**Analysis of Team 4’s Virtual Machine**

Without using any tools, I wanted to see if I could social engineer into the system. The username had a distinct identifier as TUF42559\adermn. This sequence is obviously an ID of some kind and looks like it could be a Temple University ID. Googling this, I found a site for an e-portfolio that was blank with no identifying information. A few links down I found that this person had submitted a project for a Temple QVC analytics competition. I could find out this student’s name. I could try to send a phishing type email to the student suggesting a professor told me I needed the password for the assignment but decided against it.

I scanned the host-only network with NMap and found the machine’s IP address matching that MAC address as 192.168.255.131 and named Workstation1. Pinging shows the host as up. I ran a -F which scans the most popular ports show that all those ports are filtered. The OS was also not able to be fingerprinted probably due to how much is blocked from scanning. NMap said there were too many fingerprints match to give specific details even though I know the OS is Windows 7. I also checked to see if it was vulnerable to Heartbleed but the SSL port 443 was blocked.

I tried to start the machine with Kali inserted into the CD drive. It did not boot directly into Kali. I went into the BIOS and moved the CD to first boot. I attempted to use John the Ripper which I could not get to work properly. I attempted ophcrack and got the NT Hash for the password. I did not have the space to download the rainbow tables so I let an internet tool decipher it for me. It turns out that it was the blank password hash. I attempted to sign in without a password but could not. I believe that the OS is too advanced for the ophcrack tool and passwords are better encrypted. Kali did give me some useful information. I could mount the hard drive and search through its files. I found multiple users such as administrator, Anne, Frank, and student. The only user who seemed to have unique files created (since these were created as just test user accounts) was student, who had two files named hotfix.txt and hotfix2.txt.

I also considered Cain & Abel but it seems to require knowing at least the Admin password for the target. I also attempted to sign in as Administrator, a default account in Windows 7, but that account had been disabled probably due to the computer being setup through group policy.

Not able to get into the computer, I decided to run Nessus Scans. Sadly, the scan only turned up information points, showing no vulnerabilities I could attempt to use. Nessus is usually able to classify threats as low, medium, and high on exploitable machines.

In all, I would say that this is a very secured Windows 7 machine. It is rather impenetrable over a network connection even knowing more about the computer than I would in a black box situation. Even though I didn’t send a phishing-style email, I do not believe that would’ve worked anyway. Since I did have physical access to the machine, I could retrieve files from it that I wouldn’t have seen over the network.