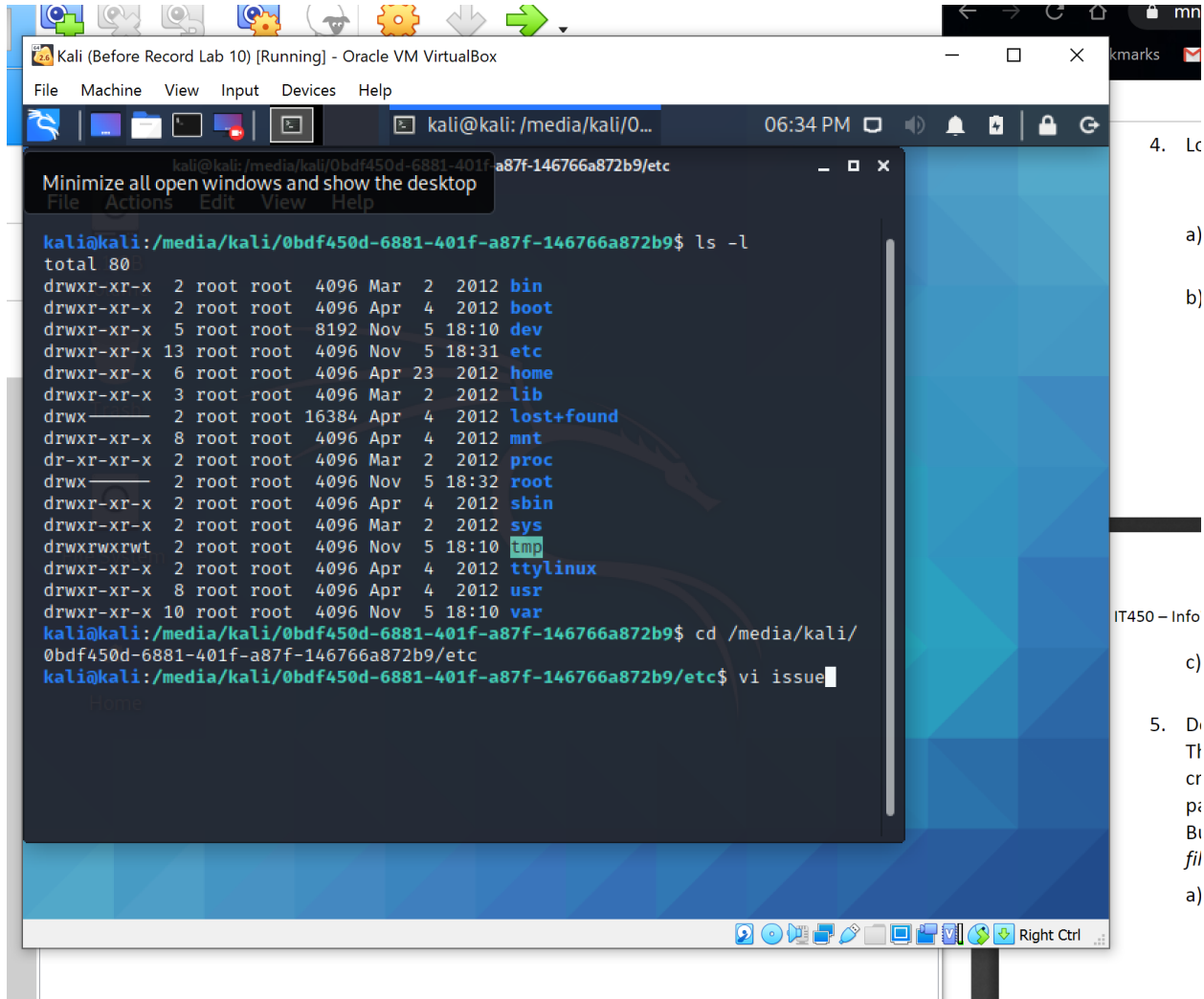


Matthew Young

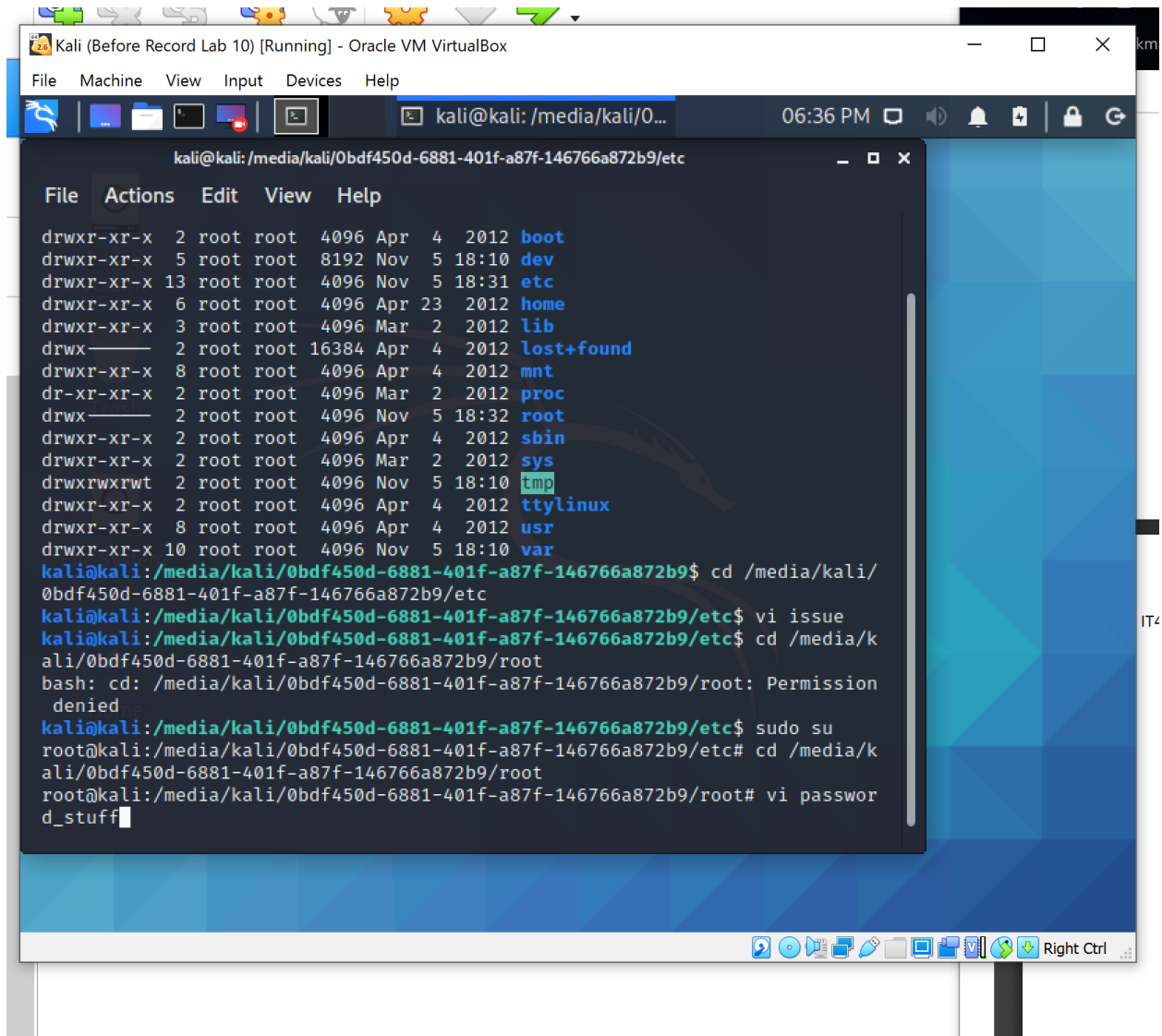
CIS 450

Lab11 – Bypassing Authentication

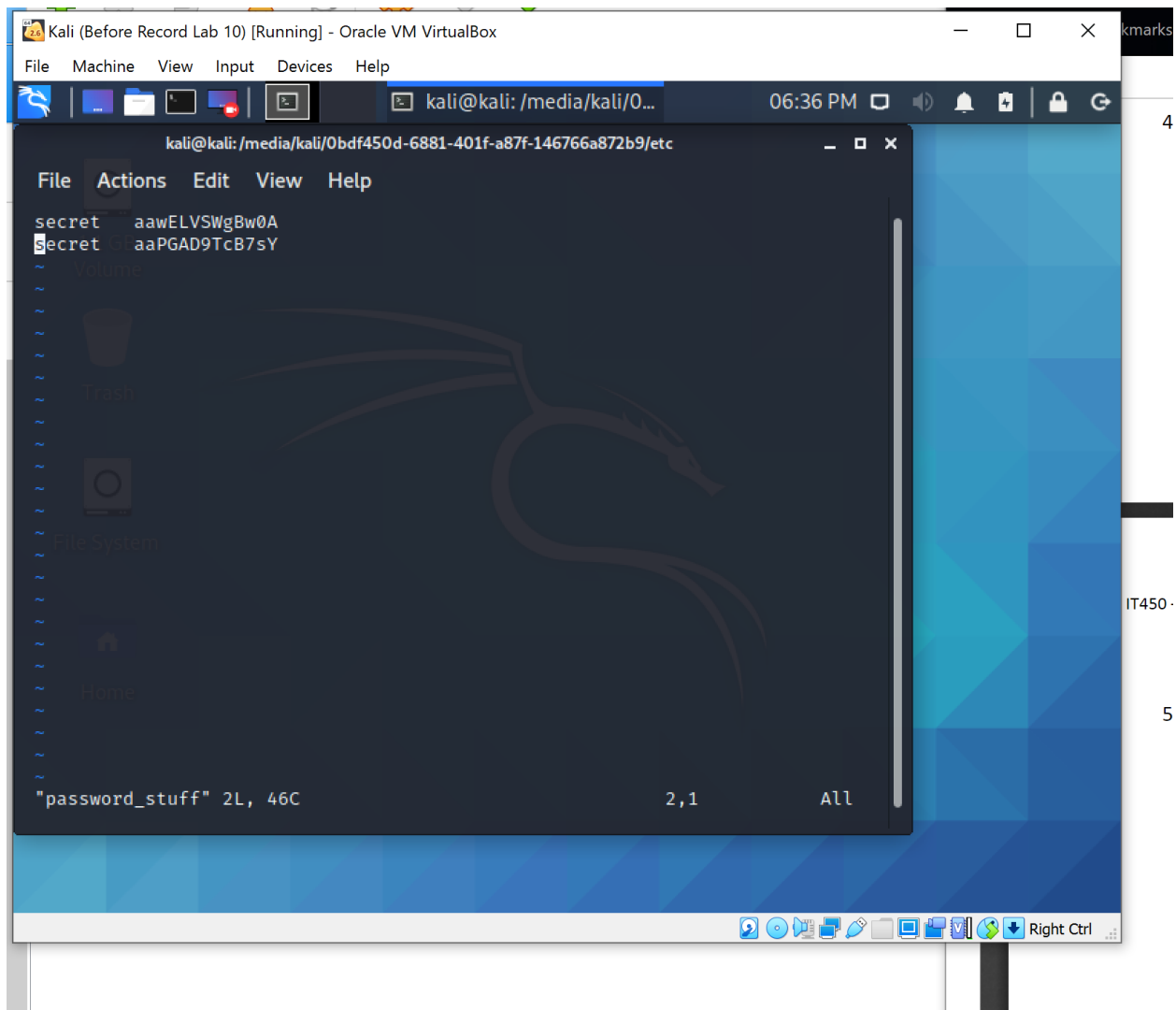
Issue file location:



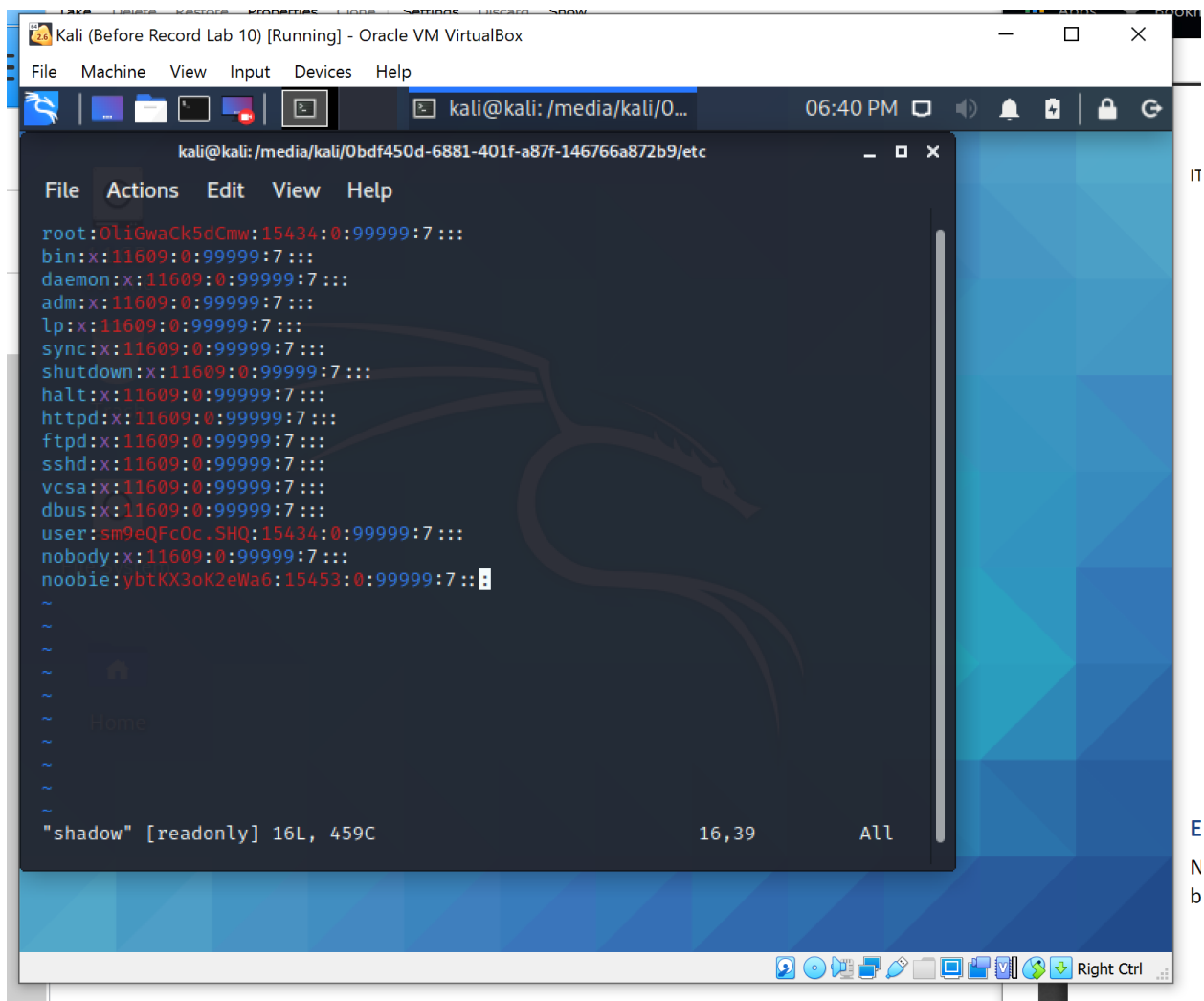
Issue file data:



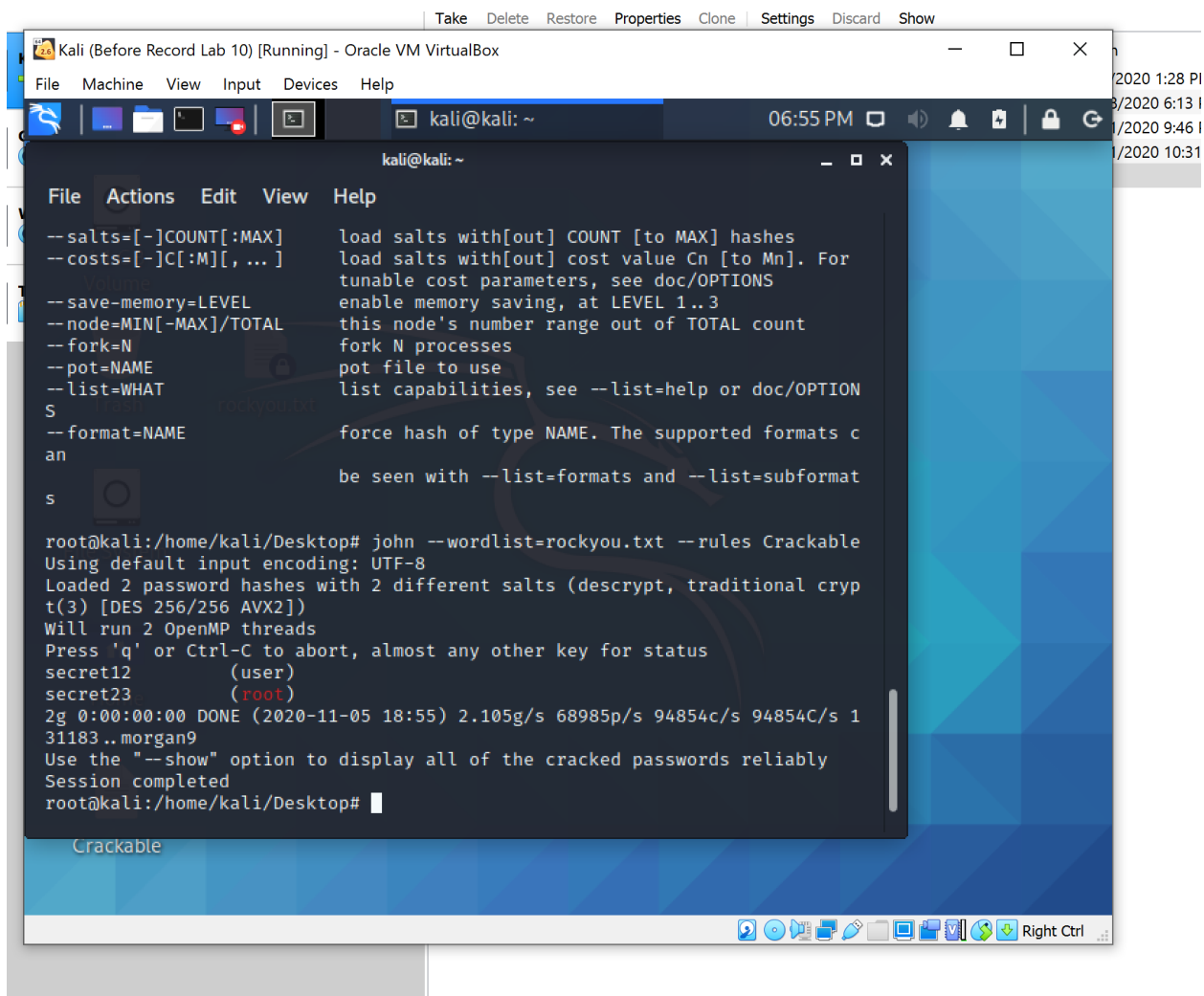
Password_stuff File data:



Shadow file of usernames and password hashes:



Cracked passwords for user and root:



```
Take Delete Restore Properties Clone Settings Discard Show
Kali (Before Record Lab 10) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~ 06:55 PM
kali@kali: ~
File Actions Edit View Help
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][, ...] load salts with[out] cost value Cn [to Mn]. For
tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count
--fork=N fork N processes
--pot=NAME pot file to use
--list=WHAT list capabilities, see --list=help or doc/OPTION
S
--format=NAME force hash of type NAME. The supported formats c
an
s
be seen with --list=formats and --list=subformat
s
root@kali:/home/kali/Desktop# john --wordlist=rockyou.txt --rules Crackable
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (descrypt, traditional cryp
t(3) [DES 256/256 AVX2])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
secret12 (user)
secret23 (root)
2g 0:00:00:00 DONE (2020-11-05 18:55) 2.105g/s 68985p/s 94854c/s 94854C/s 1
31183 ..morgan9
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/home/kali/Desktop#
```

TinyLinux authentication has been bypassed:

Lab 11: Bypassing Auth update... where are password hashes stor...
mnscu.learn.mnstate.edu/43/16/content/5065884/viewContent/44765786/view
App... Bookmarks... Inbox... Netflix... Handshake... https://www.mnscu... Highland Hills App... Work... School... Utilities... School Email... Learn site

CIS 450/550-01/02 Information Warfare

Matthew Young

Course HomeMaterialsCommunicationAssessmentsStudent Resources

Table of ContentsLab 11

TinyLinux (Running) - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

Login timed out after 60 seconds

ttlinux ver 10.0 (haznoka)
[486 class Linux kernel 2.6.34.6 (/dev/tty1)
The initial pwd was "password" for "root" & "user" accounts... but no more :)
ttlinux_host login: user
Password:
Login incorrect
ttlinux_host login:
Login timed out after 60 seconds
ttlinux ver 10.0 (haznoka)
[486 class Linux kernel 2.6.34.6 (/dev/tty1)
The initial pwd was "password" for "root" & "user" accounts... but no more :)
ttlinux_host login: user
Password:
Login incorrect
ttlinux_host login: root
Password:
Chop wood, carry water.

revised 3/24/2020
document what
root:0110
bin:x:116
daemon:x:
adm:x:116
lp:x:1160
sync:x:11
shutdown:
halt:x:11
httpd:x:1
ftpd:x:11
sahd:x:11
vcas:x:11
dbus:x:11
user:sm9e
nobody:x:
noble:yp

John-the-ripper should be able to crack the passwords for the "root" & "user" accounts in a matter of seconds. Note: remove the password hashes of any other accounts to make the process go faster.

b) Replacing option: I recommend you take a snapshot before proceeding any further. Carefully edit the password hash file and replace the password hashes for the "root" & "user" accounts with one of these already-known passwords hashes:

papAq5PwY/QQM (i.e. "password") or
LDMEpQwJgY.Mo (also "password")

6. Remember to keep detailed documentation of the actions you took and the items you found.

Example of Screenshot Proof

Note: your VM screenshot should be in the foreground, where the rectangle is. Your D2L course page should be visible in the background of your screenshot.

Type here to search

1:57 PM 11/5/2020