Sera Hill
CIDM 6341-70

Shields Up/HaveIBeenPwned

What Did I Do?

For the first part of this assignment, I visited the Shields Up website and gave it permission to send a request to each of the internet ports for my computer to see if it would get a response or not. The first option I checked was the Common Ports, which checked a total of 26 common ports for my computer to see if any of them returned with a response to the request. I then checked All Service Ports which sent a request to 1,056 of the ports for my computer and gave me a list of ports that it detected and what the status was for each of them. For the second part of this assignment, I visited haveibeenpwned.com to see if any of my emails, phone numbers, and passwords were involved in a data breach. By entering emails, phone numbers, and passwords, the site checked them against databases to see if they were found in any of the big data breaches. I checked three total emails, two being personal (one of which I do not sign into anymore) and one being the one I use at work. I also checked the one cell phone number I've ever had. Lastly, I checked five of my most used passwords for both personal sites and what I use at work.

What Were the Results?

Regarding the results from the Shields Up website, 26 of the common ports for my computer were pinged and 11 were found closed while the remaining 15 came back as stealth. Port 0, 1002, 1024, 1025, 1026, 1027, 1028, 1029, 1030, 1720, and 5000 were all responding that the ports existed, but are closed to connections. Ports 21, 22, 23, 25, 79, 80, 110, 113, 119, 135, 139, 143, 389, 443, and 445 all showed that there was no evidence of these ports or a computer existed at my IP address. As mentioned in the lecture video, a closed port is not a terrible thing to have, but it does let hackers know that there is in fact a port at my IP address even though the response was closed. To my relief, none of the ports at my IP address were open, which means that hackers do not have an easy way of gaining access to my computer and the information that it holds. The report from this probe also yielded the following results: Solicited TCP Packets – Failed, Unsolicited Packets – Passed,

Sera Hill
CIDM 6341-70

Ping Reply – Failed. This is not to say that my computer is incredibly vulnerable and will be hacked, but there is room to improve my security and prevent hackers from probing my computer completely. Below is the text summary from this report:

```
-------------------------------------------------------------
------

GRC Port Authority Report created on UTC: 2024-09-06 at 23:25:29

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                            119, 135, 139, 143, 389, 443, 445,
                            1002, 1024-1030, 1720, 5000

    0 Ports Open
   11 Ports Closed
   15 Ports Stealth
---------------------
   26 Ports Tested

NO PORTS were found to be OPEN.

Ports found to be CLOSED were: 0, 1002, 1024, 1025, 1026, 1027,
                               1028, 1029, 1030, 1720, 5000

Other than what is listed above, all ports are STEALTH.

TruStealth: FAILED - NOT all tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - A PING REPLY (ICMP Echo) WAS RECEIVED.

-------------------------------------------------------------
------
```

Sera Hill
CIDM 6341-70

For the All Service Ports scan 1056 ports were scanned. This scan resulted in 0 ports were open, 72 ports were closed, and the remaining 984 ports were stealth. Again this is not necessarily a terrible thing, but it does let hackers know that there are ports that will respond with some sort of reply when probed. The below text summary has the results from this scan:

```
------------------------------------------------------------------
------

GRC Port Authority Report created on UTC: 2024-09-07 at 01:28:25

Results from scan of ports: 0-1055

    0 Ports Open
   72 Ports Closed
  984 Ports Stealth
--------------------
 1056 Ports Tested

NO PORTS were found to be OPEN.

Ports found to be CLOSED were: 0, 1, 2, 3, 4, 5, 6, 31, 61,
                               62, 91, 92, 121, 122, 152, 153,
                               182, 183, 212, 213, 242, 243,
                               272, 273, 303, 304, 333, 334,
                               363, 364, 393, 394, 423, 424,
                               454, 455, 484, 485, 514, 515,
                               544, 545, 606, 607, 637, 638,
                               667, 668, 697, 698, 727, 728,
                               758, 759, 788, 789, 818, 819,
                               848, 849, 878, 879, 909, 910,
                               939, 940, 969, 970, 999, 1000,
```

Sera Hill
CIDM 6341-70

```
                                    1029, 1030

Other than what is listed above, all ports are STEALTH.

TruStealth: FAILED - NOT all tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - A PING REPLY (ICMP Echo) WAS RECEIVED.
```

Regarding the second part of the assignment using haveibeenpwned.com, I will first discuss the results of my email addresses. The first email I checked which is for my personal use was found in 6 data breaches. However, the email was not pasted on any public facing website to share my information. The email address in question was found in the following data breaches: Adobe – October 2013, Apollo – 2018, MyFitnessPal – 2018, Ticketyfly – 2018, tumblr – 2013, and Zynga – 2019. The second personal use email I checked was found in 7 data breaches, but was not pasted to public facing websites with my information on it. This was found in the following breaches: Adobe – 2013, Anti Public Combo List – 2016, Collection #1 – 2019, Exploit.In – 2016, Gravatar – 2020, MySpace – 2008, and Neopets – 2016. My work email was not found in any databases regarding data breaches, and my personal phone number was not found in any data breaches as well. For my passwords, I checked three of my most used passwords for personal use, and two of the ones I've used at work. None of the passwords were found to be logged in any database regarding data breach information and while that does provide me some peace of mind, it does not mean that these are necessarily strong passwords, especially the ones I have for my personal use.

What Did I Learn?

After doing the first part of the assignment with the Shields Up website, I learned a bit more about the common ports for my computer and what they are for. I thought it was

really interesting that even though the ports that did send a reply back to the scanner saying it was closed, it still means that hackers could discover my computer exists. In the Information Technology Management class, I remember seeing this site, but I'm not sure that I ever ran the scan for my own computer. I also didn't realize how many internet ports there were for computers, making potential vulnerabilities even greater than I originally thought. I also learned that through open ports, hackers can use them "to send commands to a computer, gain access to a server, and exert control over a networking device" (Jennex, 2021).

I also was interested to learn more about my computer's firewall settings and was a little surprised that, by default, the firewall setting is turned off. After doing some additional research online, I discovered that this is because "Apple does not ship any high-risk services that listen for connections on the public internet" (Kolide), and that "…all Macs have come with a built-in application layer firewall that is capable of blocking incoming connections…" (Kolide). While I have not installed any kind of program on my computer as of yet that has open connections to public networks, this does make me realize that this is something that I should keep awareness up in case this does happen in the future.

While I knew that information you put on the internet or use to sign up for things on the web can be collected and used by other people, it is easy to forget that it happens so often. One of the most recent letters I've received in the mail was from Ticketmaster regarding their data breach and that my information was part of the many individuals'' information that was collected. While I do find it alarming, it is somewhat of a comfort to know that, according to the Have I Been Pwned site at least, that my email address has not been published on sites selling information. I learned that if my information had been pasted somewhere, then a good plan of action would be to change my password to my account.

These different exercises has made me more aware of potential vulnerabilities that I face while being on the Internet, and that I should be careful with the passwords I create, what I'm inputting my information into, and to be aware that data breaches can happen no matter how secure a company may be. I think it is easy for individuals to forget how

vulnerable they can be to hackers, especially when nothing bad has happened to them and their information hasn't been stolen. With that said, the reminders in from this class, other classes I've taken at WT, and the ongoing security awareness at work has helped me become more aware of how I can better protect myself and try to reduce my attack surface.

Sera Hill
CIDM 6341-70

References

Gibson, Steve. “Shields Up!! Port Authority Edition – Internet Vulnerability Profiling.” Gibson Research Corporation, https://www.grc.com/x/ne.dll?bh0bkyd2. Accessed 6 Sept. 2024.

Hunt, Troy. “Have I Been Pwned: Check If Your Email Has Been Compromised in a Data Breach.” *Haveibeenpwned.com*, 2023, haveibeenpwned.com/.

Jennex, M. (2021). Why are Computers Vulnerable to Security Issues?. [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2701708-dt-content-rid-51952150_1/xid-51952150_1

Kolide. “How to Configure Macos Firewall to Block Unauthorized Connections.” Kolide by 1Password, www.kolide.com/features/checks/mac-firewall. Accessed 7 Sept. 2024.