nmap = network mapper – network security and activity auditing

1. Ports and Services:

```
(base) jonathan@Jonathans-MacBook-Pro ~ % nmap 34.135.30.242
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 17:27 EST
Nmap scan report for 242.30.135.34.bc.googleusercontent.com (34.135.30.242)
Host is up (0.057s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
443/tcp  closed https
3389/tcp closed ms-wbt-server
7777/tcp open   cbt

Nmap done: 1 IP address (1 host up) scanned in 43.89 seconds
(base) jonathan@Jonathans-MacBook-Pro ~ %
```

2. No, the target is not running a web server, as both the http and https protocols are closed.
    a. I confirmed this by attempting to navigate to http:// 34.135.30.242 and https:// 34.135.30.242 on a web browser (Chrome) and could not establish a connection.
3. No, the target is not running a database server.
4. OS
    a. OS: Linux
    b. Distribution: linux_kernel
5. Peculiar Port

The strange port service is CBT on port 7777. Upon connecting to it directly using `nc`, it outputs a large amount of what originally seemed to be encrypted characters to `stdout`, stopping after a few seconds of output. Then I realized it was likely a media file (and definitely not encryption). I ran `nc 34.135.30.242 7777 > output.txt` from terminal to desktop. Seeing one of the first lines read “Media file produced by Google, Inc.”, I searched for a list of Google media files and changed the desktop file’s extension until a video rendered with output.3gp. Playing this file shows a scene from *Stranger Things*.

6. Accessing Target

Seeing port 22 open, I tried `ssh`'ing in directly to the system with a random username, but received a host key error. Googling the issue, I found a flag[1] to utilize the given `ssh-rsa` flag. Then I `ssh`'d in using root as the username. I entered "password" as the password and was granted access. To modify the directory, I added a text file, `jonathan.txt`.

```
Nmap done: 1 IP address (1 host up) scanned in 54.36 seconds
(base) jonathan@Jonathans-MacBook-Pro ~ % ssh user@34.135.30.242
Unable to negotiate with 34.135.30.242 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
(base) jonathan@Jonathans-MacBook-Pro ~ % ssh user@34.135.30.242 -p 22
Unable to negotiate with 34.135.30.242 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
(base) jonathan@Jonathans-MacBook-Pro ~ % ssh user@34.135.30.242 -p 22 -o HostKeyAlgorithms=+ssh-rsa
user@34.135.30.242's password:
Permission denied, please try again.
user@34.135.30.242's password:

(base) jonathan@Jonathans-MacBook-Pro ~ % ssh root@34.135.30.242 -p 22 -o HostKeyAlgorithms=+ssh-rsa
root@34.135.30.242's password:

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.
root@vm-linux02:~# ls
root@vm-linux02:~# touch jonathan.txt
root@vm-linux02:~# ls
jonathan.txt
root@vm-linux02:~#
```

7. Open Ports (Shodan)

Open ports on 96.73.86.58 include 443 and 10001.

Looking at the information on port 10001, it looks to be a "Valero Food Mart" gas station/convenience store in Dickinson, TX near Houston.

8. NETGEAR Vulnerabilities

Searching "NETGEAR <model>" in SHODAN yields the following results:

Model	Count
NETGEAR R8000	600
NETGEAR R7000	2,132
NETGEAR R6400	1,240
Total	**3,972**

[1] https://unix.stackexchange.com/questions/699192/ssh-authentication-issue-with-openssh-private-key