One of the first things that I discovered on my machine was the windows firewall. Initially the windows firewall was disabled. In order to fix it I had to reenable the firewall. Upon doing so I also discovered an any-any firewall rule that allows all traffic through the firewall. This would make it so that the machine can be accessed completely from the network even with the firewall enabled. This rule had to be deleted and replaced with individual rules to protects the ports on the machine.

Another issue on the machine was the creation of backdoor accounts. Users with access to the domain were created such that they could be used to exploit the system. They would have their own login credentials so they were easy to track down when all the users were listed.

Several backdoors on the system were placed to collect passwords and give persistence access. One backdoor took over the process of password complexity. As passwords were being created the software would capture the password where windows would normally send the password to the process checking that the password conforms to the complexity requirements.

A remote shell was also created in the web directory of the server. That would give an administrative command shell over the network. This was almost immediately blocked when the firewall was reconfigured in the beginning.

A key logger was also installed on the system capturing everything that was typed into the system. This allowed any passwords that were typed to be captured and collected later.

Sysinternals autoruns was helpful in finding the dll backdoor that captured passwords based on password complexity.