**Ransomware Recovery by Lana Bracken**

**1. What Did You Do?**

To develop a ransomware recovery plan, I assessed my home network and critical endpoint data storage using findings from previous assignments: Managing My Network (Assignment 1), Nmap scanning and service enumeration (Assignment 2), and vulnerability assessments using ShieldsUp and Nessus (Assignment 4). This holistic approach enabled me to identify, evaluate, and prioritize both network-based and endpoint-based vulnerabilities, leading to a practical recovery strategy in the event of a ransomware attack.

I approached the task in five phases:

**A. Network Inventory and Criticality Assessment**

Using results from my Nmap scans (ping, intense, and slow comprehensive), I compiled a list of active network devices. I cross-referenced scan results with my previously documented network topology to determine each device’s function, connection method (wired or wireless), power source, and role in daily operations. This allowed me to prioritize devices based on business, educational, and personal importance, especially those with data or services that must be restored quickly after a ransomware attack.

**B. Backup Needs Identification**

I used device roles and observed services (e.g., MySQL, SMB, Intel AMT on my laptop) to determine which systems required regular backups. For each, I considered whether the system stored valuable data or held configuration settings essential for rapid recovery.

**C. Vulnerability and Update Requirements**

I then reviewed vulnerability data from ShieldsUp and Nessus to identify devices with outdated software or insecure configurations. Nessus provided internal vulnerability details and ShieldsUp helped confirm which services were externally exposed to the internet.

**D. Password Role Documentation**

Finally, I compiled a list of roles associated with device passwords that would need secure storage and recovery in a ransomware scenario. This did not include actual passwords, just identification of credentials critical to recovery.

**E. Endpoint Data Vulnerability Assessment**

I analyzed the potential impact of ransomware on data stored locally on a frequently used USB drive, identifying sensitive data types and operational dependencies.

**F. Recovery Plan Storage and Review Frequency**

As part of this process, I also planned how the recovery documentation itself would be stored and accessed in the event of an incident. Additionally, I decided on a schedule for periodically revisiting and updating the recovery plan to reflect changes in the network or its vulnerabilities.

**2. What are the results?**

The following deliverables were developed:

**a) Prioritized Recovery List**

| **Priority** | **Device** | **Role** | **Reason** |
| --- | --- | --- | --- |
| 1 | Laptop (LanaB-LP) | Work/School | Hosts critical data, SQL servers, Intel AMT, school files |
| 2 | iPhone | Communication | Essential for personal/business use, emergency alerts, and news access |
| 3 | Docsis-Gateway | Router | Provides internet access and network routing; easily replaceable |
| 4 | Wi-Fi Extender | Network Mesh | Extends signal coverage to key areas |
| 5 | HP Printer | Utility | Hosts SMB and web interface; part of workflow |
| 6 | iRobot, Google Home | Convenience | Minimal data loss; easily reconfigurable |
| 7 | Apple TV, Roku, IoT | Entertainment | Non-critical, lowest recovery priority |

This prioritized list is crucial for a phased recovery approach following a ransomware attack. Restoring the Laptop (LanaB-LP) first ensures rapid resumption of work and school activities. The iPhone is prioritized for communication, essential for coordinating recovery efforts and staying informed. The remaining devices are prioritized based on their impact on essential services and convenience, enabling a systematic and efficient restoration of network functionality.

**b) Backup List**

| **Device/Service** | **What to Back Up** | **Why** |
| --- | --- | --- |
| Laptop | Documents, MySQL/SQL config, app data | Work-critical and school-related content |
| iPhone | iCloud credentials, key app logins | Primary communication device; vital for account recovery |
| Router | Config file, SSID/passwords | Core to restoring internet and network structure |
| Printer | Admin login, network config | Avoid setup delays |
| Wi-Fi Settings | Stored SSIDs, passwords | Speeds up IoT reconfiguration |

This backup list prioritizes data and configuration settings essential for rapid system restoration. Backing up documents and application data on the laptop ensures minimal data loss for work and school. iCloud credentials and key app logins on the iPhone are vital for communication continuity. Router and Wi-Fi settings facilitate swift network reconfiguration. Printer settings minimize setup delays. A comprehensive backup strategy is critical to minimize downtime and data loss following a ransomware attack.

**c) Password Role List**

* Router admin
* Laptop local account
* Printer admin
* MySQL/SQL Server login
* Wi-Fi network credentials
* Google and Apple accounts linked to smart devices
* iCloud/Apple ID for iPhone

**d) Devices Needing Updates (from Nessus)**

| **Device** | **Vulnerability** | **Recommended Action** |
| --- | --- | --- |
| Router | DNS recursion, TFTP, UPnP | Disable TFTP, restrict recursion, disable UPnP |
| Laptop | Intel AMT, open MySQL/SQL ports | Disable unused services, enable firewall |
| Printer | Self-signed SSL, SMB, PUT method | Update firmware, restrict access, disable risky methods |
| Multiple | ICMP timestamps | Block ICMP at firewall |

Updating vulnerable devices is essential to reduce the attack surface and prevent ransomware from exploiting known weaknesses. Addressing DNS recursion on the router is a critical first step to mitigate potential DDoS attacks. Securing the laptop's services and the printer's configurations limits lateral movement and data exfiltration. Blocking ICMP timestamps enhances overall network stealth and security.

**e) Device Inventory (from Nmap)**

|  |  |  |
| --- | --- | --- |
| IP Address | Device Name | MAC Address / Vendor |
| 192.168.1.1 | Docsis-Gateway | A4:CF:D2:4E:2B:BF (Ubee Interactive) |
| 192.168.1.16 | Google-Home-Mini | 7C:2E:BD:65:4E:79 (Google) |
| 192.168.1.35 | Tstat-73C72C | B8:2C:A0:73:C7:2C (Resideo) |
| 192.168.1.49 | iRobot | 50:14:79:55:D6:3B (iRobot) |
| 192.168.1.61 | RokuStick-663 | B0:EE:7B:C3:94:5B (Roku) |
| 192.168.1.115 | Smart TV | 2C:64:1F:73:75:C8 (Vizio) |
| 192.168.1.121 | Entertanment Room | C0:95:6D:98:A1:FE (Apple) |
| 192.168.1.133 | Apple TV | B8:78:2E:32:0A:4B (Apple) |
| 192.168.1.151 | HP Printer | 3C:52:82:1C:95:C1 (HP) |
| 192.168.1.185 | Tstat-746A10 | B8:2C:A0:74:6A:10 (Resideo) |
| 192.168.1.248 | iPhone | 32:02:7A:CE:E3:67 (Unknown) |
| 192.168.1.46 | LanaB-LP | — |

This device inventory provides a comprehensive overview of network assets, allowing for targeted recovery efforts. Knowing the device type, location, and connectivity method is essential for efficient restoration of network services and connectivity after a ransomware attack. All devices are wireless exception of the router and the laptop as needed.

**f) Endpoint Data Vulnerability Assessment – USB Drive**

The analysis of the USB drive attached to the work laptop reveals a significant vulnerability to ransomware. The drive contains a wide array of sensitive personal and professional data:

* Personal identification documents
* Family photos and videos
* Medical records
* Financial information
* Schoolwork
* Work-related feedyard databases

Because this device is physically attached to my laptop, ransomware that infects the host system could easily encrypt the contents of the USB drive, potentially causing catastrophic data loss.

Additionally, the USB drive plays a functional role in my workflow by offloading large datasets from my laptop’s limited internal storage, particularly for feedyard database work and school assignments. This creates an operational dependency on the device beyond simple storage.

Mitigation strategies include:

* Encrypting the drive to protect sensitive data
* Performing regular backups to a separate, secure location
* Physically securing the drive when not in use
* Implementing endpoint protection tools on the host laptop to detect and prevent ransomware behavior
* Avoiding always-on connection: the drive should only be plugged in when actively in use to minimize exposure to malware or ransomware infections

This assessment highlights the need for robust endpoint protection and data management strategies within the overall ransomware recovery plan. Implementing encryption and regular backups are critical to ensure data recovery. Segregating personal and professional data onto separate volumes will further improve recovery efficiency and data governance.

In addition to securing the USB drive itself, it is also important to address data separation. Currently, the drive stores both personal and professional data in the same location, which creates unnecessary risk. In the event of data loss, recovery processes for personal and work-related materials may have conflicting priorities. Moreover, mixing sensitive business data with private personal content complicates compliance, confidentiality, and accountability. Going forward, these data types should be segregated onto separate encrypted storage volumes or devices to support more structured, policy-compliant recovery planning.

**Deficiencies and Fixes**

* The Wi-Fi extender did not appear in any scan. Future scans may need to include alternative methods or direct connection tests.
* Some vulnerability classifications were vague due to Nessus plugin limitations under the free license.
* Not all IoT devices provided clear service data; manufacturer tools or alternate scanning techniques may improve coverage.

The initial Nmap and Nessus scans primarily focused on network devices, neglecting the vulnerability of data stored on endpoint devices like the USB drive. This highlights the need to supplement network-centric scans with endpoint-focused data protection strategies.

**Recovery Plan Maintenance and Accessibility**

To ensure the recovery plan is both secure and accessible during an actual ransomware event, I decided to store it using a hybrid approach based on the 3-2-1 backup rule. This means maintaining three copies of the recovery plan: one primary version, one backup on a different type of media, and one offsite. Specifically, I keep an encrypted digital copy in a cloud storage account protected by two-factor authentication, and a printed hard copy stored in a secure, fireproof location in my home. For materials that can reasonably be preserved in physical form—such as network diagrams, password role lists, or emergency contact sheets—hard copies will be prioritized. For purely digital items like device configurations or encrypted credentials, backups will be stored on an external hard drive or encrypted USB device as appropriate.

The offsite backup is stored at a family farm two counties away, which includes a farmhouse, a cellar, and—if needed—a safety deposit box at a local bank in town. This location was selected specifically because it is accessible yet geographically separate, reducing the likelihood that the same natural disaster or localized event would affect both locations simultaneously.

I also established a regular maintenance schedule to review and update the recovery documentation every six months, or immediately following any major changes to the network, device inventory, or threat landscape. This helps ensure the recovery plan remains accurate, relevant, and actionable over time.

**3. What Did You Learn? (Key Takeaways)**

This assignment has significantly heightened my awareness of the threat landscape at home. I’ll admit — I’ve become a bit paranoid, but in a good way. For example, before shutting down my computer at night, I now email an updated copy of any report I’m working on to my Gmail account, just in case I wake up to a ransomware attack. That’s not fear — that’s preparedness. The assignment achieved its goal: I’m not just aware of the risks, I’m already acting to reduce them.

One of the biggest takeaways for me is how vulnerable endpoint devices really are, especially my laptop and the USB drive I rely on for both school and work. The reality that ransomware can easily encrypt both has forced me to reevaluate how I store and separate personal and professional data. From now on, I plan to keep these data types isolated and follow backup strategies like the 3-2-1 rule. Having offsite, offline, and encrypted copies is no longer optional — it's essential.

I’ve also started mapping out realistic recovery options. If my laptop is compromised, I could go into my company’s office in Amarillo and request a replacement system. Since I’m salaried, I wouldn’t miss pay — but my productivity would take a hit. In a pinch, I could also use a computer at the local library or on campus at WT. Older laptops at home could also serve as temporary recovery platforms for basic recovery tasks.

The device I worry about most, though, is my phone. It’s my communication hub — not just for work and school, but also for emergencies, authentication, and access to nearly everything I use daily. If it were lost or encrypted, I’d be in trouble. That’s why I’ve been thinking about low-cost backup options, like keeping a cheap spare phone around in case of hardware failure or even supply chain disruptions, like those triggered by tariffs. In that sense, preparing for ransomware and preparing for economic uncertainty share a common theme: prevention and planning help you stay functional when things go wrong.

When I evaluated my other devices, I realized that most IoT components (vacuum, smart TVs, etc.) aren’t critical. If ransomware hit them, it would be frustrating but not devastating. Even my smart thermostats, which are hardwired into the wall, could be isolated by disconnecting the router. It’s comforting to know I could power down or unplug most devices and deal with them later without major impact.

Finally, I now fully understand the importance of documenting configuration settings, license keys, and recovery procedures in advance. At past jobs, my developer laptops came from a prebuilt image, making recovery easier. Today, if my laptop were lost, it could take days to reinstall software and rebuild my environment from scratch. Having a structured recovery plan — not just for data but for workflow continuity — is something I’ll continue to build on.