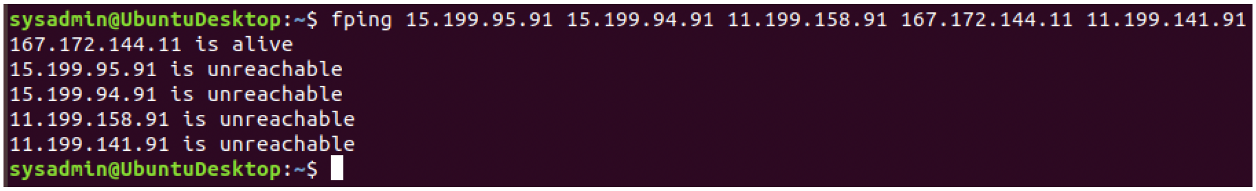
Phase 1

1. Command: fping 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91
    a. Results showed that the only IP address alive in the Hollywood office was 167.172.144.11, the rest were unreachable

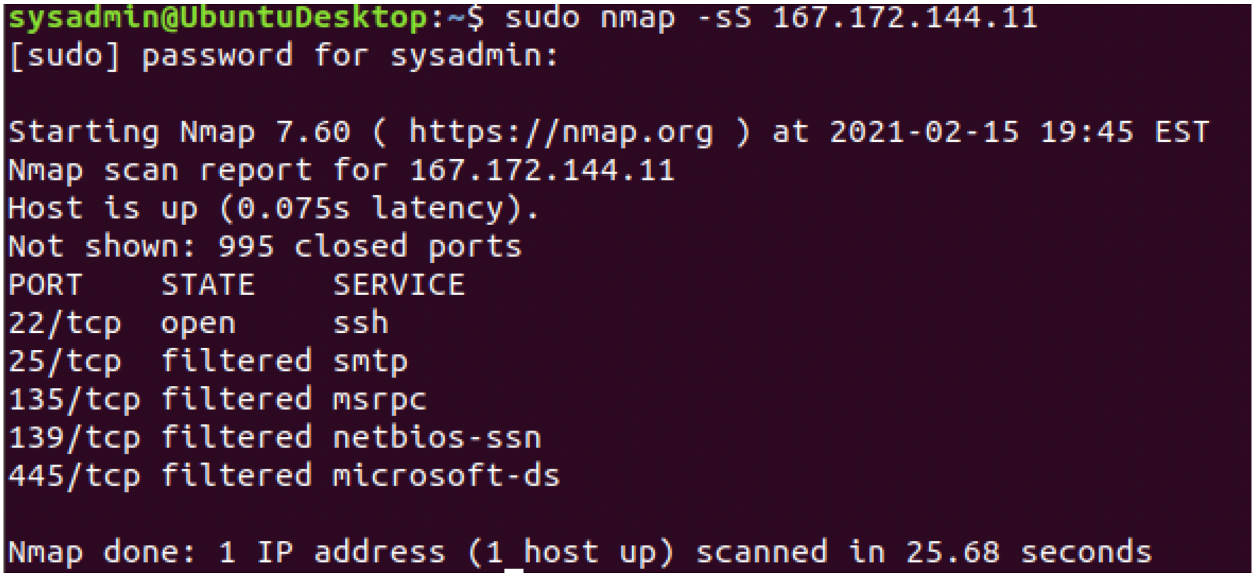


```
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91
167.172.144.11 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
sysadmin@UbuntuDesktop:~$
```

2. Vulnerabilities
    a. No vulnerabilities in phase 1
3. Findings Associated to the Hacker
    a. No findings associated to a hacker yet
4. Mitigation Recommendations
    a. If these other IP addresses that are unreachable are important, the company will want to get them back online by investigating the IP address settings and verifying the connections
5. OSI Layer
    a. Layer 3- Network. IP addresses take place in the network layer.

Phase 2

1. Command: sudo nmap -sS 167.172.144.11
    a. The command used sudo because we needed root privileges to run a syn scan to detect the open ports. Results showed that port 22, an ssh port, was open.



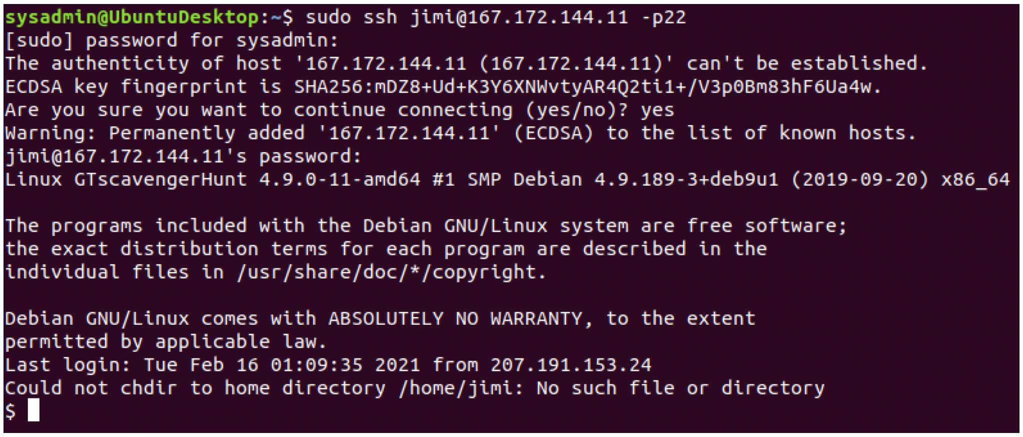
```
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-02-15 19:45 EST
Nmap scan report for 167.172.144.11
Host is up (0.075s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 25.68 seconds
```

2. Vulnerabilities
    a. Port 22 is open and this is a vulnerability

3. Findings Associated to the Hacker
    a. No signs of a hacker yet
4. Mitigation Recommendations
    a. Close the port
5. OSI Layer
    a. Layer 4: Transport. Source and destination ports are assigned on this level.

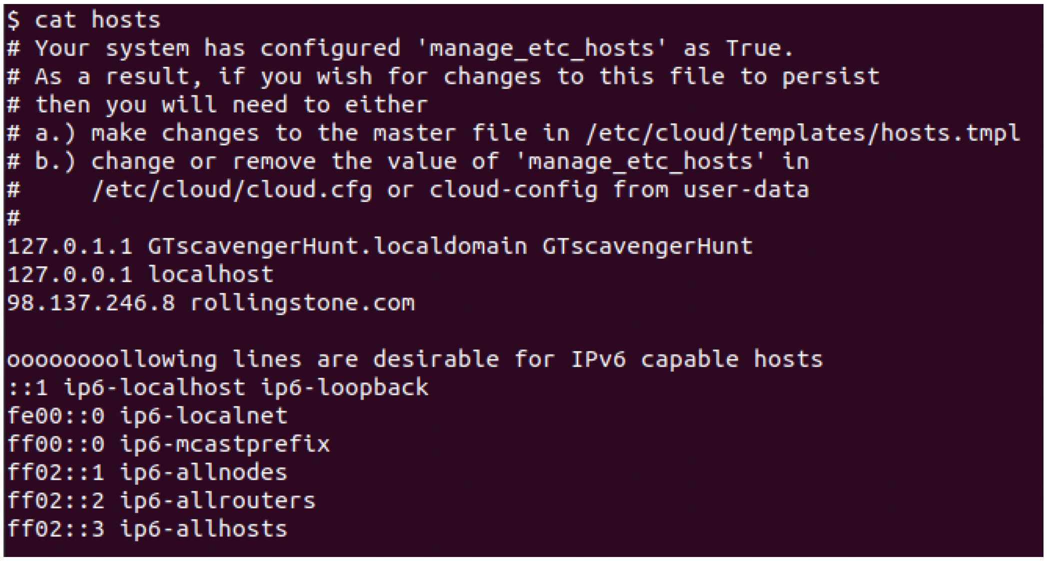
Phase 3

1. Command
    a. sudo ssh jimi@167.172.144.11 -p22
        i. This will allow us to get into port 22 through the jimi login



```
sysadmin@UbuntuDesktop:~$ sudo ssh jimi@167.172.144.11 -p22
[sudo] password for sysadmin:
The authenticity of host '167.172.144.11 (167.172.144.11)' can't be established.
ECDSA key fingerprint is SHA256:mDZ8+Ud+K3Y6XNWvtyAR4Q2ti1+/V3p0Bm83hF6Ua4w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '167.172.144.11' (ECDSA) to the list of known hosts.
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: Tue Feb 16 01:09:35 2021 from 207.191.153.24
Could not chdir to home directory /home/jimi: No such file or directory
$ 
```

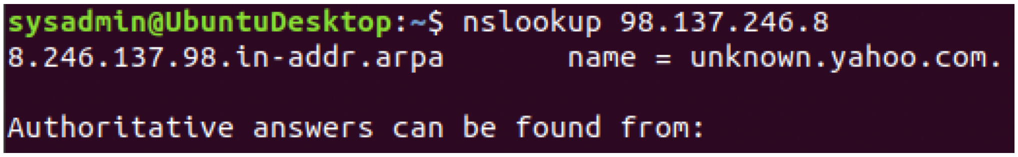
    b. cd /etc; cat hosts
        i. This will show us the IP address for rollingstone.com



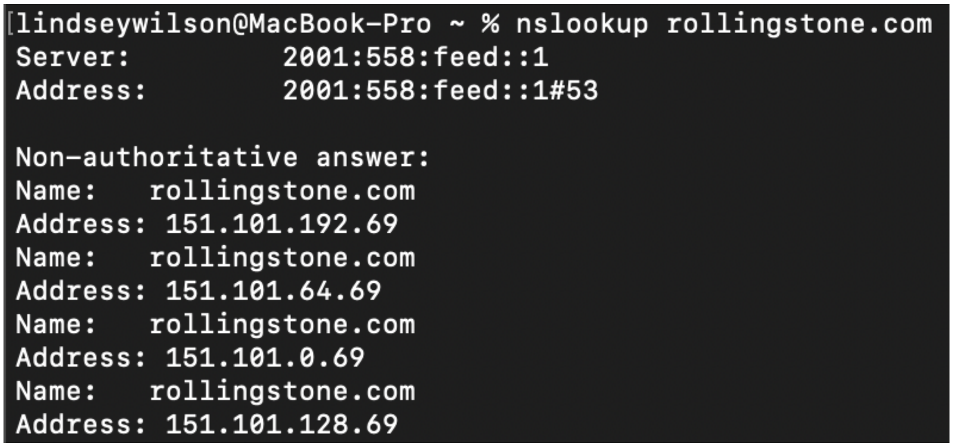
```
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /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

ooooooooollowing 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
```

    c. nslookup 98.137.246.8
        i. This shows that when employees go to rollingstone.com, they are actually being redirected to unknown.yahoo.com

ii. When using nslookup on rollingstone.com it shows the correct IP address for rollingstone.com



```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:
```

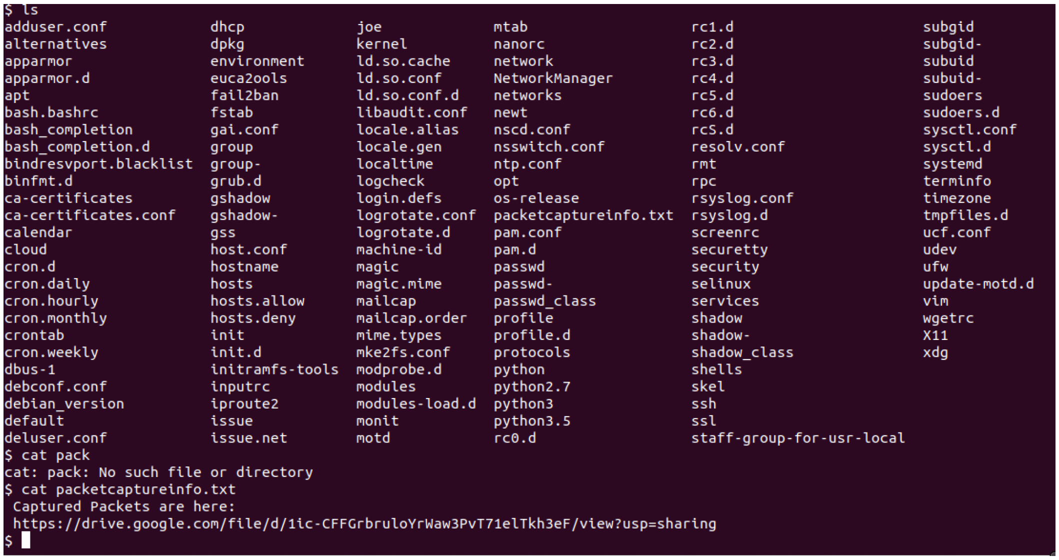


```
[lindseywilson@MacBook-Pro ~ % nslookup rollingstone.com
Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
Name:   rollingstone.com
Address: 151.101.192.69
Name:   rollingstone.com
Address: 151.101.64.69
Name:   rollingstone.com
Address: 151.101.0.69
Name:   rollingstone.com
Address: 151.101.128.69
```

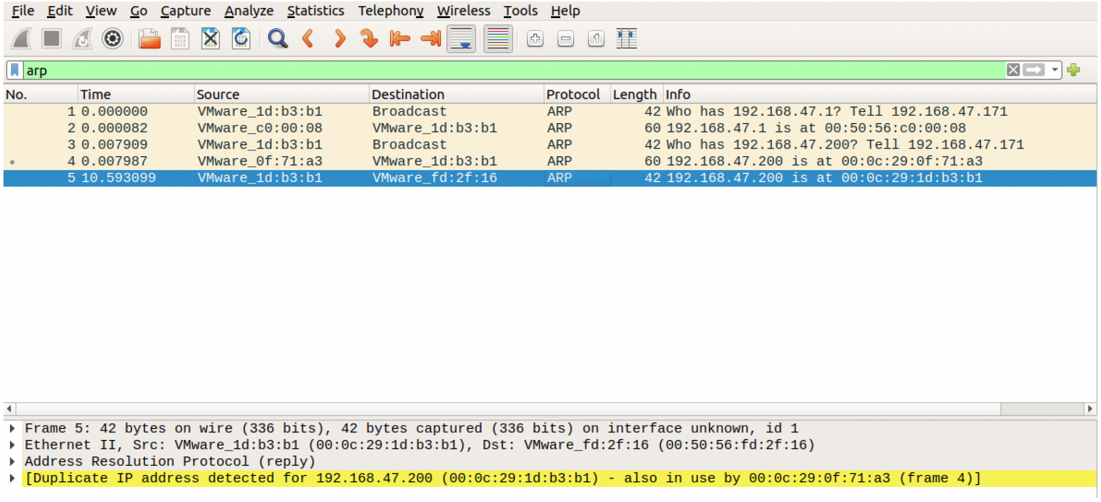
2. Vulnerabilities
    a. The first vulnerability is that multiple people use the jimi login, which means it would be hard to track who changed the IP address to be redirected to a different site. The second vulnerability is that anyone logged into jimi can open and change the hosts file.
3. Findings Associated to the Hacker
    a. The hacker redirected rollingstone.com to a bad site.
4. Mitigation Recommendations
    a. Don't allow everyone access to the jimi login credentials. Lock down the hosts file.
5. OSI Layer
    a. Layer 3- Network. The changing of IP address takes place on the network layer.
    b. Layer 7- Application. When employees interact with rollingstone.com they don't get the correct website.

Phase 4

1. Command: ssh into jimi again (sudo ssh jimi@167.172.144.11 -p22), then move into /etc file (cd /etc), then do an ls, view the packetcaptureinfo.txt (cat packetcaptureinfo.txt)
    a. This shows a google drive link with the pcap



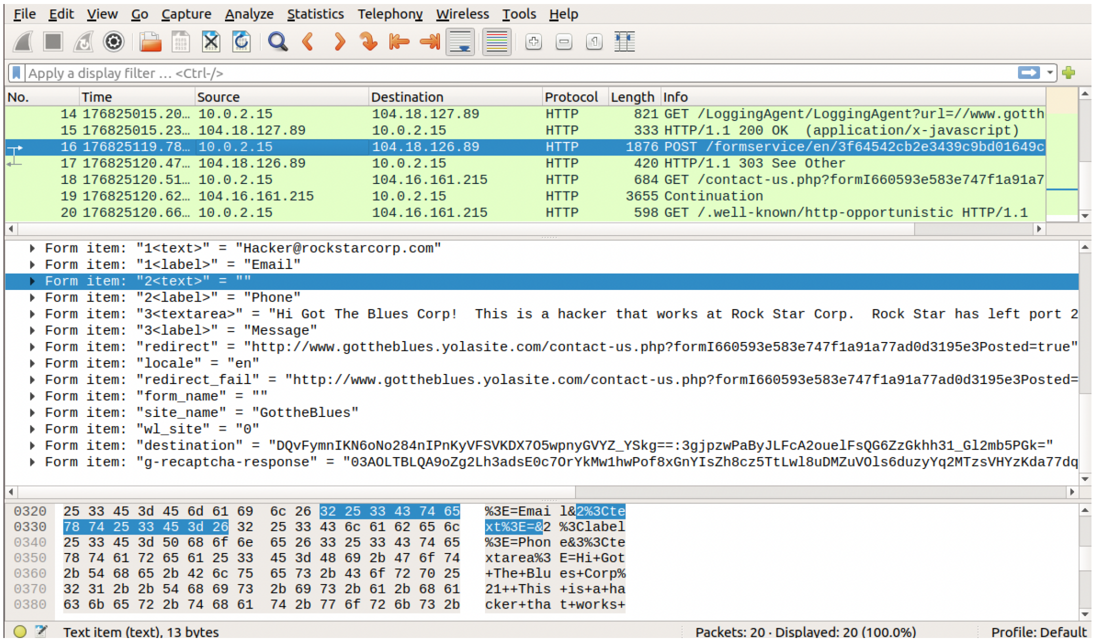
```
$ ls
adduser.conf            dhcp             joe             mtab                   rc1.d                      subgid
alternatives            dpkg             kernel          nanorc                 rc2.d                      subgid-
apparmor                environment      ld.so.cache     network                rc3.d                      subuid
apparmor.d              euca2ools        ld.so.conf      NetworkManager         rc4.d                      subuid-
apt                     fail2ban         ld.so.conf.d    networks               rc5.d                      sudoers
bash.bashrc             fstab            libaudit.conf   newt                   rc6.d                      sudoers.d
bash_completion         gai.conf         locale.alias    nscd.conf              rcS.d                      sysctl.conf
bash_completion.d       group            locale.gen      nsswitch.conf          resolv.conf                sysctl.d
bindresvport.blacklist  group-           localtime       ntp.conf               rmt                        systemd
binfmt.d                grub.d           logcheck        opt                    rpc                        terminfo
ca-certificates         gshadow          login.defs      os-release             rsyslog.conf               timezone
ca-certificates.conf    gshadow-         logrotate.conf  packetcaptureinfo.txt  rsyslog.d                  tmpfiles.d
calendar                gss              logrotate.d     pam.conf               screenrc                   ucf.conf
cloud                   host.conf        machine-id      pam.d                  securetty                  udev
cron.d                  hostname         magic           passwd                 security                   ufw
cron.daily              hosts            magic.mime      passwd-                selinux                    update-motd.d
cron.hourly             hosts.allow      mailcap         passwd_class           services                   vim
cron.monthly            hosts.deny       mailcap.order   profile                shadow                     wgetrc
crontab                 init             mime.types      profile.d              shadow-                    X11
cron.weekly             init.d           mke2fs.conf     protocols              shadow_class               xdg
dbus-1                  initramfs-tools  modprobe.d      python                 shells
debconf.conf            inputrc          modules         python2.7              skel
debian_version          iproute2         modules-load.d  python3                ssh
default                 issue            monit           python3.5              ssl
deluser.conf            issue.net        motd            rc0.d                  staff-group-for-usr-local
$ cat pack
cat: pack: No such file or directory
$ cat packetcaptureinfo.txt
 Captured Packets are here:
 https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
$ 
```



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 192.168.47.171 |
| 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 192.168.47.171 |
| 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)]
```



```
No.    Time             Source          Destination      Protocol Length Info
    14 176825015.20…   10.0.2.15       104.18.127.89    HTTP      821 GET /LoggingAgent/LoggingAgent?url=//www.gotth
    15 176825015.23…   104.18.127.89   10.0.2.15        HTTP      333 HTTP/1.1 200 OK  (application/x-javascript)
    16 176825119.78…   10.0.2.15       104.18.126.89    HTTP     1876 POST /formservice/en/3f64542cb2e3439c9bd01649c
    17 176825120.47…   104.18.126.89   10.0.2.15        HTTP      420 HTTP/1.1 303 See Other
    18 176825120.51…   10.0.2.15       104.16.161.215   HTTP      684 GET /contact-us.php?formI660593e583e747f1a91a7
    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/1.1
```

```
  ▸ 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 left port 2
  ▸ Form item: "3<label>" = "Message"
  ▸ Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
  ▸ Form item: "locale" = "en"
  ▸ Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=
  ▸ Form item: "form_name" = ""
  ▸ Form item: "site_name" = "GottheBlues"
  ▸ Form item: "wl_site" = "0"
  ▸ Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31_Gl2mb5PGk="
  ▸ Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dq
```

```
0320  25 33 45 3d 45 6d 61 69  6c 26 32 25 33 43 74 65   %3E=Emai l&2%3Cte
0330  78 74 25 33 45 3d 26 32  25 33 43 6c 61 62 65 6c   xt%3E=&2 %3Clabel
0340  25 33 45 3d 50 68 6f 6e  65 26 33 25 33 43 74 65   %3E=Phon e&3%3Cte
0350  78 74 61 72 65 61 25 33  45 3d 48 69 2b 47 6f 74   xtarea%3 E=Hi+Got
0360  2b 54 68 65 2b 42 6c 75  65 73 2b 43 6f 72 70 25   +The+Blu es+Corp%
0370  32 31 2b 2b 54 68 69 73  2b 69 73 2b 61 2b 68 61   21++This +is+a+ha
0380  63 6b 65 72 2b 74 68 61  74 2b 77 6f 72 6b 73 2b   cker+tha t+works+
```

Text item (text), 13 bytes    Packets: 20 · Displayed: 20 (100.0%)    Profile: Default

2. Vulnerabilities
    a. The first vulnerability is that the hacker had access to hide pcap files.
3. Findings Associated to the Hacker
    a. The hacker spoofed MAC addresses. He also left an email thread stating that he's a hacker and works at Rock Star Corp.
4. Mitigation Recommendations
    a. Restrict access to the jimi credentials.
5. OSI Layer
    a. Layer 2- Data Link. Wireshark decodes packets at the data link layer.