CCDC Skill Set

1. Network Administrator (Villegas)
   1. Setup switches, routers
   2. Ensure basic configuration is setup on network
   3. IP allocation
   4. Network Diagram
   5. Monitor Network
2. System Administration (Cole)
   1. Windows
   2. Unix/Linux
   3. Minimum Requirements
      1. Users, groups, sudo, permissions, passwords
      2. Remote access: ssh, vnc/rdp, access control lists
      3. Database access control: change passwords, identify PII
3. Service Administration (Villegas)
   1. IIS, MySQL, BIND/MS-DNS, Sendmail/ Exchange/qmail, Apache, Samba, OpenSSL, SSH, Microsoft Office, and Active Directory
   2. Firewall
   3. Familiarity with recommended configurations based on NSA Security Guide
4. Generalists
   1. Know how and why stuff is done
5. Forensics (Cole)
   1. Computer Forensics
   2. Logstash
6. Validating security and understanding attack strategies
   1. What does right look like
   2. How to tell when something is acting strange
   3. Tell which ports are open vs which should be open
   4. Chron jobs, services, how to start, restart, and remove
7. Social Engineering
8. Injects
   1. Create Centralized Logging System
   2. Lock Down the Wireless Network
   3. OS/Runtime Vulnerability Scanning
   4. Create Bastion (Jump Host) Infrastructure
   5. Develop Incident Response Procedures
   6. Implement Privileged Account Management
   7. Track Elevation of Privileges
   8. Install an Outbound Proxy
   9. Create Incident Report Template
   10. Provide Recommendations for System Monitoring
   11. Harden Network Cryptography
   12. Provide Recommendations for Alerts
   13. Implement Alerts
   14. Implement Security Event Tracking
   15. Implement Incident Response Tooling
   16. Implement a network packet capturing system
   17. Manage Windows Admin Account Alerts
   18. Create Dashboards
   19. Implement an API Gateway / Application Firewall
   20. Provide Situation Reports
   21. Provide Forensic Investigations
9. Communication
   1. Many injects involve written reports
   2. Team captain should avoid technical jargon