

### 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.

```
sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11
jimi@167.172.144.11's password:
Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 10 03:16:04 2020 from 73.166.62.151
Could not chdir to home directory /home/jimi: No such file or directory
$ cat etc/host
cat: etc/host: No such file or directory
$ cd /etc
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tpl
# b.) change or remove the value of 'manage_etc_hosts' in
#    /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com

ooooooooo following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
```

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:

```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa      name = media-router-fp72.prod.media.vip.gq1.yahoo.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

## 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).