Part-1-Using Nmap

1. Here the services and corresponding port numbers:

|  |  |
| --- | --- |
| SERVICE | PORT |
| ssh | 22 |
| http | 80 |
| https | 443 |
| irc | 6666 |

1. Yes, the target is running a web server.

2(a) A webserver is running on port 80. It is visible on the following url:

<http://35.231.141.75:80>

Software: nginx

Version Number # 1.10.3

1. I did not find any database on the server.
2. The operating System and Distribution target is running on:

**Device type:** WAP|general purpose

**Running:** Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012

**OS CPE:** cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux\_kernel cpe:/o:linux:linux\_kernel:2.4.37 cpe:/o:linux:linux\_kernel:3.2 cpe:/o:microsoft:windows\_xp::sp3 cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_server\_2012

**OS details:** Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012

**Network Distance:** 2 hops

**Service Info: OS:** Linux; CPE: cpe:/o:linux:linux\_kernel

1. Yes, there is a peculiar service on port 6666. I used the command:

nmap -A -T4 35.231.141.75 6666

and it identified that on port 6666 there is an unrecognized service running.

Using the command nc 35.231.141.75 6666 > output a jpeg is created which has a swimming pool with people swimming and it has something fishy/peculiar in it. Hence, the port has some peculiar service running.

1. I used the following command to get remote access to the server:

*ssh* [*root@35.231.141.75*](mailto:root@35.231.141.75)

And entered ***toor*** as the password.

Part-2-Without using Nmap

1. Open port: 47808

Target: Blackfoot Telephone Cooperative, Inc. (BTC-13)

1. Shodan showed the following figures:

NETGEAR R8000: 5849

NETGEAR 7000: 11630

NETGEAR 6400: 474