Lynis Auditing Tool

Module 12 | Activity 1

Introduction

One of the main topics in Module 12 is auditing. Auditing is a great tool for checking what security mechanisms are in place within a computer system. As we learned, auditing is often done by third parties. Although, there are many Linux tools out there to run your own audit. In Module 12 Activity 1, we will be looking at the auditing tool Lynis. Learning how to run a quick audit is a great tool that can be used when setting up/fixing your CDC machines. It will point out what security softwares are missing, so you can patch them up. Another big part of the audit process not mentioned in the Slideshow is what should be done before an audit. These steps ensure that the audit runs smoothly. There are many checklists out there to prepare for an audit, but we are going to show you a simple one in today's activity.

Getting Started

Similar to previous activities, we could just provide you with the steps of how to install and run Lynis. Although, one of the main objectives of the Cyber Defense venue is to learn how to be self sufficient. Cyber security is ever changing, so it is your responsibility to be able to research new softwares on your own. This research process involves evaluating what softwares would be the most beneficial to your systems needs, how the softwares works, and how to install/use said softwares. When doing this research, Google and Youtube are your best friends. Since the venue is coming close to an end, this activity is going to test these skills that should have been built on throughout the semester.

Step One:

Let's do some research on what to do before an audit takes place. We are going to guide you on over to this helpful website we found on Google. Although, you can easily find more resources if you search online.

Click on the Link provided.

Take a minute to read and understand the checklist. Consider what security measures you have in place and try to predict what your audit will catch.

Step Two:

It is time to find a tool to run your audit. Today we will be guiding you to learn about the auditing tool Lynis. Of course, you should take some time to learn and compare other auditing tools that are out there. Hop on over to your search engine and type in lynis. Your search should have https://cisofy/lynis pop up as a result. Click on it.

Step Three:

Time to do some reading! To make sure you are grasping the important information, make sure you can answer the following questions.

1. What is Lynis?
2. What operating systems does it run on?
3. What are the uses of Lynis?
4. How does Lynis work?
5. What are the benefits of using Lynis?
6. How is the installation process?
7. How does it compare to other auditing tools?

It is always advisable to create a quick pros and cons list for softwares you are interested in.

Step Four:

Say we have decided to go with the auditing tool Lynis, and now it is time to install. Most of the time, the website for the software you are wanting to install will have installation instructions. Go ahead and follow the instructions to install. It may also be beneficial to look for some demonstration videos on the Internet to make for a quicker installation.

Conveniently, there is a demo video on the CISOFY website. However, let's practice finding some demo videos. Go on to your search engine and look up lynis videos. You will have a variety of video demos pop up. Now it is time to weed through them. The first thing I check for is the date it was published. There are always new moods of softwares coming out so you want to make sure you are watching demos of the current softwares.

Here are a couple videos we have picked out for you…

https://youtu.be/fUIpJJn6YaM

https://www.youtube.com/watch?v=V8LbfzP6lKA

Once you have read and watched demonstrations. It is time for you to install the software. Of course, it is always a good idea to screenshot your machine before making an installation. Go ahead and install Lynis with the information you have gathered.

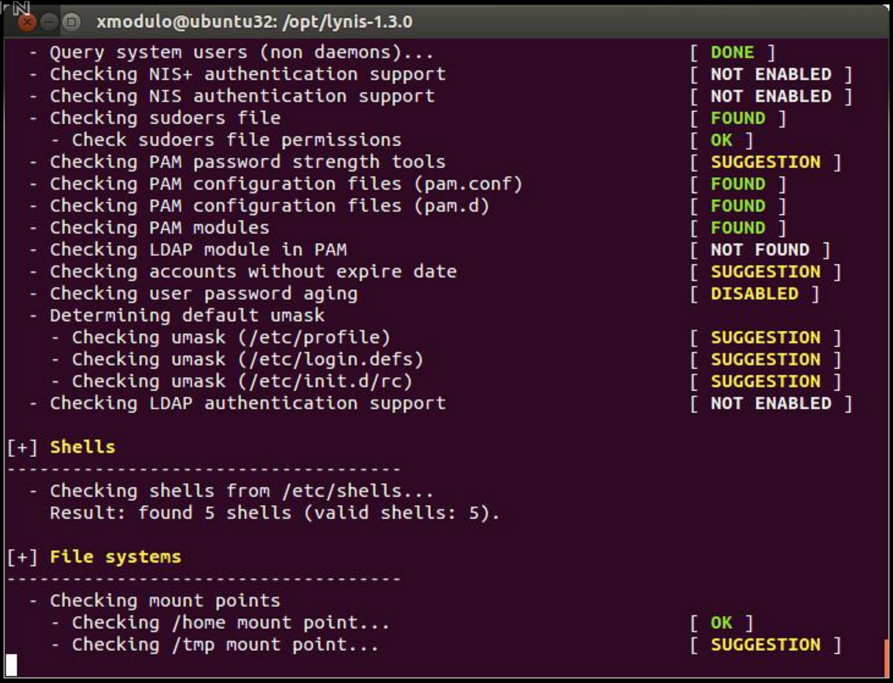
Step Five:

After you have properly installed Lynis, you can now use it. If there are any problems with the installation, you can Google those errors as well. There is a community of cybersecurity enthusiasts out there on the web, so there may be posts about similar errors. As we learn in the venue, make sure to search the web safely.

You may have seen how to run a Lynis audit in the instructions you have read or the demos you have watched. If you happened to miss this step, we decided to make this part easier for you. Go ahead and run the following command.

```
./lynis audit system
```

You should see something that looks like this. It may take a minute.



```
  - Query system users (non daemons)...                       [ DONE ]
  - Checking NIS+ authentication support                      [ NOT ENABLED ]
  - Checking NIS authentication support                       [ NOT ENABLED ]
  - Checking sudoers file                                     [ FOUND ]
    - Check sudoers file permissions                          [ OK ]
  - Checking PAM password strength tools                      [ SUGGESTION ]
  - Checking PAM configuration files (pam.conf)               [ FOUND ]
  - Checking PAM configuration files (pam.d)                  [ FOUND ]
  - Checking PAM modules                                      [ FOUND ]
  - Checking LDAP module in PAM                               [ NOT FOUND ]
  - Checking accounts without expire date                     [ SUGGESTION ]
  - Checking user password aging                              [ DISABLED ]
  - Determining default umask
    - Checking umask (/etc/profile)                           [ SUGGESTION ]
    - Checking umask (/etc/login.defs)                        [ SUGGESTION ]
    - Checking umask (/etc/init.d/rc)                         [ SUGGESTION ]
  - Checking LDAP authentication support                      [ NOT ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells...
    Result: found 5 shells (valid shells: 5).

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point...                           [ OK ]
    - Checking /tmp mount point...                            [ SUGGESTION ]
```

Notice that for each item, you will see the statements; FOUND, SUGGESTION, NOT ENABLED, OK, DONE, NONE, etc. These are telling you specifically what is being used for security measures. Look through the complete audit to see if the important security measures are indeed in place and working properly. Again you can use google to look up the specific items.

Step Six:

Once you have examined your audit, use the information you found to patch up any issues found. Update or reinstall softwares that are not being used properly or are suggested.

If anything goes wrong during this whole process, remember you can always reset your VM back to its latest snapshot.

IT-ADVENTURES
MAKING IT FUN