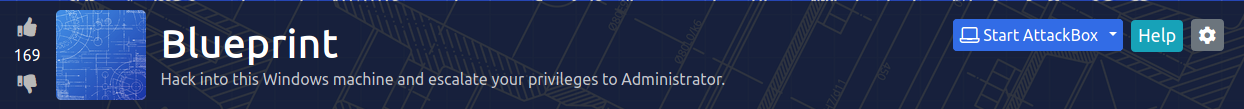
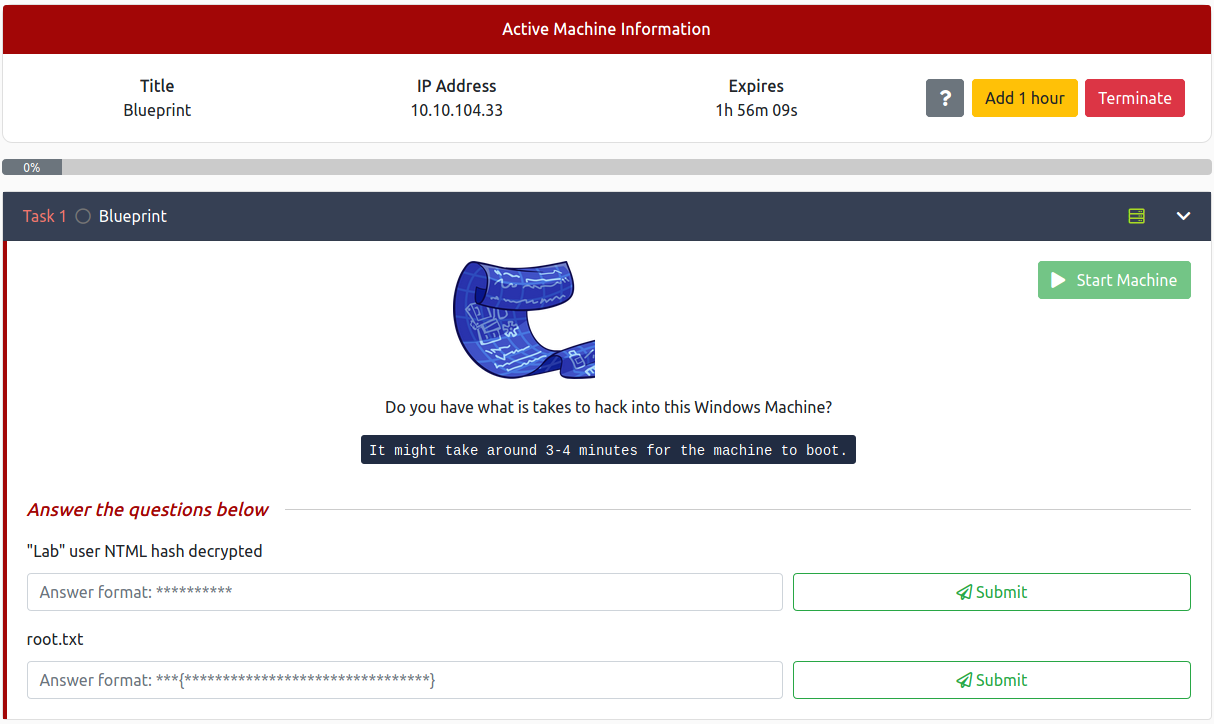
**Blueprint write-up**

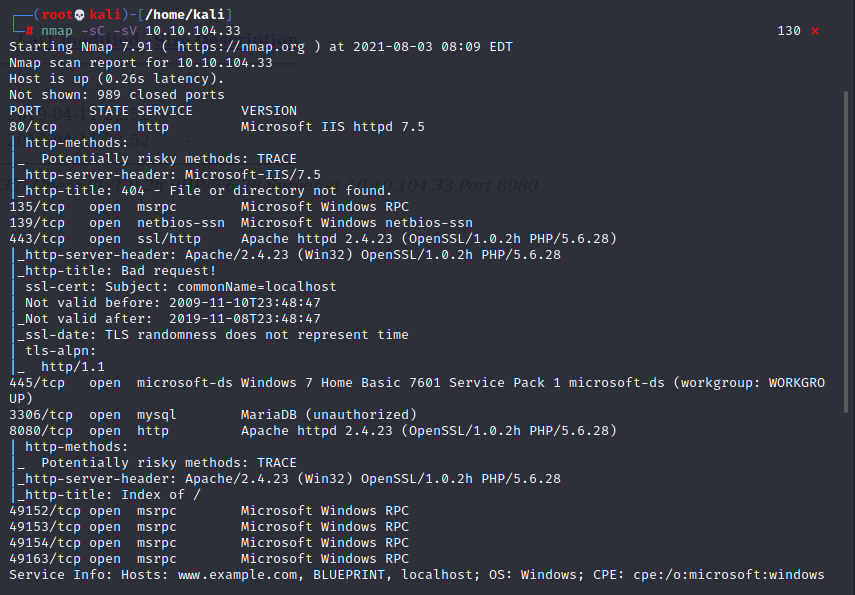
This write-up is for Blueprint room of TryHackMe which will focus on hacking Windows machine and elevate our privilege to Administrator

Site: <https://tryhackme.com/room/blueprint>

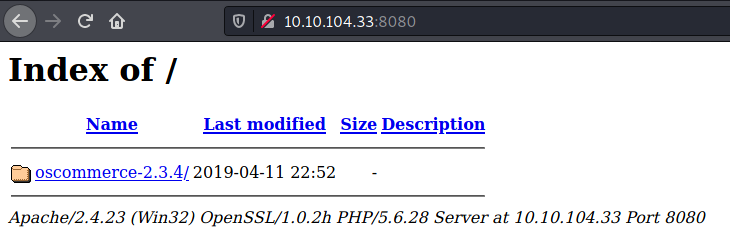




Always start with nmap to recon how many ports that target using and which services of each ports



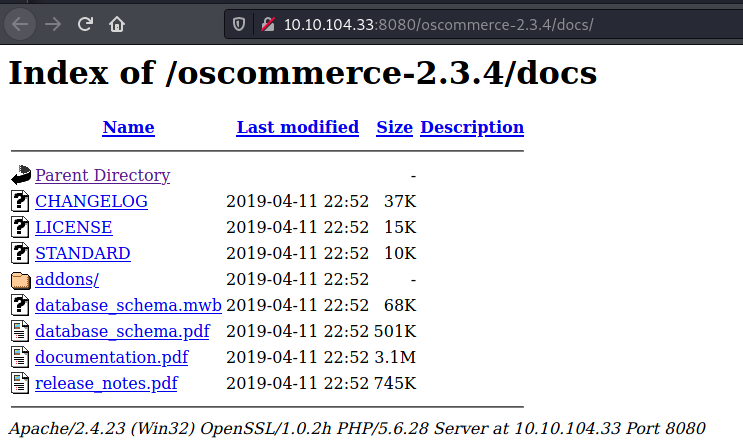
Look like we have port 8080 for http server let’s jump right it, and here I think its under-construct website



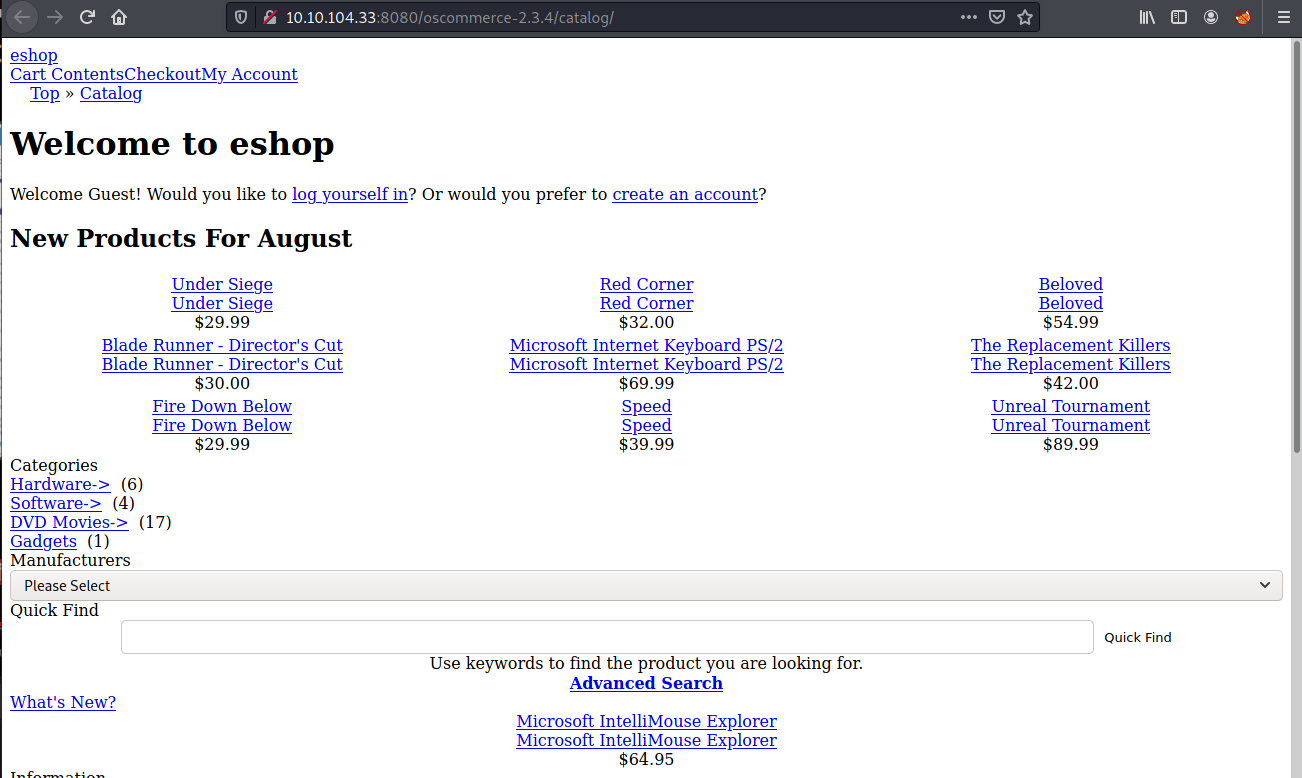
And look like we have this interesting 2 directories here



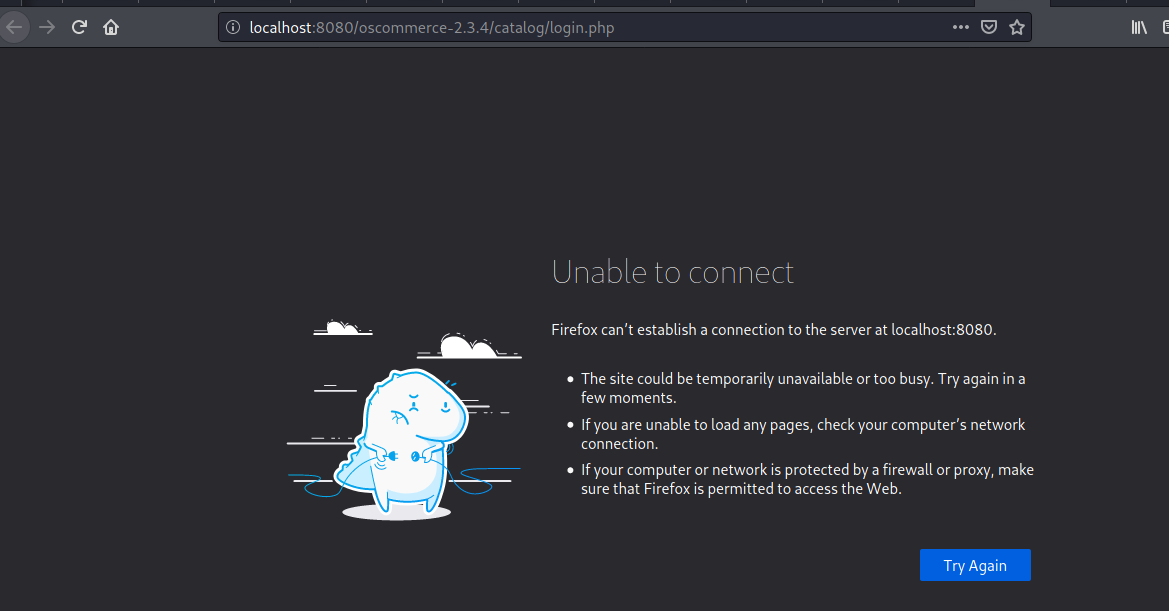
Seem like we can get all information of this project here (frontend, backend, log and any technology that they using to build this website)



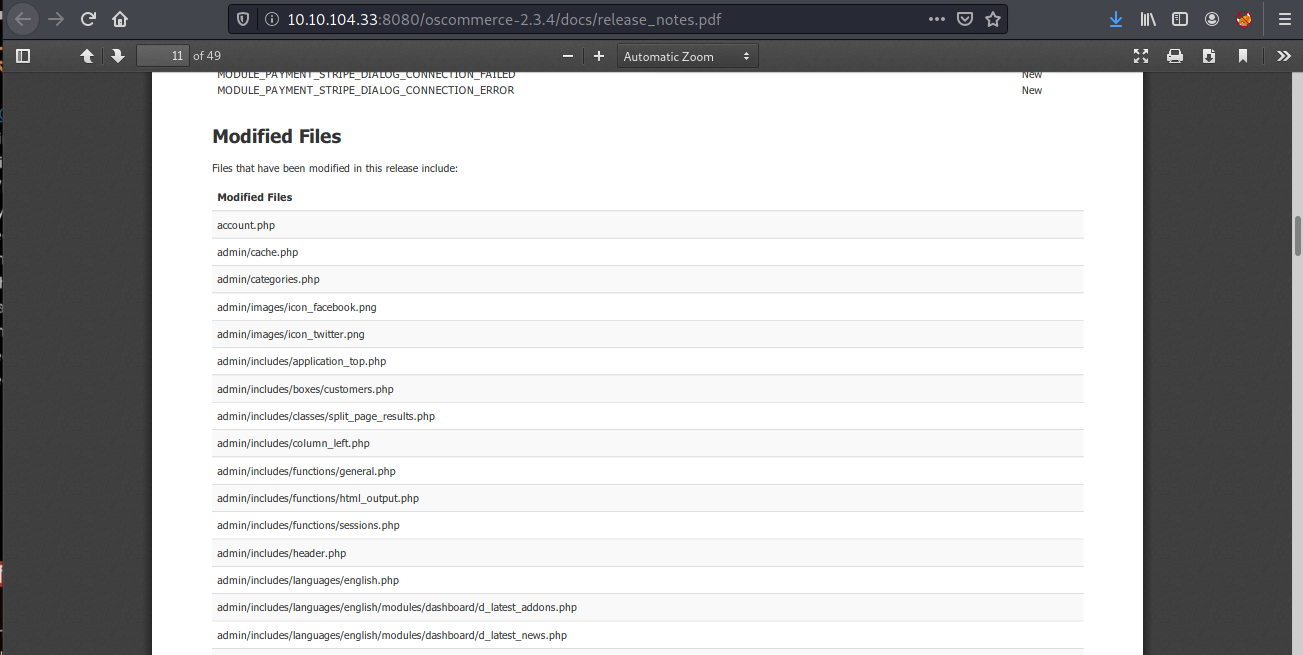
In catalog page, look like this team is building a shop-like/catalog site as they named it



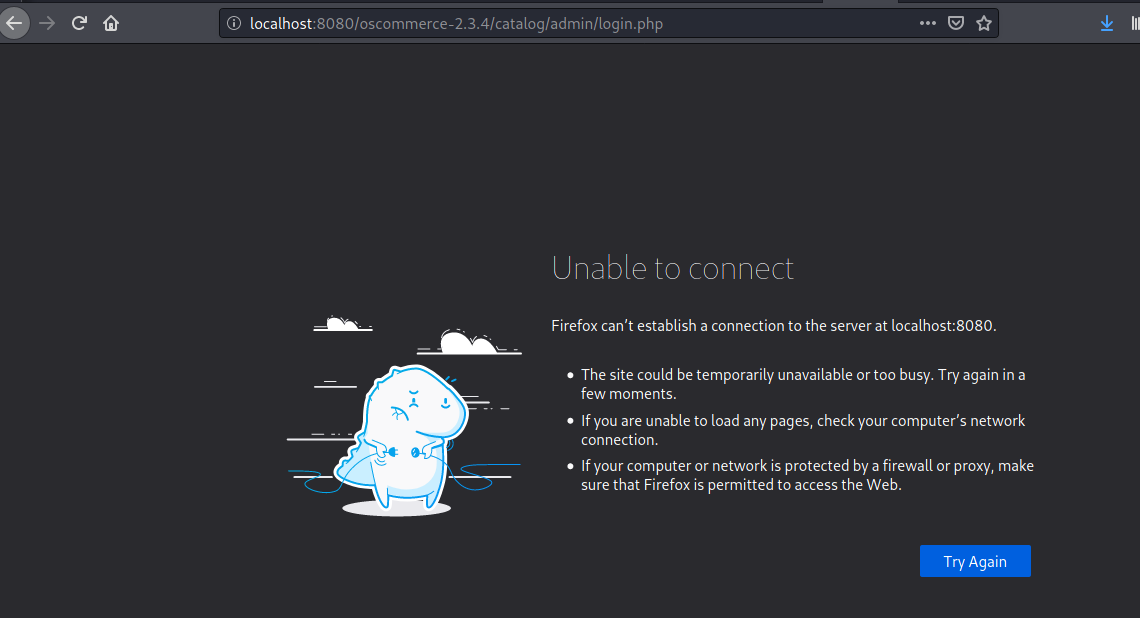
Look like we can only connect to backend via loopback ip if we were dev?



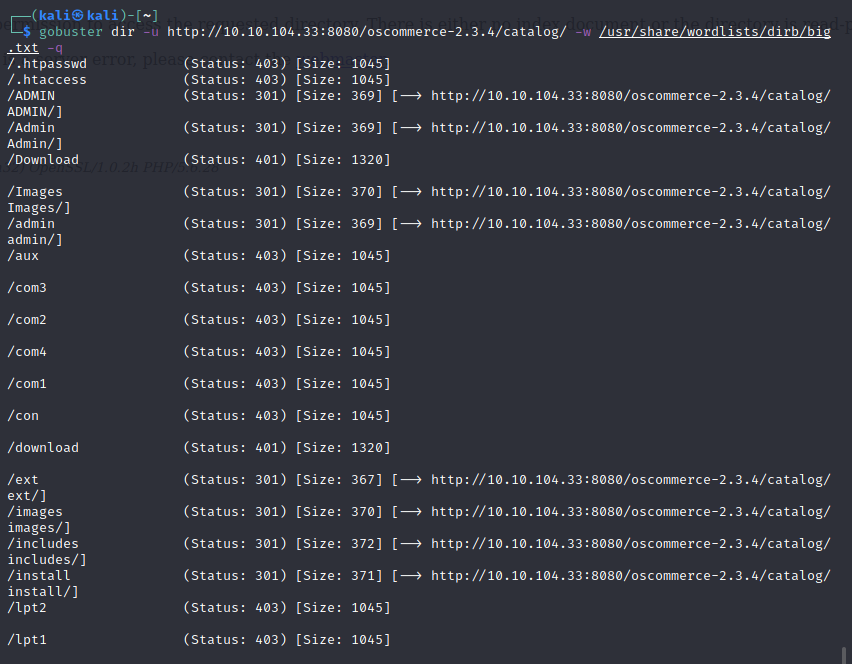
Launch a gobuster to bruteforce any useful directories that exists and while that we will look at other documents that will give us all information of this project (which I found admin subdirectory here)



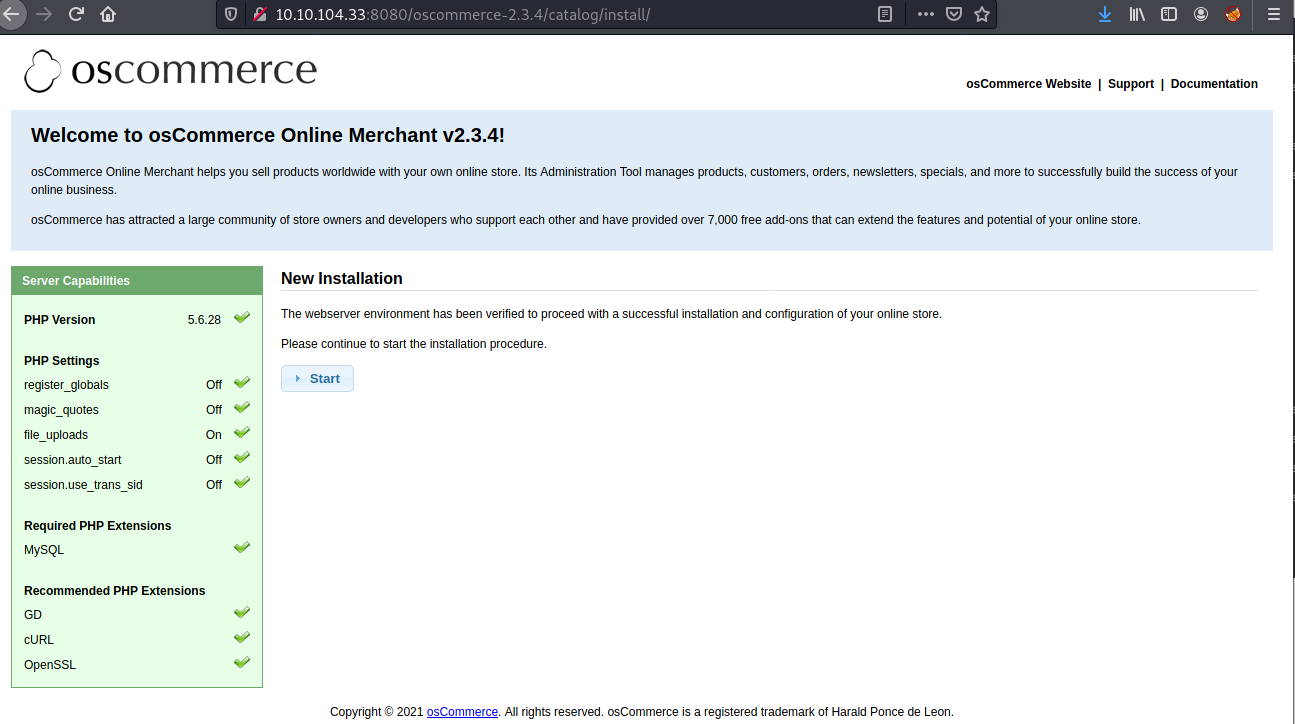
Nevermind its redirect to localhost so I’ll wait the result from gobuster



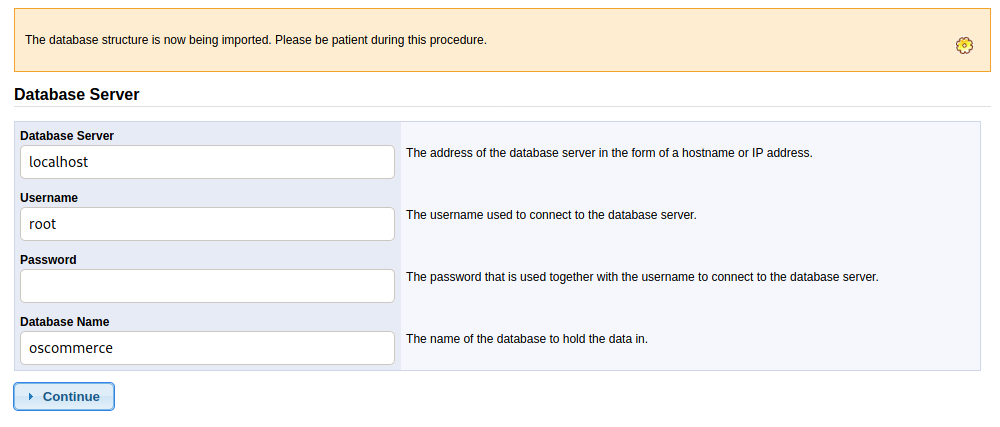
Maybe /install/ should be something we should look at



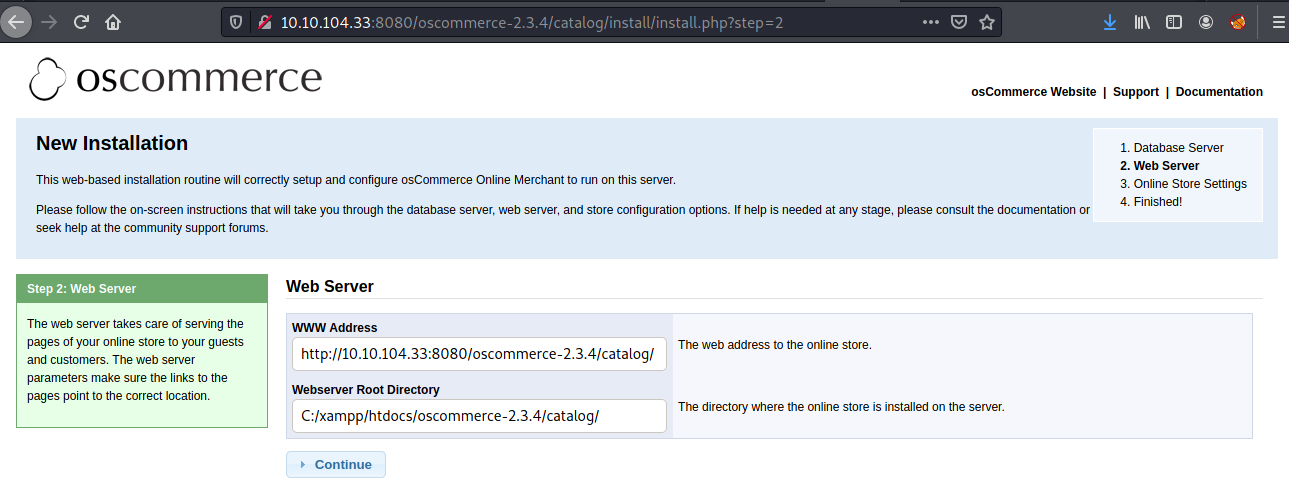
Nice! A whole new page, seem like we can set up our database as a dev from here



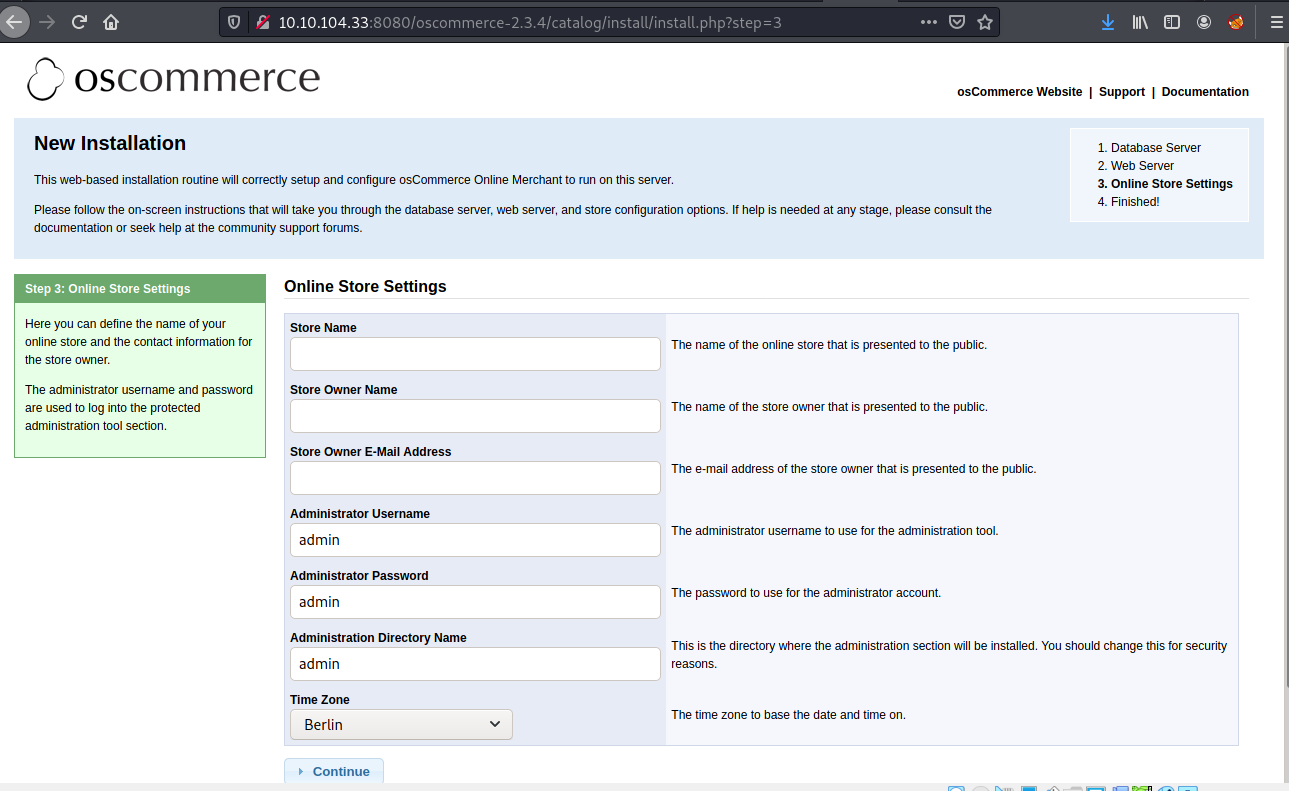
Set up database server first, and look like root user name is a valid one, now we need to wait for initialization



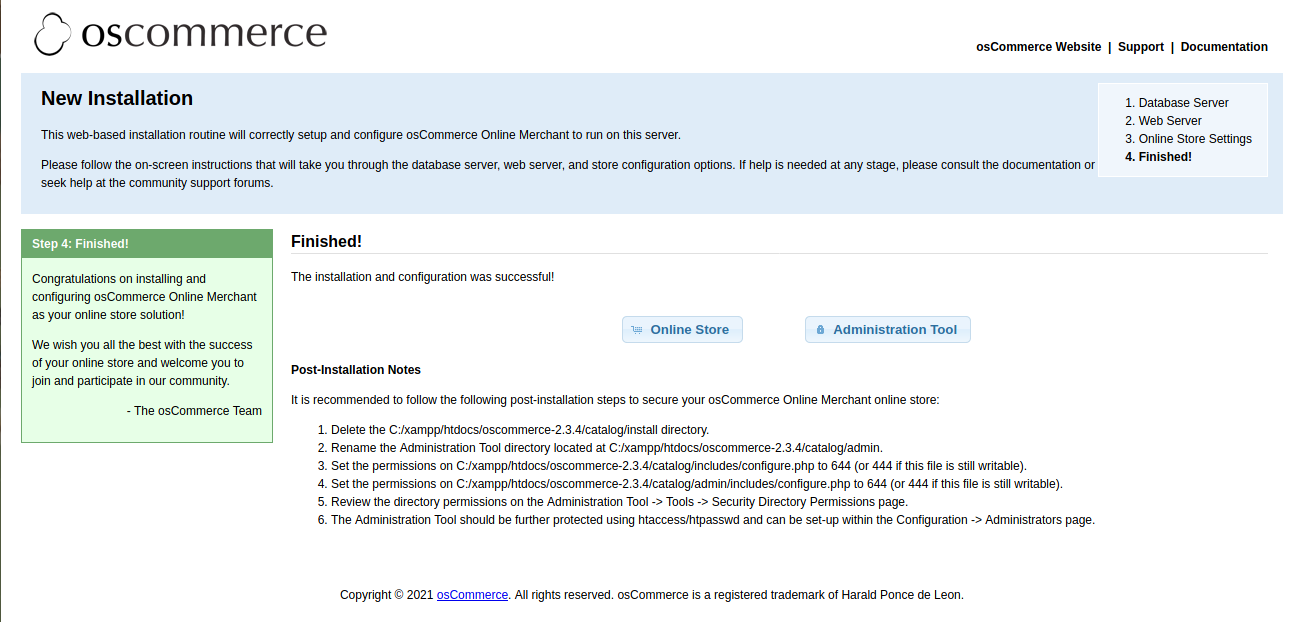
We’re at step 2 Web Server, we will go with default



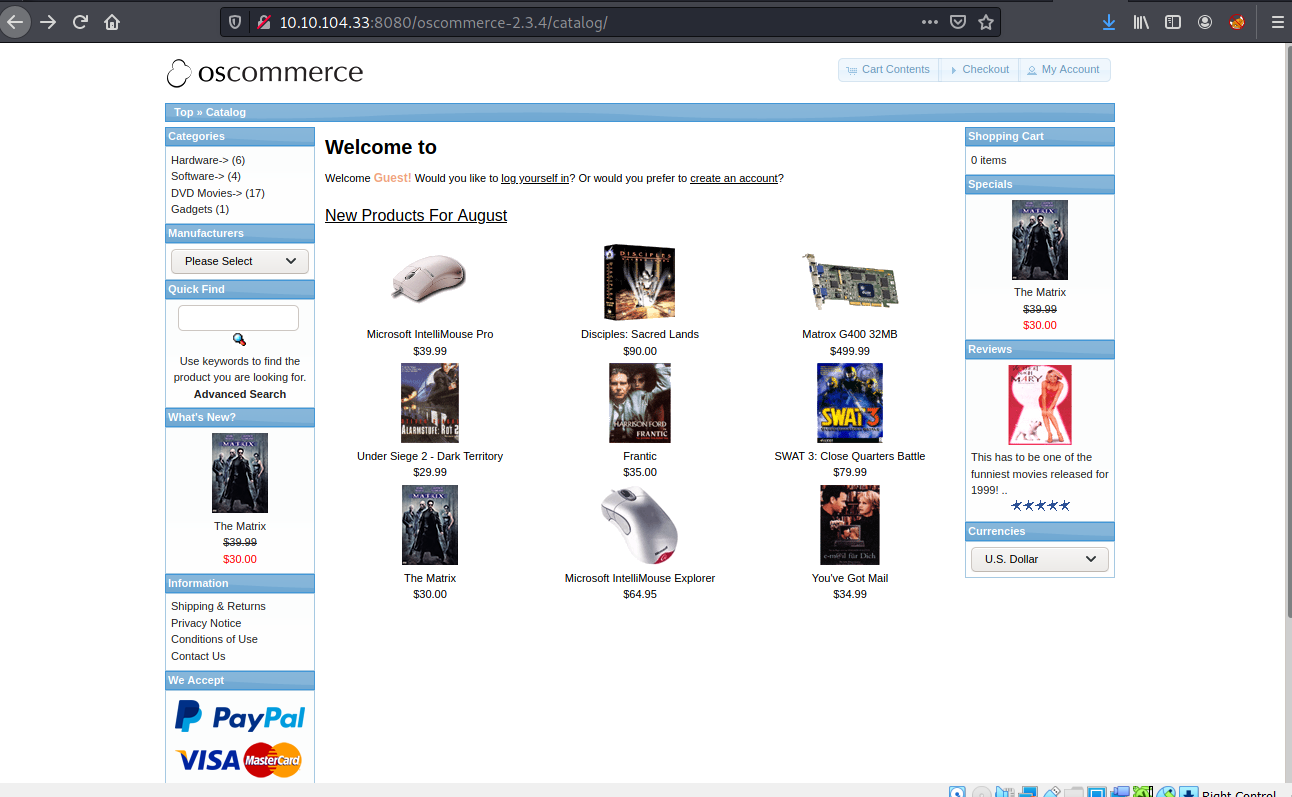
And at step 3 look like we can set up admin credentials, nice



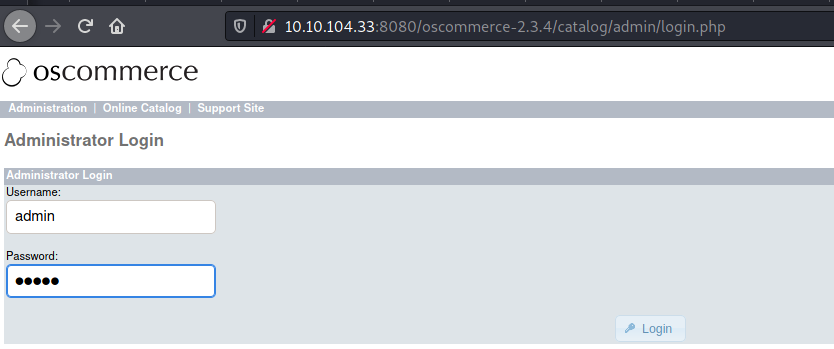
Set up credentials complete maybe we can

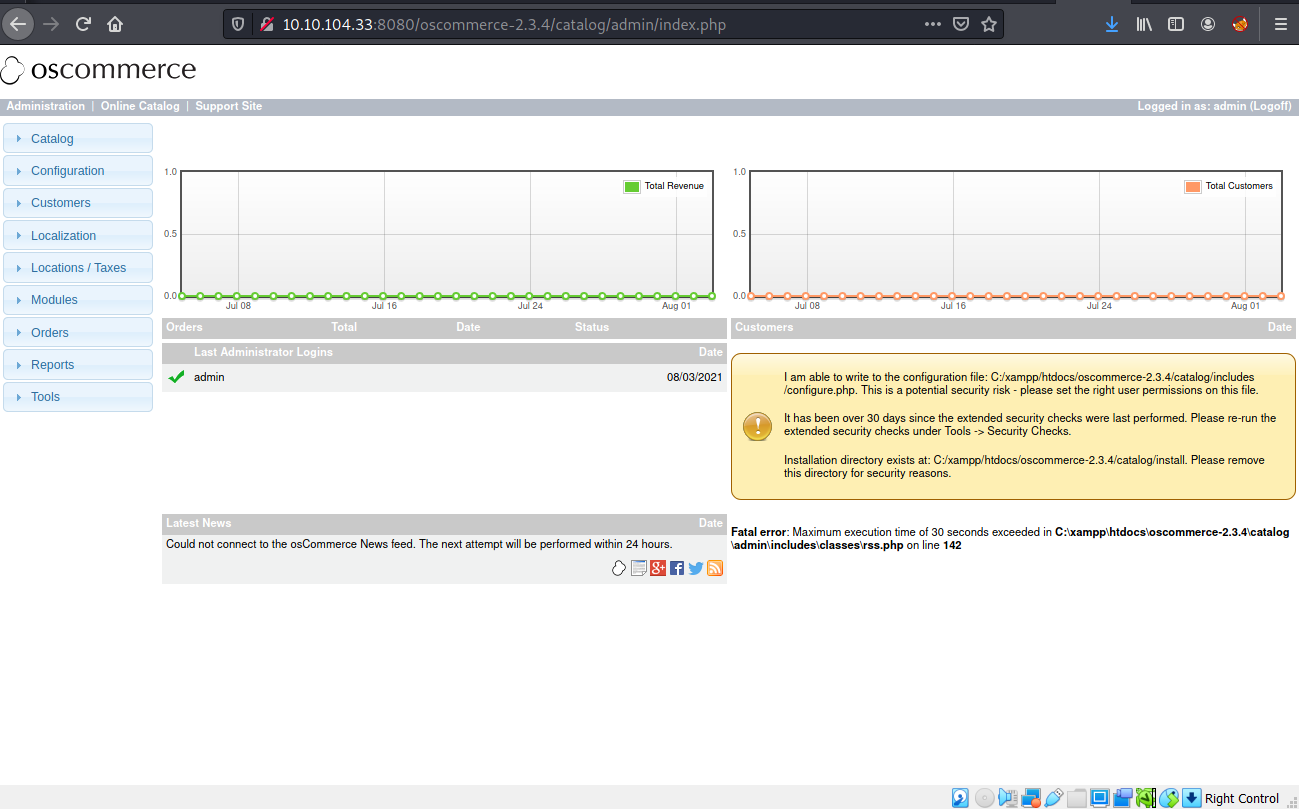


Now we have a proper website now, let’s go to admin page again

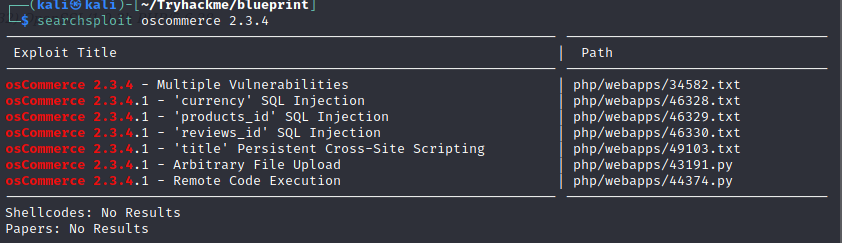


Nice we successfully login as admin but we can’t do any further than this in this website

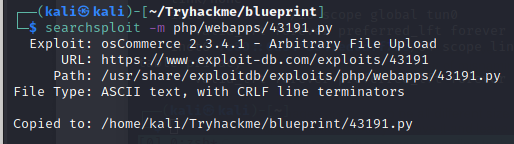




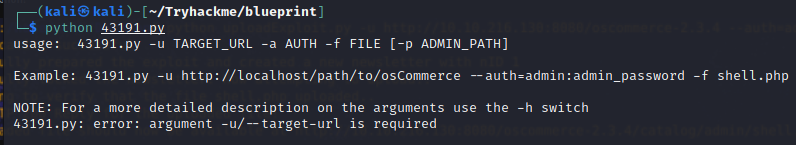
Let’s find some public exploit with searchsploit, and we found a File Upload one



Copy it and try to run



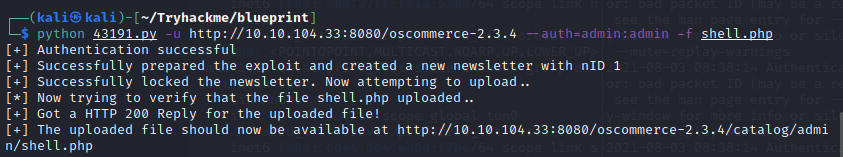
Look like we need 3 parameters here for target url, auth and shell script



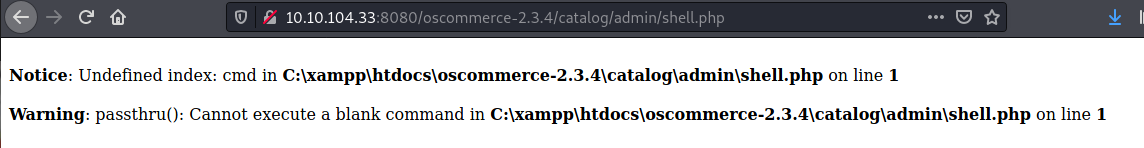
Create a php file one that get command prompt in Windows so we will put our command later



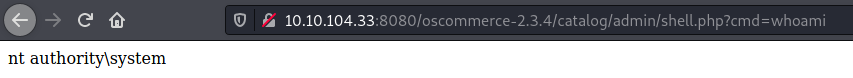
Run python to upload our shell.php and we should get a webpage that we could inject our command there



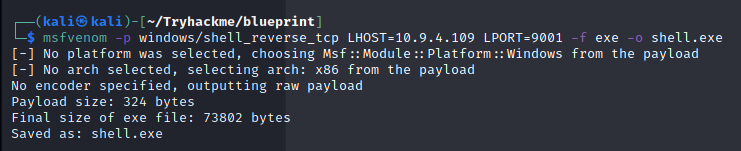
And it’s here



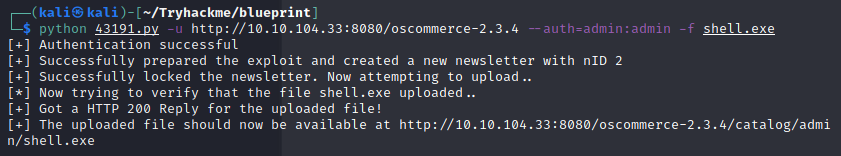
Let’s use basic command like **whoami** first to check out which privilege we have and…. SYSTEM, we have everything



It’s time for the reverse shell so we won’t bother to edit many url



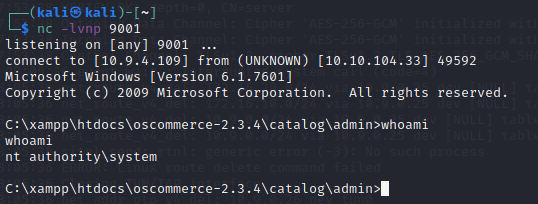
Upload it via the same exploit script



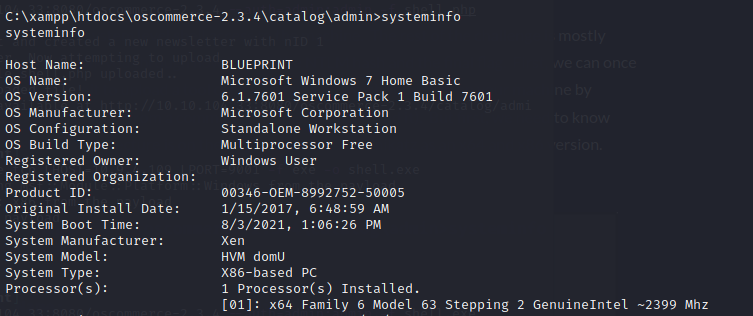
Now set netcat listener or metasploit if you prefer and run our executable shell



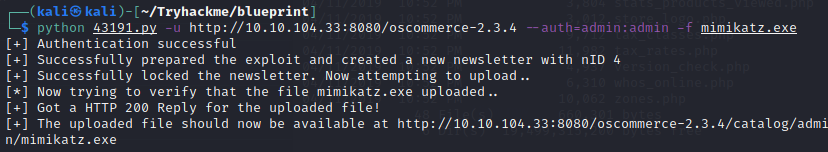
Easy shell



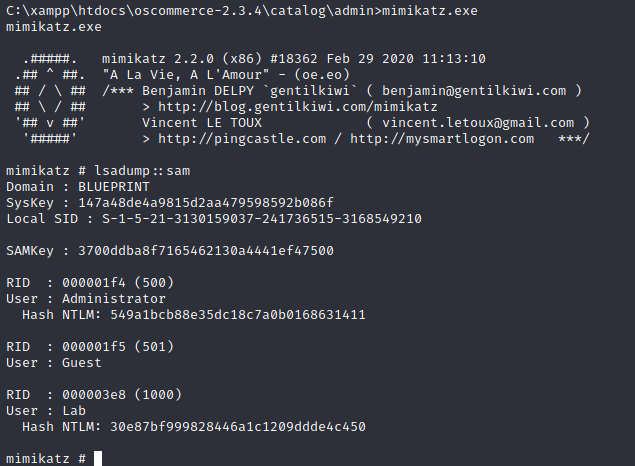
In case that we get a reverse shell in netcat we can use Mimikatz to get hashdump of Windows credentials but first check System type cause we have x86(Win32) and x64, and this is x86 type



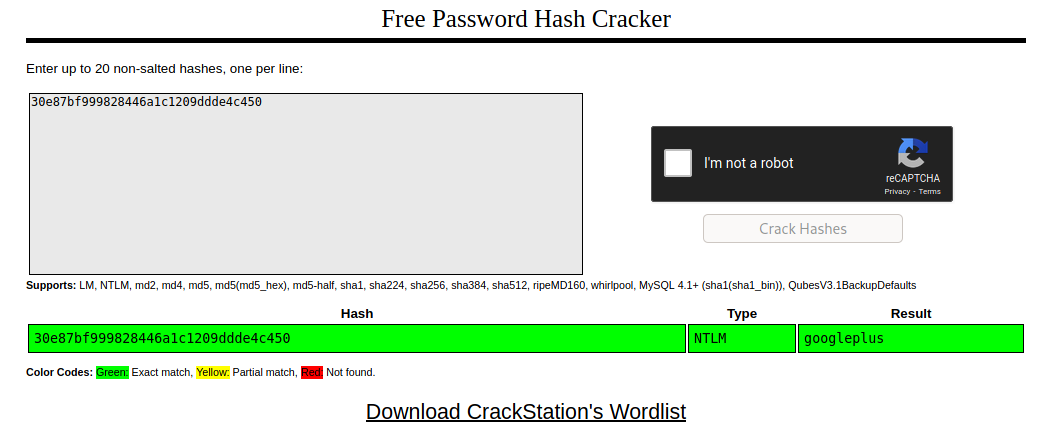
Upload Mimikatz x86 version to remote machine



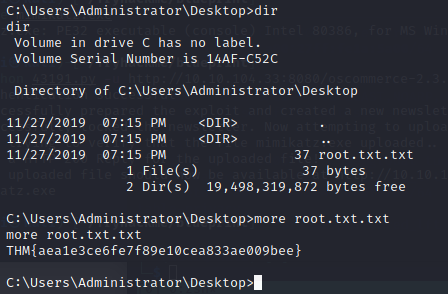
And get our hashdump via in SAM database

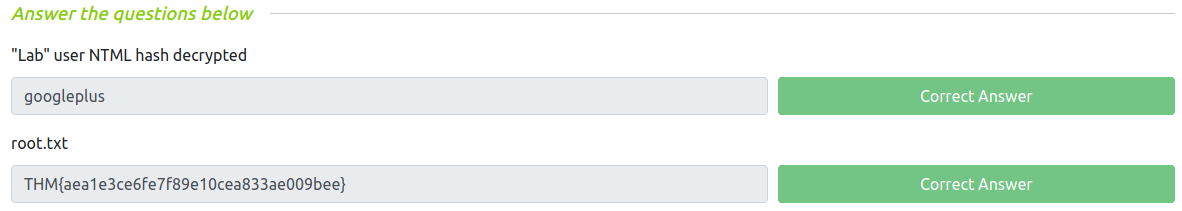


Crackstation can help us crack, now we got our first flag



Now explore Administrator directories and capture the root flag





**How about using Metasploit exploit?**

**Module:** exploit/multi/script/web\_delivery

**Payload:** windows/meterpreter/reverse\_tcp

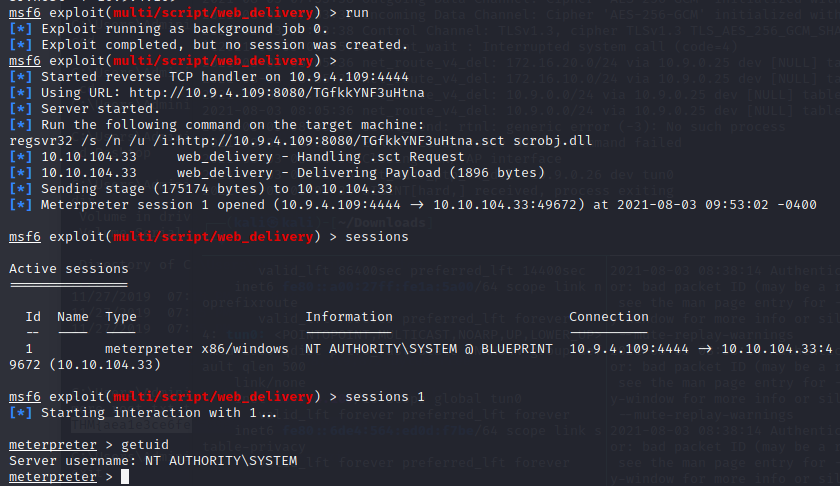
**Target**: 3 - Regsvr32

**SRVHOST and LHOST**: tun0 ip

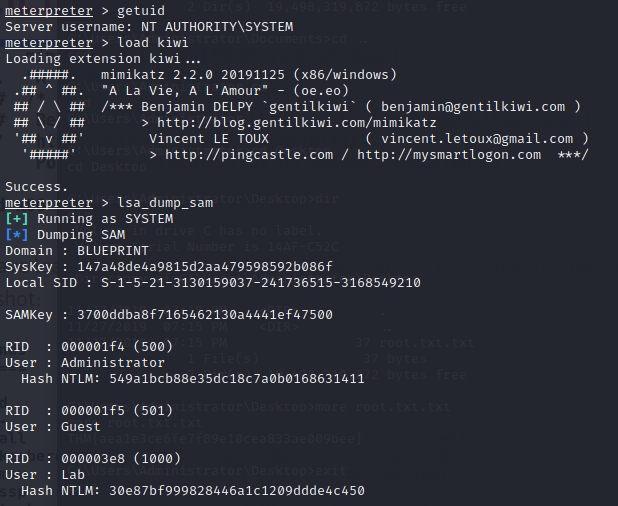
After run we will get a command that we have to run it on target machine to exploit



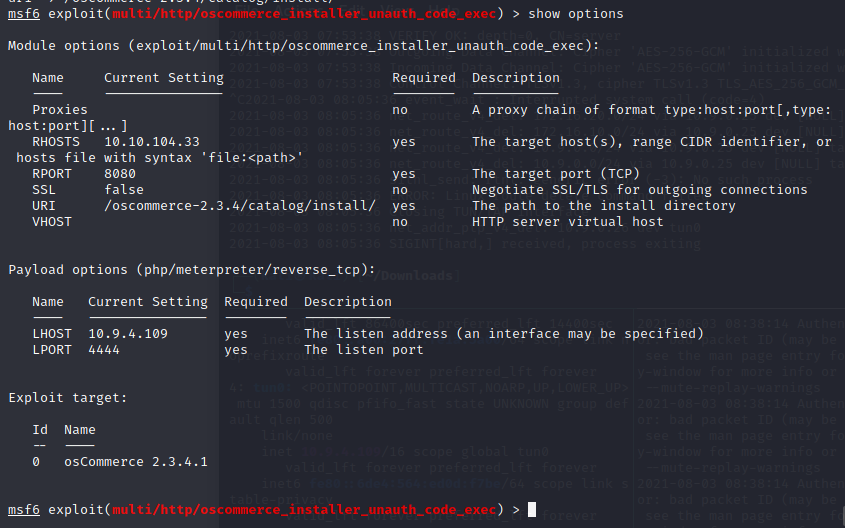
Now a sweet system shell come back to us



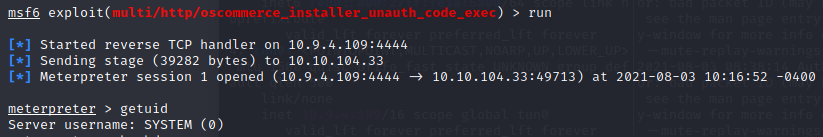
We can just use **hashdump** command or load kiwi module (Mimikatz in metasploit) to get a hash



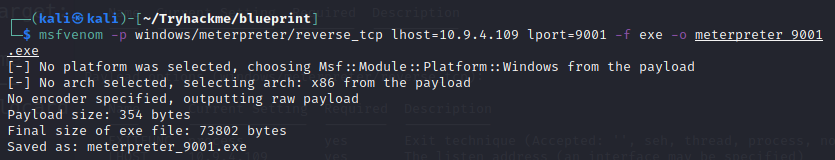
Next module is exploit/multi/oscommerce\_installer\_unauth\_code\_exec



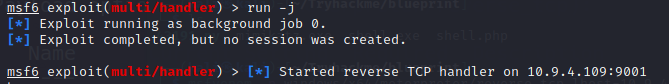
We will get a doobie doobie meterpreter shell at this point that can’t use anything much

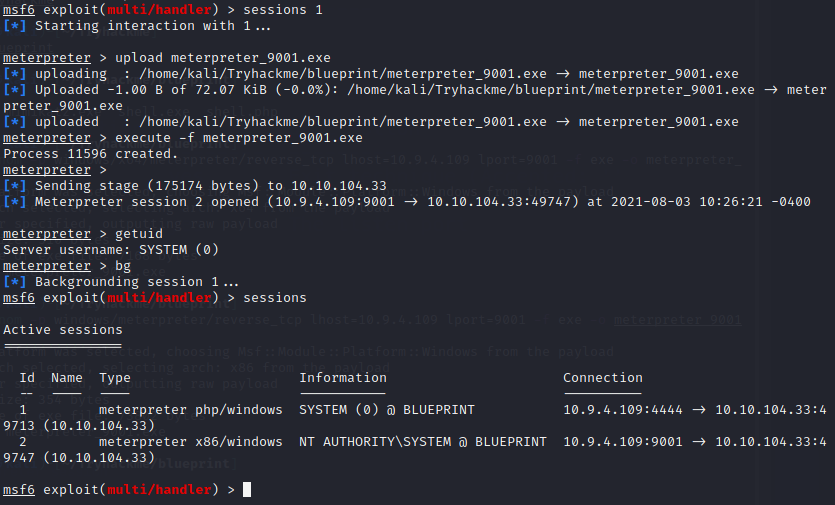


But we can get a reverse shell through this shell



Run multi/handler as a job and go to a doobie doobie shell to upload our executable file and execute it





Easy

