Phase 1

```
sysadmin@UbuntuDesktop:~$ fping -g 15.199.95.91/24 >> ~/Homework/
HollywoodDB.txt
sysadmin@UbuntuDesktop:~$ fping -g
 15.199.94.91/24 >> ~/Homework/HollywoodWeb1.txt
**Findings: No hosts responsive**
sysadmin@UbuntuDesktop:~$ fping -g 11.199.158.91/28 >> ~/Homework/
HollywoodWeb2.txt
**Findings: No hosts responsive**
sysadmin@UbuntuDesktop:~$ fping -g 167.172.144.11/32 >> ~/Homework/
HollywoodApp1.txt

**Findings: One host responsive @ 167.172.144.11 OSI Layer: 3, Network**
sysadmin@UbuntuDesktop:~$ fping -g 11.199.141.91/28 >> ~/Homework/
HollywoodApp2.txt
**Findings: No hosts responsive**

**Summary: 537 total hosts scanned, 536 unresponsive, 1 responsive**
```

Out of 537 IP addresses scanned in the provided subnets, one (167.172.144.11) returned a response using fping with the -g argument (Generate target list from IP netmask).

Phase 2: *"Some Syn for Nothin`"*

```
Nmap scan report for 167.172.144.11
Host is up (0.035s 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
```

Findings: One open port (22) @ 167.172.144.11
The syn scan corresponds to the Transport Layer of the OSI model
As a result, system SSH is accessible for potential exploitation. Possible remediation of this issue is to configure the SSH daemon to install a program like Knockd to enable port knocking and reconfiguring default SSH port so it is not accessible without port knocking. Another layer of remediation would be to require use of SSH Key-based authentication

Phase 3: *"I Feel a DNS Change Comin' On"*

```
**nano /etc/hosts**
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com
```

```
nslookup rollingstone.com
```

```
Server:        8.8.8.8
Address:    8.8.8.8#53

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

```
nslookup 98.137.246.8
8.246.137.98.in-addr.arpa    name = unknown.yahoo.com.
```

Findings: The local machine DNS was modified through /etc/hosts to spoof IP resolution to a unrelated site. This corresponds to Level 3 Network Layer in the OSI Model. NSLookup was used to determine correct IP resolution for domain as NSLookup ignores /etc/hosts DNS resolution. DNS functions at the OSI Application Layer level 7. An NSLookup query was also done to resolve the domain name for the IP address provided in /etc/hosts corresponding to unknown.yahoo.com. Remediation of this spoofing would resolve removing the entry in /etc/hosts/ for rollingstone.com

Phase 4: *"ShARP Dressed Man"*

```
cat packetcaptureinfo.txt
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
```

Finding: hacker@rockstarcorp.com posted a form contact message outlining the open port for rockstarcorp to Got The Blues Corp with an offer of providing a username/ password in exchange for $1 million.
The post request corresponds to the 7th Application layer in the OSI model
The initial ARP request to determine IP resolution belongs to the 3rd Network Layer in the OSI model. Remediation of this issue would be centered around forcing credential changes for accounts present on rockstarcorp machine to prevent future sale of credentials