CCDC Notes:

Good:

1. You showed UP!!
2. Great Learning Opportunity!
3. See how the students and colleges take the competition seriously!
4. There are many jobs important to be a part of the Team!
5. National Cyber League - $35.00 Great training Ground for the CCDC.
   1. <https://www.nationalcyberleague.org/>
6. Password changes – keep them out. Good for this
   1. Check service account Passwords
   2. Good for mysql password change
7. Make sure turn off remote Root access –
   1. sshd.conf file – needs updating to no root remote access.
8. Updates – Upgrades – this was good.
9. Firewall Rules – host based IPS – need to find an open source solution.
   1. Not sure of Host Based firewall rules
10. Monitoring to know what IP’s were being used by the Red Team
    1. This was good.
    2. Inserting Firewall rules – was good.
11. Manage Active Directory Users –
12. Good Team Effort

Some improvement thoughts:

1. NTP, Ossec, Malware Bytes, virus scans.
2. Learn the Applications – how to get them working
   1. Ecommerce – for the ecom application
   2. Dovecot and squarecube for the email
   3. Mysql database
   4. Phantom/Splunk –
      1. Splunk – forwarders for the Windows and Linux
      2. Phantom – Public and Private IP – how they get in?
   5. Bind9
   6. Debian 7.8
   7. CentOS 6.0
   8. Ubuntu 8.?
   9. Phantom running on CentOS6 Phantom 7.4
   10. Splunk – not sure what it was running on?
   11. Windows 2008
       1. Attack was to disable Domain Admin account
          1. Could only login in safe mode so locked out of AD.
   12. Windows 8.1
   13. Windows 10 – password change, anti-virus, Wireshark to monitor network, zenmap to do port scanning.
   14. NTP configuration for all systems – what system is the master clock? Splunk?
3. There are ways to protect and keep the RED Team out. St. Cloud State was able to keep the red team out of majority of systems. Passwords, firewall, anti-virus, ossec agent and server.
4. No Root remote access. – Setting the immunity attri?
5. File Permissions – confirm file access
6. QAKBOT virus – hit the Server 2008 in Alternate Pod
7. Alternates were given good instructions on how to approach injects.

Team Strategies:

1. First few injects are critical to scoring points.
   1. Have someone focused on injects and doubling up on systems to manage the injects. Double up gui with command line systems.
2. What did you do to protect the system?
3. Is your system quiet or is it a hook to other systems. They won’t attack a tool –
   1. How do you know they are not in the system?
4. If your system is quiet – does another team member need help? How about injects – can you help with injects? With 8 team members – there are systems to protect and injects to respond to.
5. Firewall – monitor the inside – outside usually has millions of hits
   1. If there is much ping traffic they may be disguising or redirecting your attention?
   2. They were doing ping sweeps every few seconds to check that services were up and running.
6. Watch out for social engineering – why would they call you and why would they ask you to install a system – it is the Red Team. We are not always performing technical support? Reply to Injects – you have to write a professional Memo: Not just screenshots but actually writing a paragraph to explain.
7. Know the judge – name information – remember names. Take notes during introductions.
8. They are always going to do something new to trick students.
9. DNS – set forwarders in the DNS Servers – Set alternate DNS.
   1. Still need Active Directory SOA
   2. Need AD DNS to Talk to Bind9 – setup forwarding
   3. Need Bind to set-up a forwarding to Outside Public DNS.

There was a DNS forwarder inject to set forwarder to 9.9.9.9

Inject related to Group Policy – add users GPO for 5 managers, 5 users.

Outdated version of Java on Windows 8.1 – delete don’t update. Delete all unnecessary software. A lot of them deleted Java and others thought that is how they got in.

Malware bytes – immediately found malware. Downloaded a file and Malware bytes.

During the intro they mentioned someone might want to enter the room which lead the team to believe social engineering would come from the door and not the phone.

Should hang up or don’t take the call. Answer the call but flagged?

Red team was in Minneapolis – know locate of Red Team.

IT we don’t answer the call – IP phone possible vulnerability with scanning?

Incident Report to get partial points back.

Instructions should always be in a documentable method that can be verified.