SUBMIT (5pts) what is the IP of your Kali linux machine? 192.168.85.130

(5pts) what is the IP of your target machine? 192.168.85.0/24 192.168.85.132

(5pts) What command did you use to find the IP of the target? Nmap -script=msql-info 192.168.85.130/24 21

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated?(5pts) What command A computer screen with white text

Description automatically generatedA screenshot of a computer program

Description automatically generateddid you run to show that MySQL isA screenshot of a computer

Description automatically generatedrunningA computer screen shot of a program

Description automatically generated

(5pts) Take a screenshot showing your connection to Metasploit right after you run the python command (this one should show ‘root@metasploitable’) couldn’t get to it ran out of time trying all day.

(5pts) Take a screenshot of MySQL after you connect with your globalID from the Kali terminal.

couldn’t get to it ran out of time trying all day.

(5pts) Take a screenshot of MySQL showing the credit card info from the owasp10 database; To ensure this isn’t just a keyboarding exercise, please answer the following: couldn’t get to it ran out of time trying all day.

(15pts) you evaluated the server, now in at least ½ page what did you learn, what are your conclusions, what are your recommendations? I know that you are not system administrators but common-sense will get you a long way. At the same time, please be specific, don’t just answer ‘fix it.’ You can still have specific recommendations. GRADS: in your response above include specific information on preventing this attack. Be specific about the steps to take, include resources/references. At least a page and a half.

After assessing the server in question, I found a number of critical problems that must be fixed to strengthen system security overall and stop future assaults. Despite the fact that I am not a system administrator, I can provide some sensible advice that may assist reduce the dangers connected to the vulnerabilities found.

1. Systems for Detecting and Preventing Intrusions (IDPS):

Install an IDPS to keep an eye out for unwanted access attempts and strange activity in network traffic. This system need to notify users or automatically restrict traffic patterns linked to well-known attack techniques.

2. A patch management system that is up to date must be installed on the server. Attackers frequently use unpatched operating systems and applications as a point of entry. As soon as important security updates are released, the server should be set up to install them automatically.

3. Make sure the encryption used for both data in transit and data at rest is sufficient. Make use of robust encryption techniques for network communication and the filesystem on the server. Configuring and routinely updating to the most recent secure versions of SSL/TLS is recommended.

4. Put in place stringent user access control procedures. System settings and sensitive data should only be accessible by authorized persons. Make use of robust authentication techniques, such as multi-factor authentication (MFA), and make sure that default passwords and usernames are quickly changed.

5. Configuring the firewall:

Firewall rules should be reviewed and updated to reduce needless exposure. By default, block all incoming and outgoing traffic, allowing just the ports and protocols that are necessary for the server to function. To ensure security, audit and update these policies on a regular basis.

6. Security Auditing and Record-Keeping:

Turn on thorough audits and server logging. This will give important information for post-incident investigation and assist in spotting suspicious activity. Examine and evaluate logs on a regular basis to look for indications of possible assaults.

7. Security of Applications:

Check the software and web apps on the server for vulnerabilities on a regular basis. To identify and address security flaws, make use of techniques such as web application firewalls (WAFs) and code review procedures.

8. Lists of access controls (ACLs):

To restrict access to certain files and directories, use Access Control Lists. Adhere to the least privilege principle, making sure that processes and users have access to only the information necessary for their designated tasks.

Stopping This Assault:

Harden your web server by following best practices for server security, which include updating your web server software, disabling unused modules, and configuring secure settings.

Put strong authentication into practice: Make sure your web applications employ robust authentication methods and that user credentials are safely stored, ideally using salting and contemporary hashing algorithms.Consider implementing a Web Application Firewall (WAF) to defend against frequent online application attacks. In addition to adding an extra degree of security, WAFs can filter out malicious traffic. Maintain an auditing and updating schedule for your web apps: Check your web apps for vulnerabilities on a regular basis, then implement any necessary patches and updates.

In summary, a thorough approach to server security combines constant upkeep, watchful observation, robust access controls, and continual security training. To safeguard your server and sensitive data, you should incorporate these suggestions into a comprehensive security plan. Documentation from institutions such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) contains specific guidelines and resources that can be utilized to effectively implement and enhance these recommendations.