**Notes from a team member I played with last year that has participated in multiple events.**

We'll all be given a VPN profile, which connects us into our client network.

your captain will be given creds for all our machines. (Spoiler...they will be weak as shit...think Admin/password)

WE will have to discover what machines are on what IP, if i remember rightly we're told they are on a /24 network (e.g 10.101.10.0/24)

We also get access to Proxmox environments for our machines. These are basically the virtualization systems running our VM's.

On here we can gain access to the console of our machines (the screen if it was a physical box)

The single Red Team have already been in our network (and all blue team networks) for a while now, planting backdoors, users, rev shells etc.

If the game plays anything like @ BSidesLV we'll be given 1 hour to try and get into as many machines as we can, change creds, patch em, clear out backdoors etc.

After an hour, the Red Team will start "playing around" with everyone, shutting down services, dropping beacons (see later on) etc

There is a main scoreboard which shows the server and a couple of ports which it's monitoring. If everything is green, we're good. If anything is red, mbad.

If a service stops, or a web server isn't what the scoreboard is expecting to see, then it goes red. For example, if theres a Drupal server running, and we just switch the web port for this to a blank Apache service....the scoreboard will mark it as offline, as it's not what it's expecting to see.

The scoreboard is expecting to see a running Drupal instance, so...we need to patch the Drupal instance and keep it online.

If we shutdown a server or service to fix it, thats fine, but we don't wanna do it for too long, as the scoreboard will mark if offline, and we'll start loosing points.

We all have the same vulnerable VM's, but IP's are different (So not just a different subnet e.g 10.101.20.0 and 10.102.20.0, but the last number too)

So...if we find a vulnerable service on one of our machines, the other Blue Teams have got the same...so...try and pop it.

Beacons. A "beacon" is a unique string you create on the scoreboard, thats linked to your user and our team. If you manage to send that string, from an opposing teams server to the scoreboard, it gets registered on the scoreboard with a skull or something.

While you have a beacon on your server, you're loosing more points. Beacons may expire so run it again to get it back on the scoreboard.

A beacon is basically "Hey i'm from Blue Team 1, and i'm on Blue Team 4's server...woohoo!"

An example of sending a beacon is - echo "uniquestring" | nc scoreboardIP 5010

Red Team will also be sending beacons from ALL Blue team servers.

For details on how to create a beacon etc see - <https://github.com/dichotomy/scorebot/tree/version3.0/CLI_BEACON_SERVER>

If we have a beacon on our server...we need to find it. We don't know what server it's on, so...using the main firewall will be handy in seeing outgoing connections.

Once you find the beacon, kill it, try and see how it was run, and if someone is still on our server, kick em off, and try and figure out how they got in and stop it for future.

When we're fixing servers it's really important for us to detail what we did.

DNS is REALLY important in this game. The scoreboard uses DNS to monitor all the servers. If the scoreboard can't resolve a server, it's marked as down.

The DNS server i think is running a vulnerable version of BIND9.

Thats about as much as i can think of for now, if i'm wrong on anything someone please correct me, and i'll try and update this. (edited)