

# TCP and UDP Ready Set Action

---



**Aaron Staines**

NETWORK/SYSTEM ENGINEER | CCISO



# Module Overview



TCP – Web session analysis

UDP – DHCP session analysis



# TCP Web Session Analysis

---



# Wired Brain Coffee Intranet

[Payroll](#)

[Forms](#)

[Directory](#)



Welcome to the new intranet for Wired Brain Coffee. Please note this site is still under construction, and not meant for company use!

# TCP Web Session Analysis



## Get

- Signals a download request

## 200 OK

- Signifies a found requested resource



# TCP HTTP SESSION ANALYSIS



# UDP DHCP Session Analysis

---



# UDP DHCP Session Analysis



Best effort

- No SYN/ACK or FIN
- Uses options

Hard coded ports

- Requesting machine uses 68
- Responding server uses 67





# UDP DHCP SESSION ANALYSIS VIDEO



# UDP DHCP OUTPUT VIDEO



# Module Review



## TCP HTTP primer

- Get - Resource request
- 200 OK - File retrieve successfully

## TCP HTTP analysis

- Multiple session creation
- Acknowledgement & Sequence numbers
- Close session through FIN/ACK



# Module Review



## UDP DHCP primer

- No flags
- Options – Especially DHCP
- Hard coded ports 67 & 68

## UDP session analysis

- Small sessions
- Ports in action
- Analyze DHCP request

