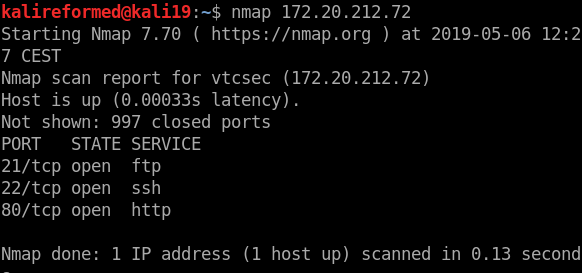


First of all we see the IP address of the machine to be attached

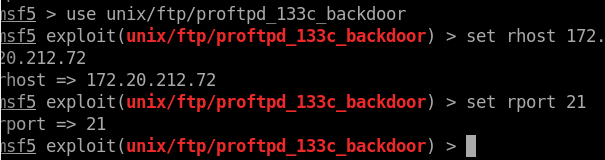


In the next step we do nmap with address of the machine to be attached (MA)

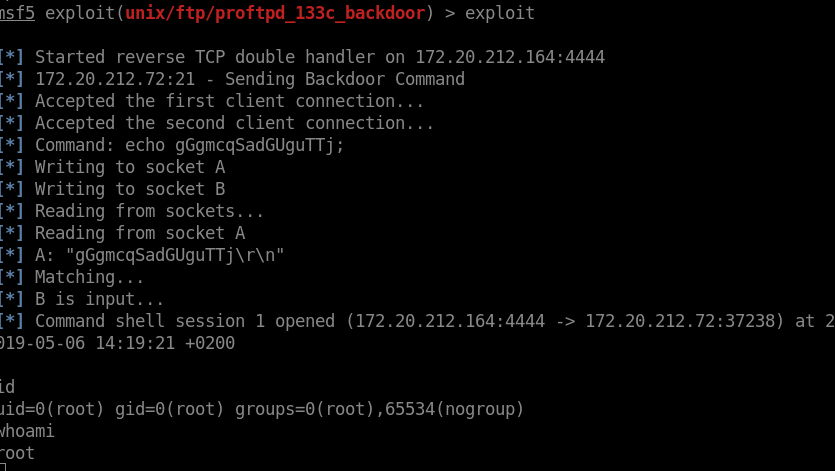
Then now that we know the ports and services 21 ftp, 22 ssh and 80 http

Let’s get into the game

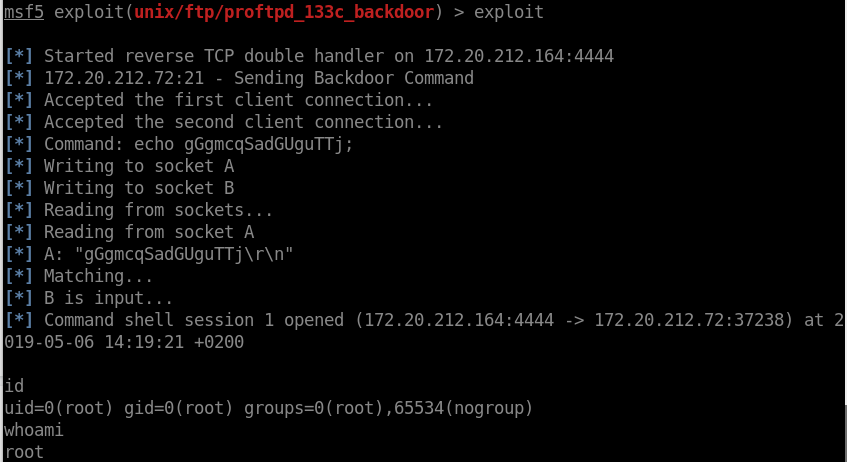
Then we configure the proftp by assigning a remote host and with its above port



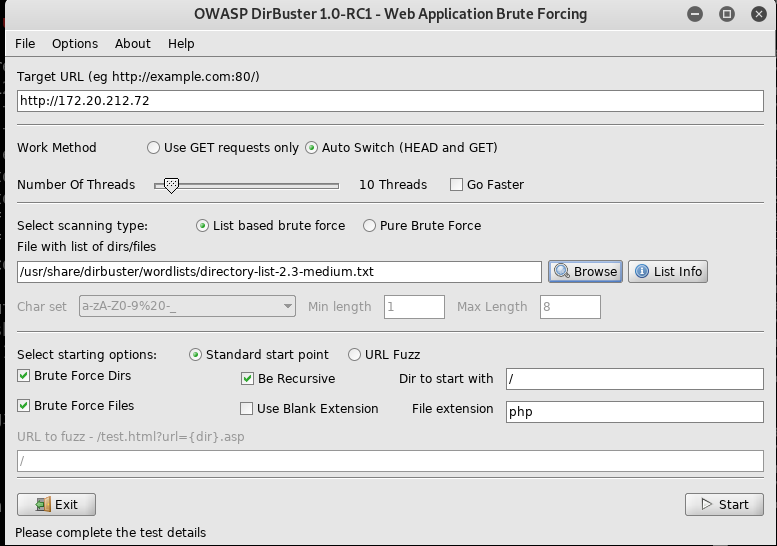
After assigning the rhost and the rport we access the part of exploits   
In the exploit part through the id command and whoami command we find that we made root access

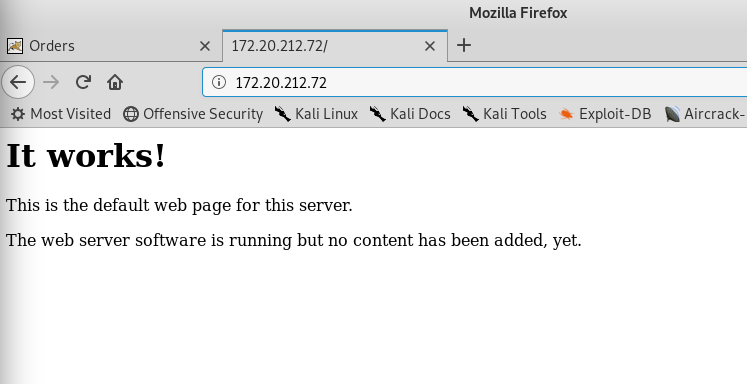


Right after we did an analysis through dirbuster

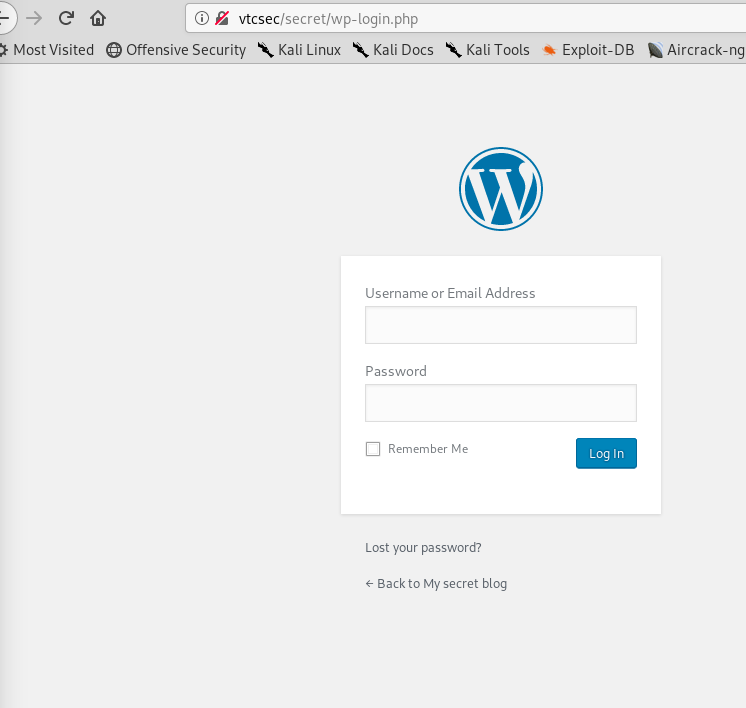


While doing the analysis we inserted in the url the address of the machine to be attached with port 80

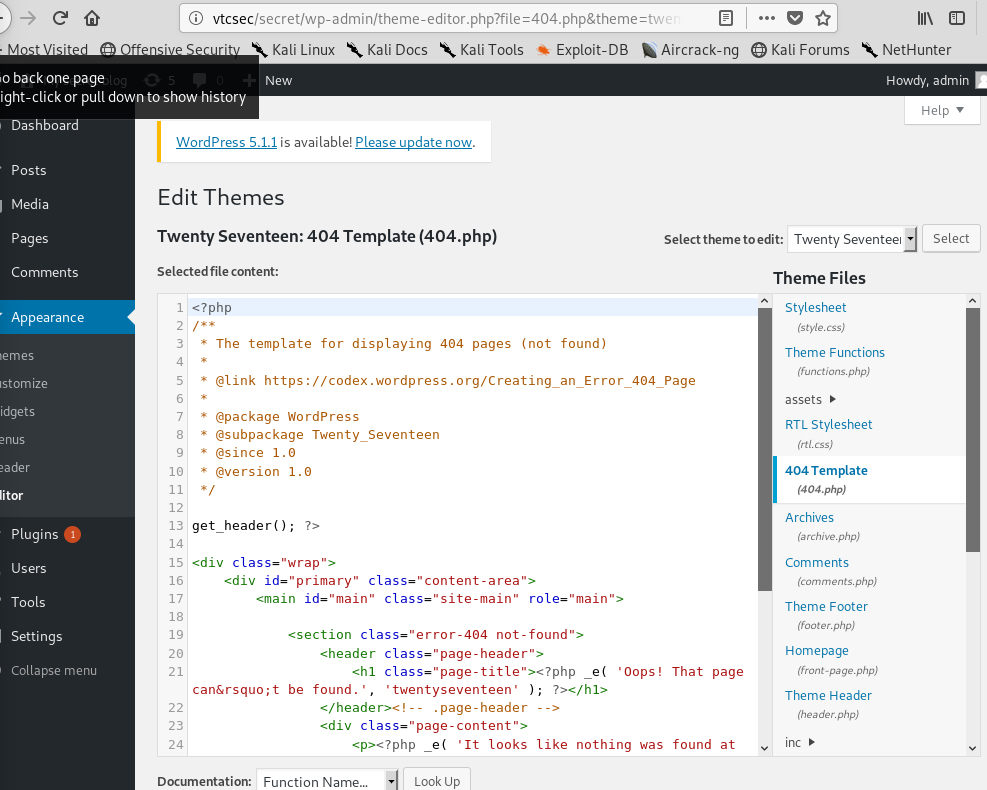


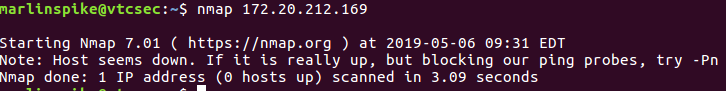
Through dirbuster we found a secret subfolder where we can access Wordpress

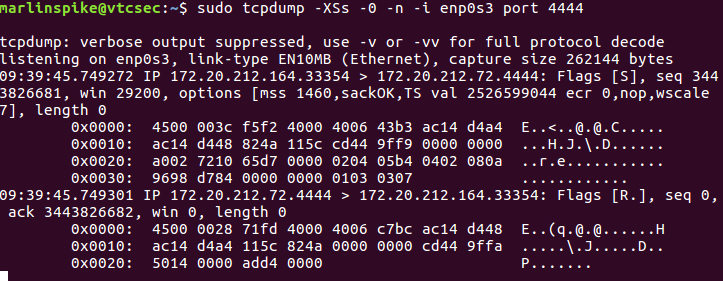
-Note:  
you can not access the login section of W3C if we have not entered the ip address of the host machine to be attached in the /hosts file of our machine   
  
I tried with admin and admin basic credentials to enter the Login section

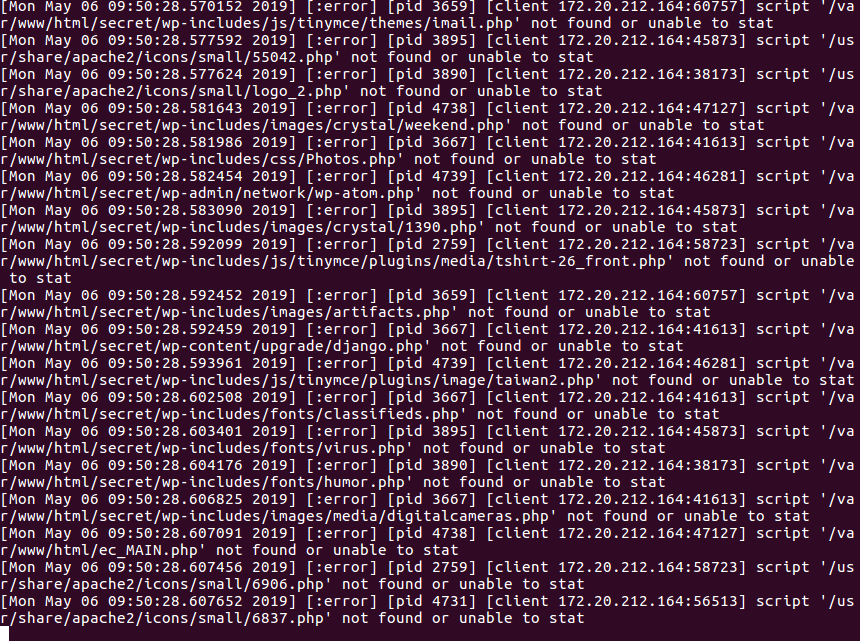


Then in the section Appearance/404 template  
we can change the page in case of error



then we put used the tcpdump from the ubuntu machine to see the established connections and in the other machine we made nmap from the attacking machine



these are the syslogs of the machine that occur on the attacking machine

-Riccardo Bruzzese