

16	15.199.95.91/28		Hollywood Database Servers
17	15.199.94.91/28		Hollywood Web Servers
18	11.199.158.91/28		Hollywood Web Servers
19	167.172.144.11/32		Hollywood Application Servers
20	11.199.141.91/28		Hollywood Application Servers

Phase 1.

Found “167.172.144.11 is alive” and can be fping’d. The other 4 IP addresses in red were “unreachable”. This would affect layer 3 Network due to certain IP address being able to be ping’d and the other IPs being unreachable. This vulnerability could be prevented by restricting the ICMP echo requests to all servers

Phase 2.

```
sysadmin@UbuntuDesktop:~$ nmap 167.172.144.11 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:15 EST
Nmap scan report for 167.172.144.11
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
```

Performed command nmap 167.172.144.11 -Pn and found “port 22/tcp open ssh”. This would affect layer 4:Transport because it puts data onto the network and assigns source and destination ports. This vulnerability could be prevented by closing port 22.

Phase 3.

```
$ 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

oooooooooollowing 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

$ █

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

oritative answers can be found from:
```

This will affect the Layer 7 application the IP address that is being requested is being sent to a different address from the browser. This vulnerability could be prevented by resetting the default user and password and limiting sudo access so files cant be edited.

Phase 4.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
19	176825120.62...	104.16.161.215	10.0.2.15	HTTP	3655	Continuation
20	176825120.66...	10.0.2.15	104.16.161.215	HTTP	598	GET /.well-known/http-opportunistic HTTP
12	176825013.38...	10.0.2.15	104.18.127.89	HTTP	784	GET /LoggingAgent/LoggingAgent?url=//www
14	176825015.20...	10.0.2.15	104.18.127.89	HTTP	821	GET /LoggingAgent/LoggingAgent?url=//www
18	176825120.51...	10.0.2.15	104.16.161.215	HTTP	684	GET /contact-us.php?formI660593e583e747f
13	176825013.45...	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascri
15	176825015.23...	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascri
17	176825120.47...	104.18.126.89	10.0.2.15	HTTP	420	HTTP/1.1 303 See Other
Terminal	176825119.78...	10.0.2.15	104.18.126.89	HTTP	1876	POST /formservice/en/3f64542cb2e3439c9bd

Frame 16: 1876 bytes on wire (15008 bits), 1876 bytes captured (15008 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.126.89

Transmission Control Protocol, Src Port: 33546, Dst Port: 80, Seq: 1, Ack: 1, Len: 1820

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "0<text>" = "Mr Hacker"
- Form item: "0<label>" = "Name"
- Form item: "1<text>" = "Hacker@rockstarcorp.com"
- Form item: "1<label>" = "Email"
- Form item: "2<text>" = ""
- Form item: "2<label>" = "Phone"
- Form item: "3<textarea>" = "Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has"
- Form item: "3<label>" = "Message"
- Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3P"
- Form item: "locale" = "en"
- Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d31"
- Form item: "form name" = ""

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_1d:b3:b1	Broadcast	ARP	42	Who has 192.168.47.1? Tell 192.168.47.1
2	0.000082	VMware_c0:00:08	VMware_1d:b3:b1	ARP	60	192.168.47.1 is at 00:50:56:c0:00:08
3	0.007909	VMware_1d:b3:b1	Broadcast	ARP	42	Who has 192.168.47.200? Tell 192.168.47.200
4	0.007987	VMware_0f:71:a3	VMware_1d:b3:b1	ARP	60	192.168.47.200 is at 00:0c:29:0f:71:a3
5	10.593099	VMware_1d:b3:b1	VMware_fd:2f:16	ARP	42	192.168.47.200 is at 00:0c:29:1d:b3:b1

Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1

Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)

Address Resolution Protocol (reply)

[Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]

- [Frame showing earlier use of IP address: 4]
- [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]
 - [Duplicate IP address configured (192.168.47.200)]
 - [Severity level: Warning]
 - [Group: Sequence]

[Seconds since earlier frame seen: 10]

This will affect layer 2 datalink because the ARP is being spoofed. This vulnerability could be prevented by setting up static ARP entries as well as RockstarCorp purchasing Host Intrusion Prevention software to detect if an ARP was spoofed. It would also be advised to find the owner of 00:0c:29:1d:b3:b1 and find the source of 10.0.2.15 that caused the redirect.