1. Captain
    a. CEO meeting: 1 page = # injects completed/underway, “working on” status of each member of the team, # compromises found/cleaning/removed in detail, future plans on how to deal with injects/team org/compromises.
2. Gopher
    a. Download
    b. Get supplies/food
    c. Step in for Cap
    d. Paperwork injects
    e. Physical security
        i. Check network cables/users/services/pwds every morning
        ii. Baseline and inventory your gear every day
        iii. Look for tape on mouses
        iv. Remove and secure all media (phys/digital) 20min before ending bell
        v. Tag (#graffiti) gear (ex. small pieces of tape to know if someone opened the door)
        vi. GSM bugs? Keyloggers? Wifi Access Points? Voice recorders?
        vii. If fire alarm goes off, ask White Cell if it’s real.
    f. Nerf assaults
3. Firewall Admin
    a. RAISE SHIELDS Mr. Sulu
    b. Monitor outbound connections
    c. Configure firewall
    d. Egress/Ingress filtering
    e. IPv6 OFF
    f. deny any any
    g. WPA2/WPS/wireless OFF + long pass phrase
    h. Pass of incident reports to IR person
    i. CAPRICA (ACL generator): http://code.google.com/p/capirca/
4. Linux Admin
    a. Upgrade kernel
    b. Fail2Ban
    c. If ($PHP) then shoot.self; fix php.ini
    d. SETUID
    e. Monitor auth logs
    f. Create a process list file so IR can diff it
    g. Remove unused users/services
    h. IPTSTATE (TCPview for Linux)
    i. GRSEC if you have time

i. Turn off ability to change grsec settings via sysctl
ii. Turn on EXEC logging
iii. Monitor audit logs for signs of escalation attempts

j. File integrity logging
i. Tripwire
ii. OSSec (use pre-configs)

k. Nothing new should appear here without your say-so:
i. /tmp/
1. .hidden directory
ii. Crontab for all users
iii. ~/.ssh/ (and /root/ not just /home)
iv. /etc/
v. /etc/passwd & /etc/shadow & /etc/sudoers

l. Know all SetUID binaries and watch for new ones

m. Final all 'immutable' files
i. find . | xargs -I file lsattr -a file 2>/dev/null | grep '^....i'
ii. 'chattr -i file' to change it back
iii. Doing this on / takes a long time, point it where it counts: /etc/, ~/, /tmp/ etc.. etc..

5. Windows Admin
a. Event Viewer (your new friend)
b. Autoruns (new bff)
c. Process Explorer + TCP View (bffs)
d. OSSEC
e. Change passwords (automate)
i. dsquery user ou=Users,dc=corp,dc=somewhatrealnews,dc=com | dsmod user -pwd MyPassw0rdChanged! -mustchpwd yes

f. Remove unused users/services
g. Turn firewall on and REMOVE EXCEPTIONS
h. Turn off Teredo
i. Mark Russinovich
j. Progs:
i. AutoIt (make a binary to do it faster = changing user pwds)
ii. http://bit.ly/bulkpasswordcontrol (AD only - not local)
iii. Dsquery user ou=Users, dc=testlab, dc=net | dsmod user -pwd RedTeamSucks! -mustchpwd yes
iv. LAPS (local admin pwds)

k. Group Policy
i. Set security options for GPO
1. Network security: LAN Manager authentication level - Send NTLMv2 response only/refuse NTLM & LM

2. Network security: do not store LAN manager hash value on next pwd change - Enabled
3. Network access: do not allow anonymous enumeration of SAM accounts and shares - Enabled
4. Network access: do not allow anonymous enumeration of SAM accounts - Enabled
5. Network access: allow anonymous SID/name translation - Disabled
6. Accounts: rename admin account - rename to something unique but memorable
7. Interactive logon: message text for users attempting to log on - sometimes an inject

ii. Audit
1. Audit process tracking - Successes
2. Audit account management - Successes, Failures
3. Audit logon events - Successes, Failures
4. Audit account logon events - Successes, Failures

iii. User rights assignment
1. Debug programs - Remove all groups/users
2. Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.

iv. Local GPO
1. Export a config from a VM or other default install for reference:
    a. secedit /export/cfg checkme.inf
2. Edit to have more secure settings then import onto your target system:
    a. secedit /configure /db secedit.sdb /cfg securecheckme.inf

6. Web Admin
    a. Mod_Security
        i. Get Linux admin to install it quickly; Windows slower
        ii. http://blog.spiderlabs.com/2013/04/web-application-defenders-cookbook-ccdc-blue-team-cheatsheet.html
        iii. Find pwds, reset them
        iv. Look for admin interfaces and restrict them to localhost or an “admin” box
        v. Figure out the use of web apps provided and how they play into the “company” you are pretending to be
        vi. Watch logs - ship them to syslog or splunk so you can watch them all at once.
    b. Client Services
        i. Turn on text only email reading if email is in play
        ii. Microsoft Security Essentials free for SMB and home users
        iii. Firewalls
        iv. Windows: install PeerBlock (IP blocking, supports large IP lists, supports egress)
        v. Linux: remove all remote access options (clients don’t even need SSHd)

7. Incident Responder
    a. Windows:
        i. Autoruns/Sysinternals
        ii. List logged in users (qwinsta)
        iii. If notepad.exe is running, you're been BREACH'd
    b. Linux/BSD/Nix
        i. .bash_history
        ii. ~/.ssh/authorized_keys
        iii. lsof -nPi / netstat -ano
        iv. Know where logs are
        v. diff process list
        vi. fuser -k pts/2
    c. Get incident response forms and fill them out ($$POINTS$$)
8. Network
    a. NetworkMiner = catch new IPs connecting to/from your system
    b. Nmap has NSE scripts to check for vulnerabilities
    c. Nikto = catch easy web app stuff
9. Red Team Tools
    a. Poison Ivy (run/know how to remove)
    b. Metasploit's attacks psexec MS08_067 (patch for XP/2003), MS09_050 (patch for Vista/7/2008 -- see changes to the system
    c. Metasploit's persistence script -- know how to remove
    d. AUTORUNS = BFF