|  |  |  |  |
| --- | --- | --- | --- |
| **Site** | **IP** | **Command Used** | **Result** |
| Hollywood Database Servers | 15.199.95.91/28 | fping -g -r 1 15.199.95.91/28 or  fping -g 15.199.95.91/28 | Unreachable |
| Hollywood Web Servers | 15.199.94.91/28 | fping -g -r 1 15.199.94.91/28 | Unreachable |
| Hollywood Web Servers | 11.199.158.91/28 | fping -g -r 1 11.199.158.91/28 | Unreachable |
| Hollywood Application Servers | 167.172.144.11/32 | fping -g -r 1 167.172.144.11/32 | alive |
| Hollywood Application Servers | 11.199.141.91/28 | fping -g -r 1 11.199.141.91/28 | Unreachable |

**Phase 1**

Ping works at Layer 3 (Network Layer).

**Phase 2**

sysadmin@UbuntuDesktop:~$ **sudo nmap -sS 167.172.144.11**

[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-26 15:17 EDT

Nmap scan report for 167.172.144.11

Host is up (0.0077s latency).

**Not shown: 999 filtered ports**

**PORT STATE SERVICE**

**22/tcp open ssh**

Nmap done: 1 IP address (1 host up) scanned in 14.21 seconds.

**Results in Bold. Only port tcp 22 open.**

**Port scan works on Layer 4 (Transport Layer).**

**Phase 3**

# 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.tmpl

# 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**

oooooooollowing lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

ff02::3 ip6-allhosts

rollingstone.com is set to 98.137.246.8.

nslookup shows different IP for ollingstone

sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

**Name: rollingstone.com**

**Address: 151.101.192.69**

Name: rollingstone.com

Address: 151.101.64.69

Name: rollingstone.com

Address: 151.101.128.69

Name: rollingstone.com

Address: 151.101.0.69

Used ssh to get into the server and found the host DNS entries. Both ssh and DNS (and nslookup) works at application layer.

**Step 4**

**ssh** [**jimi@167.172.144.11**](mailto:jimi@167.172.144.11)

**password**

cd /etc

ls -l

drwxr-xr-x 2 root root 4096 Oct 15 2019 opt

lrwxrwxrwx 1 root root 21 Sep 8 2019 os-release -> ../usr/lib/os-release

**-rw-r--r-- 1 root root 112 Mar 18 2020 packetcaptureinfo.txt**

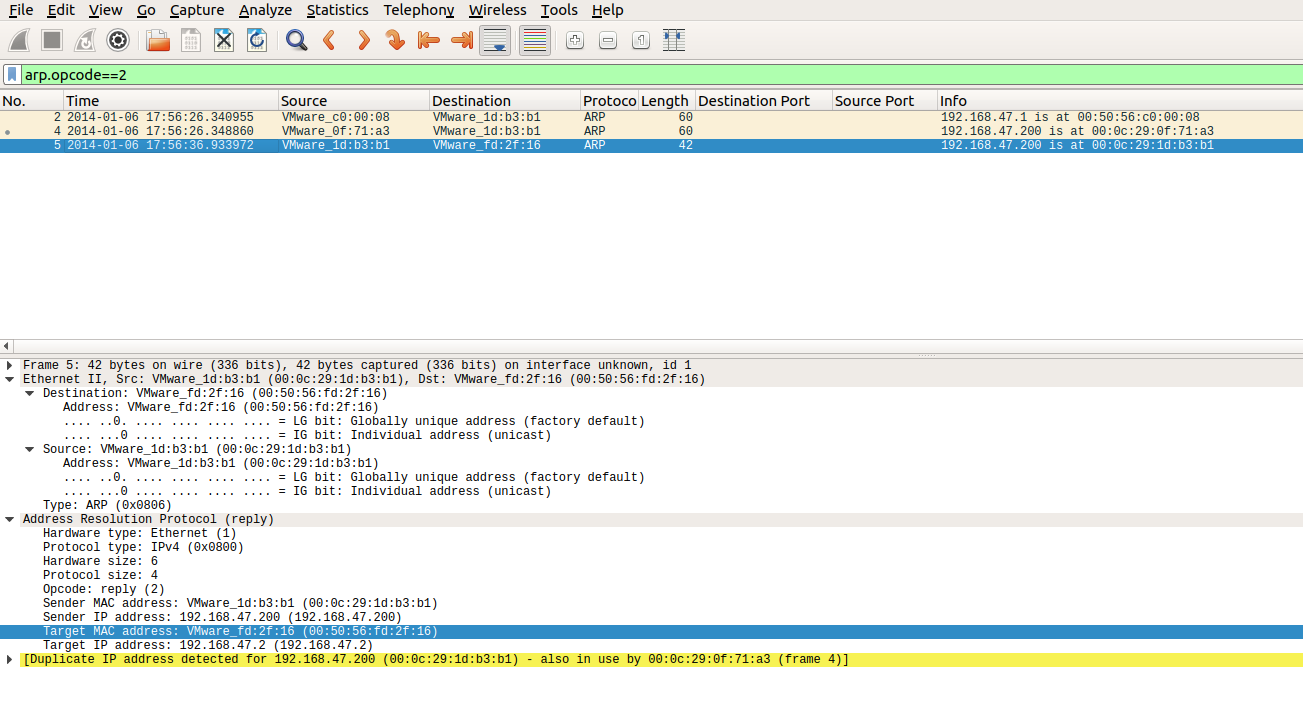
-rw-r--r-- 1 root root 552 May 27 2017 pam.conf

$ **cat packetcaptureinfo.txt**

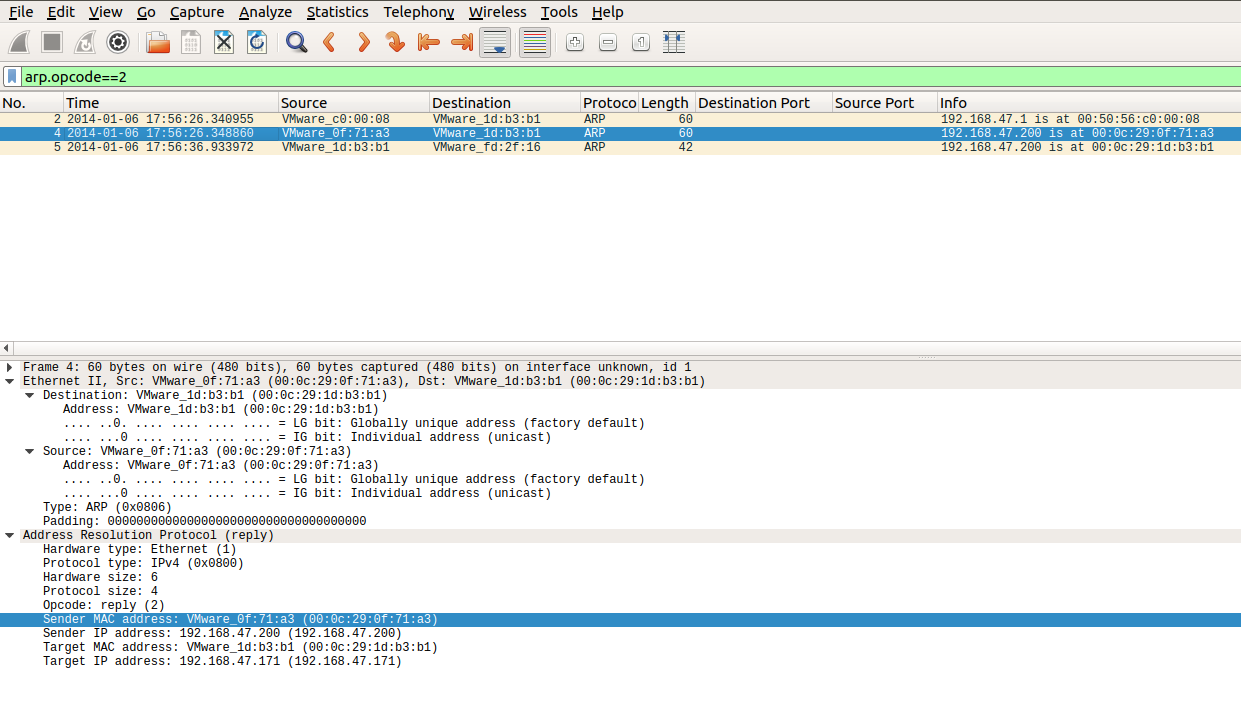
Captured Packets are here:

<https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>

Packet cap file analysis shows there was a duplicate IP address 192.168.47.200



Capture shows the IP 192.168.47.2 in use by mac address VMWare\_1d:b3:b1 (00:0c:29:1d:b3:b1) was also used by VMWare\_0f:71:a3 (00:0c:29:0f:71:a3). The suspected MAC address in this case is (00:0c:29:1d:b3:b1).



sysadmin@UbuntuDesktop:~$ nslookup gottheblues.yolasite.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: gottheblues.yolasite.com

**Address: 104.16.159.215**

**Name: gottheblues.yolasite.com**

Address: 104.16.162.215

Name: gottheblues.yolasite.com

Address: 104.16.163.215

Name: gottheblues.yolasite.com

Address: 104.16.160.215

Name: gottheblues.yolasite.com

Address: 104.16.161.215

Name: gottheblues.yolasite.com

Address: 2606:4700::6810:a3d7

Name: gottheblues.yolasite.com

Address: 2606:4700::6810:a0d7

Name: gottheblues.yolasite.com

Address: 2606:4700::6810:a1d7

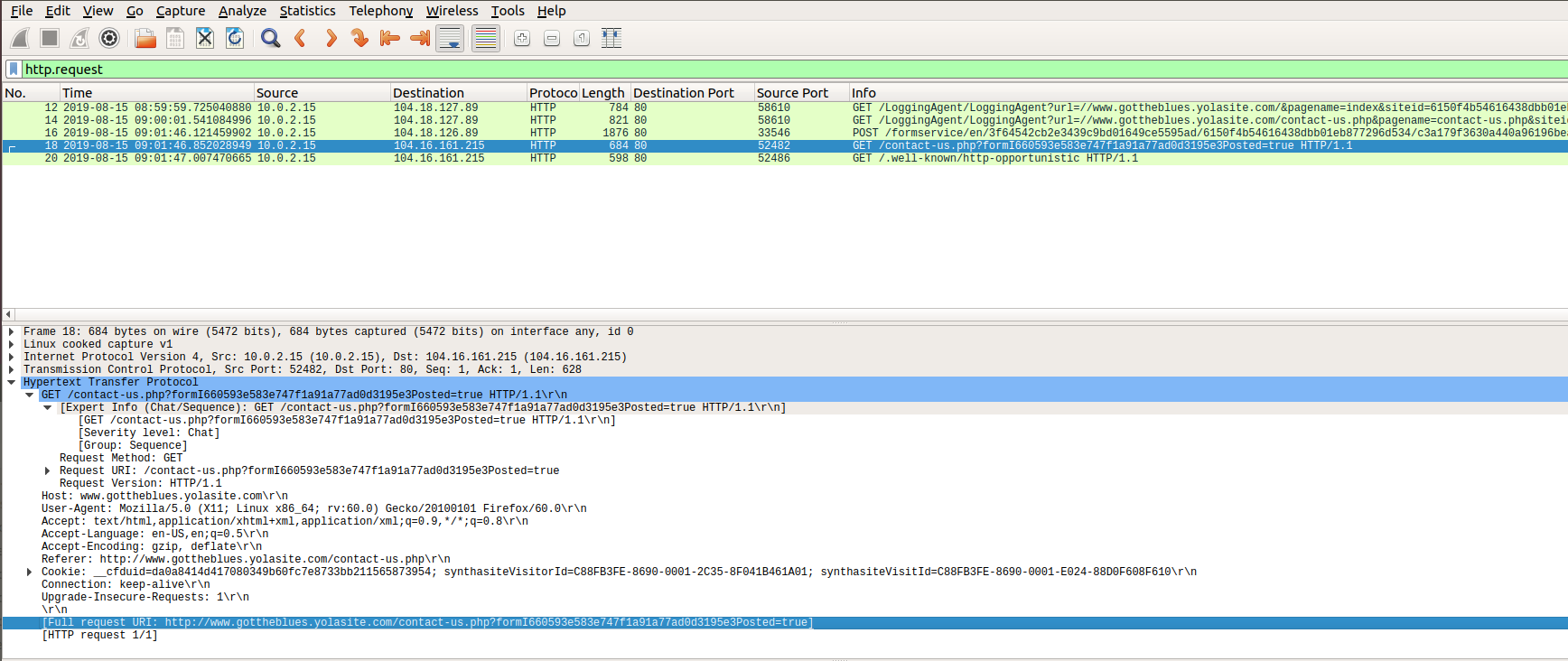
Name: gottheblues.yolasite.com

Address: 2606:4700::6810:9fd7

Name: gottheblues.yolasite.com

Address: 2606:4700::6810:a2d7

Nslookup shows gottheblues.yolasite.com has an IP address 104.16.162.215. Pcap shows it was directed to another IP address 104.18.127.89. This means hacker redirected all http requests to his own server (104.18.127.89).



Immediate Actions to be taken to secure the network.

**Actions:**

1. Change the password.
2. Close ssh port or set ssh port accepting connection from an authorized (e.g., Jump server or certain Terminal Serer) host.
3. Change the host file and setup monitoring of hosts file modification.
4. If WIFI is in use, set to WPA2 and/or strong password.
5. WIFI users shall be in separate vlans
6. Servers should be behind firewalls. Firewalls must be locked to allow certain port/protocols and knows/trusted source.
7. Put servers in different vrfs than clients and route traffic from clients or non-servers vrf through IPS/FW and enforce security policies.
8. Check all the users especially when they make system wide changes like DNS/hosts file, admin/root account used etc.