6.3 Module 6 Discussion Read Chapters 20 and 21 Anderson, R. (2008). Security Engineering (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Hi again!

In any discussion about network security -- which includes protecting both the voice and data communications -- there is always some mention of "ports." By this, we do \*not\* mean deep-sea harbors (which are my favorite!), of course, but the "holes" made in the firewall so that some communication protocols can pass through.

It is not intended for you to get too deep technically on this topic, but it is an item of importance. Plus, there is uncertainty whether 100% of everyone fully understands what significance ports play in a networked environment. So, let's discuss that... specifically, what do you do (or should you do) as it pertains to ports and securing an environment? When responding to this topic, it is important to consider the context of ports, services, and protocols. If you are involved in network security, explain your approach.

And related to this, what is the best rule -- shut everything off, then allow the services you need \*or\* turn everything on and shut off the bad stuff?

By the way, if you do need a quick link that identifies some of the ports and services, check out:

[Service Name and Transport Protocol Port Number Registery (iana.org)](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)

Papers should be written using Times New Roman, 12-point font. The page layout should employ one-inch margins, **double-spacing**, and left justification. If section headings are used, make sure they are **bolded**, *italicized*, or ***both***. While most papers are not formal, they are to be professional.Use a spell-checker, and proofread carefully to ensure proper usage of syntax, punctuation, wording, etc. Ideally, have someone else proofread your papers.

Please write essays and papers using the third person format. When stating something that you think, use: "The author thinks...." rather than "I think..." This usage can take a while to master but it soon becomes second nature; the reader would assume it is the author's opinion as determined by the writing style. Similarly, do not refer to the reader as "you." As an example, rather than say "When using this program, you would use the Tools menu," try something like "When using this program, the user would use the Tools menu."

References

You must properly cite and reference any material that is not your own. Proper citation format must be followed in the body of the text as well as in a separate references section of your assignments/papers. APA format for citations and references is required. For more information on APA, check out an APA manual from a library, buy a manual at most bookstores, or check out online APA references at [Purdue University (Links to an external site.)](http://owl.english.purdue.edu/owl/resource/560/01/), [University of Illinois (Links to an external site.)](http://www.cws.uiuc.edu/workshop/writers/citation/apa/), or Monash University (Links to an external site.).

CLASSMATES DISCUSSION POSTS

## John

I don't have direct experience working with network firewalls, so my knowledge on ports and protocols is limited. The experience I do have comes with submitting requests to firewall teams in order to permit certain devices to communicate with one another. Firewall Rules can be established to allow only certain devices (instead of the whole network) to communicate with each other.

As an example, my organization has 2 computers that are used to transfer data to external servers. No other computers require this ability. Initially, the firewall blocked the ports and protocols necessary to make these transfers happen. A firewall request had to be submitted requesting these two computers (identified by IP address), and only these 2 computers, be able to communicate with the external servers (also identified by IP address). A problem we later ran into was that all devices on our network had to receive new IP addresses, and these two computers then lost their ability to communicate with the servers. Once that happened, a new firewall request had to be submitted, associating the computers with the new IPs. Communication between the computers and server ceased from the time the IPs changed to when the new firewall request was approved and implemented.

The default rule for firewalls should be to deny all and only allow what's needed. Opening up everything exposes a network to malicious traffic such as malware and hackers.

Some of the most commonly used network protocols and their associated ports that should be allowed are:

1. Hypertext Transfer Protocol, or HTTP (Port 80) (Used for web browsing)

2. Hypertext Transfer Protocol Secure, or HTTPS (Port 443) (Used for secure web browsing)

3. Simple Mail Transfer Protocol, or SMTP (Port 25) (Used for email)

4. File Transfer Protocol, or FTP (Port 21) (Used for transferring files over a network)

5. Domain Name System, or DNS (Port 53) (Used for translating domain names to IP addresses)

References:

SEOPressor (Nov 2019). HTTP vs HTTPS: The Difference and Everything You Need to Know. Retrieved from [https://seopressor.com/blog/http-vs-https/ (Links to an external site.)](https://seopressor.com/blog/http-vs-https/)

Service Name and Transport Protocol Port Number Registry. Retrieved from <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

[Sarah Smith](https://erau.instructure.com/courses/104834/users/203012)

## Sarah

The company I work for blocks ports and opens them as needed. We open the most common ports such as port 80. Port 80 is basically the port to access the internet. It is the HTTP port. Port 443 is another port we open, and it is https. Port 110 is for incoming emails and 25 is for outgoing. Port 53 is for DNS which is basically the process of pulling up a web page by its web address rather than by the numbers it is assigned. These are some of the most common ports that are opened.

We get a lot of requests from gamers to open ports for Xbox live. We usually research the specific ports they want to be opened and depending on the circumstances, we may or may not open them. We have requests for cameras and other devices as well but normally they don’t need special ports opened.

The reason we block these ports is for security reasons. It is a way of securing the network so unwanted traffic isn’t able to access it. Since most of the properties that we monitor are rentals, we usually don't open ports for them. and if we do open ports for a long term renter, we close them once they are gone.  We don't want to leave our network vulnerable.

References

# Brown, M. (2018) How to get open NAT on Xbox One with port forwarding. Retrieved

# from [https://www.windowscentral.com/xbox-one-port-forwarding (Links to an external site.)](https://www.windowscentral.com/xbox-one-port-forwarding)

Wilkins, S. (2012) TCP/IP Ports and Protocols. Retrieved from

<http://www.pearsonitcertification.com/articles/article.aspx?p=1868080>