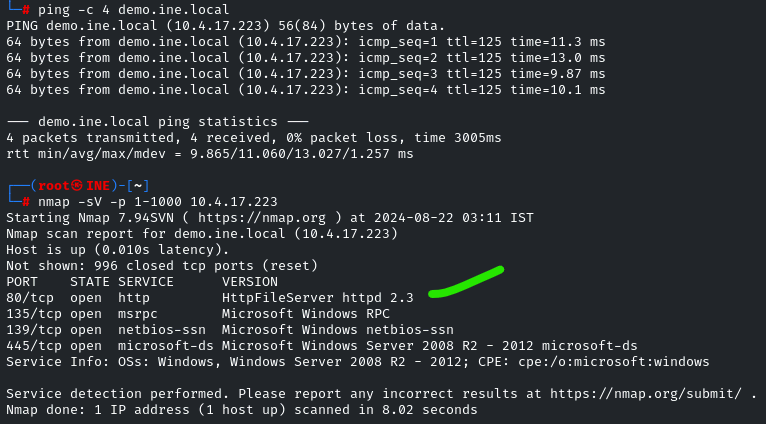
Basic ping to test target, then scan the first 1k ports.

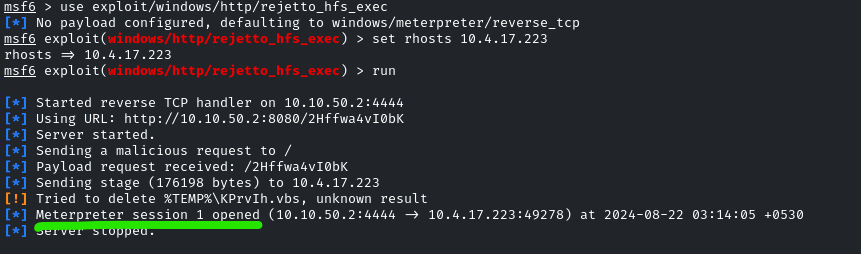
We’re tasked with looking at port 80 here and messing with it.



Magic your way into associating the exploit rejetto hfs exec with httpFileServer httpd 2.3

Set the rhosts and run it.

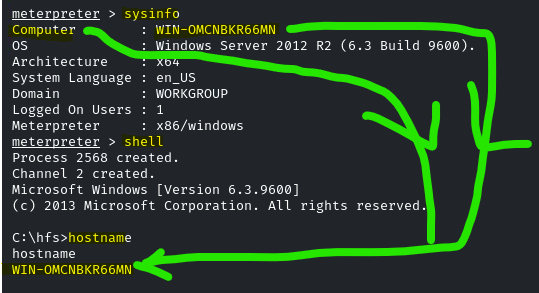
We get a meterpreter session



Expand on sysinfo… we see the computer name is the same as the shell’s return for the command: hostname

Note the same WIN- … item

This is just a matter of info, not really expanded on in the lab.



Our target is getting hotfix information which we can also find from this console, so that’s done

The witchcraft command: wmic qfe list full

Tells me all the hotfixes. This is a similar screencap from a more comprehensive command too.

