IPv6 and Tunnels
IPv6 and Tunnels in the same presentation?

• The work for both was done around the same time
• Most IPv6 traffic at the time was still tunneled (and likely still is at most sites)
IPv6

• It’s turned on like you’d expect it to be and you can’t turn it off
• Not overly exciting
  – Different addresses in your logs
• Lots of strange edge cases supported
Tunnels

• Everyone has tunnels
  — Even if you don’t know it
• Most tunnels are for locally enabling IPv6 on end hosts
Tunnel Decapsulators

• Teredo
• IP-in-IP (includes 6to4)
• AYIYA
• GTPv1
• SOCKS

— Yes, SOCKS is a proxy protocol but internally we treat it similar to a tunnel
Tunnel Recursion

• Tunnels in tunnels
### Forensic Logs - tunnel.log

<table>
<thead>
<tr>
<th>ts</th>
<th>1232039480.93499</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>YQCEFJ6DEh1</td>
</tr>
<tr>
<td>id</td>
<td>99.241.86.237 50361 10.0.0.254 65123</td>
</tr>
<tr>
<td>tunnel_type</td>
<td>Tunnel::TEREDO</td>
</tr>
<tr>
<td>action</td>
<td>Tunnel::DISCOVER</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ts</th>
<th>1232039548.03295</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>YQCEFJ6DEh1</td>
</tr>
<tr>
<td>id</td>
<td>99.241.86.237 50361 10.0.0.254 65123</td>
</tr>
<tr>
<td>tunnel_type</td>
<td>Tunnel::TEREDO</td>
</tr>
<tr>
<td>action</td>
<td>Tunnel::CLOSE</td>
</tr>
</tbody>
</table>
Forensic Logs - conn.log

<table>
<thead>
<tr>
<th>ts</th>
<th>1232039480.93499</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>YQCEFJ6DEh1</td>
</tr>
<tr>
<td>id</td>
<td>99.241.86.237 50361</td>
</tr>
<tr>
<td>proto</td>
<td>udp</td>
</tr>
<tr>
<td>service</td>
<td>teredo</td>
</tr>
<tr>
<td>duration</td>
<td>66.901215</td>
</tr>
<tr>
<td>orig_bytes</td>
<td>100565</td>
</tr>
<tr>
<td>resp_bytes</td>
<td>23818</td>
</tr>
</tbody>
</table>
### Forensic Logs - `conn.log`

<table>
<thead>
<tr>
<th>ts</th>
<th>1232039480.93499</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>mYlaTkpbEY9</td>
</tr>
<tr>
<td>id</td>
<td>2001:0:4137:9e50:3c6e:3b46:9c0e:a91251232 2001:0:4137:9e50:414:19c:5b94:3ca2 21050</td>
</tr>
<tr>
<td>proto</td>
<td>udp</td>
</tr>
<tr>
<td>service</td>
<td>-</td>
</tr>
<tr>
<td>duration</td>
<td>66.901215</td>
</tr>
<tr>
<td>orig_bytes</td>
<td>85545</td>
</tr>
<tr>
<td>resp_bytes</td>
<td>10386</td>
</tr>
<tr>
<td>tunnel_parents</td>
<td>YQCEFJ6DEh1</td>
</tr>
</tbody>
</table>
Summary

• Awareness of IPv6 and Tunnels in Bro
• Normally don’t need to worry about them