Blue Team Defender: Survival Guide

Before Start of Play:

Who will be the team organizer? The team organizer documents the networks, system names, OS versions, IP addresses, open ports, passwords/passphrases, and updates configuration changes for everyone to see (such as on a whiteboard); helps to prioritize tasks; ensures that no systems are forgotten; reminds players to periodically check for compromise; monitors the functioning of the fictional production application(s) and otherwise maintains the "big picture" and a calm head while others are absorbed in the details and chaos of gameplay.

Exactly which port numbers must be available on which systems for the scorebot? Can't block these.

How will the scorebot confirm that your other target applications are still running? Don't block the scorebot.

Which target systems are running the most vulnerable operating systems and/or services (such as IIS, RPC, SMB, and/or older unpatched software versions with known exploits)? Important to prioritize.

What special tools will be available? Process Explorer? WireShark? PowerShell? Tripwire? Best to ask.

Does everyone on the team know how to view listening ports and established sessions? Does everyone know how to reset a password from the command line? Does everyone know how to kill a process? Does everyone know how to configure IPSec and/or the Windows Firewall and/or iptables for packet filtering?

Who are you permitted to ask for help if necessary? What can or can't they do for you?

When Play Begins:

Block all non-scorebot-required ports on all systems using IPSec/Windows Firewall/iptables.

Assign a different 15+ character long passphrase to every administrative account on every system.

Change all default application and service passwords to a different 15+ character passphrase.

Remove all accounts from all administrative groups on each system except for one.

Delete or disable all user accounts, including Guest, except for the one administrative account on each system.

Establish a baseline by saving lists of your current processes, listening ports, services, device drivers, user accounts, and all files ("`dir /s /b`" or "`ls -lARt`") to text files on each machine. If possible, generate a checksum database using a tool like Tripwire (or just `md5sum`). Use this information to detect compromise.

Enable useful audit policies, clear all logs, and keep Event Viewer open (Windows) or "`tail -f`" critical log files (Linux). When you look at a log, if you notice that the only new events are of no security consequence, clear that log to reduce clutter during the games (it's not real life).

Continuously watch your list of established sessions, running processes, target applications and logs to try to detect malicious changes. Write scripts or use command history (up-arrow or F7) to help automate this work. Detect changes and respond: kill offensive processes, delete new user accounts, delete new binaries, etc.

Finally, focus on your plan and *don't panic!*