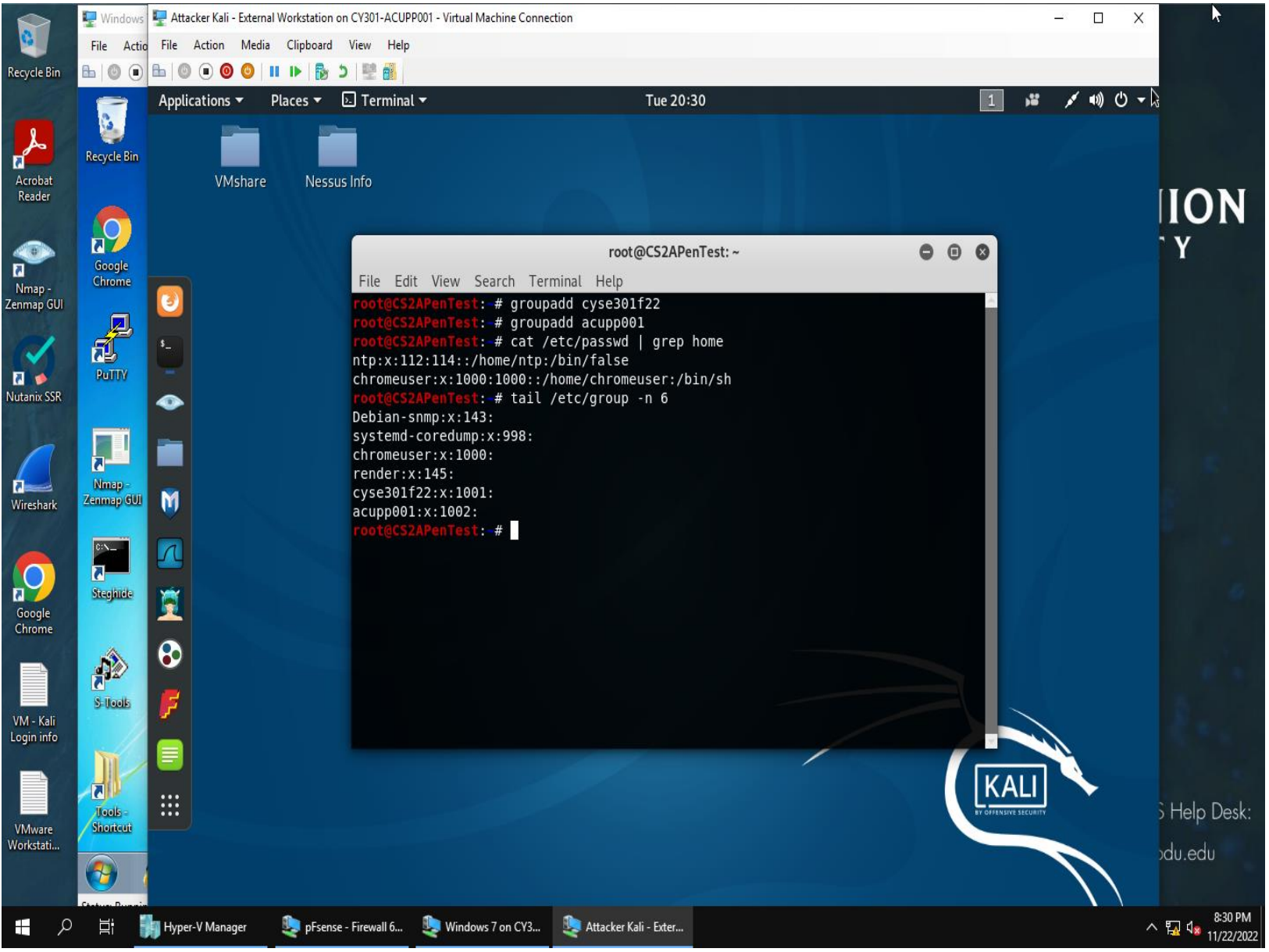
OLD DOMINION

CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS

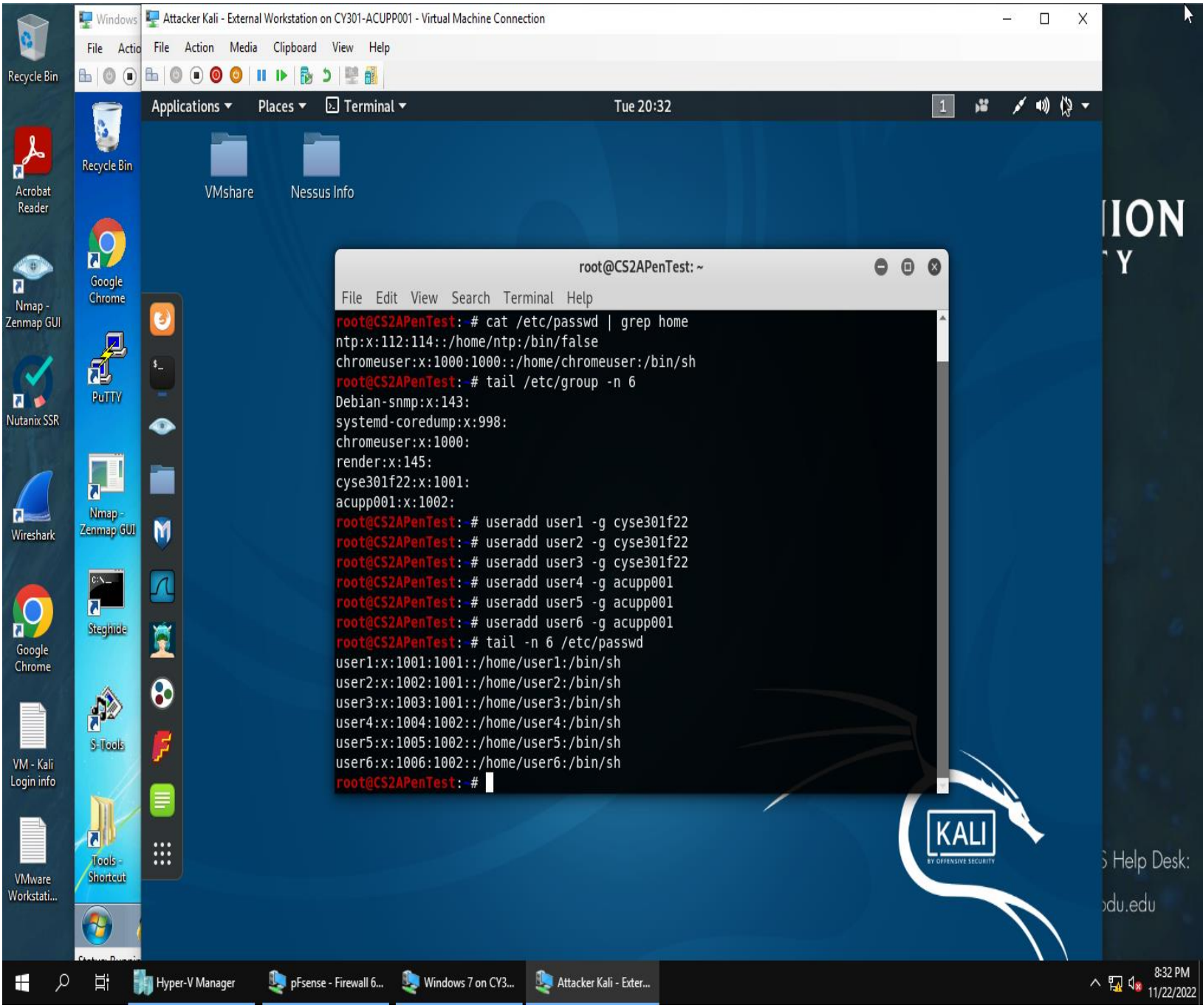
Assignment #5 – PASSWORD CRACKING

AUSTIN CUPP

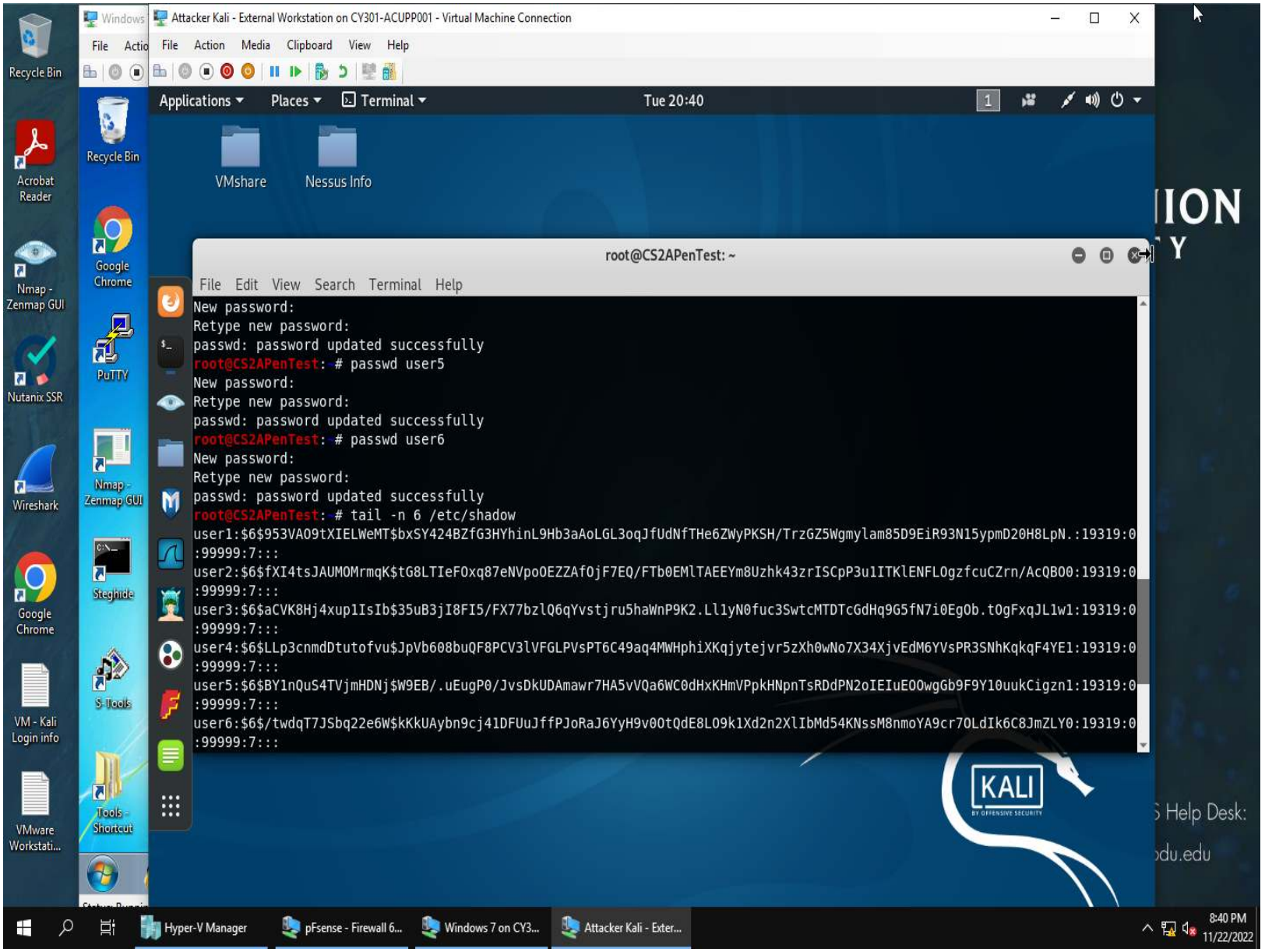
01183567



A.1 Two groups are created. one is cyse301f22, and the other is acupp001 which is my midas ID.



A2. Created and assigned three users to each group with information displayed.



A3. Six new passwords chosen, from easy to hard, and assigned to the users I created.

Username and password below

User1: password

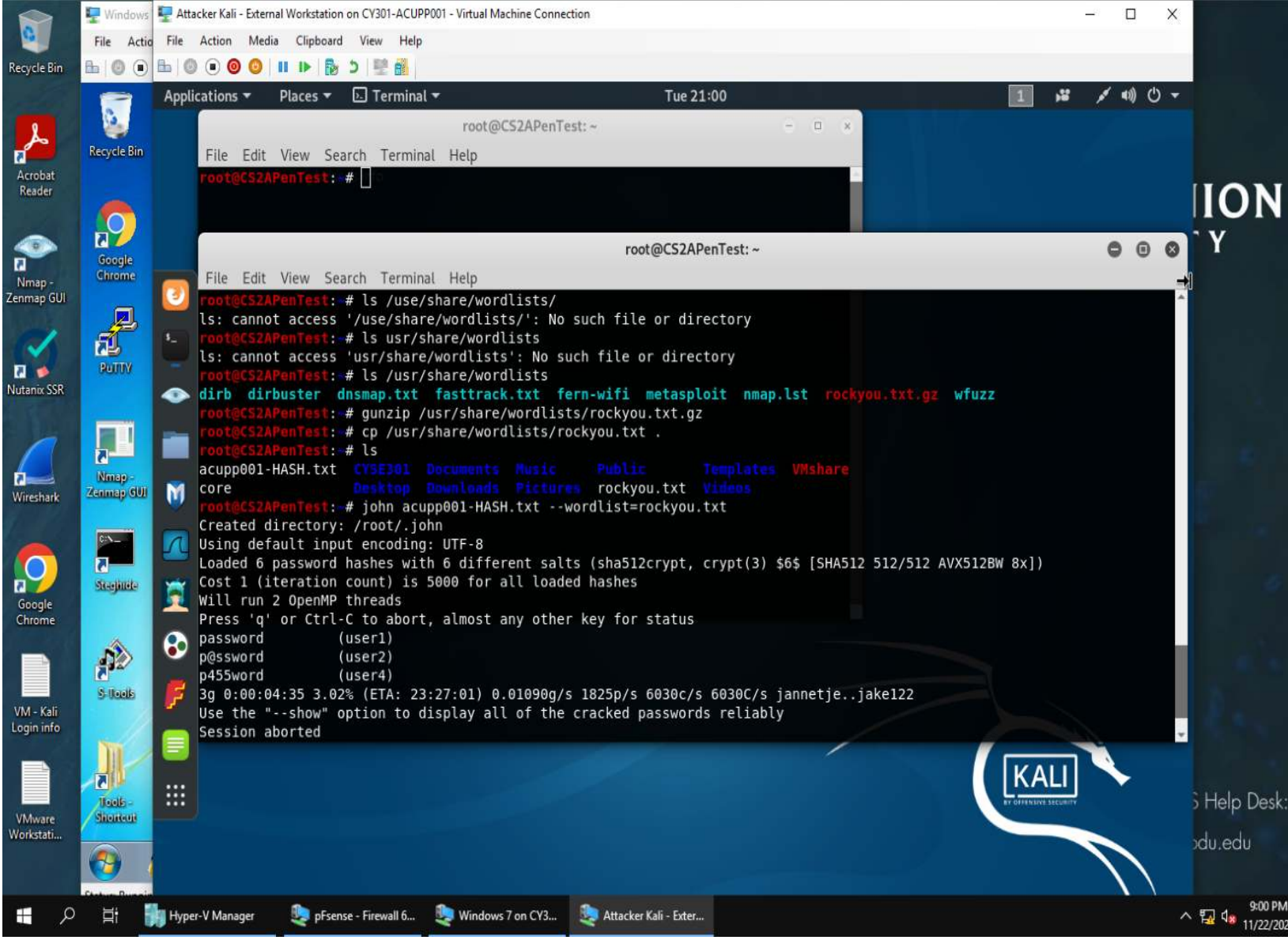
User2: p@ssword

User3: claudion125

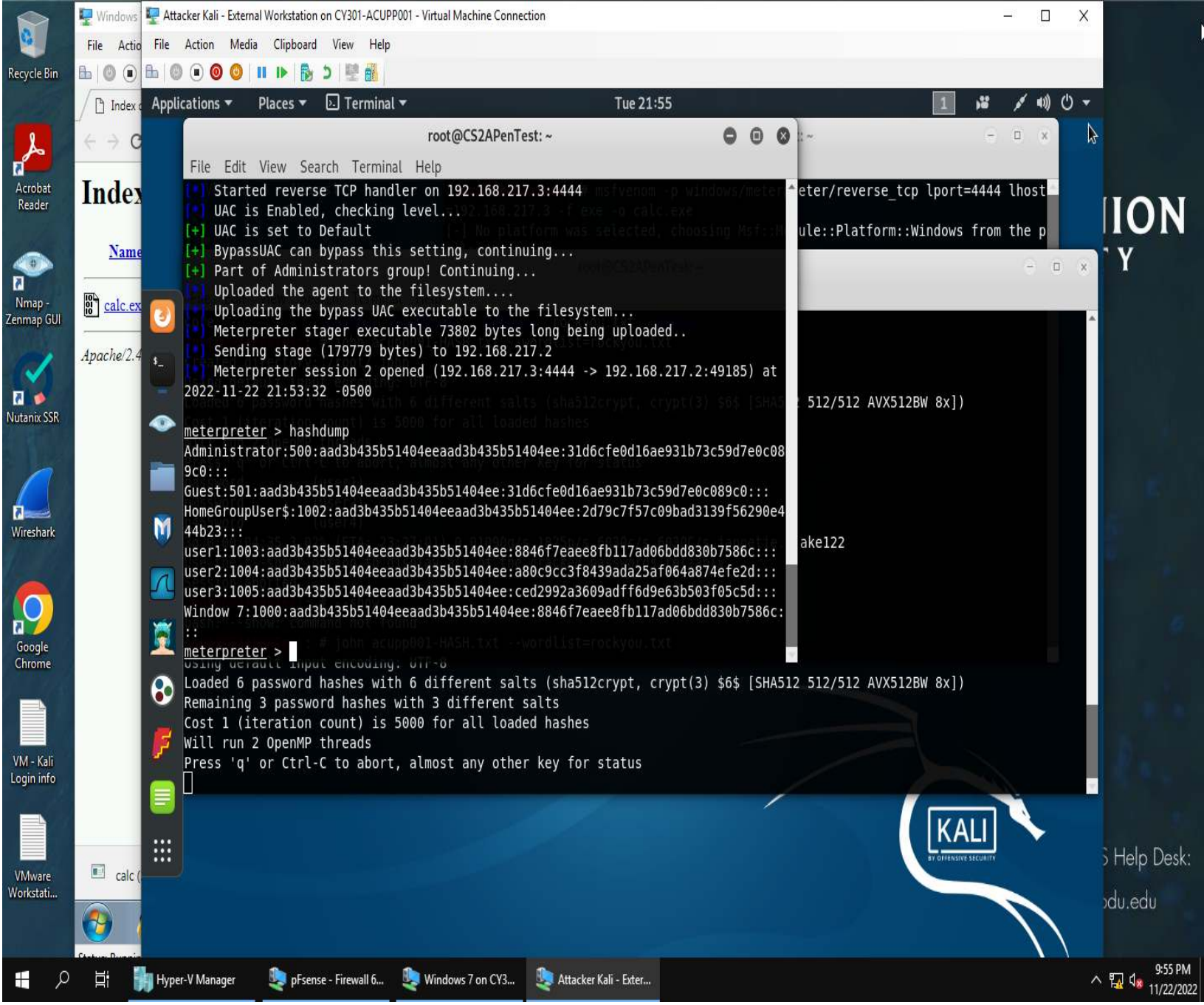
User4: p455word

User5: pa55wordx

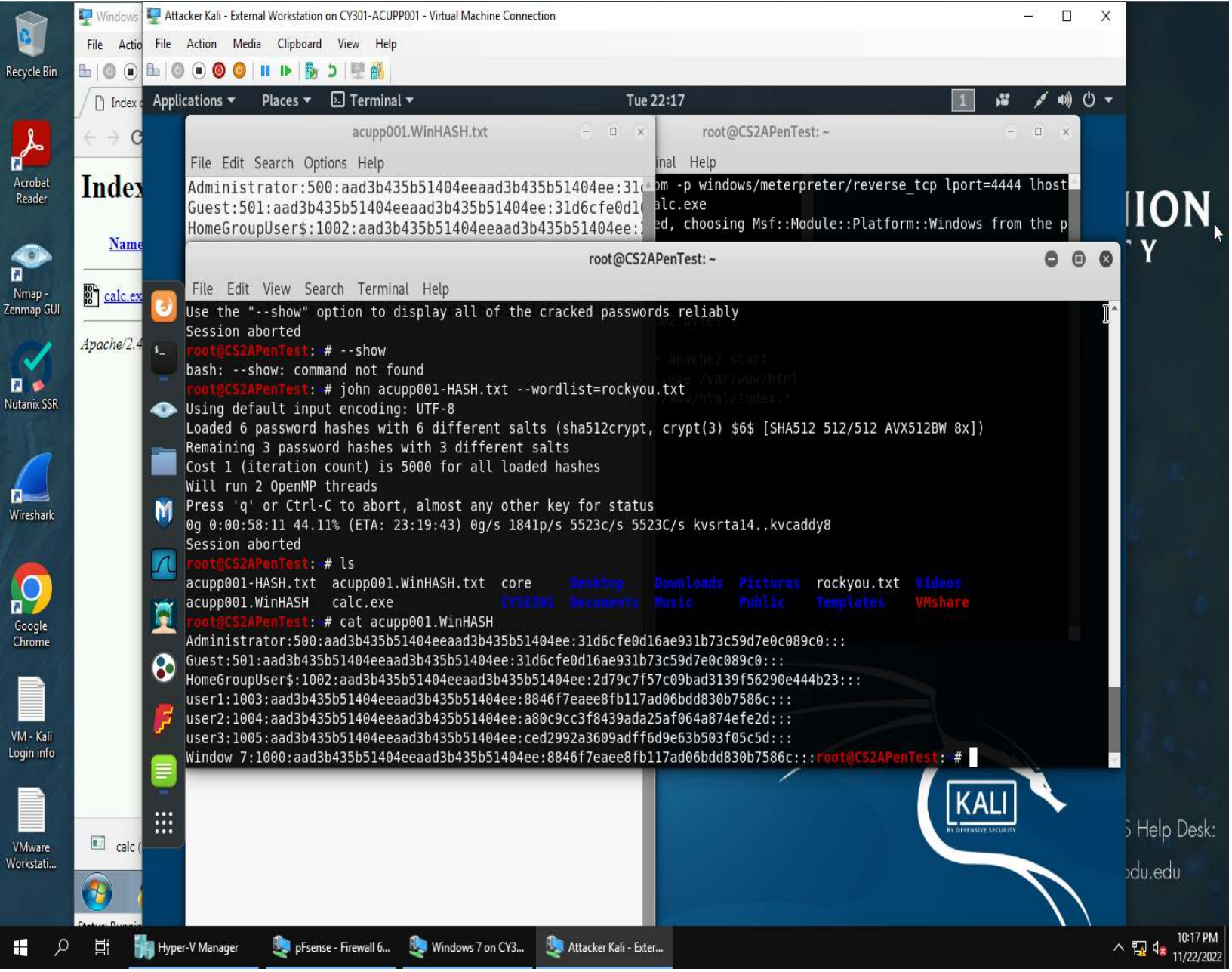
User6: p455wordxx



A4. All six users' password hashes are exported into a file named acupp001-HASH.txt. Then a dictionary attack is launched to crack the passwords. 3 passwords are cracked, user1, user2, and user4

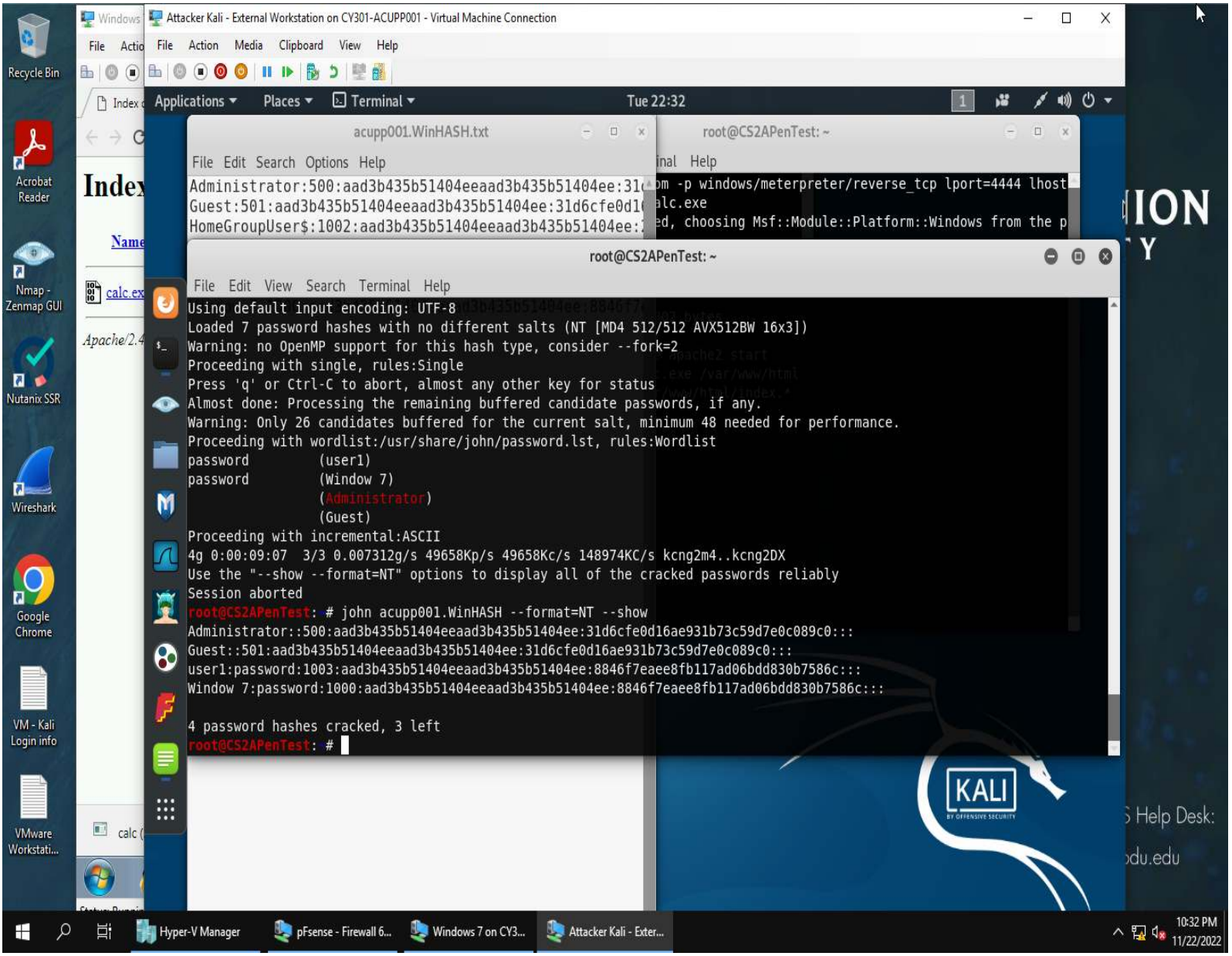


B1. Password hashes are displayed by using the “hashdump” command in the meterpreter shell.

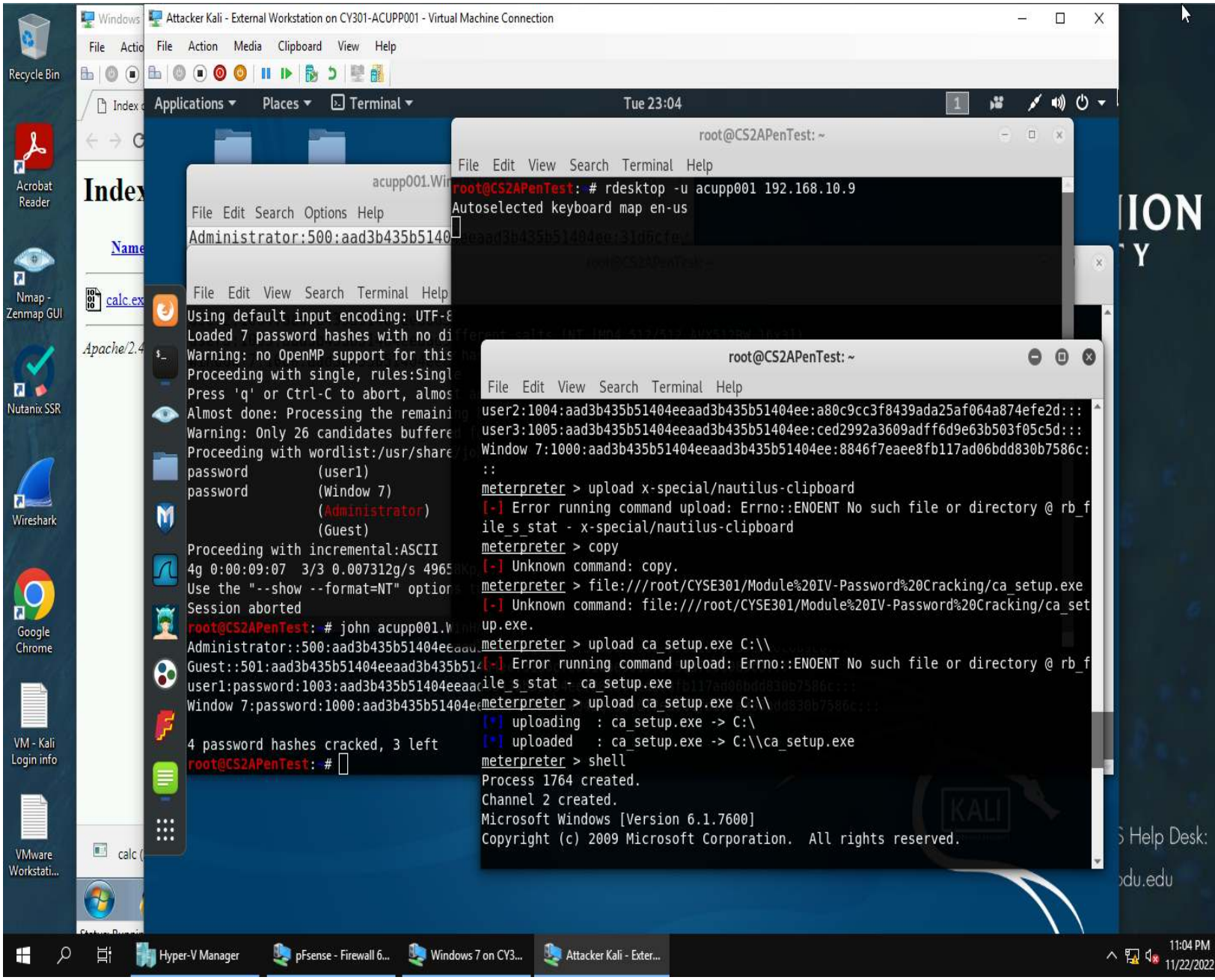


B2. Password hashes are saved into a file named acupp001.WinHASH in Kali Linux.

THE REST OF B2 IS ON THE NEXT PAGE

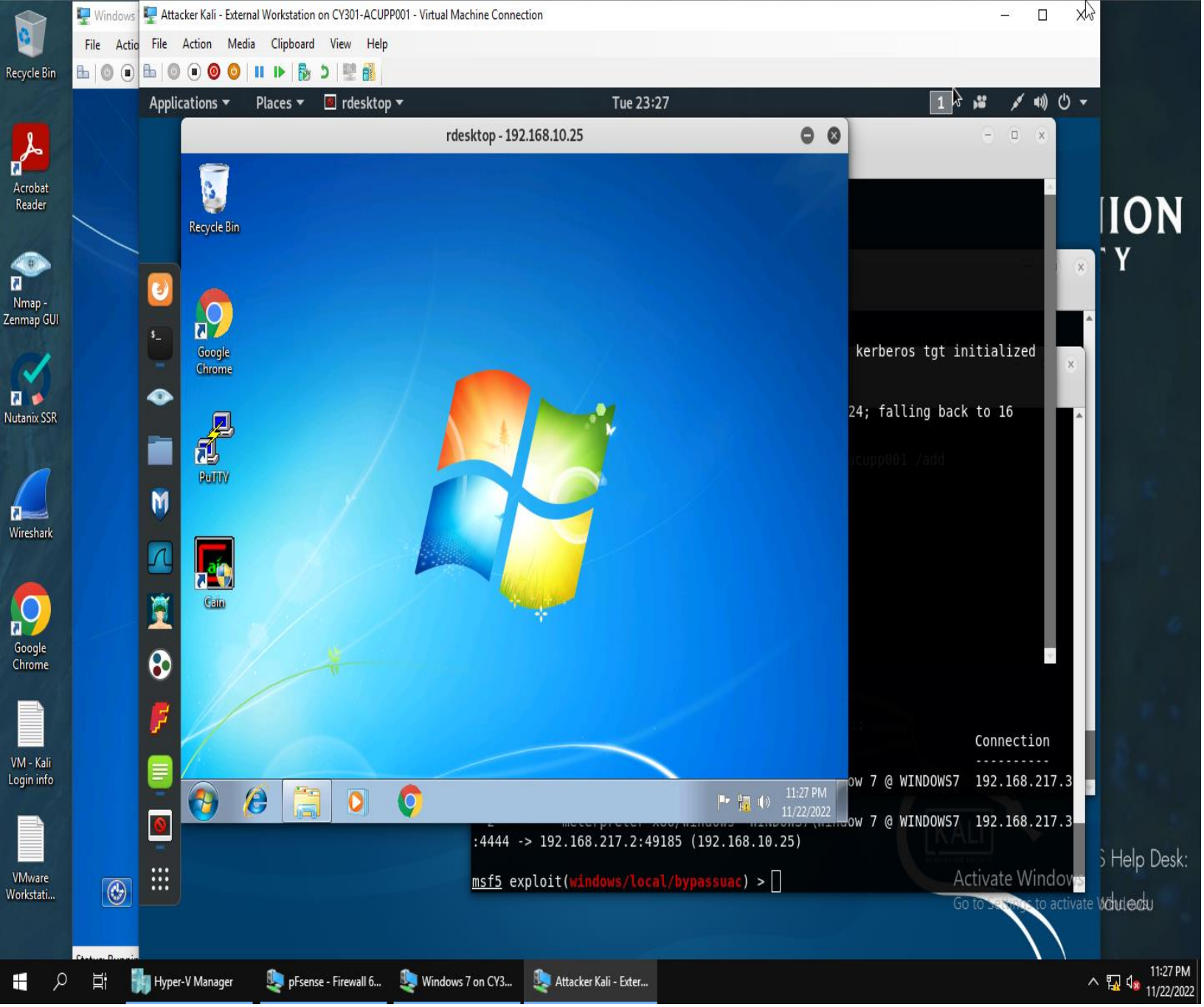


B2. John the ripper is run for 10 minutes to crack the passwords. 4 passwords were cracked, with 3 left.



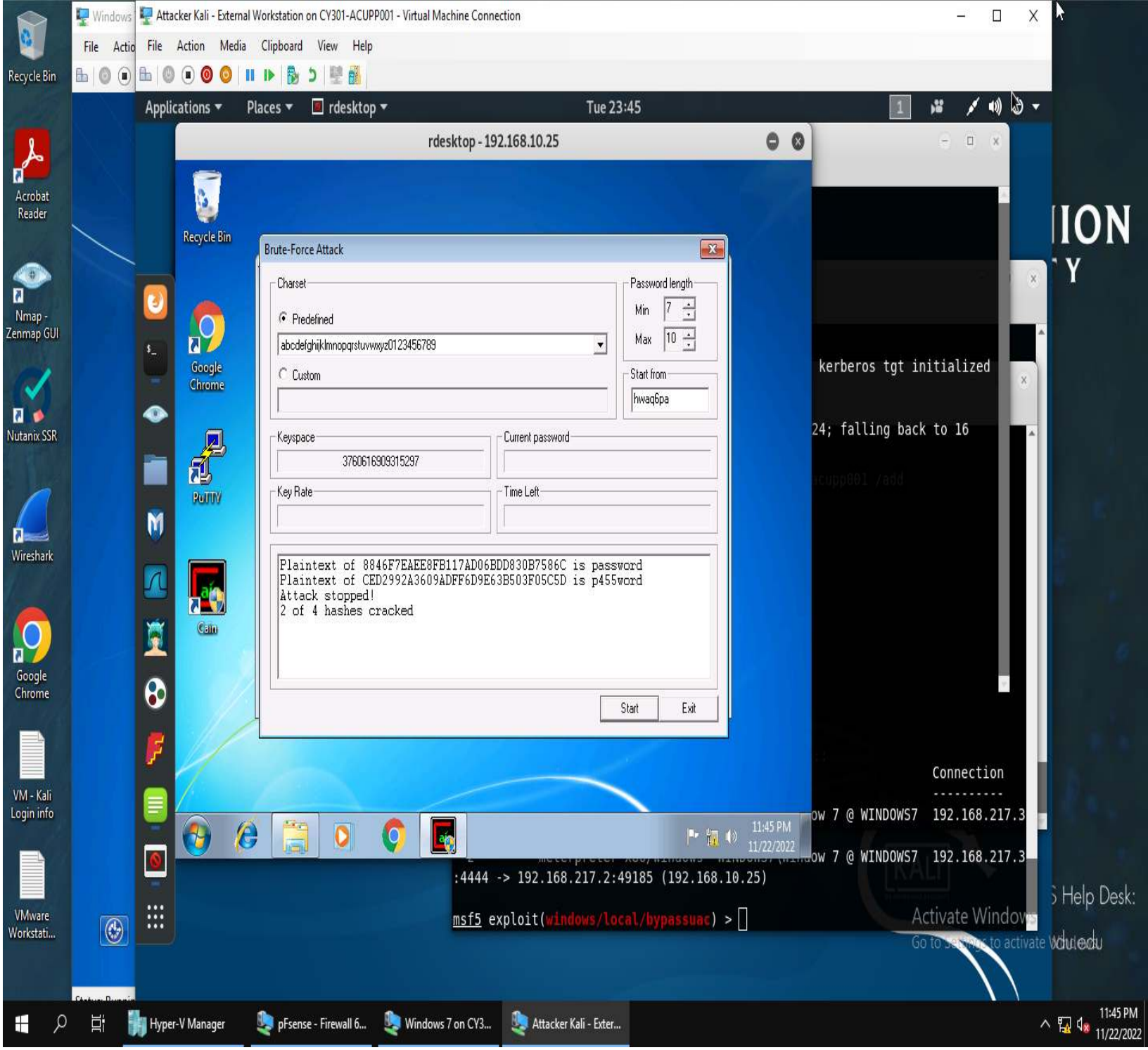
B3. Uploaded the password cracking tool, Cain and Abel, to the remote Windows 7 VM.

B3 CONTINUES ONTO THE NEXT PAGE



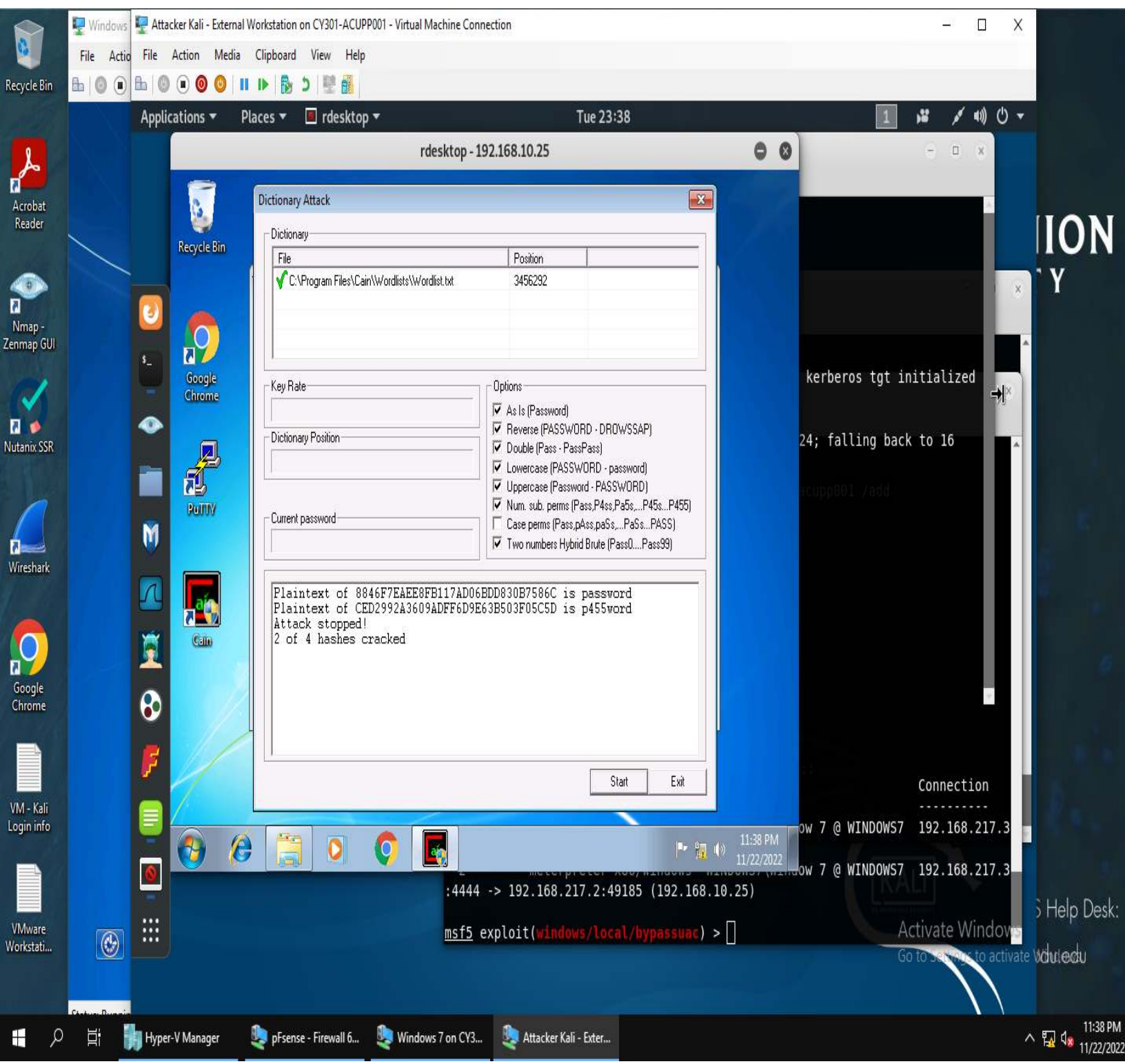
B3. Cain and Able is installed via a remote desktop window.

B3 CONTIUES ONTO THE NEXT PAGE



B3. Brute force attack is implemented to crack the passwords, 2 of 4 are cracked.

B3 CONTIUES ONTO THE NEXT PAGE



B3. Dictionary attack is implemented to crack the passwords, 2 of 4 are cracked.