CIDM 6341-01 Current issues in Cybersecurity

Mariam Adegbindin

Buff Id: 1133249

Shields Up

**Question 1: What did you do?**

When checking the common ports, it sent a ping to each of the ports I had in my computer (for example SMTP, HTTP, TELNET etc) and router replied to the ping meaning it is visible on the internet. It sent out solicited TCP packets which failed because it responded to the deliberate attempt to establish a connection, but no unsolicited packet was received back in the process which would have been an after effect from attempting to establish a connection.

**Question 2: What were the results?**

I had one open port, one closed port and 24 ports stealth. The closed port service is Nil which means there is nothing to worry about. The open port is a 443 port which is a Hypertext transfer protocol secure (HTTPS), what this means is that a secure web browser communication takes place over this port. These connections have extremely strong anti-eavesdropping and anti-interception protection for data transport. This port is used by web servers to accept and establish secure connections and web browsers looking for high levels of communication security can connect to them.

**Question 3: What did you learn?**

Finding out I have an open port was a bit scary but researching on what port 443 entails made me understand that HTTPS uses security certificates when transacting online by providing your credit card information when making a purchase. What I have learnt from this is that an https is used when providing sensitive information and or when just browsing some websites and the way to tell the difference between an http and an https website Is by looking out for the padlock symbol. The port for the non-secure web connections is port 80. So as much as the port is opened what I can do is be more vigilant when buying things online and to make sure the page that I am typing in information to is an https port by identifying the padlock symbol on the web browser or by checking the properties of the page to see what sort of secured certificates it holds.

The port being open is not a bad thing, I would say that my firewall has it open by default seeing that it is needed when going through ecommerce websites and logging into websites were you must provide your username and password.

Taking into consideration the secure icon that is the padlock should be probed further, even if it says the connection is secure some websites which some might say are illegal with pop ups might bring more harm than good to your system. For example, using the Shields up system it tells you the connection is secure but also advises you not to provide certain information because it is not fully secured (Fig 1)



*Fig 1. (Gibson Research Corporation,2020)*

Apart from checking the common ports, I also checked all the ports which went through 1056 ports on my system. It gave the same results has having one closed port, one open port and 1054 stealth ports.

A screenshot of a grid

Description automatically generated

*Fig 2. (Gibson Research Corporation,2020)*

*Determining the status of the first 1056 TCP ports.*

Have I been pwned

**Question 1: What did you do?**

I checked my two emails both yahoo mails. One email I use but don’t check often I use that for sites that I don’t want to be bothered by. My second email is my official email which I check all the time. I put it into the search bar and it ran through the different websites that the email is associated with.

I also checked my passwords; I use one password for most of my things and another I use and tend to forget for sites I deem not important.

**Question 2: What were the results?**

Both emails have been breached, funny enough by websites and applications I don’t use anymore. The email I use for important work was breached twice.

A red background with white text

Description automatically generated

*Fig 3 (Have I been pwned)*

*The first email tested showing two breaches with one stating unverified.*

One of the breaches is classed as unverified meaning the breach could have been fabricated or that its possible there had been a breach but are not able to establish the legitimacy.

The second email had three breaches giving out data such as geographic locations and IP addresses. These breaches were on what I would say are 3 heavy corporations in their field (Fig3).

Also, one of the breaches (Wattpad) is among the top 10 breaches that have happened in recent times according to the results.

A screenshot of a computer

Description automatically generated

*Fig 4 (Have I been pwned)*

*The second email showing 3 breaches when tested.*

The good news is there were no breaches for the two passwords I tested which means I am doing something right.

**Question 3: What did you learn?**

One thing we discussed in class is that these breaches are not necessarily our fault, the onus lies with the corporations that we provide the information to, and it being breached is not a bad thing especially in a case where only the email has been breached but not the password.

There would be issues if the email and password has been breached. One thing I have learnt and appreciate is the transparency to be able to use a site like have I been pwned to see how our data has been exposed where it does the work of searching through the internet checking where the email or the password has been entered and checking if it has been breached. Also providing information to what data’s have been comprised. In terms of my email being breached there is nothing I would be doing about it for now especially because it does not serve as an immediate threat.

# Works Cited

Gibson reasearch corporation . (2020). *Shields Up*. Retrieved from A Gibson research corporation website: https://www.grc.com/x/ne.dll?bh0bkyd2

Hunt, T. (n.d.). *Have i been pwned*. Retrieved from Have i been pwned: https://haveibeenpwned.com/

SSL Dragon. (2014 - 2023). *What is HTTPS 443 and how to open it?* Retrieved from A SSL Dragon blog: https://www.ssldragon.com/blog/https-port-443/