HPC Security: Best Practices and Common Sense for Security with HPC

Tuesday, August 8, 2023

SDSC SAN DIEGO SUPERCOMPUTER CENTER

UC San Diego

Agenda

- Re-enforce the importance for Data security
  - What do we need to protect
  - When do we need to protect ourselves
  - Who do we need to protect ourselves from
- Provide quick and easy tips/reminders to keep your resources safe
  - Secure your data, credentials, physical devices

Session Objective

- Revisit your security practices
- Data Breach
  - Any incident in which confidential or sensitive information has been accessed without permission, including unauthorized access to a computer system or network. The offending party then steals the private, sensitive, or confidential personal and financial data of the customers or users.

- Data Security
  - The safeguarding digital information throughout its life cycle to protect it from loss, corruption, theft, or unauthorized access”. Including hardware, software, storage devices, and user devices.

Why do we need data security?

- Protect our data and resources from unauthorized access
  - To Avoid
    - Data corruption
    - Loss of data
    - Organizational loss of access to resources, data
  - To maintain
    - Direct Access to resources, data
    - Indirect access to resources/data
      - A compromised personal computer can compromise external resources
      - An attacker on your computer can do anything you can

Who do we need to protect from

- Nefarious Character (deliberate, intentional)
- Friendly Character (inadvertent, unintentional)
  - Deleting personal files
    - > rm –rf *
    - > rm –rf / directory/file (notice the space after the '/')
- System issues

When do we need to protect ourselves

- Always
  - Even if you don't….
    - have anything interesting
    - have sensitive data, your research is public
  - But……..
    - Attackers are opportunistic
    - Attackers are not aware of what you have
    - Attackers are interested in information you are not aware they are interested in
    - "Attack" may not be deliberate

What do we need to protect!

- Client, Resource
  - Personal Devices, credentials
  - Remote Devices
- Data
  - Files, directories (Data corruption/modification/deletion)
- Code/Project
  - Project dependencies
  - Project repository
- Research
  - Someone else publishes your work
  - Research integrity

Security is a Shared Responsibility

- Resource provider is responsible to:
  - Provide Access to Computational Resources
  - Protect your accounts/data from unauthorized users
  - Enforce the permissions you set for your data
- End user will: (review ACCESS AUP)
  - Protect their account credentials
  - Protect your data with permission controls
  - Use resources only for purpose you have been authorized to use

Best Practices

- Secure your accounts/allocations
  - Protecting your credentials
- Secure your data
  - File management
  - Have a contingency plan(Data recovery plan)
  - Clean up
- Secure your research
  - Client Security
  - Reduce dependencies
    - For the parts of your project that you can not control (3rd party libraries, modules, external users)

Best Practices: Secure your Research

- Client Security
  - Protect your resources
  - Install and run anti-malware software
  - Keep personal machine and software updated

Best Practices: Secure your credentials

- Passwords
  - Longer is better
  - Don’t reuse passwords
  - Don’t keep digital plaintext copies of passwords
  - Use password-manager program
  - Don’t share passwords
- Use SSH keys, ssh agent

Best Practices: Secure your Data

- Manage Access
  - Controls: Permissions granularity levels
    - (Attribute), User, Group, Other
    - Read(4), Write(2), Execute(1)
    - Default 755 (User(read, write, execute):Group(read, execute): Other(read, execute)
    - Use chmod, chown commands to modify ownership and permissions
- Data Resiliency
  - Clean up unnecessary files
  - Back up Data
  - Use integrity checking
    - Data transfers, bad hardware
- Have a contingency plan(Data recovery plan)
  - Off site backup

Best Practices: Secure your Research

- Project Security
- Reduce dependencies with in projects
  - Many larger software project depend on third party libraries and modules
  - Therefore the project is relying on the best practices of others to maintain the security and integrity of the project
- Protect web based application on our machines (Jupyter Notebooks, Globus connect personal)

Review and helpful links

- Security Awareness
- Best Practices
- ACCESS AUP
  - https://identity.access-ci.org/aup.html
- SSH Key setup
  - https://github.com/sdsc/sdsc-summer-institute-2022/blob/main/2.5_data_management/SSH.md#easy-access-setting-up-ssh-keys-key
  - https://github.com/sdsc-hpc-training-org/hpc-security
- Comet Webinar- Indispensable Security: Tips to Use SDSC's HPC Resources Securely
  - *https://www.sdsc.edu/event_items/202007_CometWebinar.html*
- Expanse Webinar: Enduring Security: The Journey Continues
  - *https://education.sdsc.edu/training/interactive/202204_expanse_enduring_security/index.html*
- Training Catalog
  - *https://www.sdsc.edu/education_and_training/training_hpc.html#catalog*

Thank You!