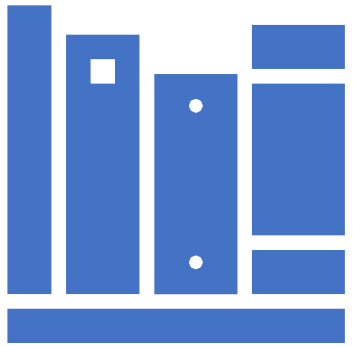


Proposal Presentation

HardnBot :
Server Hardening Automation Software

HardnBot

Research Crew

- IT16054400 -R.M Budditha Rathnayake
- IT16022416-G.G.L Anjula
- IT16167742-W.M.K.M.W Wijekoon
- IT16099746-Aruna Shan H.G.R

Introduction

HardnBot

- Here fully automated free open source hardening platform is developed with the capability to detect poor or non-compliant configurations in a system (OS/DB/Application) and applying industry recommended fixes/configurations and secure systems by reducing its surface of vulnerabilities.
- This research composes a great business value as it can cover 90% of an Information Systems Audit and hardening process.
- By helping the organization understand and control risks and identifying opportunities/industry best practices to embrace.
- This software also will allow internal audit to position themselves as trusted advisors.

HardnBot

Research Problem

- Manual Server auditing and hardening is a process that server custodian will manually audit the server for any compliance failures and correct them manually.
- There is no fully automated hardening platform implemented yet. Even the network administrators plan to do the Hardening processes manually, it might take more than 6 hours for the complete harden processes to complete.

Research Gap

HardnBot

- Design formatted configuration libraries/Design Solution structures/libraries.
- Design OS commands/Queries.
- Implement scans to detect non-compliant parameters in OS/DB components.
- Implement backup functions.
- Implement methods to apply fixes.
- Implement follow up sheets to track audit progress.
- Track performance of applied fixes and logging.

Solution Proposed

HardnBot

- Fully automated operations.
- Automatically detect OS/Database/Application components.
- Perform registry scans to identify registry errors.
- Comprehensive scans on group policies.
- Automatically execute quarries to detect configurations (OS/DB).
- Compare output with pre-defined configuration libraries.
- Generate detailed reports on detected vulnerabilities.
- Apply fixes upon user confirmation.
- Brings industry best practices into your system configurations.
- Provide audit checklists/questionnaires covering all functions of a comprehensive audit.
- Maintain follow up sheets to track audit progress.
- Backup system configurations before applying any fixes.

Product Comparison

HardnBot

Features	Lynis	YoLinux	Open Audit	Pentana Software	NetWrix	SolarWinds	Audit Prodigy
No need to Expert knowledge for doing the audit	*	*	*	*	*	*	*
Generate detailed reports	*		*		*		
Risk Assessment				*			*
Monitoring Network Devices		*	*			*	
Backup Functions for all the settings							
Compare with previous reports							
Mobile Access							*
Vulnerability detection	*	*					

HardnBot

Tools and Techniques

Tools

- Microsoft Visual Studio IDE
- VMware Workstation
- PuTTY

Techniques

- C#
- Ansible
- Python
- Perl
- Shell Script

HardnBot

Task Distribution

Member	Task
IT16054400 **R.M Budditha Rathnayake**	• Design the main dashboard and integrate the system. • Setup SSH connection to servers through dashboard. • Implement scans to detect OS/DB/Application components/versions. • Design OS commands/Query • Ansible installation and its configurations • Manage node requirements to communicate through SSH • Create Ansible configuration files by CIS benchmarks for separate OS/DB/Application versions.
IT16022416 **G.G.L Anjula**	• Design formatted external configuration files. • Manage privileges. • Implement customizable configuration files. (Install updates, patches and additional software's/OS services /Special purpose services) • Create Ansible configuration files by CIS benchmarks for separate OS/DB/Application versions. • Design interface for backup and Implement backup functions. • Setup secure VPN tunnel.

HardnBot

Task Distribution

Member	Task
IT16167742 **W.M.K.M.W Wijekoon**	• Implement audit checklist. • Create Ansible configuration files by CIS benchmarks for separate OS/DB/Application versions. • Implement follow up sheets to track audit progress. • Implement customizable configuration files. (Network configuration and Firewalls / Logging and Auditing / System Access and Environment) • Generate detailed reports and implement export functions for reports. • Perform Dry-Run and make a report for every hardening. • Design interface for reporting.
IT16099746 **Aruna Shan H.G.R**	• Create Ansible configuration files by CIS benchmarks for separate OS/DB/Application versions. • Implement customizable configuration files. (Warning Banners / System maintenance) • Implement scan function using Ansible audits. • Track performance of Applied fixes and logging. • Design interface for scanning.

Setup connection and perform hardening

HardnBot

- Eliminate potential attacks by attack vectors and minimize the system's attack surface.
- Remote access is more commonly accomplished using a secure software solution like a VPN software, by connecting hosts through a hard-wired network interface or Wi-Fi network interface or by connecting via the internet
- After identifying the system type hardening is carried out by Ansible scripts according to industry best practices or CIS benchmark's best practices

Implementation of backup functions

- The good way of hardening is hardening the backup image of the system.
- This backup server is responsible for restoring files, folders, databases in order to prevent the loss of data in the event of a hardening failure, user error, disaster or accident.
- This backup server should have or Create/Use a local account with administrative access which has suitable privileges to perform hardening.
- As an example backup should be stored in a cloud storage, hard drive or a network share folder.

HardnBot

Implementation of Audit and Reporting

- Before the hardening process starts, the software needs to audit the server to find any failed compliances which is generally called as “server compliance audit”, and then if any failed compliances exist, the software needs to launch fixes against them.
- Also, these repots must be consists with all the applied fixes when carrying out the hardening process so that later the company’s information security team can use for their monthly and yearly general and board meetings
- addition to report generation this software will track the audit progress using follow-up lists.

HardnBot

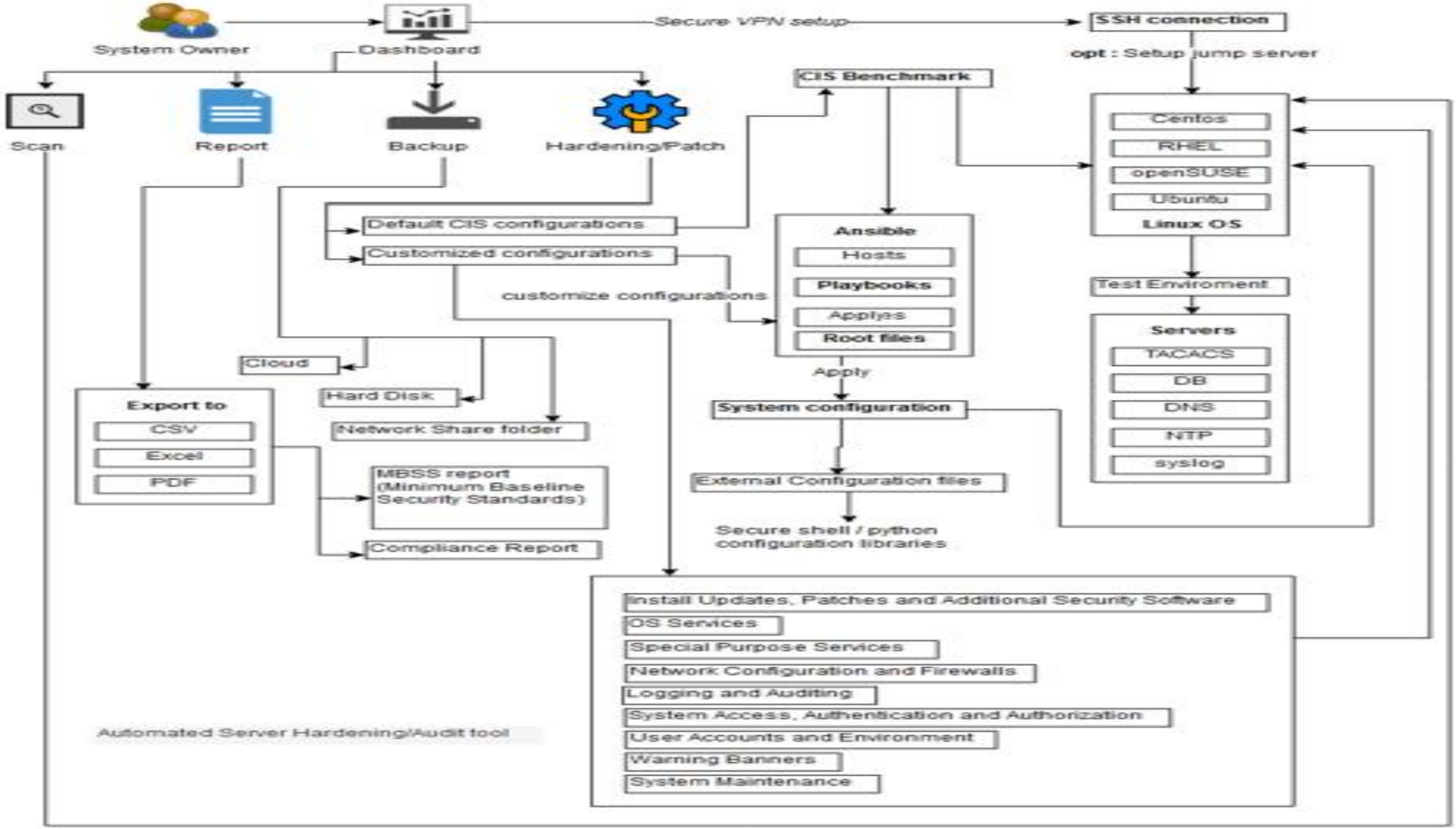
Implementation of scan function using Ansible audits

- Main and basic task of our tool is to scan a unix based server and find any information security related issues, such as poor policy configurations, security banner issues, etc..
- . This task is performed using the operating system vendor’s guidelines (CIS Benchmarks) or configured guidelines according to the company’s information security policy.
- This tool needs to perform an audit scan using ansible audits.
- Also, by applying correction countermeasures by automated hardening process (which is the main task of or tool) the tool also needs to track the performance of these applied fixes (countermeasures) and automatically generate a log file.

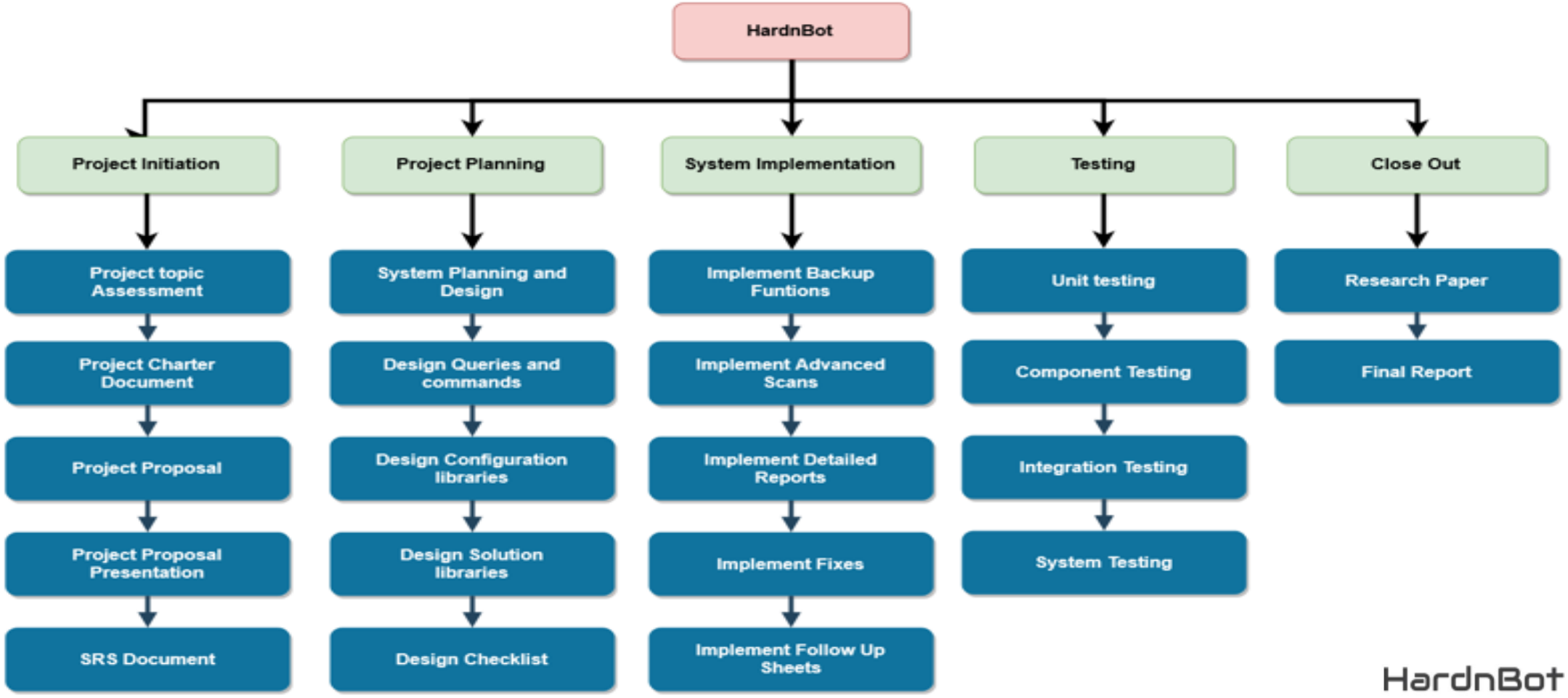
HardnBot

System Diagram

HardnBot

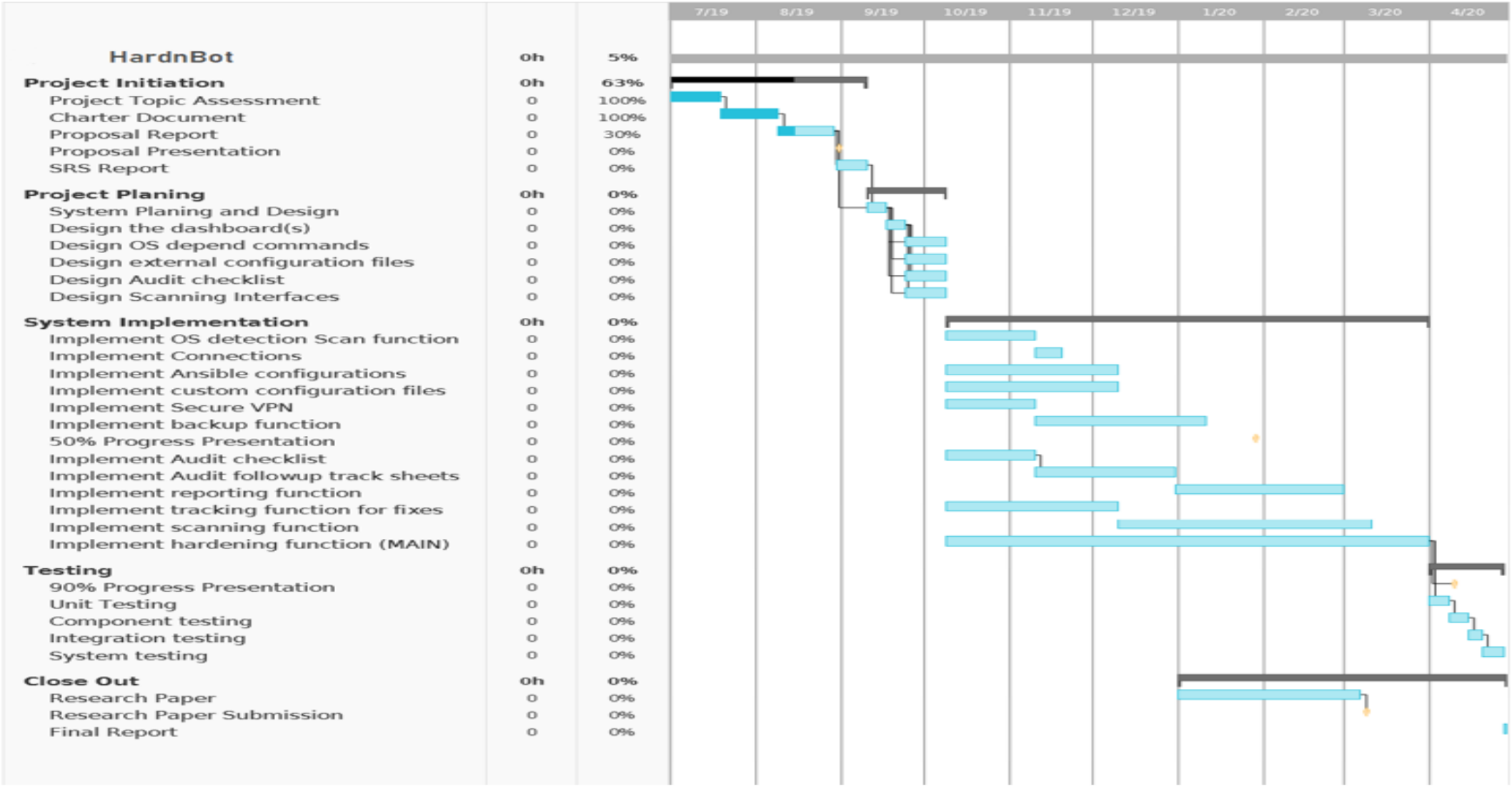

System Owner
Dashboard
Secure VPN setup
SSH connection
opt : Setup jump server
Scan
Report
Backup
Hardening/Patch
CIS Benchmark
Centos
RHEL
openSUSE
Ubuntu
Linux OS
Default CIS configurations
Customized configurations
customize configurations
Ansible
Hosts
Playbooks
Applys
Root files
Test Enviroment
Servers
TACACS
DB
DNS
NTP
syslog
Cloud
Hard Disk
Network Share folder
Apply
System configuration
Export to
CSV
Excel
PDF
MBSS report
(Minimum Baseline
Security Standards)
Compliance Report
External Configuration files
Secure shell / python
configuration libraries
Install Updates, Patches and Additional Security Software
OS Services
Special Purpose Services
Network Configuration and Firewalls
Logging and Auditing
System Access, Authentication and Authorization
User Accounts and Environment
Warning Banners
System Maintenance
Automated Server Hardening/Audit tool

Work Breakdown

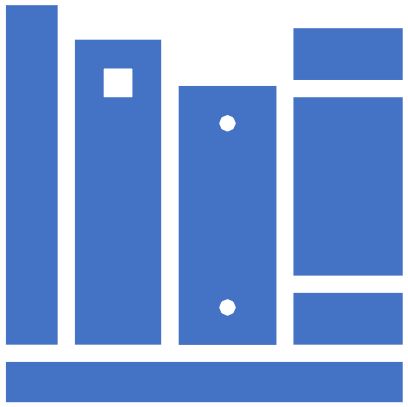


HardnBot

Evaluation Plan



HardnBot	0h	5%
Project Initiation	0h	63%
Project Topic Assessment	0	100%
Charter Document	0	100%
Proposal Report	0	30%
Proposal Presentation	0	0%
SRS Report	0	0%
Project Planing	0h	0%
System Planing and Design	0	0%
Design the dashboard(s)	0	0%
Design OS depend commands	0	0%
Design external configuration files	0	0%
Design Audit checklist	0	0%
Design Scanning Interfaces	0	0%
System Implementation	0h	0%
Implement OS detection Scan function	0	0%
Implement Connections	0	0%
Implement Ansible configurations	0	0%
Implement custom configuration files	0	0%
Implement Secure VPN	0	0%
Implement backup function	0	0%
50% Progress Presentation	0	0%
Implement Audit checklist	0	0%
Implement Audit followup track sheets	0	0%
Implement reporting function	0	0%
Implement tracking function for fixes	0	0%
Implement scanning function	0	0%
Implement hardening function (MAIN)	0	0%
Testing	0h	0%
90% Progress Presentation	0	0%
Unit Testing	0	0%
Component testing	0	0%
Integration testing	0	0%
System testing	0	0%
Close Out	0h	0%
Research Paper	0	0%
Research Paper Submission	0	0%
Final Report	0	0%




Thank You