Assignment 4 Ransomware Recovery

What Did You Do

I utilized the nmap results to identify assets on my network that are important to my current network and external environment. I utilized the results of Nessus to identify any areas that needed to be shored up to be more secure. I also researched cloud-based solutions that could be used to help achieve additional security.

What Are the Results

Deliverables

Procedures and Policies

- Good policies and procedures are crucial to not only restoring access in case of the worst case scenario but also help by (hopefully) preventing the necessity. The types of procedures and policies that are important for ransomware attacks include:
    - Backup Policy: All files that are unrecoverable (e.g., not a part of the base OS or that are easily retrieved) need to be backed up.
        - Utilizing a cloud-based backup where files can be easily backed up to. Examples of this can include services like OneDrive from Office 365, which can store files as if they were local copies in the cloud. To be secure, they need to be versioned, which (Gluck, Mazzoli, Buck, Davies, & Simpson, 2023) indicates is a standard feature of Office 365. Versioned files help with the restoration effort if any files are encrypted.
        - Cloud-based servers (e.g., VPS) can be backed up by the cloud service provider at a specific cadence. This way, if a ransomware attack succeeds, the backups are kept with the cloud vendor, which is normally controlled in a completely different way. For example, if a developer is compromised, they may provide access to a specific system, but a central admin controls the actual cloud-based servers from an administrative perspective.
            - (Gupta, 2023) also suggests storing encrypted backups in multiple locations (e.g., Microsoft Azure) to ensure extra redundancy.
        - Local backups can be utilized for files that must be shared across multiple devices on a network. Utilizing a NAS that can be configured to back their data up to cloud services like OneDrive or Box is essential.
        - Network Devices should have backup copies of their configurations loaded to a cloud source whenever changes are made as a part of the deployment strategy. Preferably with versioning history capabilities, so changes can be quickly reverted in case of encryption.

    - Restoration policy: which defines if the worst happens and how we recover. For my network, this would be:
        - Web server – Since this is a VPS, we should be able to make restoration very quickly and utilize database backups and any files related to the web services. Minimizing impact on customers means that we lose less money over time and is essential for us to get those services up and running first.
            - (Gupta, 2023) recommends conducting test restorations in a test environment at regular cadences, weekly tests should be sufficient.
        - NAS – The NAS provides access to common files across the network and can be used to more quickly restore computers that need to be wiped clean. Restoring a clean version of the NAS from backups can help ensure that data is available (e.g., copies of software that needs to be installed on computers will load much faster from a NAS instead of downloading it multiple times from the internet)
        - Individual Computers – The individual computers should be prioritized last since they will take the longest to restore and offer relatively low value for the most part.
- Password Policies:
    - The required use of a password manager tool that is cloud-based (e.g., 1Password). This also helps ensure that users have secure passwords using the generate a password functionality since they can quickly store the username and password within the password manager.
        - Using tools like these allows us to store common items (e.g., passwords, encryption keys, certificates) into secured areas (1Password uses vaults) that can be granted to individual users when needed. This helps with the separation of duties and also helps minimize the risk of users having too much access since the access is provided centrally.
    - Using a single sign-on tool (such as Okta) is also essential from a security perspective. Most commonly used software (especially cloud-based ones, more on that later) have the ability to do single sign-on. Tools like this help to:
        - Enforce policies:
            - Password requirements, frequency of changes
            - Multifactor authentication (e.g., using a YubiKey, Duo)
        - Easily provision users (e.g., create a user with appropriate permissions)
            - This is particularly useful when using an HR system like Workday, where users can be pre-configured based on their role to get all of the tools that they need without needing individual configurations.
        - Termination of access if employees are terminated.
- Email Policy
    - The email server is configured with phishing protection tools (e.g., Material) that require users to verify that they requested sensitive things (e.g., password resets, invoices). They do this by implementing a second level of protection using MFA.
    - Prevent certain types of attachments from being included (e.g., zip files). If files do need to be shared, use a company-authorized service (e.g., OneDrive sharing) should be used

after establishing that it is a file that is needed by communicating with the sender in some fashion other than a simple email.

- Antivirus/Malware Protection
    - Require that Antivirus and/or Malware protection of some sort has been configured on the system before it is allowed onto the network (e.g., Windows Defender)
- Assets
    - An ITAM system (e.g., Atlassian) should be used to track all hardware and software assets. To help with Ransomware, using a cloud-based system would allow for additional security since the cloud-based system can't be encrypted against its will since most systems like Atlassian or Service Now give users access in a walled garden. Backups of those systems can be done separately.
    - (Ellingwood & Garnett, 2022) suggest regular (weekly) service audits of systems using tools (e.g., Nessus) should be used to scan for any open ports needed to ensure proper security.
    - Regular (weekly) general audits should be conducted using tools (e.g., Nessus) to identify any vulnerabilities that need to be addressed (e.g., zero-day vulnerabilities)
    - Unattended updates/upgrades should be configured for all systems to ensure that they are kept as up-to-date as possible

Backups

Backups of the Cloud server (in accordance with the policy) are controlled as follows:

1) Utilize the VPS (DigitalOcean) backup systems to
    a. Store encrypted copies backups in a separate Azure bucket
2) Backup cloud-based solutions data, sometimes this requires a separate backup service that is specifically configured to work with that solution (e.g., OwnBackup and ServiceNow)

Backups of the local network (in accordance with the policy) are controlled as follows:

1) Router (192.168.1.1): A backup of the router's configuration is kept on the NAS.
2) NAS (192.168.1.254): Configured to back up to a cloud service (OneDrive)
3) Main Computer (192.168.1.75): All essential (unrecoverable) files are backed up to OneDrive automatically using OneDrive business, which is versioned, and, therefore, automatically protects against ransomware.
4) Work computer (192.168.1.83): All files are backed up via OneDrive (stored in my works OneDrive instance)

Software Updates

Cloud Servers

(Ellingwood & Garnett, 2022) suggest using unattended updates and upgrades with any instances running.

Network Devices (e.g., Router, NAS)

If available, unattended updates else checking on a weekly basis

Individual Machines

Use policy-based tools (e.g., Active Directory) to enforce automatic updates of local software (e.g., OS, browsers). My work computer (192.168.1.83) is configured as a part of such a policy tool

Passwords

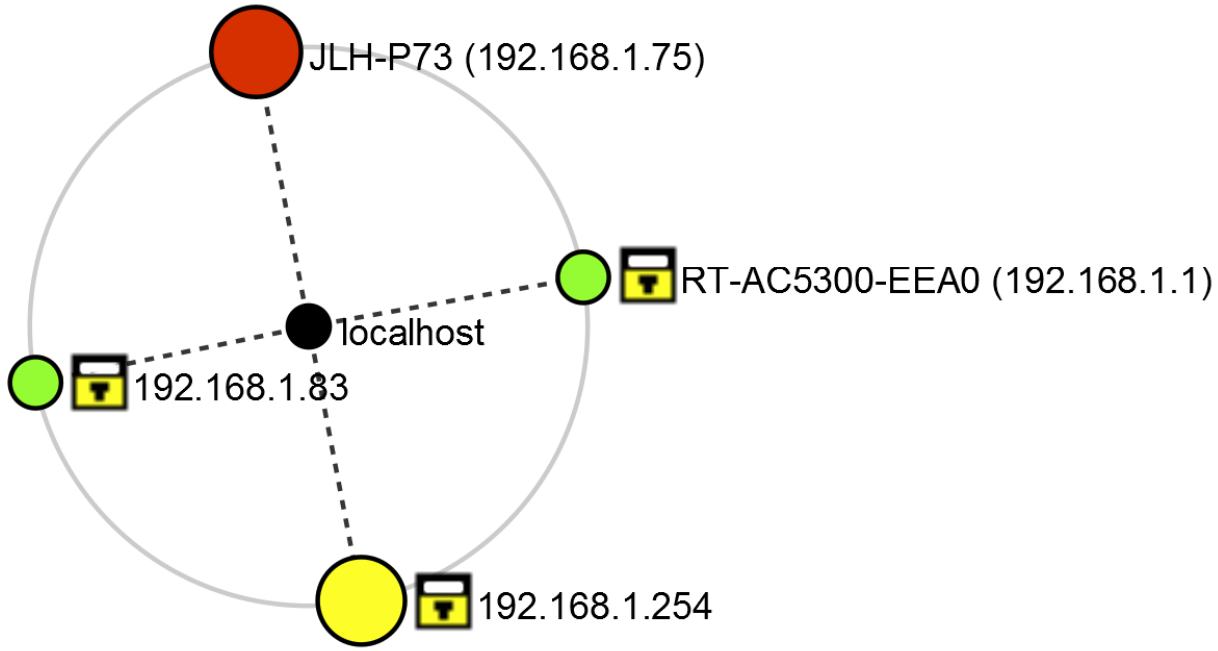
- Password managers are utilized to store all passwords needed for access. The only password I need to remember is the master password for the password manager. I use a personal password manager as well as one that my work provides me to store the data that I need in a secure fashion (e.g., software keys, SSH keys, credit cards). Some passwords that I have identified as needing to be backed up (and are) in my password manager are:
    - Router
    - NAS
    - Office365 (which contains my backups)
    - DigitalOcean (Cloud VPS provider)
- My cloud-based server is configured with key-based authentication, which is handled by 1Password acting as the SSH authentication agent and requires me to use biometric and/or master password authentication to access my cloud server via SSH.
- I also use a work-provided 1password account for my work computer. It stores information I need in order to access work systems that aren't done via Okta (normally service accounts)

Inventory

The following is the order by which access should be restored in case of a ransomware attack:

- cidm-5310.hardy-computer.systems – Cloud VPS
- 192.168.1.1 – Router
- 192.168.1.254 – NAS
- 192.168.1.75 – Personal PC
- 192.168.1.83 – Work PC

Network Topology



Deficiencies

- Nessus found that my cloud-based server had two bugs identified. They were low-impact and would be addressed with automatic software updates.
- SSL Certificate – The certificate was identified as one that wasn't completely trustworthy; remediation would be to get a different certificate

What Did You Learn

Due to my years in IT, I am very familiar with most of the aspects of Ransomware.

Takeaways

- My prior experience in IT has prepared me for many of the fundamentals of security for Ransomware. I have outlined the information based on my experience in IT over the past 20+ years as well as working in various industries that require different security requirements (e.g., financial services and publicly traded companies).
- Cloud-based technology is the largest gap that I saw with some of the design approaches; I learned that according to (Gluck, Mazzoli, Buck, Davies, & Simpson, 2023), Office 365 has many ransomware features built into their solution.

Future Organization Value

- Security is one of the fastest-growing sections of IT. Ransomware attacks are some of the most pernicious that have been seen in recent years. With proper policy and preparation, they are also some of the most preventable. Security is something that is everyone's responsibility within an organization. Organizations, both small and large, must work on having their security procedures well-defined and practiced. In addition to being in IT for the past 20+ years, I also grew up in an IT household. I grew up listening to my father conducting disaster recovery drills

(he still does to this day, we were just chatting about a recent one he did a couple of weeks ago), and ransomware is just another type of disaster. Organizations that follow (and enforce) policies that are forward-thinking will find themselves in much better stead.

References

Ellingwood, J., & Garnett, A. (2022, May 05). *Recommended Security Measures to Protect Your Servers*. Retrieved from DigitalOcean: https://www.digitalocean.com/community/tutorials/recommended-security-measures-to-protect-your-servers

Gluck, D., Mazzoli, R., Buck, A., Davies, J., & Simpson, D. (2023, 03 02). *Malware and ransomware protection in Microsoft 365*. Retrieved from Microsoft Compliance: https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

Gupta, B. (2023, 02 06). *Cloud backup best practices for SMBs*. Retrieved from DigitalOcean: https://www.digitalocean.com/blog/cloud-backup-best-practices-startups-smbs