WGU CCDC Plan of Attack – Brainstorming Draft

General Procedures

* Physical sweep
  + Check network connections and label
  + Check for attached devices – usb/wifi/network
* Identify access credentials
  + Documentation
  + Physical – written under keyboard, taped to machine, etc.
* Identify OS
* Identify and list active services on each machine – FTP servers, web servers, etc.

Network

* Change admin pw and restrict/disable add’l users
* Configure Firewall
  + Open/close ports as need on WAN/DMZ side
  + Open/close ports on LAN side as needed.
  + Create alias names for machines and services
  + Assign NAT for any external facing services
* Wireshark
  + Install Wireshark on unused machine in promiscuous mode.
  + Mirror port on router/switch for Wireshark
* Penetration testing/scanning
  + Nmap, nessus, etc.

OS – General

* Admin/root pw resets
* Disable (do NOT delete) all user accounts
* Configure local firewalls (Windows Firewall/Iptables)
* Disable IPv6
* Install patches (or perform in-place upgrades to OS if possible)

OS – Windows

OS – Linux

Services

* DNS
* FTP
* HTTP/S
* SMTP
* SQL/DB
* SSH
* Active Directory
* Other

Applications

* Remove harden various applications (ie. Browsers, notepad, mail clients, etc.)

Tools

* Install log monitoring tools – OSSEC, others
* Install IDS/IPS tools – Snort, others
* Install live streaming services of our competition machines for Red Team to watch (only after all services up for 8 hours straight)