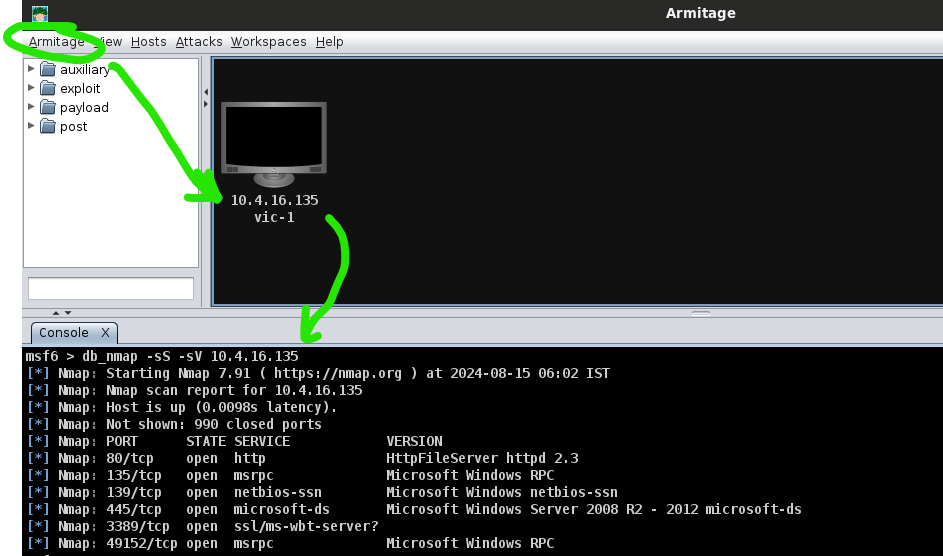
Big Armitage demo:

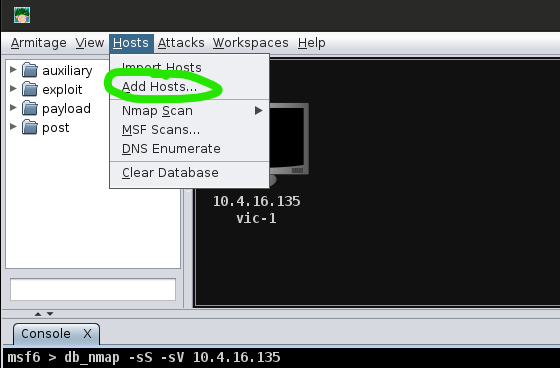
1 open up Armitage, then set up a host. In this case, we have 10.4.16.135.

Under the top nav-bar, “hosts” will have a dropdown letting you make a new one.

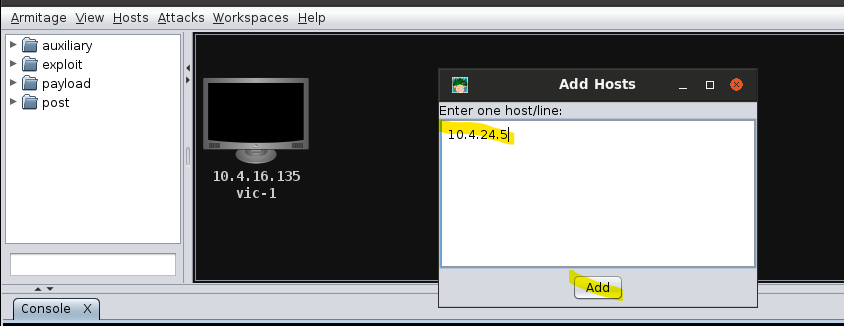
Then, to the nmap scan thing from within msfconsole as shown in the console



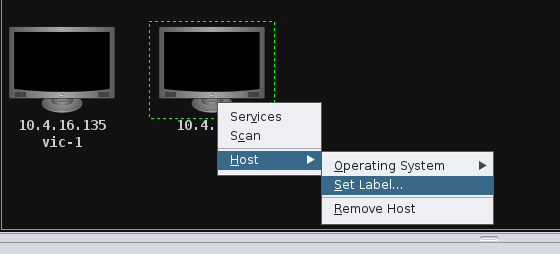
Showing how to add hosts



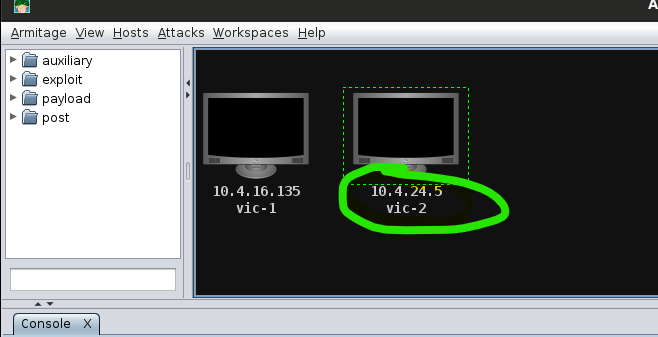
Example of adding a second host.



I can right-click and give it a name too, like how the one on the left is called “vic-1”

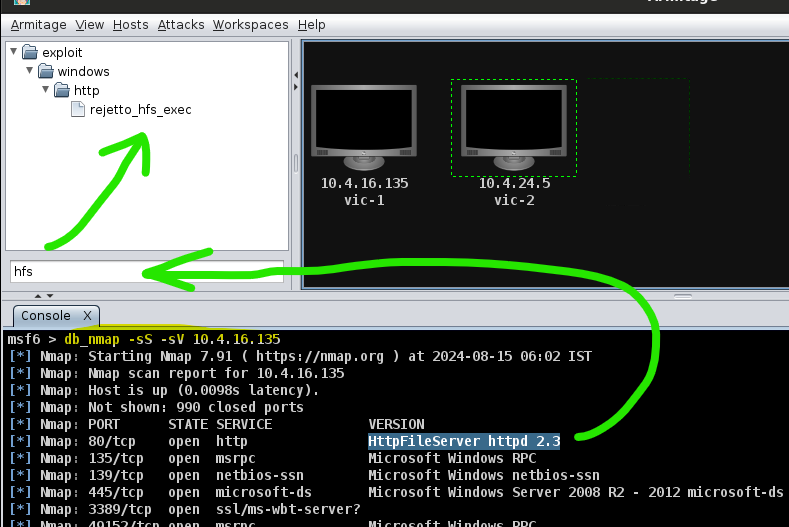


Showing the name change to vic-2 for the new host

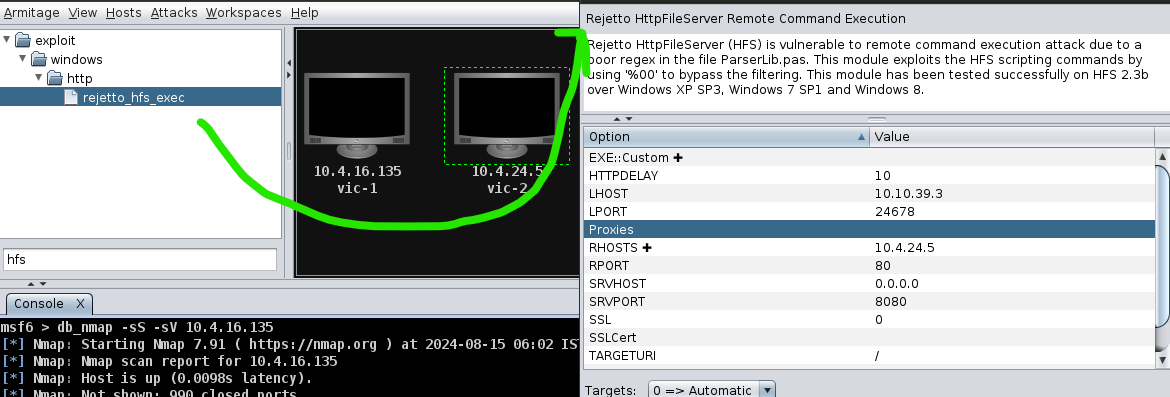


Looking at the results of the db\_nmap scan,we see http file server running.

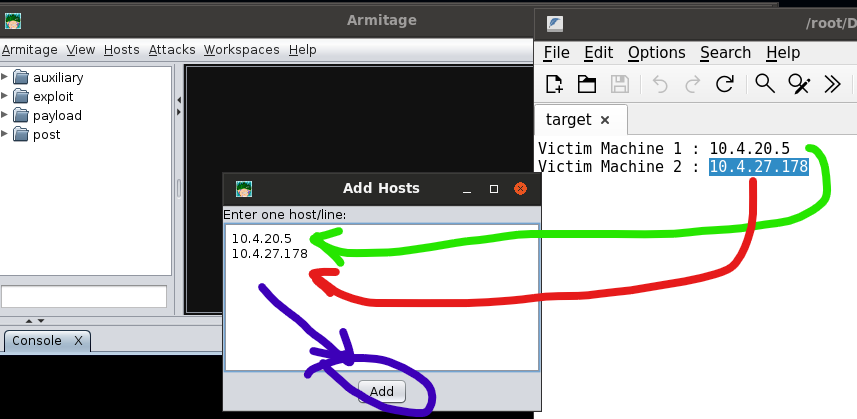
The keyword “hfs” gives us the rejetto exploit we can use for this situation.

…

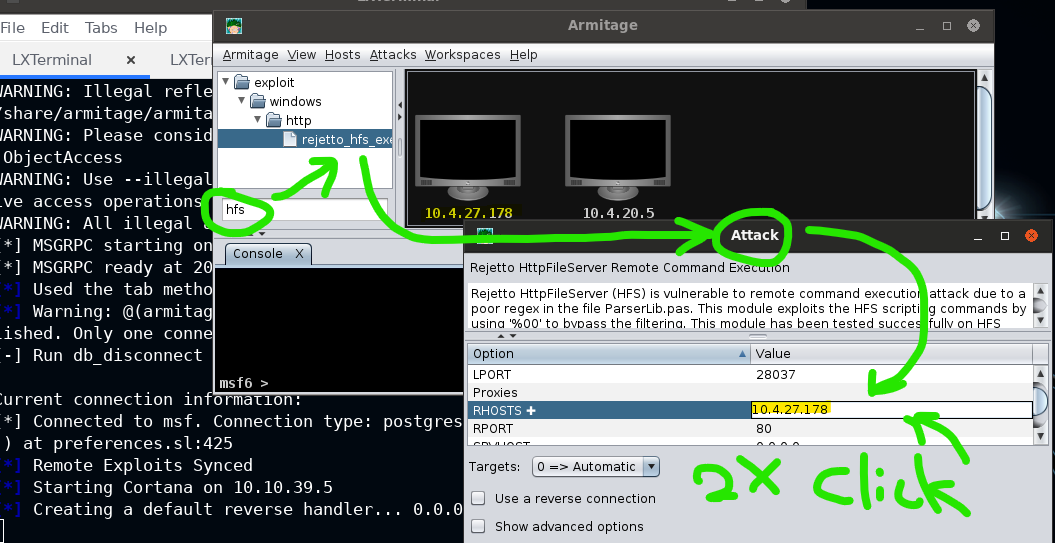
Double click to open up details, then within the options we can set the values.



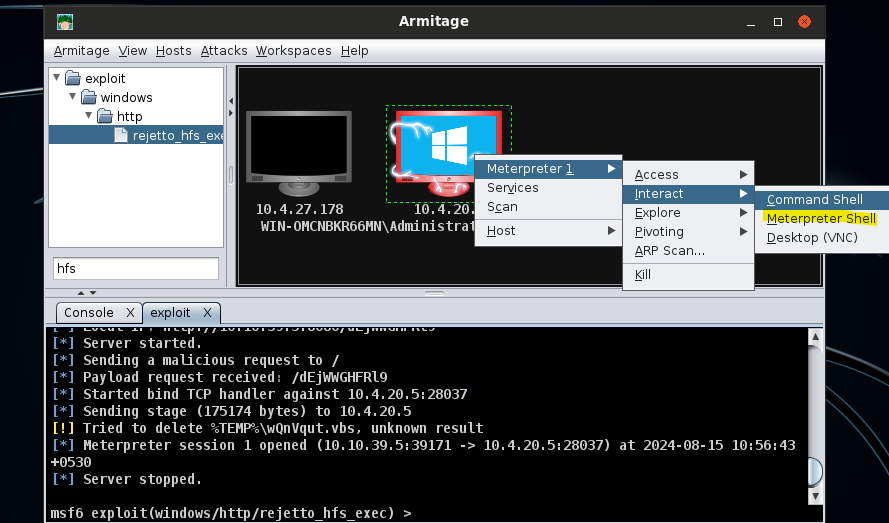
I had to re-set up the lab, so here’s another way to add multiple hosts at once for when I re-booted Armitage to complete the exercise



Double clicking on the value field in the attack window lets you edit values

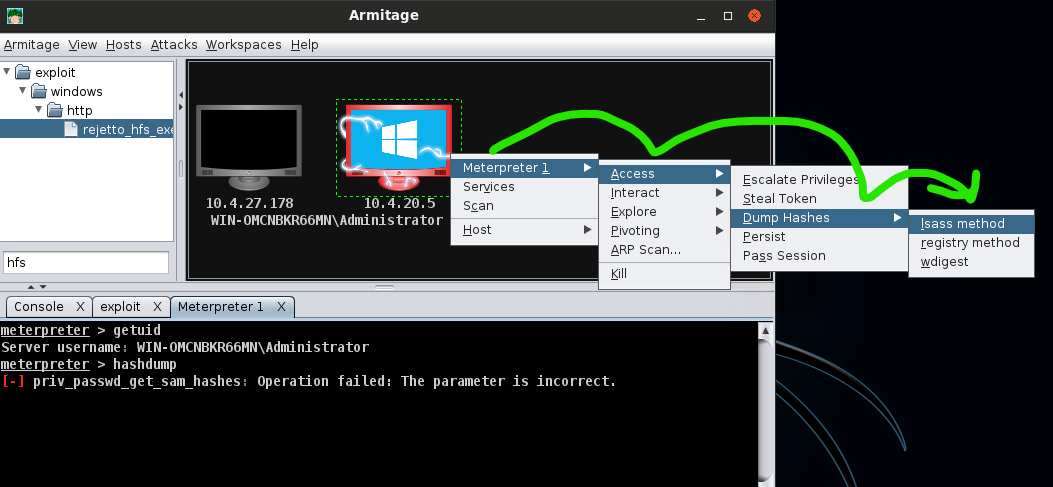


After setting the rhost to the target, we run the program. When an exploit has worked on a system, we see the icon change. Here, it has the windows logo because we know it’s running windows as an OS.



In the following dropdown structure you can see how hash-dumps can get obtained.

Meterpreter > access > dump hashes > (choose a method)

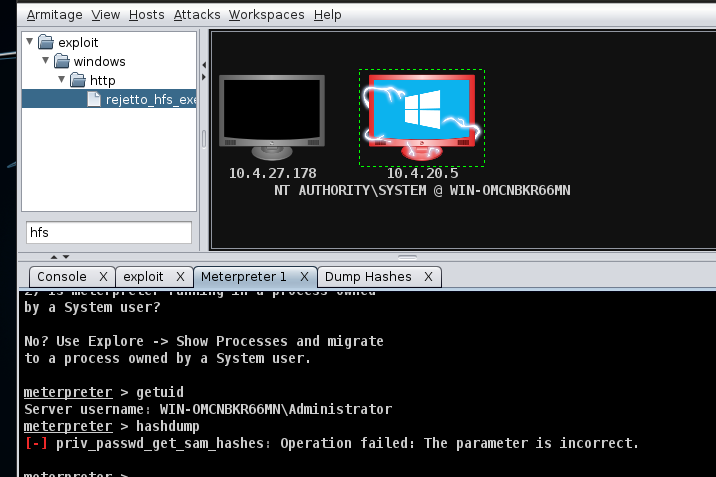


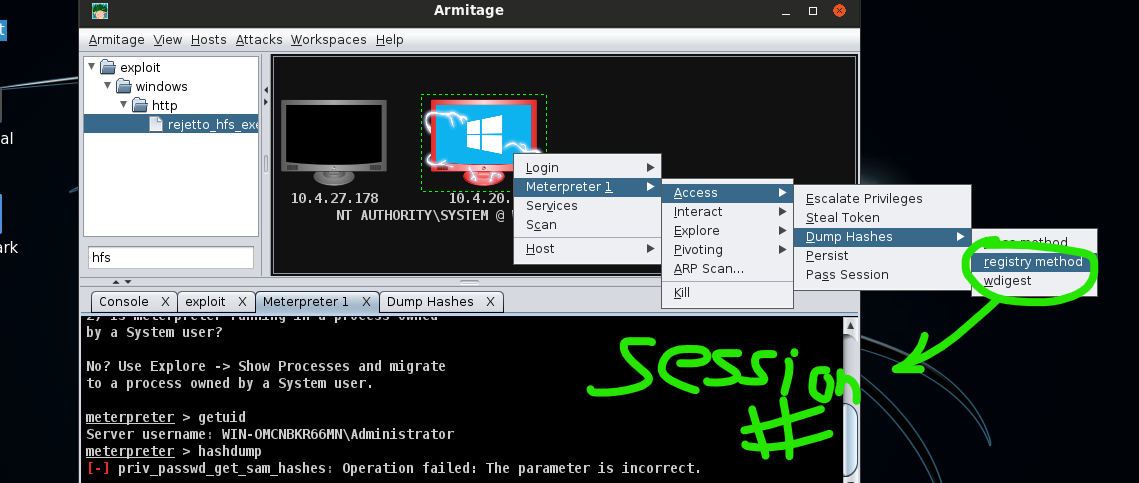
The above lsass method is like, from cli, doing

Find process ps lsass.exe, then migrate to process #.

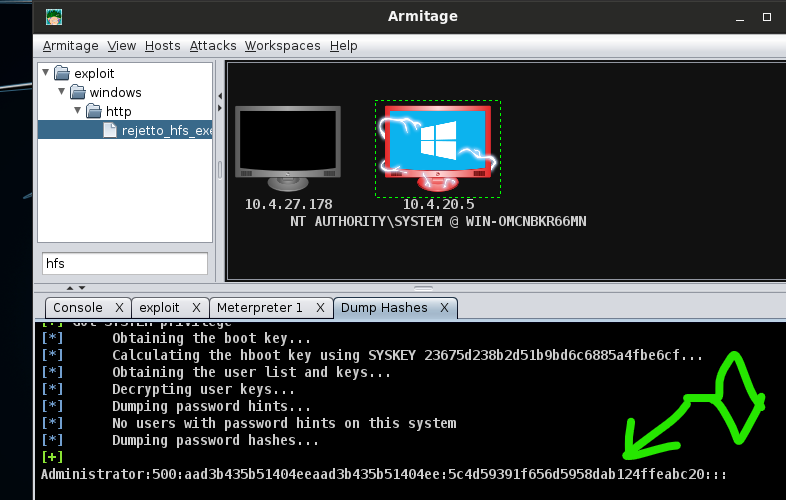
Then running hashdump in meterpreter.

Below, we see that the lsass method failed

.

Easy to continue on, let’s try the registry method to get some hasdump info

After running the registry method hashdump, we get the admin’s hash



Remember, the password data is after the : (meaning it’s the second ridiculous string of letters and numbers found there.)