

An Introduction to Network Forensics

Identifying Reconnaissance and Attack
Processes on the Network

Laura Chappell

Founder | Wireshark University

SHARKFEST '08

Foothill College

March 31 - April 2, 2008

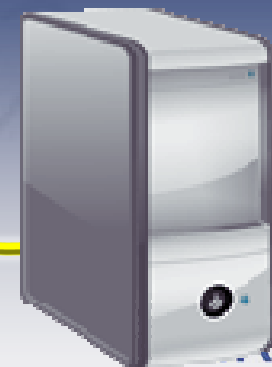
Case Studies

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

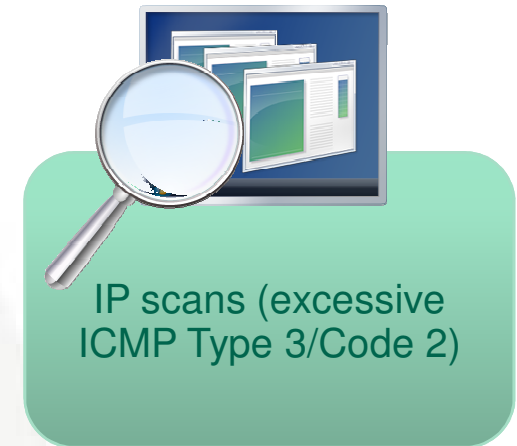
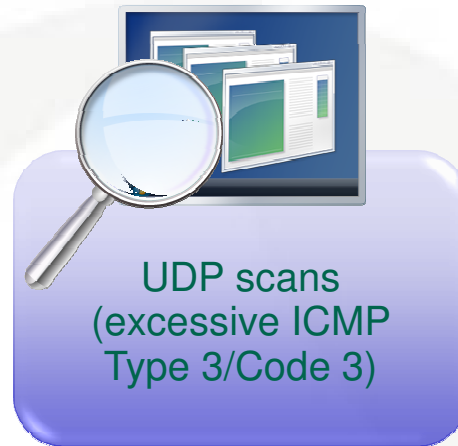
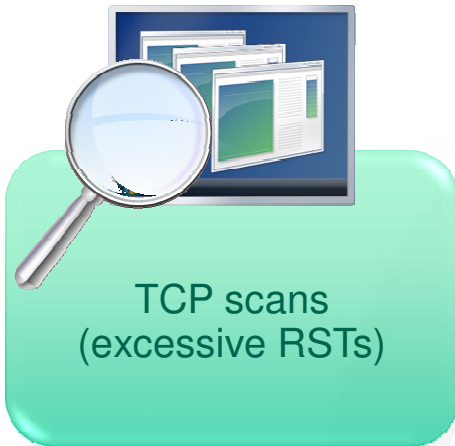
Tap-In Points

Tap-in points

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



Evidence of Reconnaissance



Evidence of Attacks and Breaches

! Unusual communication pairs

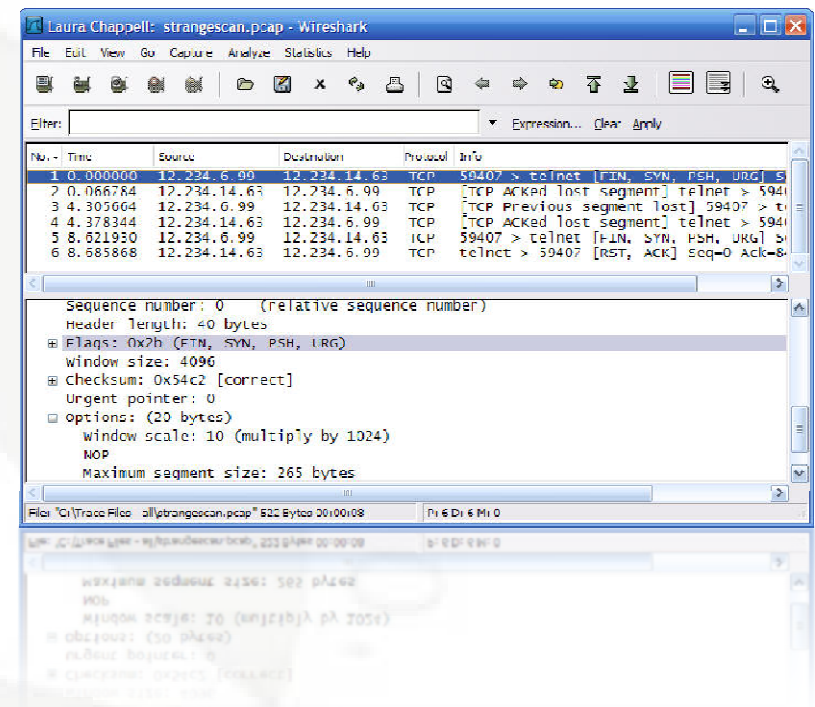
! Unusual protocols and ports

! Excessive failed connections

! Unusual inbound connections

! Unusual outbound connections

! Peer-to-peer traffic paths



Reviewing Unusual Traffic

bootup-infection.pcap	(not a public trace file)
nmap-ipscan.pcap	(LLK9)
active-scan.pcap	(LLK9)
sick-client.pcap	(LLK9)

Signature information:

- www.snort.org
- www.bleedingthreats.net

What's Next?

Laura's Lab Kit v9

In show bags as well as...

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

