What did you do?

Given directive guidance, I approached the problem set with the following prioritization:

Generate

1. Inventory of network devices
2. List of devices that need to be updated
3. Prioritized list of components for recovery
4. List of passwords that need to be backed up
5. List of backups that need to be prepared and maintained

First, I captured and generated reflective reports of my home network. Without access to a business/organization network, I made mine as complex as possible by connecting all my LAN devices at once. This will provide the inventory of network devices and a list of devices that need to be updated.

1. Had my kids turn on, connect, and start data flow on every single device that connects to our home network
2. Opened Wireshark, began capture on Wi-Fi
3. Using Zenmap GUI typed IPv4 range 192.168.1.0/24 into target field and scanned
4. Signed into Nessus Essentials webpage
5. Created target scan of IPv4 range 192.168.1.0/24
6. 10 devices found within Home Network
7. Nmap scan completed
8. Nessus vulnerability scan completed
9. Stopped Wireshark capture
10. Saved Wireshark capture for reference
11. Printed Zenmap GUI to pdf “Nmap\_Home Network”
12. Used Snipping Tool to capture Home Network Topology
13. Printed to pdf “Nmap\_Topology\_Home Network”
14. Generated Nessus Report Vulnerabilities by Host Summarized
15. Printed to pdf “Nessus\_Home Network\_Summarized”
16. Generated Nessus Report Vulnerabilities by Host Detailed
17. Printed to pdf “Nessus\_Home Network\_Detailed”
18. Had my kids reduce our EM footprint to a normal level
19. Analyzed vulnerabilities found
20. Acted on remediation of vulnerabilities

Second, I met with the board of directors (my wife) to discuss a prioritized list of components for recovery. We approached this from the macro level and built toward micro by thinking through what is most critical for our household to continue operations. We began with the services we require most, then I examined where those services are pulled from and how we access them. We identified and itemized the assets of hardware, software, applications, and data (see excel “Prioritized Asset List\_Home Network”)

1. Examined services and prioritized from critical through nice to have
2. Assigned a 1-10 scale of necessity to each service
3. Correlated services with device that provides them
4. Prioritized every service to prepare steps of importance for recovery plan

Third, I compiled a list of password roles that need to be backed up.

1. Admin, Encryption, VM credentials, ESXi, SQL, Active Directory, and vCenter are critical but N/A on this network
2. Passwords to services and applications compiled on tracker
3. Password tracker encrypted on PC
4. Password tracker printed and kept in physical safe

Fourth, I created a list of backups that need to be prepared and maintained using the 3-2-1 model. Keep 3 copies of your data, on 2 different storage types, with 1 copy off-site. The first copy is the working edition on the network. The second copy is an external hard drive with limited permissions for unauthorized users and password protected. The third copy is off-site utilizing Google Cloud storage.

1. Inherently excluded applications and program files from consideration
2. Scoured File Explorer to find all nooks and crannies of data for each user
3. Reworked Data Tree of folders to simplify backup process
4. Created data backup schedule
5. Explored options for automating this process

What are the results?

Each of the ten devices including the Gateway router are listed below with their IP, Nomenclature, Common name, TCP port status, IP Sequence Generation, Protocols used, OS, Keys and encryption algorithms, and vulnerability scan results.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.168.1.1 | Docsis-Gateway  (Wi-Fi Router) | | 989 Closed TCP Ports | |
| 53 – DNS – Open  80 – HTTP – Open  443 – HTTPS – Open  8000 – HTTP ALT – Open  49152 -UPNP – Open  49153 – UPNP – Open  49154 – UPNP – Open  49155 – UPNP – Open | 22 – SSH – Filtered  23 – TELNET – Filtered  9000 – CSLISTENER – Filtered  IP ID Sequence Generation:  All Zeros | | Protocol 6: TCP Used for 11 ports | Linux 4.9 |
| Public Key: RSA-2048 | Signature Algorithm: SHA-256 |
| Uptime 16.214 days  0.0079s latency | 1 Hop, RTT 12.08ms  33434 – Traceroute | | TCP Sequence Prediction:  Difficulty=246 | |
| Name | Severity | CVSS V3.0 | VPR Score | Plugin |
| IP Forwarding Enabled | Medium | 6.5 | 4.0 | 50686 |
| SSL Certificate Cannot be Trusted | Medium | 6.5 | - | 51192 |
| SSL Self-Signed Certificate | Medium | 6.5 | - | 57582 |
| TLS Version 1.0 Protocol Detection | Medium | 6.5 | - | 104743 |
| TLS Version 1.1 Protocol Deprecated | Medium | 6.5 | - | 157288 |
| DHCP Server Detection | Low | 3.3 | - | 10663 |
| 31 Info Vulnerabilities Identified | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 192.168.1.15 | DESKTOP-3SHPIF1 (PC) | | 997 Closed TCP Ports | |
| 135 – MSRPC – Open  139 – NETBIOS-SSN – Open  445 – MICROSOFT-DS – Open | IP ID Sequence Generation:  Incremental | | Protocol 6: TCP Used for  3 ports | Windows 10 |
| SMB signing enabled, not required | |
| Uptime 23.667 days  0.00044s latency | 0 Hops | | TCP Sequence Prediction: Difficulty=258 | |
| Name | Severity | CVSS V3.0 | VPR Score | Plugin |
| SNB Signing not Required | Medium | 5.3 | - | 57608 |
| 17 Info Vulnerabilities Identified | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.104 | Unknown (iPhone) | 998 Closed TCP Ports | |
| 49152 – UPNP – Open  62078 – TCPWRAPPED – Open | IP ID Sequence Generation:  All Zeros | Protocol 6: TCP Used for  2 ports | Unknown OS (iOS) |
| Uptime 0.000 days  0.0079s latency | 1 Hop, RTT 7.94ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=256 | |
| 8 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.110 | 32PhilipsROKUTV (Smart TV) | 999 Closed TCP Ports | |
| 7000 – RTSP – Open | IP ID Sequence Generation:  All Zeros | Protocol 6: TCP Used for  1 port | Android 5.1.1 |
| Uptime 0.497 days  0.0094 latency | 1 Hop, RTT 9.43ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=261 | |
| 17 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.129 | Galaxy-Tab-A7-Lite (Tablet) | 1000 Closed TCP Ports | |
|  | IP ID Sequence Generation:  Unknown |  | Unknown OS |
| Uptime Unknown  0.017s latency | 1 Hop, RTT 16.53ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=Unknown | |
| 5 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.187 | BRW5C61999450D8 (Printer) | 995 Closed TCP Ports | |
| 80 – HTTP – Open  443 – HTTPS – Open  515 – LPD - Open  631 – IPP - Open  9100 – PDL - Open | IP ID Sequence Generation:  Random Positive Increments | Protocol 6: TCP Used for 5 ports | Unknown OS |
| Public Key: RSA-2048 | Signature Algorithm: SHA-256 |
| Uptime 30.092 days  0.022s latency | 1 Hop, RTT 22.37ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=256 | |
| 4 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.211 | RokuPremiere (Roku) | 998 Closed TCP Ports | |
| 7000 – RTSP – Open  9080 – GLRPC - Open | IP ID Sequence Generation:  All Zeros | Protocol 6: TCP Used for 2 ports | Android 5.1.1 |
| Uptime 0.241 days  0.012s latency | 1 Hop, RTT 11.61ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=252 | |
| 17 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.217 | Unknown (Xbox 360) | 999 Filtered TCP Ports | |
| 1025 – TCPWRAPPED – Open | IP ID Sequence Generation:  Unknown |  | Unknown OS |
| Uptime Unknown  0.047s latency | 1 Hop, RTT 47.42ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=Unknown | |
| 9 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.227 | Unknown (Amazon Tablet) | 1000 Closed TCP Ports | |
|  | IP ID Sequence Generation:  Unknown |  | Unknown OS |
| Uptime Unknown  0.014s latency | 1 Hop, RTT 13.85ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=Unknown | |
| 5 Info Vulnerabilities Identified | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.1.252 | Gena-s-s10e (Android Phone) | 1000 Closed TCP Ports | |
|  | IP ID Sequence Generation:  Unknown |  | Unknown OS (Android) |
| Unknown Uptime  0.032s latency | 1 Hop, RTT 31.89ms  33434 – Traceroute | TCP Sequence Prediction: Difficulty=Unknown | |
| 5 Info Vulnerabilities Identified | | | |

The largest risk found by Nessus was TLS Version 1.0 and 1.1 Protocol vulnerabilities. TLS 1.0 has been around since 1999 giving bad actors plenty of time to find the weak spots. It is largely utilized for backwards compatibility but can easily be disabled. TLS 1.1 is in a similar vein, just an outdated Transport Layer Security. I disabled both TLS 1.0. and 1.1 in my system’s Internet Properties to reduce the attack surface. TLS 1.3 is the current version as of 2018. I won’t be able to connect to any https that support TLS 1.0 and 1.1, but that is only 0.4% of websites.¹

The following ports and protocols were filtered to identify the scope of data traffic. TCP is the major protocol used during execution of NMAP and Nessus (TCP = 95.5%, UDP = 2.6%, ICMP = 0.4%, IGMP = 0.1%). Results would vary with standard Wireshark capturing of a network in its natural state. I did not include any packet type that had less that 500 during this capture.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Port** | **Source IP** | **Protocol** | **Bytes Range** | **Packets** |
| 51712 | Ephemeral – Streaming? | 192.168.1.15 | TCP | 58-60 | 16676 |
| 9080 | GLRPC | 192.168.1.211 | TCP | 54-1514 | 13052 |
| 7000 | AFS3-Fileserver | 192.168.1.211 | TCP | 54-1514 | 11031 |
| 443 | HTTPS | 192.168.1.1 | TCP | 54-1514 | 5182 |
| 8060 | Aero | 192.168.1.211 | TCP | 54-1514 | 3278 |
| 80 | HTTP | 192.168.1.1 | TCP | 54-1514 | 2933 |
| 8000 | HTTP-ALT | 192.168.1.1 | TCP | 54-1514 | 2076 |
| 51714 | Ephemeral – Streaming? | 192.168.1.15 | TCP | 58-60 | 1789 |
| 1025 | Teradata Database Management System | 192.168.1.217 | TCP | 54-1514 | 779 |

The following table shows our lines of effort for priority of recovery. The overarching theme of priority is capability to connect, memento photos, important documents, school, Office 365, public keys, printing, and a work application. There were quite a few assets that ranked low due to either redundant means of accessing data or simply downloading an application/software on a new device such as GPS, Weather, Encrypted Chat Services, Online Libraries, Streaming Video, or any service provided by web browser. I did not include the 56 assets that merited a low priority rating here. You can view these in the excel “Prioritized Asset List\_Home Network.”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority** | **Hardware** | **Software/Application** | **Data/Utility** | **Priority Rating** |
| 1 | Gateway-Docsis | Connectivity | WAN Access | 10 |
| 2 | Keyboard | Bluetooth Connection | Input | 10 |
| 3 | Mouse | Bluetooth Connection | Input | 10 |
| 4 | PC | File Explorer | Photos – Nostalgic History | 9 |
| 5 | PC | Microsoft SQL Server | Database Management | 8 |
| 6 | iPhone | Photos | Photos – Nostalgic History | 8 |
| 7 | Android Phone | Gallery | Photos – Nostalgic History | 8 |
| 8 | PC | File Explorer | Important Documents – Taxes | 7 |
| 9 | PC | File Explorer | Important Documents – Mortgages | 7 |
| 10 | PC | File Explorer | School – WTAMU Assignments | 5 |
| 11 | PC | McAfee | Virus Scan | 5 |
| 12 | PC | Microsoft PowerPoint | Army Presentations | 4 |
| 13 | PC | File Explorer | Personal Projects – Cookbook | 4 |
| 14 | PC | Microsoft Defender | Online Security | 4 |
| 15 | iPhone | MilGPS | MGRS GPS | 4 |
| 16 | PC | Microsoft Word | Document Writing | 3 |
| 17 | PC | Microsoft Excel | Planning | 3 |
| 18 | PC | Microsoft Excel | Tracking | 3 |
| 19 | PC | Brother Printer | Printing Documents | 3 |
| 20 | PC | Brother Printer | Scanning Documents | 3 |
| 21 | PC | Microsoft S/MIME | Email PKE | 3 |
| 22 | Printer | Printer Drivers | Printing Documents | 3 |
| 23 | Printer | Printer Drivers | Scanning Documents | 3 |
| 24 | PC | File Explorer | Resumes | 2 |
| 25 | PC | SPEED | Radio Line-of-Sight Analysis | 2 |

I believe the intent for making a list of passwords for backup is aligned with a network administrator’s role in managing the network. There is a degree of notional allotment I must consider when doing so for a home network. Identifying critical passwords for backup and isolating a password manager are applicable for Admin, MFA account tokens, Encryption, VM credentials, ESXi, SQL, Active Directory, and vCenter passwords. Regardless, below is a list of password roles compiled for my home network.

|  |  |  |  |
| --- | --- | --- | --- |
| **Critical** | **Bills** | **Services** | **Vendors** |
| Mortgage | Energy | Netflix | Home Depot |
| Car Insurance | Property Manager | Daily Wire | Lowes |
| Home Insurance | Toll Tag | Peacock | Walmart |
| Vanguard | Internet Service Provider | Paramount+ | USPS |
| Property Taxes | Credit Cards | Homeschool | Amazon |
| Property Managers | Cell Phones | WTAMU |  |
| Tax Documents | Water/Sewer/Garbage | Shutterfly |  |
| Vehicle Registration | Streaming Memberships | AAA |  |
| Banks |  | Hilton Honors |  |
| Merrill Lynch |  | Email |  |
|  |  | iCloud |  |
|  |  | American Airlines |  |

What did you learn?

A group of black text

Description automatically generated

Prior to exploring this exercise, I didn’t realize there was no prevention tool with total protection from ransomware. I can understand the forms of ransomware that are still developing, newly found vulnerabilities that haven’t been exploited yet. I was surprised by the lack of a 100% prevention tool with known forms of ransomware. I believe the knowledge to create semi-automated ransomware remediation software and services exist (although that opens up yet another attack surface). I wonder if there is hesitancy to create a prevention tool of known ransomware due to liability. If the tool is being implemented and ransomware still infects a system, the developer could have serious legal repercussions. When looking at the sheer monetary value of ransom and how it has exponentially increased over the past decade, that liability could easily be in the billions.

SpinOne seems to be the most versatile and closest to being an all-in-one ransomware protection software. “SpinOne is automated security software that combines advanced backup functionality with ransomware prevention. This solution follows the 3-2-1 strategy, offers multiple backup versions, and automatically backs up data three times a day while utilizing advanced ransomware methods. SpinOne utilizes an innovative ransomware detection method-behavioral analytics. This method is based on understanding ransomware patterns via abnormal file behavior. Powered by machine learning algorithms, it allows achieving 99% accuracy in detecting ransomware.”² This sounds like quite the winning software, but they don’t offer recovery plan development nor assistance. This is like having an IDPS for ransomware that streamlines backups for user ease. Still short of the mark.

You need a map just to navigate the oversaturated cybersecurity digitalscape:³

A group of logos on a white background

Description automatically generated

It’s a wild concept to me still even after researching ransomware that recovery is the only protection against ransomware. At least without paying the ransom of course. The idea of paying ransom for access to MY data leaves a simmering anger behind. I can understand organizations paying the ransom to continue productivity. I was directly affected by the Colonial Pipeline ransomware in May 2021. I was doing a Permanent Change of Duty Station (PCS) from Fort Stewart, GA to Fort Hood, TX. Driving a U-Haul Truck across the country where 2 of 3 gas stations were out of fuel was a painful experience. The threat of being Absent Without Leave (AWOL) is a great motivator and I made it to Texas on time, but fear blooming from something I have absolutely zero control over was severe.

The website Safety Detectives has an extensive rundown of statistics regarding ransomware. The graphs below⁴ show humans are the weak link in cyber awareness and fall victim to social engineering. We’re too trusting! Turn up the skeptical-meter. I was surprised that the cost of downtime for businesses was so high, especially in comparison to the average cost ransomware extorters demand. It seems like the extorters do their research into what a company will be willing to pay prior to enabling

A close-up of a graph

Description automatically generated

the ransomware. This creates a negative spiral of perpetuity. Ransomware strikes 🡪 Cost/benefit analysis shows paying ransom cheaper than recovery measures 🡪 ransom paid, hopefully data decrypted 🡪 extorters have business model to use again.

Knowledge management is an art and completely essential. Having your data organized in a consistent manner, scoured regularly to delete unnecessary data, and branched in file explorer for ease of backup is crucial. Far too often, I’ve seen a PC desktop inundated with random folders and files in a messy hodge podge. Cleaning up and maintaining your data needs to be a staple in your battle-rhythm to ensure efficient bandwidth and data storage usage.

It's probably a good practice to NOT backup your downloads folder, as that’s the likely location for malware. This means taking the precious few seconds to move files out of the download folder and placed into an appropriate folder.

Another concept that came from left field for me is with added protection, we enabled bad actors. Strong encryption like RSA-2048 or AES are an amazing tool to help the average user. These algorithms have helped protect our data…. until ransomware extorters used the same algorithms to withhold our data from us. The average organization doesn’t have access to Uber-advanced AI, quantum computing, or billions of years to decipher these encryptions.

Ransomware doesn’t just appear on a system. It must be loaded by a user. Cybersecurity awareness and policies are the most important deterrent. If something looks slightly off or incorrect, play it safe. Don’t open the attachment, click the link, visit bad news bears websites, or play around with weak passwords. A cyber smart workforce sounds amazing but getting buy-in and shared understanding prior to an incident is a struggle. The Department of Defense mandates all network users to complete a Cyber Awareness Training at least once a year. Soldiers have been known to start the lesson, open another browser tab, search for the answers, and continue mission with their brain turned off. That’s check the block training that isn’t being absorbed.

I feel like the slimiest part of ransomware is the software sits idle before code execution. It can be timed or have a trigger. This creates the possibility for the ransomware to be present on the data backups which is an additional risk. There are ways to mitigate this by complete disconnection from networks known as air gap and by troubleshooting within a sandbox. The only action that smells more of a weasel would be a ransom paid and no key delivered.

Ransomware as a Service (RaaS) is relatable to bot creation for DDoS. These ransomware developers are using morally challenged opportunists to exploit organizations. Several articles spoke on RaaS being a response or product of Software as a Service (SaaS). It’s almost as if the RaaS developers are taking business cues and models from SaaS professionals in Silicon Valley. I was also intrigued that the primary geographical locations of ransomware and other malware attacks come from centralized places. They operate in a grey area of not being state sponsored, but also not prosecuted by the state they live in. I’m not sure on an answer to this dilemma, but it could very easily lead to armed conflict if the wrong target is chosen.

The NIST cybersecurity framework continues to be the standard – Identify, Protect, Detect, Respond, and Recover. An additional protective measure is network segregation. In the military, we use this daily. We have four popular forms of network security levels:

1. Colorless Network or “Dirty Internet”
2. Non-Classified Internet Protocol Router Network (NIPR) – For General Use
3. Secret Internet Protocol Router Network (SIPR) – Classified network that requires US Security Clearance
4. Combined Enterprise Regional Information Exchange System (CENTRIX) – Classified network for non-US coalition partners

This is a broad stroke on segregating networks or capabilities, but the concept can be refined and dialed down to a micro level to help protect an organization’s network. The military also uses Multi-Factor Authentication (MFA) for access to any service or website that contains Controlled Unclassified Information (CUI) or a higher level of classification. This is similar to WTAMU’s MFA to sign into the student portal.

Without a deliberate plan in place to deal with a real-life ransomware incident, chaos can ensue quickly. Airman Dzimeila walked into a scenario in Western Texas without a plan in place, but his team and the Texas National Guard were able to rapidly take corrective action. Delineating who is in charge given a scenario, or created a decision matrix for leaders to reference can also come in handy to expedite the recovery process. We can’t always rely on the government to save the day. Contingency planning has its place as long as we don’t go too far down the rabbit hole and plan for every possible scenario. That’s just a waste of time.

With ransoms being paid, ransomware will continue rise as a threat. Vigilance in cyber security awareness training, policies – both administrative and network rules, IDPS, firewalls, incident recovery plan testing, and humans making smart decisions are critical for network security. The ongoing struggle of black hats and white hats will carry on. Do your part to be one of the good guys and think before you click.

1. The 2021 TLS Telemetry Report

https://www.f5.com/labs/articles/threat-intelligence/the-2021-tls-telemetry-report

1. Ransomware Backup Strategy: Secure Your Backups

https://spinbackup.com/blog/ransomware-backup-strategy/#Keep\_Multiple\_Backup\_Versions

1. The Current State: Vendor Saturation

https://www.apptega.com/blog/too-many-cybersecurity-vendors

1. Ransomware Facts, Trends & Statistics for 2023

https://www.safetydetectives.com/blog/ransomware-statistics/