

The background is a dark blue gradient with a subtle pattern of white dots. Overlaid on the left side are several concentric circles and a large circular scale with degree markings from 140 to 260. Some of the circles have arrows indicating a clockwise direction.

EVALUATING NCCS SYSTEM SECURITY COMPLIANCE

AMAN THANVI (GSFC-6062)

SUMMER 2020

MENTOR: GEORGE RUMNEY

ACKNOWLEDGEMENTS

- It has been an honor and privilege to be a summer intern with NCCS.
- I would like to convey a special thanks to:
 - George Rumney
 - John Jasen
 - Jasaun Neff
 - Jordan Caraballo-Vega

PRESENTATION BACKGROUND

- The objective of this project was to evaluate NCCS system security compliance using OpenSCAP, CIS, NASA, and other government and industry standards.
- Given two OpenStack images, one CentOS 7 base image and one CentOS 7 NCCS hardened image, the task was to evaluate their security compliance. I used CIS and OpenSCAP security profiles and agency guidelines to evaluate the degrees of system compliance while referencing government documentation, policies, and standards.
 - Scaptest1 – the CentOS 7 hardened image. Scaptest1 is a representative node of the ADAPT OpenStack functional group managed by the Security Team configuration management ecosystem.
 - Scaptest2 – the CentOS 7 base image. This is CentOS 7 as configured by the vendor and is what you would get upon a fresh installation and no initial configuration. Scaptest2 is a vendor-configured base image. All configurations are set up as they would be upon fresh installation from a vendor image. Note: Scaptest2 is a fresh ADAPT OpenStack image.

PRESENTATION BACKGROUND

- SCAP – Security Content Automation Protocol (SCAP) is a protocol used to audit and assess a target system with a defined set of configuration requirements and rules.
- What is OpenSCAP?
 - OpenSCAP is a security tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF) file format. OpenSCAP is based on a framework of libraries to improve the accessibility of SCAP and enhance the usability of the information it represents and provides.
- What is CIS-CAT?
 - CIS-CAT is a security tool that performs assessments according to the CIS benchmark rules. CIS-CAT offers a powerful tool for analyzing and monitoring the effectiveness of internal security processes.

OpenSCAP vs. CIS-CAT

OpenSCAP	CIS-CAT
Not supported on all OS distributions	Needs Java to run
Faster	Slower
Less comprehensive and less widely available and maintained benchmark files for a variety of OSs	Does not have severity information
Open source	Not free (licensed by NASA)

PRESENTATION METHODOLOGY - INPUT

- Given a detailed, scored report generated by the benchmarking tools:
 - Document flagged issues
 - Determine to how to resolve them
 - Assess the feasibility of the implementation of resolutions to known issues, and
 - Document benchmarks and revise and improve preexisting baselines.

PRESENTATION METHODOLOGY - PROCESS

- Using this documentation and referencing current NCCS implementations and mitigating controls, detailed analysis was performed for each Security Control to identify if established controls need to be modified to improve the NCCS security posture and operations over time.
- Evaluations were made systems and their baselines were made between the NASA Recommended and NASA Required CentOS 7 profiles.
- OpenSCAP and CIS CAT reports
 - Profiles used:
 - NASA Recommended baseline for CentOS 7 Systems
 - NASA Required baseline for CentOS 7 Systems

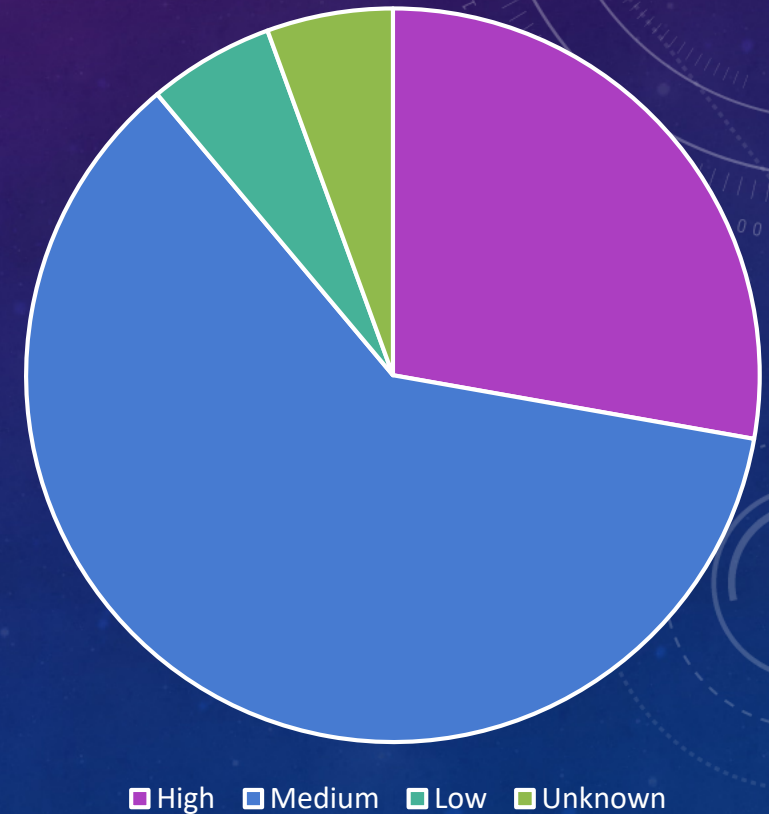
PRESENTATION METHODOLOGY - OUTCOME

- Many current checks were in need of reevaluation.
 - Referencing best practices and policies put into place by NIST publications and more modern security documentation and guidelines, there were multiple risk areas which would benefit from revised implementations and newer checks.
- Identified a revised set of baseline configurations that would benefit NCCS's systems deployment and maintenance infrastructure.
 - NCCS uses a "Puppet"/cloning approach in deploying in their service stacks.
 - It is crucial to determine the representative node
 - The representative node is the most compliant system that is used in the cloning of the rest of the service stack.
 - This security evaluation was comprehensive to allow consideration of multiple cloning approaches currently in use by the NCCS.

PRESENTATION RESULTS AND CONCLUSIONS

- All OpenSCAP reports utilized the default scoring system profile (urn:xccdf:scoring:default). The maximum score a system could achieve was 100.000000
- 18 checks were analyzed for each system, which is approximately 10% of the given sample size. This included:
 - 5 checks with a reported severity of 'High'
 - 11 checks with a reported severity of 'Medium'
 - 1 checks with a reported severity of 'Low,' and
 - 1 checks with a reported severity of 'Unknown.'

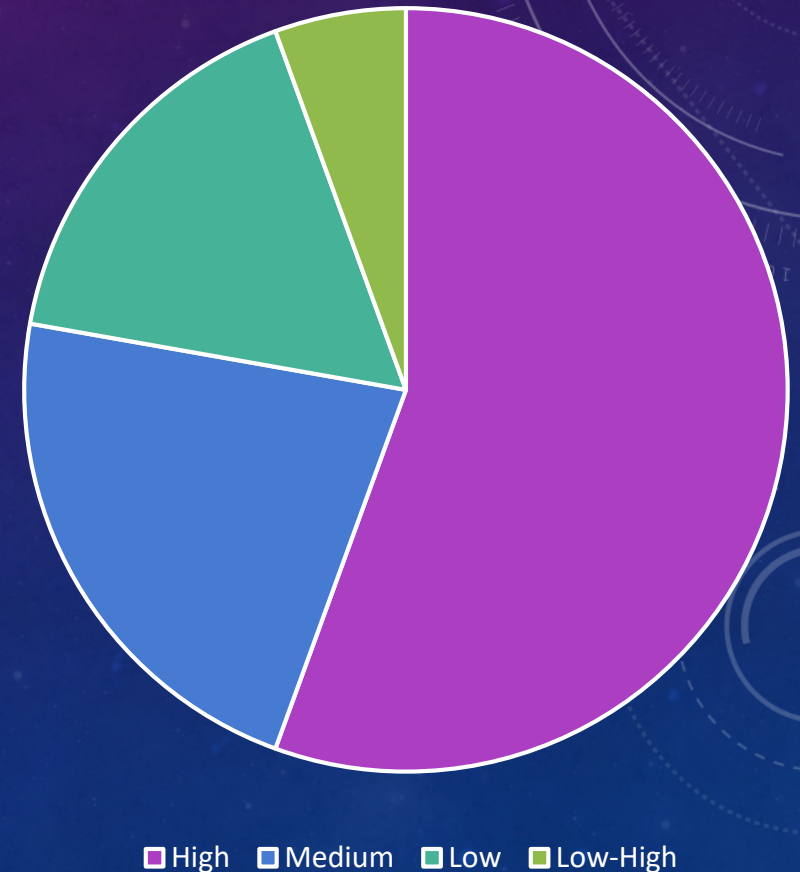
Scaptest1: Number of Checks
(Reported Severity)



PRESENTATION RESULTS AND CONCLUSIONS (CONT.)

- Upon evaluation:
 - 10 checks with a determined severity of 'High'
 - 4 checks with a determined severity of 'Medium'
 - 3 checks with a determined severity of 'Low,' and
 - 1 checks with a determined severity of 'Low-High.'
- The evaluation showed that NCCS security baselines required revisions and implementation of new guidelines and baselines. Some types of recommended remediations discussed amongst the team were:
 - Automation is crucial in our operation. Prioritize the deployment of automated security dashboards and interfaces using web platforms and pipelines for scanning, detection, remediation, and logging.
 - Revisions to current security baselines, benchmarks, and profiles were required.

Scaptest1: Number of Checks
(Determined Severity)



CONSIDERATIONS

- Since NCCS is a High Performance Computing (HPC) environment, some checks are expected to fail. However, the reported risks are mitigated by pre-existing mitigating controls.
 - Take for example NCCS's configuration of auditd, a Linux Audit Daemon:
 - NCCS implements custom audit rules and switches that allow for performance needs to be met.
 - NCCS does not use the Advanced Intrusion Detection Environment (AIDE) package, as it has additional security controls using custom audit rules and scripts paired with customized/tailored logging and detection systems that supplement the presence of AIDE and other existing packages without sacrificing performance.

ADDITIONAL WORK

- Generated a pipeline that allows the remote execution of scans over systems using GitLab.
- The pipeline gets triggered automatically when a file changes in the repository.
- Returns HTML artifact that the system administrator can analyze. Future work includes a better visual approach using dashboards.



OpenSCAP Evaluation Report

Characteristics Compliance and Scoring Rule Overview Result Details

Characteristics

Unauthenticated and unprivileged user **root** started the evaluation at **2014-07-17T13:46:34**. Evaluation finished at **2014-07-17T13:53:55**. The target machine was called **localhost.localdomain**.

Benchmark from **/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml** with ID **xccdf_org.ssgproject.content_benchmark_RHEL-6** was used. Profile was selected.

CPE Platforms

- cpe:/o:redhat:enterprise_linux:6
- cpe:/o:redhat:enterprise_linux:6:client

Addresses

IPv4	127.0.0.1
IPv4	192.168.122.148
IPv6	0:0:0:0:0:0:0:1
IPv6	fe80:0:0:0:5054:ff:fe67:dc41
MAC	00:00:00:00:00:00
MAC	52:54:00:67:DC:41

Compliance and Scoring

The system is **not compliant!** Please review rule results and consider applying remediation.

138 passed 169 failed 80 other

Scoring system	Score	Maximum	%
urn:xccdf:scoring:default	54.081947	100.000000	54.08%

ADDITIONAL WORK

- Participated in knowledge sharing sessions with the team.
- Conducted research pertaining to and prepared informational, in-depth presentations on topics such as Intrusion Detection Systems (IDS) and Incident Response.
- Recommended the formation of a dedicated Incident Response Task Force comprised of professionals and experts spanning different functional areas and involved organizations, stressing the importance of inter and intra-organizational communication and collaboration.

An Introduction to Intrusion Detection Systems

FRIDAY, JULY 17, 2020
AMAN THANVI (GSFC-6062)



AN INTRODUCTION TO INCIDENT RESPONSE

MONDAY, JULY 27, 2020
AMAN THANVI (GSFC-6062)

FUTURE PLANS

- Complete Bachelors degree in Computer Science and Computer Engineering at the University of Maryland, College Park
- Pursue additional cybersecurity intern and research opportunities with NASA.
- Explore the field of artificial intelligence and machine learning as it pertains to cybersecurity.
- Pursue a career in the field of Cybersecurity.



REFERENCES

- NIST Special Publications
- NASA Procedural Requirements and Directives
- NASA Security Handbooks
- OpenSCAP Documentation
- CIS-CAT Documentation