Network Monitoring and Traffic Analysis
Network Monitoring

Agenda

- A Quick Review of Network Monitoring
- A Collection of Common Network Traffic Tools
  - This Will be a “Play As We Go” Lecture
  - The Tools We Will Cover:
    - FlowTools, Sniffers, Graphical, and Hacker
Network Monitoring

- FlowTools
  - flow-capture, flow-cat, flow-nfilter, flow-report
- Sniffers
  - tcpdump, (snort), nload, iptraf
- Graphical Tools
  - wireshark, etherape, ntop
- Hacker Tools
  - dsniff, driftnet, ettercap
Warning

- We’ll Be Sniffing Traffic From Here On Out
- dsniff will be running during this lecture
- We’ll Report At the End If We Caught Anything
Monitoring Location

- Tends to be at the Distribution Layer (center) of Your Network
- On HP Switches, it’s called the “Monitor Port”
- On Cisco Switches, it’s called the “SPAN Port”
- Cisco Switches have much more powerful Capabilities for controlling the Monitoring, can control RX and TX, and even forward to another switch: RSPAN
Monitor Location

- Can be Off a passive Optical Splitter (fiber)
- Need Out-of-Band Management Only (you do not want this box getting hacked... ever!)
- Requires Powerful Box: CPU/MEMORY/IO
- May need to tune NIC
- May need to tune OS
- see: ethtool, and sysctl
Promiscuous Mode

- Some of These Commands do NOT put the interface into “promiscuous mode”. To sniff all frames you need to be in promiscuous mode.

- This means your NIC will pay attention to more frames instead do just your own IP/MAC frames.

- To force promiscuous mode if necessary:
  - `sudo ifconfig eth0 promisc`

- To turn off promiscuous mode if necessary:
  - `sudo ifconfig eth0 -promisc`
FlowTools

🔺 A Cisco Router Export Flow Format: NetFlow
🔺 A Standard for Connecting Packet Statistics
🔺 Information tends to include additional Router Information, such as ASPATH
🔺 You must configure the router to export flows
🔺 Different Versions: v5, v7, etc. Make sure that you export a version that is the same as your collector
FlowTools

How it Works

• The Router Samples Packets
• This is a “lossy” Mechanism
• Flows are “connection” oriented
• The export to the collector is over UDP
• The Traffic can be fairly High
• A Single SYN packet will generate a “flow”
FlowTools

- Installation on the Collector
  - `sudo apt-get install flow-tools`
  - `dpkg -L flow-tools`
- Configuration in `/etc/flow-tools`
- Startup is `/etc/init.d/flow-capture`
- Startup config is `/etc/init.d/flow-capture.conf`
- Example: `-w /var/flow 0/0/3002`
  - Listen on port 3002 from anywhere
Simple Processing Example:
Report All Flows For Yesterday

#!/usr/bin/perl

@files=`find /flows -type f -daystart -mtime -1`; chomp(@files);

foreach $file (@files) {
open(INPUT,"flow-cat $file | flow-report | ");
while(<INPUT>) { print; }
}

Network Monitoring

11

Wireless Network Security
FlowTools: Output Format

- Defaults for flow-report command
- Configured in: /etc/flow-tools/stat.cfg
- Sorting can be any of: flows, octets, packets, duration, avg-pps, min-pps, max-pps, avg-bps, min-bps, max-bps
FlowTools: Output Format

```
stat-report default
type @{TYPE:-ip-source/destination-address/
ip-protocol/ip-tos/ip-source/destination-port}
output
format ascii
sort @{SORT:-+flows}
fields @{FIELDS:-+}
options @{OPTIONS:-+header,+xheader,+totals}
path | flow-rptfmt @{RPTOPT:--f ascii}
stat-definition default
report default
```
FlowTools: Filter Format

- Define Address Matches

- Filter "Primitives" plus Filter "Definitions" To Make Matches

filter-primitive UDPTCP
  type ip-protocol
  permit tcp
  permit udp

filter-definition udptcp
  match ip-protocol UDPTCP

filter-primitive mynetaddr
  type ip-address-mask
  permit 123.234.0.0 255.255.0.0
  default deny

filter-definition mynet
  match ip-source-address mynetaddr
  match ip-destination-address mynetaddr
FlowTools: Commands

Flow Tools Binaries - Chaining Commands

% flow-cat  # concatenate binary flow files and output
% flow-nfilter  # apply filters to input flow stream
% flow-report  # process and output flow reports

Example:

flow-cat $filelist | flow-nfilter -F $filterdef | flow-report -S
$report-format
FlowTools: Web Interface

- There are Three Web CGI Interface Tools
- FlowViewer, FlowGrapher, and FlowTracker
- Website: [http://ensight.eos.nasa.gov/FlowViewer/](http://ensight.eos.nasa.gov/FlowViewer/)
**FlowReport**

Report: 132 Columns
Start Time: December 12, 2007 17:00:00 GMT
Device: gsfc_6509
Source:

Source Port:
Source I/F: 7, 62
Source AS:
DSCP Field:
Include if: Any part of flow in Time Period
Lines Cutoff: 100

<table>
<thead>
<tr>
<th>Start</th>
<th>End</th>
<th>Sif</th>
<th>SrcIPaddress</th>
<th>SrcP</th>
<th>DIF</th>
<th>DstIPaddress</th>
<th>DstP</th>
<th>P</th>
<th>Fl</th>
<th>Pkts</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1212.16:28:15.506</td>
<td>1212.17:00:15.669</td>
<td>62</td>
<td>172.160.254.16</td>
<td>22</td>
<td>0</td>
<td>111.222.162.166</td>
<td>1837</td>
<td>6</td>
<td>0</td>
<td>66</td>
<td>4620</td>
</tr>
<tr>
<td>1212.16:20:828</td>
<td>1212.17:00:20.828</td>
<td>7</td>
<td>172.160.195.52</td>
<td>3045</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32771</td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1212.16:20:836</td>
<td>1212.17:01:20.836</td>
<td>7</td>
<td>172.160.195.52</td>
<td>3045</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32771</td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1212.16:29:43.005</td>
<td>1212.17:01:53.025</td>
<td>62</td>
<td>172.160.254.52</td>
<td>22</td>
<td>0</td>
<td>111.222.162.166</td>
<td>1415</td>
<td>6</td>
<td>0</td>
<td>846</td>
<td>887540</td>
</tr>
<tr>
<td>1212.16:21:09.092</td>
<td>1212.17:02:15.092</td>
<td>7</td>
<td>172.160.195.2</td>
<td>53</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32768</td>
<td>17</td>
<td>1</td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>1212.16:30:29.323</td>
<td>1212.17:01:36.422</td>
<td>62</td>
<td>172.160.195.52</td>
<td>3045</td>
<td>0</td>
<td>198.119.135.34</td>
<td>50500</td>
<td>6</td>
<td>0</td>
<td>134</td>
<td>20656</td>
</tr>
<tr>
<td>1212.16:21:09.092</td>
<td>1212.17:02:15.092</td>
<td>7</td>
<td>172.160.195.2</td>
<td>53</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32768</td>
<td>17</td>
<td>1</td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>1212.16:31:14.747</td>
<td>1212.17:03:14.373</td>
<td>62</td>
<td>172.160.254.18</td>
<td>22</td>
<td>0</td>
<td>111.222.162.163</td>
<td>35690</td>
<td>6</td>
<td>0</td>
<td>66</td>
<td>5544</td>
</tr>
<tr>
<td>1212.17:03:00.620</td>
<td>1212.17:03:00.620</td>
<td>7</td>
<td>172.160.195.2</td>
<td>53</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32768</td>
<td>17</td>
<td>1</td>
<td></td>
<td>176</td>
</tr>
<tr>
<td>1212.17:03:20.848</td>
<td>1212.17:03:20.848</td>
<td>7</td>
<td>172.160.195.52</td>
<td>3045</td>
<td>0</td>
<td>172.160.220.2</td>
<td>32771</td>
<td>6</td>
<td>1</td>
<td></td>
<td>141</td>
</tr>
<tr>
<td>1212.16:59:35.670</td>
<td>1212.17:00:00.032</td>
<td>62</td>
<td>172.160.254.27</td>
<td>53817</td>
<td>0</td>
<td>137.78.58.79</td>
<td>20378</td>
<td>6</td>
<td>0</td>
<td>9700</td>
<td>13741937</td>
</tr>
</tbody>
</table>
FlowGrapher

Report: Flow Graph Bits/Second
Start Time: December 11, 2007 19:00:00 GMT
End Time: December 11, 2007 20:00:00 GMT
Sample Time: 5s
Exporter:
Destination Port:
Source:
Source Port:
Source AS:
Protocol:
TOS Field:
Include if: Any part of flow in Time Period
Detail Lines: 20

Flow data from gsfc_6509

<table>
<thead>
<tr>
<th>Start</th>
<th>End</th>
<th>Len</th>
<th>Source Host</th>
<th>Port</th>
<th>Destination Host</th>
<th>Port</th>
<th>Total Bytes</th>
<th>Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>19:27:06</td>
<td>19:28:42</td>
<td>95.7</td>
<td>xxgur.mocsan.mirh.org</td>
<td>36392</td>
<td>samantha.cral.mirh.org</td>
<td>50676</td>
<td>101,199,734</td>
<td>8.457</td>
</tr>
<tr>
<td>19:28:44</td>
<td>19:30:28</td>
<td>104.5</td>
<td>xxgur.mocsan.mirh.org</td>
<td>36462</td>
<td>samantha.cral.mirh.org</td>
<td>19602</td>
<td>101,174,434</td>
<td>7.742</td>
</tr>
</tbody>
</table>
SNIFFERS
Can Do Flag Matching Using TCPDUMP


SYN Grabbing:

'tcp[13] & 0xFF == 0x2'

SYN/ACK Grabbing:

'tcp[13] & 0xFF == 0x12'

Example Command Line:

'/usr/sbin/tcpdump -n -i eth1 -s 64 -w /data/tcp/synackdata/${HOUR} 'tcp[13] & 0xFF == 0x12' < /dev/null 1>/dev/null 2>&1 &
TRY IT!

run tcpdump on the command-line, match SYN using the flags option:  \texttt{tcp[13] \& 0xFF == 0x02}
NLOAD

- This is a quick command-line curses view of the traffic total on your interface
- `sudo apt-get install nload`
- Example: `% nload -u m -i 200`
- megabits/second, 200msec update interval
- TRY IT!
**NLOAD**

Network Monitoring

---

Incoming:

```
#..............................................
#..............................................
#..............................................
#..............................................
#..............................................
| #..............................................
| #..............................................
#..............................................
```

| #.............................................. | Curr: 95394.72 kBit/s  
| #.............................................. | Avg: 8439.34 kBit/s 
| #.............................................. | Min: 0.00 kBit/s 
| #.............................................. | Max: 95540.48 kBit/s 
| #.............................................. | Ttl: 105.71 MByte |

Outgoing:

```
.. ...... ....
```

```
#..............................................
#..............................................
```

| #.............................................. | Curr: 1427.49 kBit/s  
| #.............................................. | Avg: 126.07 kBit/s 
| #.............................................. | Min: 0.00 kBit/s 
| #.............................................. | Max: 1518.58 kBit/s 
| #.............................................. | Ttl: 1.59 MByte |

---

Wireless Network Security
IPTRAF

- Curses View of Active Talkers and Interface Statistics
- Top Talkers, SRC and DEST
- Sortable by Packet Total, Byte Total ETC.

"monitor" == TCP Connections, Source/Dest
"Detailed" == Interface Only Statistics
"Statistical Breakdown" == by Protocol/Port
"Lan Station Monitor" == by MAC Address
IPTRAF

- Other Options: “o”
  - “R” for DNS Lookups
  - “F” force promiscuous mode
  - “M” show packet sizes

- Filters:
  - Edit Filter, Attach Filter, Detach Filter
  - 10.1.1.1/0:65535 <-> 0.0.0.0/0:0
  - Must Specify Port Ranges
  - SRC/DST Reporting is TCP Only
IPTRAFAF

- Can also run a Batch Mode to a File
  - % iptraf -i eth0 -B
  - % pkill iptraf
  - % cd /var/log/iptraf
- TRY IT!
GRAPHICAL TOOLS
WIRESHARK

- http://www.wireshark.org/
- More than Just a Sniffer
- Protocol Decoding
- Transport Stream Reassembly
- Used to Be “Ethereal”
- Supports Filter Expression Matching
- Supports Reading/Writing Various Captures Formats
- Text-based version is: "tshark"
**WIRESHARK**

- Standard Packet Format is "pcap", (like tcpdump)
- Filter Language is like tcpdump filters
- Output Display Format Supports Naming
  - ethernet oui, tcp/udp ports, hostnames
- Protocol and Traffic Statistics Reporting
- `% sudo apt-get install wireshark`
- **TRY IT!**
Network Monitoring

Wireless Network Security

WIRESHARK

Frame 51 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Parallel_c5:b1:15 (00:1c:42:c5:b1:15), Dst: Parallel_00:00:02 (00:1c:42:00:00:02)
Internet Protocol, Src: 10.211.55.5 (10.211.55.5), Dst: 203.159.31.69 (203.159.31.69)
EtherApe

- Creates a MESH of Talking Nodes In A Window
- Lines in the MESH Get Wider as Traffic Increases
- Includes Protocol Statistics
- Some filtering expression capabilities
NTOP

- Network Monitor Daemon
- [http://www.ntop.org/](http://www.ntop.org/)
- Luca Deri, University of Pisa
- Project is now Ten Years Old!!!
- Named after "top", but for Networks
- Builtin Web Server Interface
- Builtin RRD Graphing
NTOP FEATURES

- Traffic Characterization
- Host Characterization, History, Protocols
- Network Interface Statistics Graphs
- ASN Reporting
- sFLOW/netFlow Reporting
- Can act as Both a Receiver and Sender of NetFlow
- ThruPut Reports
- Activity Reports
- Plugins Provide Additional Feature
NTOP Installation

- `% apt-get install ntop`
- `% dpkg -L ntop`
- NTOP Configuration: `/etc/ntop`
- NTOP Configuration: `/var/lib/ntop/init.cfg`
- `% sudo ntop --set-admin-password`
- `% /etc/init.d/ntop start`
- Now Point Your Browser At:
- `http://localhost:3000`
- TRY IT!
HACKER TOOLS
**DRIFTNET**

- A Sniffer for Grabbing Image Files
- http://ex-parrot.com/~chris/driftnet/
- Also Located on the BackTrack CD
- `% locate driftnet`
- Also able to Grab MPEG Audio Files
- So the Hackers Can Grab Files Too!!!
- TRY IT!
DRIFTNET
DSNIFF

- Dug Song
- http://www.monkey.org/~dugsong/dsniff/
- DSniff, Usenix Conference, Year 2000
- Producing Behavior Change Through Embarrassment!
- A Collection of Tools
DSNIFF

- What Tools Does The DSNIFF Package Include?
  - dsniff, arpspoof, dnsspoof, macof, sshmitm, webmitm, filesnarf, webspy

- What Kind of Password Strings Does it Grab?
  - FTP, Telnet, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec
DSNIFF

- DSNIFF Report: Did we see any ClearText Passwords?