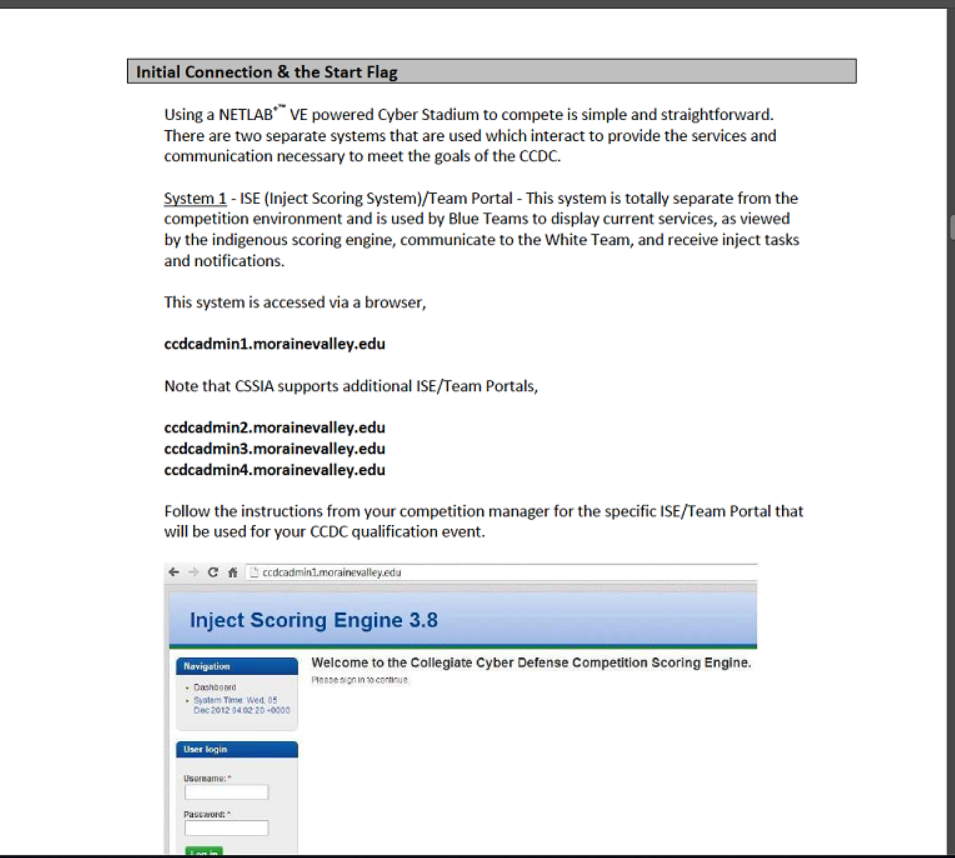


2 concurrent events running – Minnesota and Indiana



**Minnesota**

ccdcadmin1.morainevalley.edu

You will receive a team assignment and that is the team you will use to log into the scoring engine

team1, team2, team3…

The first think you want to do is log into the ISE. When you get into the Inject Scoring Engine you will receive information about the <http://ccdc.cit.morainevalley.edu/>

v1u1, v1u2,v1u3, v2u8 – with password – provided as an inject.

After you reply to the initial Inject to let them know you have been able to access the ISE and are ready to access the topology – then they will send the drop flag with the password information to get into the topology.

They recommend one person log into the ISE to monitor but any team members can log into the ISE. The ISE will give a short time running average of the last few polling status.

Look for a password change policy for service bearing accounts. Other accounts not used for scoring you do not need to do a change.

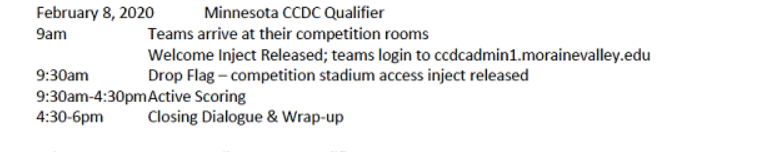
Change root, admin, sysadmin - no need to change passwords on systems that are not scored.

Look for an inject that will have input for tech support. If your service is down you have to manage that, if your lab topology is frozen or freezing then you can call Dave Durkee.

Content initial access credentials – status will give you a status of the VM. The read team does not have direct access to your VMs through Netlab. They have to come through the team network.

Option to undock each machine to put them into a separate window. Not recommended to have too many VM windows on your system – if every team member has multiple monitors open it will tax the system.

Minnesota will be going until 4:00 PM.



No IoT devices – Windows 10 is outside the firewall so you are able to monitor your systems from an external viewpoint.

Service accounts they need to send passwords into .

You need to discover which accounts are tied to which service.

Incident Response – 1 open inject where you can put in incident response. Can recover points from a successful attack from a Red Team. Very often in the end game there is a lot of false positives. A lot of history of incident response that are fake. Ghost of the red team.

If you detect recon worthy of an incident – existing malware is ripe for an incident response. See from the template have to prepared to give some detail.

What was the incident – detail and remediation or corrective action did you do in response to the attack.

No accounts that they cannot change passwords to. May test and login. Nothing tied or attached to the scoring engine.

SLA feature in the scoring engine but they do not do that – they would penalize a team if the service is down for too long – do not penalize for that only at regionals.

There are going to be services down – no way to hold back the Red Team because of the configuration that is in the network. If services are down don’t think you are out of the event. Don’t know what the other teams are going through.

All teams should stay in the game believing they are there to learn and be as much as they can. Stay with the game and stay with it.

Minnesota teams should be physically onsite – 9:00 arrive in the competition room. Registration table ready at 8:00 AM – 8:30 rules and regulations – 9:00 people to the room.

Whether they issue the drop flag is up to the MN management.