

ProLUG Security Engineering

Unit 5 Worksheet

Instructions

Fill out this sheet as you progress through the lab and discussions. Hold your worksheets until the end to turn them in as a final submission packet.

Discussion Questions:

Unit 5 Discussion Post 1: Review the rocky documentation on Software management in Linux. https://docs.rockylinux.org/books/admin_guide/13-softwares/

1. What do you already understand about the process?
2. What new things did you learn or pick up?
3. What are the DNF plugins?
 - a. What is the use of the versionlock plugin?
4. What is an EPEL?
 - a. Why do you need to consider this when using one?

Unit 5 Discussion Post 2: Do a google search for “patching enterprise Linux” and try to wade through all of the noise.

1. What blogs (or AI) do you find that enumerates a list of steps or checklists to consider?
2. After looking at that, how does patching a fleet of systems in the enterprise differ from pushing “update now” on your local desktop?
 - a. What seems to be the major considerations?
 - b. What seems to be the major roadblocks?

Definitions/Terminology

- Patching
- Repos
 - o Software
 - o EPEL
 - o BaseOS v. Appstream (in RHEL/Rocky)

- Other types you can find?
- httpd
- patching
- GPG Key
- DNF/YUM

Notes During Lecture/Class:

Links:

- <https://wiki.rockylinux.org/rocky/repo/>
- <https://www.sans.org/information-security-policy/>
- <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>
- <https://public.cyber.mil/stigs/downloads/>

Terms:

Useful tools:

- STIG Viewer 2.18
- SCC Tool (version varies by type of scan)
- OpenScap

Lab and Assignment

Unit5_Repos_and_Patching - To be completed outside of lecture time.

Digging Deeper

1. After completing the lab and worksheet, draw out how you would deploy a software repository into your system.
 - a. How are you going to update it?
 - b. What tools do you find that are useful in this space?

Reflection Questions

1. Why is it that repos are controlled by root/admin functions and not any user, developer, or manager?
2. What questions do you still have about this week?
3. How are you going to use what you've learned in your current role?