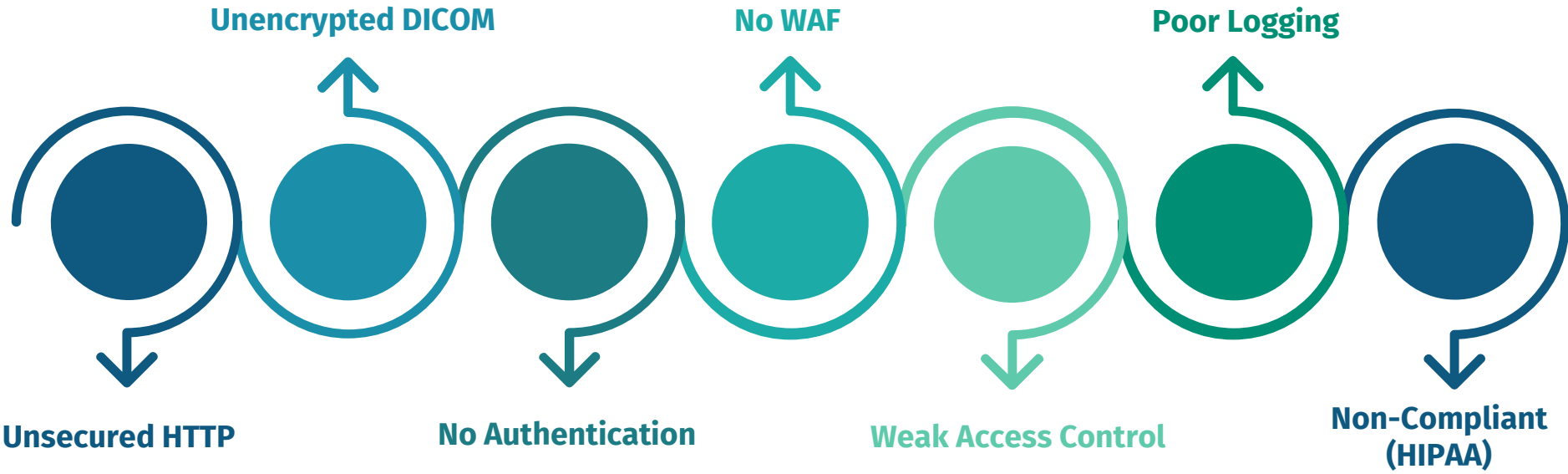
PACS-DICOM VIA ORTHANC

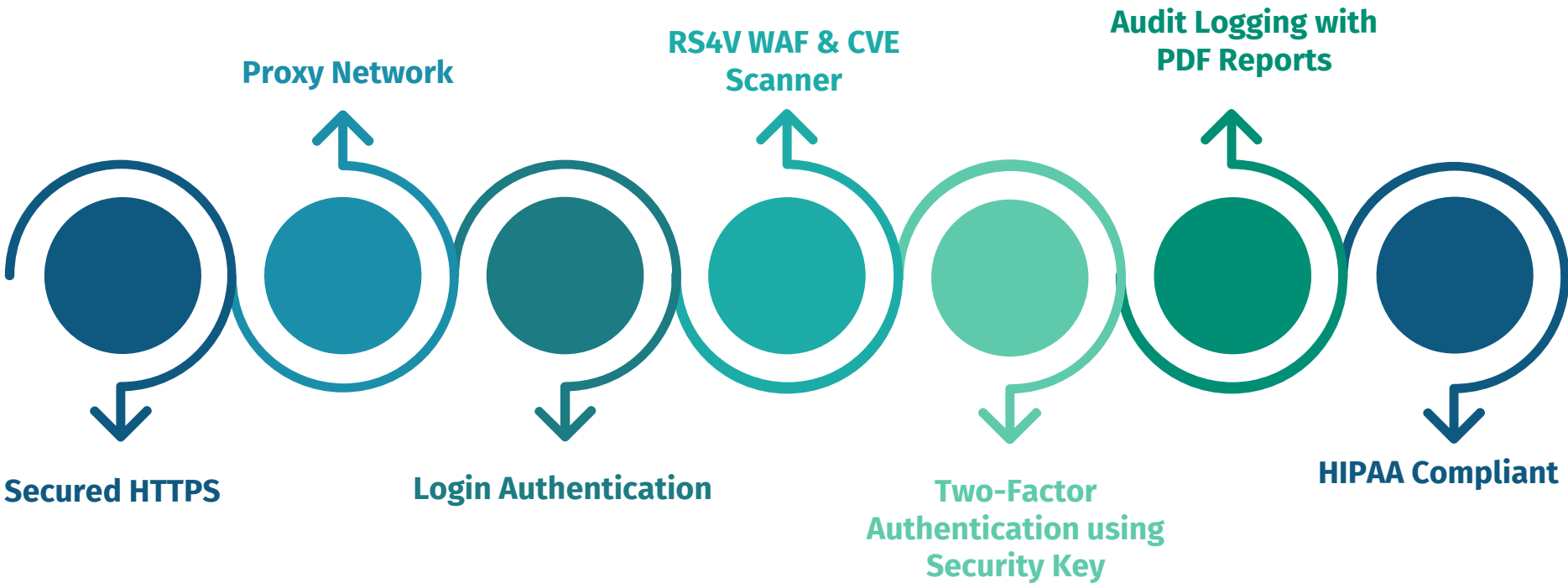
- Regan
- Shashank
- Shravan
- Varad

RS4V

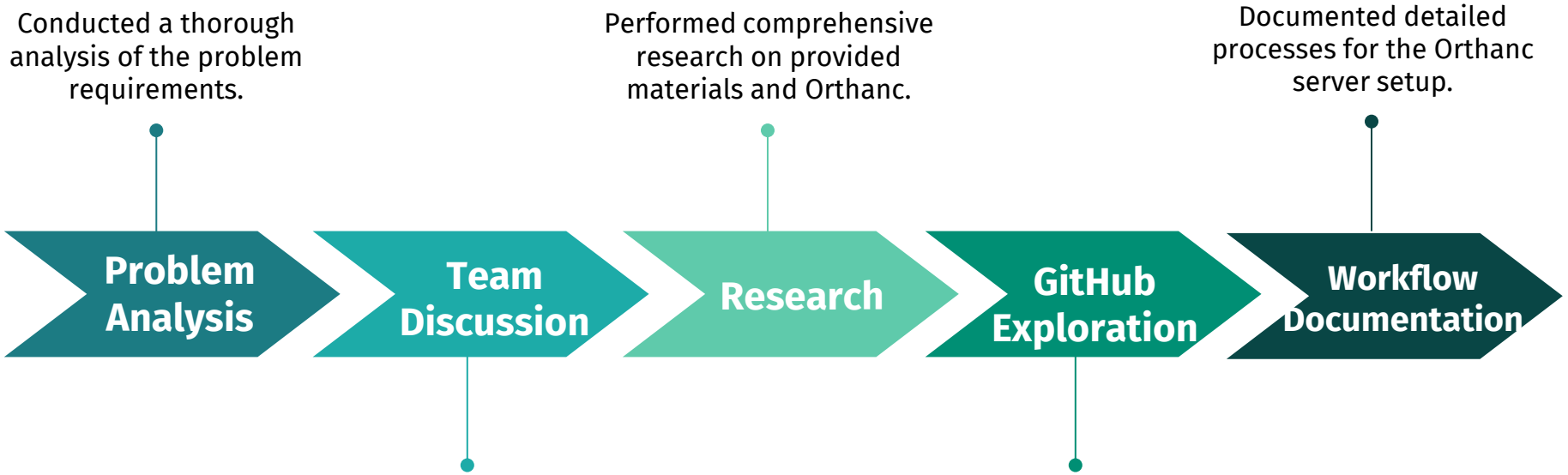
Vulnerabilities in Official Orthanc



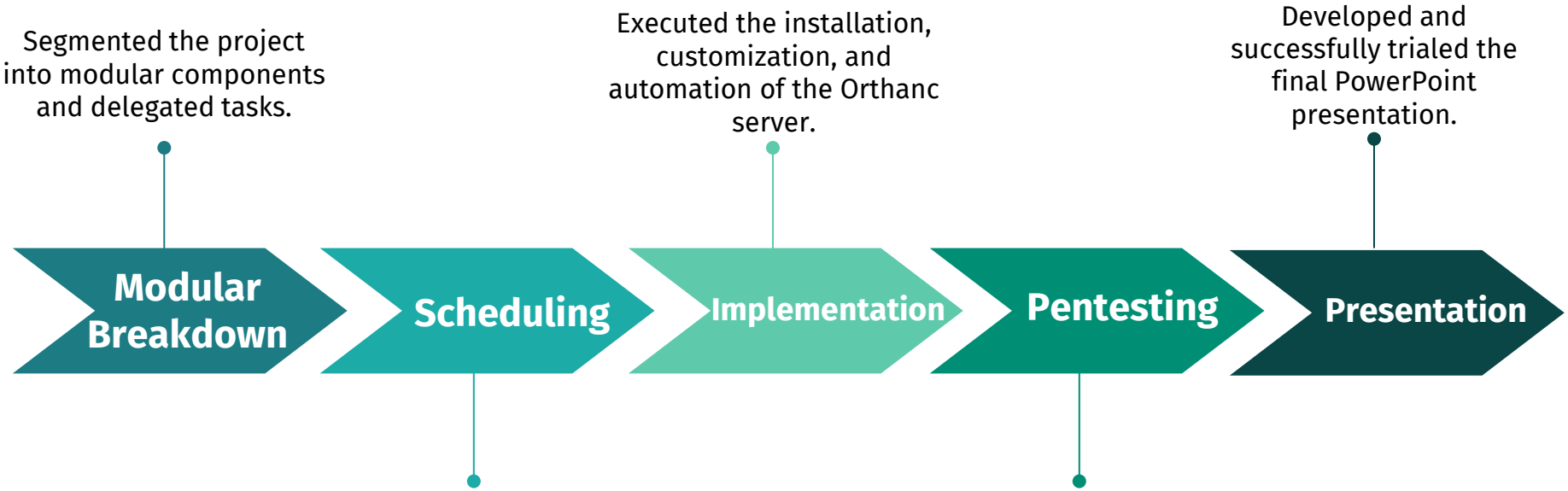
Fixed Vulnerabilities in RS4V Orthanc



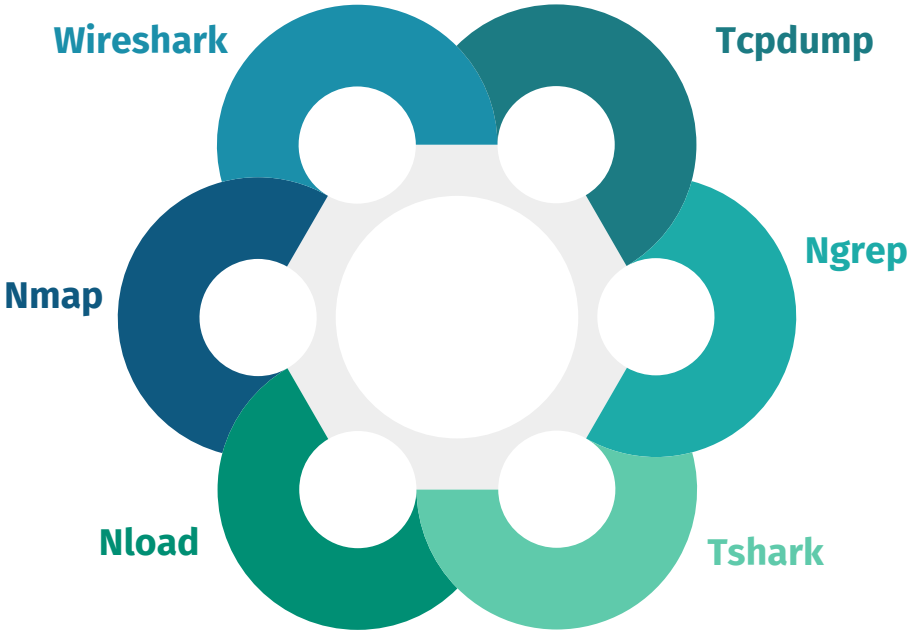
Methodology



Methodology

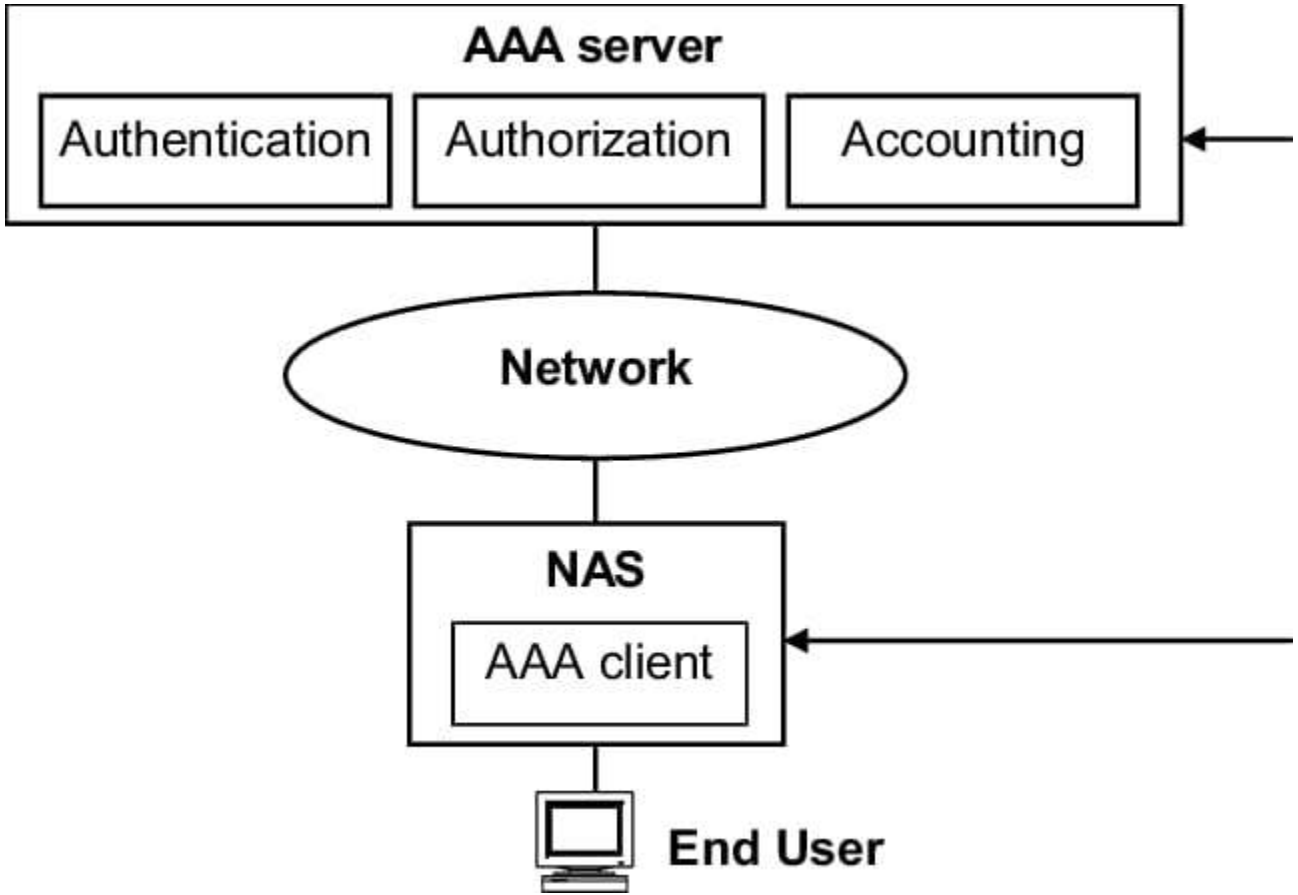


Tools Used for Pentesting

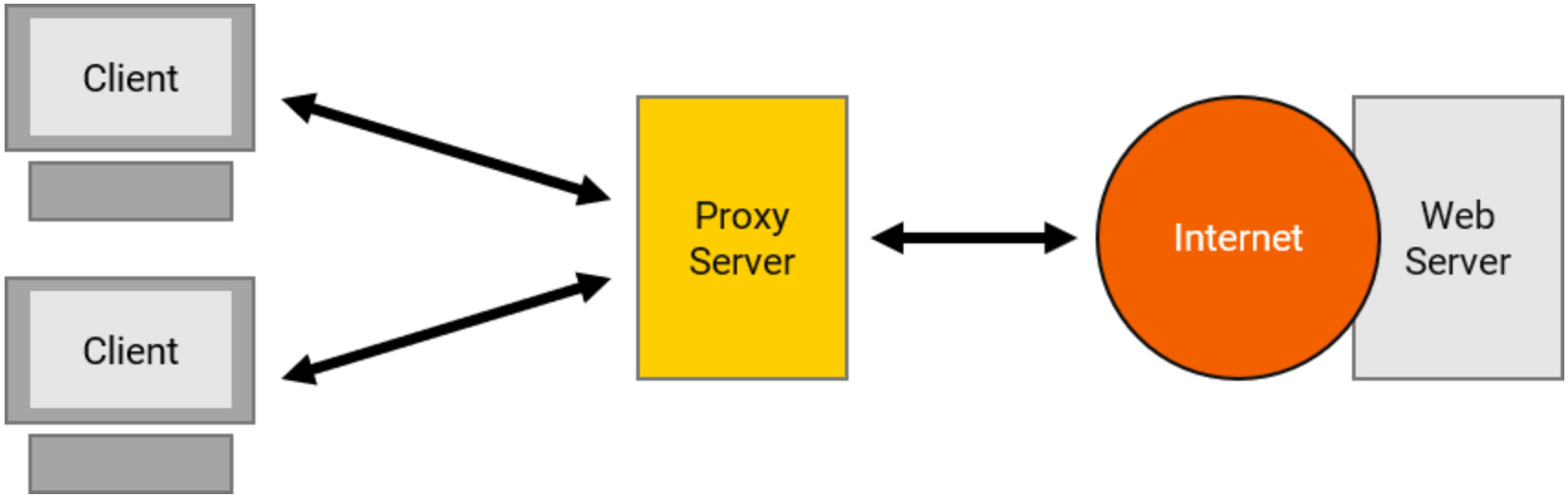


Product Demonstration

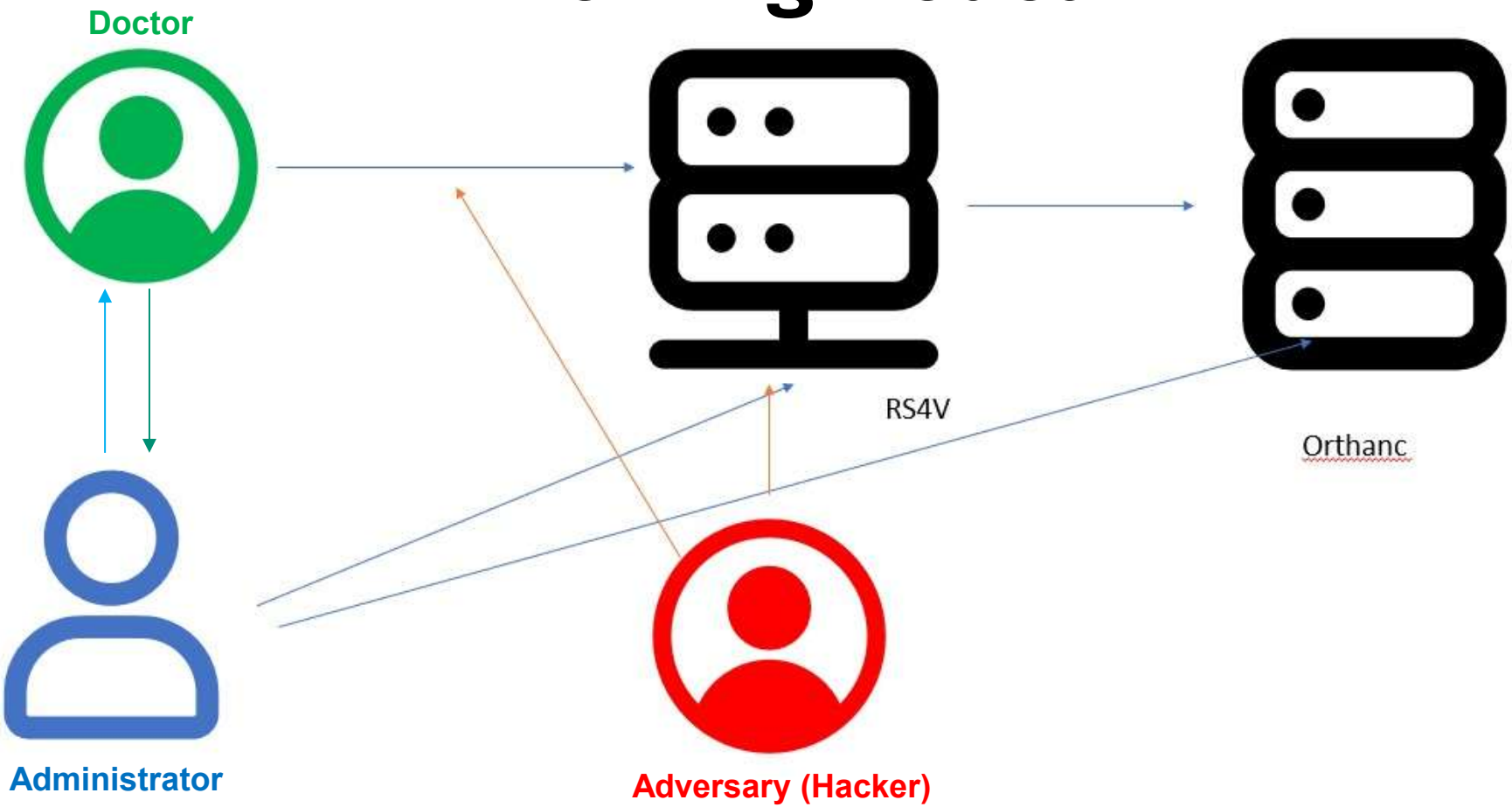
Triple A Framework



Proxy Network



Working Model



NIST Cybersecurity Framework

Scans Orthanc for CVE

Orthanc Vulnerability Scan Report

Orthanc Version: 1.12.2

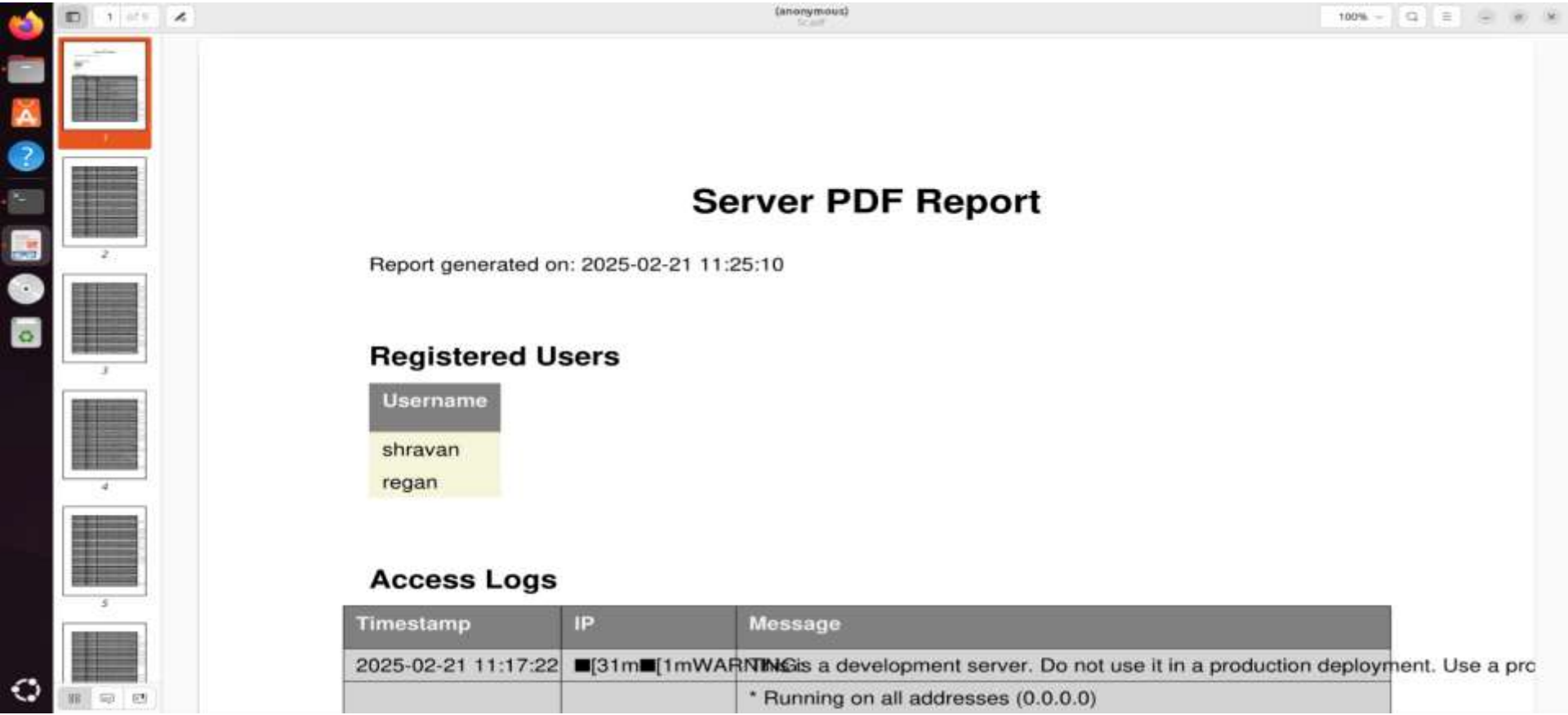
CVE	Category	Score	Status	Fix	Details
CVE-2019-11687	Dicom	7.5	True	----https://www.cisa.gov/news-events/ics-alerts/ics-alert-19-162-0	
CVE-2023-33466	Orthanc	9.0	True	----	https://nvd.nist.gov/vuln/detail/CVE-2023-33466
CVE-2024-22725	Orthanc	8.5	True	----	https://nvd.nist.gov/vuln/detail/CVE-2024-22725
CVE-2025-0896	Orthanc	8.0	True	https://www.securityweek.com/orthanc-server-vulnerability-poses-risk-to-medical-data	
CVE-2023-7238	Orthanc	7.0	True	---- https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-7238	

Orthanc Configuration Issues:

- Default HTTP port (8042) is used. Consider changing it.
- HttpDescribeErrors is enabled. It can expose sensitive information. Disable it.
- Default Dicom port (4242) is enabled. This might be a security issue.
- SSL is disabled. Connection is not encrypted. Security issue.
- Dicom TLS is disabled. Security issue.

As of February 21(today) we have latest CVE Database. Example: CVE-2025-0896, which no other plugin does

Audit Logging PDF Report



Server PDF Report

Report generated on: 2025-02-21 11:25:10

Registered Users

Username
shravan
regan

Access Logs

Timestamp	IP	Message
2025-02-21 11:17:22	■[31m■[1mWARNING	is a development server. Do not use it in a production deployment. Use a prc
		* Running on all addresses (0.0.0.0)

Audit Logging PDF Report

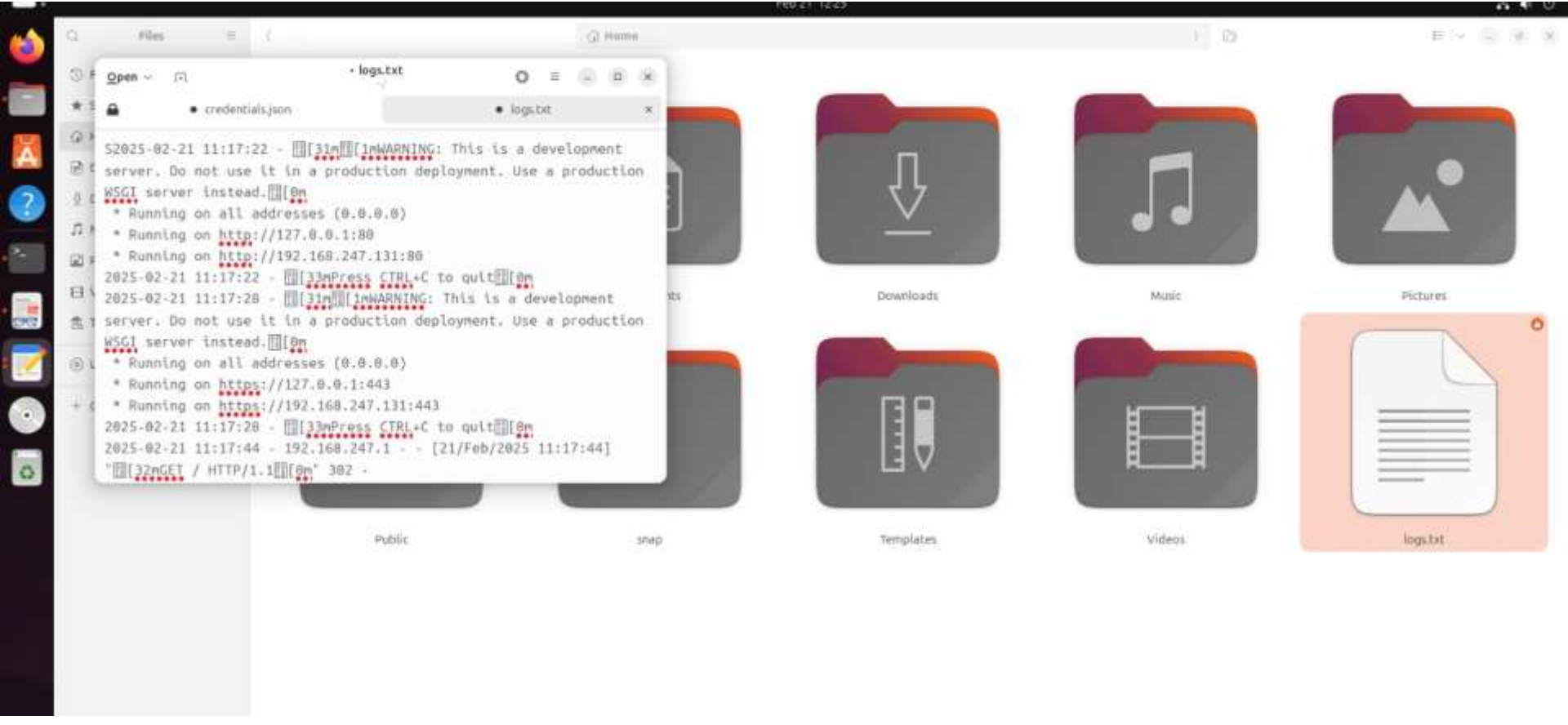
2025-02-21 11:18:26	192.168.247.1	- - [21/Feb/2025 11:18:26] "GET /login?next=https://rs4v.com/favicon.ico HTTP/1.
2025-02-21 11:18:30	192.168.247.1	- - [21/Feb/2025 11:18:30] "■[32mGET /admin HTTP/1.1■[0m" 302 -
2025-02-21 11:18:30	2025-02-21	11:18:30 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/a
2025-02-21 11:18:30	192.168.247.1	- - [21/Feb/2025 11:18:30] "GET /login?next=https://rs4v.com/admin HTTP/1.1" 20
2025-02-21 11:18:30	192.168.247.1	- - [21/Feb/2025 11:18:30] "■[32mGET /favicon.ico HTTP/1.1■[0m" 302 -
2025-02-21 11:18:30	2025-02-21	11:18:30 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/f
2025-02-21 11:18:30	192.168.247.1	- - [21/Feb/2025 11:18:30] "GET /login?next=https://rs4v.com/favicon.ico HTTP/1.
2025-02-21 11:18:33	192.168.247.1	- - [21/Feb/2025 11:18:33] "■[32mGET / HTTP/1.1■[0m" 302 -
2025-02-21 11:18:33	2025-02-21	11:18:33 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/
2025-02-21 11:18:33	192.168.247.1	- - [21/Feb/2025 11:18:33] "GET /login?next=https://rs4v.com/ HTTP/1.1" 200 -
2025-02-21 11:18:34	192.168.247.1	- - [21/Feb/2025 11:18:34] "■[32mGET /favicon.ico HTTP/1.1■[0m" 302 -
2025-02-21 11:18:34	2025-02-21	11:18:34 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/f
2025-02-21 11:18:34	192.168.247.1	- - [21/Feb/2025 11:18:34] "GET /login?next=https://rs4v.com/favicon.ico HTTP/1.
2025-02-21 11:18:55	2025-02-21	11:18:55 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/
2025-02-21 11:18:55	192.168.247.1	- - [21/Feb/2025 11:18:55] "POST /login?next=https://rs4v.com/ HTTP/1.1" 200 -
2025-02-21 11:18:55	192.168.247.1	- - [21/Feb/2025 11:18:55] "■[32mGET /favicon.ico HTTP/1.1■[0m" 302 -
2025-02-21 11:18:55	2025-02-21	11:18:55 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/f
2025-02-21 11:18:55	192.168.247.1	- - [21/Feb/2025 11:18:55] "GET /login?next=https://rs4v.com/favicon.ico HTTP/1.
2025-02-21 11:19:00	2025-02-21	11:19:00 - 192.168.247.1 accessed https://rs4v.com/login?next=https://rs4v.com/
2025-02-21 11:19:00	192.168.247.1	- - [21/Feb/2025 11:19:00] "GET /login?next=https://rs4v.com/ HTTP/1.1" 200 -

Password Encryption

Orthanc Config File

RS4V Stores Credentials with Irreversible Hash Function

Automatic Logs From the starting of Server



THANK YOU

Any Questions ?