



Name : Noor Malik

Roll No : 230964

Section : BSIT-II-B

Submitted To :

Muhammad Ayaz Khan

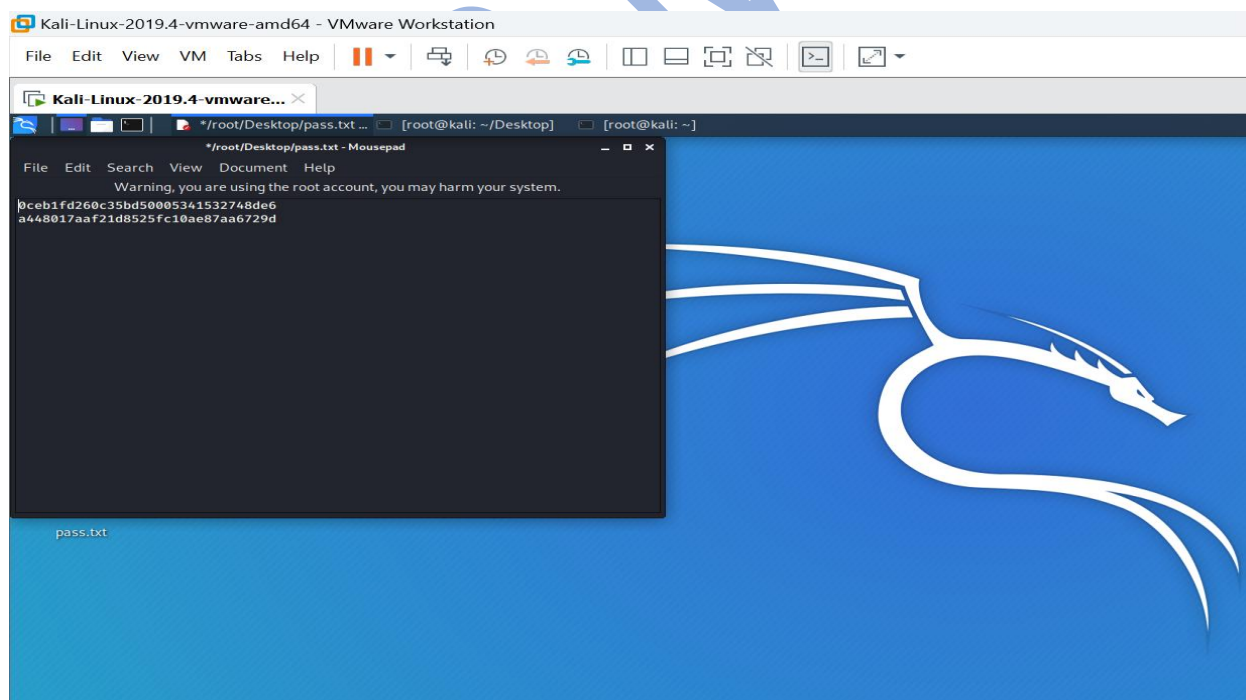
Password extracting from Hash Value

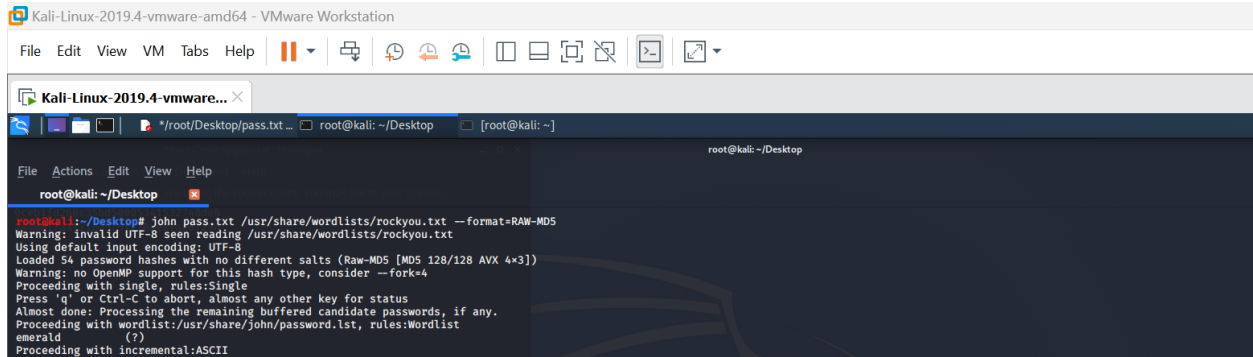
- Go To File System -> Usr->Share->Wordlists->Rockyou.Zip
- Unzip That Rockyou File.
- GO TO KALI LINUX AND OPEN TERMINAL IN DEKSTOP BY RIGHT CLICKING ON THE DESKTOP.
- Create a document named hash.txt
- Copy paste the hash values provided by your instructor.
- NOW TYPE john hash.txt /usr/share/wordlists/rockyou.txt

1 and 2

0ceb1fd260c35bd50005341532748de6
a448017aaf21d8525fc10ae87aa6729d

This also appears to be an MD5 hash, following the same 32-character hexadecimal format.

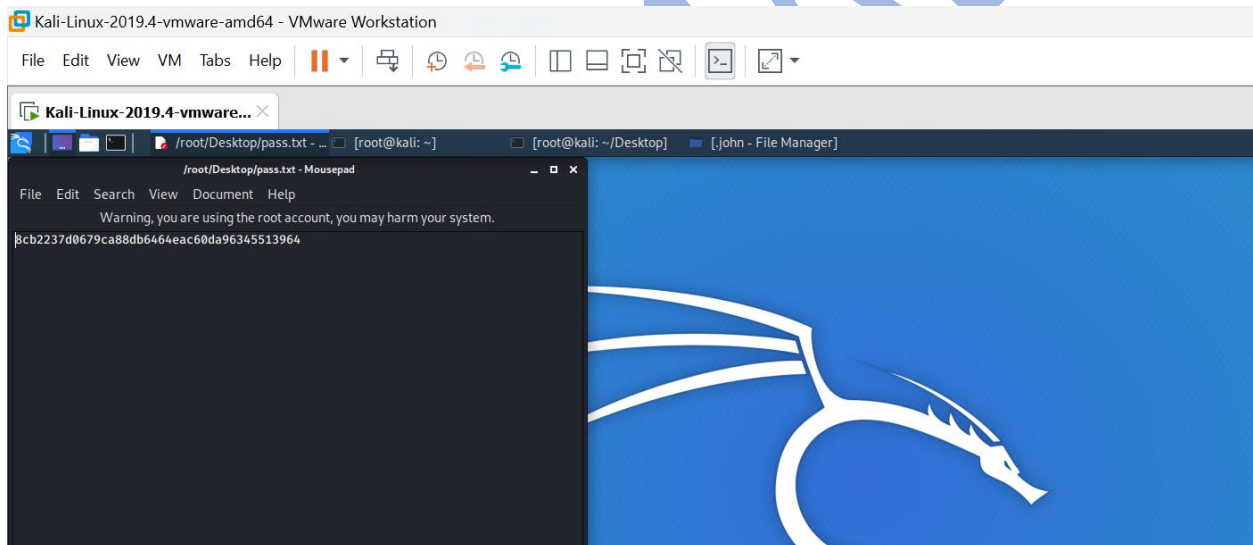




```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
* /root/Desktop/pass.txt ... root@kali: ~/Desktop [root@kali: ~]
root@kali: ~/Desktop
File Actions Edit View Help
root@kali:~/Desktop x
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=RAW-MD5
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 54 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
emerald
(?)
Proceeding with incremental:ASCII
```

3) 8cb2237d0679ca88db6464eac60da96345513964

This is a SHA-1 hash. SHA-1 produces a 40-character hexadecimal number.



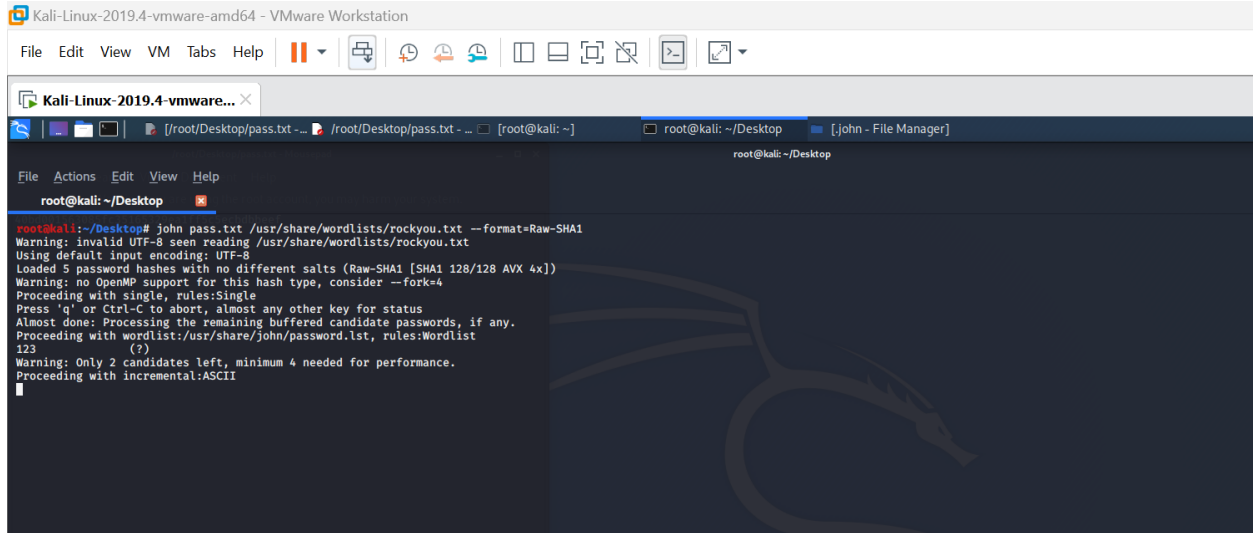
```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
/root/Desktop/pass.txt - [root@kali: ~] [root@kali: ~/Desktop] [john - File Manager]
/root/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
8cb2237d0679ca88db6464eac60da96345513964
```

```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware...
/root/Desktop/pass.txt - ... root@kali: ~ root@kali: ~/Desktop .john - File Manager
root@kali: ~/Desktop
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
12345 (?)
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
12345
```

4) 40bd001563085fc35165329ea1ff5c5ecbdbbeef

This is another SHA-1 hash, following the same 40-character format.

```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware...
/root/Desktop/pass.txt - ... /root/Desktop/pass.txt - ... [root@kali: ~] [root@kali: ~/Desktop] [john - File Manager]
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
40bd001563085fc35165329ea1ff5c5ecbdbbeef
```



Kali Linux-2019.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

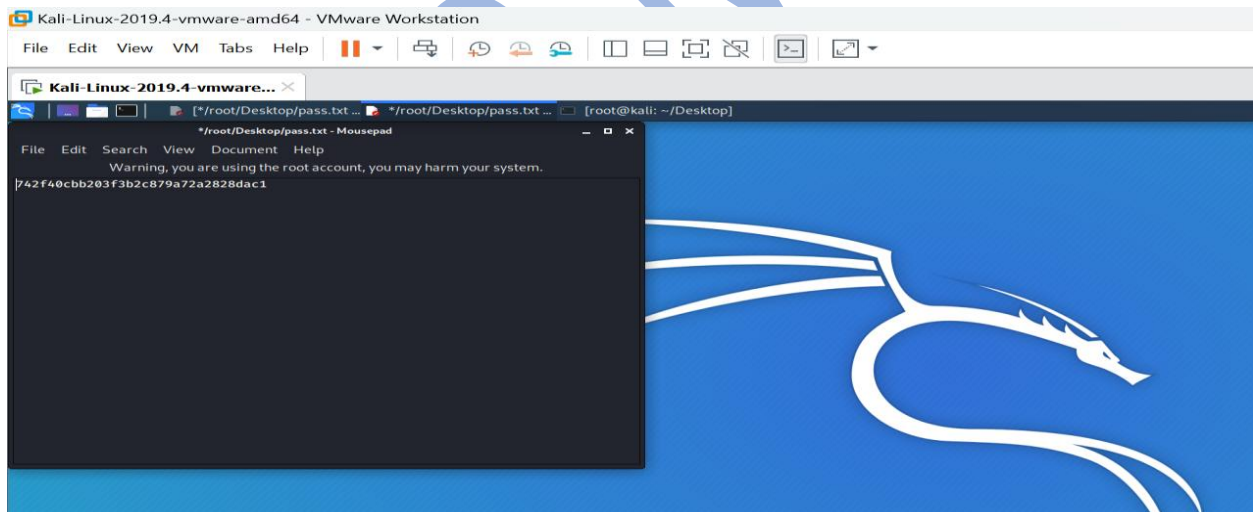
Kali Linux-2019.4-vmware... X

root@kali: ~/Desktop

```
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
123
(?)
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
```

5) 742f40cbb203f3b2c879a72a2828dac1

This is likely an MD5 hash.



Kali Linux-2019.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali Linux-2019.4-vmware... X

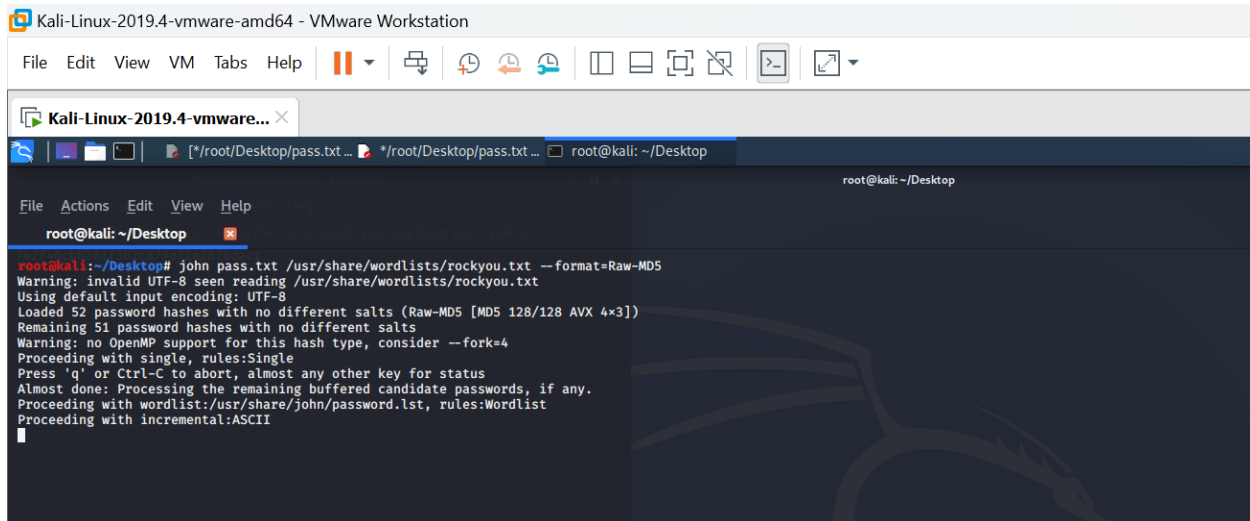
root@kali: ~/Desktop

* /root/Desktop/pass.txt - Mousepad

File Edit Search View Document Help

Warning, you are using the root account, you may harm your system.

742f40cbb203f3b2c879a72a2828dac1



Kali-Linux-2019.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali-Linux-2019.4-vmware... x

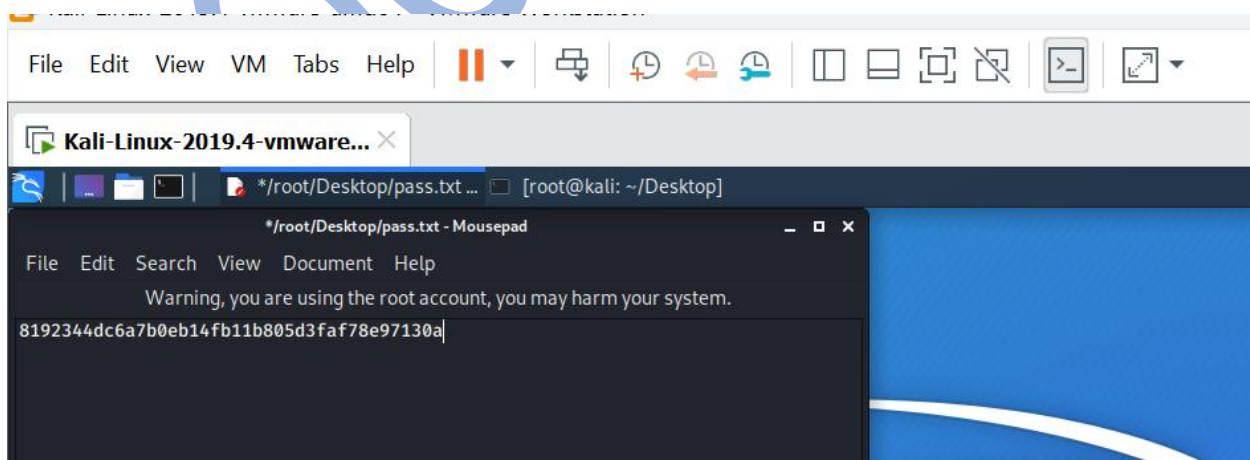
root@kali: ~/Desktop

```
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-MD5
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 52 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 51 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Proceeding with incremental:ASCII
```

The lack of displayed passwords when running `john` could be due to several reasons. The hashes in `pass.txt` might not be valid or correctly formatted MD5 hashes, and there could be encoding issues with the wordlist file. Additionally, the cracking process might still be running, as it can take time, especially with an incremental attack. Lastly, the correct passwords might not be included in the provided wordlist.

6) 8192344dc6a7b0eb14fb11b805d3faf78e97130a

This is a SHA-1 hash.



File Edit View VM Tabs Help

Kali-Linux-2019.4-vmware... x

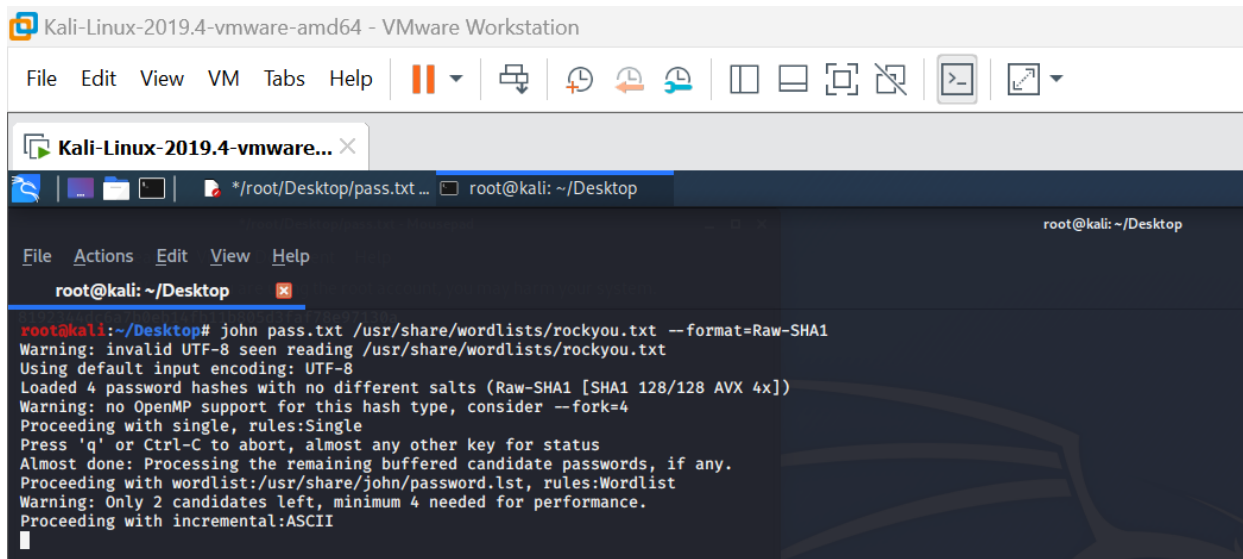
root@kali: ~/Desktop

* /root/Desktop/pass.txt - Mousepad

File Edit Search View Document Help

Warning, you are using the root account, you may harm your system.

8192344dc6a7b0eb14fb11b805d3faf78e97130a

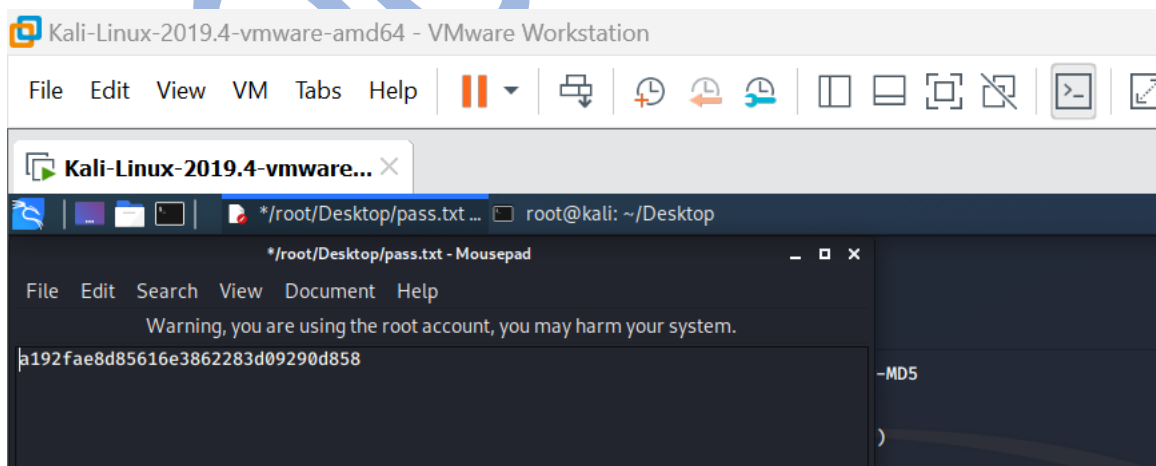


```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
*/root/Desktop/pass.txt ... root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
1
```

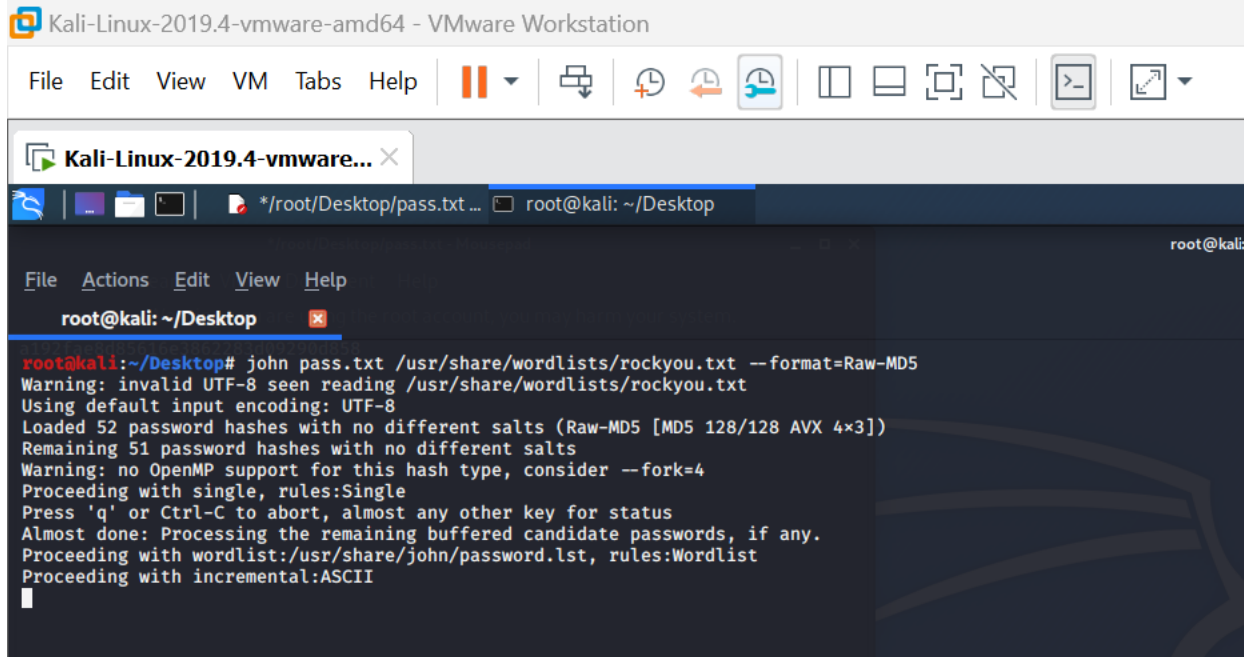
The passwords may not be showing because the hashes in `pass.txt` might not be valid or correctly formatted SHA1 hashes. The wordlist file has encoding issues, as indicated by the UTF-8 warning. The cracking process could still be running, requiring more time, especially with the incremental attack. Additionally, the correct passwords might not be present in the provided wordlist.

7) **a192fae8d85616e3862283d09290d858**

This is likely an MD5 hash.



```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
*/root/Desktop/pass.txt ... root@kali: ~/Desktop
*/root/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
a192fae8d85616e3862283d09290d858
-MD5
)
```

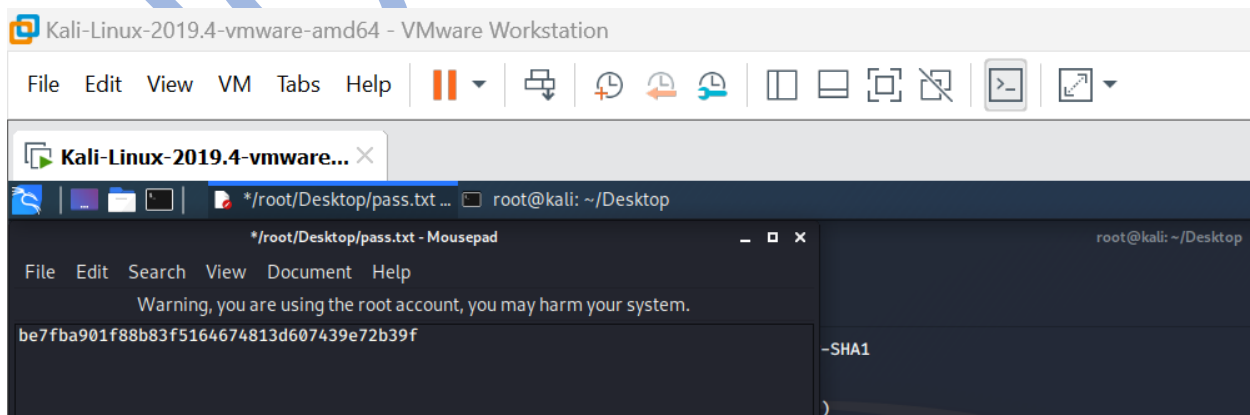


```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
/root/Desktop/pass.txt ... root@kali: ~/Desktop
root@kali: ~/Desktop
File Actions Edit View Help
root@kali: ~/Desktop x
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-MD5
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 52 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 51 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Proceeding with incremental:ASCII
█
```

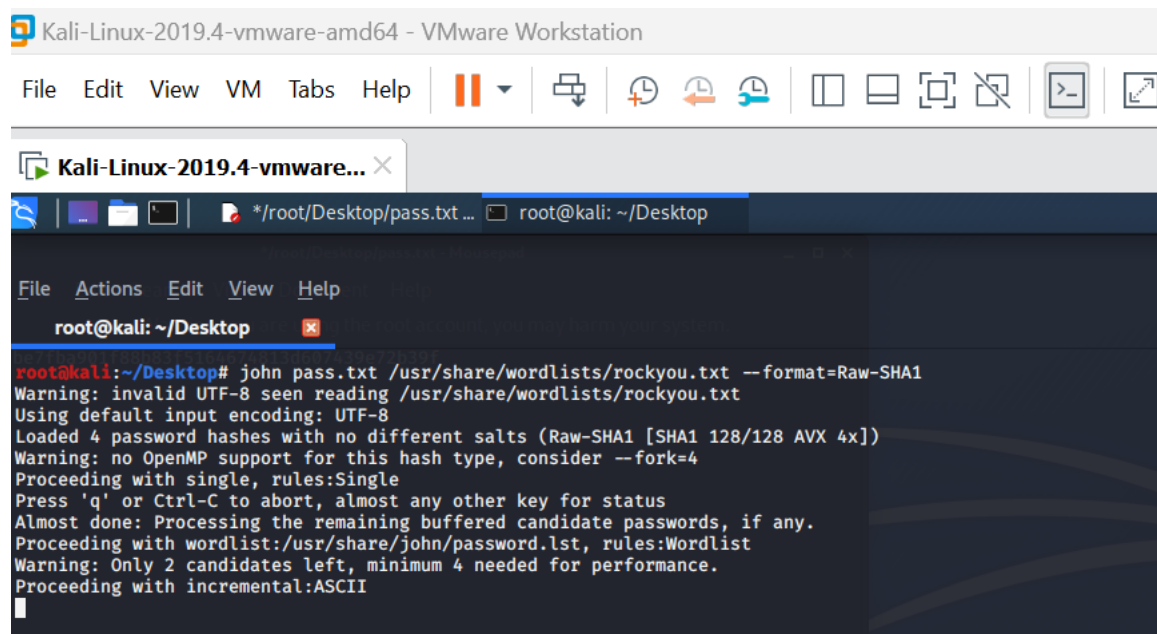
The passwords may not be showing because the `rockyou.txt` wordlist has encoding issues, as indicated by the UTF-8 warning, which could prevent `john` from reading it correctly. The cracking process might still be running, especially since it's proceeding with incremental mode, which can be time-consuming. Additionally, the correct passwords might not be present in the provided wordlists, causing `john` to continue without finding matches.

8) **be7fba901f88b83f5164674813d607439e72b39f**

This is a SHA-1 hash.



```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
/root/Desktop/pass.txt ... root@kali: ~/Desktop
*root/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
be7fba901f88b83f5164674813d607439e72b39f
-SHA1
)
```

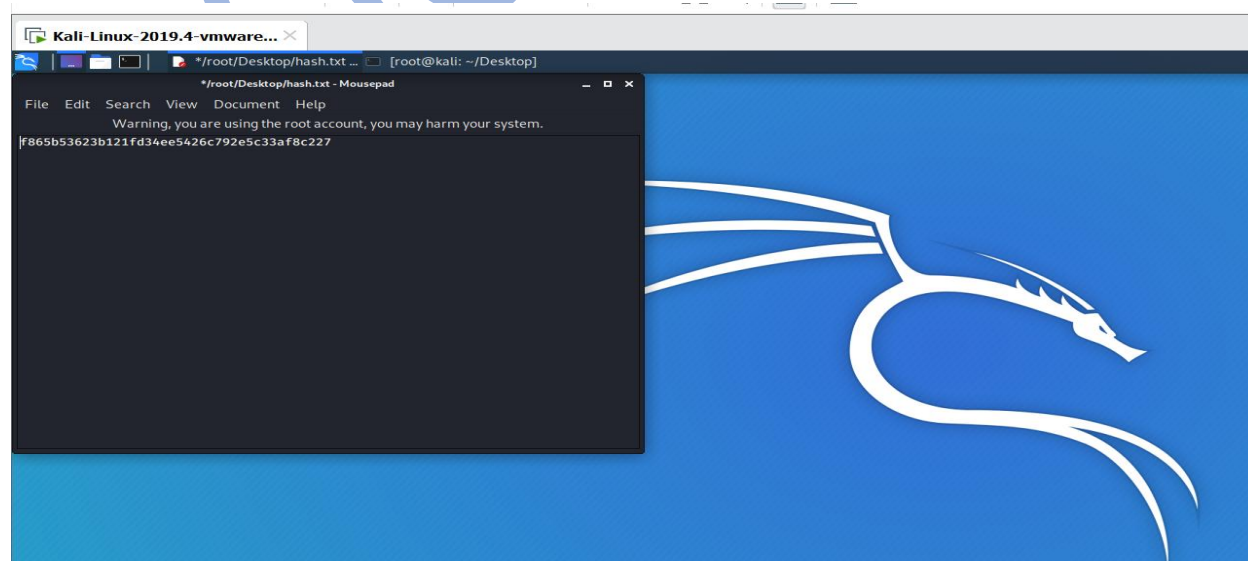
The screenshot shows a Kali Linux terminal window titled "Kali-Linux-2019.4-vmware-amd64 - VMware Workstation". The terminal is running the command `john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1`. The output shows a warning about invalid UTF-8 encoding, followed by the loading of 4 password hashes. The terminal is currently processing the hashes, and the user is prompted to press 'q' or Ctrl-C to abort.

```
root@kali: ~/Desktop
File Actions Edit View Help
root@kali: ~/Desktop
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
█
```

The passwords might not be showing because the `rockyou.txt` wordlist has encoding issues, as indicated by the UTF-8 warning, which can prevent `john` from reading it correctly. Additionally, the incremental mode is time-consuming and may still be running, processing potential password candidates. The correct passwords may also not be present in the provided wordlists, causing `john` to continue without finding matches. Lastly, the warning about needing more candidates for performance suggests that the process may not be running optimally.

9) f865b53623b121fd34ee5426c792e5c33af8c227

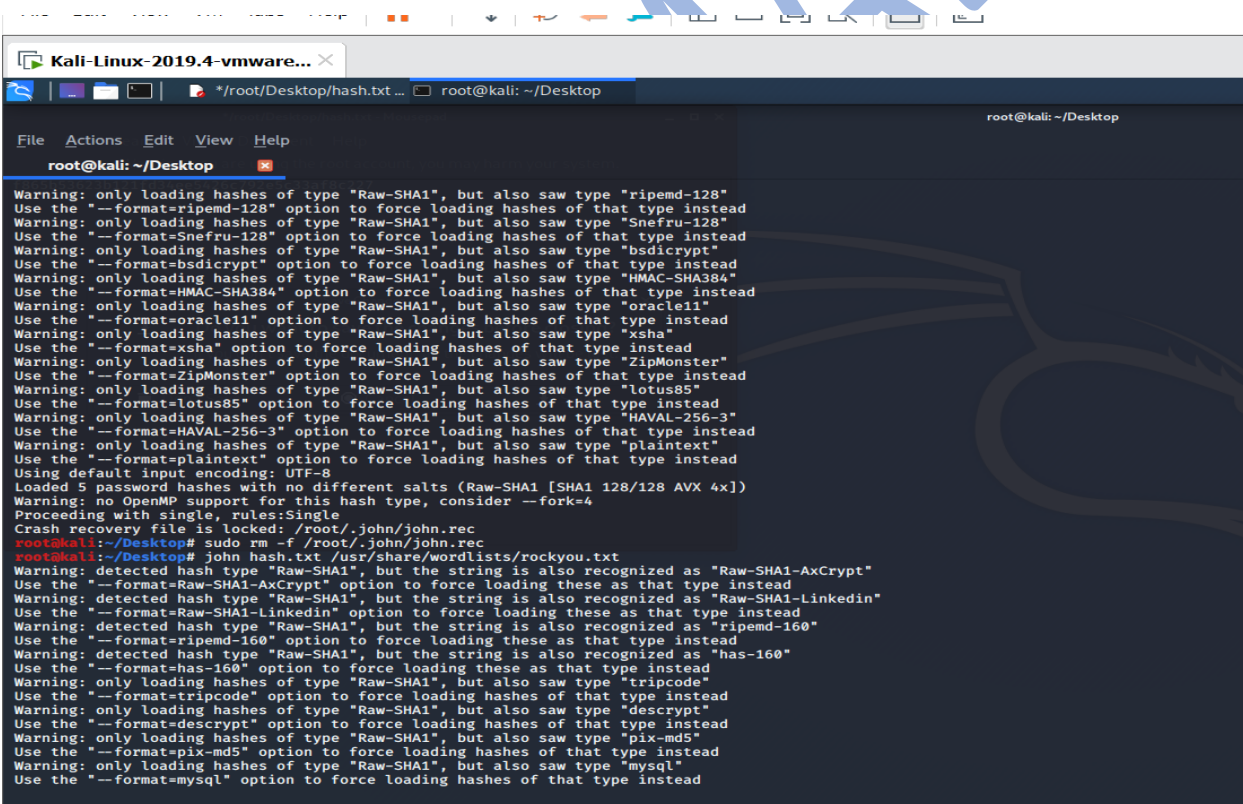
This is another SHA-1 hash.



```

root@kali: ~/Desktop# john hash.txt /usr/share/wordlists/rockyou.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-LinkedIn"
Use the "--format=Raw-SHA1-LinkedIn" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "tripcode"
Use the "--format=tripcode" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "pix-md5"
Use the "--format=pix-md5" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "mysql"
Use the "--format=mysql" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "oracle"
Use the "--format=oracle" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "bfegg"
Use the "--format=bfegg" option to force loading hashes of that type instead
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "Raw-SHA1", but also saw type "dynamic-md5($p)"
Use the "--format=dynamic-md5($p)" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Raw-SHA256"
Use the "--format=Raw-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "HMAC-SHA256"

```



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

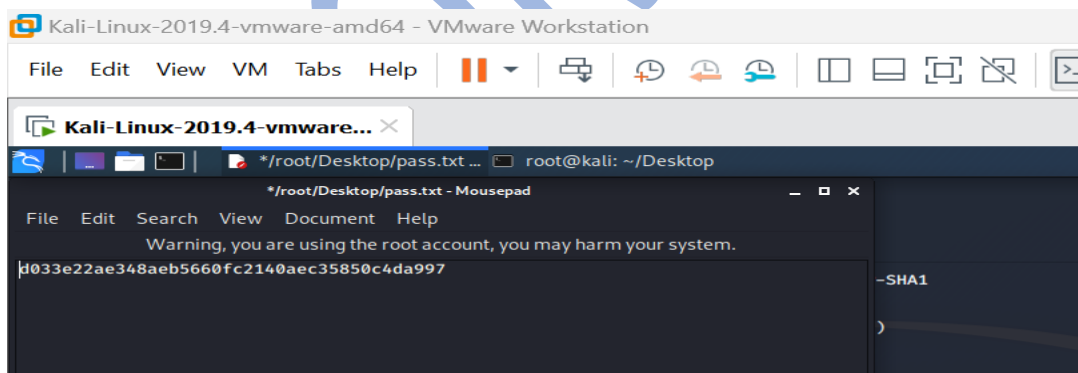
```

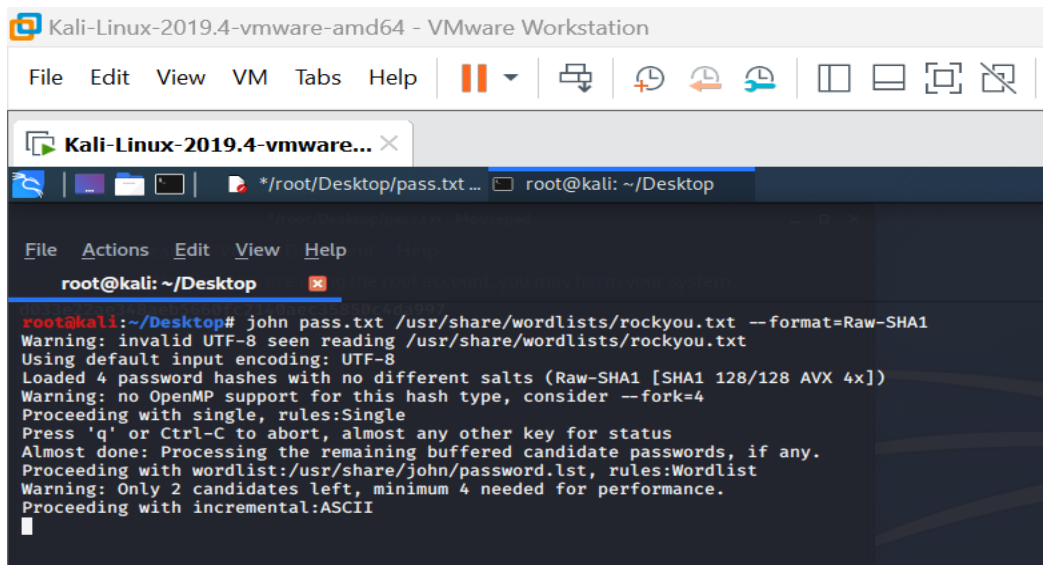
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "hMailServer"
Use the "--format=hMailServer" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "gost"
Use the "--format=gost" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "ripemd-128"
Use the "--format=ripemd-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "Snefru-128"
Use the "--format=Snefru-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "bsdicrypt"
Use the "--format=bsdicrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "HMAC-SHA384"
Use the "--format=HMAC-SHA384" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "oracle11"
Use the "--format=oracle11" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "xsha"
Use the "--format=xsha" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "ZipMonster"
Use the "--format=ZipMonster" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "lotus85"
Use the "--format=lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "HAVAL-256-3"
Use the "--format=HAVAL-256-3" option to force loading hashes of that type instead
Warning: only loading hashes of type "Raw-SHA1", but also saw type "plaintext"
Use the "--format=plaintext" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
admin123
(?)

```

10) d033e22ae348aeb5660fc2140aec35850c4da997

This is a SHA-1 hash.



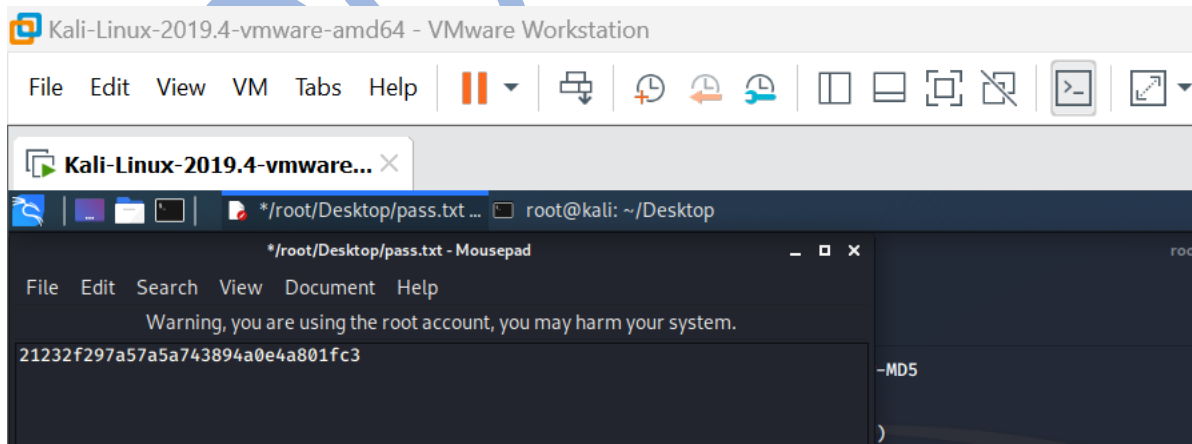


```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
*/root/Desktop/pass.txt ... root@kali: ~/Desktop
File Actions Edit View Help
root@kali: ~/Desktop
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-SHA1
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Warning: Only 2 candidates left, minimum 4 needed for performance.
Proceeding with incremental:ASCII
█
```

The passwords might not be showing because the `rockyou.txt` wordlist has encoding issues, as indicated by the UTF-8 warning, which can prevent `john` from reading it correctly. Additionally, the incremental mode is time-consuming and may still be running, processing potential password candidates. The correct passwords may also not be present in the provided wordlists, causing `john` to continue without finding matches. Lastly, the warning about needing more candidates for performance suggests that the process may not be running optimally.

11) 21232f297a57a5a743894a0e4a801fc3

This is likely an MD5 hash.



```
Kali-Linux-2019.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware... x
*/root/Desktop/pass.txt ... root@kali: ~/Desktop
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
21232f297a57a5a743894a0e4a801fc3
-MD5
)
```


Kali-Linux-2019.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali-Linux-2019.4-vmware... X

*/root/Desktop/pass.txt ... root@kali: ~/Desktop

File Actions Edit View Help

root@kali: ~/Desktop

```
root@kali:~/Desktop# john pass.txt /usr/share/wordlists/rockyou.txt --format=Raw-MD5
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 52 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 51 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
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, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:04 3/3 0g/s 3514Kp/s 3514Kc/s 179242Kc/s kc6g51..samamoooh
```

NOOR MALIK