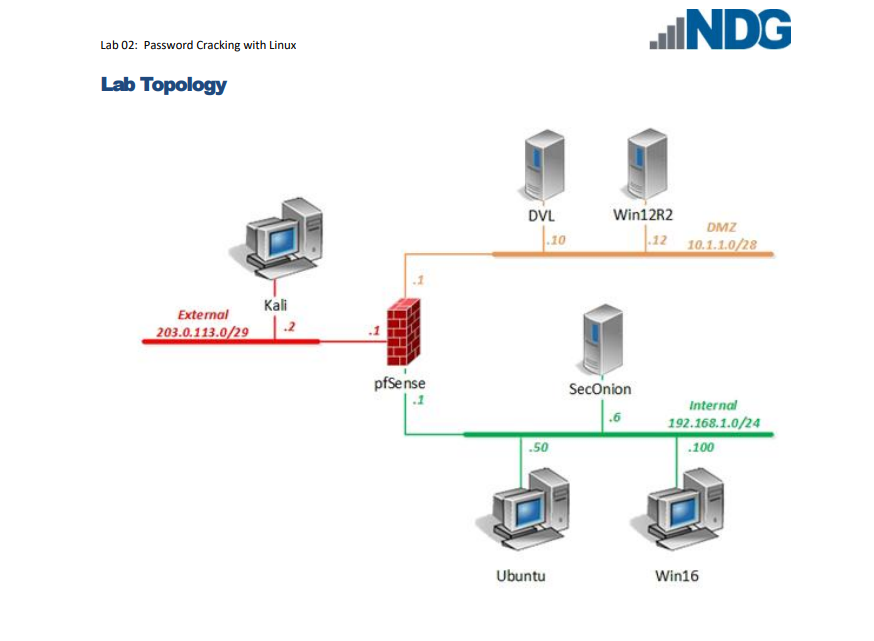
Lab 2-3 password cracking

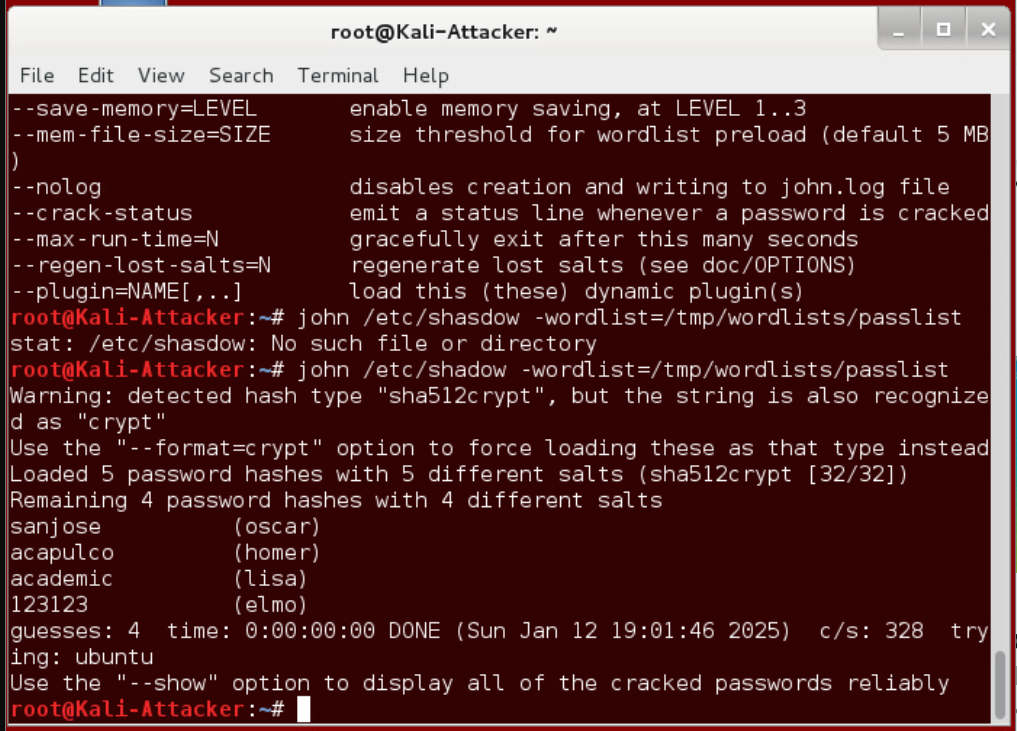


Initially created 4 different accounts on the virtual kali machine with different passwords

And confirmed their hashes exists by looking into the /etc/shadow directory.

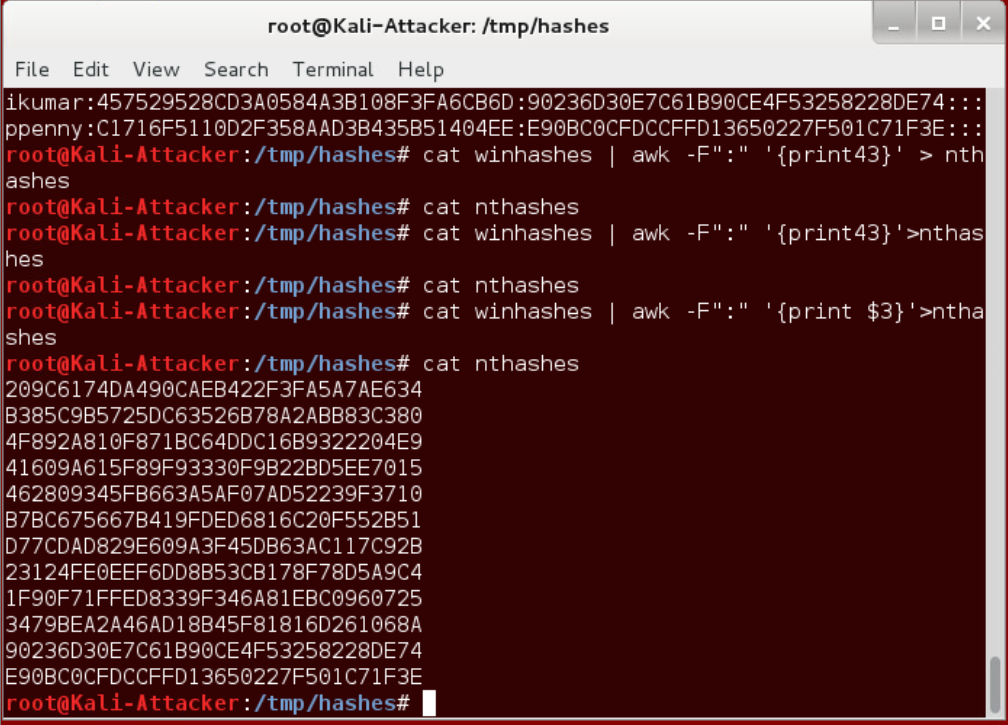
The command I need to use is ‘john /etc/shadow –wordlist=/tmp/wordlists/passlist’

John in this case is using John the Ripper program against /etc/shadow file with a wordlist that is pre existing in the virtual machine. (passlist)

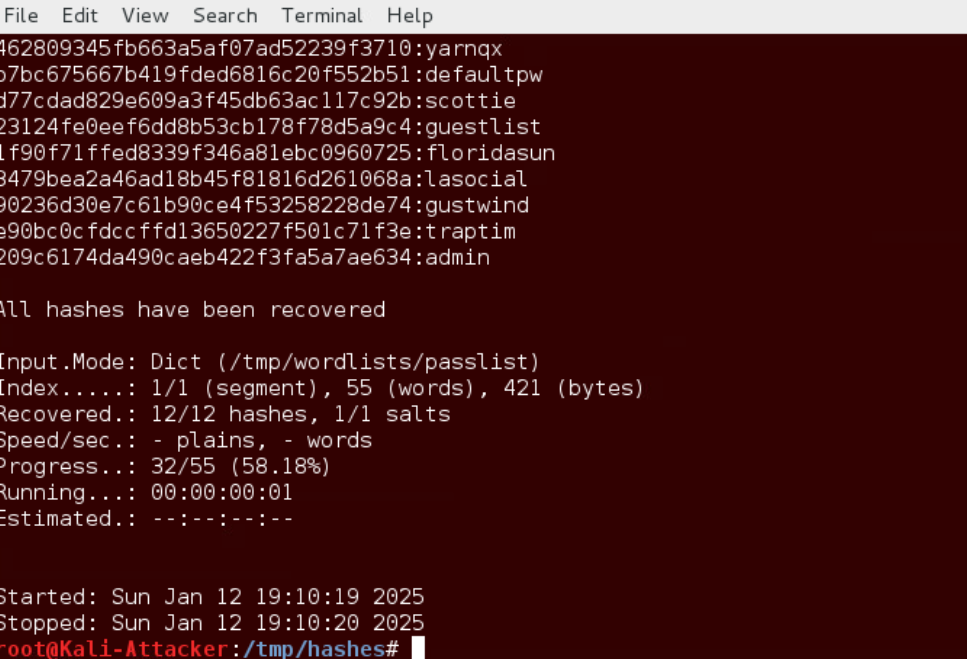


With that, the terminal is indicating that it detected 5 sha512 hashes with salts. And within less than a second, it managed to crack the passwords for 4 arbitrary accounts I have created for this exercise.

From the same machine, I parsed out 32 hexadecimal NThashes from its winhashes file.



By running Hashcat against the newly parsed list of NThashes, also with the help of existing passlist dictionary file, I managed to crack the password.



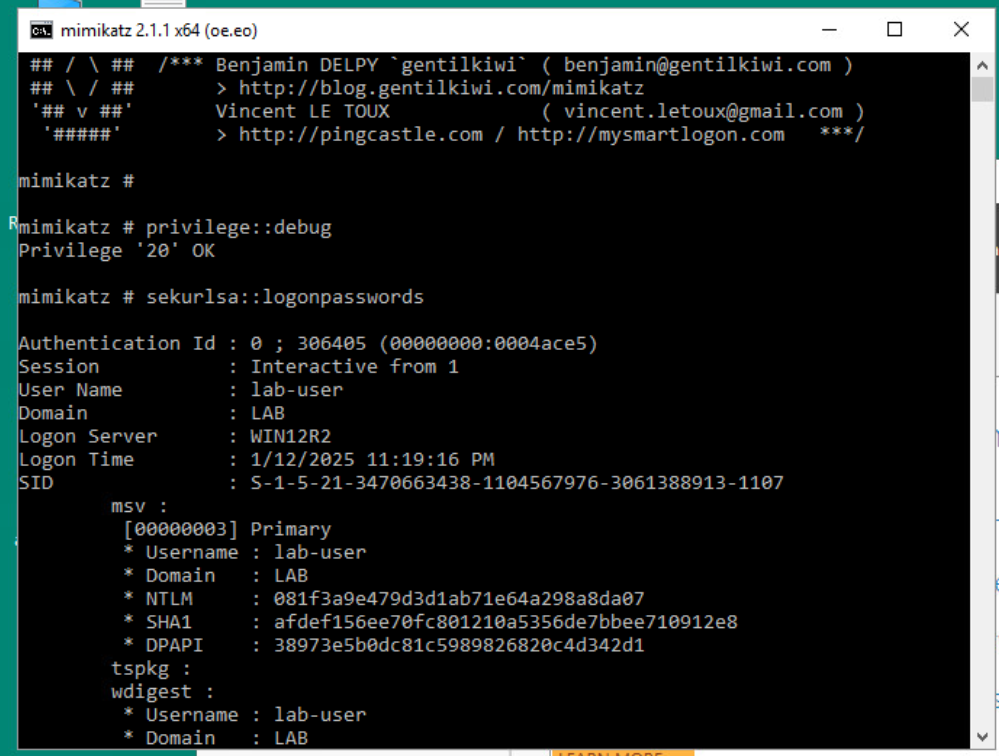
I initiated ftp 10.1.1.10 to remotely FTP into a separate machine (10.1.1.10) that has FTP service enabled. Then I navigated to 10.1.1.10’s etc folder to ‘get’ shadow file.

Since now I have 10.1.1.10’s password hash file, I can repeat the previous steps of using john the ripper to crack the passwords.

It was simple to port into another machine and test john the ripper and hashcat on linux OS.

For window,

I found a credential information of the test account with mimikatz application and sekurlsa module.



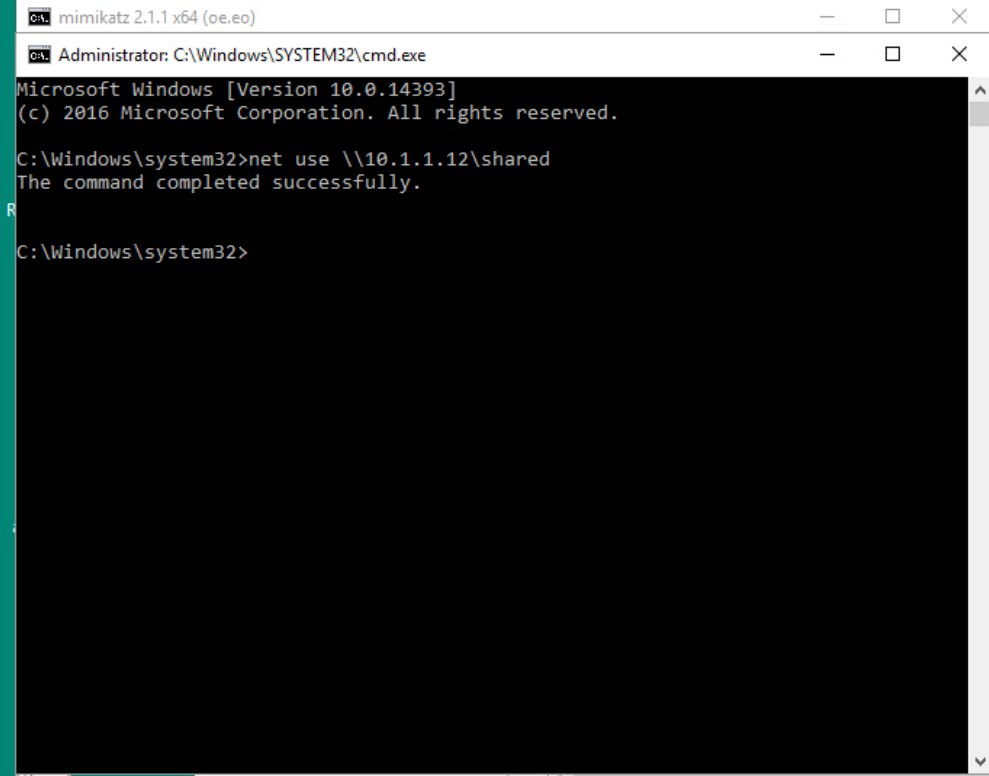


Its still in hash form.

mimikatz # sekurlsa::pth /user:lab-user /domain:LAB /ntlm:<NTLM hash> /run:cmd.exe

pth means pass the hash. So perform the pass the hash attack on user name: lab-user of domain: LAB, verifying with the NTLM hash I pasted and commanded to open another command prompt window.

The theory is by using the known NT hash, I can use it to authenticate over NTLM.



And by testing it on 10.1.1.12 (win12 not win16 machine that we pulled the NTLM hash from), I was about to connect it.

So by having the admin level hash from one machine, I can utilize it to move laterally to another machine within the same network. I could repeat to fine the NTLM hash of next machine and keep moving.