Victoria – please pass to the NASA participants

NCX LIVE FIRE – clarification from Parsons to questions received (wanted to share with all competing and non-competing teams; please pass along as needed)

* What is the IP address of the Mail server? 192.168.*.9

* What kind of operating systems are the services? Mostly Linux, with two of them being Windows.

* Are there any mystery boxes on the defendable network? There will be a couple systems tangentially related to the 5 key services that you'll quickly learn about as the event kicks off.

* Can we influence network traffic? I would say yes, for any of the traffic destined for any server deemed in the attackable subnet ranges.

* Are exploitable boxes going to be more mismanagement/misconfiguration or more like cyberstakes live with custom programs on there? More mismanagement/misconfiguration.

* Can we attack our other teams from the Naval Academy? If that's the case then how we do prevent teams from using their other teams as scapegoats to farm flags for them. A team could have their A-team getting points from their B-teams. The B-teams could block traffic from everybody except the A-team which would allow only the A-team to gain points. You can attack them, but teams are grouped by school so you won't be able to score attack points (or lose defend points) off other teams aligned to the same school as you.

* Can we get more clarification on how the availability is scored? As in where is it being check from? Is it like Cyberstakes and old CDX where each service is checking other services? Or is it coming from random IPs from some other subnet? The availability checks are coming from random IPs from other subnets, with the goal that you can't just block all traffic but the IPs checking the availability, since you never know where the availability checks are coming from.

As an example: For the web service availability check, the Intel Server has a service that delivers a file to that specific binary's web service and checks to make sure the previously delivered intel was available before it made the delivery. So it uses the normal capabilities of that service, ensuring that the intel delivered remains on the server and is thus available for others to steal.

Thanks,

- shirley