Phase 1: ***"I'd like to Teach the World to Ping"***

You have been provided a list of network assets belonging to RockStar Corp. Use fping to ping the network assets for only the Hollywood office.

- Determine the IPs for the Hollywood office and run fping against the IP ranges in order to determine which IP is accepting connections.
    - Download fping first: sudo apt install fping
- Next fping the ipaddress ranges:
- fping -g 15.199.95.91/28
- fping -g 15.199.94.91/28
- fping -g 11.199.158.91/28
- fping -g 167.172.144.11/32
- fping -g 11.199.141.91/28

  15.199.95.91/28 unreachable

  15.199.94.91/28 unreachable

  11.199.158.91/28 unreachable

  167.172.144.11/32 is alive

  11.199.141.91/28 unreachable

- 167.172.144.11 (Hollywood Application Servers) is alive and vulnerable and can put the company at risk of unauthorized access.
- fping -s -g 167.172.144.11/32
- Your summary should determine which IPs are accepting connections and which are not.
  An active IP address and open port provide for the possibility of a DoS attack or DNS hijacking.
- Also indicate at which OSI layer your findings are found.
  OSI Layer 3: Network

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

- **List the steps and commands used to complete the tasks**
    - **Ran a SYN SCAN against the IP address that is alive**
      sudo nmap -sS 167.172.144.11/32 OR
    - **port 22/tcp ssh is open and should be closed**
    - **The fact that the port is open is suspicious, but it doesn't prove that it's associated to a hacker**
    - **Close the port so that no one is able to ssh into the system**
    - **OSI Layer 4: Transport.**

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

With your findings from Phase 2, determine if you can access the server that is accepting connections.

- We know that port 22 is open on the 167.172.144.11 (Hollywood Application Servers) Server and that RockStar typically uses the same default username and password for most of their servers.
    - Therefore we'll run: sudo ssh jimi@167.172.144.11 -p22
    - Password: hendrix
- ls
- cd etc
- ls
- cat hosts

    See this information:

    127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt

    127.0.0.1 localhost

    98.137.246.8 rollingstone.com

- Next run nslookup 98.137.246.8
- They should not have the same user and password for their servers
- Hijacked the dns – ip address is going to a different site than it should
- The hacker hijacked the DNS and changed the host file to send us to a different website
- Reset the IP address to your preferred setting first. We must block port 22 and make the alive IP address unavailable because the open port allowed the hacker to change his IP.
- Add DNS filter
- OS Layer 7: Application Layer

Phase 4: ***"ShARP Dressed Man"***

Within the RockStar server that you SSH'd into, and in the same directory as the configuration file from **Phase 3**, the hacker left a note as to where he stored away some packet captures.

Provide the following for each phase:

- List the steps and commands used to complete the tasks.
    - sudo ssh jimi@167.172.144.11 -p22
    - ls
- cat packetcaptureinfo.txt

- Now I see “Captured Packets are here” with the googledrive link.
- I copied that link (https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing) and I opened the file in Wireshark
- Run http.request.method =="GET"
- Run http.request.method =="POST"
- Run arp
- OSI Layer 7: Application Layer