TEAM INSTRUCTIONS : ACCESSING & CONFIGURING SERVERS

As per Primary Objective 2 (Defensive Objective), you will need to setup your agency's Team Server and defend against all attackers. If an attacker manages to get into your server and disable or modify any services, you will lose defensive points for your team. Or if you yourself stop your services which are supposed to be open, that will also cause you to lose defensive points for your team. Thus, defending your agency's Team Server is critical for denying other parties the ability to cause you to lose your Team's defensive points.

IMPORTANT REMINDER : THE MOMENT YOU HAVE ACCESS TO YOUR SERVER, YOU SHOULD IMMEDIATELY CONFIGURE YOUR SERVER IP ADDRESS AS INSTRUCTED BELOW. DON'T DELAY - THIS SHOULD BE THE VERY FIRST THING YOU DO. THE GAMEMASTER WILL NOT BE ABLE TO HELP YOU IF YOUR SERVER IS NOT REACHABLE BY THE SERVER'S USERS WHO ARE DETERMINING IF YOUR SERVER IS UP. ALSO, WE RECOMMEND THAT YOU IMMEDIATELY CHANGE ALL YOUR SERVER'S OS AND APPLICATION ACCOUNT PASSWORDS *UNLESS SPECIFICALLY EXPRESSLY INSTRUCTED *NOT* TO DO SO IN THE INSTRUCTIONS BELOW* TO SOMETHING ONLY YOUR TEAM WOULD KNOW.

Accessing Your Team's Virtual Server

1. To access your Team's Virtual Server, use the following credentials and then follow the steps from step 2 thereafter :
   Note : These credentials are the same for everyone's Team Virtual Servers, so unless you want someone to compromise your server using the credentials below, you should first unplug the LAN cable from your Team Virtual Server laptop as soon as possible, then power on the Team Virtual Server to change all the passwords below on your own Team Virtual Server and firewalling/disabling/patching services BEFORE re-connecting the LAN cable back to the laptop and rebooting your Team Virtual Server using the "init 6" command.

   Team Server Console / SSH default account login credentials : userid : osboxes
   password : password

   Note : if using this osboxes account, you have to use the "sudo" command to execute root-level commands. "Ask The Oracle" (i.e. Google-search) on how to do that. If you want to execute everything as root without using sudo, then just execute the command "sudo /bin/bash " after logging in as the user osboxes.

   At the application layer, you have the following services and credentials :

   MySQL Service on TCP3306 : userid : root / **password : password**
   userid : app / **password : password**

   Web Application Service on TCP80 : userid : admin / **password : password**

   FTP Service on TCP21: userid : ftpuser / **password : password**

   Note : FTP access is already configured on this FTP service so you might want to see whether the FTP service is running using the least-required privilege. Again, "Ask The Oracle" on how to check for that.

2. First, ensure that the physical server laptop housing your Team's Virtual Server has a network adapter that is detected by your Windows OS and connected to the network and is active. Do a ping to 192.168.168.254 to confirm your network adapter is up and active. You should get an ICMP reply. If not, troubleshoot the problem yourself by Asking The Oracle (hint : standard troubleshooting approach is you ping yourself first, then ping any IP address belonging to a computer under your team, then ping to 192.168.168.254 . Where is stops is where the problem is. Just because you can't ping

out doesn't mean the network is at fault (we always hear "internet down" - the internet doesn't go down unless all the telcos in the world have had their equipment destroyed). Check your physical cable jacks are making good contact with your computer's RJ45 port, see if you disabled your adapter inside your OS, did you set a static IP and gateway to the wrong values, etc.

3. Inside the Windows host OS of the laptop housing your Team's Virtual Server, you should be able to see the Virtualbox icon. Double-click on it to start up Virtualbox and see your Team's Virtual Server image in the Virtualbox dashboard. Start up this image to power on the server and login accordingly using the abovementioned credentials. .

   Note : your server's files should be inside the directory called c:\Virtual Machines. Make sure you back them up using snapshots in Virtualbox, as well as create a backup of the directory into another part of your filesystem. Lastly, don't delete, move or modify any of the files inside this directory unless you know what you are doing !

Configuring Your Team's Virtual Server

In order not to lose defensive points when your server's users start trying to access your server, you need to set your server IP address to a specific IP address and have it online **before** they start trying to access.

Your Team Server has been assigned a specific IP address and gateway IP address (see under the "Team Server IP Address / Gateway" section of the "Profile" section of the G@meGe@r™ dashboard).
You must configure it using the following procedure :

1. Login to your Team's Virtual Server image (i.e. your "Team Server").

2. The Virtual Server image starts up in runlevel 3 and you should see a terminal shell after a successful login.

3. Inside the terminal shell, configure the virtual server by typing the following command sequence to allow you to set a static IP address for your Team :

```
nmcli connection edit 'Wired connection 1'
set ipv4.addresses X.X.X.X/24
set ipv4.gateway Y.Y.Y.Y
save persistent
quit
init 6
```

   The X.X.X.X value above is the unique IP address that has been assigned to you for your Team Server IP address (see under the "Team Server IP Address / Gateway" section of the "Profile" section of the G@meGe@r™ dashboard).
   The Y.Y.Y.Y value above is the unique IP address that has been assigned to you for your Team Server's GATEWAY IP address (see under the "Team Server IP Address / Gateway" section of the "Profile" section of the G@meGe@r™ dashboard).

4. Make sure you can ping the internet gateway router by typing the following inside the terminal shell :
   ping 192.168.168.254

IMPORTANT NOTE : You MUST use ONLY the specific IP address and gateway (see under the "Team Server IP Address / Gateway" section of the "Profile" section of the G@meGe@r™ dashboard) to assign to your agency's Team Server and must continually check to ensure this is maintained. If the system randomly decides to poll your server IP and cannot find it or cannot reach it for any reason, the system will then make a deduction from your defensive point balance!

Setting Up Services On Your Team's Virtual Server

In order not to lose defensive points, you will need to secure and bring the following services on your server IP address online and active with certain conditions **before 1000 hours** (which is when the agency users will start accessing your Team Server):

1. MySQL service listening on TCP port 3306 :
   - ensure this service is only & always accessible by the '**app**' user (using the password : '**password**'); and
   - ensure the user '**app**' can ALWAYS perform the **SELECT** operations on the **LOGIN** table defined inside the APPDB database; and
   - ensure that the content of the LOGIN table remains EXACTLY THE SAME AT ALL TIMES as per what is originally configured before the tournament.

2. SSH service listening on TCP port 22 :
   - ensure this service is always accessible by any authorized users (represented by the GameMaster); and
   - ensure the server's root user account is always allowed to login via the pre-configured key method.

3. HTTP service listening on TCP port 80 :
   - ensure this service is always accessible by any authorized users (represented by the GameMaster); and
   - ensure the existing pre-tournament web content remains EXACTLY THE SAME AT ALL TIMES after the start of the tournament (as the authorized user will be comparing some parts of the content obtained against a baseline to determine if any changes have been made to the web content).

You can choose to run the existing server packages already installed in your server image, or you can download and install your own, or do any patching, or do what you feel is required to secure the service.
However, the existing content and any applications that each respective service offers should continute to be made accessible to anyone visiting the server.
For example, if you change your default webserver to another webserver codebase, you need to migrate all the content offered by the default webserver to the new webserver.

If we don't see the existing content or be able to perform the existing actions, then defensive points will be deducted.

If the service is disabled (either by you or an attacker) or unreachable across the network, defensive points will also be deducted.

If you plan to use your own server versions to replace the default services, please note that the existing content of each service can be found within the default content directories of the default packages that belong to each of the aforementioned services which come bundled with your server image.
Thus you will have to identify the content and then migrate it to the new servers that you want to replace the existing ones with.

To illustrate the above as a hypothetical example only (i.e. may not be actually what is present in the server), let's suppose the server comes with the Apache 2.0 web server that enables the HTTP service and you want to replace it with Lighttpd web server instead. You would thus have to migrate all the existing contents and web-applications inside the web document directory (for example /var/www/html , etc) **as-is** into whatever is the default content directory that Lighttpd web server uses.

You must also **NOT** delete or modify the version of any **application** that the server is offering up, e.g. if you are using SmallHTTPServer offering up a Joomla web-application and you migrate from SmallHTTPServer to Apache, then your Joomla web-application and its contents must remain the same even though it is now offered up by Apache instead of SmallHTTPServer.
If you need to defend the server applications, you need to find some way to defend it without changing its version and content.

These limitations reflect how IT-security practitioners often encounter real-world business and/or legacy requirements (e.g. similar to what is commonly found in banks, financial institutions, governments, etc) that hinder some avenues you may have to securing a platform, thus requiring you to become more creative on defense.

Whichever approach you decide to take, bear in mind that any existing or new server package may or may not have vulnerabilities so you will have to decide whether you want to patch whichever server codebase that you decide to use or run the risk of another team compromising your server.

IMPORTANT NOTE 1 : You MUST ensure that the services as listed above are setup correctly in the manner described above (how you comply is your problem :)). If the agency users randomly decide to poll your server ports and cannot find them or cannot reach them for any reason, the system will then make a deduction from your defensive point balance!

IMPORTANT NOTE 2 : if you want to edit anything on your server, you can use a command-line text editor such as Vi which is already installed on the server.

Other Important Things You Need To Do On Your Agency's Team Server

1. Copy your "Team Secret" value under the "Profile" section of your Team's G@meGe@r™ dashboard into a new plain-text file called **team-secret.txt** .
   Then move this new **team-secret.txt** file into the **/etc** directory of your Team Server (i.e. location is now **/etc/team-secret.txt** ; Replace any existing team-secret.txt file if there is one already inside with the one you created).
   If you don't know how to do this, then Ask The Oracle.

2. Run the following commands inside a terminal shell on your Team Server if you are logged in as root :
   ```
   chmod 600 /etc/team-secret.txt
   chown root:root /etc/team-secret.txt
   ```

   If you are logged in as a non-root account (e.g. osboxes), then type the following :
   ```
   sudo chmod 600 /etc/team-secret.txt
   sudo chown root:root /etc/team-secret.txt
   ```

3. Do not delete or modify any existing OS-level user accounts except if you want to change their default login passwords.

4. Do not delete or modify anything inside the /root directory and its sub-directories.

5. Before you start configuring your Team's Virtual Server, it is a good idea to make a backup of the virtual image directory to a new separate directory so that you can restore if disaster happens. Then after you finish configuring, do the same thing to a new separate directory so that you have an audit trail and can restore to different points even if your snapshots get wiped out.

6. Ensure that all the required application-level files and directories are not modified or deleted.