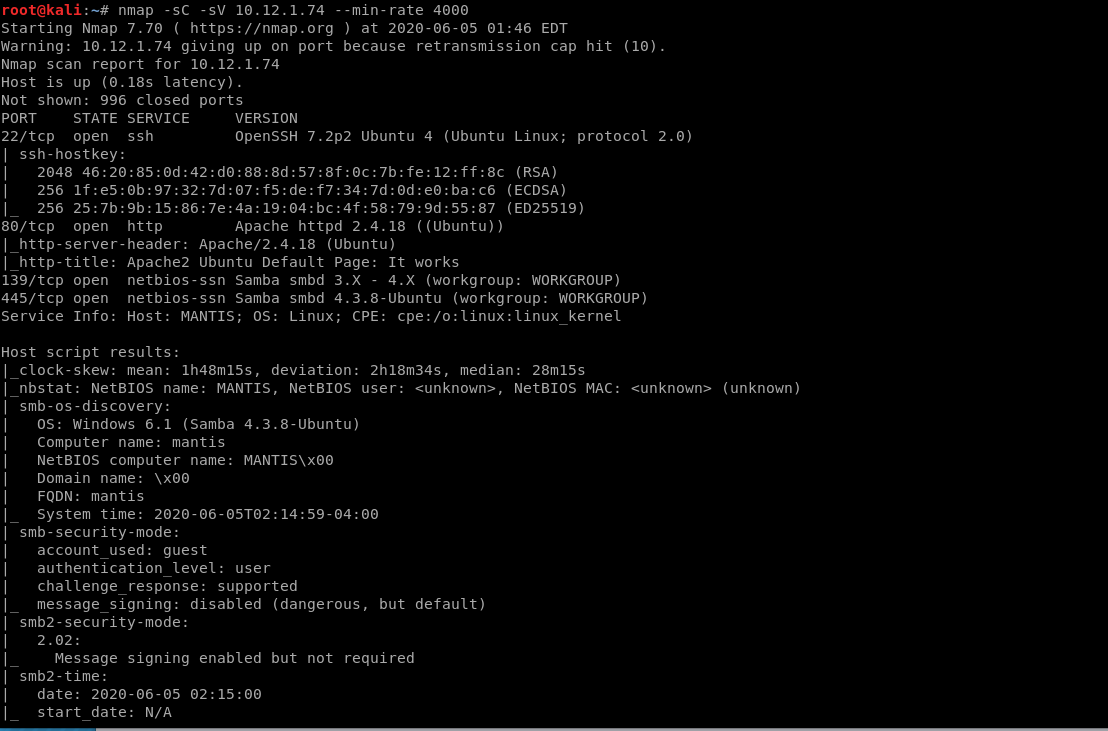
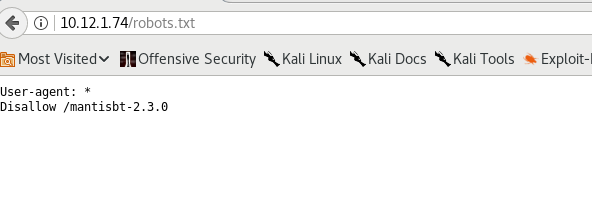
Mantis(10.12.1.74)-GhostIA

Sarah Ferenczi

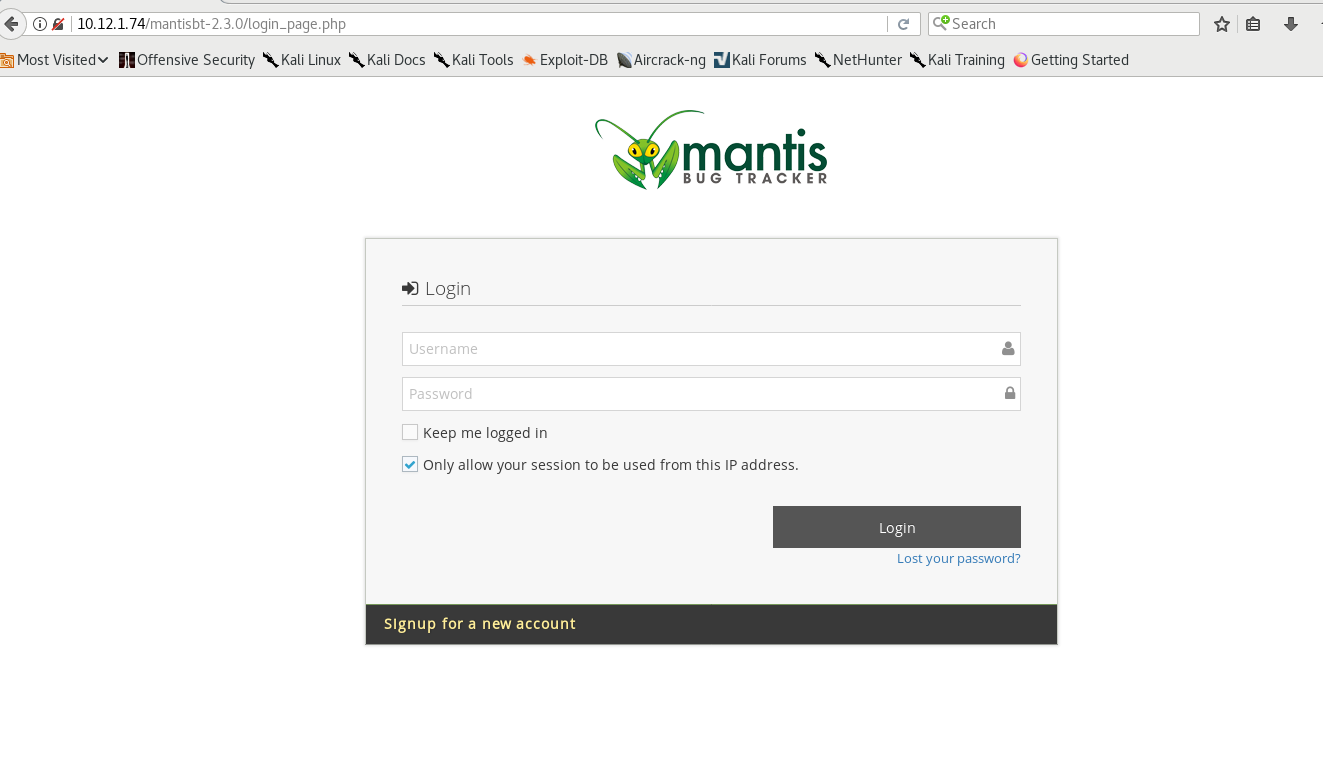
Enumeration



First let’s run an nmap scan. We can see that port 80 is open.

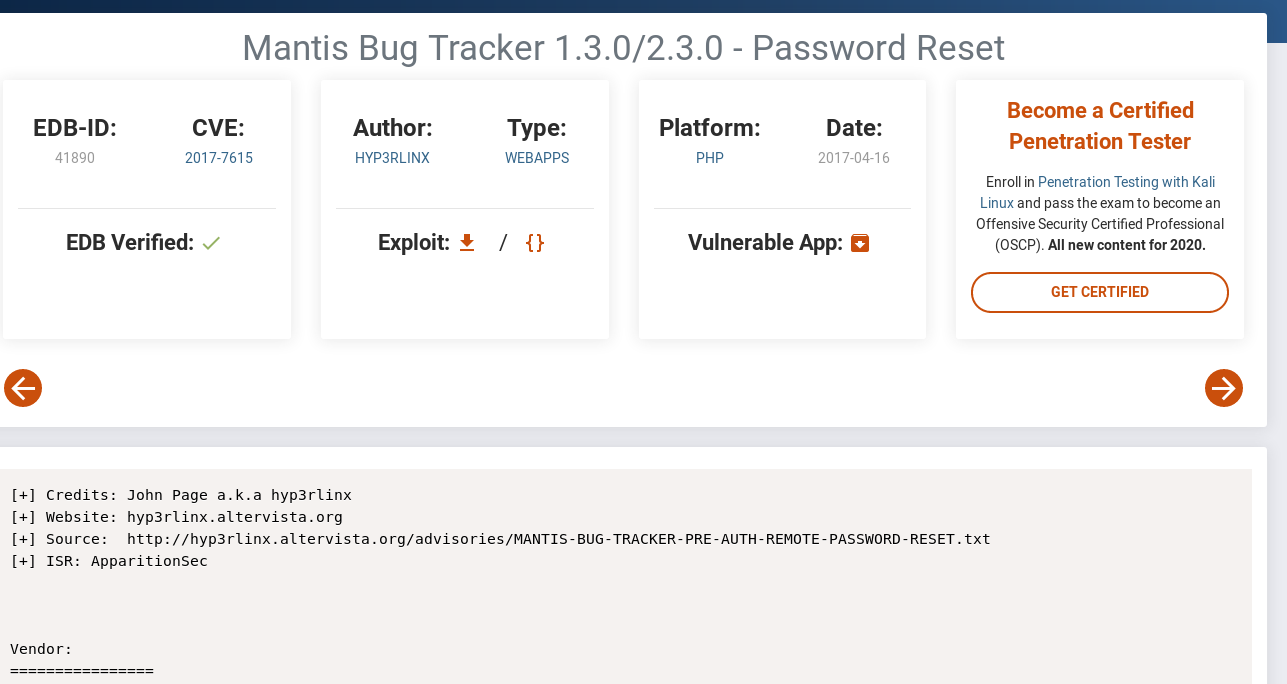


If we go ahead and see if robots.txt has been disabled, we can find another interesting directory.

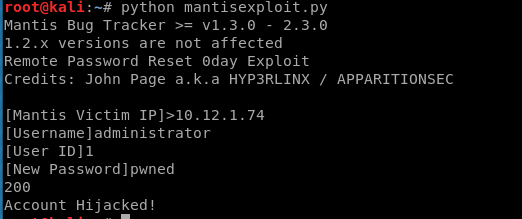


We are directed towards this login page. Let’s see if we can use that to find any exploits.

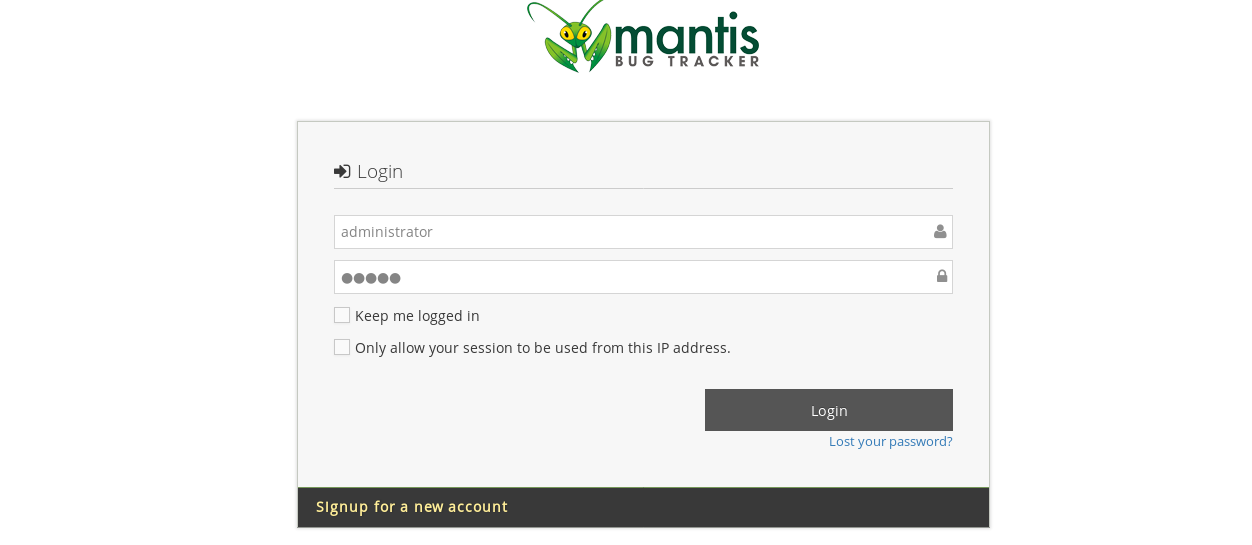
Exploitation



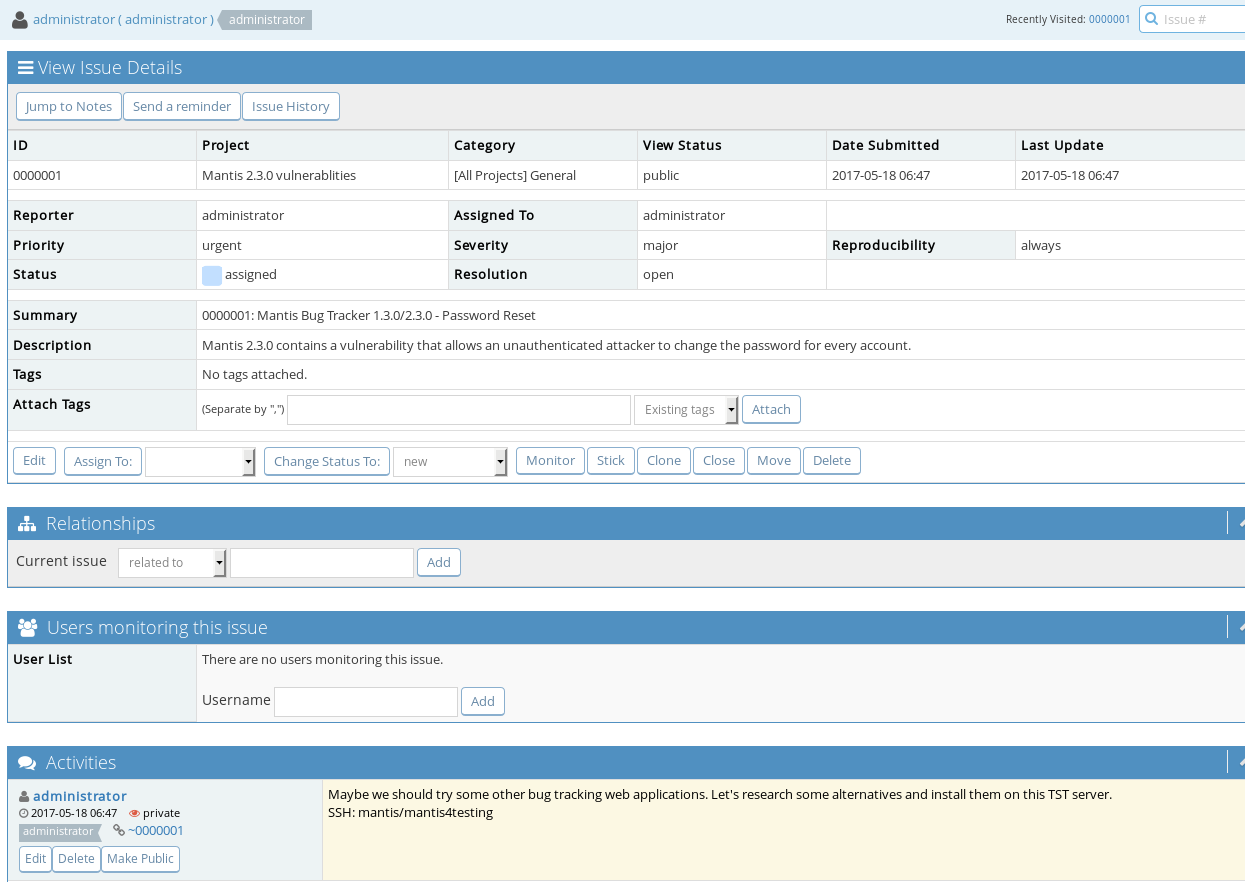
We find a password reset when we go and look up the vulnerability.



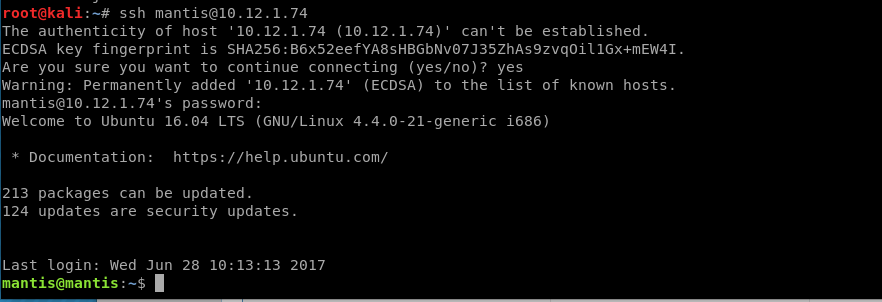
We can go ahead and use this proof of concept Python script to hijack the account.



Then let’s log in with the credentials we made with the exploit.



If we click on reports, we can find ssh credentials.



Then we can go ahead and ssh in.

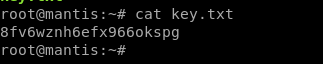
Privilege Escalation



If we check our permissions, we can run anything we want as sudo.



Let’s use that to get root.



From there, we can head to /root and get the key.