**Phase 1**: Id like to teach the world to ping  
Commands:

fping -g 15.199.95.91/28 - unreachable

fping -g 15.199.94.91/28 - unreachable

fping -g 11.199.158.91/28 - unreachable

fping -g 167.172.144.11/32 - Live

fping -g 11.199.141.91/28 - unreachable

Summary: after fpinging the hollywood IP’s, only one IP received packets which was 167.172.144.11/32 .this is an indication of malicious activity as the hacker as gained access to the servers and opened the port to be able to remotely access. This can be prevented by network scanning and logging, disabling pinging, and adding additional vpn layers to the company’s application servers

The OSI layer for pinging happens on the Network Layer (third layer).

**Phase 2:**

Command: nmap -sS 167.172.144.11

The results that came back were  
  
Nmap scan report for 167.172.144.11

Host is up (0.24s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open ssh

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

593/tcp filtered http-rpc-epmap

646/tcp filtered ldp

What we can see here is that only the ssh port is open while the rest are filtered; Filtered ports just means that only specific machines are able to access these ports. Having an open ssh port is very dangerous for the company as it allows hackers to easily remote into their systems. The best way to remedy this is to either filter the port so only certain machines can access that port or increase firewall provisioning.

The layer that this happens on is the transport layer (Layer 4)

**Phase 3:**

Commands:

Sudo ssh jimi@167.172.144.11 -p 22

Cat /etc/hosts

Nslookup 98.137.246.8

The results we get when we check the host file is: 98.137.246.8 rollingstone.com

The results from the nslookup is: 8.246.137.98.in-addr.arpa unknown.yahoo.com

Summary: As we can see there is definitely some malicious activity happening. Someone had altered the etc/hosts file to redirect the user from rollingstones to another domain. When we use the nslookup tool we can confirm that the IP addresses are not the same which is a tell that something isn't right.

The layer that this is happening on is the Network Layer (layer 3)

**Phase 4:**

Found a file in /etc called packetcaptureinfo.txt and inside that was a link to secretlogs.pcap file   
  
Command: cat /etc/packetcaptureinfo.txt  
  
Results : https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing

Summary:   
  
After analyzing the packet capture, I have noticed that packets 4 and 5 using the ARP protocol the IP 192.168.47.200 are directing traffic to TWO MAC addresses. Also in another packet the hackers tries to contact [www.gottheblues.com](http://www.gottheblues.com) and sends them the message

“Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Milliion Dollars I will provide you the user and password!”

So no doubt there is some malicious activity going on. Rockstar corp should monitor their network traffic more thoroughly and to update their firewall settings to diable unauthorized traffic from the ssh port and to always check the hosts file to make sure there is no redirections.  
  
The Layer this happens on is the Network layer( layer 3)