Trace File Analysis

Worms, Backdoors, etc.

Laura Chappell
Founder | Wireshark University

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

Case Studies

1. Company servers ‘locked down’ on Thanksgiving morning; traffic paths indicate tunnel into network from a foreign country
2. Network traffic to and from the compromised host revealed a back-channel and the propagator of the malicious code
3. Excessive outbound traffic alerted the staff to a possible data leak; examination of the data flow and the target confirmed the leak
4. Unique peer-to-peer data flow prompted the IT team to investigate; the investigation revealed improper network use, but no security leak

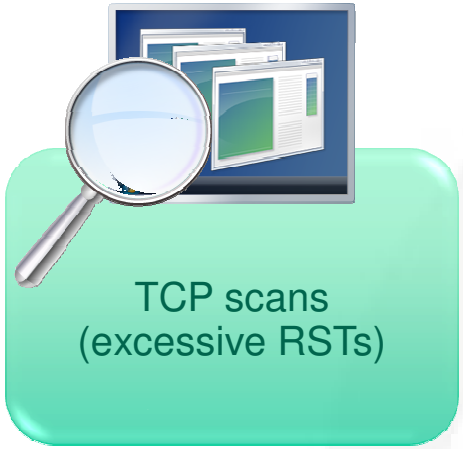
See notes from session T2-7: An Introduction to Network Forensics

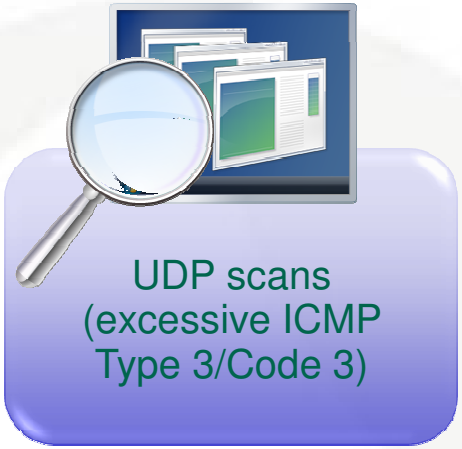
Tap-In Points

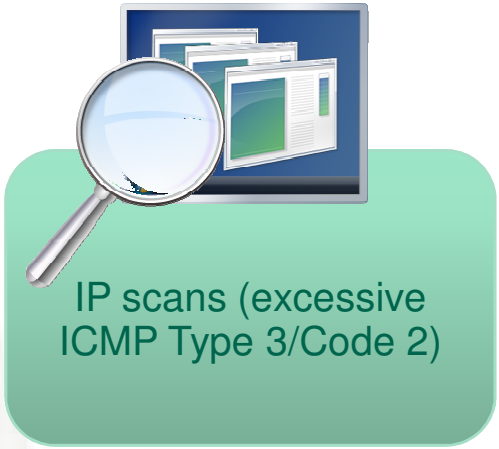
Tap-in points

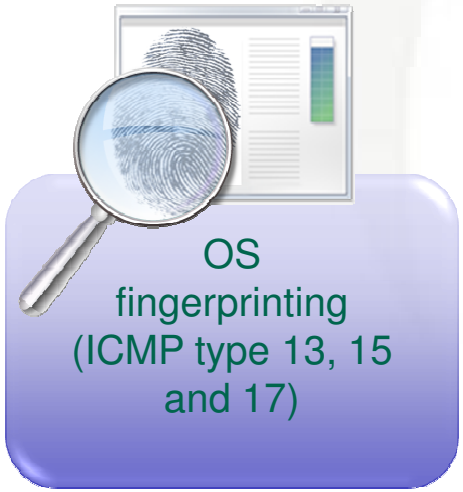
- Hub networks: Easy
- Switch networks: Issues
- Routed networks: Issues
- Full-duplex: Issues

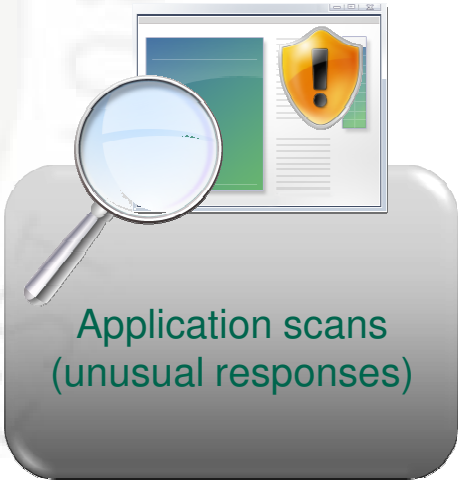
Evidence of Reconnaissance











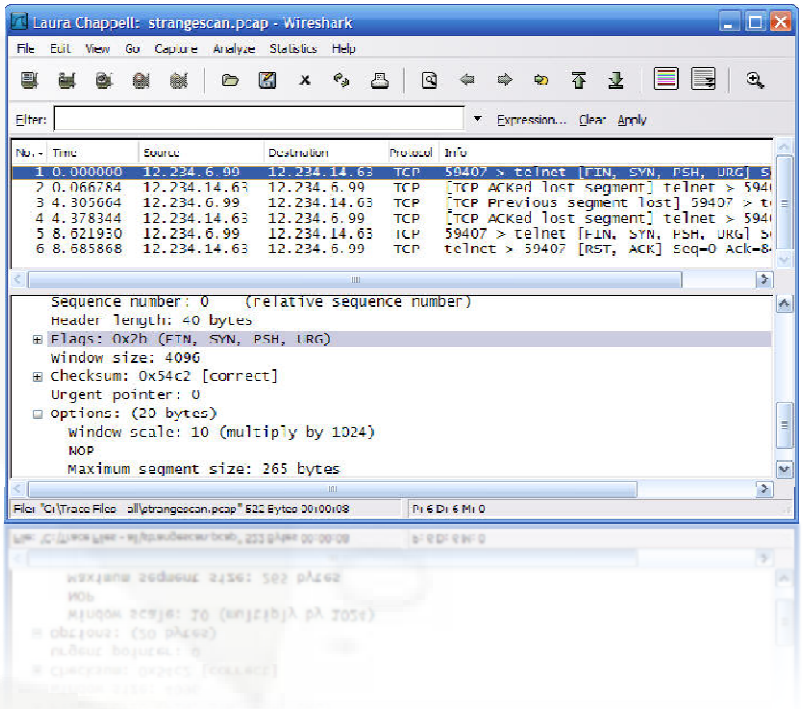
CACE TECHNOLOGIES

Download the free ICMP protocol poster:
www.packet-level.com/downloads.htm

www.wiresharkU.com
WIRESHARK UNIVERSITY

Evidence of Attacks and Breaches

- Unusual communication pairs
- Unusual protocols and ports
- Excessive failed connections
- Unusual inbound connections
- Unusual outbound connections
- Peer-to-peer traffic paths



CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

Unusual Traffic Patterns

blaster.pcap	(LLK9)
bootup-infection.pcap	(not a public trace file)
sick-client.pcap	(LLK9)
arp-poison.pcap	(LLK9)
macof.pcap	(LLK9)
secret-ftp.pcap	(LLK9)
clientdying.pcap	(LLK9)
evilprogram.pcap	(LLK9)

Signature information: www.snort.org or www.bleedingthreats.net

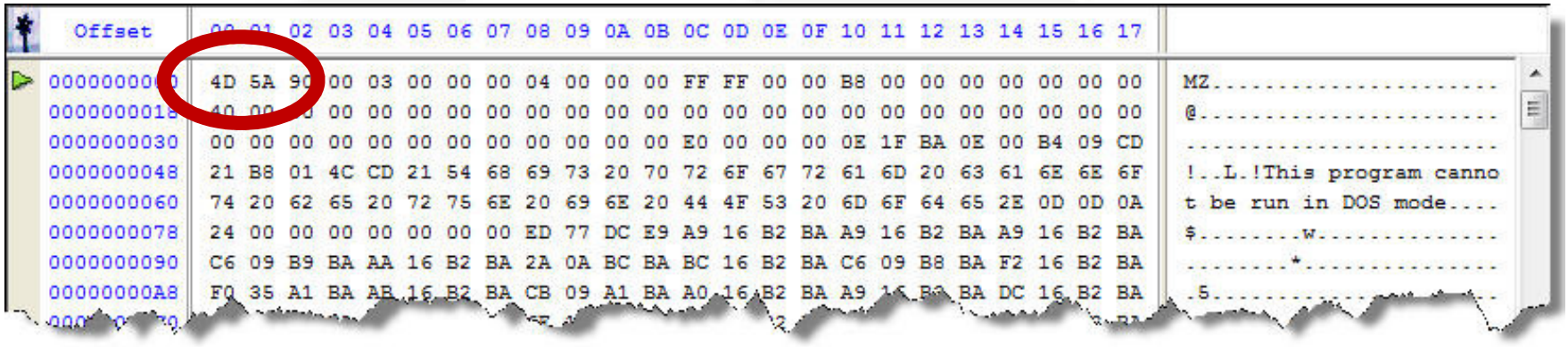
Sample Signatures

#by Lance James and Michael Ligh, referenced in paper at http://ip.securescience.net/advisories/pubMalwareCaseStudy.pdf

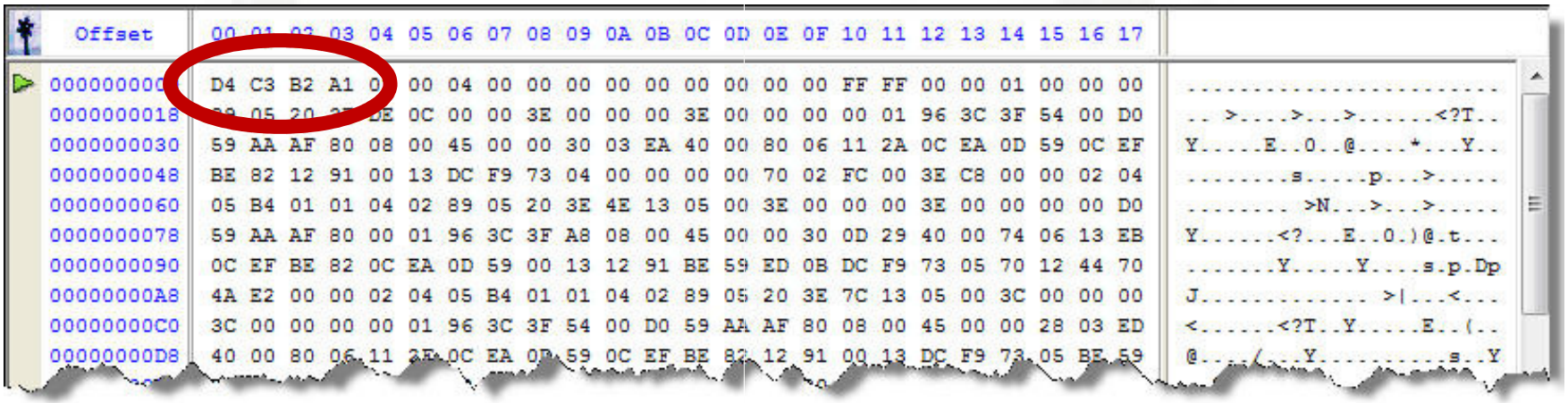
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"BLEEDING-EDGE TROJAN Prg Trojan v0.1-v0.3 Data Upload"; flow:to_server,established; content:"POST"; uricontent:"php?"; content:"Content-Type|3a20|binary"; within:512; content:"LLAH"; within:512; reference:url,ip.securescience.net/advisories/pubMalwareCaseStudy.pdf; classtype:trojan-activity; sid:2003182; rev:2;)

Signatures in File Transfers

Use a hex viewer on files to locate the file signatures



Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17	
0000000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00	MZ.....
0000000018	40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@.....
0000000030	00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00 0E 1F BA 0E 00 B4 09 CD	.....
0000000048	21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	!..L.!This program canno
0000000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A	t be run in DOS mode....
0000000078	24 00 00 00 00 00 00 00 ED 77 DC E9 A9 16 B2 BA A9 16 B2 BA A9 16 B2 BA	$........w.....
0000000090	C6 09 B9 BA AA 16 B2 BA 2A 0A BC BA BC 16 B2 BA C6 09 B8 BA F2 16 B2 BA	........*.....
00000000A8	F0 35 A1 BA AB 16 B2 BA CB 09 A1 BA A0 16 B2 BA A9 16 B2 BA DC 16 B2 BA	.5.....



Offset	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17	
0000000000	D4 C3 B2 A1 0 00 04 00 00 00 00 00 00 00 00 00 FF FF 00 00 01 00 00 00	.....
0000000018	39 05 20 3 DE 0C 00 00 3E 00 00 00 3E 00 00 00 00 01 96 3C 3F 54 00 D0	.. >....>...>.....<?T..
0000000030	59 AA AF 80 08 00 45 00 00 30 03 EA 40 00 80 06 11 2A 0C EA 0D 59 0C EF	Y.....E..0..@....*...Y..
0000000048	BE 82 12 91 00 13 DC F9 73 04 00 00 00 00 70 02 FC 00 3E C8 00 00 02 04	.....s.....p...>.....
0000000060	05 B4 01 01 04 02 89 05 20 3E 4E 13 05 00 3E 00 00 00 3E 00 00 00 00 D0	..... >N...>...>.....
0000000078	59 AA AF 80 00 01 96 3C 3F A8 08 00 45 00 00 30 0D 29 40 00 74 06 13 EB	Y.....<?...E..0.)@.t...
0000000090	0C EF BE 82 0C EA 0D 59 00 13 12 91 BE 59 ED 0B DC F9 73 05 70 12 44 70	.....Y.....Y....s.p.Dp
00000000A8	4A E2 00 00 02 04 05 B4 01 01 04 02 89 05 20 3E 7C 13 05 00 3C 00 00 00	J..... >|...<...
00000000C0	3C 00 00 00 00 01 96 3C 3F 54 00 D0 59 AA AF 80 08 00 45 00 00 28 03 ED	<.....<?T..Y.....E..(..
00000000D8	40 00 80 06 11 2A 0C EA 0D 59 0C EF BE 82 12 91 00 13 DC F9 73 05 BE 59	@....*...Y.....s..Y

CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

What's Next?

Laura's Lab Kit v9

In show bags as well as…

ISO image: www.novell.com/connectionmagazine/laurachappell.html

CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY