

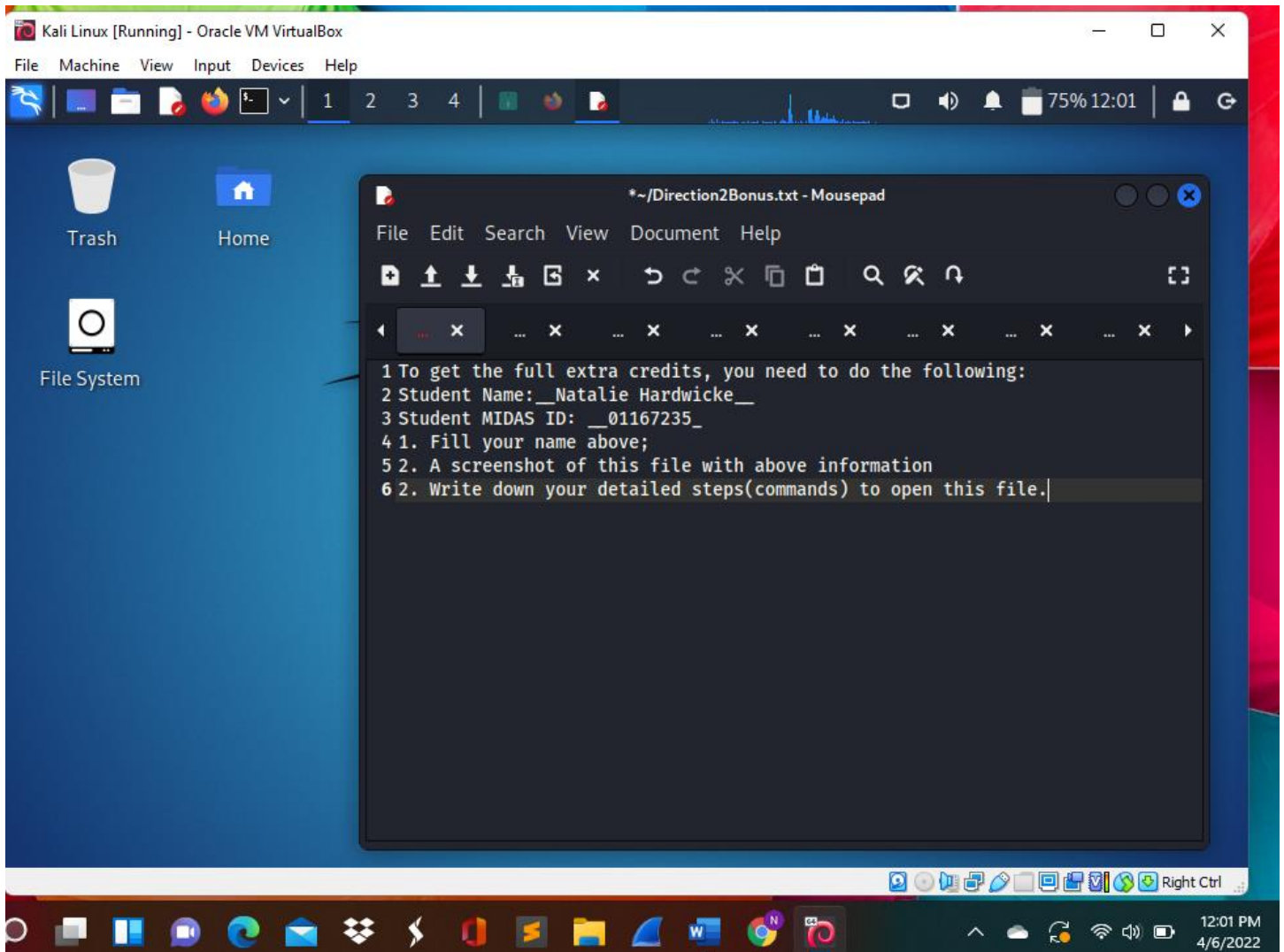
OLD DOMINION UNIVERSITY

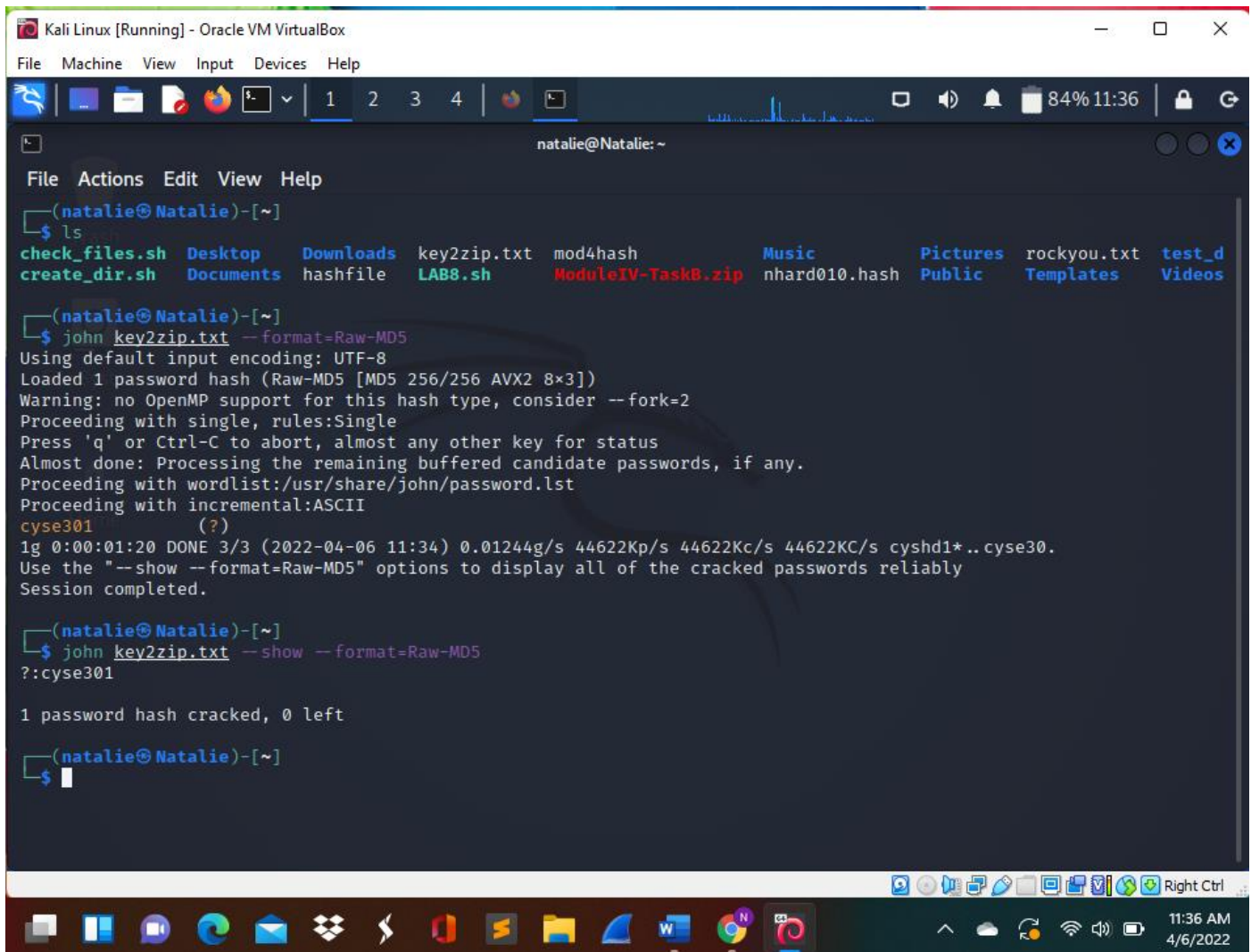
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #M4 Password Cracking

Natalie Hardwicke

01167235





```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
84% 11:36

natalie@Natalie: ~
File Actions Edit View Help
(natalie@Natalie)-[~]
$ ls
check_files.sh Desktop Downloads key2zip.txt mod4hash Music Pictures rockyou.txt test_d
create_dir.sh Documents hashfile LAB8.sh ModuleIV-TaskB.zip nhard010.hash Public Templates Videos

(natalie@Natalie)-[~]
$ john key2zip.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
cyse301 (?)
1g 0:00:01:20 DONE 3/3 (2022-04-06 11:34) 0.01244g/s 44622Kp/s 44622Kc/s 44622KC/s cyshd1*..cyse30.
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

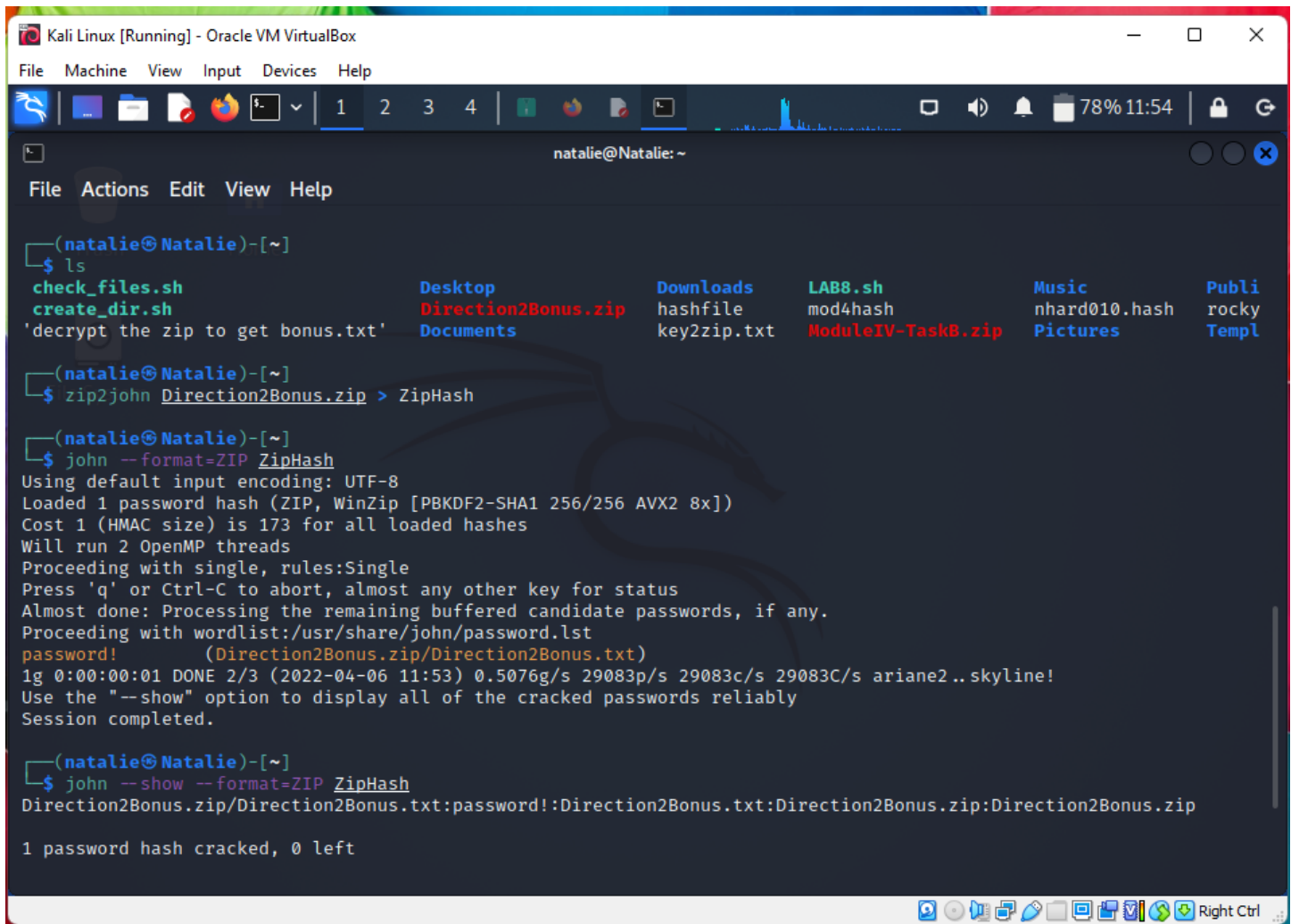
(natalie@Natalie)-[~]
$ john key2zip.txt --show --format=Raw-MD5
?:cyse301

1 password hash cracked, 0 left

(natalie@Natalie)-[~]
$
```

First step was to download the files onto Linux.

Second step, crack the key2zip.txt with john the ripper using the MD5 format. Screenshot above. The password for the ModuleIV-TaskB.zip is "cyse301."



```
(natalie@Natalie)-[~]
$ ls
check_files.sh      Desktop      Downloads    LAB8.sh      Music      Publi
create_dir.sh       Direction2Bonus.zip  hashfile     mod4hash     nhard010.hash  rocky
'decrypt the zip to get bonus.txt' Documents     key2zip.txt  ModuleIV-Task8.zip  Pictures      Templ

(natalie@Natalie)-[~]
$ zip2john Direction2Bonus.zip > ZipHash

(natalie@Natalie)-[~]
$ john --format=ZIP ZipHash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 173 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password! (Direction2Bonus.zip/Direction2Bonus.txt)
1g 0:00:00:01 DONE 2/3 (2022-04-06 11:53) 0.5076g/s 29083p/s 29083c/s 29083C/s ariane2..skyline!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(natalie@Natalie)-[~]
$ john --show --format=ZIP ZipHash
Direction2Bonus.zip/Direction2Bonus.txt:password!:Direction2Bonus.txt:Direction2Bonus.zip:Direction2Bonus.zip

1 password hash cracked, 0 left
```

Third step, Copy the “Direction2Bonus.zip” to my home directory.

Fourth step, get the hash from “Direction2Bonus.zip” using the command “zip2john Direction2Bonus.zip > ZipHash (filename)”

Fifth Step crack the zipfile using John the Ripper with command “john –format=ZIP ZipHash” the password is “password!”

Sixth step, open the “Directions2Bonus.txt” using mousepad and enter your name, midas, and write out the steps. (First screenshot)