nmap = network mapper – network security and activity auditing

1. Ports and Services:

A screenshot of a computer error

Description automatically generated

1. No, the target is not running a web server, as both the http and https protocols are closed.
   1. 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.
2. No, the target is not running a database server.
3. OS
   1. OS: Linux
   2. Distribution: linux\_kernel
4. 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*.

1. 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]](#footnote-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.

A screenshot of a computer program

Description automatically generated

1. 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.

1. 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 [↑](#footnote-ref-1)