
# 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`

| | |
|---|---|
| ts | 1232039480.93499 |
| uid | **YQCEFJ6DEh1** |
| id | 99.241.86.237 50361 10.0.0.254 65123 |
| tunnel_type | Tunnel::TEREDO |
| action | Tunnel::DISCOVER |

| | |
|---|---|
| ts | 1232039548.03295 |
| uid | **YQCEFJ6DEh1** |
| id | 99.241.86.237 50361 10.0.0.254 65123 |
| tunnel_type | Tunnel::TEREDO |
| action | Tunnel::CLOSE |

# Forensic Logs - `conn.log`

| | | | |
|---|---|---|---|
| ts | 1232039480.93499 | | |
| uid | **YQCEFJ6DEh1** | | |
| id | 99.241.86.237 50361 | 10.0.0.254 | 65123 |
| proto | udp | | |
| service | teredo | | |
| duration | 66.901215 | | |
| orig_bytes | 100565 | | |
| resp_bytes | 23818 | | |

# Forensic Logs - `conn.log`

| | |
|---|---|
| ts | 1232039480.93499 |
| uid | **mYlaTkpbEY9** |
| id | 2001:0:4137:9e50:3c6e:3b46:9c0e:a91251232<br>2001:0:4137:9e50:414:19c:5b94:3ca2 21050 |
| proto | udp |
| service | - |
| duration | 66.901215 |
| orig_bytes | 85545 |
| resp_bytes | 10386 |
| tunnel_parents | YQCEFJ6DEh1 |

# Summary

- Awareness of IPv6 and Tunnels in Bro
- Normally don't need to worry about them