TME7-Policies for School/Career website

Business Related Security Issues:

Security is a fact that should get a very high priority on any business. There is infinity number of security issues on an online server. Some of them are known and some are unknown. But, it?s a must for all web server administrators to ensure the server the maximum protection. Security threat or hacking attack can come across many filed like: Hardware, Network, Servers, Website exploit etc.

In any business securing the hardware and network takes the first place. If the server is physically accessible for number of people then it is a high security risk. Because it?s very easy to compromise a server or copy all the data from the server and database if someone has access to the physical device.

For network side there are also a lot of security concerns. If the server is built in a network which network is accessible for the users easily that?s actually very bad risk for a server. On the other hand the firewall is a very big issue. If the firewall is not configured or secured then it could open thousand ways for a hacker to compromise the server.

Security threats can also come from the server side. Just like the DOS/DDOS attack. Some web server versions has some vulnerability in default installation. So it?s a very easy gateway for the hackers to exploit the servers if the server isn?t secured properly. On the other hand the web server leaves a lot of security issue during the configuration process.

Another most common security risk is the website. If the website has not secured properly and if it is vulnerable then a malicious user can gain access to the server and can compromise the server as well.

After securing the server side and the website completely it?s still not the end of everything. The users can be affected by a hacker as a personal target. The database could be compromised with SQL attacks and that will fall all the users in danger.

These are the most common security issues that are the first target of a hacker or a malicious user. And during day by day hackers are improving themselves and they are discovering some new and unknown hacking methods and exploits and they will keep doing it.

Analyze Security Risks:

In this scenario there are already a live web server configured with some PHP application but it has not secured properly yet. Now this server should be analyzed for all possible security risks.

Hardware: This server has been bought from Amazon Web Service so it?s definitely stored in a highly secured data center. It was a wise decision to buy servers from trusted and well known source. But the security of the AWS account and the SSH authentication file takes place.

Network: The server has been created on AWS datacenter so it?s inside the secure network of AWS. But the firewall should be configured properly and should be secured.

Web Server:

i) The apache2 web server is currently installed as a backdated version 2.4.29 that has lot of well-known securi vulnerabilities.

ii) Directory indexing is enabled by default. Any one on the internet can see all the directories on the server.

iii) All the website files are currently uploaded on the currently used directory root. So it?s a high security rule. I anyone can compromise the server they can destroy or change the main files. Some symbolic links should be created

instead if keeping the original files on the directory root.

iv) The database_connection.php is accessible from the browser. So it will represent all the database credential t
user. A malicious user can easily guess this filename and see the file.

MySQL Server: MySQL server is having a week password and it?s allowing root login remotely. The database is allowing the php application to login as root so it is a very high security issue.

PHP App: The PHP application has been configured securely so there are no major security issue. But the application is using the database root password so it should be modified to use a different user than using the root user.

Now all the security policies has been implement on the server. The first step is securing the access to the hardware and the server.

To secure the aws.amazon.com account there is a very strong password that?s very hard to guess is configured Also 2 factor authentication has been enabled with the administrator cellphone number. The browsing cookies, history, cache has been deleted from the browser. From now no one can access that aws account but the system admin. The SSH Public key has been uploaded to the google drive on that email address that is associated with that aws account. It will be deleted immediately from the administrator system once the other things are done.

To secure the network the firewall has been configured. In this scenario the most popular linux firewall that named iptables that was installed on the system by default. It has been configured by using the following commands.

Now the firewall has been configured securely. It?s also allowing a few ports: 22/SSH, 80/HTTP, 443/HTTPs. ICMP traffics are also blocked. Below is the listening port list from the server.

Now the hardware and the network is all. It?s time to fix the security issues that are on the other parts.

The Apache2 web server has been updated to the latest version and now the current version of the Apache2 web server is 2.4.37. All the well-known vulnerabilities are removed from this version.

The commands that are used to upgrade the server are:

apt-get install software-properties-common

add-apt-repository ppa:ondrej/apache2

apt-get update

apt-get dist-upgrade

Then the directory indexing has been disabled from the apache2 configuration file. Now it will disallow the users to list the directories are on the servers document root.

Now all the files are moved from the servers root directory and has been placed to some directory that?s not accessible for the website visitors. And for all the files there is a symbolic link created to the current root directory of the server. It will increase the servers security in very high amount. From now if any hacker hacks the website and try to modify any file then it should not harm the main files. And the hacker will never know where the main files are.

After that the database file and all the .htaccess files has been hidden from the server by using IndexIgnore directive.

Because they are the most sensitive data on the server.

The MySQL database has also been updated. The root login from remote machine has been disabled from inside the database. And the port for MySQL 3306 is also closed from the firewall. That means no one on the internet can connect this MySQL server with any application instead of the application that?s installed on the same server.

The PHP Application has been reconfigured to use a different user to connect to the database than using the root password. SSL Certificate has been installed on the server so the communication between the users and the server is now private.

These security updates has updated the server and the website 2 steps. But the system administrator should always have to monitor the server and the server log also for any unauthorized access or hacking attempt and make the server up to date and have to implement more security policy in day by day. It was just the beginning. The hackers are always trying to find a new ways to compromise a server. So the IT team should be aware of that and should not take this things lightly. The security update has been configured on the server is gonna take a very positive effect for the users also. They could manage the student data more securely.

References:

- http://www.maxi-pedia.com/IndexIgnore
- https://websiteforstudents.com/install-apache2-disable-directory-listing-ubuntu/
- https://www.mysterydata.com/update-apache-2-4-to-latest-version-on-ubuntu-16-04-server-vestacp/