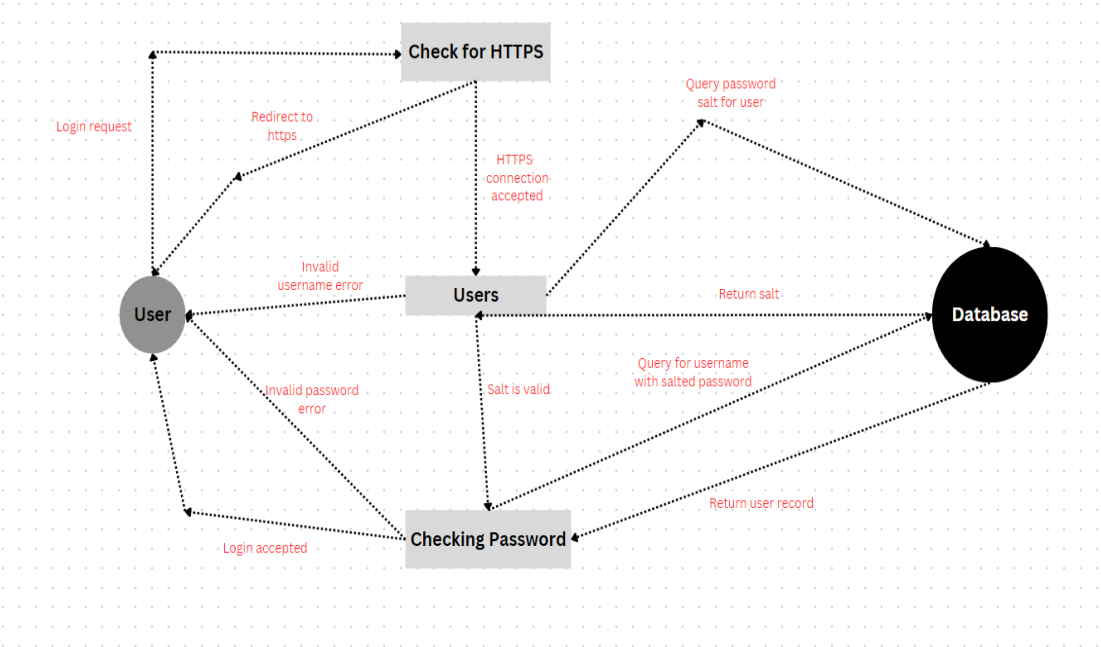
Task 1:

To uphold the security against various cybercrimes, including potential servers and accounts, several things can be taken care of like Keep software, operating systems, and applications up to date with security patches to protect against known vulnerabilities, Limiting the access privileges to critical systems and data, granting access only to those who need it and regularly back up important data to secure, off-site locations to mitigate data loss in case of malware attacks. Also, we can Utilize strong, unique passwords for all accounts. Implementing multi-factor authentication where possible to add more security. Installing anti-virus can secure from malicious attacks and Implement email filtering and train staff to recognize phishing attempts.

Regarding personal experiences with cybercrimes, I don't have personal experiences with any kind of cybercrimes but for preventing for attacks we need to knowledge evolving threats and also staying updated to the latest threats and security practices is the best way to be safe.

Task 2:



Task 3: Social media security policy

The social media security policies are a class of guidelines where every individual or any institution should follow as the policy says. Social media became a part of our daily life that they are portals to news, information, communication between friends and families, business opportunities, political mattes and also mainly for entertainments.

Importance of social media security policy:

Social media platforms are now a days relevant in personal and professional purposes of every human and platforms like Facebook, Instagram, Twitter, YouTube, WhatsApp, LinkedIn for sharing information and interact with other people. For securing all these information a fine security policy is required which boost the trust of customer's using these platforms and increases the value of the company too. It also helps the employees to know about what do's and do not are there in the platform and also stand ecofriendly to the society without doing anything wrong.

Using different automated social media managing tools, tracking and ensuring vulnerable activities, unusual behaviours and other kinds of malpractices, it can act as it is coded and alert the customers and companies at the same time. So, breaking such kind of policies can easily find and took essential steps against that which is easy and completely automated now a days.

Social media policies can be updated so that we can prevent the malwares and other kind of social media attacks such as phishing attacks, account hacking or fake profiles etc...

Giving awareness on exposing too much personal information is through social platforms will lead to protect from hackers and other attacks. Clarifying account ownership should do because other people may enter into other's account and the platform would not be responsible, they can alert us only the account owner has been specified.

Content Guideline:

Providing information about what kind of contents are allowed to pass and share through the platform. Most of the policies include content guideline as it affects their standard of usage and people of all kind are using it. Also highlight the consequences and other actions taken by the company if any sensitive contents shared or sharing confidential information.

Privacy:

Instructing users about the privacy requirements and enabling security increasing settings like two-factor authentication on their social media profile also preventing them from sharing of personal information. Taking care of privacy settings can keep the users their profile private or they get notified any outsider trying to infiltrate. Security policy provide a clear process for reporting any suspicious activities in our social media account so that we can report them.

In this era of technological changes, maintaining a social media policy is crucial. As social media is emerging, so do the threats too. A social media security policy is necessary as it is related to our privacy, so that usage of social media platform should be very careful and should not affect any other person in any way. Monitoring the activities on social media platforms can make sure that the customers or users are following security guidelines as it says so that can prevent attackers to a certain extent. As we discussed Automated tools, Login authentication, Privacy setting managing, Policy updating are some of the major ways of monitoring.

CLOUD USAGE/SECURITY POLICY

A cloud usage and security policy are a set of procedures to govern the use of cloud service and also it ensures the security of data or documents in the cloud. Cloud usage refers to practice of utilizing cloud computing services to manage, process and access data and application all over the internet. Such a technology is crucial in today's life, as more businesses and institutions are adopting cloud technology for their development. The cloud advantages have contributed to the widespread adoption in various industries. A security policy is a critical component of organizations all over also in information security strategy. It serves for maintaining the security of data, systems and resources.

The scope of cloud usage or security policy defines where this policy applies within an organization. In applicability specifies in which individuals, groups or entities within the organizations are subjects to the policy. If in cloud service it defines the type of cloud service and providers that fall within the scope of the policy. In data classification it describes how data classification is addressed within the policy and in access control explain the requirement of managing access to cloud services. Security monitoring is essential to protect sensitive content stored in cloud environment and in data encryption specifies the encryption requirements relevant to the industry or geographic location.

Authorized cloud services refer to cloud computing services that have been evaluated or approved by an organization or government entity. These services meet specific security, compliance, and regulatory requirement, making them suitable for data storing, processing. Some of the examples of authorized cloud services providers may include Amazon Web Services (AWS), IBM Cloud, and Oracle Cloud, Microsoft Azure, Google Cloud Platform (GCP), among others. Some key aspects of authorized cloud services are security compliances, data encryption, audit and logging, incident response, continuous monitoring and also data residency and sovereignty. Additionally, organizations may need to implement their own security measures and policies to ensure protection of their own data.

Data classification and security policies are essential components of cloud storage and data security strategies and they help organizations define, categorize, and protect their data based on its sensitivity and importance. Data classification define categorizing data into different levels of sensitivity or importance based on its value and constants. This classification helps organizations determine how data can be handled, stored or protected in the cloud. Common data classification includes public data, internal data, confidential data and critical data. A security policy for cloud storage includes rules, procedures and measures how data is protected within the cloud environment. Key elements for cloud storage security policy include access control, data retention and deletion, monitoring and auditing and third-party vendor assessments.

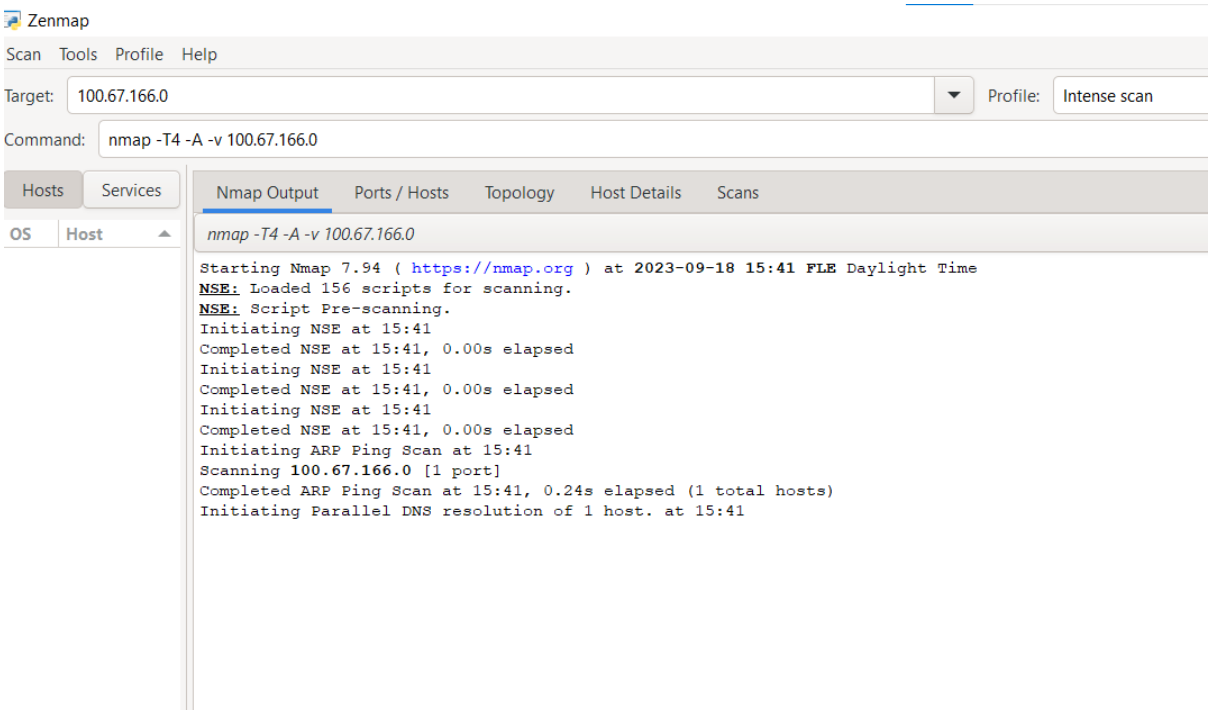
Access control is a critical component of cloud storage security policies and it can determine who can access cloud resources, what action they can perform, and under what conditions. Also, they help to protect our data and prevent unauthorized access and ensure confidentiality, integrity, availability of information stored in the cloud. Authentication, authorization, user roles and permissions, least privilege principle and resource level access control. Data backup and recovery policies are essential components of comprehensive cloud storage policy and it define how an organization's data is backed up, stored and recovered in the event of data loss, disaster or security incidents. A well-defined data backup and recovery policy helps to reduce data loss and also recover from data incidents efficiently and effectively.

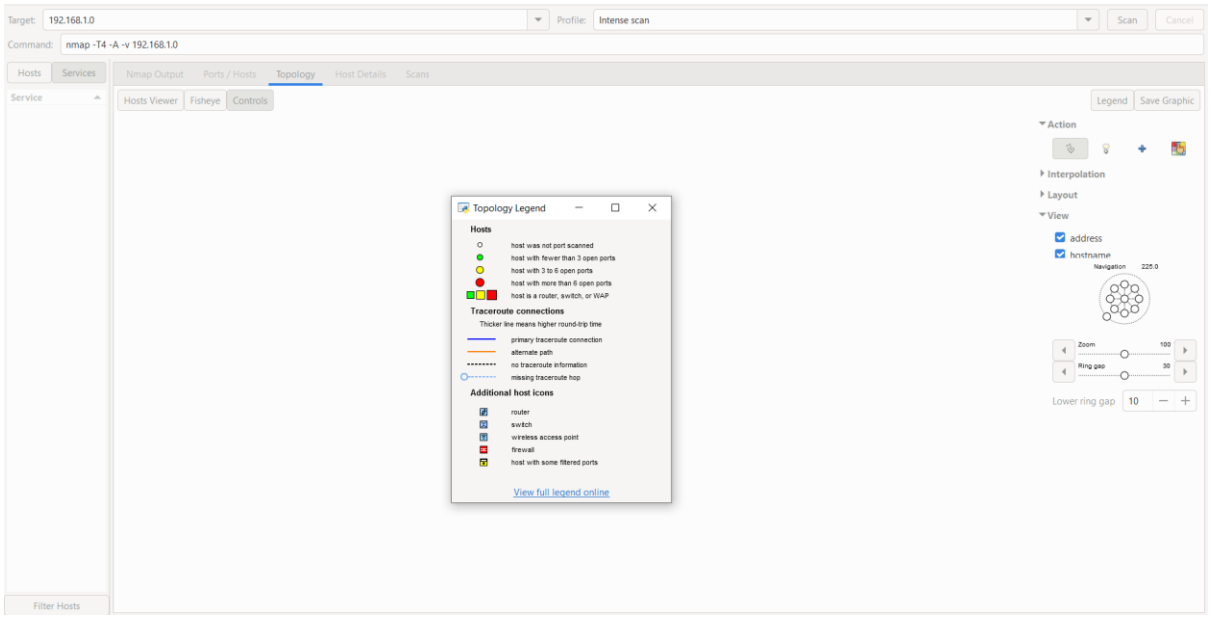
Compliance and regulations are crucial aspects of a cloud storage security policy and it help to ensure that data is stored in the cloud and it's important to work closely when developing and implementing compliances related policies. A significant role in shaping both cloud storage and security policies. Security monitoring is a crucial aspect of both cloud storage and security policy and it include continuous monitoring of your cloud environment to detect and respond to security threats. It is an integral part of an effective security for cloud storage and by adding security policy and ensure it is well-integrated cloud storage. Incident responses is critical components of both cloud storage policy and a broader security policy, these plans and procedures help organizations to detect, mitigate, and recover from security incidents.

Training and awareness are vital components and it helps to educate employees and stakeholders about security best practices and procedures related to cloud storage. It should be tailored to the specific needs and roles of employees within the organization. Regular policy reviews are crucial to ensure the cloud storage and security policies remains effective and up to date in organization's operations.

Task 4:

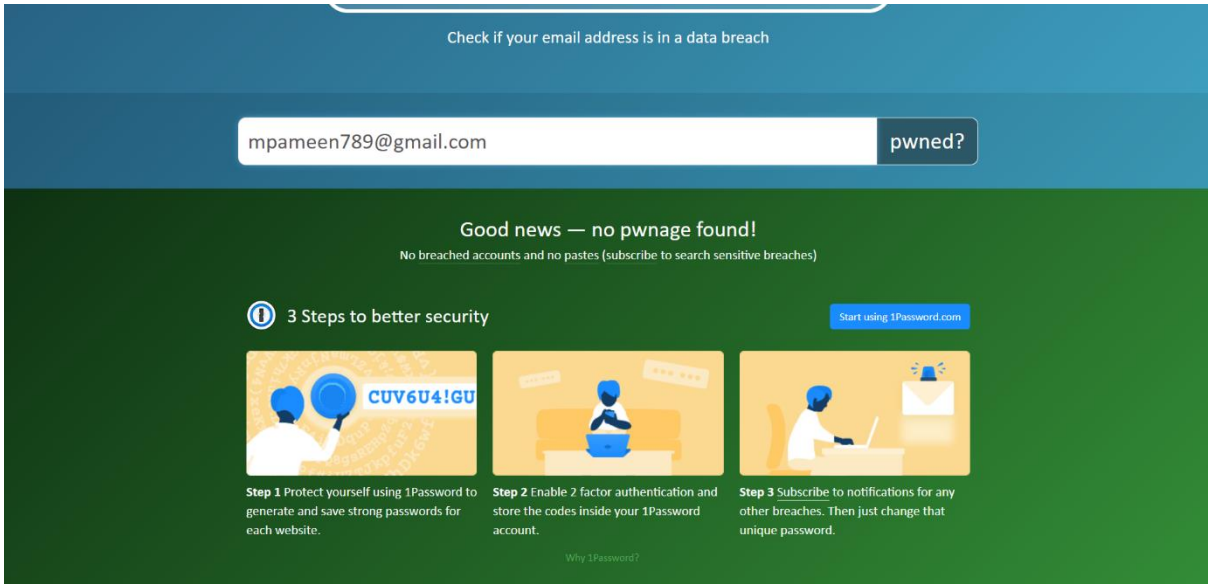
A:





No, I haven’t found any devices that not to my knowledge. Nmap didn’t find any vulnerabilities with the sc

B:



My account details haven't leaked so that I didn't change the password.

C: Facing some problems dealing with the localhost.