Research Report 4 Ransomware Recovery

1. What did you do?

I began by re-reading my first assignment over Nmap scanning. Once this was done I opened the original scan files in Nmap. I reviewed each host that Nmap had found determined a level of importance for each one. The importance ranged from unimportant-nice to have-necessary. An unimportant device is one that retains no data or will limit any work done. A necessity is a device with data that is important or is necessary for work. I also listed out any important network equipment that could allow a path from the internet to an important host.

For step two I began similarly by reading my assignment 3 over Shields Up and Nessus. I then reviewed the Nessus scan I did of the 16 hosts. I compared the hosts I determined as important to their vulnerability scan. I then reviewed the network devices included in the scan. I noted the vulnerabilities and solutions to them. This gave me a list of devices that need to stay updated.

Finally reread the second report over Wireshark. I also reviewed the capture it performed. I limited the review to the IPs for the important devices I had already determined. I then went though each device and captured the credentials for the primary administrator accounts. Once that was done I reviewed all that I had gather to make sure it was complete *specifically a prioritized list of components for recovery, a list of backups that need to be prepared and maintained, a list of passwords that need to be backed up, a list of devices that need to be updated, and finally, a inventory of network devices.*

1. What are the results?

My prioritized list of components that would need to be recovered in the event of ransomware is really just 2 host. They are 10.0.0.10 and 10.0.0.51. The first is a server and the only important data on it is a back up from the other host. The other host is a Windows desktop. I do all my schoolwork from it and it has important data, mostly photos, that need to be backed up or recovered. If both of these hosts went down, I’d have to get another machine going for schoolwork and for the data there really is no monetary value that I could put on it.

For a list of network devices that matter it is really two but there is a couple “Dumb” switches being used that need to stay up. I also have a Wireless Access Point at 10.0.0.41 and a router at 10.0.0.1. These two were chosen since they both have regular updates that come out and are paths into the network.

The list of backups that need to be prepared and maintained would include each device I’ve mentioned, 10.0.0.1, 10.0.0.10, 10.0.0.41, and 10.0.0.51. Each of these needs backups made and maintained. A configuration file of both the router and WAP needs to be backed up and saved. The workstation .51 backups up important files to .10. For school files those are backed up to OneDrive continually so there is no worry on that data. On the note of cloud back ups or offsite backups they are needed in some form. Since backups can get trapped with ransomware and offsite backup could save the day. Backups are definitely a deficiency.

For passwords and backups, I have a password manager that has multifactor authentication setup. I also have my “vault” shared with my Wife and she has hers shared with me. Any local Admin account like the one for the router is saved there. An offline copy of the data can be made of it but presently there is not one.

The same devices that need to be backed up, 10.0.0.1, 10.0.0.10, 10.0.0.41, and 10.0.0.51, need updates continually done as well. But also any machine on the network is a potential path into the network so even if it is not important it needs updates. This includes cell phones, other workstations, smart home devices, and anything else that connects to the Wi-Fi. The cell phones and workstations are checked on regularly. The other smart home devices are not checked to make sure updates are being done regularly.

1. What did you learn?

Ransomware is something that I’ve gotten fairly familiar with over my career in IT. I’ve never been at a company that has gotten ransomed or had a client get ransomed while I was there. I’ve known several companies that have gotten ransomed including several in the Amarillo area. I feel like ransomware is the last thing most people think about. I commonly see phishing emails or email accounts that have gotten hacked. I’ve also seen many devices with viruses. Ransomware seems like it happens less often but when it does it is bigger than anything else. But as long as you are practicing safe IT it should be easily avoided. That would include three levels of backups at minimum one offsite, updating all devices regularly, and training users on what to look out for.

My current organization uses a software called Huntress as a anti-Virus. It also does monitor for ransomware events. It does this by putting many “canary” files randomly on a drive. If Huntress detects that one of these files is gone or changed it will quarantine the machine and not allow it to communicate with the network. Something I thought was brilliant and very simple.

References

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch01\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650746\_1/xid-51650746\_1

Jennex, M. (2023). Why Computers Are Vulnerable r3 [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650747\_1/xid-51650747\_1

Jennex, M. (2023). CIDM6341 Introduction [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650748\_1/xid-51650748\_1

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch12\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646267-dt-content-rid-51650758\_1/xid-51650758\_1