**CMSC 491/791 Active Cyber Defense HW 4**

**Name:**

**Due: October 2, 2019 at 7:00pm**

Setup:

Download a Windows Server 2008 .iso file from the following website:

<https://www.microsoft.com/en-us/download/details.aspx?id=5023>

Once you have done this, install Windows Server 2008 in VirtualBox.

Install Active Directory Domain Services on the server, including the other supplemental services required (DNS, etc).

Download Mimikatz from:

<https://github.com/gentilkiwi/mimikatz/releases>

Questions:

1. Create a group policy object which will enforce the following policies: (16 pts)
	1. Enforce a minimum password length of 8 characters
	2. Prohibit access to the control panel
	3. Prevent windows from storing LanMAN (LM) hashes
	4. Disable SMBv1

Export the group policy object as a file and attach it to your homework submission.

1. For each of the four policy requirements from the previous question, explain in a sentence or two why that policy helps increase security. (16 pts)
2. In your own words, explain the difference between a forest and a domain. (8 pts)
3. What is the process name for PID 4? Describe what this process does. What happens if you kill PID 4? (10 pts)
4. Which registry key stores a list of every website you’ve typed in internet explorer? How did you find this information? (10 pts)
5. Run the mimikatz tool on your server as Administrator. Include a screenshot of the results. Answer the following questions: (15 pts)
	1. What impact could a tool like this have on the security of an entire enterprise network?
	2. What was introduced in Windows versions starting with 8.1 to make these types of attacks more difficult?
	3. What is the underlying process type which makes this protection work?
6. What is the difference between a golden ticket and a silver ticket in the context of active directory? (10 pts)
7. Install a golden ticket into your VM’s Active Directory using mimikatz or your choice of tools. Provide a screenshot and describe what you did to install the golden ticket. (15 pts)