SANS Defense

Primers/Reference

- **Primers**

- Linux CLI 101
- Linux CLI
- PowerShell Get-WinEvent

- **Reference**

- Windows Event Logs Table
- Packet Analysis
- HEX/DEC/ASCII Chart

- **James Summers' TCP/IP Cheat Sheets**

- IP
- IPv6
- TCP
- UDP
- ICMP
- DNS
- Full Packet Analysis SpreadSheet

Tools

- **Key Tools**

- Bro
- freq.py
- tshark
- PowerShell Get-WinEvent

- **Linux Command Line**

- Linux CLI 101
- Linux CLI

BT: Courses|Certs

- **Blue Team Courses**

- 555 - SIEM
- 511 - SecOps
- 503 - IDS
- 505 - Windows
- 506 - Unix
- 579 - Virtualization

- **Upcoming Courses**

- 545 - Cloud (**New**)
- 530 - Architecture (**Upcoming**)
- 487 - OPSEC (**Upcoming**)

- **Blue Team Certifications**

- GMON - 511
- GCIA - 503
- GCWN - 505
- GCUX - 506
- GSE

BT: Faculty

- **Blue Team Authors**

- Eric Conrad, 511

- Jason Fossen, 505
- Justin Henderson, 555
- Judy Novak, 503
- Hal Pomeranz, 506
- Dave Shackleford, 579
- Rob Vandenbrink, 579

- **Blue Team Instructors**

- Instructors