Lab # — Assessment Worksheet

**Course Name and Number: IAM302**

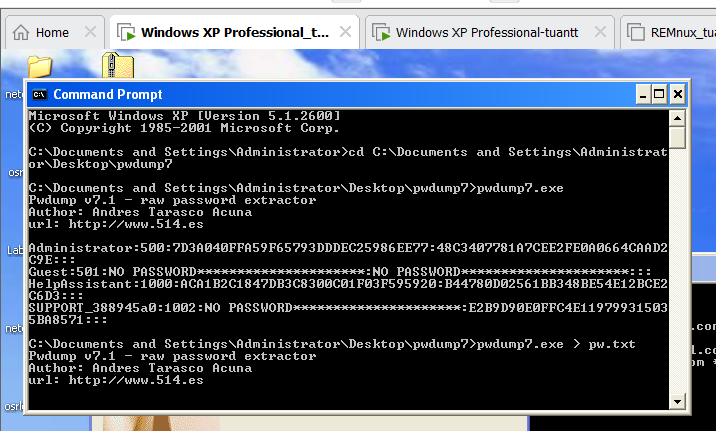
**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

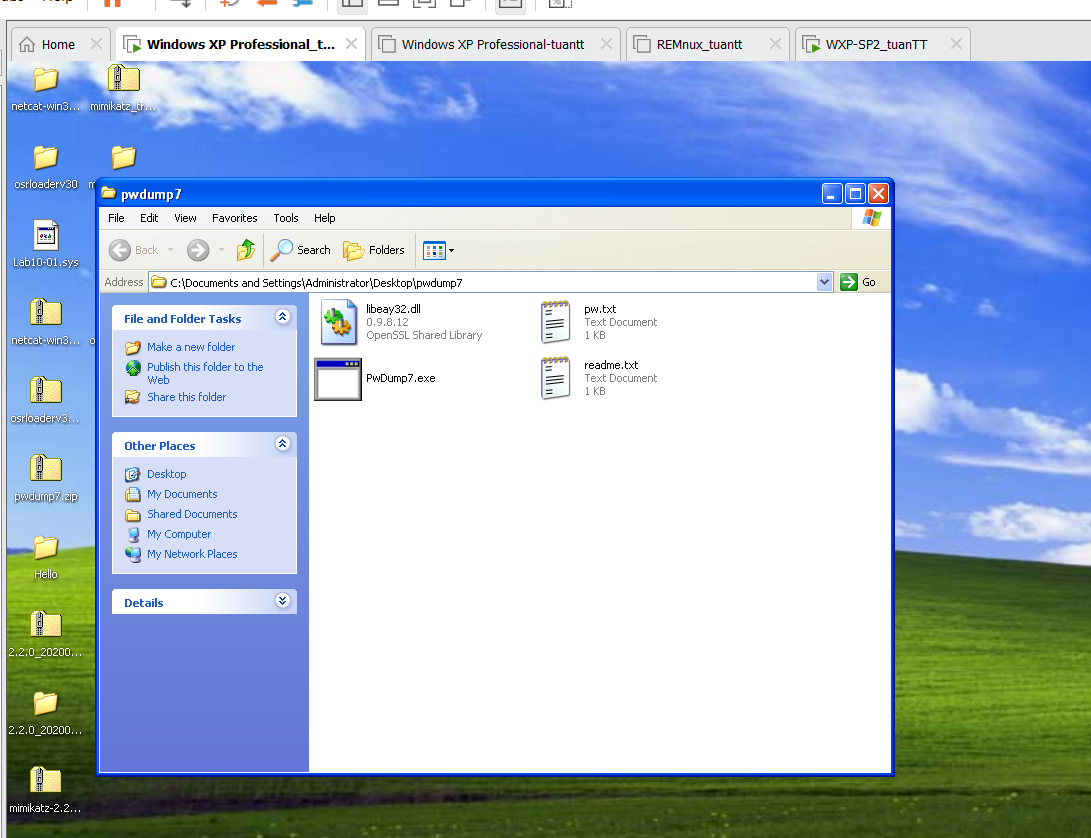
**Instructor Name: Vu Duc Ly**

**Using Pwdump**

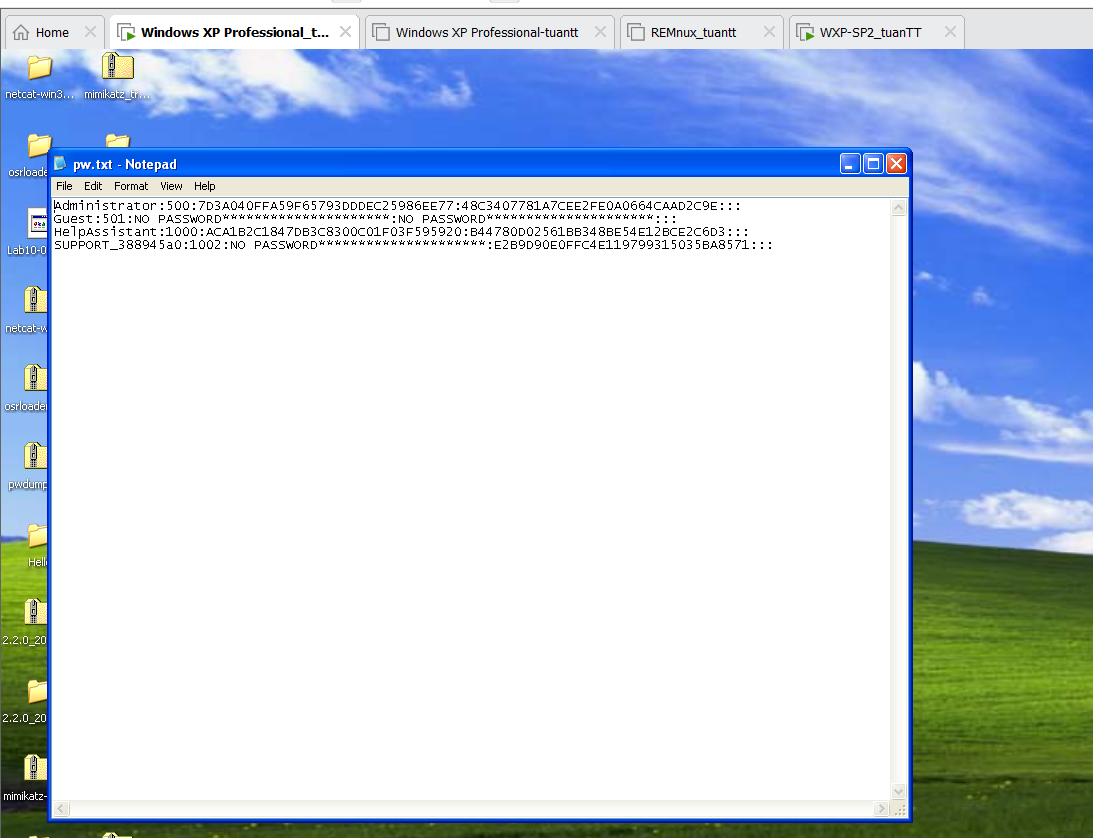
***Running Pwdump7***



***Saving the hash to pw.txt***



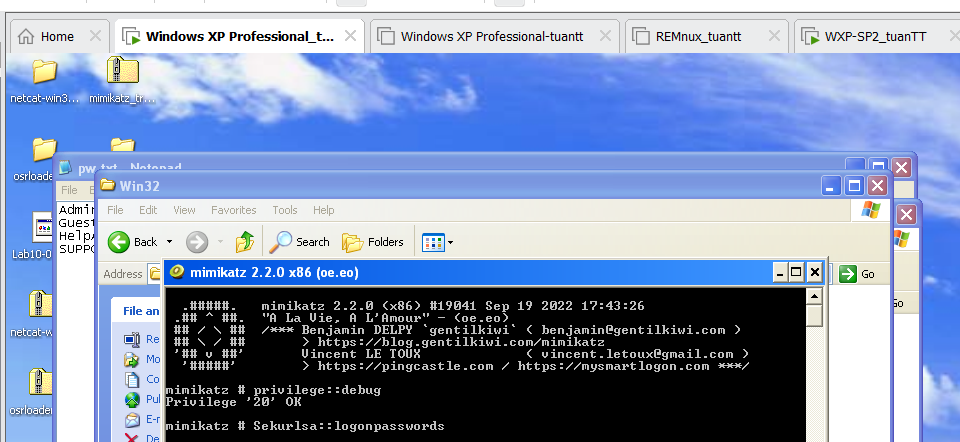
***Result***



***Using Mimikatz***

I set the admin password to #5802$Tttu@N!. After running pwdump, we will see the user information as well as the password in the form of a hash.

Normally, this hash code has many ways to pass such as using some tools like HashCat as well as Pass-The-Hash Toolkit. However, all the tools above have one thing in common that they are all based on a password attack called Bructe Force, which means it will scan for matching characters based on a WORDLIST built-in about more than 10,000 different concatenated characters. Bructe Force in this situation happens quite difficult and takes more time for very difficult password cases such as adding a few special characters (@ # $ ^&A)



***Results***

