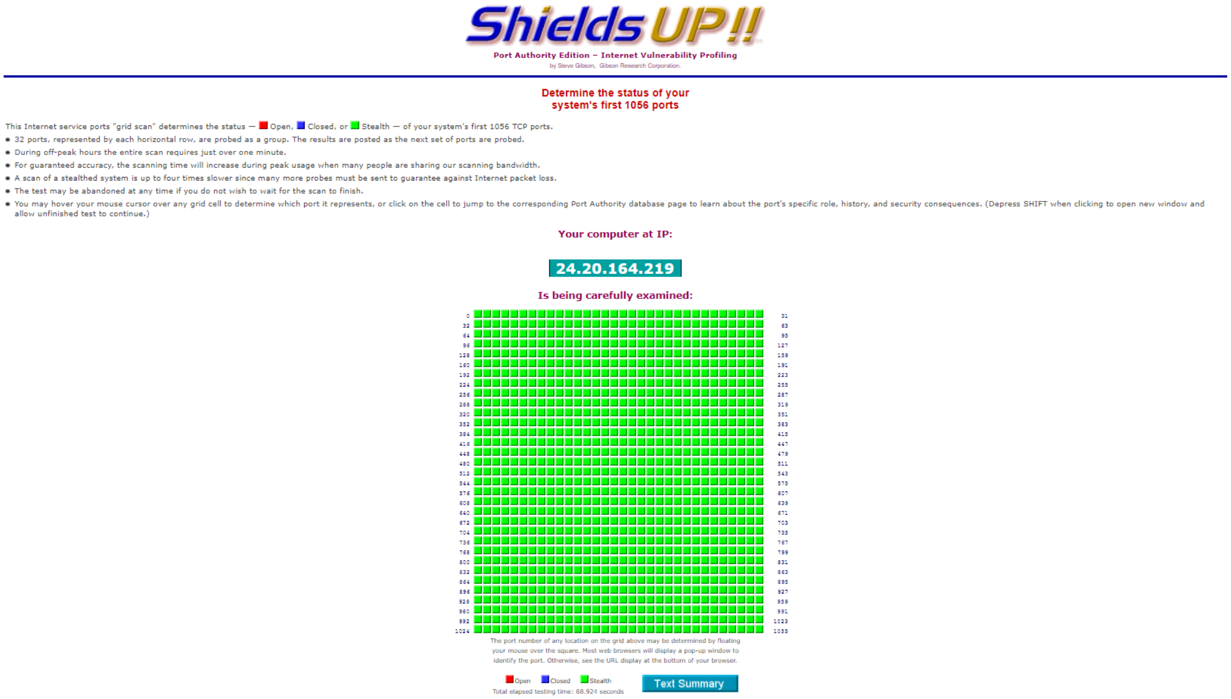
Morgan Bartlett
CIT 383
Phil Colbert
April 2021

Project 3

- Identify which ports are used for the following services. In addition to identifying the port number, also look up and provide a description of each service or activity.
    - SSH
        - Port number 22
        - Secure Shell Protocol (SSH) is used for remotely logging into a computer from a separate one. It's typically used in corporate settings where it can provide secure network access for users, allows users to execute remote commands, and can transfer files securely.
    - SMTP
        - Port number 25
        - Simple Mail Transfer Protocol (SMTP) is the method used for sending emails between servers. It is also the same protocol used for when a user is sending outgoing mail.
    - SQL Server
        - Port number 156
        - Structured Query Language (SQL) Server uses port 156 to communicate and respond to queries for database management systems.
    - SNMP
        - Port number 161
        - Simple Network Management Protocol (SNMP) allows for communication between devices on a network, even if they have different hardware or software.
- Identify which ports are used for the following services. Also note if the port is considered "Official" or "Unofficial."
    - MySQL database system
        - Port number 3306, "Official"
    - Discord
        - Port numbers 6463-6472, "Unofficial"
    - OpenVPN

        - Port number 1194, “Official”
    - Call of Duty
        - 28960, “Unofficial”
- In your own words, describe the difference between TCP and UDP
    - TCP and UDP both send packets of data over the Internet, but do it differently. TCP is more thorough where the sender will request from the recipient that the package arrived successfully. If it didn’t, then the sender will send that specific packet again. On the other hand, UDP lacks this error checking and will keep sending packets, even if some don’t arrive successfully. TCP is typically used more often as applications usually require strong and stable connections, but where speed is more of a concern, then one should use UDP instead.
- UDP is frequently used for gaming. Describe why. Describe also if using UDP over TCP raises potential security issues.
    - UDP is typically used for gaming because it’s having to deal with “real time.” For example, when moving a character around a space, you want to see that movement immediately and not have to wait for the network to check that all the packets containing the data to move that character have made it successfully. You want to constantly be up to date with the game’s current state, hence why it’s important to be using UDP. However, using UDP raises the risk of becoming susceptible to spoofing and DDOS attacks. This is because UDP is stateless, meaning the packets aren’t tracked and error-checked like TCP and are thus easier to spoof by hackers.
- Describe why TCP/IP ports range from 0 to 65535. You may have to recall facts you learned in CIS 110!
    - Because the number 65535 is the highest number that can be represented in a 16-bit value, which is how long ports were originally designed to be. If it were 32 bits, that would significantly increase the amount of ports and is way more than we technologically need.

- Use screen capture to record the results of your test, and include in your final deliverable



Shields UP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Determine the status of your system's first 1056 ports

This Internet service ports "grid scan" determines the status — 🟥 Open, 🟦 Closed, or 🟩 Stealth — of your system's first 1056 TCP ports.

- 32 ports, represented by each horizontal row, are probed as a group. The results are posted as the next set of ports are probed.
- During off-peak hours the entire scan requires just over one minute.
- For guaranteed accuracy, the scanning time will increase during peak usage when many people are sharing our scanning bandwidth.
- A scan of a stealthed system is up to four times slower since many more probes must be sent to guarantee against Internet packet loss.
- The test may be abandoned at any time if you do not wish to wait for the scan to finish.
- You may hover your mouse cursor over any grid cell to determine which port it represents, or click on the cell to jump to the corresponding Port Authority database page to learn about the port's specific role, history, and security consequences. (Depress SHIFT when clicking to open new window and allow unfinished test to continue.)

Your computer at IP:

24.20.164.219

Is being carefully examined:

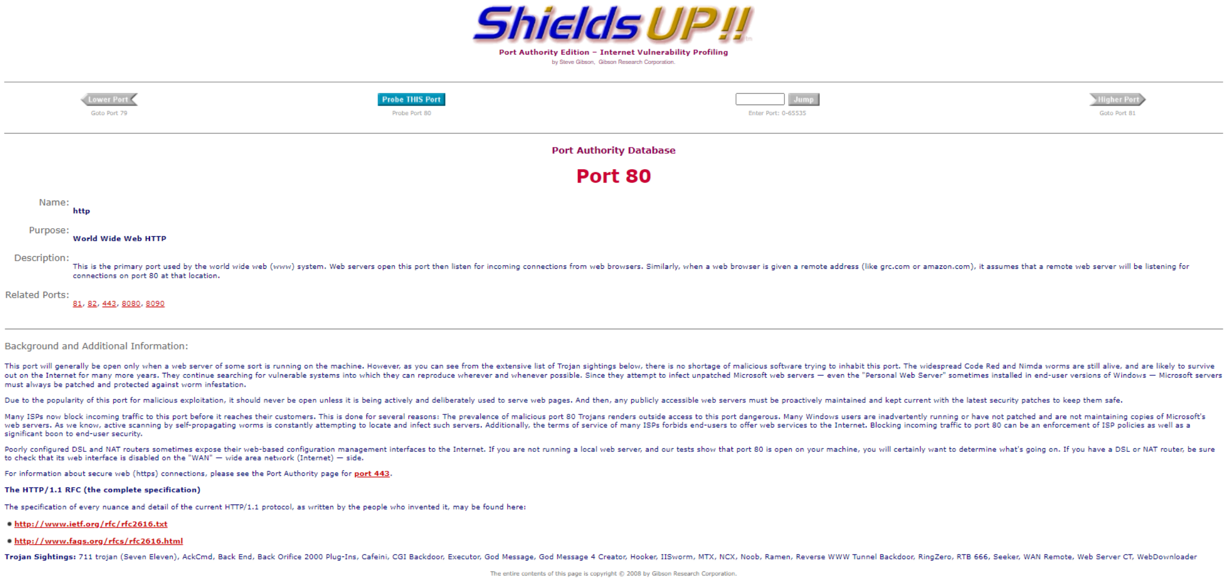
0	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	31
32	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	63
64	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	95
96	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	127
128	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	159
160	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	191
192	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	223
224	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	255
256	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	287
288	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	319
320	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	351
352	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	383
384	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	415
416	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	447
448	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	479
480	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	511
512	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	543
544	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	575
576	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	607
608	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	639
640	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	671
672	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	703
704	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	735
736	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	767
768	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	799
800	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	831
832	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	863
864	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	895
896	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	927
928	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	959
960	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	991
992	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	1023
1024	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	1055

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

🟥 Open 🟦 Closed 🟩 Stealth

Total elapsed testing time: 68.924 seconds

- Whether you had red squares or not, find and click on the square for port 80, and screen capture the page



Shields UP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Port Authority Database

Port 80

Name:
http

Purpose:
World Wide Web HTTP

Description:
This is the primary port used by the world wide web (www) system. Web servers open this port then listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port 80 at that location.

Related Ports:
81, 82, 443, 8080, 8090

Background and Additional Information:

This port will generally be open only when a web server of some sort is running on the machine. However, as you can see from the extensive list of Trojan sightings below, there is no shortage of malicious software trying to inhabit this port. The widespread Code Red and Nimda worms are still alive, and are likely to survive out on the Internet for many more years. They continue searching for vulnerable systems into which they can reproduce wherever and whenever possible. Since they attempt to infect unpatched Microsoft web servers — even the "Personal Web Server" sometimes installed in end-user versions of Windows — Microsoft servers must always be patched and protected against worm infestation.

Due to the popularity of this port for malicious exploitation, it should never be open unless it is being actively and deliberately used to serve web pages. And then, any publicly accessible web servers must be proactively maintained and kept current with the latest security patches to keep them safe.

Many ISPs now block incoming traffic to this port before it reaches their customers. This is done for several reasons: The prevalence of malicious port 80 Trojans renders outside access to this port dangerous. Many Windows users are inadvertently running or have not patched and are not maintaining copies of Microsoft's web servers. As we know, active scanning by self-propagating worms is constantly attempting to locate and infect such servers. Additionally, the terms of service of many ISPs forbids end-users to offer web services to the Internet. Blocking incoming traffic to port 80 can be an enforcement of ISP policies as well as a significant boon to end-user security.

Poorly configured DSL and NAT routers sometimes expose their web-based configuration management interfaces to the Internet. If you are not running a local web server, and our tests show that port 80 is open on your machine, you will certainly want to determine what's going on. If you have a DSL or NAT router, be sure to check that its web interface is disabled on the "WAN" — wide area network (Internet) — side.

For information about secure web (https) connections, please see the Port Authority page for **port 443**.

The HTTP/1.1 RFC (the complete specification)

The specification of every nuance and detail of the current HTTP/1.1 protocol, as written by the people who invented it, may be found here:

- **http://www.ietf.org/rfc/rfc2616.txt**
- **http://www.faqs.org/rfcs/rfc2616.html**

Trojan Sightings: 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader

- Write up a summary of your thoughts about what you feel you've learned from this short project. The summary should be at least two sentences, but can certainly be longer.
    - One of the things I’ve learned is the details about SMTP. It’s used for sending an email from the client to the client’s email’s server in addition to being used to send email between email servers. Through this research, I also learned that the recipient of a sender’s email receives the info from their email server via Internet Message Access Protocol (IMAP) and not SMTP. Another thing I learned is why UDP is preferable for streaming content/online gaming. When applications are all about real time, there’s no time for packet error checking like in the process of TCP. That’s why UDP is useful since it doesn’t have that aspect and is thus speedier.