Systems and Security Evaluation

Rubric and Resources

General Notes

Our goals, as judges and staff, are:

- To encourage learning about HPC systems and security
- Keep the competition friendly, fair, and relatively stress-free
- For no one to get hacked, that would make the SCC and SCinet sad

There are a great many national and international cybersecurity standards. Years of practice have revealed that best practices are best practices. As a result, we've tried to digest things back to what various standards and best practices documents have in common.

In interviews and any written documents, we want to see that you have and use plans, tools, best practices, and documentation to make it through the contest and deal with contingencies. It's a short competition and it's okay to be brief, but there should be enough present that your team could use what you have (alongside the references and materials you collect and cite) to cover for a missing team member or bring someone who joined late up to date.

On that note, we will accept anything that you can map back to a national, international, or community standard; vendor best practices document; project documentation; or justify through fundamental computer science or data. No two sites, clusters, projects, or standards are alike - the SCC isn't any different.

Judges and contest officials will not engage in any malicious activity. Everyone else should be treated with friendly levels of suspicion. SC is a lovely place for making friends, engaging in social engineering, and attracting the attention of advanced persistent threat (APT) groups.

Judges may ask teams to view and/or upload logs, command output, and documentation at different points during the competition - it's part of setting up for the final interview. We are not using that information for any other purpose. Do feel free to tell us to come back later if it's a bad time. No scoring or submission is final until after the formal interview.

NOTE: If we ask to see something **before the contest starts** we won't hold it against you if there's a finding. We will provide a trustworthy, validated, and correct reference to remediate.

Once the contest starts, we will still inform you of the finding with supporting materials, post a clarification, and give you a chance to remediate, but it will impact scoring.

WARNING: Unauthorized penetration testing of anything anywhere that we or SCinet can detect, “black hat” activities, and anything that would be ethically, morally, or legally questionable that would cause disrepute and/or the SCC staff a serious headache or heartache is strictly forbidden and will have serious consequences.

If you have questions about something you’re considering doing as part of evaluating your security, that of the SCC infrastructure, or another friendly team by their invitation that could be misunderstood, please contact us first and we will issue written permission (or a denial) in the form of a clarification with any notes or restrictions.

Deliverables as text files (unless noted):

1. Your documentation
2. A copy of your /var/log as a tar.gz
3. Listing of your shared discoveries sorted by team
4. Any information that supports your interview answers

Rubric for judging:

1. Documentation (20 points)
    a. Does it exist?
        i. 0 pts for having no written documentation
        ii. 1 pt for lots of random notes
        iii. 3 pts for yes and it's organized but incomplete
        iv. 5 pts for yes and it's complete and covers all cluster management procedures
        v. 7 pts for yes and it's complete and covers all cluster management procedures with explicit security plan and incident management
    b. Do you have links or copies of vendor or software documentation?
        i. 1 pt for minimal
        ii. 2 pts for the majority
        iii. 4 pts for everything
    c. How is it managed?
        i. +1 pt for random members being able to find it
        ii. +1 pts for there being a single point to find it
        iii. +1 pt for being in a repo
        iv. +1 pt for being up to date

    d. Does it identify points of contact?
        i. +1 pts for a listing of team members with responsibilities
        ii. +1 pts for having a secure means of contacting them
        iii. +2 pts for cross-training to avoid single points of failure
        iv. +1 pts for emergency contacts
2. Strong account management, authentication and authorization, and encryption (20 points)
    a. +2 points if a random team member can explain the concepts of separation of roles and least privilege
    b. +4 pts everyone has their own account / no account sharing
    c. +3 pts for use of least privilege (e.g. using service accounts, sudo, or doas) rather than running an interactive shell as an administrative user
    d. +2 pts for minimum password complexity enforcement
    e. +2 pts all default accounts have had their passwords changed, are locked, or otherwise disabled
    f. +2 pts for limiting user remote access
    g. +2 pts for locking root, admin, and daemon accounts
    h. +2 pts all services are using encryption
    i. +1 pt the OS has had “weak” default encryption options turned off
3. Configuration management (10 points)
    a. +1 pts for knowing what it is
    b. +3 pts for having something we’d qualify as configuration management
    c. +4 pts for being able to produce a configuration inventory showing the state of the cluster (and any deviations from planned configuration) on demand
    d. +2 pts for having different roles based on node function
4. Patching (10 points)
    a. +1 pt for knowing how to patch the OS
    b. +3 pts for having done any patching
    c. +4 pts for having no currently insecure packages per the 3.c. inventory or documentation for mitigations
    d. +2 pts for being up to date or documenting why you're not up to date
5. Software Management (10 points)
    a. +1 pt for having a plan
    b. +3 pts for keeping installed software and services to a minimum
    c. +3 pts for using trustworthy sources for software
    d. +3 pts for having a bill of materials for installed packages or being able to build out one with one's package manager(s)
6. Network sanitation (10 points)
    a. +5 pts for minimizing attack surface
    b. +3 pts for limiting remote access to the cluster
    c. +2 pts for excellence in configuration (e.g. VLANs and PKEYs - keeping network functions separate, using configuration management, locking down management interfaces)

7. Logging and monitoring (10 points)
    a. +3 pts for logging all activity
    b. +3 pts for doing any systems monitoring beyond power
    c. +1 pt for centralized logging
    d. +1 pt for catching attempts to attack
    e. +2 pt for actually doing something with the logging and monitoring data
8. Communication with peers (5 points)
    a. +0.25 pt for each team to which you've worked out a way to communicate systems and security tips, tricks, and concerns and actually done so (each team will have to affirm a mutual exchange of information)
    b. +0.25 pt for having acted on what each team has shared with you (both teams will have to affirm you've done so)
    c. +1 pt bonus for any security issues you detect and report with the SCC contest infrastructure before we find and mitigate them.
9. Surprise and Delight! (5 points)
    a. The judges reserve 5 points to reward teams who have gone above and beyond in the administration of their system, showing goodwill and sportsmanship, and/or did you do an excellent job in resisting attempted compromises?

NOTE: We will assess a -2 to -10 pts to penalty for any activity that destabilizes the network, indicates an unplanned compromise of your system, or could be seen as an egregious misconfiguration. You will be informed of any penalty-inspiring condition and given a chance to mitigate the situation and recover points.

HPC Cluster Systems and Security General References

General References and Tools

Linux Hardening and Security Guides

- Red Hat Enterprise Linux 8: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/security_hardening/index
- Debian: https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html

- SUSE Linux Enterprise Server: https://documentation.suse.com/sles/15-SP6/html/SLES-all/book-security.html
- Ubuntu: https://ubuntu.com/security

Configuration Management Tools

- Ansible: https://ansible.readthedocs.io/
- Salt: https://saltproject.io/
- Puppet: https://help.puppet.com/osp/
- CFEngine: https://docs.cfengine.com/docs/3.24/
- Git for Configuration Management: https://superuser.com/questions/1037211/is-it-a-good-idea-to-use-git-for-configuration-file-version-controlling

Monitoring and Logging Tools and References

- Brendan Gregg's Homepage: https://www.brendangregg.com/
- DevConnected Linux Logging Guide: https://devconnected.com/linux-logging-complete-guide/
- Prometheus: https://prometheus.io/
- Performance Co-Pilot: https://pcp.io/
- OVIS: https://github.com/ovis-hpc/ovis-wiki/wiki
- Check-MK: https://checkmk.com/product/checkmk-raw
- Zabbix: https://www.zabbix.com/documentation/current/en/

HPC Cybersecurity Communities and Events

- S-HPC 2024 Workshop: https://sc24.conference-program.com/presentation/?id=wksp154&sess=sess320
- Ian Lee's Publications (LLNL): https://ianlee1521.com/resume/#publications
- Regulated Research Community of Practice: https://www.regulatedresearch.org/

Listing of Cybersecurity Organizations and Standards

International Organizations and Standards

Center for Internet Security (CIS)

- Main website: https://www.cisecurity.org/

ISO 27001

- Appendix A (reflects most national standards)
- ISO 27001 Annex A overview: https://www.isms.online/iso-27001/annex-a/

(Multi)National Standards and Agencies

European Union (EU)

European Union Agency for Cybersecurity (ENISA)

- Main website: https://www.enisa.europa.eu/

NIS Directive

- Minimum Security Measures for Operators of Essentials Services: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services

Finland

National Cyber Security Centre Finland (NCSC-FI)

- Main website: https://www.kyberturvallisuuskeskus.fi/

Germany

Federal Office for Information Security (BSI)

- Main website: https://www.bsi.bund.de/EN/Home/home_node.html

People's Republic of China

National Information Security Standardization Technical Committee (TC260)

- Main website: https://www.tc260.org.cn/

Key Standards

- GB/T 22239-2019: Information Security Technology – Baseline for Classified Protection of Cybersecurity https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF

- GB/T 25070-2019: Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity https://std.samr.gov.cn/gb/search/gbDetailed?id=88F4E6DA63444198E05397BE0A0ADE2D

Republic of China (Taiwan)

Administration for Cyber Security

- Main website: https://moda.gov.tw/en/ACS/

Switzerland

National Cyber Security Centre (NCSC)

- Main website: https://www.ncsc.admin.ch/ncsc/en/home.html

United States

National Institute of Standards and Technology (NIST)

- Computer Security Resource Center: https://csrc.nist.gov/
- Cybersecurity Framework: https://www.nist.gov/cyberframework

Key NIST Special Publications

- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/pubs/sp/800/171/r3/final
- NIST SP 800-223: High-Performance Computing Security: Architecture, Threat Analysis, and Security Posture https://csrc.nist.gov/pubs/sp/800/223/final

Rubric Crosswalk to Specific Sources

1. Documentation (20 points)

1.1 / 1.2 Full System and Operational Documentation

- ISO 27001:2013 A.12.1.1 Documented operating procedures
- NIST SP 800-171 Rev. 2 3.12.1: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-223 (Draft) Section 4.1: https://csrc.nist.gov/publications/detail/sp/800-223/draft

1.3 Documentation Management

- ISO 27001:2013 A.12.1.2 Change management
- SANS Information Security Policy Templates: https://www.sans.org/information-security-policy/

1.4 Points of Contact

- ISO 27001:2013 A.6.1.1 Information security roles and responsibilities
- NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

2. Strong Account Management, Authentication, Authorization, and Encryption (20 points)

- ISO 27001:2013 A.9 Access control
- NIST SP 800-171 Rev. 2 3.1 Access Control: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- EU NIS 2 Directive Article 21: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- Singapore MAS Technology Risk Management Guidelines Section 5: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
- CIS Benchmarks for Linux distributions: https://www.cisecurity.org/cis-benchmarks/
- ANSSI (France) Linux Configuration Guide: https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/
- BSI (Germany) IT-Grundschutz-Kompendium AP.4: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

3. Configuration Management (10 points)

- ISO 27001:2013 A.12.1.2 Change management
- NIST SP 800-223 (Draft) Section 4.2: https://csrc.nist.gov/publications/detail/sp/800-223/draft
- NIST SP 800-128: https://csrc.nist.gov/publications/detail/sp/800-128/final
- UK NCSC Configuration Management guidance: https://www.ncsc.gov.uk/collection/configuration-management

4. Patching (10 points)

- ISO 27001:2013 A.12.6.1 Management of technical vulnerabilities
- NIST SP 800-40 Rev. 4: https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final
- BSI (Germany) OPS.1.1.3 Patch and Change Management: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.pdf

5. Software Management (10 points)

- ISO 27001:2013 A.12.5 Control of operational software
- NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: https://csrc.nist.gov/publications/detail/sp/800-218/final
- OWASP Software Component Verification Standard: https://owasp.org/www-project-software-component-verification-standard/
- Spack Documentation - Best Practices: https://spack.readthedocs.io/en/latest/packaging_guide.html#best-practices
- EasyBuild Documentation - Contributing: https://docs.easybuild.io/en/latest/Contributing.html

6. Network Sanitation (10 points)

- ISO 27001:2013 A.13 Communications security
- NIST SP 800-223 (Draft) Section 4.3: https://csrc.nist.gov/publications/detail/sp/800-223/draft
- SANS Institute Network Security Resources: https://www.sans.org/security-resources/ipv6/
- NSA Network Infrastructure Security Guide: https://media.defense.gov/2022/Aug/09/2003052979/-1/-1/0/CTR_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220809.PDF
- ANSSI (France) Network Security Guide: https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-recommandations_pour_un_usage_securise_dopenvswitch-v1.0.pdf

7. Logging and Monitoring (10 points)

- ISO 27001:2013 A.12.4 Logging and monitoring
- NIST SP 800-92 Guide to Computer Security Log Management: https://csrc.nist.gov/publications/detail/sp/800-92/final
- EU NIS 2 Directive Article 23: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

- CERN Computer Security - Logging and Monitoring Best Practices: https://security.web.cern.ch/recommendations/en/logmonitoring.shtml
- EGI Security Monitoring: https://documents.egi.eu/public/ShowDocument?docid=3145
- Gregg, B. (2020). Systems Performance: Enterprise and the Cloud (2nd ed.). Addison-Wesley Professional.

8. Communication with Peers (5 points)

- ISO 27001:2013 A.6.1.4 Contact with special interest groups
- NIST SP 800-150 Guide to Cyber Threat Information Sharing: https://csrc.nist.gov/publications/detail/sp/800-150/final
- FIRST (Forum of Incident Response and Security Teams) Best Practice Guide: https://www.first.org/resources/guides/
- UK NCSC Information sharing guidance: https://www.ncsc.gov.uk/guidance/information-sharing
- Open Source Security Foundation (OpenSSF) Best Practices Badge Program: https://bestpractices.coreinfrastructure.org/en

9. Surprise and Delight (5 points)

- SCC Systems and Security Judging Meeting https://www.youtube.com/watch?v=dQw4w9WgXcQ