Born2beRoot Defense Checklist

By Adrian Musso-Gonzalez (@amusso-g)

Note: If something does not work as expected or is not clearly explained, stop evaluation.
When you need help with checking something, the student should be able to help you.

Preliminary tests

☐ Git repo cloned successfully.

General instructions

☐ Git repo contains a signature.txt file.
☐ Check the signature against the students ".vdi" file, make sure it's identical.
☐ Clone VM || create a snapshot && open VM.

Mandatory Part (Questions for the student)

☐ *How does a virtual machine work and what is its purpose?*
☐ *The basic differences between CentOS and Debian?*
☐ *Their choice of operating system?*
☐ *If CentOS: what SELinux and DNF are.*
☐ *If Debian: the difference between aptitude, apt and what APPArmor is.*
☐ During the defense, a script must display all information every 10 minutes. Its operation will be checked in detail later.
☐ All explanations are satisfactory (else evaluation stops here).

Simple setup

☐ Ensure that the machine does not have a graphical environment at launch.
☐ Connect to VM as a created user (which isn't a root)
☐ Ensure the password follows the required policy (2 days min, 7, 30 days max).
sudo chage -l username
☐ Evaluator checks UFW service is started.
sudo ufw status *//look for status: active*
☐ Evaluator checks SSH service is started.
sudo systemctl status ssh

☐ Evaluator checks the chosen operating system (Debian or CentOS).
lsb_release -a || cat /etc/os-release

User

☐ The subject requests that a user with the login of the student being evaluated is present on the virtual machine. Check that it has been added and that it belongs to “sudo” and “user42” groups.

getent group sudo
getent group user42

Password policy check:

☐ Create new user (e.g. user42).

sudo adduser new_username

☐ Assign a password of your choice, respecting subject rules.

getent group sudo

☐ Explanation from student explaining how to implement the password policy.

☐ Normally there should be one or two modified files. If there is any problem, the evaluation stops here.

☐ With the new user, ask the student to create a group named “evaluating” and assign it to the new user.

sudo groupadd evaluating
sudo usermod -aG evaluating your_new_username

☐ Check if the new user belongs to the “evaluating” group.

getent group evaluating

☐ Ask the student to explain advantages of the password policy (beyond the fact that it is required for the project)

☐ Ask the student the advantages/disadvantages of the policy implementation.

Hostname and partitions

☐ Check the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).

hostnamectl

☐ Modify this hostname by replacing the login with yours, then restart VM.

sudo hostnamectl set-hostname new_hostname
sudo reboot

Note: If on restart, the hostname has not been updated, the evaluation stops here.

☐ Restore the machine to the original hostname, then restart VM.

sudo hostnamectl set-hostname new_hostname
sudo reboot

☐ Ask the student being evaluated how to view the partitions for the VM.

lsblk

☐ Compare the output with the example given in the subject (if there are bonuses, refer to the bonus example).

☐ Ask the student for a brief explanation of LVM and how it works.

SUDO

☐ Check that the “sudo” program is properly installed on the virtual machine.

dpkg -l | grep sudo

☐ The student being evaluated shows assigning a new user to the “sudo” group.

☐ The subject imposes strict rules for sudo. The student being evaluated must explain the value and operation of sudo using examples of their choice.

sudo visudo ls

☐ Second step, must show the implementation of the rules imposed by the subject.

☐ Verify the “/var/log/sudo/” folder exists and has at least one file. Check the contents of the files in the folder, you should see a history of the commands used with sudo.

☐ Run a command via sudo. See if the file(s) in the “/var/log/sudo/” folder have been updated.

UFW

☐ Check the “UFW” program is properly installed on the VM and works properly.

sudo ufw status numbered

☐ Ask the student for a basic explanation of UFW and the value of using it.

☐ List the active rules in UFW. A rule must exist for port 4242.

☐ Add a new rule to open port 8080. Check that this one has been added by listing the active rules.

sudo ufw allow 8080

☐ Delete this new rule with the help of the student being evaluated.

sudo ufw delete 4

sudo ufw delete 2

SSH

☐ Check that the SSH service is properly installed on the VM, and is working properly.

sudo service ssh status *//check if its active and port 4242*

☐ Ask the student for an explanation of what SSH is and the value of using it. *(answer: secure shell, allows 2 computers to securely talk to each other)*

☐ Verify that the SSH service only uses port 4242.

☐ Ask the student to help you use SSH in order to log in with the newly created user. To do this, you can use a key or simple password, depending on the student being evaluated.

ssh new_user@127.0.0.1 -p 4242

☐ Make sure you cannot use SSH with the “root” user as stated in the subject.

ssh amusso-g42@127.0.0.1 -p 4242 *//should come up as permission denied*

Script Monitoring (questions for the student)

- [ ] Ask the student how their script works and see their code for it.

Script inputted in the monitoring .sh file to display system information

cd /usr/local/bin && vim monitoring.sh

- [ ] *What is “cron”?*
- [ ] *How does the script run every 10 minutes from when the server starts?*
- [ ] Once correct functioning of the script is verified, ask the student to make sure the script runs with dynamic values correctly.

sudo crontab -u root -e (change 10 value to 1***)***

- [ ] The student being evaluated should make the script stop running when the server has started up, without modifying the script itself. To check this, restart the VM.

sudo cronstop
sudo cronstart

- [ ] At startup, check if the script still exists in the same place, the rights have remained unchanged and that it has not been modified.

sudo reboot
sudo crontab -u root -e