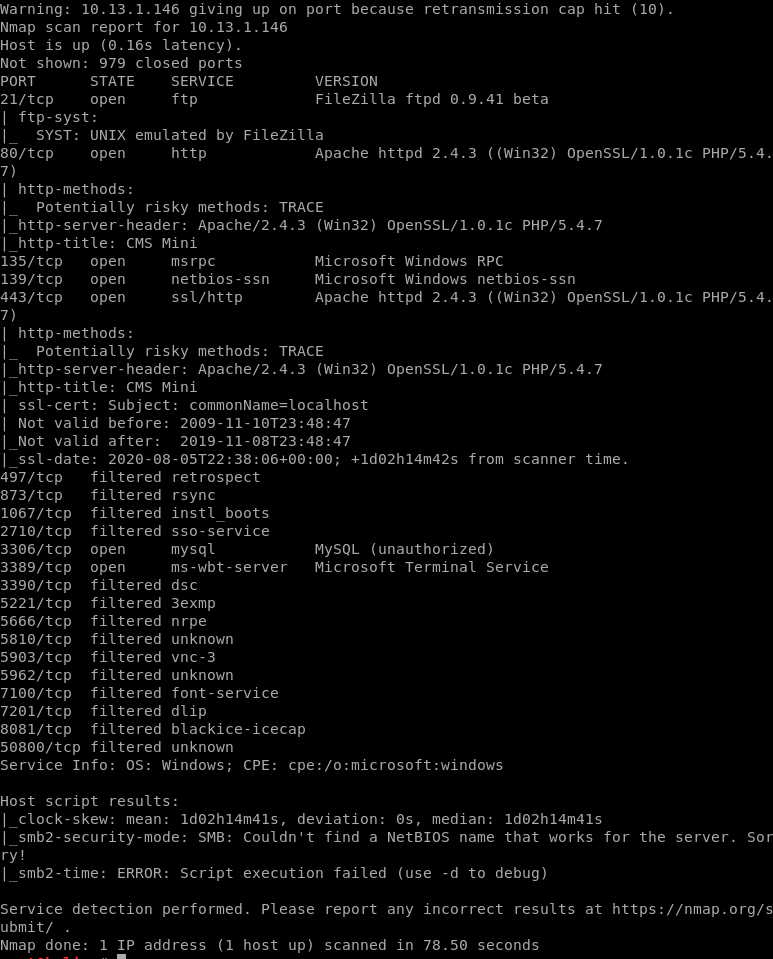
Jennifer(10.13.1.146)-GhostIA

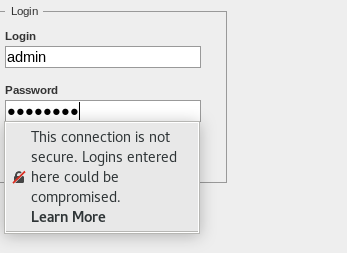
Sarah Ferenczi

Enumeration

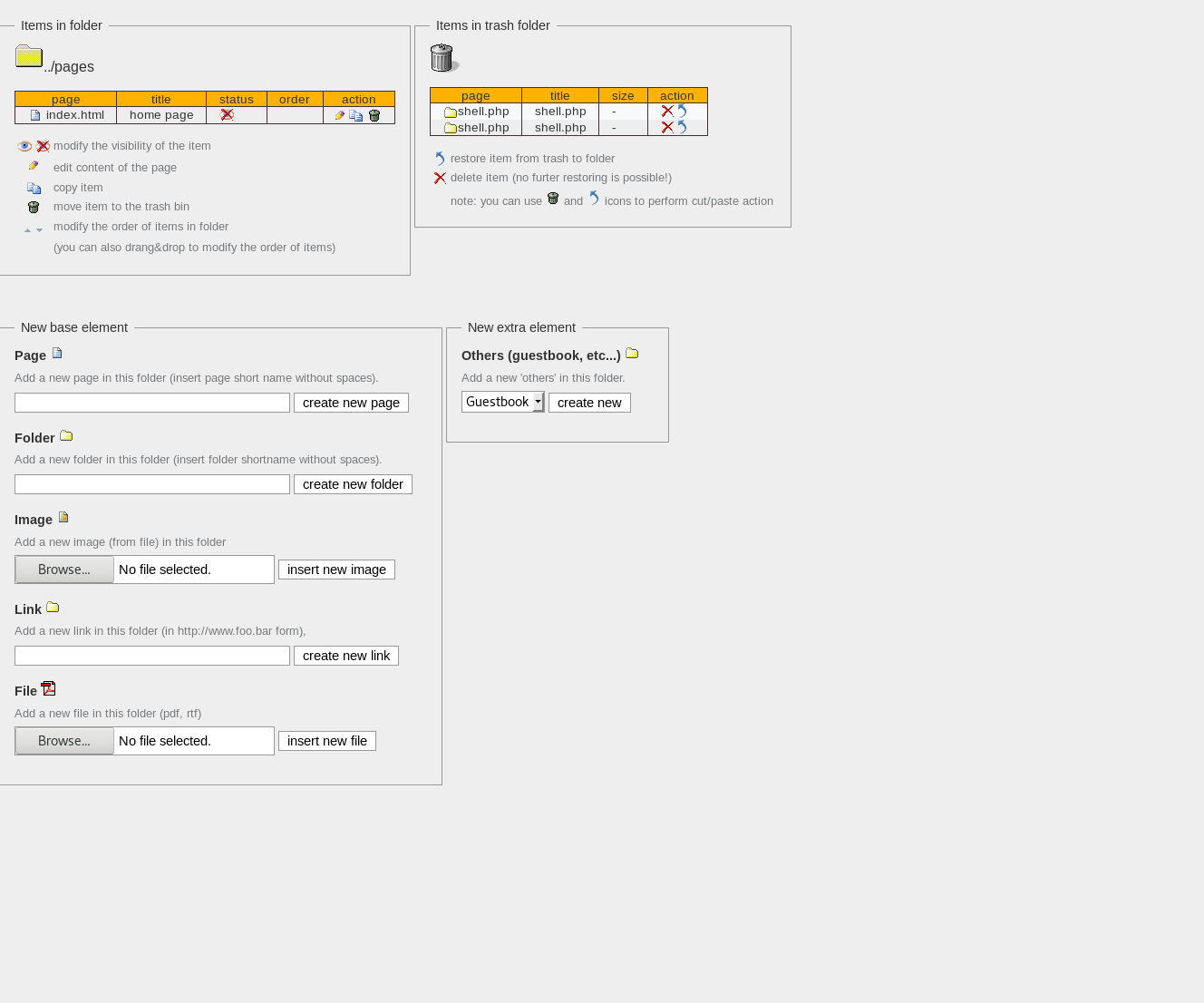


First we run an nmap scan. First thing we can notice is that port 80 is open with a webserver running on it.

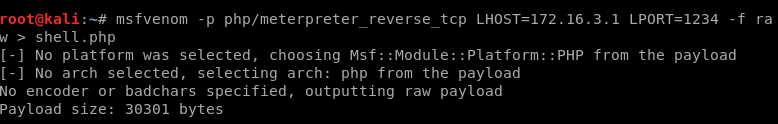
Exploitation



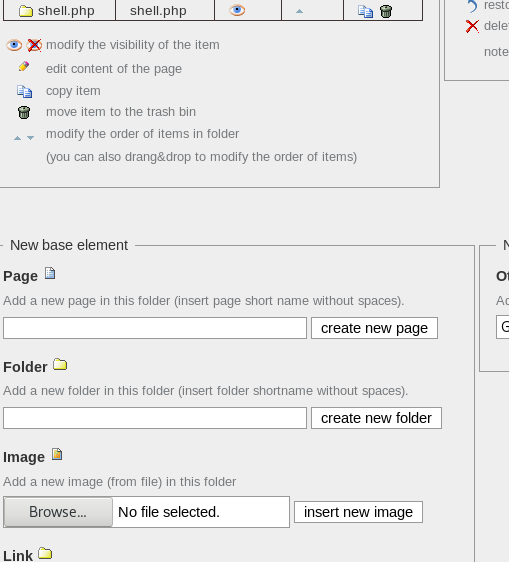
We can head to the login page by navigating to /admin on the webserver and use default credentials: admin/password to go ahead and log in.



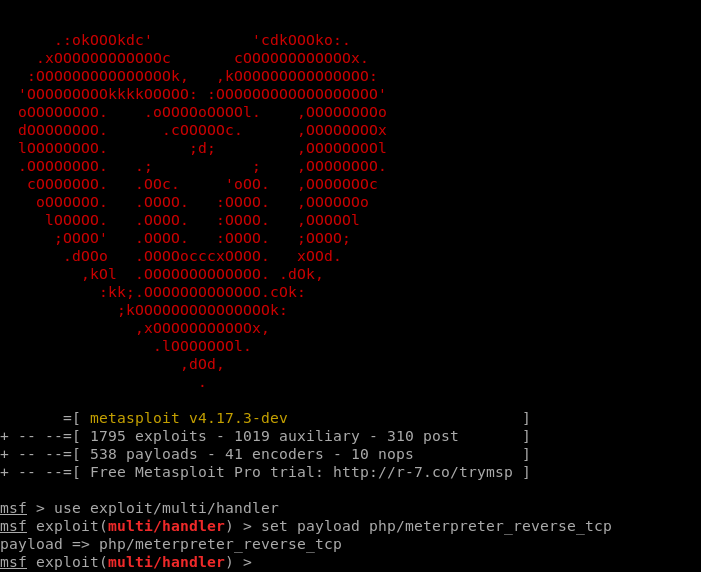
When we look at the file upload, we can notice that there are no restrictions on uploading a file.



Let’s go ahead and generate an msfvenom payload since this system is running Windows

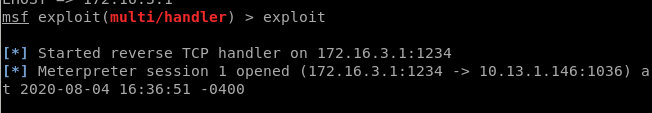


Now we can go ahead and upload the file.



Meanwhile, in msfconsole, we can go ahead and set up our listener

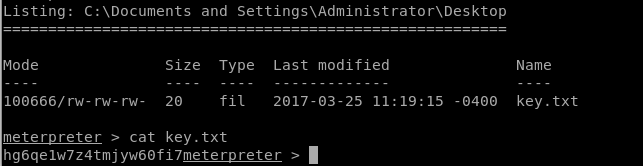




Then if we navigate to /pages/shell.php, we will get a shell on our meterpreter listener.



Now we know we are an administrator on this system.



Then, we can head to C:\Documents and Settings\Administrator\Desktop and get the key