# CCDC Week 5 Homework

Server2019
NEBULA\Administrator:swift

Sevrer2016
Administrator:Password1!

## Questions (30 Points)

1. (10 pts) Write a Powershell command to find AD users created within the last 24 hours. You may use an LDAP query or just derivatives of the information readily available from Get-ADUser.
2. (15 pts) Why would someone want to disable NTLM within their AD environment? Are there any specific negative side effects to doing so?

## Lab (70 Points)

1. (10 pts) Configure the firewall such that there is inbound access to the FTP server running on Server2016. Block all other inbound access.
2. (20 pts) An internal audit revealed that there may be signs of startup persistence on the Server2016 machine in the registry. Can you investigate some common registry keys for signs of persistence and report back on your findings and how you validated what you found to be malicious/harmless?
3. (20 pts) Create a domain group policy that only applies to the Server2016 VM and sets STIG-compliant password policies (Hint: you may need to create an OU)
4. (25 pts) Management has decided that it is time to start an internal wiki for the company. The end goal is to load it with information about their competitors, Galactic Aerospace Yachts. We've installed the XAMPP framework on the machine now all we ask is that you install and configure MediaWiki so that we can begin to provision accounts for employees and use the site.