Tips from last year's event.

Note: Some info may not apply due to slightly different formats of events

Backup your firewall and DNS first. If they go down so does everything else (as far as points go)

Update Update Update - Boxes have updates disabled and practically have none installed. Everything is old.

Ensure that the required services are running

Ensure that the required applications are running

Change Admin passwords on all devices (discover unknown accounts)

Check for accuracy of the documentation provided (hidden servers, services, and accounts?)

Use what you know - bring your own system with familiar software

Time management! Be aware of the clock as you do what needs doing

Try something new!

Don’t lock yourself out - the firewall (network or host) can be your best friend or worst enemy!

Check local user accounts

Check permissions (Guest acct with admin rights?!?)

Check Shared files (“C:\” is shared to the world?!?)

Get familiar with your systems (user accounts? suspicious software?)

Communicate with your team on findings - get help if you need it!

Know your people’s strengths!

Google is your friend

Know your vulnerabilities - scan your own network

Making a Major system change - get your captain's approval.

Document everything you do and everything you find

Protect what you write down (passwords / vulnerabilities)

Research - Balance your time on researching and assigned tasks

Remember - Red Team always wins. (The networks you defend are very, Very, VERY vulnerable...)

There is not enough time to fix everything, this is an exercise in triage.

Bring Stuff - Notepad/Laptop/Snack/Caffeine Drinks/Open Mind

Take breaks. Rotate out for bio needs and mental down time.

Relax - have fun and learn!