What Did you Do?:

For this exercise we were tasked with creating a Ransomware Recovery plan for an organization based on our previous 3 exercises. This was a tad tricky in my case as all of my previous exercises had been run on my personal network which is obviously not as expansive in terms of network size, servers, devices etc. Nonetheless I tried my best to apply my situation to the exercise. A ransomware attack occurs when a hacker threatens to reveal personal or organizational information to the public or potentially use that information for their own personal benefit, for example a bank information or a social security number. Additionally hackers may hack a network and block users from accessing files, servers etc. The hacker expects some sort of monetary compensation to stop them from sharing information or to get them out of your system. Surprisingly a fair amount of organizations do in fact give into these demands and end up paying the hackers. This is not sustainable and frankly what is to stop the hacker from doing it again. That is why security upfront is vital however equally important is a plan of action if a ransomware attack was to occur. The main methods for overcoming such attacks are creating backups, keeping software up to date, keeping passwords secure, having a strong inventory of all network assets, and finally having formal procedures for response documented. The first step in creating my personalized ransomware attack plan was to prepare an inventory of network devices. In order to achieve this list it was necessary to go back and review the NMAP results from assignment #1 to identify network devices. In addition to reviewing the previous assignment I did a quick visual inspection of every room in my living space to make sure I was truly capturing everything. After identifying which network devices were being used it was necessary to identify any servers that needed to be backed up, and again assignment 1's NMAP results were used. After those two pieces were identified it was necessary to identify any components that needed to be updated. In order find these components it was necessary to review the Nessus Vulnerability Scan from assignment #3. Anything that showed up as a vulnerability would need to be updated. Lastly I reviewed all assignments to identify any critical passwords to the network. After getting all of these various items written down and listed it was necessary to analyze them and determine which were the most significant. It was also important for me to think in context of how I use my network and what possible attacks could come onto my attack surface.

What were the results?:

To start, the identified network devices were as follows (in order of importance and potential impact): Network router, my laptop,Cellphone, garage door (connected to wifi), home security camera system,NEST thermostat, Smart TV, Roku,and PS5. This attack surface is not just limited to the devices themselves but also bluetooth connections and any applications and associated servers of those apps. A device is as weak as its least secure software is. Hackers can find an opening in the software to find a way into the total network. If this were to be conducted on an organization network I would expect to find a lot more devices including more network manipulation devices like extenders, multiple routers, and switches. Obviously the most important network component of my setup would be the router. Most recovery plans would be centered around the router. Which is why a configuration backup should be created.

Following the router would be my laptop as this an easy way to access the network and make drastic changes. Similar to the router a backup of laptop settings should be made in case the device was to be compromised. Next in importance would be my cellphone as similar to my laptop this is a great way to attack a network. Again a back should be created for the cellphone, and again it is important to remember that attacks can come from any application on the phone as well, which is why it is necessary to make sure all applications are checked for available updates frequently (at least bi-weekly). After the cell phone I have my garage door listed, and that is because the router is actually located in the garage, and physical security plays a role as well. If the door is able to be hacked open it would grant someone physical access to the router and have their way. While no backup is possible for this it is still important to monitor and keep in mind. For the Camera System and NEST Thermostat they are both connected to the network and could be opening for a hacker, especially since for these two items there is not a whole lot of control on their setting as they are provided by my landlord. The last three devices are all media streaming devices that again could be an opening for a hacker and should be kept in mind and monitored. The tricky thing with a lot of these internet of thing type devices is that you have to rely on the companies that create these products, due to a lot of them requiring updates to keep functioning normally. This means you have to rely on these companies' security practices and testing to ensure any new updates do not have any potential vulnerabilities. The only devices that require a backup are the router, my laptop and cellphone. The other items don't necessarily have those capabilities. Coincidentally those are three devices that will need to have password backups as well. These are three easiest ways to penetrate my network. While my Nessus scan returned no vulnerabilities and everything appeared to be up to date it is still extremely important to monitor for updates frequently. I would benefit from doing an individual device check as well to fully ensure that all devices are running the most up to date versions of software. Also with so many third party applications on my phone, computer, and media devices it is important to keep abreast of news of hacks and to keep these applications updated as well. As it could be an obvious trigger that would prompt me to review my network. Luckily for me I have a relatively small attack surface and if I were to notice any indication of a ransomware attack I would be able to relatively quickly investigate each device to determine the source, and then proceed to restore to backups as needed, reset passwords, etc.

What Did you Learn?:

Personally I think my network is a little underwhelming to fully understand the scope needed to create a ransomware recovery plan for an organization. As I mentioned they obviously have so much of a wider network and users. This honestly ended up feeling extremely similar to my previous Info-Sec assignment where we identified potential vulnerabilities. I do think this is somewhat normal as our information becomes more and more synched with our networks. However my personal network has such a small footprint that it pales in comparison. I do think that it is a good reminder that no matter what kind of network you are running, organization or personal, that diligence is one of the best defenses available. Especially considering how many 3rd party devices are connected to my network and their security practices are out of my control. I do think it will be necessary for me to review a few bigger recovery plans from organizations in order to get a better understanding of a wider net recovery plan.