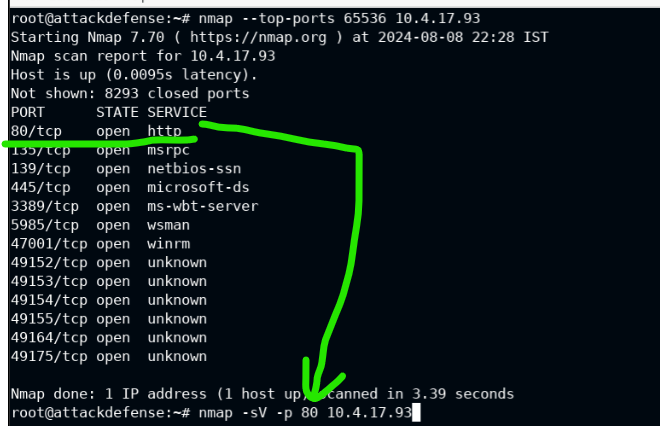
Start with a basic scan, noticing that port 80 is open

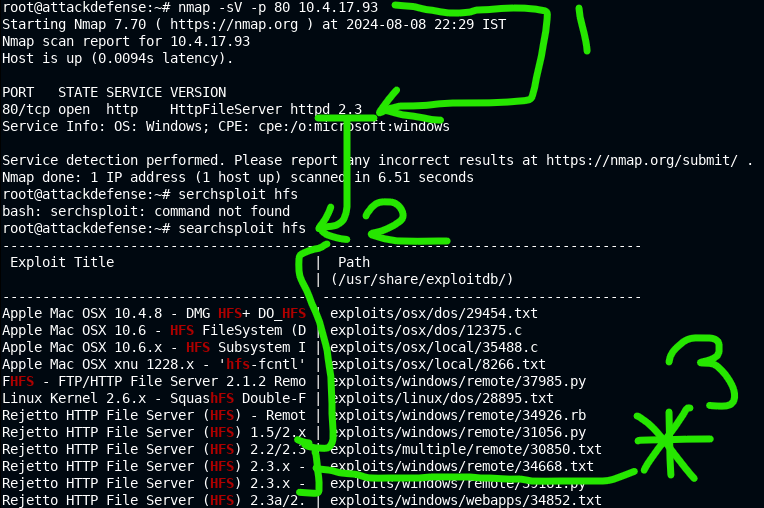
Specifically scan what version is on that port.

(kind of lame since the first scan should probably have been -sV, though yes, it would take longer)

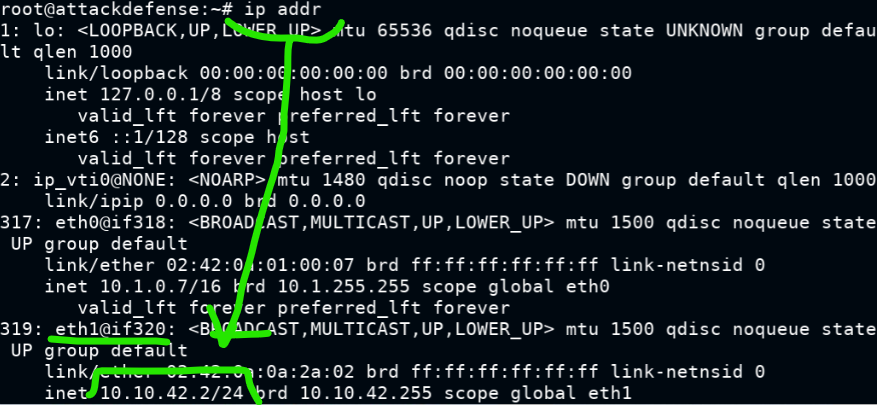


http file server httpf 2.3 is revealed, so we search for hfs relating to this number

\*http file server = HFS – you must memorize this

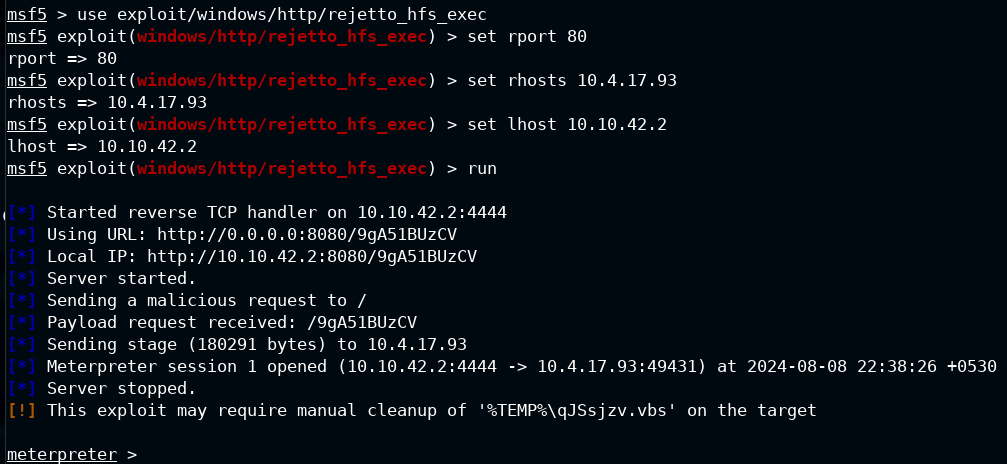


You need to set up a listener on my current machine, so in this environment we check it with ip addr. Unclear how this is the address, like it’s not clear why eth1@if is the thing we’re looking for, but just pull yourself up by the bootstraps, right?



Exploit then gets set up, using out address as lhost.

Command : use exploit/windows/http/rejetto\_hfs\_exec



That’s a meterpreter session, and a simple bit of navigation to the flag.

