

Where serious technology buyers decide

# **Network Forensics**

**Tracking Hackers Through Cyberspace** 

Sherri Davidoff and Jonathan Ham

## Once Upon a Time..

- Hard drive forensics
- Useful, but:
  - You can't trust a compromised host
  - Limited space for logs
  - Just a small piece of the puzzle
- Like an autopsy of a body at a crime scene



Image: http://commons.wikimedia.org/wiki/File:Hdd-serial\_ata.jpg

### **Now: Network Forensics**

- The <u>rest</u> of the crime scene
  - Footprints, fingerprints, bullets in the wall
- Firewalls
- Web proxies
- DHCP servers
- Central log servers
- Flow records
- Traffic on the wire (or in the air)

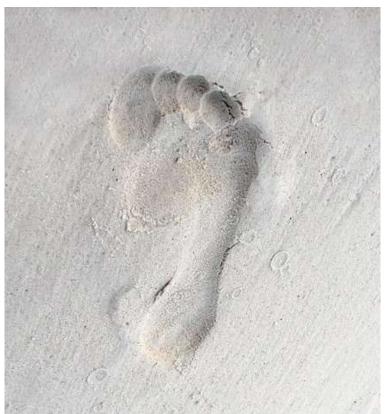


Image: Nevit Dilmen, http://commons.wikimedia.org/wiki/File:Maldives\_00147\_foot\_print\_on\_earth.jpg

## Catch a Brute Force Attack – Flow Records

- Successful brute force attack
- Regular automated attempts (every 2 seconds)
- Followed by large data transfer

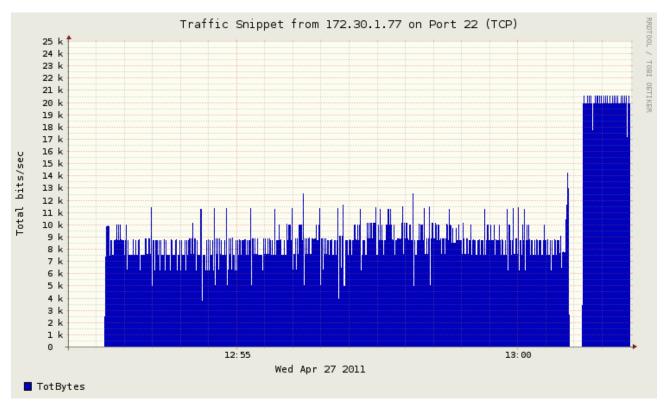


Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 5) - Day 1 of the Black Hat class

### **Brute Force – Event Logs in Splunk**

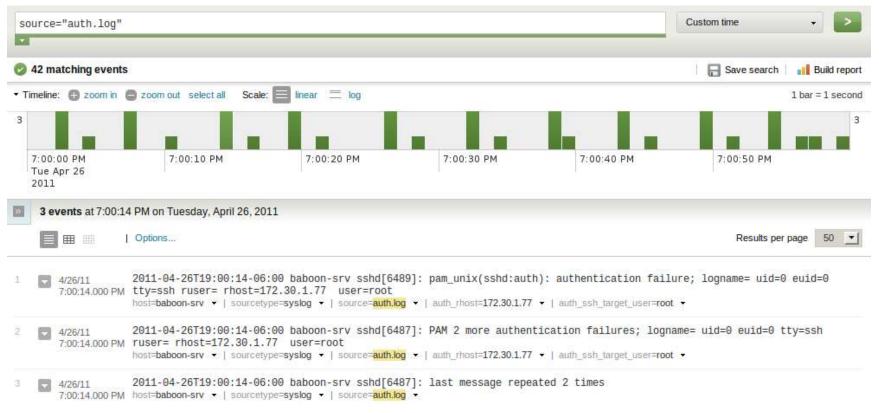
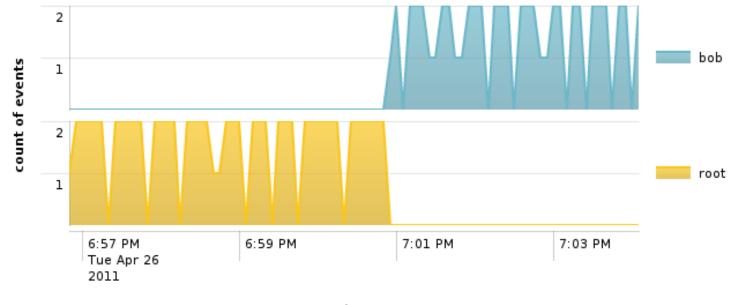


Image: Copyright LMG Security, 2011. Used with permission.

### From "Network Forensics" (ch. 8)

### **Brute Force – Targeted Accounts in Splunk**



time

Image: Copyright LMG Security, 2011. Used with permission.

### From "Network Forensics" (ch. 8)

### Wireless – Track Down Rogue Laptops

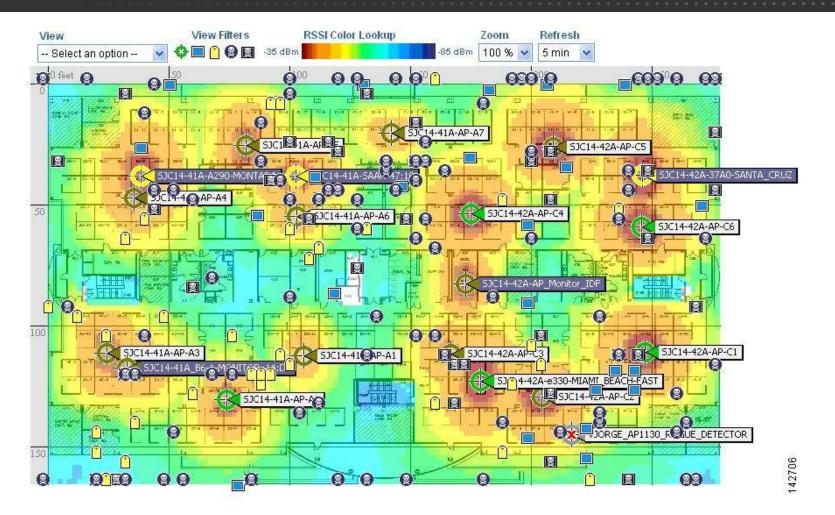


Image: Copyright Cisco.Systems, 2011.

From "Network Forensics" (ch. 6) – Day 2 of the Black Hat class

## Web Proxies – Browsing Histories for Everyone



#### Squid User Access Reports

		Peri	od: 2011№	fay18-201	i May18				
		Use	r: 192.168	3.1.170					
		Sor	: BYTES, :	reverse					
	ACCESSED SITE	CONNECT	BYTES	% BYTES	IN-CAC	HE-OUT	ELAPSED TIME	MILISEC	%TIME
ч,	www.boingboing.net	72	2.64M	21.25%	4.44%	95.56%	00:00:51	51,118	10.06%
ч,	safebrowsing-cache.google.com	19	2.54M	20.44%	0.00%	100.00%	00:00:10	10,823	2.13%
ч,	a.fsdn.com	41	1.31M	10.57%	60.33%	39.67%	00:00:07	7,210	1.42%
ч,	threatpost.com	71	782.52K	6.29%	2.90%	97.10%	00:00:18	18,476	3.64%
ч,	boingboing.net	27	693.88K	5.58%	45.63%	54.37%	00:00:09	9,721	1.91%
ч,	s0.2mdn.net	21	555.72K	4.47%	0.23%	99.77%	00:00:03	3,730	0.73%
۳9	craphound.com	14	502.73K	4.04%	0.00%	100.00%	00:00:13	13,145	2.59%
ч,	news.discovery.com	31	313.73K	2.52%	0.00%	100.00%	00:00:05	5,712	1.12%
۳9	www.computerworld.com	68	287.21K	2.31%	12.50%	87.50%	80:00:00	8,926	1.76%
ч,	science.slashdot.org	4	2 52 .68K	2.03%	25.58%	74.42%	00:00:02	2,504	0.49%
Φ9	www.kqed.org	48	172.90K	1.39%	3.09%	96.91%	00:00:16	16,320	3.21%
ч,	lakemissoulagroup.com	27	169.10K	1.36%	0.00%	100.00%	00:00:02	2,667	0.52%
чь	s.ytimg.com	8	161.27K	1.30%	66.55%	33.45%	00:00:00	800	0.16%
ч,	tech.slashdot.org	2	133.19K	1.07%	0.00%	100.00%	00:00:01	1,220	0.24%
ч,	hardware.slashdot.org	2	126.66K	1.02%	0.00%	100.00%	00:00:01	1,541	0.30%
чь	pagead2.googlesyndication.com	9	126.35K	1.02%	23.44%	76.56%	00:00:00	920	0.18%
<b>m</b> L			110.057	0.054	0.000/	100.000	00 00 0F	E 84.0	

Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 10) - Day 3 of the Black Hat class

### Carving a JPG Out of a Web Proxy Cache

New Open	S	E ave	Ur	do	Red		Cut		Ъ ору	Past	<u>1</u>	Find		ind a	nd Re	eplac	e						
00000EB-ec	lited	.htm	8	0000	000F8	3 🖾																	
00000a8	31	39	3A	35	36	3A	32	30	20	47	4D	54	0D	0A	53	65	72	76	65	72	3A	19:56:20 GMTServer:	2
00000bd		41	70	61	63	68	65	2F	32	2E	32		33	20	28	46		29			4C	-	
00000d2	61	73	74	2D	4D	6F	64	69	66	69	65	64	3A	20	4D	6F	6E					ast-Modified: Mon, 26	1
00000e7		1.122-04	61	79	20	32	30	30	38	20	31	31		32	37		31			1200	4D	May 2008 11:27:13 GM	
00000fc			0A	45	54	61	67					64				33						TETag: "bd50e3-bf60	
0000111	1000	37	36	30	38	30	36	34	30			0A			63	65	70		2D			-76080640"Accept-Ra	
0000126			65	73	3A	20	62	79	74	12.7		0D		43		6E	74					nges: bytesContent-	
000013b		65	6E	67	74	68	3A	20	34	38	39	39	32		0A			6E	6E			Length: 48992Connec	
0000150	74	69	6F	6E	3A	20	63	6C	6F	1005	65	0D		43	6F	6E			6E		and the second	tion: closeContent-	
0000165	-	79	70		3A		69	6D						70					0D				
000017a 000018f			E0 43	00	10	4A	46	49	46	100	01	01	00	00	01	00	01	00			FE		
000018f	5.5		1.2.2	52	45	41	54	4F	52		20				6A				20			.; CREATOR: gd-jpeg v1	
00001a4				20	75 71	73	61	6E	67		49					50						.0 (using IJG JPEG v6 2), quality = 90C	
	1.1.1				1.1																	2), quality = 90c	
00001Ce	00	03	02	02	03	02	02	03	03	0.5	0.5	04	03	0.5	04	05	00	05	05	04	04	• • • • • • • • • • • • • • • • • • •	
Search for:	FFD	8														as	He	exade	ecima	al 🗘	] ,	🔑 Find Next 🛛 🔶 Find Previous	83
		_													_						9		
Signed (	3 bit:	: -1					Si	gned	32 b	it: [-	2555	936							Hexa	deci	mal:	FF D8 FF E0	83
Unsigned 1	3 bit	25	5				Unsi	gned	32 b	it: 4	292	4113	60							Deci	mal:	255 216 255 224	
Signed 1	5 bit	: -40	)					Float	32 b	it: 📭	JaN									0	ctal:	377 330 377 340	
Unsigned 1	5 bit	65	496				3	Float	64 b	it: [-	7.02	2101	6560	01957	7E+3	07				Bir	hary:	11111111 11011000 11111111 1	
🗌 Shov	/ littl	e end	dian d	deco	ding				🗆 s	how	unsi	gned	as h	exad	lecim	al			A	SCIL	Text:	7777	
										Off	set	117	0/0	kc0d8	2				Sal	ectio		x0 to 0x178 (0x179 bytes) INS	

Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 10) – Day 3 of the Black Hat class

### Carving a JPG Out of a Web Proxy Cache



Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 10) – Day 3 of the Black Hat class

### Malware – Metasploit in Network Traffic

F <u>i</u> lter:		•	E <u>x</u> pression Cl	ea <u>r</u> App <u>l</u> y	
No	Time	Source	Destination	Protocol	Info
1652	2 2010-04-28 17:42:02.001752	10.10.10.70	10.10.10.10	ТСР	[TCP Port numbers reused]
1653	3 2010-04-28 17:42:02.001815	10.10.10.10	10.10.10.70	ТСР	4445 > 1044 [RST, ACK] Se
1654	2010-04-28 17:42:02.548001	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [SYN] Seq=197
1655	2010-04-28 17:42:02.548065	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [RST, ACK] Se
1656	2010-04-28 17:42:02.985483	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [SYN] Seq=197
1657	2010-04-28 17:42:02.985580	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [SYN, ACK] Se
1658	3 2010-04-28 17:42:02.985870	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [ACK] Seq=197
1659	2010-04-28 17:42:03.217075	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [PSH, ACK] Se
1660	2010-04-28 17:42:03.220699	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143
1661	2010-04-28 17:42:03.220800	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143
1662	2 2010-04-28 17:42:03.221154	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [ACK] Seq=197
1663	2010-04-28 17:42:03.221372	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143
Win	dow size: 5840				
Þ Che	cksum: 0x0730 [correct]				
≬ [se	Q/ACK analysis]				
	(1460 bytes)				
	a: 405AE8000000005B52455589E5				
		81C3CB110000FFD3890	.30/		
[ [Le	ngth: 1460]				
0030 16	6 d0 07 30 00 00 <mark>4d 5a e8 00</mark>	00 00 00 5b 52 45	0MZ		
	589e581c3cb110000ff	d3 89 c3 57 68 04	U	Wh.	
0050 00	0 00 00 50 ff d0 68 f0 b5 a2	56 68 05 00 00 00	PhVh.		
0060 50	offd300000000000000000	00 00 00 00 00 00	Р		
0070 00	0 00 d8 00 00 00 0e 1f ba 0e	00 b4 09 cd 21 b8	<b>.</b>	. ! .	

.L.!This

progra

be run

DOS mo de....9

Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 12) - Day 4 of the Black Hat class

01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d

20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69

6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00

00 00 00 00 00 00 8a e2 9d d8 ce 83 f3 8b ce 83

© TechTarget

0080

0090

00a0

00b0

00c0

### Malware – Bad Bad JavaScript

Filter:	ip.addr == 10.10.10.70) && (ip.ad	dr == 10.10.10.10)	▼ Expression C	lea <u>r</u> App <u>l</u> y				
No	Time	Source	Destination	Protocol	Info			
2332	2010-04-28 17:39:59.311284 2010-04-28 17:39:59.311382 2010-04-28 17:39:59.656689 2010-04-28 17:39:59.656768 2010-04-28 17:39:59.656892 2010-04-28 17:39:59.657013 2010-04-28 17:39:59.657108	10.10.10.70 10.10.10.10 10.10.10.10 10.10.10.10 10.10.10.10 10.10.10.10 10.10.10.70	10.10.10.10 10.10.10.70 10.10.10.70 10.10.10.70 10.10.10.70 10.10.10.70 10.10.10.10	HTTP TCP TCP TCP TCP TCP TCP TCP	GET /index.php HTTP/1.1 8080 > 1035 [ACK] Seq=3420183379 Ack=3905816560 Win=8576 Len=0 [TCP segment of a reassembled PDU] [TCP segment of a reassembled PDU] [TCP segment of a reassembled PDU] [TCP segment of a reassembled PDU] 1035 > 8080 [ACK] Seq=3905816560 Ack=3420189219 Win=65535 Len=0			
10 10 11	2 2010-04-28 17:39:59.657213 2 2010-04-28 17:39:59.773396 2 2010-04-28 17:39:59.773513 2 2010-04-28 17:39:59.878427 2 2010-04-28 17:40:00.048501 2 2010-04-28 17:40:00.048501	10.10.10.10 10.10.10.70 10.10.10.10 10.10.10.10 10.10.10.70	10.10.10.70 10.10.10.10 10.10.10.70 10.10.10.70 10.10.10.10	HTTP HTTP TCP HTTP TCP	HTTP/1.1 200 OK (text/html) GET /index.phpmfKSxSANkeTeNrah.gif HTTP/1.1 8080 > 1035 [ACK] Seg=3420189251 Ack=3905816921 Win=9648 Len=0 HTTP/1.1 200 OK (GIF89a) 1035 > 8080 [ACK] Seg=3905816921 Ack=3420189398 Win=65356 Len=0			
<pre>     Internet Protocol, Src: 10.10.10.10.10.10.10.10.10), Dst: 10.10.10.70 (10.10.10.70)     Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 1035 (1035), Seq: 3420189219, Ack: 3905816560, Len: 32     [Reassembled TCP Segments (5872 bytes): #3(1460), #4(1460), #5(1460), #6(1460), #8(32)]     Hypertext Transfer Protocol     Line-based text data: text/html     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">    \n</pre>								
var var for {\r c	(i = 0; i < 1300; i++)∖n SNgVkOrdIjaiFpPTfDjbPHQppHSG SNgVkOrdIjaiFpPTfDjbPHQppHSG	SGTZPMOOYQEbLEFxNq tzpmOOyqEbLEFxNqAx	icRyZKKWiRWmUaDHF	=OuzHPHqLrR	rRFSzQuPusTnQyqpQwVpARdlR = new Array();\n FSzQuPusTnQyqpQwVpARdlR[i] = document.createElement(UWnHADOfYHiHDDXj) FSzQuPusTnQyqpQwVpARdlR[i].data = "vEI";\n			
4								
00f0 6 0100 5 0110 4 0120 4 0130 4 0130 7	d       45       4e       54       22       3b       0a       76       61       72         b       4f       72       64       49       6a       61       69       46       70         0       48       51       70       70       48       53       47       74       72         5       62       4c       45       46       78       42       71       41       78         5       70       52       57       6d       55       61       44       48         8       71       4c       72       52       24       53       7a       51       75         9       71       70       51       77       56       70       41       52         8       71       4c       72       52       46       53       7a       51       75         9       71       70       51       77       56       70       41       52       64         86       bytes       Reassembled TCP (58)       58       59       59       59       50       50       50       50       50       50       50	) 50 54 66 44 6a 6 1 70 6d 4f 4f 79 7 3 69 63 52 79 5a 4 3 46 4f 75 7a 48 5 5 50 75 73 54 6e 5 1 6c 52 20 3d 20 6	Z kordījai FpPT 1 PHQppHSG tzpm 5 EbLEFxNq Axic 0 KWiRWmUa DHFQ 1 HqLrRFSz QuPu	fDjb 100yq RyZK JuzHP IsTNQ				

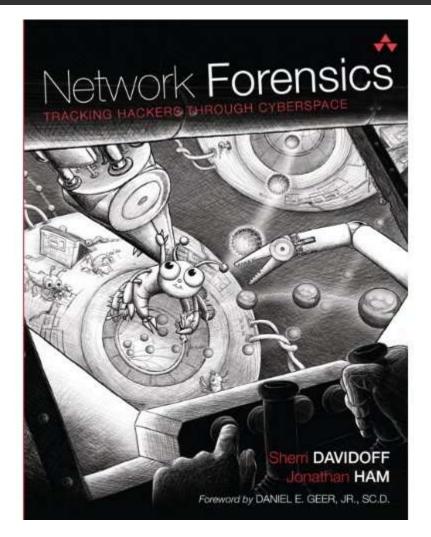
### From "Network Forensics" (ch. 12) – Day 4 of the Black Hat class

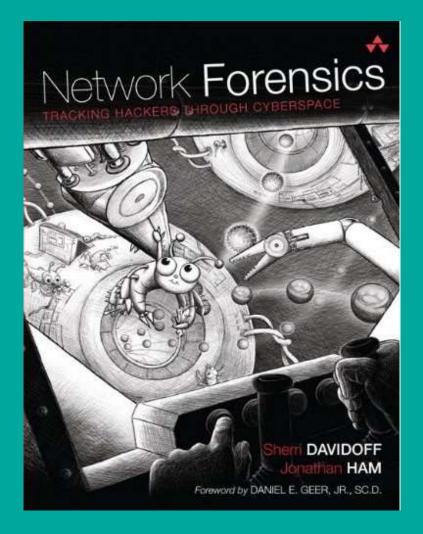
Image: Copyright LMG Security, 2011. Used with permission. 12

## **'Network Forensics'**

- The book!
  - Brand new material
  - Released next week
- Also: Join us at Black Hat
  - 4-day intensive class
  - Taught by the authors
  - Network Forensics: Black Hat Release
  - July 21-24
  - Register today!

### http://NetForensicsClass.com





# TechTarget Questions?

Send them to Sherri and Jonathan via the text chat area on the left

- Select "Presenters" to submit your question privately
- We'll answer as many as we can!

# The speakers:

Sherri Davidoff & Jonathan Ham - sherri@Imgsecurity.com - jonathan@Imgsecurity.com

Join us at Network Forensics: Black Hat Release (July 21-24) - http://NetForensicsClass.com