anti-virus alerts, IDS alerts, “the computer is slow”
  - ◆ Incident – action that results in harm or potential harm to computer system or data
    - Examples: worms, viruses, unauthorized usage (kiddie porn)
- ◆ False Positive
- ◆ False Negative



# The 6 Steps of Incident Response

---

- ◆ Preparation
- ◆ Identification
- ◆ Containment
- ◆ Eradication
- ◆ Recovery
- ◆ Lessons Learned



# Preparation

---

- ◆ Skills
- ◆ Practice
- ◆ Notification
- ◆ Time synchronization
- ◆ Management support
  - ◆ Legal
  - ◆ Data
- ◆ Awareness
  - ◆ <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>



# Preparation

---

- ◆ Intruder Detection Checklist (Unix)
  - ◆ [http://www.cert.org/tech\\_tips/intruder\\_detection\\_checklist.html](http://www.cert.org/tech_tips/intruder_detection_checklist.html)
- ◆ Intruder Detection Checklist (Windows)
  - ◆ [http://www.cert.org/tech\\_tips/win\\_intruder\\_detection\\_checklist.html](http://www.cert.org/tech_tips/win_intruder_detection_checklist.html)
- ◆ Steps for Recovery
  - ◆ [http://www.cert.org/tech\\_tips/root\\_compromise.html](http://www.cert.org/tech_tips/root_compromise.html)



# Preparation – jump bag

---

- ◆ Phone list/phone book
- ◆ Pens, pencils, CDs, floppies, ZIP disks, USB flash drives
- ◆ Response CD, hubs (if you can find them), ethernet cables
- ◆ Flashlight, screwdrivers, digital camera
- ◆ Spare batteries (flashlight, phone,...)
- ◆ Incident response forms
- ◆ System baselines – understanding of what “normal” is.



# Preparation

---

- ◆ Just like disaster recovery, no one likes to think about it, but once the incident occurs, it is too late to plan your response.
- ◆ Plan the work, work the plan
  - ◆ Checklists



# Identification

---

- ◆ Alert / inform early
  - ◆ The tightrope between “crying wolf” and letting management getting blindsided.
- ◆ Verify that an incident has actually occurred.
  - ◆ System account / audit logs
  - ◆ Correlate with other logs (router, IDS, ????)



# Containment

---

- ◆ Limit the damage
- ◆ Preserve business data
- ◆ Preserve evidence
- ◆ Assess business risk
- ◆ Possible responsive actions:
  - ◆ Change passwords / IP addresses
  - ◆ Segment or block the system (attacker or victim)
  - ◆ Alert others “nearby”
  - ◆ Increase monitoring
  - ◆ Get sample malware to A/V vendor



# Containment

---

- ◆ Business decisions
  - ◆ Instrument and observe
  - ◆ Pull the plug
  - ◆ Call in law enforcement
    - ◆ When is this **required**?



# Eradication

---

- ◆ Clean it up
- ◆ Determine when and how the incident began (this can impact the decisions below)
- ◆ Possible eradication methods
  - ◆ Restore from backup (you do have backups, right?!)
  - ◆ Remove malware
  - ◆ Rebuild from scratch
  - ◆ Review trust relationships (where else could this have gone?)
  - ◆ Improve countermeasures (system and network)



# Recovery

---

- ◆ Validate system has been secured
- ◆ “System owner” determines whether the system is ready to return to service.
- ◆ Follow up monitoring



# Lessons Learned

---

- ◆ Follow up report
  - ◆ What worked?
  - ◆ What didn't?
  - ◆ What else needs to be done to minimize risk?
- ◆ Communicate the lessons
  - ◆ Learn from others
- ◆ Apply the fixes



# What is Forensics?

---

- ◆ Definition
  - ◆ “Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what happened in the past on a system or network.” -Venema & Farmer (1999)
- ◆ Key pieces
  - ◆ Preserving evidence
  - ◆ Seizure policy
  - ◆ Data gathering
  - ◆ Data analysis
  - ◆ Reporting



# Forensics

---

- ◆ Order of Volatility
  - ◆ Memory
  - ◆ Swap/page
  - ◆ Network status / connections
  - ◆ Running processes
  - ◆ File system information
  - ◆ Disk blocks



# Forensics – steps

---

- ◆ Verify incident
- ◆ Gather system description
- ◆ Collect (and preserve) evidence, logs, reports
  - ◆ Cryptographic hashes
  - ◆ Chain of custody
- ◆ Create timeline
- ◆ Media analysis
  - ◆ Recover deleted files
  - ◆ Keyword search
- ◆ Report



# Forensics – media analysis

---

- ◆ OS specific
- ◆ Validate integrity of key parts of the OS
  - ◆ Windows registry
  - ◆ Configuration files
- ◆ Investigate user areas
- ◆ Usage patterns
  - ◆ Temporary files
  - ◆ Recycle bin
  - ◆ Browser history



# Forensics – Timeline reconstruction

---

- ◆ File system MAC times
  - ◆ Modified (file contents)
  - ◆ Accessed
  - ◆ Created/Changed (directory entry)
- ◆ Limitations
  - ◆ Only the *last* modification/access/change is recorded
  - ◆ MAC times can be manipulated
- ◆ Use tools to automate



# Forensics

---

- ◆ Remember the definition
  - ◆ “as free from distortion or bias as possible”
- ◆ Anything we do on a system changes the system state
- ◆ Best evidence
- ◆ Chain of custody
- ◆ Media imaging
- ◆ Cryptographic hashing
- ◆ Document the collection process
  - ◆ Buddy system



# How are they related?

---

- ◆ Pretty closely 😊
  - ◆ Sometimes described as orthogonal
- ◆ Incident handling – the framework
- ◆ Forensics – the detailed analysis



# The 6 steps in practice – prep (tools)

---

## ◆ Preparation

- ◆ Make sure you have a response CD for every OS in your environment
- ◆ Always use trusted software (your response CD)
- ◆ Windows Forensic Toolchest (WFT 2.0)
- ◆ Windows Resource Kit tools
- ◆ Sysinternals tools: RegMon, FileMon, TCPView, autoruns
- ◆ Foundstone tools: fport, pslist
- ◆ Winpcap/windump, ethereal (now known as Wireshark)
- ◆ RegShot



# More preparation

---

- ◆ Establish baselines
  - ◆ Tripwire/osiris
  - ◆ RegShot
  - ◆ Installed apps (versions)
  - ◆ Service packs
  - ◆ Hot fixes
  - ◆ Local accounts
  - ◆ Shares
  - ◆ Enable auditing
  - ◆ Logging to central log host



# Still more preparation

---

- ◆ Policy
  - ◆ Acceptable use policy (AUP)
  - ◆ HIPPA/FERPA/GLBA
- ◆ Locate the logs
  - ◆ Perimeter firewalls
  - ◆ Perimeter IDS



# Identification

---

- ◆ Collect data
  - ◆ System
    - Event logs
    - Firewall logs
    - A/V logs
  - ◆ Network
    - IDS
    - Firewall logs
    - Routers (net flow)



# Identification: Network

---

- ◆ Check the logs
  - ◆ Did the IDS alarm?
  - ◆ Who was the system talking to?
    - Firewall logs
    - Proxy logs
    - Router net flow
- ◆ Capture traffic
  - ◆ SPAN port on the switch
  - ◆ That hub in the jump bag



# Why windump/tcpdump?

---

- ◆ Windows SMS includes Network Monitor which could be used.
- ◆ Winpcap/windump (or tcpdump and libpcap for Unix/Linux) are free
- ◆ The PCAP format is understood by many tools (especially on Unix/Linux).
- ◆ Ethereal (wireshark)



# windump switches

---

- ♦ `-s <snaplen>` how many bytes to capture, 1514 will include ethernet headers and full data
- ♦ `-w <outfile>` name of the file to save the output to (in pcap format)
- ♦ `-i <interface>` which interface to capture from (use `-D` to figure out which is the appropriate one)
- ♦ `-n` Don't do DNS name resolution
- ♦ “host x” or “tcp port 445” Berkeley packet filter language to limit scope of the capture



# What to look for from the network?

---

- ◆ Connections to many hosts, especially on the SMB ports 135-139 and 445.
- ◆ Large volumes of ICMP traffic
- ◆ IRC traffic
  
- ◆ Analysis techniques
  - ◆ Top talkers
  - ◆ Odd port combinations
  - ◆ Use ethereal (wireshark) to do protocol analysis



# System information

---

- ◆ Computer location
  - ◆ Building
  - ◆ Room
  - ◆ Office
  - ◆ Jack/Port
- ◆ User and login ID
- ◆ User's phone number
- ◆ System name
- ◆ MAC address
- ◆ IP address



# What to gather on the live system

---

- ◆ Collect data from most volatile to least volatile
- ◆ Collect it in “forensically sound” manner
  - ◆ Minimal impact to system
  - ◆ Don't store on the live system's disks (if you can help it)
  - ◆ Automate it if you can (e.g., using WFT)
- ◆ Document/record all your actions
- ◆ Preferably using buddy system
  - ◆ Person 1 – records
  - ◆ Person 2 – touches the system
- ◆ SANS SCORE site has IR forms
  - ◆ Who, what, where, when, why



# Data collection

---

- ◆ First pass – collect as whatever user is logged into the system
- ◆ Second pass – collect any additional data available to Administrator
- ◆ Data storage
  - ◆ Clean floppy
  - ◆ Pre-formatted CD-RW
  - ◆ Clean USB flash drive
  - ◆ Network share
  - ◆ Using netcat to “handler” workstation/laptop
  - ◆ As last resort, on the system itself



# Trusted environment

---

- ◆ Use known good “cmd.exe” from response CD
  - ◆ This is why you need a response CD for each OS in your environment.
- ◆ Run all the tools from this command window



# Windows RunAs

---

- ◆ To collect the data as Administrator use RunAs facility.
- ◆ Right-click (or use command line version)



# System State Info

---

- ◆ System date, time, uptime
- ◆ Process information
  - ◆ psinfo, pslist, fport, cmdline, autoruns, Rootkit Revealer
- ◆ Network information
  - ◆ netstat -a -n -o (-o option not available on 2000)
- ◆ Sysinternals real-time tools
- ◆ File system information
  - ◆ mac.exe



# Where does malware hide?

---

- ◆ Directories
  - ◆ Recycle bin
  - ◆ Temp directories
  - ◆ \windows\system32 and the like
    - ◆ names similar to legit apps
- ◆ Registry Keys
  - ◆ [http://www.silentrunners.org/sr\\_launchpoints.html](http://www.silentrunners.org/sr_launchpoints.html)
- ◆ Scheduled Tasks
- ◆ Running processes
- ◆ Listening services



# The Windows Forensic Toolchest (WFT)

---

- ◆ Provides repeatability/consistency
- ◆ Extensible
- ◆ Forensically sound
- ◆ Well organized
- ◆ Extensive logging
- ◆ Web front-end for analysis



# Using WFT

---

- ◆ Verify date/time/system info
- ◆ Examine processes – anything unexpected (compare to baseline)
- ◆ Services – ditto
- ◆ Network – Fport, netstat, net user
- ◆ Login history – has anyone been attempting to login as Administrator
- ◆ Registry – Especially run keys and autostart
- ◆ Install history
- ◆ MAC times – import into Excel
- ◆ Alternate Data Streams



# Containment in practice

---

- ◆ Disconnect from the network (What is the criticality of the system? What is the policy?)
- ◆ Isolate accounts
  - ◆ Change passwords (local and domain)
- ◆ Backup local data
  - ◆ Critical data (license keys)
- ◆ Remove shares, unneeded registry keys
- ◆ Update file permissions
- ◆ Use boot floppy or CD to change Administrator password



# More containment

---

- ◆ Work through the data collected
- ◆ When did the breach occur?
- ◆ When were your last good backups?



# Eradication in practice

---

- ◆ Boot to safe mode and run A/V software
- ◆ Search for and remove malicious registry entries
- ◆ Remove malware from the system
- ◆ Verify all passwords have been changed
- ◆ Sanitize disk (low-level format plus DOD erase), then reinstall OS
- ◆ Determine patch / service pack levels
  - ◆ Apply **BEFORE** reconnecting to the network



# Recovery in practice

---

- ◆ Monitor the system
- ◆ Validate functionality
- ◆ Work with system owner on data recovery and risk acceptance
- ◆ Use tools like Microsoft Baseline Security Analyzer to verify system is current on patches
- ◆ Run external vulnerability scan (ISS, nessus, ...)
- ◆ Configure / verify Auto Update for A/V tool (patches)
- ◆ Recheck in relatively short order
- ◆ Monitor for abnormal traffic (IRC, ...)



# More recovery

---

- ◆ Additional instrumentation/protection
  - ◆ Add anti-spyware software
    - Spybot-Search and Destroy (resident, aka TeaTimer)
    - SpySweeper
  - ◆ Add software firewall
    - The built-in XP firewall is weak
  - ◆ Add A/V
- ◆ Use the CIS Benchmarks to make sure you have hardened the OS appropriately



# Lessons Learned

---

- ♦ What additional instrumentation/protection should we add to *all* of our systems?
- ♦ What can we do to improve our perimeter?
- ♦ Does everyone really need to run as a local admin?
- ♦ “Prevention is ideal, but detection is a must”



# Lessons Learned

---

- ◆ Defense-in-depth
  - ◆ Updated security software on all machines
    - A/V, anti-spyware, personal firewall, privacy
  - ◆ E-mail filtering
    - Gateway and local
  - ◆ Regular backups
  - ◆ Policy
  - ◆ Awareness



# Winfingerprint

**Winfingerprint 0.6.2**

**Input Options**

- IP Range
- IP List
- Single Host
- Neighborhood

IP Address:

**Scan Options**

- Domain
- Active Directory
- WMI API
- Win32 OS Version
- Users
- Patch Level
- Null IPC\$ Sessions
- Services
- MAC Address
- NetBIOS Shares
- Disks
- Sessions
- Date and Time
- Groups
- Event Log
- Ping Host(s)
- RPC Bindings
- Show Errors
- Traceroute Host

**General Options**

Broadcom NetXtreme Gigabit Ethernet - Packet Schedu

Timeout for TCP/UDP/ICMP/SNMP:

Retries:  Max Connections:

TCP Portscan Range:

UDP Portscan Range:

SNMP Community String:

Pinging 127.0.0.1 with 44 bytes of data:  
Reply from 127.0.0.1: 0 ms (id= 1, seq= 1)  
IP Address: 127.0.0.1 localhost  
Computername: ISO\CLAUSINGT430

MAC Addresses:  
005056c00008  
005056c00001  
0010c6cf7d90

Patch Level:  
Operating System: 5.1  
Role: NT Workstation  
Role: LAN Manager Workstation  
Role: LAN Manager Server  
Comment:  
Service Pack 2  
KB873333 Windows XP Hotfix - KB873333  
KB873339 Windows XP Hotfix - KB873339  
KB883939 Security Update for Windows XP (KB883939)  
KB885250 Windows XP Hotfix - KB885250  
KB885626 Windows XP Hotfix - KB885626  
KB885835 Windows XP Hotfix - KB885835



# FileMon

File Monitor - Sysinternals: www.sysinternals.com

File Edit Options Volumes Help

#	Time	Process	Request	Path	Result	Other
123	00:57:13	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Attributes: A
124	00:57:13	explorer.ex...	OPEN	C:\Program Files\PGP Corporation\PG...	SUCCESS	Options: Open Access: Execute
125	00:57:13	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Length: 855040
126	00:57:13	explorer.ex...	CLOSE	C:\Program Files\PGP Corporation\PG...	SUCCESS	
127	00:57:13	rundll32.ex...	OPEN	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Options: Open Access: All
128	00:57:13	rundll32.ex...	LOCK	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Excl: No Offset: 0 Length: -1
129	00:57:13	rundll32.ex...	QUERY INFORMATION	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Length: 6246
130	00:57:13	rundll32.ex...	READ	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Offset: 0 Length: 6246
131	00:57:13	rundll32.ex...	UNLOCK	C:\PROGRA~1\ThinkPad\UTILIT~1\...	RANGE NO...	Offset: 0 Length: -1
132	00:57:13	rundll32.ex...	CLOSE	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	
133	00:57:13	rundll32.ex...	OPEN	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Options: Open Access: All
134	00:57:13	rundll32.ex...	LOCK	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Excl: No Offset: 0 Length: -1
135	00:57:13	rundll32.ex...	QUERY INFORMATION	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Length: 6246
136	00:57:13	rundll32.ex...	READ	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	Offset: 0 Length: 6246
137	00:57:13	rundll32.ex...	UNLOCK	C:\PROGRA~1\ThinkPad\UTILIT~1\...	RANGE NO...	Offset: 0 Length: -1
138	00:57:13	rundll32.ex...	CLOSE	C:\PROGRA~1\ThinkPad\UTILIT~1\...	SUCCESS	
139	00:57:15	PGPTray.e...	OPEN	C:\Documents and Settings\jac.JCLAU...	SUCCESS	Options: Open Access: All
140	00:57:15	PGPTray.e...	QUERY INFORMATION	C:\Documents and Settings\jac.JCLAU...	SUCCESS	Attributes: A
141	00:57:15	PGPTray.e...	CLOSE	C:\Documents and Settings\jac.JCLAU...	SUCCESS	
142	00:57:15	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Attributes: A
143	00:57:15	explorer.ex...	OPEN	C:\Program Files\PGP Corporation\PG...	SUCCESS	Options: Open Access: Execute
144	00:57:15	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Length: 855040
145	00:57:15	explorer.ex...	CLOSE	C:\Program Files\PGP Corporation\PG...	SUCCESS	
146	00:57:17	PGPTray.e...	OPEN	C:\Documents and Settings\jac.JCLAU...	SUCCESS	Options: Open Access: All
147	00:57:17	PGPTray.e...	QUERY INFORMATION	C:\Documents and Settings\jac.JCLAU...	SUCCESS	Attributes: A
148	00:57:17	PGPTray.e...	CLOSE	C:\Documents and Settings\jac.JCLAU...	SUCCESS	
149	00:57:17	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Attributes: A
150	00:57:17	explorer.ex...	OPEN	C:\Program Files\PGP Corporation\PG...	SUCCESS	Options: Open Access: Execute
151	00:57:17	explorer.ex...	QUERY INFORMATION	C:\Program Files\PGP Corporation\PG...	SUCCESS	Length: 855040
152	00:57:17	explorer.ex...	CLOSE	C:\Program Files\PGP Corporation\PG...	SUCCESS	



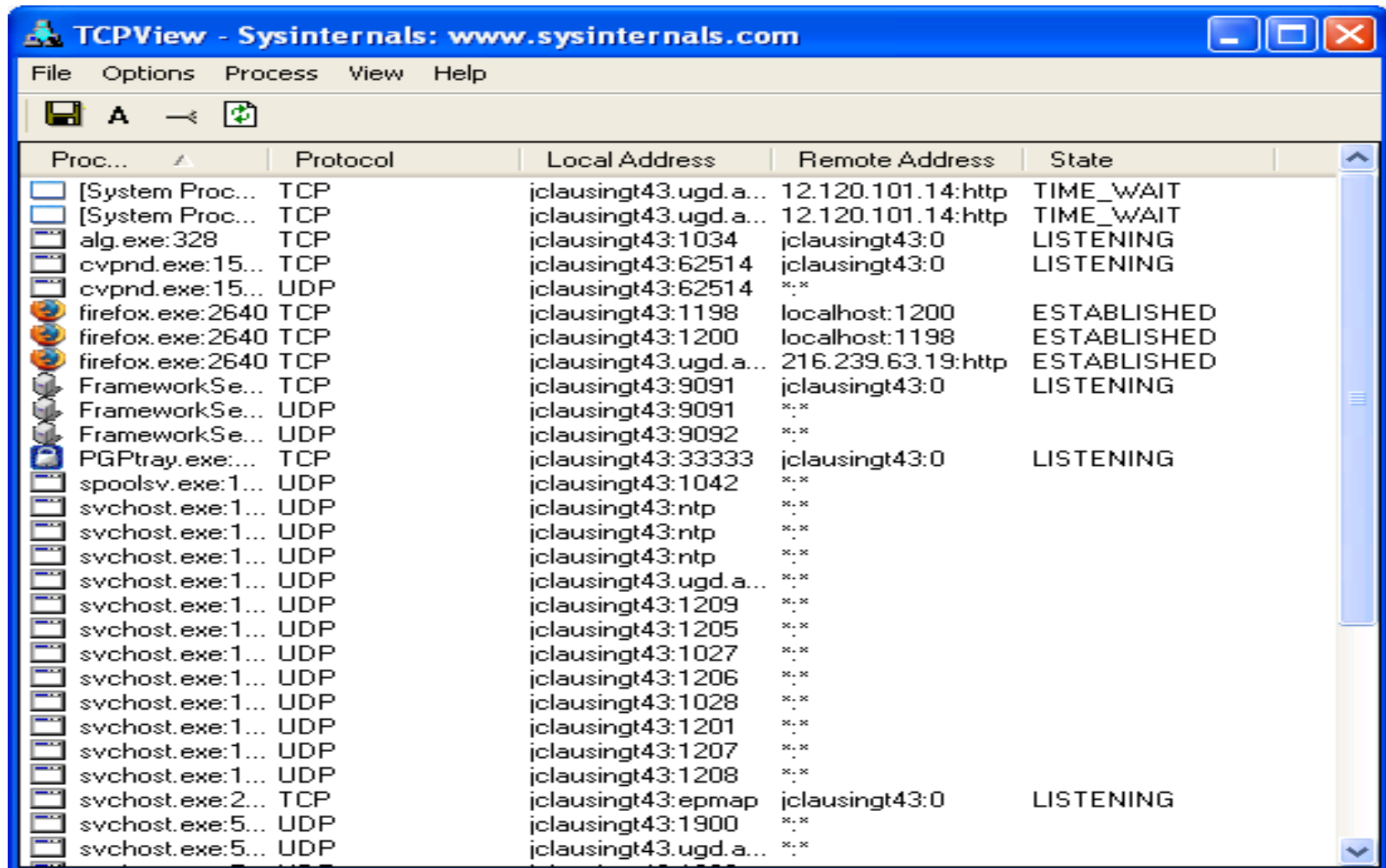
# RegMon

Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Process	Request	Path	Result	Other
8071	9.45685890	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8072	9.45688377	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8073	9.47031089	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8074	9.47033659	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8075	9.47036034	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8076	9.48298904	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8077	9.48301474	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8078	9.48303849	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8079	9.49813817	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8080	9.49816387	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8081	9.49818762	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8082	9.51122280	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8083	9.51124878	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8084	9.51127252	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8085	9.55073340	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8086	9.64387234	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8087	9.73792982	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8088	9.82557252	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8089	9.92502343	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8090	10.01879010	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8091	10.01879876	acs.ex...	OpenKey	HKLM\SOFTWARE\Atheros\Athgina	NOTFO...	
8092	10.01884010	QCW...	OpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCE...	Access: 0x...
8093	10.01885295	acs.ex...	OpenKey	HKLM\SOFTWARE\Atheros\Athgina	NOTFO...	
8094	10.11254307	SynT...	CreateKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	Access: 0x...
8095	10.11257632	SynT...	QueryValue	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	0x11
8096	10.17623217	SynT...	CloseKey	HKCU\Software\Synaptics\SynTPEnh...	SUCCE...	
8097	10.17624475	QCW...	QueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCE...	"PCI\VEN ...

# TCPView



The screenshot shows the TCPView application window from Sysinternals. The title bar reads "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The toolbar contains icons for saving, a search box with the letter 'A', a back arrow, and a refresh icon. The main area is a table with columns: "Proc...", "Protocol", "Local Address", "Remote Address", and "State".

Proc...	Protocol	Local Address	Remote Address	State
[System Proc...	TCP	jclausingt43.ugd.a...	12.120.101.14:http	TIME_WAIT
[System Proc...	TCP	jclausingt43.ugd.a...	12.120.101.14:http	TIME_WAIT
alg.exe:328	TCP	jclausingt43:1034	jclausingt43:0	LISTENING
cvpnd.exe:15...	TCP	jclausingt43:62514	jclausingt43:0	LISTENING
cvpnd.exe:15...	UDP	jclausingt43:62514	*:*	
firefox.exe:2640	TCP	jclausingt43:1198	localhost:1200	ESTABLISHED
firefox.exe:2640	TCP	jclausingt43:1200	localhost:1198	ESTABLISHED
firefox.exe:2640	TCP	jclausingt43.ugd.a...	216.239.63.19:http	ESTABLISHED
FrameworkSe...	TCP	jclausingt43:9091	jclausingt43:0	LISTENING
FrameworkSe...	UDP	jclausingt43:9091	*:*	
FrameworkSe...	UDP	jclausingt43:9092	*:*	
PGPTray.exe:...	TCP	jclausingt43:33333	jclausingt43:0	LISTENING
spoolsv.exe:1...	UDP	jclausingt43:1042	*:*	
svchost.exe:1...	UDP	jclausingt43:ntp	*:*	
svchost.exe:1...	UDP	jclausingt43:ntp	*:*	
svchost.exe:1...	UDP	jclausingt43:ntp	*:*	
svchost.exe:1...	UDP	jclausingt43.ugd.a...	*:*	
svchost.exe:1...	UDP	jclausingt43:1209	*:*	
svchost.exe:1...	UDP	jclausingt43:1205	*:*	
svchost.exe:1...	UDP	jclausingt43:1027	*:*	
svchost.exe:1...	UDP	jclausingt43:1206	*:*	
svchost.exe:1...	UDP	jclausingt43:1028	*:*	
svchost.exe:1...	UDP	jclausingt43:1201	*:*	
svchost.exe:1...	UDP	jclausingt43:1207	*:*	
svchost.exe:1...	UDP	jclausingt43:1208	*:*	
svchost.exe:2...	TCP	jclausingt43:epmap	jclausingt43:0	LISTENING
svchost.exe:5...	UDP	jclausingt43:1900	*:*	
svchost.exe:5...	UDP	jclausingt43.ugd.a...	*:*	



# Autoruns

The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns [JCLAUSINGT43\jac] - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Entry", "Options", "User", and "Help". The toolbar contains icons for "Image Hijacks", "Applnit", "KnownDLLs", "Winlogon", "Winsock Providers", and "Print Monitors". The main toolbar includes "Everything", "Logon", "Services", "Explorer", "Internet Explorer", "Scheduled Tasks", and "Boot Execute".

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
<input checked="" type="checkbox"/> C:\WINDOWS\... Userinit Logon Application	Userinit Logon Application	Microsoft Corporation	c:\windows\system32\useri...
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
<input checked="" type="checkbox"/> Explorer.exe	Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Acrobat Assist...	AcroTray	Adobe Systems Inc.	c:\program files\adobe\acr...
<input checked="" type="checkbox"/> ATIPTA	ATI Desktop Control Panel	ATI Technologies, Inc.	c:\program files\ati technol...
<input checked="" type="checkbox"/> BCWipeTM St...	BCWipeTM	Jetico, Inc.	c:\program files\jetico\bcwi...
<input checked="" type="checkbox"/> BLOG			c:\program files\thinkpad\u...
<input checked="" type="checkbox"/> Doctor Install	Doctor Install - Installation ...	AT&T	c:\program files\doctor inst...
<input checked="" type="checkbox"/> EZEJMNAP	IBM ThinkPad EasyEject S...	IBM Corp.	c:\program files\thinkpad\u...
<input checked="" type="checkbox"/> HumMeteringCL...	Metering Client DLL for Win...	Hummingbird Ltd.	c:\program files\hummingbir...
<input checked="" type="checkbox"/> ISUSPM Startup			File not found: C:\Program ...
<input checked="" type="checkbox"/> ISUSScheduler	InstallShield Update Servic...	InstallShield Software Corpo...	c:\program files\common fil...
<input checked="" type="checkbox"/> iTunesHelper	iTunesHelper Module	Apple Computer, Inc.	c:\program files\itunes\itun...
<input checked="" type="checkbox"/> Logitech Hard...	Logitech KHAL Main Process	Logitech Inc.	c:\program files\common fil...

Ready.



# Demo

---

Let's actually run wft

Demo: <http://www.clausing.us/~jac/tc7/wft-demo.zip>

Can be played by mplayer on Linux  
(<http://www.mplayerhq.hu/>) or on any Windows AVI  
player with the VMware codec  
([http://www.vmware.com/download/eula/moviedecoder\\_v55.html](http://www.vmware.com/download/eula/moviedecoder_v55.html))

Config:

[http://www.clausing.us/~jac/tc7/wft\\_XP\\_short.cfg](http://www.clausing.us/~jac/tc7/wft_XP_short.cfg)

Output: <http://www.clausing.us/~jac/tc7/index.html>



# Q & A

---

- ◆ E-mail questions: [jclausing@isc.sans.org](mailto:jclausing@isc.sans.org)

! THANKS !

# Handlers on the loose in Vegas





# References

---

- ◆ <http://www.sans.org/rr/whitepapers/incident/>
- ◆ <http://www.sans.org/rr/whitepapers/forensics/>
- ◆ <http://isc.sans.org> ☺
- ◆ <http://www.sans.org>
  - ◆ Security 504 (GCIH)
  - ◆ Security 551 - Stay Sharp: First Responder (Windows)
- ◆ <http://www.foolmoon.net/security/wft/>
- ◆ [http://www.foolmoon.net/downloads/Monty\\_McDougal\\_GCFA.pdf](http://www.foolmoon.net/downloads/Monty_McDougal_GCFA.pdf)
- ◆ <http://www.sans.org/score/>



# References

---

- ♦ <http://winfingerprint.sourceforge.net>
- ♦ File System Forensic Analysis, Brian Carrier, Addison-Wesley. ISBN 0-32-126817-2
- ♦ Incident Response & Computer Forensics, Second Edition, Mandia, Prorise, and Pepe, McGraw-Hill Osborne. ISBN 0-07-222696-X
- ♦ Computer Security Incident Handling Step-By-Step, Stephen Northcutt, SANS Press.  
[http://store.sans.org/store\\_item.php?item=62](http://store.sans.org/store_item.php?item=62)