Sniper Forensics

“One Shot, One Kill”

Chris Pogue- Trustwave
Who Am I?

• Senior Security Consultant for the Trustwave SpiderLabs
• Master’s degree in Information Security
• CISSP, CEH, CREA, GCFA, QSA
• Author of “Unix and Linux Forensic Analysis” by Syngress
• Author of the blog, “The Digital Standard”
  • http://thedigitalstandard.blogspot.com
• Member of the Board of Governors for the HTCIA
• Speaker at SANS, The Computer Forensics Show, Direct Response Forum
• Former US Army Signal Corps Warrant Officer
• Former CERT team member – SEI at CMU
Agenda

- What is Shotgun Forensics?
- What is Sniper Forensics?
- Guiding Principles
- Create an Investigation Plan
- Data Reduction
- Volatile Data Gathering and Analysis
- Tools
- Case Studies
- Bring it All Together
- Conclusion
Shotgun Forensics

The process of taking a haphazard, unguided approach to forensic investigations:

• “Old school”
• Image everything
• Reliance on tools – autopilot
• Pull the plug
Sniper Forensics

The process of taking a targeted, deliberate approach to forensic investigations:

- Create an investigation plan
- Apply sound logic
  - Locard
  - Occam
  - Alexiou
- Extract what needs to be extracted, nothing more
- Allow the data to provide the answers
- Report on what was done
- Answer the questions
Three Round Shot Group

Infiltration

• How did the bad guy(s) get onto the system(s)

Action

• What did they do
• What did they steal

Exfiltration

• How did they get off the system
• How did they get stolen data off the system
What Others are Saying

Q: How important do you think it is to have a clear plan of attack for a forensic investigation?

A: “I’d suggest that its paramount...whether you develop the plan from scratch or start with documented processes. If you have a plan and miss something, you can determine what you missed; without a plan, you can't do that.”

Harlan Carvey, VP of Advanced Security Projects, Terremark/Author

“Having an investigative plan is critical. Such a plan should describe what you're looking for, how you'll know when you've found it, and when to stop. Without it, an investigation can become mired or unfocused.”

Jesse Kornblum, Senior Forensic Scientist, Mantec/Former OSI Special Agent
“You cannot just cross your fingers and magically hope you will find the evil you are looking for. You have to know what you are looking for. Finding evil requires you to know what you need to prove and then use a combination of scientific analysis and proven techniques to find it.”

Rob Lee, Principle Consultant, Mandiant/SANS

“Having a clear plan of attack for a forensic investigation is absolutely paramount. This is especially true when operating in environments when a forensic team may not be necessarily welcome. A clear plan of attack allows the investigator to conduct their investigation in a efficient and deliberate manner.”

Auston Davis, Former US Director Cyber-Security and Investigations, Visa/OSI Officer, USAF
Guiding Principles

• Locard’s Exchange Principle

• Occam’s Razor

• The Alexiou Principle
Locard’s Exchange Principle

- Established by Edmund Locard (1877-1966)
- Regarded as the father of modern forensics
- Uses deductive reasoning
  - A and B come into contact with one another
  - A will have traces of B
  - B will have traces of A
Occam’s Razor

• Establish by William of Occam
  – 13th century Franciscan Friar
  – Major contributor to medieval thought
  – Student of Aristotelian logic

• The simplest answer is usually right
  – The modern KISS principle
    • “Keep It Simple Stupid”
  – Don’t speculate
  – Let the data be the data
The Alexiou Principle

Documented by Mike Alexiou, Terremark

- Former Global Manager of the X-Force ERS team
  - What question are you trying to answer?
  - What data do you need to answer that question?
  - How do you extract that data?
  - What does the data tell you?
Create an Investigation Plan

What are your goals?
• Write them down
  – Clear, concise, obtainable
  • If they are not CLEAR and CONCISE, you need to make them that way
• Success indicators
  – What will it look like when you find what you are looking for
  – Don’t blow this off, REALLY think about this
• Make sure you are on the same page with the client
  – Define and deliver
  – Give them what you told them you were going to give them

Plan the work and work the plan
• Answer the questions you ask yourself
• Show your work
• If an answer cannot be found, provide the negative evidence
Create an Investigation Plan

This is THE MOST important phase of the investigation process. (If you blow this, the entire case will be in jeopardy.)

- You CANNOT be asked to “find the bad guy stuff” and walk away! There is no way to qualify or quantify that kind of statement!

[Diagram showing the process: Identify the target, Lock on, Engage]
Data Reduction

- Determine what is “normal”
- Eliminate “normal” from your view
- What’s left over is abnormal
- Provides good ole fashioned “leads”
- Document what you did, why you did it, and the results
- Answer the new questions
Volatile Data Gathering

Critical to the investigation

• Likely your only chance to review the live system
  – Attackers may still be present
  – Malware is running in its original state
  – THIS is the crime scene live

• Gather as much as you can
  – Use “trusted” tools
  – No such thing a “court approved”
  – Know your footprint, and be able to account for it

• Review during image acquisition
  – Major developments in minutes
  – Customer is good source of intel
  – Feeds back into the investigation plan
Volatile Data Analysis

What is the suspect system “supposed” to be doing

• Primary function of system
• Define what “normal” looks like
• Use the customer’s knowledge of their own system

What does it look like it’s doing

• Process to port mappings
  – What is running
  – From where
  – Why
• Network connections
  – What connections are being made
  – To where
  – Why
Volatile Data Analysis (cont.)

Event Logs (if you are lucky enough to have them)
- Who is logged in
- What have they done
- From where

Registry
- GOLD MINE – Basically a huge, detailed, log file
- What has each user been doing (ntuser.dat)
  - How
  - From where (know which keys record this data)
  - LastWrite times
- Can be extracted from a live system
- Parsed with RegRipper
Volatile Data Analysis (cont.)

Restore Points (Shadow Copy Volumes)

- Record major changes to the system or chronological
- Can be parsed to show when things took place
  - Malware was not present yesterday, but is there today
  - System was “updated” – something was installed
  - Registry changes are included (THIS IS HUGE)
    - Can be parsed with RipXP

System Information

- Operating System
- Patch level
- Auditing policies
- Password policies
Volatile Data Analysis (cont.)

RAM

- Another GOLD MINE
- Encryption keys
- Running processes
  - Open handles
  - Mutexes
    - Garble
    - Least frequency of occurrence
  - Dlls being used
  - Network connections
  - Binaries have to be unpacked to run
- Strings
  - Usernames and passwords
  - Regexes
  - Luhn checks
Tools

- Handle
- Autoruns
- Process Explorer
- Auditpol
- SigCheck
- Tlist
- ListDlls
- DumpEl
- Highlighter
- Red Curtain
- Miss Identify
- MDD
- Fastdump Pro
- Volatility
- RegRipper

- RipXP
- Memoryze
- FlyPaper
- RegScan
- SR
- Uassist_lv
- Pclip
- Fport
- TcpVcon
- Strings
- HexWorkshop
- MD5Deep
- HashDeep
- SSDeep
- F-Response
Case Studies

Caught Red Handed
- RAM Dump
- Fly Paper
- Process Explorer
- Username and Password to attackers server

Initial Point of Entry
- RDP Logs
- Multiple breaches
- Flat MPLS network

Dame los llaves
- What do certain registry keys mean
- What can you logically assume from those keys
- Totally changed the direction of the case
Initial Point of Entry

Logon User Name: chris pogue
LastWrite Time: Tue Jul 07 18:50:17 2009 (UTC)

Terminal Server Client\Servers
Software\Microsoft\Terminal Server Client\Servers
LastWrite Time: Fri Jul 10 14:12:21 2009 (UTC)

Hostname: 10.101.1.11
Domain/Username: DOMAIN1\chris pogue
LastWrite: Tue Jul 07 18:50:12 2009 (UTC)

Hostname: 10.101.1.18
Domain/Username: DOMAIN1\anesbitt
LastWrite: Wed Feb 18 18:25:36 2009 (UTC)

Hostname: 10.101.1.12
Domain/Username: DOMAIN1\chris pogue
LastWrite: Tue Jul 07 16:16:19 2009 (UTC)

Hostname: 10.101.1.13
Domain/Username: DOMAIN1\chris pogue
LastWrite: Wed Dec 10 19:29:48 2009 (UTC)

Hostname: 10.101.1.15
Domain/Username: DOMAIN1\chris pogue
LastWrite: Mon Jan 5 15:40:39 2009 (UTC)

Hostname: 10.101.1.17
Domain/Username: DOMAIN1\chris pogue
LastWrite: Wed Oct 22 16:40:03 2009 (UTC)

Hostname: 10.101.1.27
Domain/Username: DOMAIN1\anesbitt
LastWrite: Wed Feb 18 18:03:46 2009 (UTC)

Hostname: 10.101.1.66
Domain/Username: DOMAIN1\desbitt
LastWrite: Fri Jul 10 14:12:21 2009 (UTC)
Initial Point of Entry

Hostname: 10.33.44.143
Domain/Username: WIN2003\administrator
LastWrite: Thu May 28 15:28:47 2009 (UTC)

Hostname: 10.33.78.133
Domain/Username: WIN2003\helpdesk
LastWrite: Tue May 12 23:09:51 2009 (UTC)

Hostname: 10.33.78.145
Domain/Username: WIN2003\helpdesk
LastWrite: Tue May 12 22:22:04 2009 (UTC)

Hostname: 18.57.7.9
Domain/Username: WIN2003\anesbit
LastWrite: Thu Nov 20 15:29:15 2008 (UTC)

Hostname: server1
Domain/Username: WIN2003\administrator
LastWrite: Thu May 28 19:14:01 2009 (UTC)

Hostname: server01
Domain/Username:
LastWrite: Thu Nov 20 17:00:25 2008 (UTC)

Hostname: server01
Domain/Username:
LastWrite: Tue Dec 16 14:17:43 2008 (UTC)

Hostname: server01
Domain/Username:
LastWrite: Tue Dec 16 14:01:31 2008 (UTC)

Hostname: server01
Domain/Username:
LastWrite: Tue Dec 16 14:25:45 2008 (UTC)

TSClient
Software:Microsoft\Terminal Server Client\Default
LastWrite Time Fri Jul 10 16:59:29 2009 (UTC)
MRU0 -> 10.101.1.27
MRU1 -> 10.101.1.2
MRU2 -> 10.101.1.12
MRU3 -> 10.101.1.11
MRU4 -> 10.101.1.17
Dame los llaves
Dame los llaves
Dame los llaves
Bring it all together

What was your goal

• Restate your objectives
  – “The goal of this investigation was to determine BLAH…”

• Conclusions should support objectives
  – “It was determined that BLAH took place…”

• Clear, concise, direct
  – Know your audience
    • C-Staff / technical / small business owner
  – No fluff
    • Say what you need to say and move on...DO NOT be verbose
  – No erroneous information
    • Deliver what you were brought in to deliver
Bring it all together (cont.)

What data provided answers

• Here is where to be specific
  – Should be repeatable by anyone
  – State exactly what you did and why
  – Avoid “lameness”

What were the answers

• How do they support the goals
• Sound conclusions are indisputable
• You are the expert
Conclusion

• Develop an analysis plan
• Apply sound logic
• Use data reduction
• Identify anomalies
• Generate a conclusion based on:
  – Customer objectives
  – Guiding principles
  – Data analysis

• Let the DATA guide your theory…NEVER force the data into your theory!
Final Thought

“-- The cardinal rule of criminal detection was carved in stone more than a century ago. It is a capital mistake to theorize before you have all the evidence, ... It biases the judgment.”

Sherlock Holmes
Questions
Contact Information

cepogue@trustwave.com

http://thecisualstandard.blogspot.com