ProLUG Security Engineering

Unit 3 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 3 Discussion Post 1: There are 16 Stigs that involve PAM for RHEL 9. Read the guide from Rocky Linux here: https://docs.rockylinux.org/guides/security/pam/

1. What are the mechanisms and how do they affect PAM functionality?
    a. Review /etc/pam.d/sshd on a Linux system, what is happening in that file relative to these functionalities?
2. What are the common PAM modules?
    a. Review /etc/pam.d/sshd on a Linux system, what is happening in that file relative to these functionalities?
3. Look for a blog post or article about PAM that discusses real world application. Post it here and give us a quick synopsis. (Bonus arbitrary points if you find one of our ProLUG members blogs on the subject.)

Unit 3 Discussion Post 2: Read about active directory (or LDAP) configurations of Linux via sssd here: https://docs.rockylinux.org/guides/security/authentication/active_directory_authentication/

1. Why do we not want to just use local authentication in Linux? Or really any system?
2. There are 4 SSSD STIGS.
    a. What are they?
    b. What do they seek to do with the system?

Definitions/Terminology

PAM

AD

LDAP

sssd

oddjob

krb5

realm/realmd

wheel (system group in RHEL)

Notes During Lecture/Class:

Links:

- https://www.sans.org/information-security-policy/
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
- https://docs.rockylinux.org/guides/security/pam/
- https://docs.rockylinux.org/guides/security/authentication/active_directory_authentication/
- https://docs.rockylinux.org/books/admin_guide/06-users/

Terms:

Useful tools:

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

Lab and Assignment

Unit3_Identity_and_Access_Management - To be completed outside of lecture time.

Digging Deeper

1. How does /etc/security/access.conf come into play with pam_access? Read up on it here: https://man7.org/linux/man-pages/man8/pam_access.8.html
    a. Can you find any other good resources?
    b. What is the structure of the access.conf file directives?
2. What other important user access or user management information do you learn by reading this? https://docs.rockylinux.org/books/admin_guide/06-users/
    a. What is the contents of the /etc/login.defs file? Why do you care?

Reflection Questions

1. What questions do you still have about this week?

2. How are you going to use what you've learned in your current role?