CS 6542 Attack Defense Write-up

Rajat Vij

1. What activities were you responsible for during the exercise?

Ans. We didn't really have set responsibilities as we were all involved in all the activities and setting up the network. I worked in setting up the mail server and securing it using windows Firewall. I was also involved in attacking the other teams network and I was able to get into Group 4's system and close their web and mail services. I also wanted to create a backdoor there, i.e. create a persistent connection in meterpreter but I got in to their system during final minutes of the exercise so I was more interested in bringing down their services at that time and I worked on that only.

[NOTE: I think I was too greedy setting up the mail services as I tried to implement authentication and that led it to not work with any other mail service outside our network as it required authentication, so at the end I had to remove all that to make it work in class]

2. What would you do differently if you did the exercise again?

Ans. I would have tried to identify the attacking networks as kevin already mentioned after the exercise and blocked them or would have allowed only the networks which had services running and your monitoring network which I had identified in the exercise. That way nobody would have been able to attack our network.

3. What was your biggest lessoned learned from the exercise?

Ans. I learned a lot as I only knew the theory behind the exercise but not the practical before the exercise, I knew only part of practical which I tried on the network I requested before the exercise. Biggest lesson would be the general understanding regarding the working of a network and how to attack and defend a network in itself, we also got to know different approaches one can take to defend a network after learning how other teams worked to defend their network.