REVA UNIVERSITY
Bengaluru, India
Established as per the section 2(f) of the UGC Act, 1956,
Approved by AICTE, New Delhi

REVA Academy for Corporate Excellence (RACE)

Automation of Server Security Assessment

Varun CP

Date: 23-12-2022

race.reva.edu.in

Agenda

01 Introduction

02 Literature Review

03 Problem Statement

04 Project Objectives

05 Project Methodology

06 Resources Specification

07 Software Design

08 Implementation

09 Testing and Validation

10 Analysis and Results

12 Suggestions and Conclusion

13 Reference

Introduction

Automation of Server Security Assessment

Configuration

Technical Accuracy

Business decisions

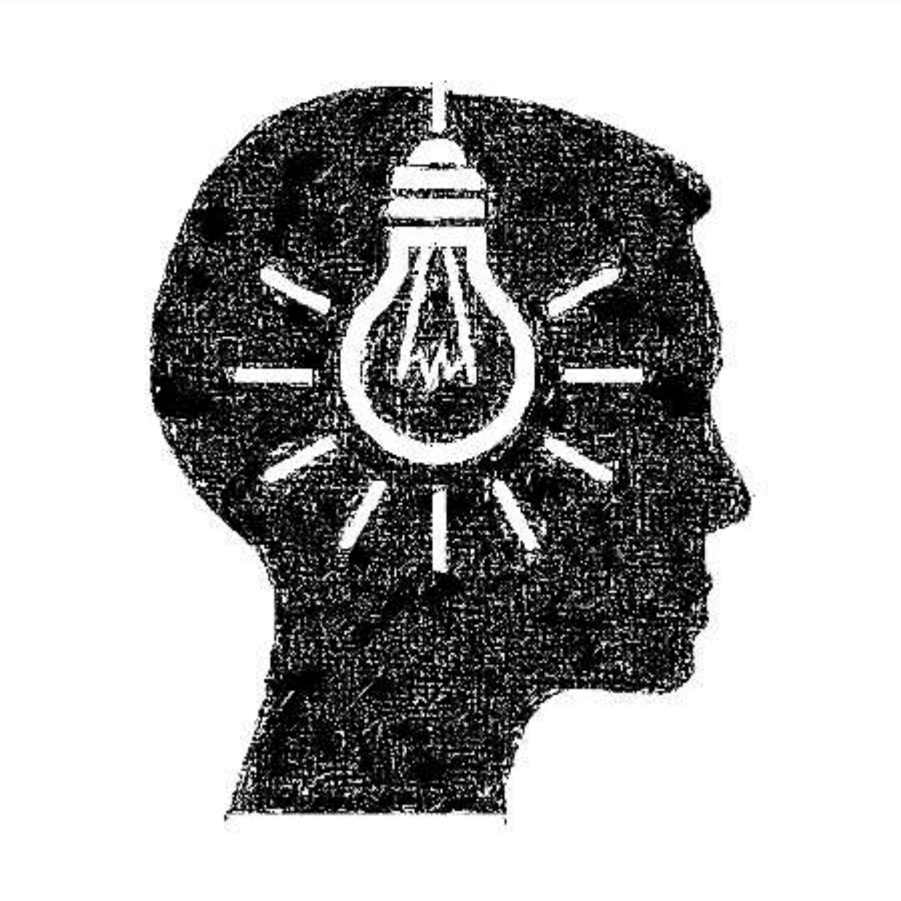
Compliance

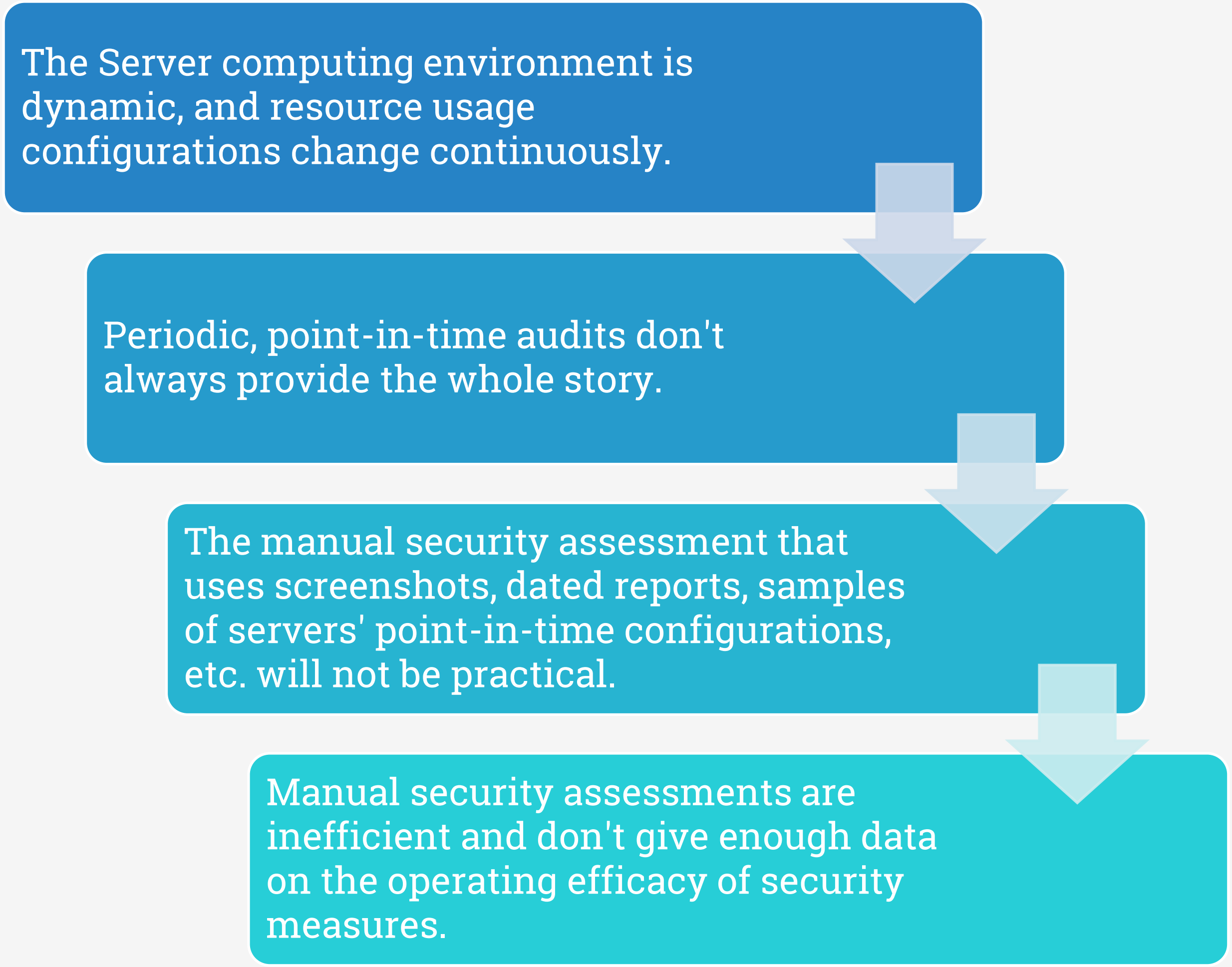
- Default Passwords
- Hardcoded passwords
- Software Patching
- Privilege access controls
- BIOS Configuration
- Unencrypted Data at rest

Literature Review

Paper Title	Authors	Journal	Objective	Research Gap (if any)
An Automated Approach For Mitigating Server Security Issues	Sonali Patra, N C Naveen, Omkar Prabhakar	IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India	To create a framework by designing an automated tool which would perform an audit of the servers and check if it is compliant to all the prescribed security policies. As there are multiple platforms upon which the servers run, the tool is designed to adapt to heterogeneous environment.	The solution address only on USB devices connection, Antivirus, whether the patches are update
Auditing Linux Operating System with Center for Internet Security (CIS) Standard	Wadlkur Kurniawan Sedano, Muhammad Salman	2021 International Conference on Information Technology (ICIT)	Implementation of the CIS Benchmark using the Chef Inspec application.	NA
Automated Hardening of a Linux Web Server	Olencin, Michal and Perhá ˇ c, Ján	NA	The design and implementation of automated hardening a Linux web server after the clean installation based on configuration	The Hardening is addressed only during the initial assessment and techniques used don't allow it to implement the same continuously.
Automated Audit of Compliance and Security Controls	Gerhard Koschorreck	2011 Sixth International Conference on IT Security Incident Management and IT Forensics	discuss the challenges security organizations are facing and present approaches for automation of security checks. The OVAL and XCCDF languages are examined in greater detail and an example for their use is given. We describe use cases for these languages and explain the benefits of their deployment.	NA

Problem Statement





The Server computing environment is dynamic, and resource usage configurations change continuously.

Periodic, point-in-time audits don't always provide the whole story.

The manual security assessment that uses screenshots, dated reports, samples of servers' point-in-time configurations, etc. will not be practical.

Manual security assessments are inefficient and don't give enough data on the operating efficacy of security measures.

Project Objectives

Automation of server configuration evaluation.

- To analyze the information from the servers, which can provide the data points of the configuration for the security evaluation

Low-cost operations and Implementation

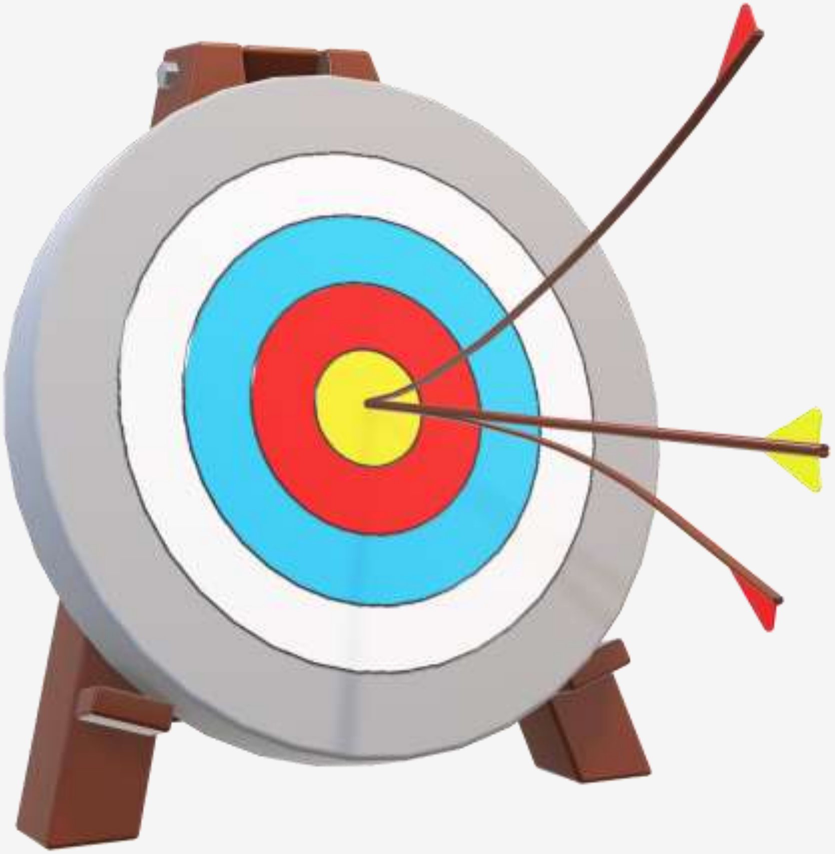
- Affordable solution and improve the capabilities to ensure that most configuration evaluations can be automated.

Compliance

- Fine-tuning the logical settings of security assessment which can be adjusted to the relevant security standards

Installing & Configuration the dependencies

- Installing the dependent tools and modules for Server configuration assessment



Project Methodology

Server configuration assessment framework

- Ansible
- Lynis

Ansible

- Installation & Execution of Lynis
- Authentication Strategy

Lynis

- Security audit tool
- System hardening

https://t4.ftcdn.net/jpg/03/45/87/51/360_F_345875119_qp8HoV1xvKu6DBHvnTWihzQ5aidEqYHW.jpg

Resource Specifications

Laptop

- Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz
- 8.00 GB (7.86 GB usable)

Base Machine

- Windows Home.

Virtualization

- VMware® Workstation 16 Pro

Virtual Machine

- Ubuntu 20.04.4 LTS (Focal Fossa)

Interpreter

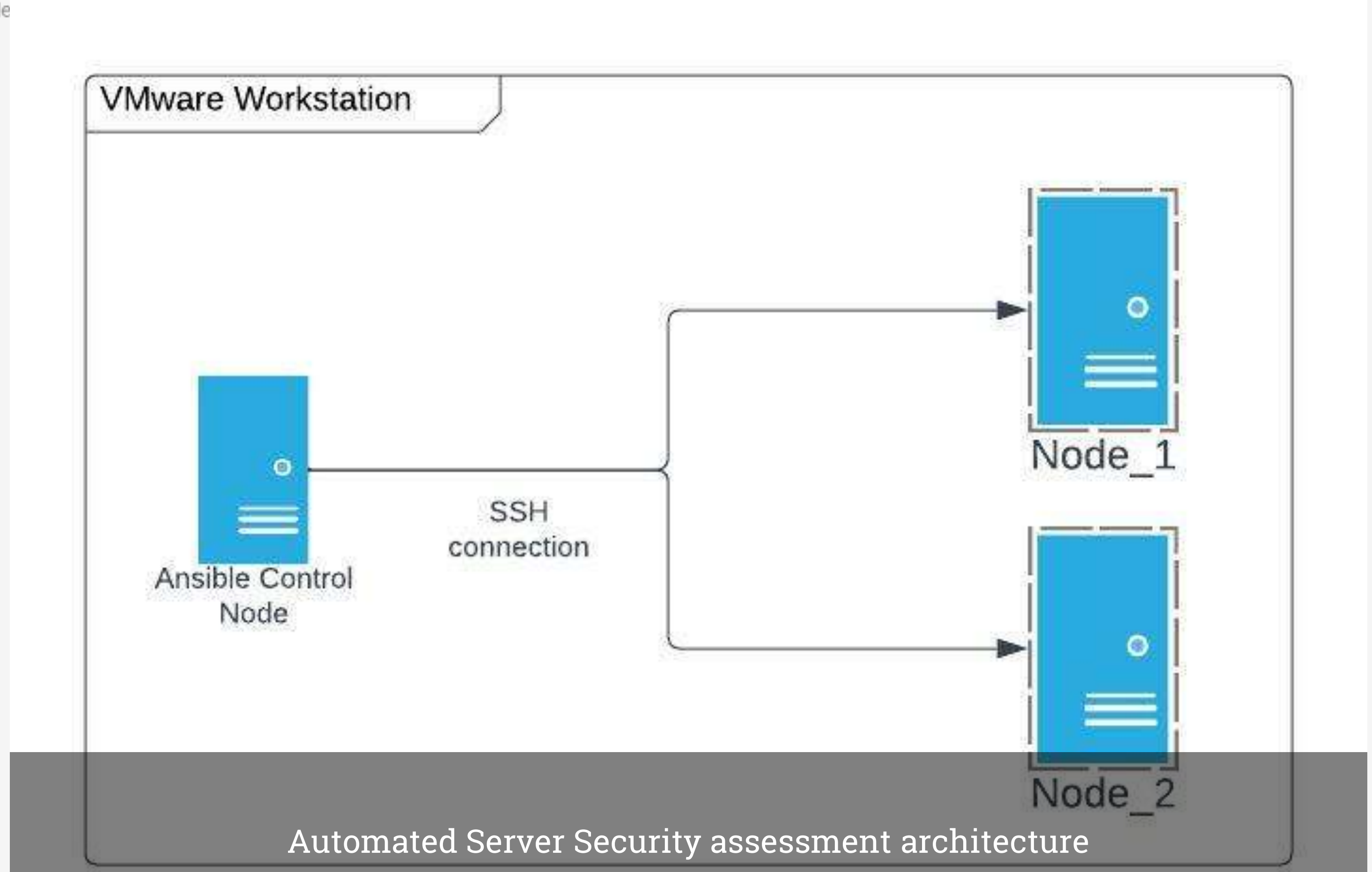
- Python 3.9

Security Assessment framework

- Lynis
- Ansible
- ansi2html

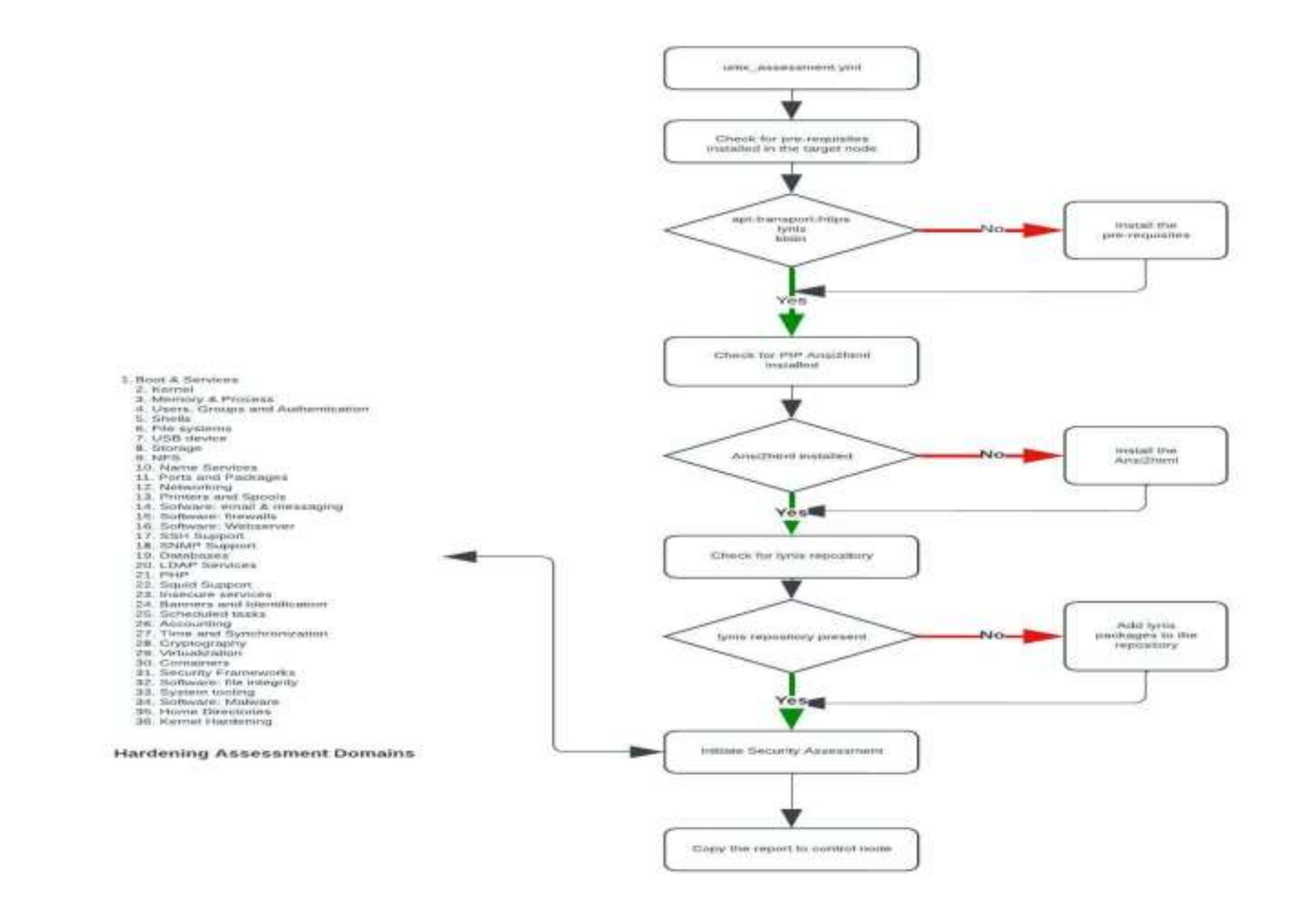
https://static.thenounproject.com/png/2754537-200.png

Software Design



Automated Server Security assessment architecture

Data Flow Diagram



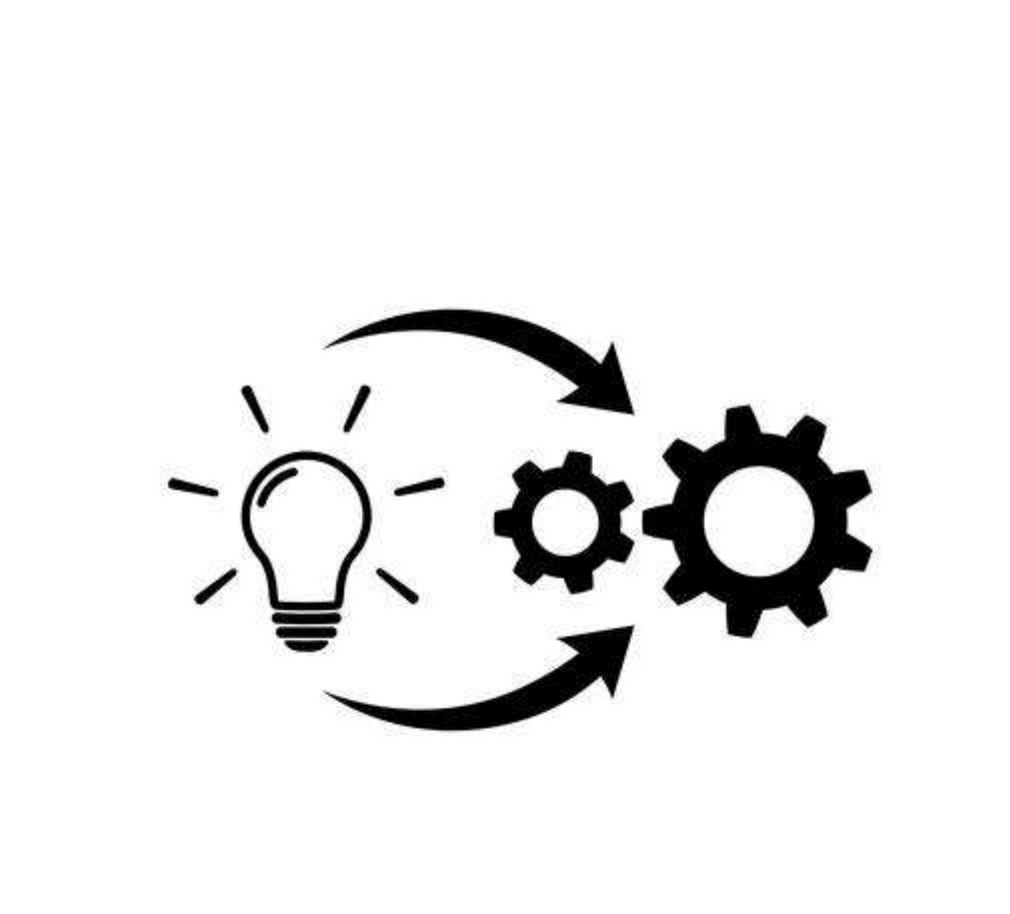
Data flow diagram of Automated server security assessment

Implementation

Installation of Ansible in the control node

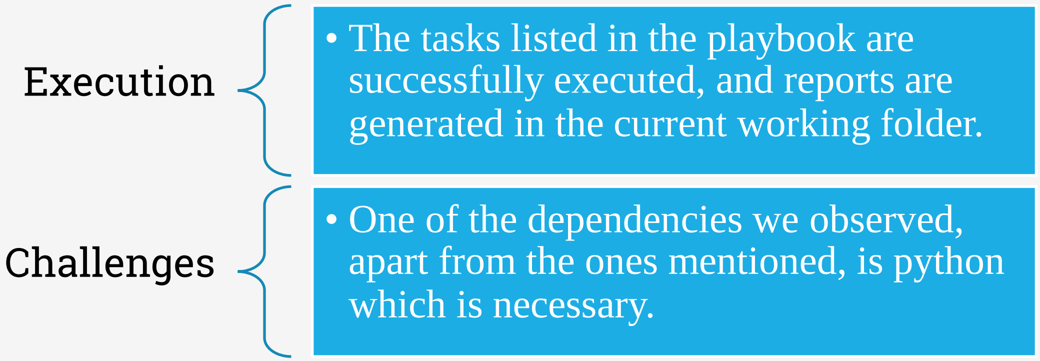
Configuring Key based ssh authentication between servers and Ansible control node.

Installing Ansible and executing the playbook



https://c8.alamy.com/zooms/9/b46398bd17d7421097009c651828339a/p3g9eg.jpg

Testing and Validation

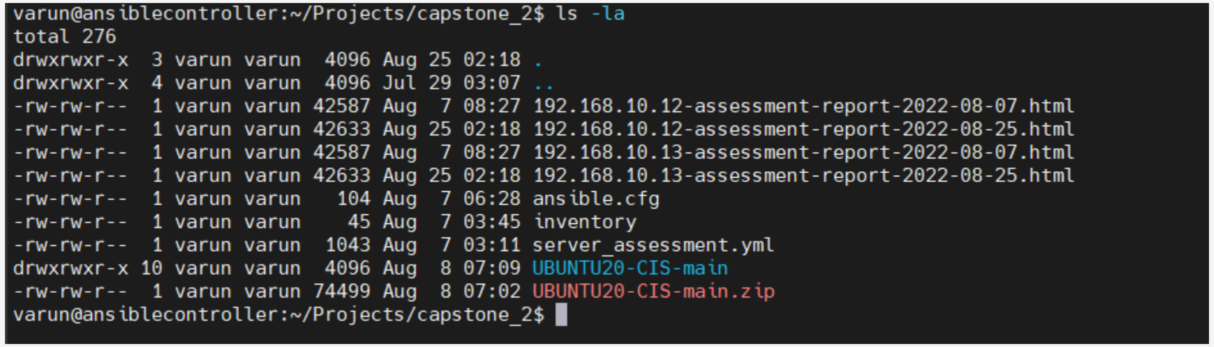


Execution

- The tasks listed in the playbook are successfully executed, and reports are generated in the current working folder.

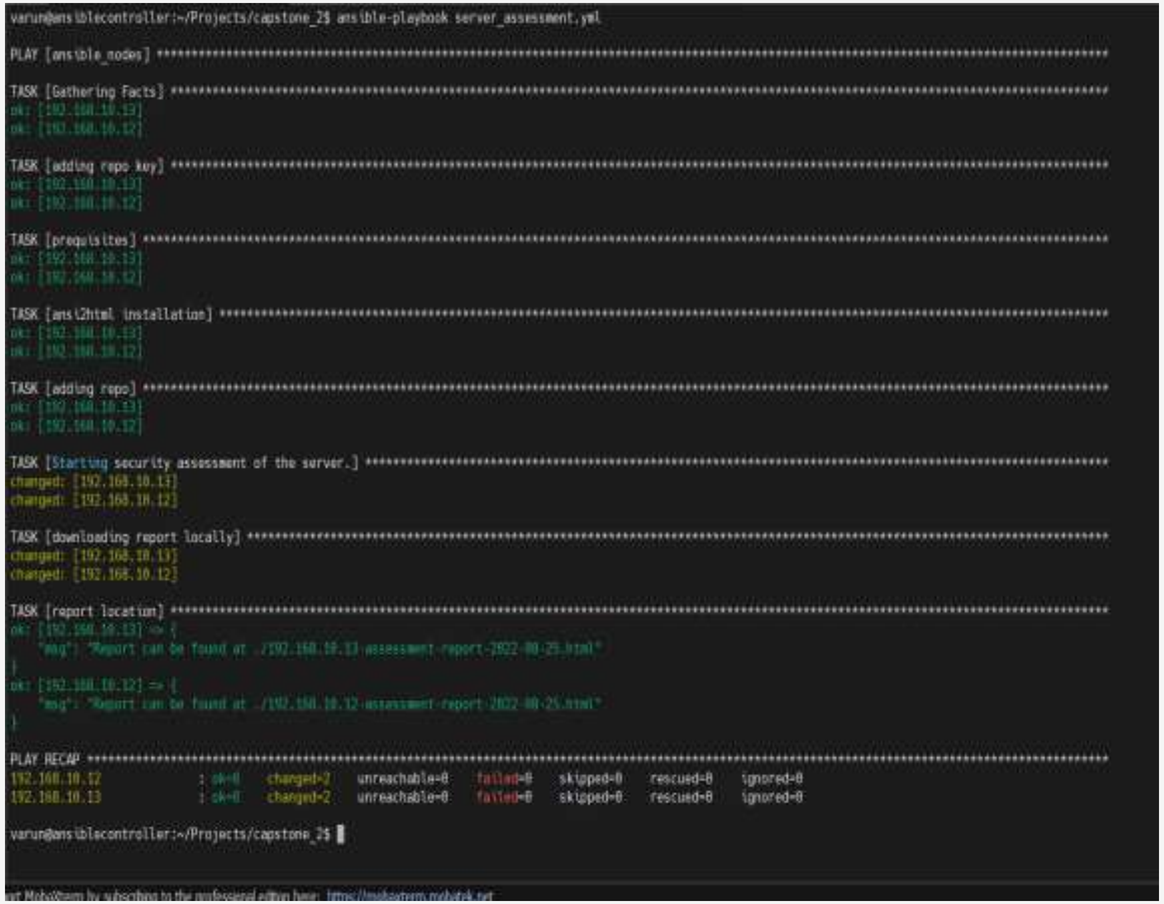
Challenges

- One of the dependencies we observed, apart from the ones mentioned, is python which is necessary.



```
varun@ansiblecontroller:~/Projects/capstone_2$ ls -la
total 276
drwxrwxr-x  3 varun varun  4096 Aug 25 02:18 .
drwxrwxr-x  4 varun varun  4096 Jul 29 03:07 ..
-rw-rw-r--  1 varun varun 42587 Aug  7 08:27 192.168.10.12-assessment-report-2022-08-07.html
-rw-rw-r--  1 varun varun 42633 Aug 25 02:18 192.168.10.12-assessment-report-2022-08-25.html
-rw-rw-r--  1 varun varun 42587 Aug  7 08:27 192.168.10.13-assessment-report-2022-08-07.html
-rw-rw-r--  1 varun varun 42633 Aug 25 02:18 192.168.10.13-assessment-report-2022-08-25.html
-rw-rw-r--  1 varun varun   104 Aug  7 06:28 ansible.cfg
-rw-rw-r--  1 varun varun    45 Aug  7 03:45 inventory
-rw-rw-r--  1 varun varun  1043 Aug  7 03:11 server_assessment.yml
drwxrwxr-x 10 varun varun  4096 Aug  8 07:09 UBUNTU20-CIS-main
-rw-rw-r--  1 varun varun 74499 Aug  8 07:02 UBUNTU20-CIS-main.zip
varun@ansiblecontroller:~/Projects/capstone_2$
```

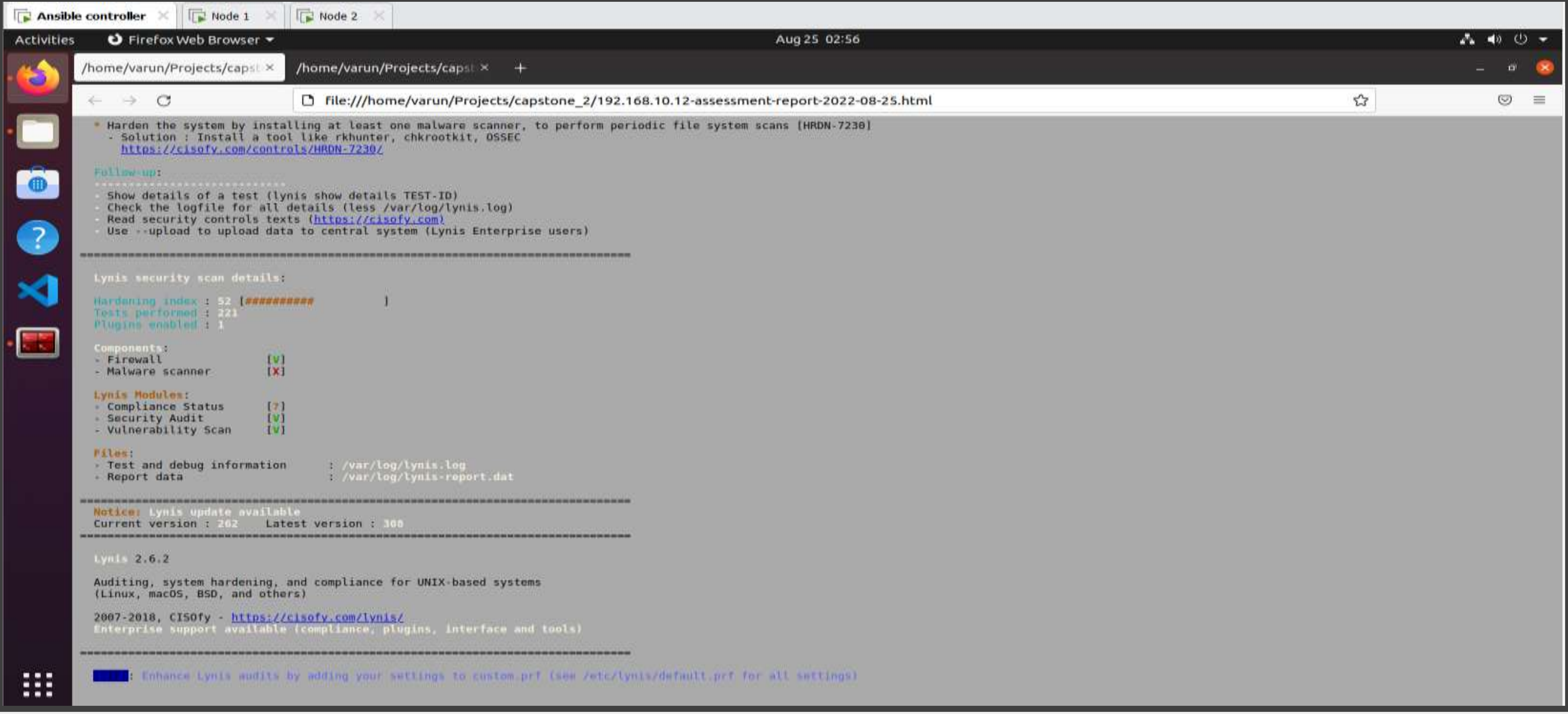
Reports generated post execution of the server assessment



```
varun@ansiblecontroller:~/Projects/capstone_2$ ansible-playbook server_assessment.yml

PLAY [ansible_nodes] ************************************************************************

TASK [Gathering Facts] **********************************************************************
ok: [192.168.10.13]
ok: [192.168.10.12]

TASK [adding repo key] **********************************************************************
ok: [192.168.10.13]
ok: [192.168.10.12]

TASK [prequisites] **************************************************************************
ok: [192.168.10.13]
ok: [192.168.10.12]

TASK [ansi2html installation] ***************************************************************
ok: [192.168.10.13]
ok: [192.168.10.12]

TASK [adding repo] **************************************************************************
ok: [192.168.10.13]
ok: [192.168.10.12]

TASK [Starting security assessment of the server.] ******************************************
changed: [192.168.10.13]
changed: [192.168.10.12]

TASK [downloading report locally] ***********************************************************
changed: [192.168.10.13]
changed: [192.168.10.12]

TASK [report location] **********************************************************************
ok: [192.168.10.13] => {
    "msg": "Report can be found at ./192.168.10.13-assessment-report-2022-08-25.html"
}
ok: [192.168.10.12] => {
    "msg": "Report can be found at ./192.168.10.12-assessment-report-2022-08-25.html"
}

PLAY RECAP **********************************************************************************
192.168.10.12              : ok=8    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
192.168.10.13              : ok=8    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

varun@ansiblecontroller:~/Projects/capstone_2$
```

rt MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Executing the Ansible Playbook



Ansible controller
Node 1
Node 2
Activities
Firefox Web Browser
Aug 25 02:56
/home/varun/Projects/capst
/home/varun/Projects/capst
file:///home/varun/Projects/capstone_2/192.168.10.12-assessment-report-2022-08-25.html

```
 * Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
   - Solution : Install a tool like rkhunter, chkrootkit, OSSEC
     https://cisofy.com/controls/HRDN-7230/

 Follow-up:
 ----------------------------
 - Show details of a test (lynis show details TEST-ID)
 - Check the logfile for all details (less /var/log/lynis.log)
 - Read security controls texts (https://cisofy.com)
 - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

 Lynis security scan details:

 Hardening index : 52 [##########          ]
 Tests performed : 221
 Plugins enabled : 1

 Components:
 - Firewall               [V]
 - Malware scanner        [X]

 Lynis Modules:
 - Compliance Status      [?]
 - Security Audit         [V]
 - Vulnerability Scan     [V]

 Files:
 - Test and debug information      : /var/log/lynis.log
 - Report data                     : /var/log/lynis-report.dat

================================================================================
 Notice: Lynis update available
 Current version : 262    Latest version : 308
================================================================================

 Lynis 2.6.2

 Auditing, system hardening, and compliance for UNIX-based systems
 (Linux, macOS, BSD, and others)

 2007-2018, CISOfy - https://cisofy.com/lynis/
 Enterprise support available (compliance, plugins, interface and tools)

================================================================================

 [illegible]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Analysis and Results

- Ensure the real-time point information is available for the assessor
- The hardening index which can be used to fix the existing deviation or to affirm the security posture of the organization.

Suggestions and Conclusion

In conclusion, the result of this work is a fully functional configuration playbook, which in comparison to existing solutions, achieved the automated security assessment; the project comprehensively solves the automation of server security assessment.

However, the security assessment tools used do not cover the potential vulnerabilities. The designed solution has improved Server security assessment. In addressing the problem, care must be taken to continually improve and mend the security of existing solutions, monitor these solutions, and maintain cyber hygiene.

References

[1] Verizon, “DBIR Data Breach Investigations Report,” 2008.

[2] S. Patra, N. C. Naveen, and O. Prabhakar, “An automatedapproach for mitigating server security issues,” in *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016 - Proceedings*, Jan. 2017, pp. 1075–1079. doi: 10.1109/RTEICT.2016.7807996.

[3] W. K. Sedano and M. Salman, “Auditing Linux Operating System with Center for Internet Security (CIS) Standard,” in *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, Jul. 2021, pp. 466–471. doi: 10.1109/ICIT52682.2021.9491663.

[4] K. A. Asmitha and P. Vinod, “A machine learning approach for linux malware detection,” *Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques, ICICT 2014*, pp. 825–830, 2014, doi: 10.1109/ICICICT.2014.6781387.

[5] R. Montesino and S. Fenz, “Information Security Automation: How Far Can We Go?,” in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 280–285. doi: 10.1109/ARES.2011.48.

References

[6] Isaca, “Auditing Linux/Unix Server Operating Systems.” [Online]. Available: www.isaca.

[7] G. Koschorreck, “Automated Audit of Compliance and Security Controls,” in *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, 2011, pp. 137–148. doi: 10.1109/IMF.2011.12.

[8] “CIS_Ubuntu_Linux_20.04_LTS_STIG_Benchmark_v1.0.0”.

[9] H. Dabthong, M. Warasart, P. Duma, P. Rakdej, N. Majaroen, and W. Lilakiatsakun, “Low Cost Automated OS Security Audit Platform Using Robot Framework,” in *2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C)*, 2021, pp. 31–34. doi: 10.1109/RI2C51727.2021.9559826.

[10] M. Olenčin and J. Perháč, “Automated Hardening of a Linux Web Server.”

[11] HUNTSMAN | TIER-3 PTY LTD, “Cyber security audit challenges in 2020,” Chatswood NSW 2067, 2020. [Online]. Available: www.huntsmansecurity.com/blog/audit-compliance-risk-cyber-security-

REVA UNIVERSITY
Bengaluru, India

Established as per the section 2(f) of the UGC Act, 1956,
Approved by AICTE, New Delhi

Thank you!