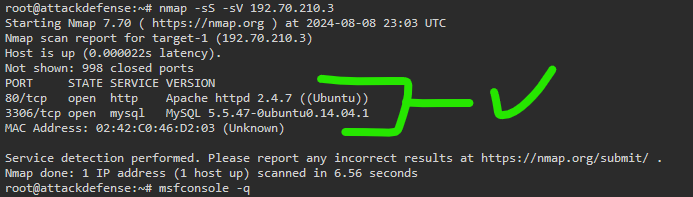
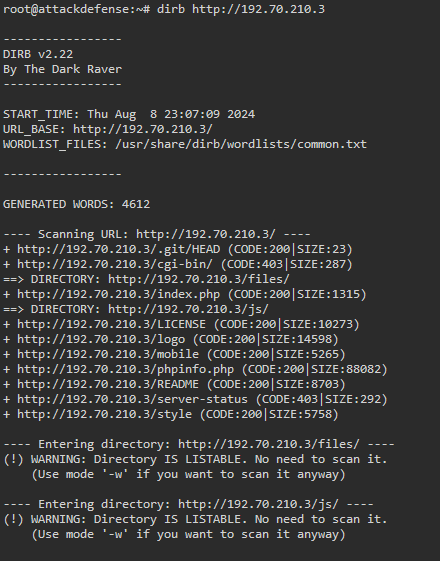
Start with a stealh service version nmap scan on the target

It’s running some kind of apache 247 plus mySQL. Note this junk for later.



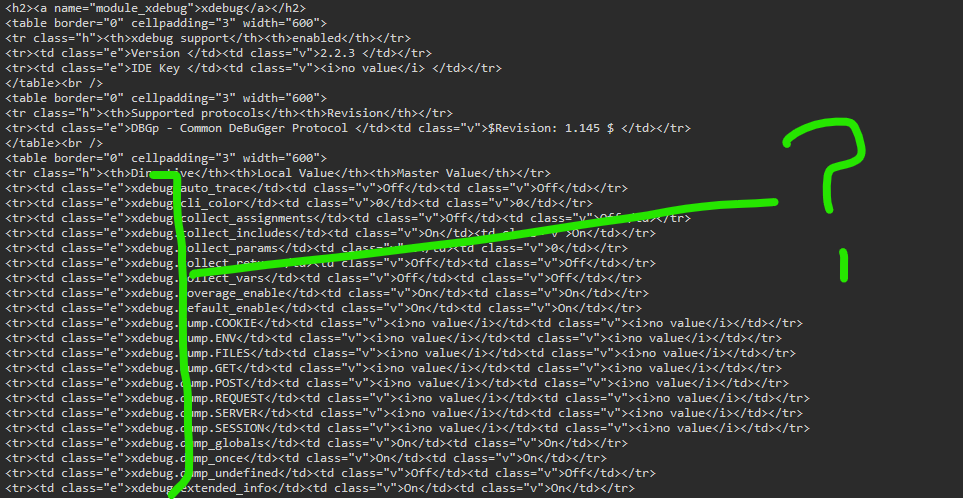
Since port 80 is open, run dirb to enumerate the directories on the target url (in this case, that’s the ip address that’s running the http port 80)



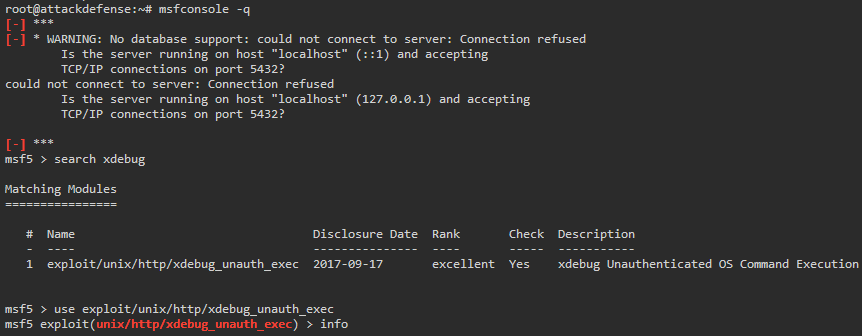
…

Inside the HTML we see xdebug.

Magic your way into noticing this and knowing it’s an attack vector.

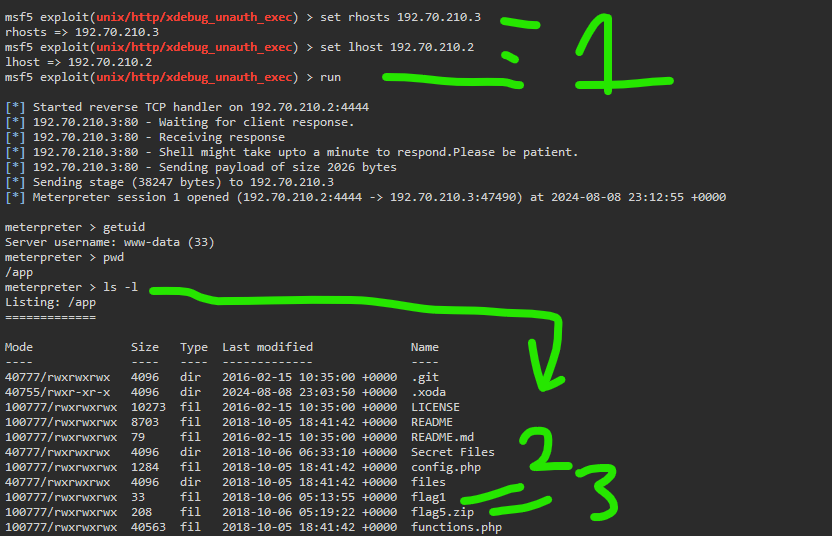


Start up msfconsole and search for the keyword from the funny html tag



Check out the info, then set the rhost to the target and an lhost to a machine you control as the listener to get a response back. This needs a listerner to establish the reverse tcp with.

It opens up meterpreter, so we can navigate and find a couple of flags.



Can download flag5 by using command : get flag5.zip and then opening it on your own machine. This should be sandboxed, but that’s not demonstrated by these garbage labs.