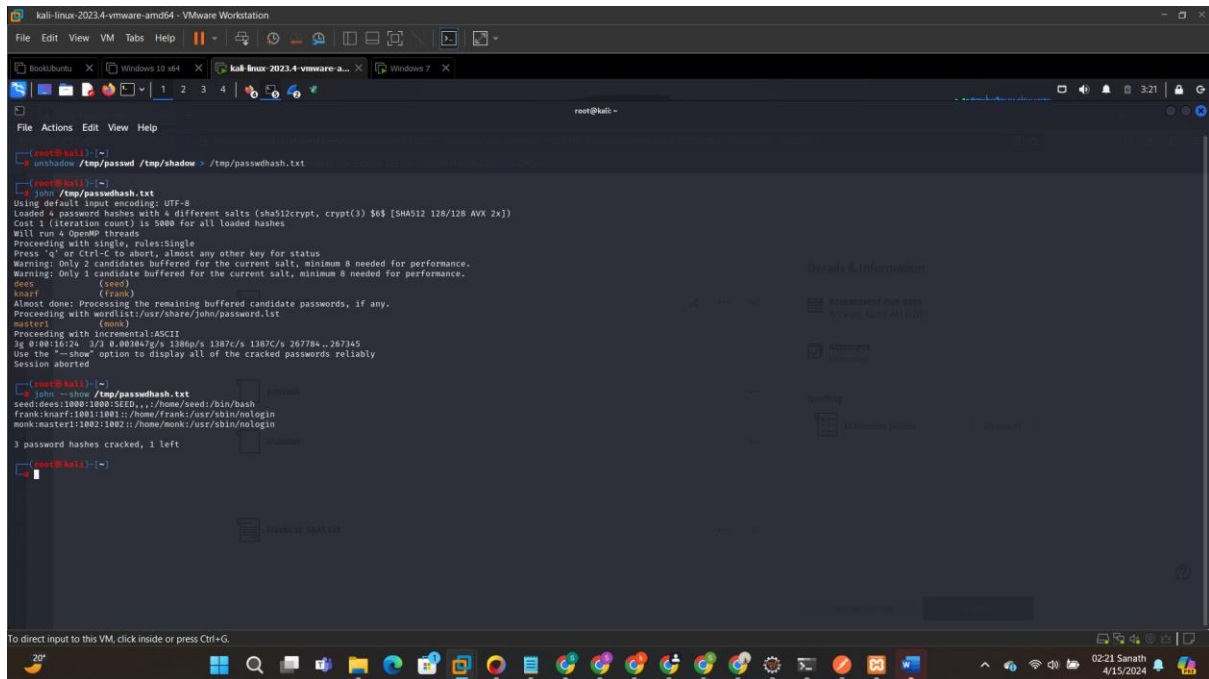


ETHICAL HACKING LAB -15

Name: Dasari Sanath Kumar

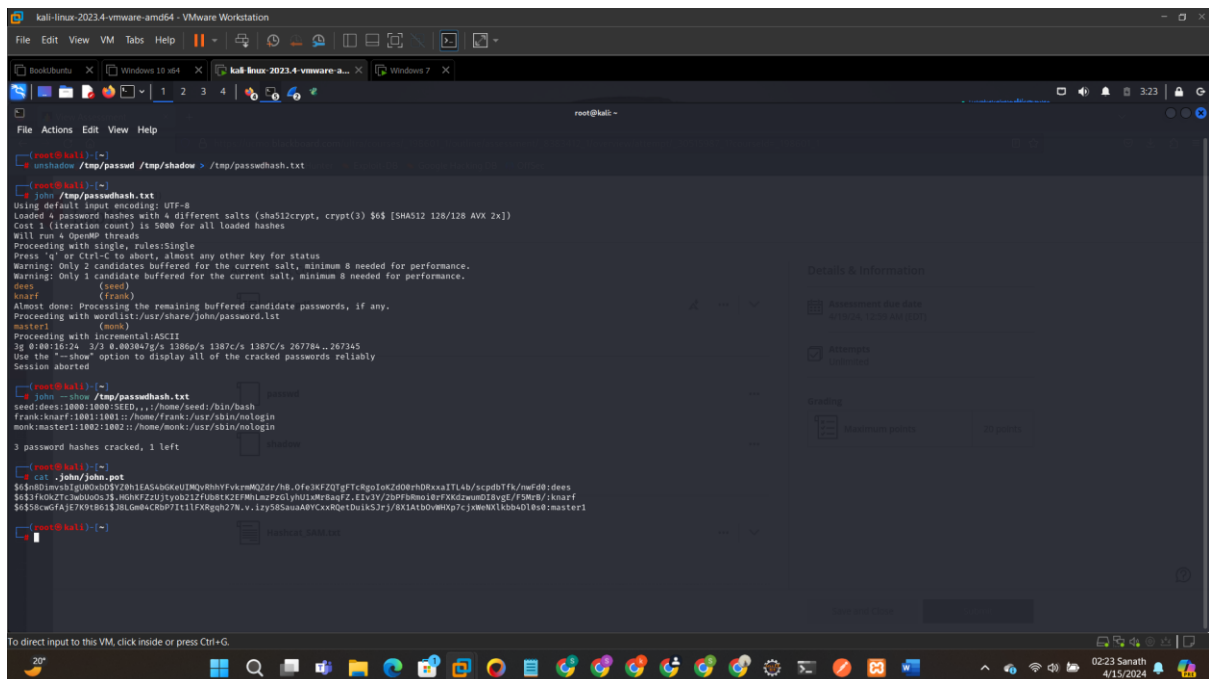
ID:- 700760349

Screenshot 1:



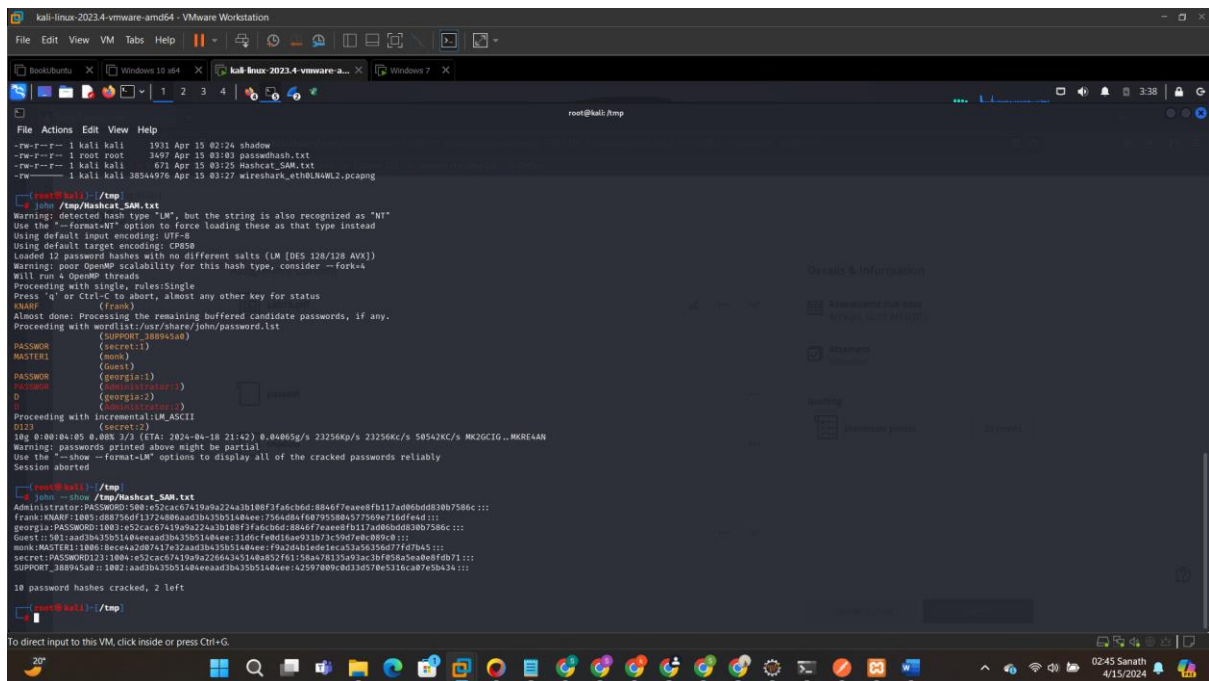
```
root@kali:~# john --show /tmp/passwd /tmp/shadow > /tmp/passwdhash.txt
root@kali:~# john /tmp/passwdhash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
dees (seed)
knarf (frank)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
master1 (monk)
Proceeding with incremental:ASCII
3g 0:00:16:24 2/3 0.003047g/s 1386p/s 1387c/s 1387C/s 267784..267345
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@kali:~# john --show /tmp/passwdhash.txt
seed:dees:1000:1000:SEED,,,/home/seed:/bin/bash
frank:knarf:1001:1001::/home/frank:/usr/sbin/nologin
monk:master1:1002:1002::/home/monk:/usr/sbin/nologin
3 password hashes cracked, 1 left
root@kali:~#
```

Screenshot 2:

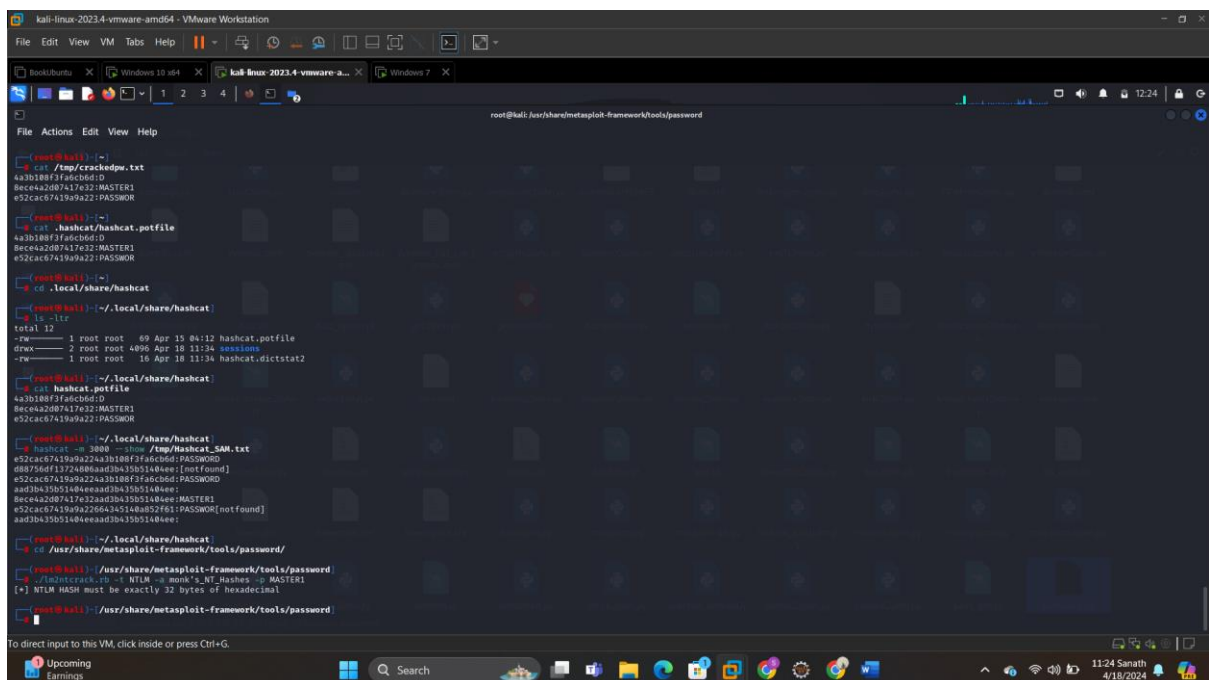


```
root@kali:~# john --show /tmp/passwd /tmp/shadow > /tmp/passwdhash.txt
root@kali:~# john /tmp/passwdhash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
dees (seed)
knarf (frank)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
master1 (monk)
Proceeding with incremental:ASCII
3g 0:00:16:24 2/3 0.003047g/s 1386p/s 1387c/s 1387C/s 267784..267345
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@kali:~# john --show /tmp/passwdhash.txt
seed:dees:1000:1000:SEED,,,/home/seed:/bin/bash
frank:knarf:1001:1001::/home/frank:/usr/sbin/nologin
monk:master1:1002:1002::/home/monk:/usr/sbin/nologin
3 password hashes cracked, 1 left
root@kali:~# cat /john/john.pot
$6$B0lmsvsh1gU0x05Y20H1EASu0kU1MqVmhYfvkwmQ2dr/hb.0F63KfZQ7gTcRgoinC2d0rpdEaxITLb/scpbTfX/nf48:dees
$6$130mZTCw0b0035:MONKzCufjy0z21fU0tKzEFMLuapZc0YH0LmW8a0Fz.1i3Yz0P0bmo18tFACzwm018gcfP0m0r/knarf
$6$58cwfAJ7K91861$38L0m4CRBP71t1FXRghq27N.v.1zy58SuuABVcxR0tDuikS3rj/8XIA1b0VM0p7cjw0NKLb040180b:master1
root@kali:~#
```

Screenshot 3:



Screenshot 4:



Screenshot 5:

