An important new attack discovered in the past year or so has been the Mimikatz attack.

- Describe the attack: What is it? How does it work?
- Provide a demonstration of how it can be exploited. Be sure to include screenshots or other evidence of success.
- Describe the traces left by the attack in the system logs.
- Describe how the attack might be detected by an intrusion detection system.
- Can this problem be mitigated with a patch? If so, which one(s)?
- Can this problem be mitigated by changing system settings? If so, which one(s)?

You may find this tool helpful in the final exercise.

Remember- all sources must be cited, and direct quotes must be indicated with quotation marks. I will check.