# ‘Safe’ network analysis

## Generating network traffic captures within a virtual network.

Presented by Andrew Martin

# Introduction

- What is a sniffer
- How does sniffing work
- Usages
- Scenarios
- Building safe repositories using VM technologies
- Wireshark
- Movie

# What is a sniffer

- Sniffer is a term given to applications that capture network data
- Some examples include:
  - Wireshark
  - Snort
  - EtherApe

# How does sniffing work?

- Data enters the network
- NICs are supposed to be honest and turn away packets not meant for them
- Sniffing applications simply tell the NIC card to lie

# Applications

- Both legitimate and illegitimate purposes
- End users complaining of network “problems”
- User cannot connect to a machine
- Curiosity over one’s instant messenger conversation
- Need access to a system to which you currently have no access

# Problem

- Educate students about network sniffing technologies
- Production networks generate massive amounts of traffic
  - Realtime analysis is impractical
- Protect privacy of network users

# Situation

- Capture data and store it for later educational analysis
- AND keep network users' data private?

# Solution

- Solution 1: Capture traffic and analyze it later
  - Chances are private data will be captured
- Solution 2: Capture traffic on a non-production network
  - Costly to create a non-production network
- Solution 3: Create virtual network and capture traffic
  - Ding ding ding, we have a winner!

# Virtualization

- It's not new
  - Been around since the 1960s
- Cheap
- Can run off a fairly low-end PC
- One PC can host a slew of VM
- Create a heterogeneous virtual lab with just one PC

# Virtual Lab Setup

- Host: VMWare Workstation
- Guests: FreeBSD, Red Hat 7.3, Windows 2000
- FreeBSD - extensive collection of software apps
  - security utilities easily installed via port
- Red Hat 7.3 & Windows 2000
  - relatively old and susceptible to network attacks

# Virtual Lab Setup Cont'd

- Network is a virtual network controlled by VMWare workstation
- Uses private addresses
- Connected to the outside world via using N.A.T.

# Capturing network traffic

- Build a repository consisting of two types of traffic
- Normal
  - FTP, HTTP, SMTP, IRC, SSH...
- Irregular
  - Network scans, exploits, infected computers
  - using tools such as nmap, or metasploit framework

# Personal Favorite


- Wireshark (formally Ethereal)
- Network traffic capturer and analyzer
- Uses libpcap (or winpcap) library to abstract network types and support many more networks
- Intuitive interface
- Supports capture and display filters

# Useful Techniques

- ARP Spoofing / Poisoning Detection
  - Attacker will try to trick a target into “thinking” that the attacker is not who they say they are
  - Wireshark can easily detect such attacks
    - ARP -- simple filter
- tshark can be scripted to automatically capture traffic
  - scripts can be written to parse data to look for certain types of network data - lua.org

# Getting what you want

- There are many filters that can be applied
  - network - net 192.168.1.0/24
  - source - src 192.168.1.15
  - destination - dst 192.168.1.10
  - host - host 192.168.1.1
- Combining filters is quite useful
  - dst port 135 and tcp port 135 and ip[2:2]==48 (blaster worm)

# Display filters

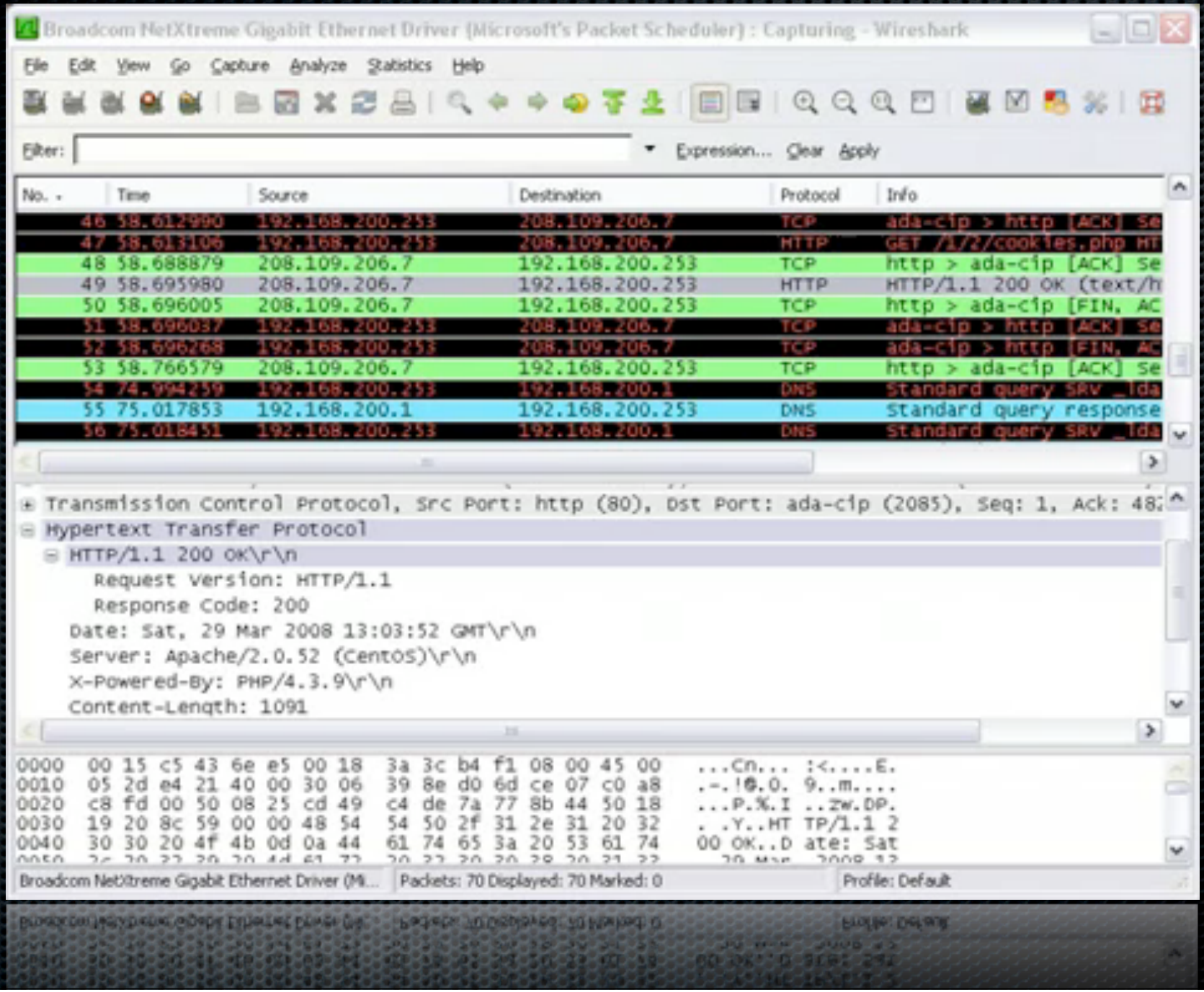
- Capture filters and display filters sometimes have different reserved words
- Display filters have a nice front end for assistance

# TCP Streams

- Follow TCP stream
  - wireshark will display the application layer data in the order in which it was received

# Packet reassembly

- Save packets that contain binary data, and fuse them together


Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
46 58.612990 192.168.200.253 208.109.206.7 TCP ada-cip > http [ACK] Se
47 58.613106 192.168.200.253 208.109.206.7 HTTP GET /1/2/cookies.php HT
48 58.688879 208.109.206.7 192.168.200.253 TCP http > ada-cip [ACK] Se
49 58.695980 208.109.206.7 192.168.200.253 HTTP HTTP/1.1 200 OK (text/h
50 58.696005 208.109.206.7 192.168.200.253 TCP http > ada-cip [FIN, AC
51 58.696037 192.168.200.253 208.109.206.7 TCP ada-cip > http [ACK] Se
52 58.696268 192.168.200.253 208.109.206.7 TCP ada-cip > http [FIN, AC
53 58.766579 208.109.206.7 192.168.200.253 TCP http > ada-cip [ACK] Se
54 74.994459 192.168.200.253 192.168.200.1 DNS Standard query SRV _lda
55 75.017853 192.168.200.1 192.168.200.253 DNS Standard query response
56 75.018451 192.168.200.253 192.168.200.1 DNS Standard query SRV _lda
Transmission Control Protocol, Src Port: http (80), Dst Port: ada-cip (2085), Seq: 1, Ack: 48
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Request Version: HTTP/1.1
Response Code: 200
Date: Sat, 29 Mar 2008 13:03:52 GMT\r\n
Server: Apache/2.0.52 (CentOS)\r\n
X-Powered-By: PHP/4.3.9\r\n
Content-Length: 1091
0000 00 15 c5 43 6e e5 00 18 3a 3c b4 f1 08 00 45 00 ...Cn... :<....E.
0010 05 2d e4 21 40 00 30 06 39 8e d0 6d ce 07 c0 a8 .-.!@.0. 9..m....
0020 c8 fd 00 50 08 25 cd 49 c4 de 7a 77 8b 44 50 18 ...P.%.I ..zw.DP.
0030 19 20 8c 59 00 00 48 54 54 50 2f 31 2e 31 20 32 . .Y..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..D ate: Sat
Broadcom NetXtreme Gigabit Ethernet Driver (Mi...
Packets: 70 Displayed: 70 Marked: 0
Profile: Default

# Conclusion

- Privacy is incredibly important while educating students on the importance of network analyzation
- Best to generate samples on a private network
- Virtual networks are much cheaper than physical networks
- Wireshark in the hands of a skillful user is both powerful and dangerous

# References


- http://www.wireshark.org/docs/wsug_html_chunked/
- http://wiki.wireshark.org/TCP_Reassembly
- http://www.wiresharktraining.com/
- http://en.wikipedia.org/wiki/ARP_spoofing
- P. Li, C. Li, T. de Mohammed. Building a repository of network traffic captures for information assurance education. Journal of Computing Sciences in Colleges 2009. Pages 99-105
- http://www.vmware.com/
- http://www.youtube.com/watch?v=7ezGTP99xSw