Black Team

- HI
- I’m James
- Build Team:
  - Me
  - Davie
  - Jarrad
  - Joe
  - Brian
  - Jake
  - Emilio

Black Team

- Infrastructure
  - Networking
  - Servering
  - Desktoping

- All builds are fully secured and ‘optimized’ as a courtesy. ;-)

Black Team

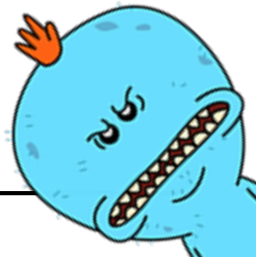
- Services
  - Checks are functional, beyond a port scan.
  - Source IP is randomized per check round.
  - Check time for round is automated.
  - HTTP/S: Checks page content.
  - FTP: Checks for files and checksums.
  - DNS: Looks for specific name/IP combos.

Black Team

- Services
  - Service Level Agreement (SLA)
  - Services down too long? Ain't nobody got time for that…
  - Service penalty assessed for each set of consecutive failed checks (approx. 30 mins.)
  - Yes, you can go negative. Many will.
  - SLA violations will be weighted (much) heavier during the first few hours of competition.

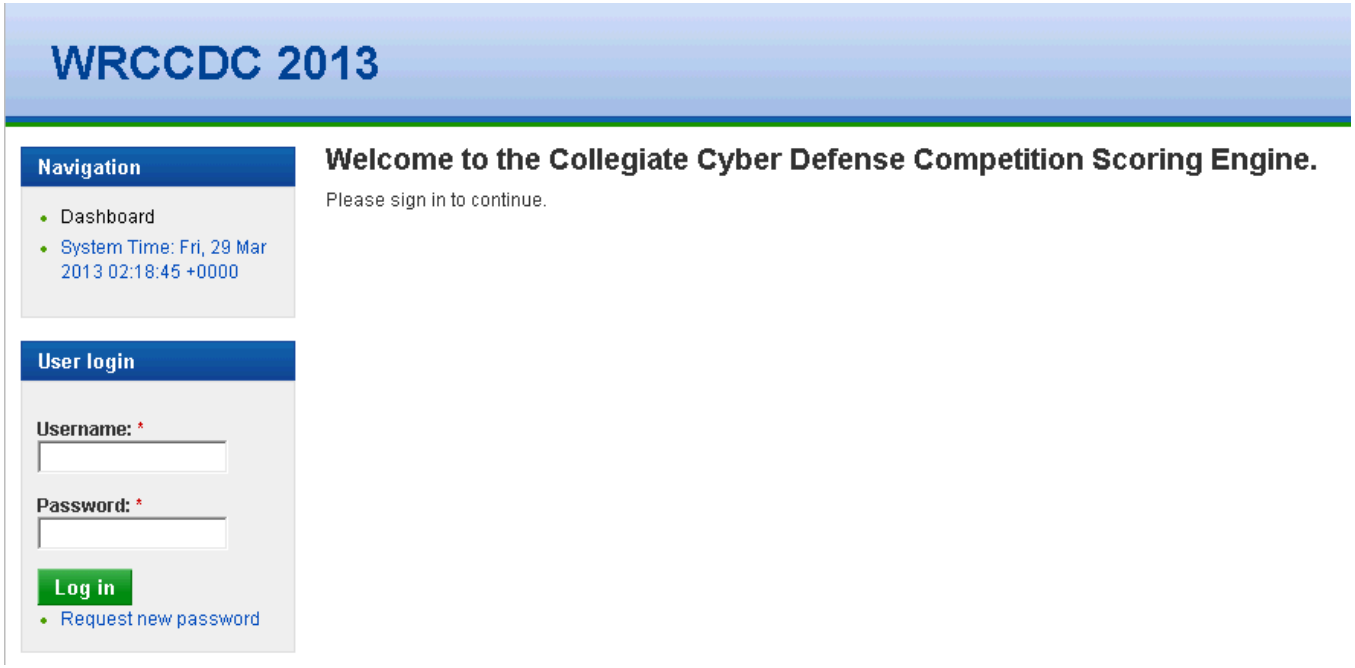
Black Team

- Services
  - You may call x911 and ask why a service is being marked as down. Please consult your access logs for the service before doing so. Check using your bastion instance.
- Consulting
  - You may ask for help from the Black Team for a particular issue.
  - If it requires us to speak to you for more than 30 seconds, a small point penalty will be assessed.
  - We can also come to your pod for a larger point fee.



Black Team

- Inject Scoring Engine
  - https://ise.wrccdc.org



Black Team

- Only use our central recursive DNS servers as your forwarders. External DNS servers will not be reachable.
- Everything will break if your DNS is broken, just like real life.
- If an inject specifies a resource using a specific URL, use the specified URL, or you'll be sad.

Black Team

- If you don't like being laughed at, read the entire inject before asking questions.
- The black team usually has no idea what injects you've been given or when. Call white team unless it is a technical question.
- When in doubt, start with white team.

Black Team

- File Repo
  - We have many ISO's already pre-downloaded.
  - Other files that may be needed for injects or other operations.
  - URI: files.wrccdc.secure
    - HTTP
    - SMB
    - NFS (/export/isos)

Black Team

- Cloning Station
  - You may clone your own machines.
  - Cloning stations available in center of competition area.
  - Machine is PXE booted, and image is selected from menu.
  - Must remain present for entire cloning process.
  - One box/team at a time.

Black Team

- Printing
  - Printing is now centralized.
  - Information provided in pod.
  - No limit, but be reasonable.
  - Save a tree, print to PDF, or email a copy of your important documents to redteam@wrccdc.org for archiving.

Black Team

- Password Change Restrictions
  - Only a single mass-update will be accepted in digital form via the ISE.
  - CSV format. (format details in ISE)
  - Further password changes will require an accompanying incident report form.
  - CSV format. (format details in ISE)
  - Submit CSV's via open inject in ISE.
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)
  - CSV format. (format details in ISE)

Black Team

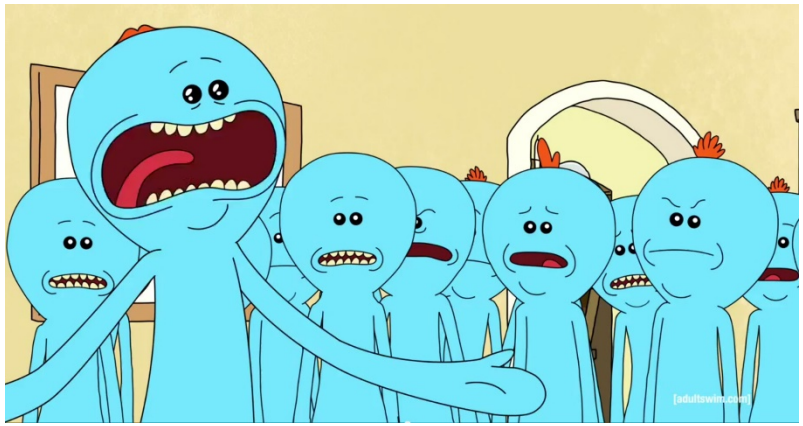
- Password Change Restrictions
  - We do not care about your ISE password.
  - We do not care about your root password.
  - We do not care about your Administrator password.
  - End-user passwords are the only credentials used by the service engine.

Black Team

- Bastion Host
  - External assessment tool.
  - Small Debian-based container.
  - Out of scope for Red Team.
  - May only update packages and connect to own pod. No other access.
  - Information in pod.

Black Team

- Scenario Development
  - Iterative Process
  - Extremely collaborative.
  - Excellent cross-section of talent and expertise.
  - Four distinct phases.



Black Team

- Scenario Development – Phase I
  - Initial design and discovery.
  - Scenario formulation.
  - Determine available hardware and software.
  - Naming scheme and topology.
  - Basic builds.

Black Team

- Scenario Development – Phase I

Black Team

- Scenario Development – Phase II
  - Knowing you can do better.
  - More scenario formulation.
  - Acquire more hardware and sponsors.
  - Somewhat advanced builds.

Black Team

- Scenario Development – Phase II

Black Team

- Scenario Development – Phase III
  - Knowing you can do even better!
  - Acquire more hardware and sponsors.
  - Complex configurations and interleaved dependencies between hosts.

Black Team

- Scenario Development – Phase III

Black Team

- Scenario Development – Phase IV
  - Everything is awesome when you're part of a team…
  - Still needs…something…
  - Personal introspection.
  - Enlightenment…

Black Team

- Scenario Development – Phase IV

Black Team

- Questions?
  - x911
  - @disturbedmime