**Seth Ayers**

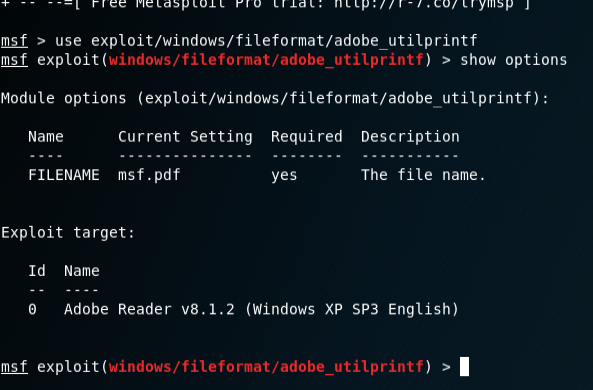
**04/07/2018**

**IT 430**

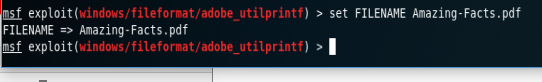
**Lab 07**

**SAyers\_Lab07.docx**

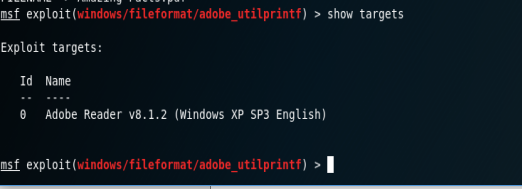
**Part A: Exploiting a Windows machine**



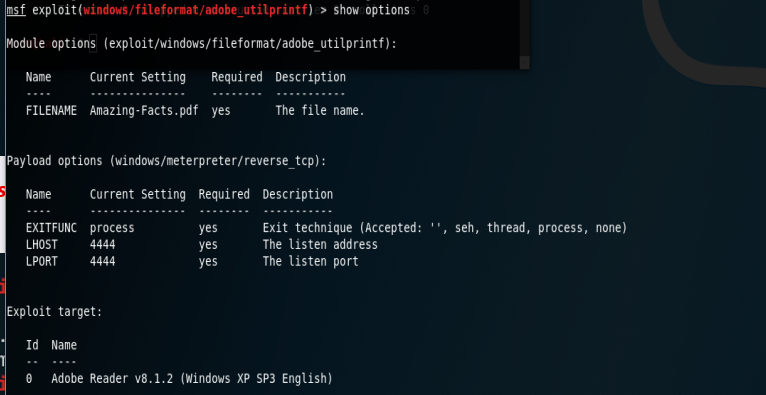
*Enabling the pdf file exploit to create the exploit.*



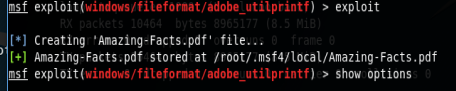
*Renaming the default file to something specific.*



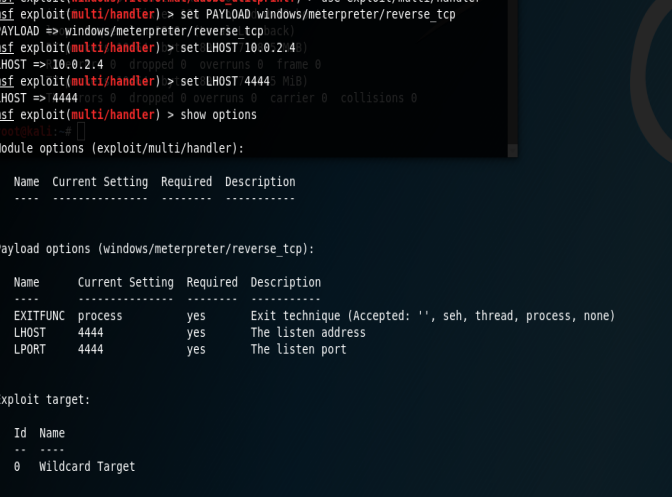
*Ensuring the exploit conditions are met with our target machine.*



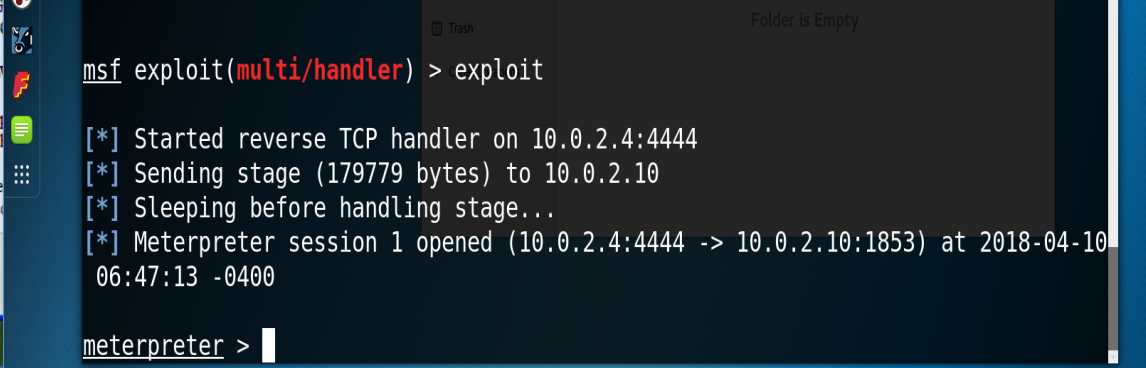
*Setting the PAYLOAD options for our host and listing port. Note that the screenshot is incorrect. I did change the LHOST to my host after noticing the mistake.*



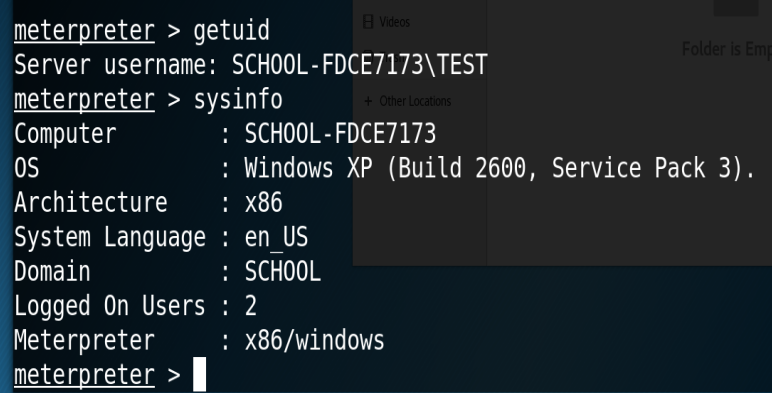
*Creating the actual file to be used to place on the WIN XP target.*



*Using the handler exploit and reverse TCP payload to set up the listening session.*

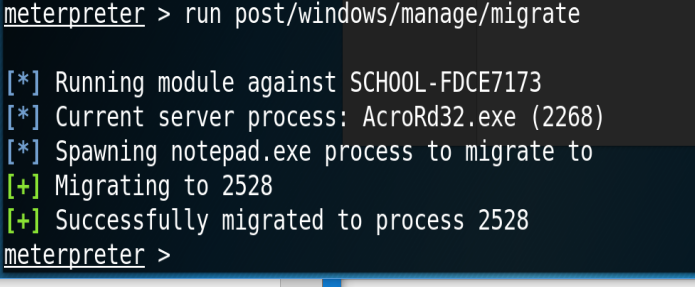


*With the file placed on the target machine and opened, the connection to the target is finalized and shell access is open.*

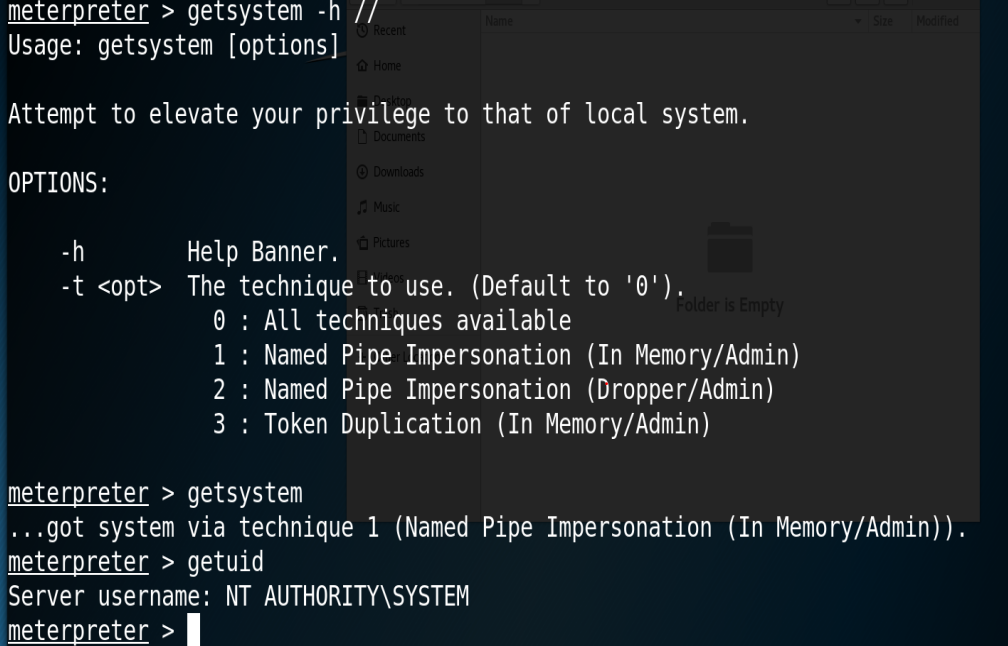


*Confirmation that the attack is successful.*

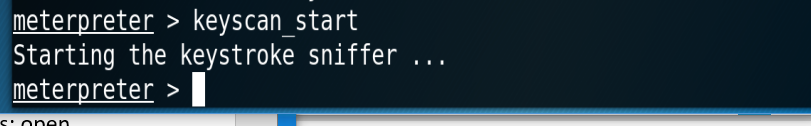
**Part B: Post exploitation and backdoor installation.**



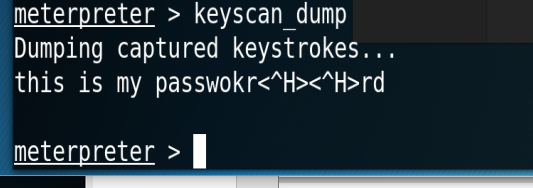
*The attack vector is established and therefor different process can be selected to maintain a connection in case the user closes Adobe Reader. Considering the nature of the attack, this should be done as quickly as possible to ensure a connection before a backdoor is installed.*



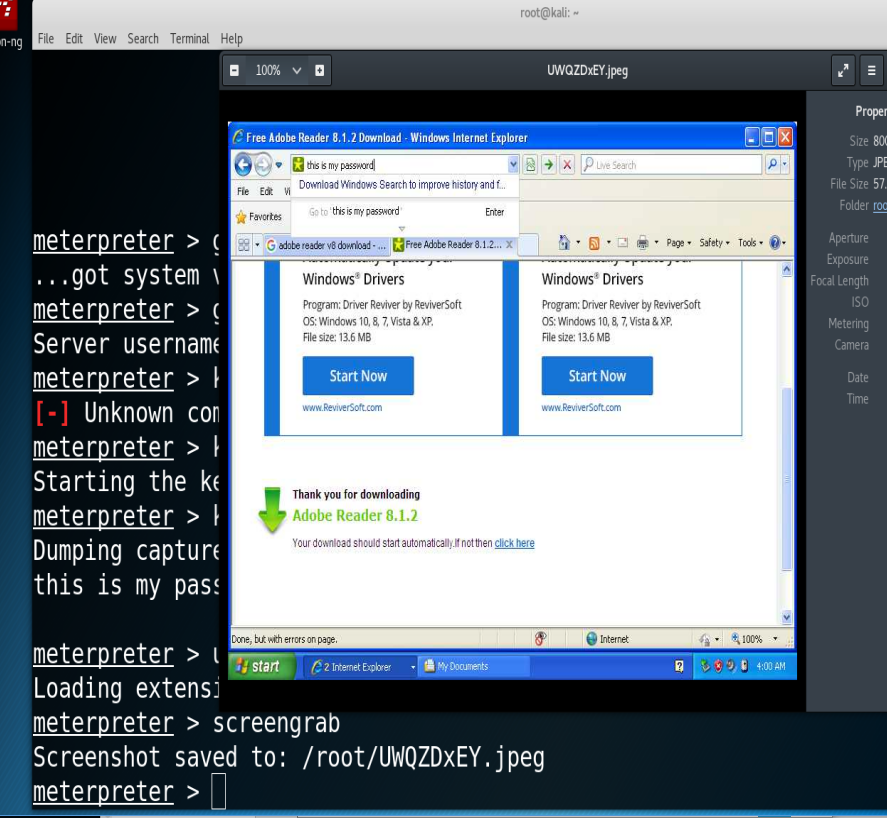
*Used getsystem command to obtain a vector into the target to obtain admin rights. The named pipe impersonation was used, and admin rights were granted.*



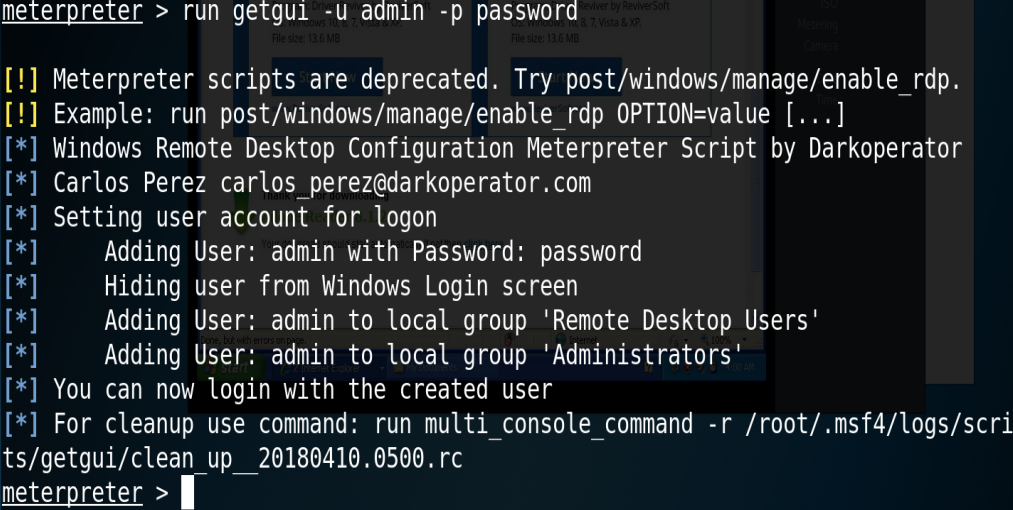
*Starting the keylogger.*



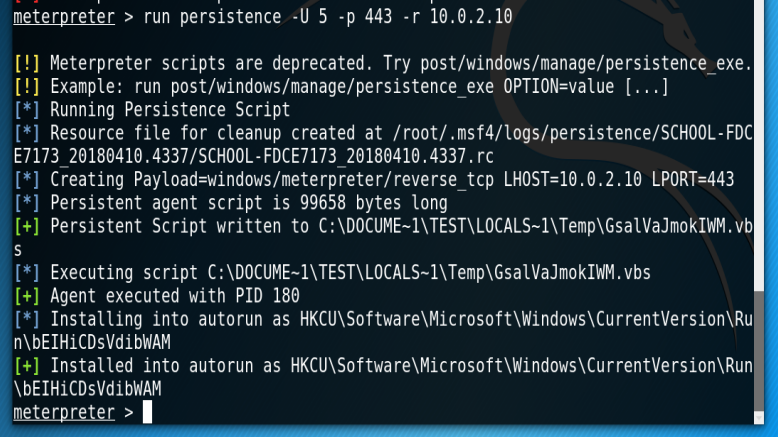
*Keylogged strokes are shown.*



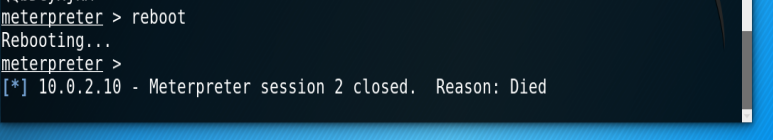
*Screen grab of the targets desktop.*



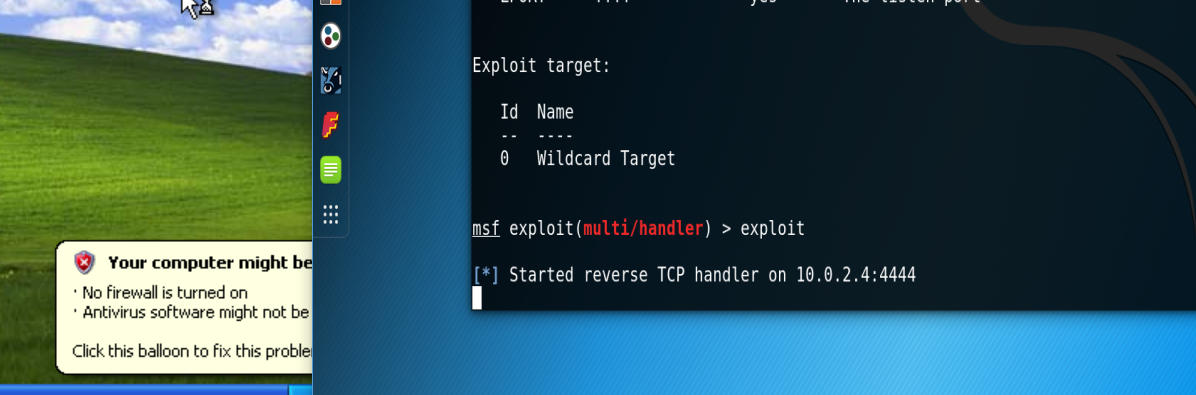
*Creates a new admin account that is not displayed on the WIN XP user login screen.*



*Installation of backdoor.*



*Closing of the session.*



*Unfortunately, I was not able to reconnect to the target despite the installation of the backdoor. I do however know what happened. In a few steps above, I botched up a step and installed the backdoor twice. This created 2 of the same scripts, in which the started mutli/handler exploit called upon. This created a direct problem when accessing the backdoor script because the exploit was calling on both, in which I received a runtime error on the target machine. I am confident that, if I only installed 1, the backdoor would operate as requested.*

**Refection:**

This lab definitely reinforced the concept of “Finding the right target” and the importance of good reconnaissance. It also shows the importance of patch updates and OS upgrades, as our targets were using fairly old, and known, attack vectors (Adobe v8, WIN XP). This concept had me reflect on my current mindset when it comes to updating and patching the programs on my own devices. Although our targets were seemingly archaic, it’s not out of the realm of possibility that a standard computer user, or even professional organization, would still use these configurations shown in the lab. In fact, I feel that quite a few users still have computers and devices they’ve owned for years, without upgrades, and programs that haven’t been patched since the software was downloaded and installed. In short, there’s billions of devices connected to the internet, and chances are pretty good that there’s more than a few that fit an attackers needs/parameters no matter how specific they need to be. Being mindful of patching personal/professional devices and maintaining a relatively new OS upgrades on systems can mitigate the attack vectors that may be used for an attack.