ITP 457 Midterm Report

By Erik Martin

\*Group Members: Andrew Prajogi and Matt Davis

Questions:

1. In order to create the router, I used PFSense. This was the software that was recommended by Chi. However, I did not just use it mainly because of Chi’s recommendation. I researched how many resources there were for PFSense. My research concluded that there were plenty of resources available. This software was easy to configure (minus the constant snapshots on virtualbox) and also lock down. This provided me with an easy way to adblock as well as redirect websites to others.

We are in fact not using iptables. Not using ip tables makes it much simpler to figure out.

The only issue that I ran into was the fact that I would constantly have to reconfigure pfsense before I saved the states. Fist I was able to forward all traffic from port 80 using firewall rules. Next, I was able to block ads by using pfblockerng. This downloads data from sites that are updated daily. I then blocked a fake new site – cnn. I used a reject setting in the firewall alias. To reroute traffic from UCLA to USC, I created a NAT rule that included all ips that ucla used. In order to lock down the console, I password protected it so no one could edit it without the password.

1. Overall, I was able to get everything to be up and running. Once I got everything up and running, I would do checks on the system. I did have one issue when I had to reboot my second DC02, the time was off. I googled how to solve it and was back on track within minutes. There was some confusion with setting the local group policy vs global group policy.
2. For Gilly bates: I made admin and domain admin. For Shigeto Minamoto: I made domain admin. For Lady Googo: I made just a user. For Biggs Porkin: I made just a user. For Vincent Vangoo: I made just a user. I felt as if Vincent, even though a CEO, would not need to be an admin. In terms of creating an hourly schedule, I only restricted biggs Porkins and lady Googoo, This was because everyone else had some other sense of importance and might need to actually work outside of the typical 9-5 Monday thru Friday hours.
3. Yes I did. First, I went into local server and then adjusted the settings through there. However, After testing out all of the edits I made I realized that they did not work, only the 9-5 hours that I made. I was confused by this. However, I soon realized that the changes were not working. I then went , I made it so that users would not be able to access the command promt or powershell. Second, I made it so automatic updates would not occur. Third, I updaded the hours of each user. I only made guest, bigs borkins, and lady googo to be 9-5. Everyone else I felt like may need to access their account as they have. I also disabled the admin tool policy to everyone except Gilly and Shigeto. This was because I believed that we needed to excluded who wouldn’t need it. To add the workstation, I first imported the ova. I then went to the advanced system setting to connect to the domain. This connected the workstation to the Sosoft Domain.
4. In order to add each to the drive, I used the following guide: <http://swissperience.ch/techtalk/2016/08/17/ubuntu-16-04-pbis/>. In order to connect the nix machine to the domain, I used powerbroker (PBIS). I put this on the system then ran through a tutorial I found online. See above. While probelsm did occur, I was able to get help from m partners.
5. Bacula: First off, I made a bacula server on an ubuntu machine. However, I was able to get the linux machine up and running. There were many issue with the windows side which made installing it very difficult. In terms of backups, I am doing full backups every first Sunday. I am doing differential backups every Sunday after the first. And I am doing Incremental backups on all other days of week besides Sunday. I also established a zfs raid 5 partition by adding 4 addition hard rives and configuring them. Each is 1.5 gb.
6. Samba: I was able to get samba working with the Debian, from your website. I was able to automount all the windows users to a share folder by the network mapping tool on the file explorer . For the linux machine, you can use autofs to mount all of the users to the networ. If you log into the Debian machine, you can access samba and thus fulfill the web browser requirement.
7. Windows Hardening: In order to harden I went into the sosoft domain and went to default domain policy in the domain controller policy. From there I went into edit and changed system and network settings. I disallowed access to cmd, powershell(both versions), and registry edits. Additionally, in network settings, I made it so the users could not mess with the network, specifically remote connections. I also removed scripting access ability and also removed the ability for users (not admins) to access the control panel. I also disallowed all regedit type programs. I encrypted my linux machines to ensure there was not able ot be access. Lastly, AD users do not have access to sudo and cannot use administrator privileges.

\*I would have made the passwords all relatively easy as I know you would be using them. Otherwise, I would have made them more complex.

Passwords:

Machine Logins:

* Router:
  + Username: admin
  + Password: pfsense
* DC01:
  + Username: Administrator
  + Password: Password!
* DC02:
  + Username: Administrator
  + Password: Password!
* WWS01
  + Username: wws01
  + Password: Password!
* LWS01
  + Username: lws01
  + Password: ITP457Midterm!
* BAC01
  + Username: backula
  + Password: Password!
* FS01
  + Username: root
  + Password: ITP457Midterm!

Employee Passwords:

* Gilly Bates
  + Username: gillybates
  + Password: Pizzabox19
* Shigeto Minemoto
  + Username: shigetominamoto
  + Password: Hondaboy04
* Lady Googoo
  + Username: ladygoogoo
  + Password: Ihatemusic15
* Biggs Porkins
  + Username: biggsporkins
  + Password: Piggyman22
* Vincent Vangoo
  + Username: vincentvangoo
  + Password: Artist4lyfe