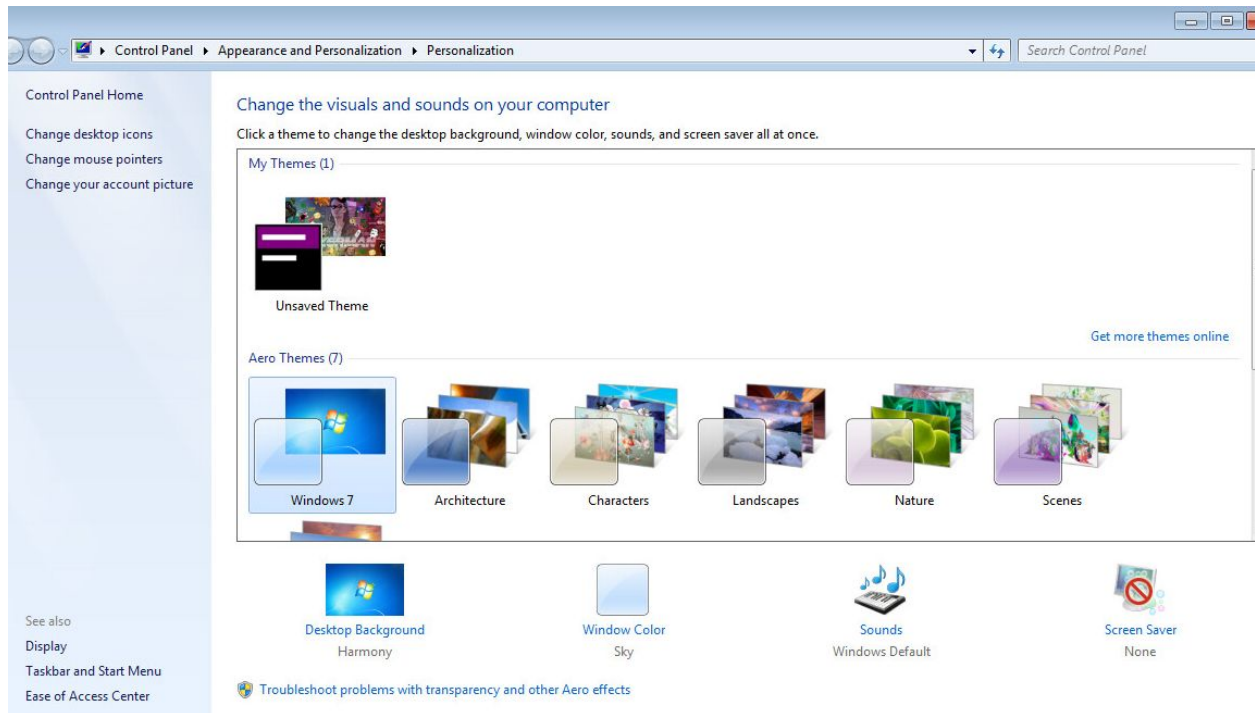


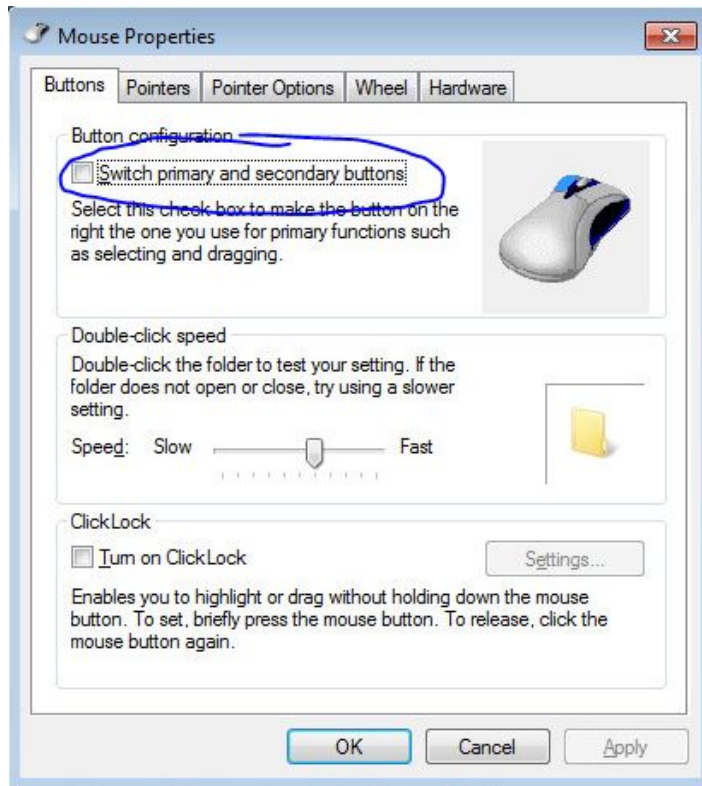
NTS103 Malware Removal Lab Assignment

Mohanad Horani

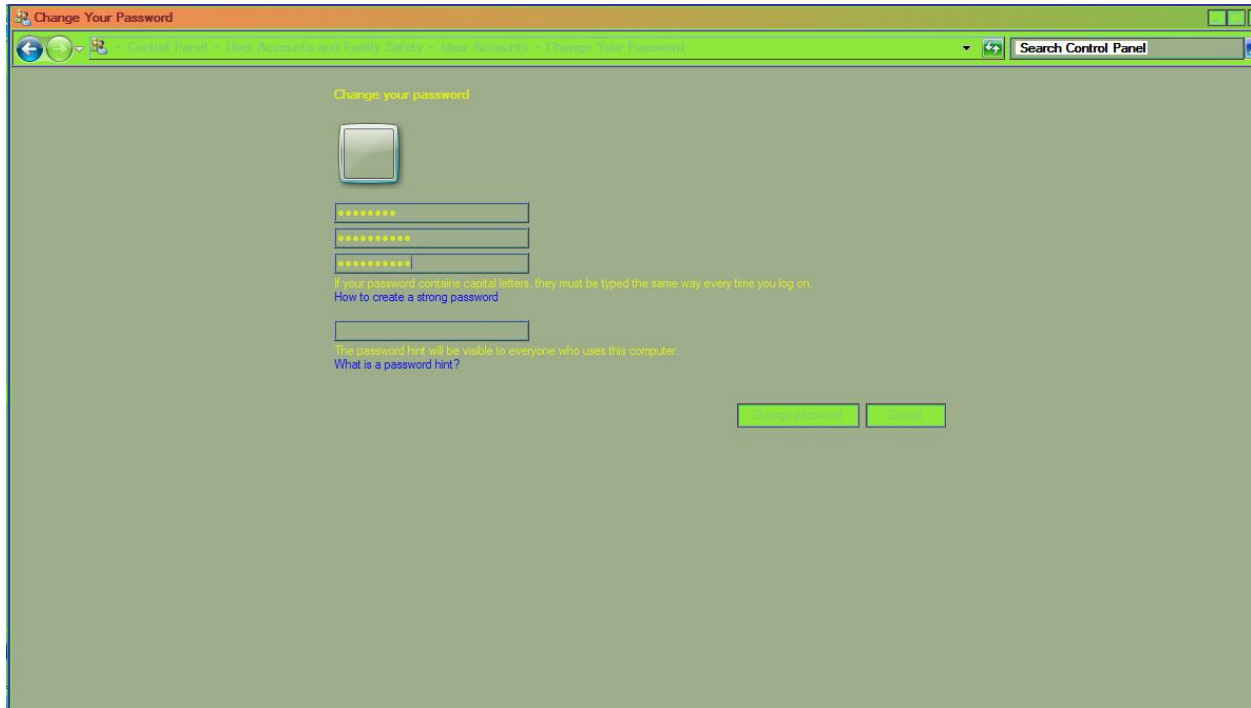
University of Advancing Technology



To begin with, I changed the theme, which, ideally, would only take a few seconds, in order to view everything properly. The theme that the malware had by default made it extremely hard to read the screen, so this makes optimizing the VM much easier.



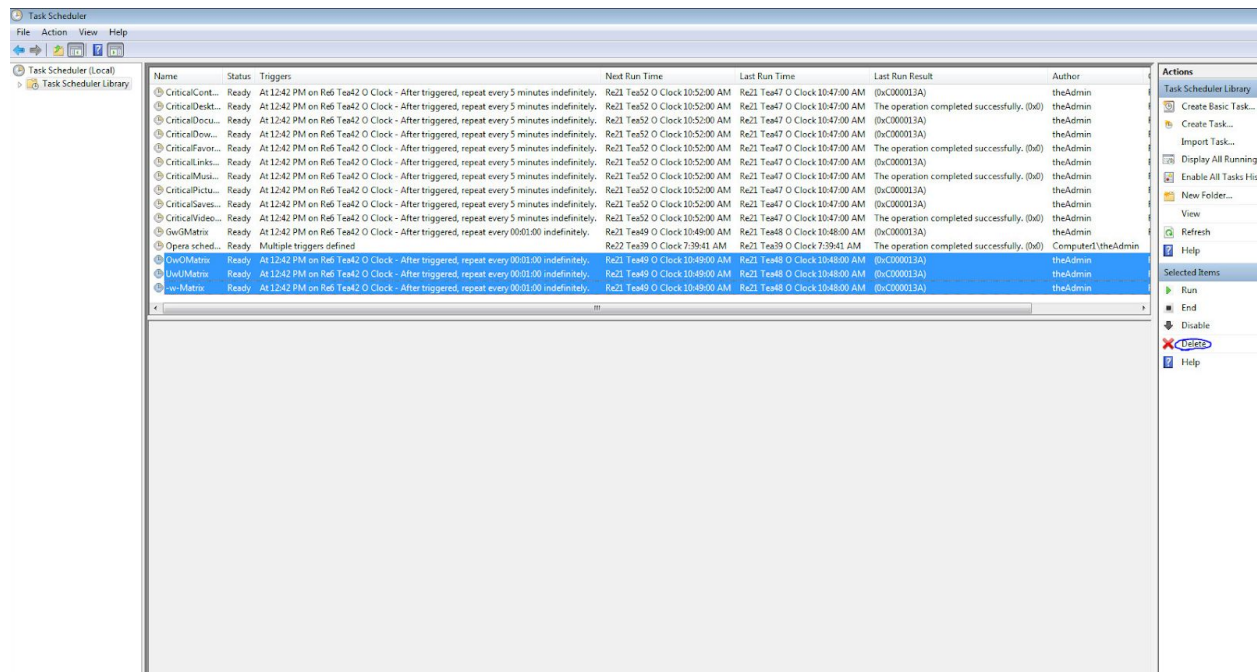
Next, I quickly opened up the mouse properties and set the mouse options to normal. By default, the malware switched the left and right mouse buttons, so being able to use the mouse normally allows more comfort, ensuring efficiency while attempting to stop the malware from spreading.



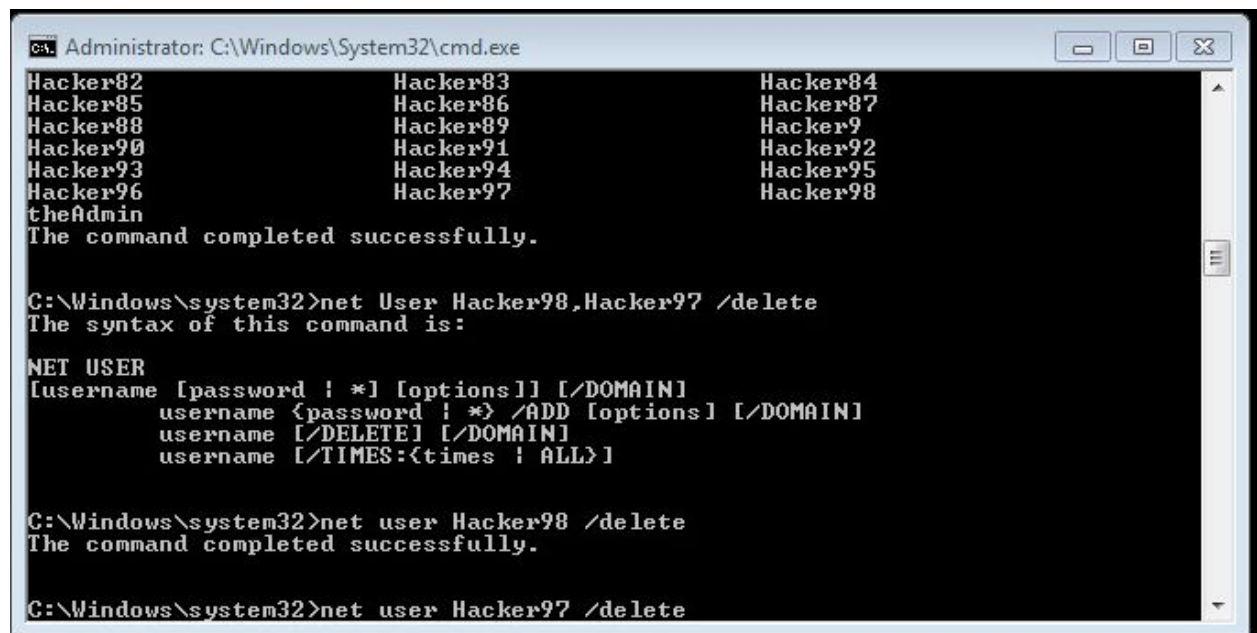
Next, I changed the default password, “P@ssw0rd” to a custom password, so that the “hacker” can’t get access via the main administrator account. This helps to prevent another way for the hacker to get into the system.

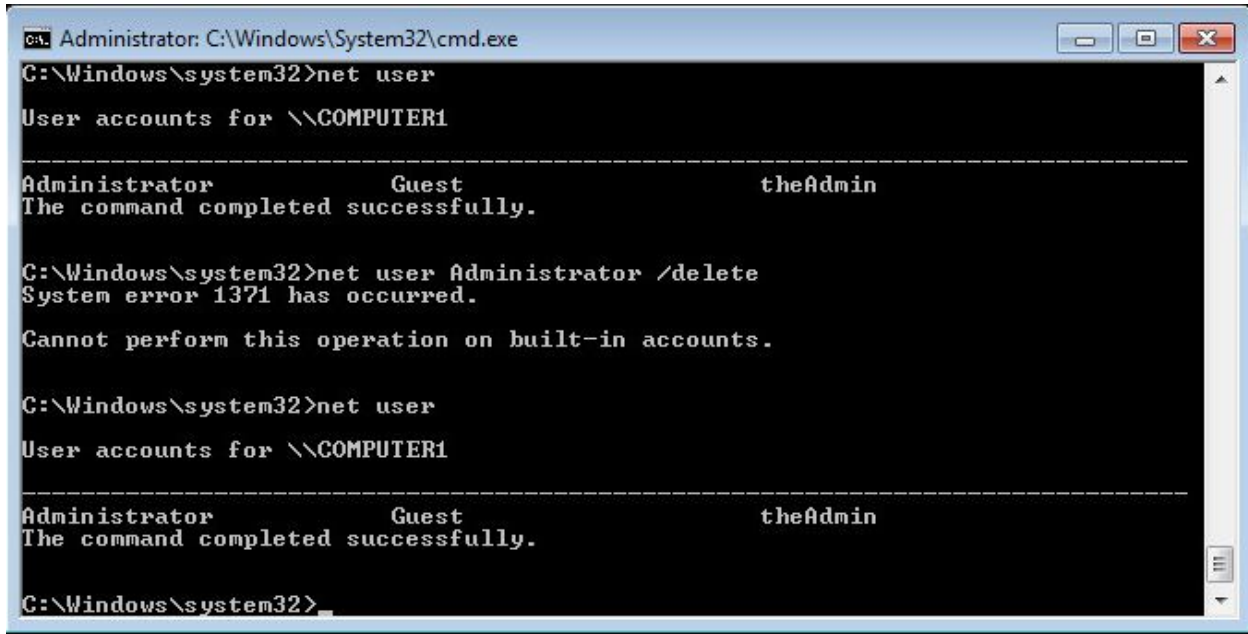


In the meanwhile of accomplishing all of this, I have been deleting all of the command prompts that have been appearing as annoyances every minute, before I have been able to stop the scheduled tasks, in order to prevent lag, in the meanwhile, for more efficiency.



At a certain point, I finally deleted all of the scheduled tasks in the task scheduler. This stops the scheduled annoying four command prompts every minute as well as stops the updating hacker user accounts and the hacker files showing up in several places in the system every five minutes.





```
c:\. Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>net user

User accounts for \COMPUTER1

-----
Administrator          Guest          theAdmin
The command completed successfully.

C:\Windows\system32>net user Administrator /delete
System error 1371 has occurred.

Cannot perform this operation on built-in accounts.

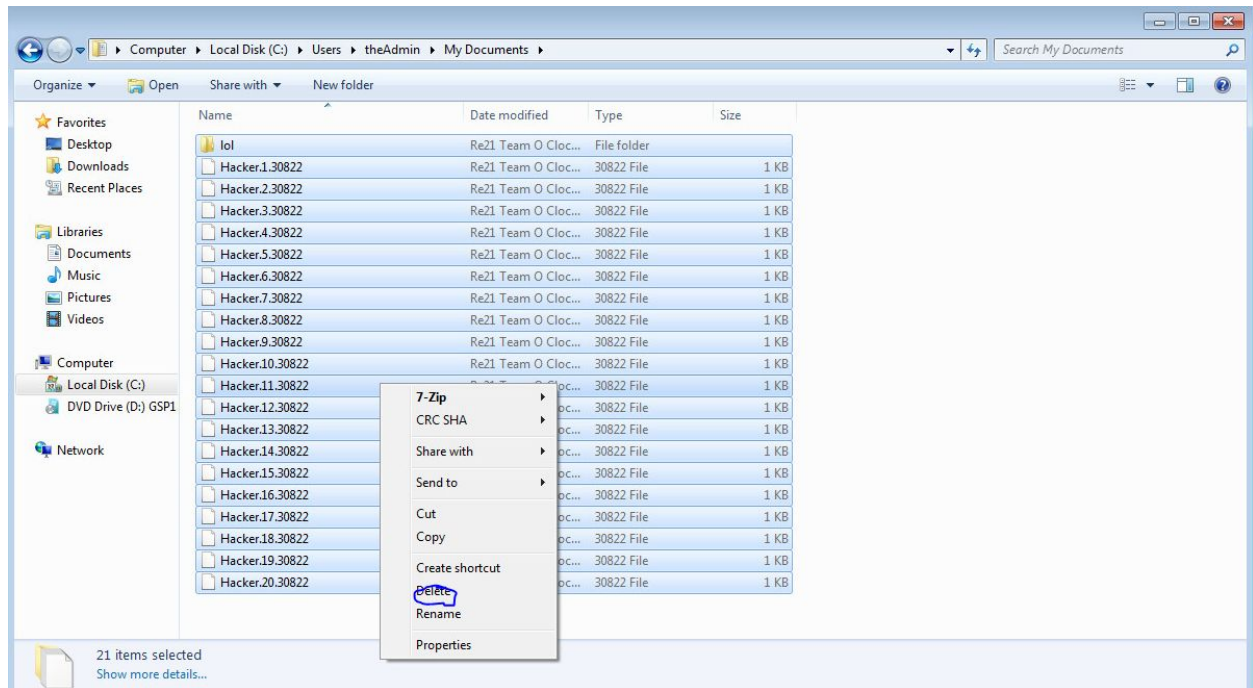
C:\Windows\system32>net user

User accounts for \COMPUTER1

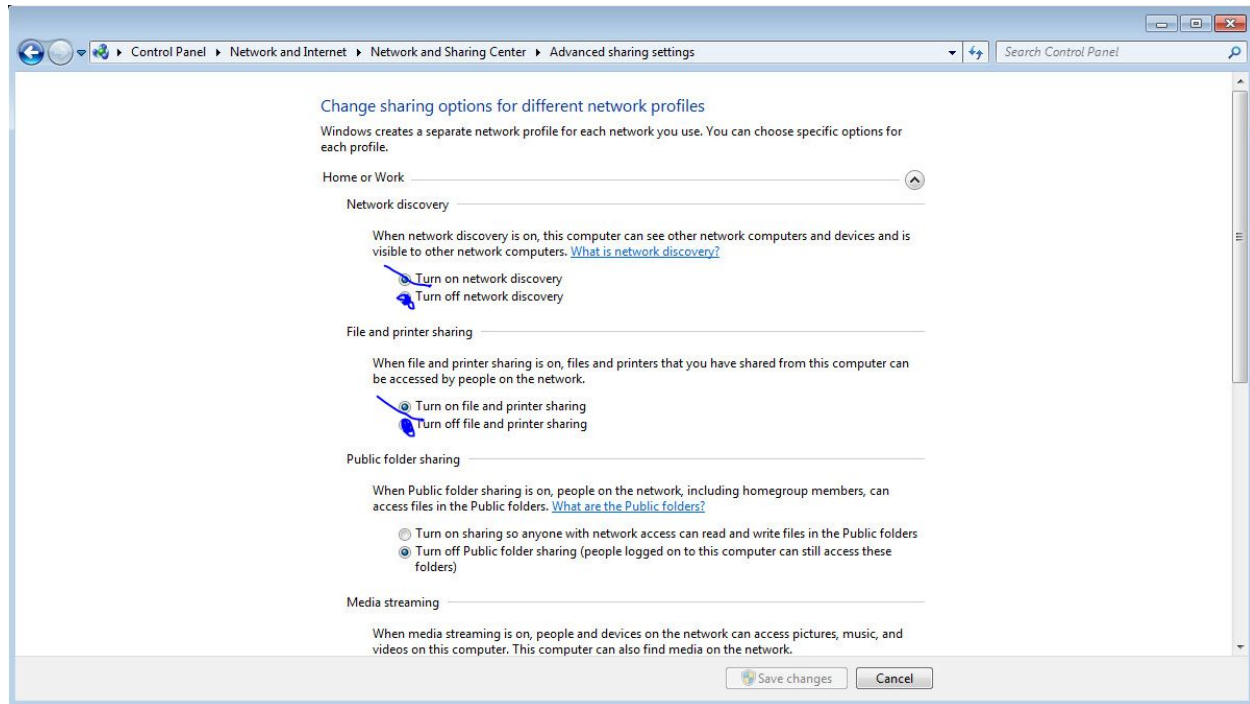
-----
Administrator          Guest          theAdmin
The command completed successfully.

C:\Windows\system32>
```

Next, I deleted all of the hacker accounts, which can be used in order to gain access to the main administrator accounts via the command line, as they are all administrator accounts as well. I deleted them one by one in the command line using the command “net user <ACCOUNT> /delete” for every account. An alternative which could take much less time would be to create a batch file that runs a script to delete all of the accounts, but I thought of this AFTER I deleted all of the accounts, so I did not do that.



Next, now that these Hacker files are no longer being added every five minutes, I deleted all of them from the system, showing a more clean look without as much influence from the “hacker”. This could potentially be a way for the hacker to get into the system, so it is important to finally delete all of the files.

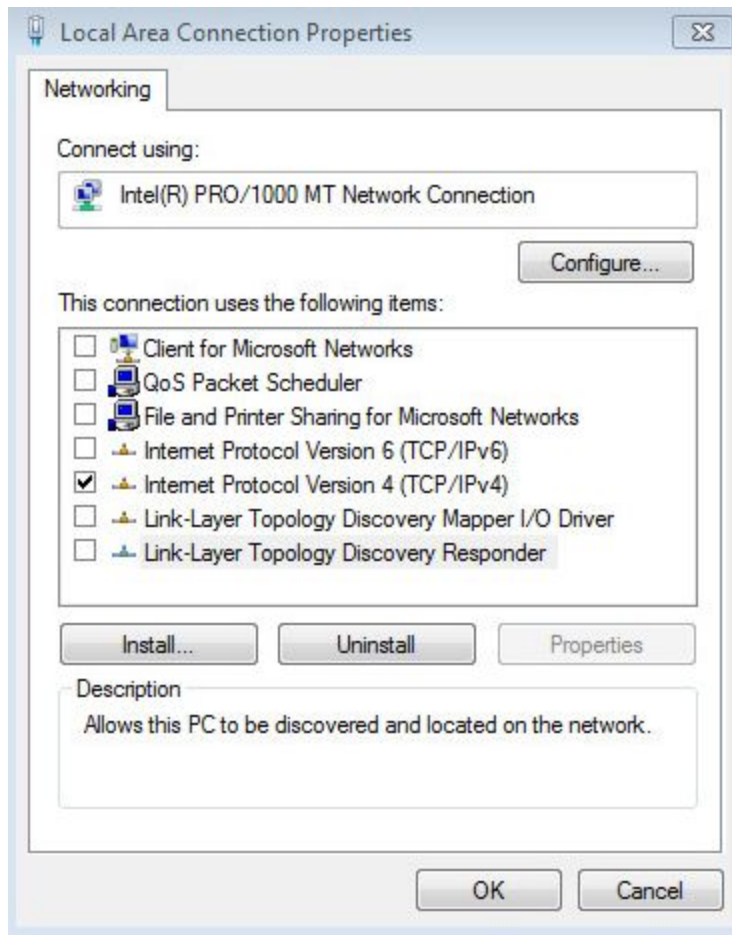


In this screenshot, I turned off network discovery as well as file and printer sharing. The reason for that was to defend against the malware for this lab primarily. This was done simply by going to the control panel and then clicking on network and internet settings as displayed in the screenshot.

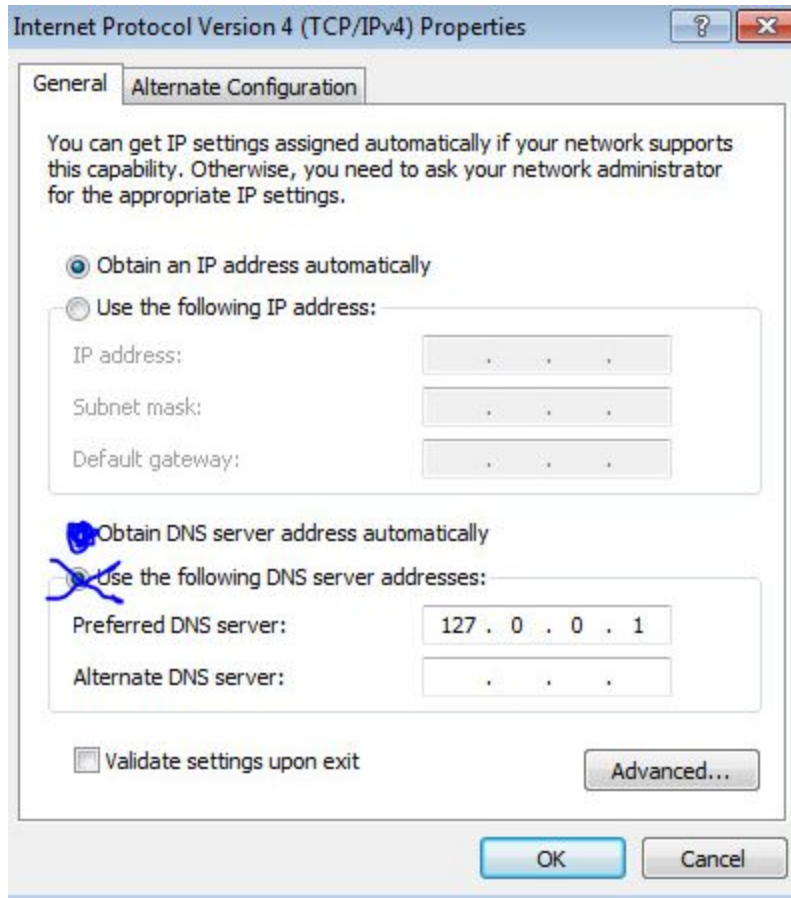




In this screenshot, I deleted all the unnecessary text of the hosts file. The reason for that was primarily in order to connect to the internet on the VM properly.



In this screenshot, I changed the internet settings and turned off the unnecessary settings that were not required. The purpose of doing so was in order to connect to the internet on the Virtual Machine properly.



In this screenshot, I changed the IPv4 settings and enabled the option for the DNS server to be obtained automatically. This also was to cause the Virtual Machine to connect to the internet properly since it was not doing so beforehand. In addition, it was set at the wrong address causing the internet to not work on the VM.