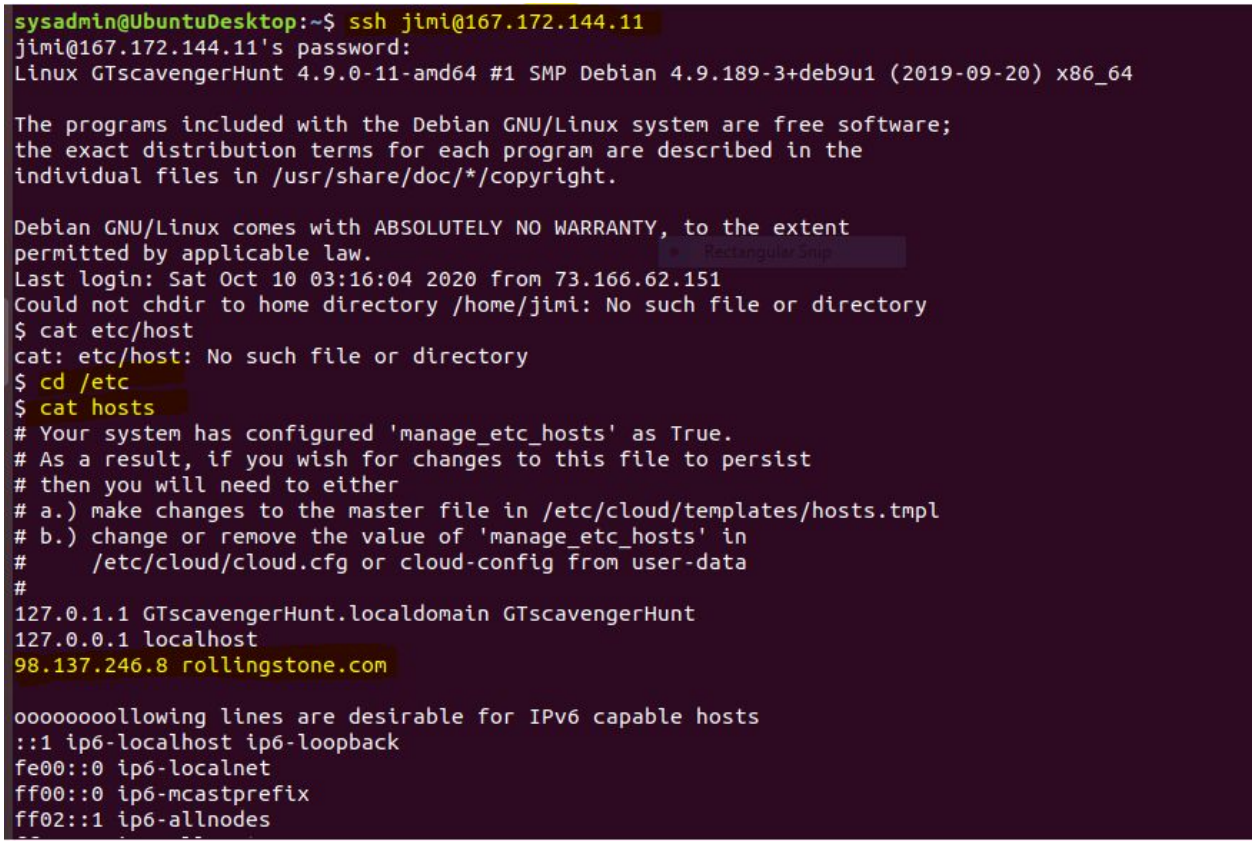
Phase 3: "I Feel a DNS Change Comin' On"

Solution:

Log into the ip address 167.172.144.11 that is open for connection with the ssh command and the credentials given:
$ssh jimi@167.172.144.11

Open the hosts file in the /etc directory to check for possible DNS hijacking.




The hosts file DNS cache has been updated to direct all traffic meant for rollingstone.com to go to an IP address 98.137.246.8.

Run nslookup on the IP address 98.137.246.8:


Summary

rollingstone.com was redirected by an attacker to an IP address 98.137.246.8, which is another domain (media.router.fp72.prod.media.vip.gq1.yahoo.com). These findings fall into the Application layer (layer 7).