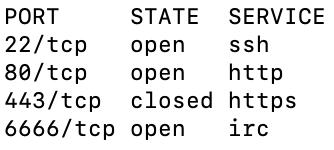
Part 1: Using Nmap

For questions 1 to 6, the target's IP address is 34.86.157.28. You are granted permission to attack this remote system.

**1. List the services and corresponding port number(s) that the target is running.**command: nmap 34.86.157.28  
****

**2. Is the target running a web server --YES or NO?**  
Yes

**2a. If the target is running web server software, how do you know? What web server software and version number is being used?**  
Web Service name is “http” and the status is open.   
Via command nmap -A -P0 34.86.157.28 we know that web software is nginx with version # 1.14.2

**3. Is the target running a database server of some kind --YES or NO?**No

**3a. If the target is running a database server, how do you know? What database server software and version number is being used?**N/A

**4. What operating system \*and\* distribution is the target (most likely) running?**Operating system is Linux with Debian distribution.  
nmap -O --osscan-limit 34.86.157.28   
  
*Output:* HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 3.1 (90%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (90%), Linux 3.7 (90%), Linux 5.0 (90%), Linux 5.1 (90%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%), Linux 2.6.32 - 3.13 (89%), Linux 3.0 - 3.2 (89%)

**5. There is a peculiar service running on this target.  What port number is this peculiar service?  What gives you the impression that this is a peculiar service?  What does this service do, provide?  NOTES: You must make a network connection to this peculiar service and determine what it does. Just looking up the service associated with the port number is not enough.**  
The peculiar service seems to be IRC at port 6666. When we use multiple commands to get more details (software or versions) on the service, nmap isn’t able to identify target service IRC port 6666. In return, nmap produces a fingerprint that can gives us clues on what this service can be. We can use command nc IP port to see what’s inside. Then I used string on the result before piping and scanning it to see what’s the inside and it was mp3.

**6. Gain remote access to the target. To put it more bluntly: break into the server, gain access, have permission to modify the filesystem! You have authorization to do so! Explain how you gained access to the target.**sudo ssh 34.86.157.28 with rsa public fingerprint key of kBmv4ZT969Wu4Y4SLE9MEO6DSB/alQ8ghUXft62ZGu4  
Then, I created an empty file “touch lab3.docx” and then I delete it afterwards vis shred command.

Part 2: Usage of Nmap Not Allowed!

**7. Here is a new target IP address: 97.73.176.234. \*\*\*\*\*Without using Nmap or directly accessing the target via IP address\*\*\*\*\*, determine the open ports of this target and what this target is.  Examples: Going to http://97.73.176.234/ , https://97.73.176.234/, ssh 97.73.176.234, are all NOT ACCEPTABLE!  Don't use ping. Don't use Netcat.**Port 1900 UPnP

Port 10001 automated-tank-gauge

Target is Hughes Network Systems (local gas station)

**8. NETGEAR R8000, R7000, and R6400 routers have known vulnerabilities. Using SHODAN, determine how many of them are (still) exposed on the Internet. An article from December 2016:**[**https://arstechnica.com/security/2016/12/unpatched-bug-allows-hackers-to-seize-control-of-netgear-routers/**](https://arstechnica.com/security/2016/12/unpatched-bug-allows-hackers-to-seize-control-of-netgear-routers/)

R8000: 1,748  
R7000: 2,308  
R6400: 266  
Total: 4,322 (\*\*\*the above number are keep changing\*\*\*)