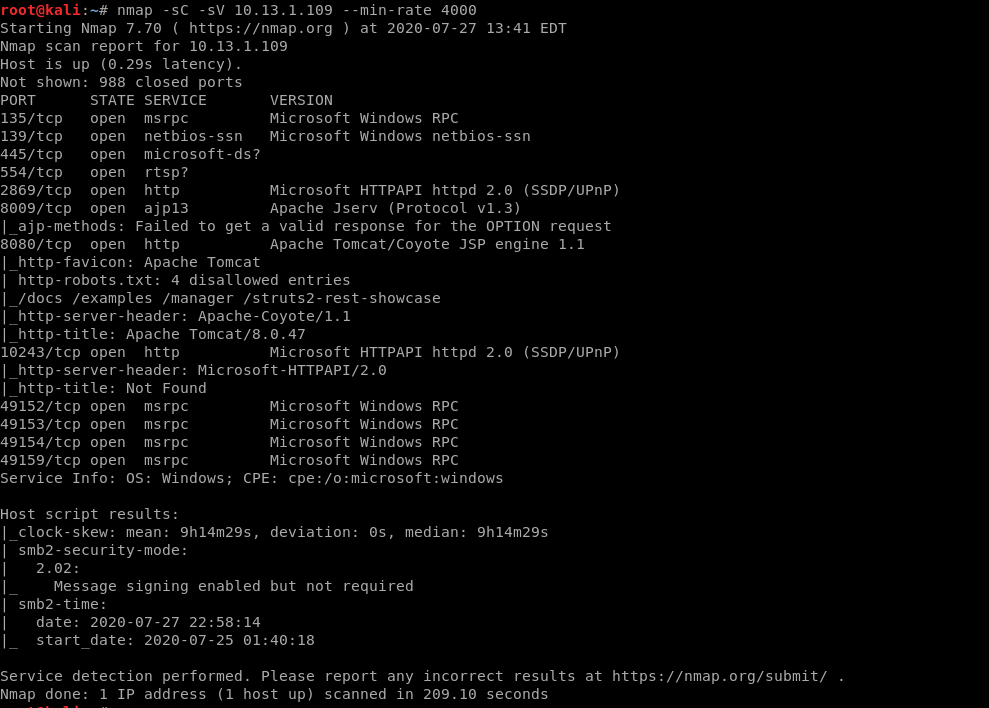
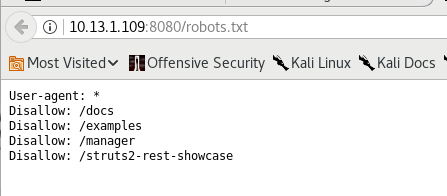
AS45(10.13.1.109)-GhostIA

Sarah Ferenczi

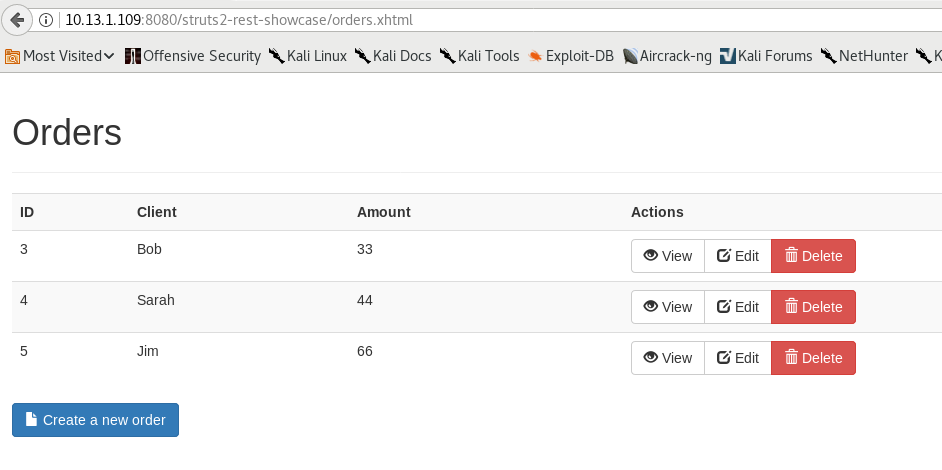
Enumeration



First, we run an nmap scan on the machine. Notice how port 8080 is open.

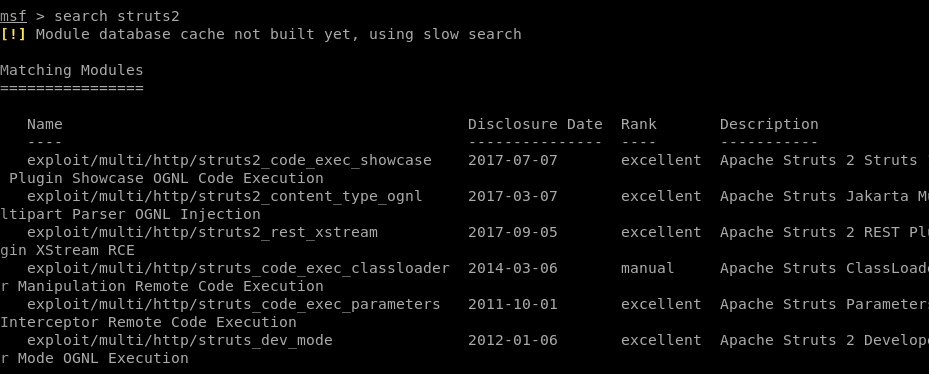


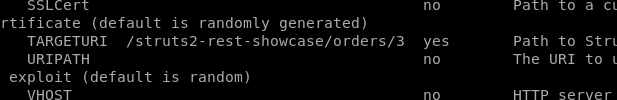
In the scan, it said robots.txt was still open. If we navigate to the other pages, we do not have access.



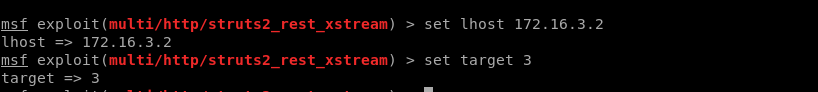
Now that we know that it’s using apache struts, we can go ahead and look for exploits

Exploitation

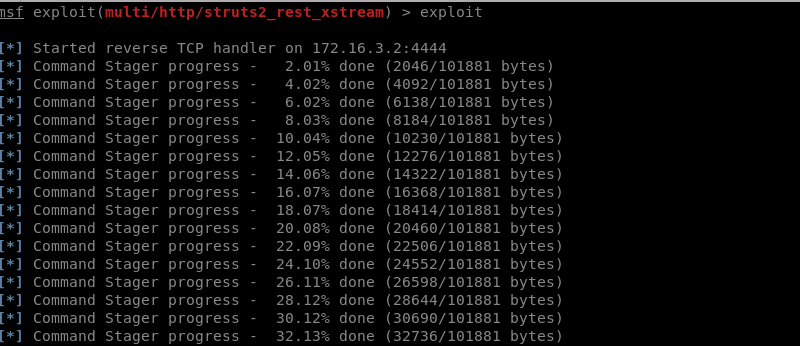




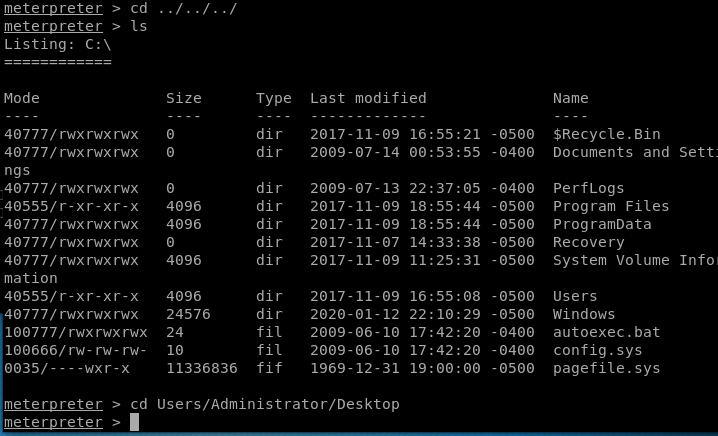
Let’s search up all exploits. I chose to use rest\_xstream due to the uri being used.



We then change the settings to Windows.



Then exploit.



Then go to the directory and get the flag.

