International Journal of Computer Trends and Technology Volume 68 Issue 2, 1-4, February 2020
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I2P101 © 2020 Seventh Sense Research Group®

Original Article

Host Hardening Review Management System in Enterprise

Ricky Hermawan[1], Nia Rahma Kurnianda[2]

Information System, Department of Computer Science, Mercu Buana University
Jl. Meruya Selatan No.01, Kembangan, West Jakarta, Indonesia

Received Date: 31 December 2019
Revised Date: 30 January 2020
Accepted Date: 09 January 2020

Abstract - *In the Computer Science context, a host is a computer that serves a specific function. It can be a workstation, database server, web server, application server, file server, jump host, and sometimes a combination of two or more functions. Even though each host serves a different function, all of them are installed with fabricated software. This means every service, protocol, and configuration between host A and host B are basically similar. Therefore, we must harden a host by disabling unnecessary services, closing unused ports, and managing the user access control. There are many frameworks available online which can be used as a standard. It's easy to implement because it has guidance, but on an enterprise-scale that has a hundred servers, it'll be tedious work if not managed properly. That's why this paper is intended to share a design of the Host Hardening Review Management System which could be used to manage this kind of work on a bigger scale.*

Keywords - *Host Hardening, Security, Management System, Server Security.*

I. INTRODUCTION

In the current era of technology, a computer is a common thing in an enterprise. It can support the business and give multiple advantages to it. In some cases, computer technology is the backbone of the company itself. That's why each company should secure their main asset; otherwise, it could be damaged the company itself.

In this case, the company already has a host hardening procedure which held biannually for all servers. The problem is there are hundreds of servers in it. Even though the hardening report can be generated by using the script but still the tracking of which server is already compliant and which is not still tracked manually. The data is updated by the Security team every time they get an email from a requestor. This leads to tedious work for them, and sometimes there's a human error.

In this research, we'll look at the problems that arise in the company and design a system to manage those problems. The goal of this research to be achieved in the results is to:

1. Minimizing errors in the host hardening tracking process.
2. To improve the speed of the host hardening review process.
3. To give a more efficient way of tracking and reviewing host hardening status.

II. RESEARCH METHOD

Below is the flow of conducted research:

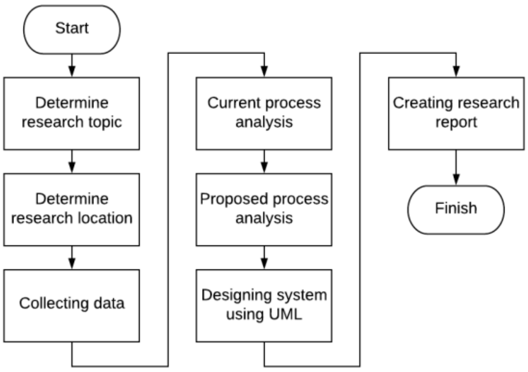


Fig. 1 Research Flow

A. *Data Collection Method*

This research uses data collection method as below:

a) Observation, we had a few days in observing how the Security team reviewed the host hardening report and then updated the status in the tracking table. Also, the process of reviewing deviation if the host can't follow standard configuration. Last is the process of generating a weekly report for a management meeting.

b) Literature, we read through the company documentation, such as a procedure for the host hardening process, procedure for requesting host deviation, and procedure of implementing host hardening.

c) Interview, we held a few discussions with the Security team to get their perspective of the currently running process.

B. *Analysis Method*

This research uses SWOT as its method in analysing current and proposed processes. SWOT analysis is a strategic planning method used to evaluate Strengths(S), Weaknesses(W), Opportunities(O) and Threats(T) in a project or business speculation. And can be applied by analysing and sorting out various things that affect the four factors. Erwin Suryatama (2014: 29) [1].

C. Design Method

This research uses UML for designing the system. UML is a Unified Modelling Language that has many diagrams for the modelling process. The diagram being used in this research are:

- Use Case Diagram
- Activity Diagram
- Sequence Diagram
- Class Diagram

III. STUDY RESULTS

This section will explain two things, which are analysis of business process and design of a proposed system.

A. Analysis of Current Business Process

Figure 2 explains the host harden process at a high level, while Figure 3 explains the low-level process.

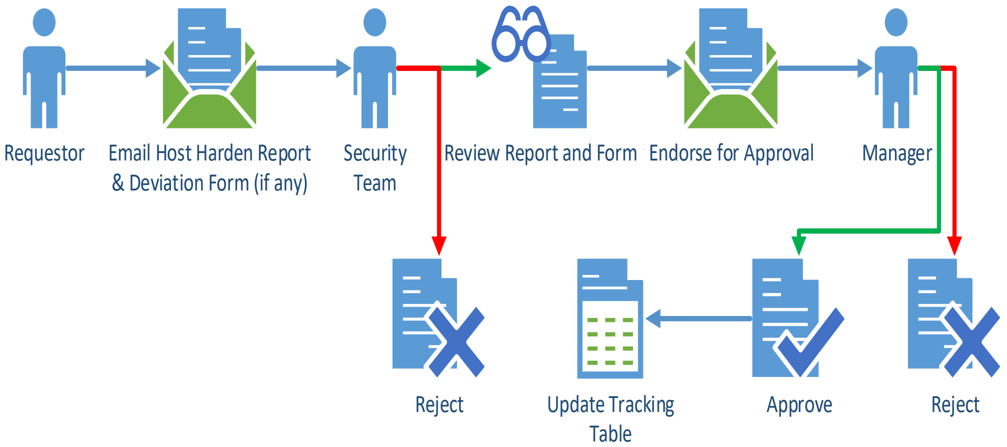


Fig. 2 High-Level Host Harden Process

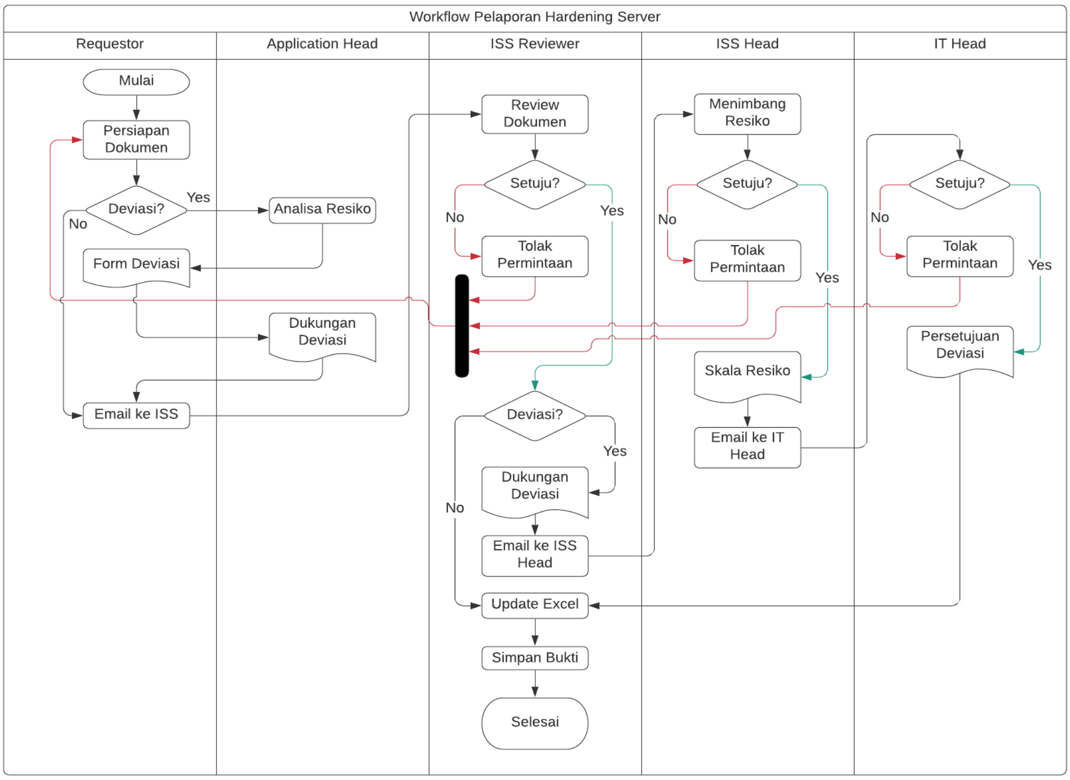


Fig. 3 Low-Level Host Harden Process

The whole process is defined in Figure 3. Start from the requestor preparing all documents needed, such as ISCD report (OS, DB, Web Server), and then if the server requires deviation, then requestor also must submit the deviation forms which already pass the risk assessment from the application manager and get his/her endorsement.

After all, a document is obtained, the requestor must submit it to the ISS reviewer via email, and then the ISS reviewer will decide whether the ISCD report and its supporting document can be considered as Compliant or not. ISS reviewer also needs to check whether the server requires a deviation or not. If yes, then the ISS reviewer also needs to check the deviation form and supporting documents. If the ISS reviewer confirms the justification and supporting documentation is reasonable, then the ISS reviewer will forward the email to ISS Head to approve considering the risk. If ISS Head confirm the risk is acceptable, then ISS Head will forward the email to IT Head for approval. If approval is obtained, then the ISS reviewer must update the server status to “Complete” and keep all email trails and documents in the ISS repository. Sometimes this step got tricky because the ISS reviewer isn’t aware when the deviation got approved, which leads to the status being “Pending” for a long time.

B. SWOT Analysis

Below is the comparison between the current and proposed systems using SWOT analysis.

Table 1. SWOT Analysis

Parameter	Current	Proposed
Strength	Can do backdate review	The dashboard provides real-time data
Weakness	Human error when updating tracking table	Data correction can only be done within DB level
Opportunity	All team are experienced with the current process	The system could be connected to asset data & vulnerability scan later on
Threat	Few teams consider the current process is complicated	Fully dependent on internet availability

C. Design of Proposed System

Below is the design of a proposed system

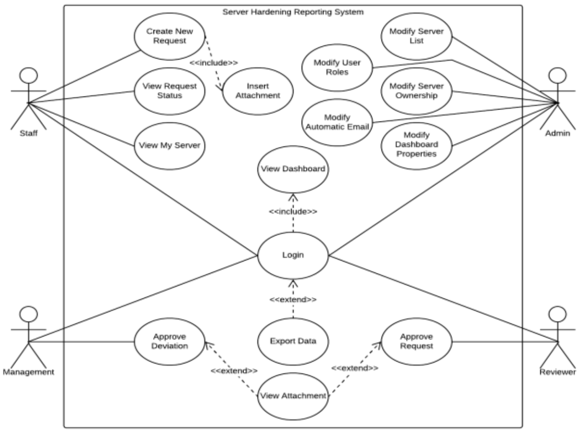


Fig. 4 Use Case Diagram

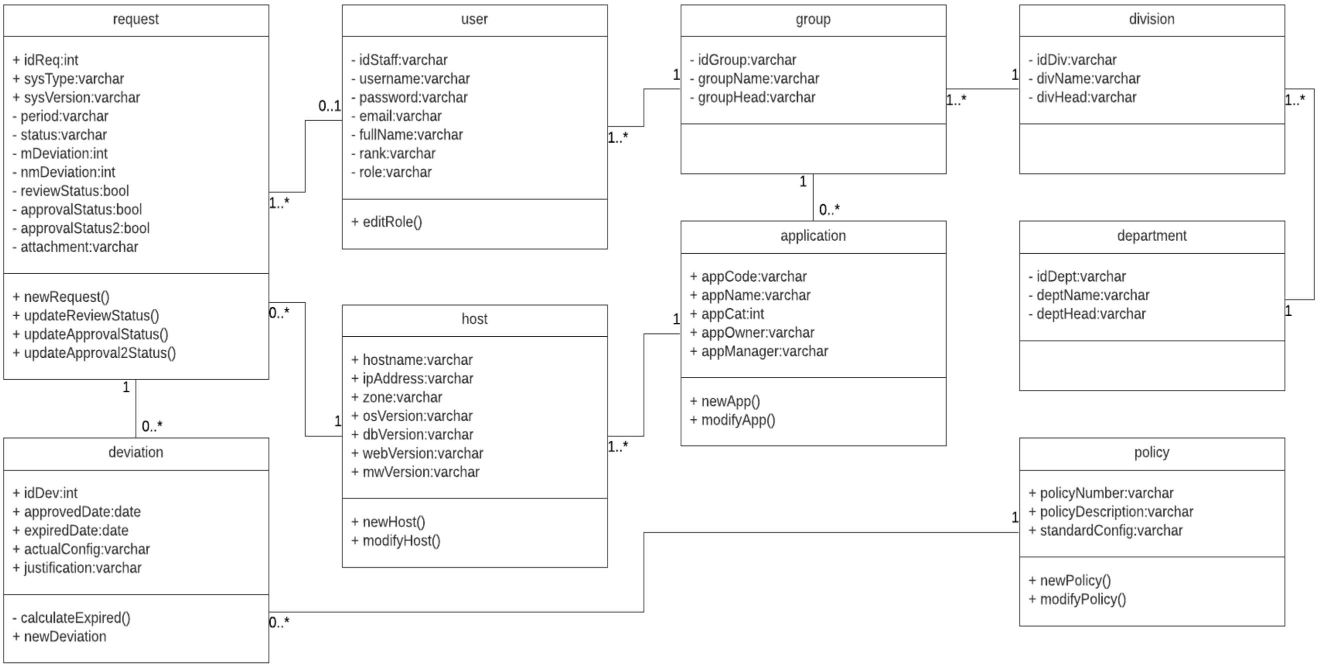


Fig. 5 Class Diagra

Figure 6 is the login page of a system. There’s no forgotten password function because it’s designed to be integrated with the Active Directory server.

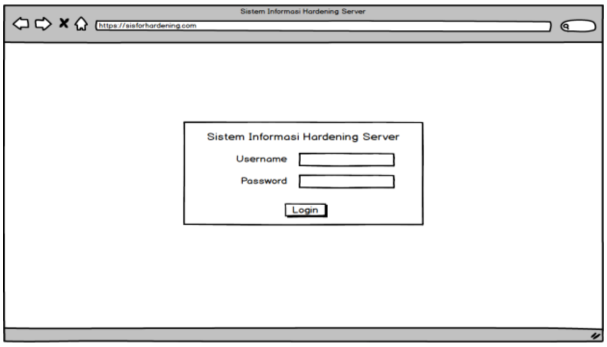

Sistem Informasi Hardening Server
https://sisforhardening.com
Sistem Informasi Hardening Server
Username
Password
Login

Fig. 6 Login Page

Figure 7 is the dashboard that displays the tracking status of hardened host in real-time

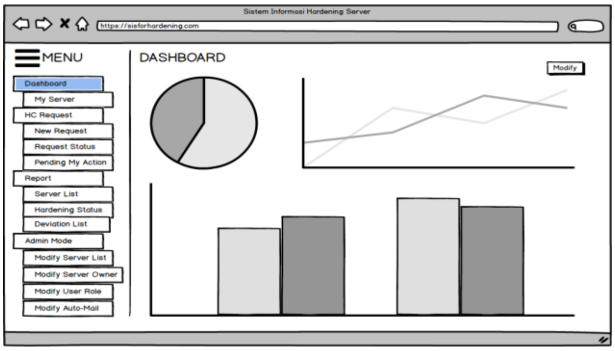
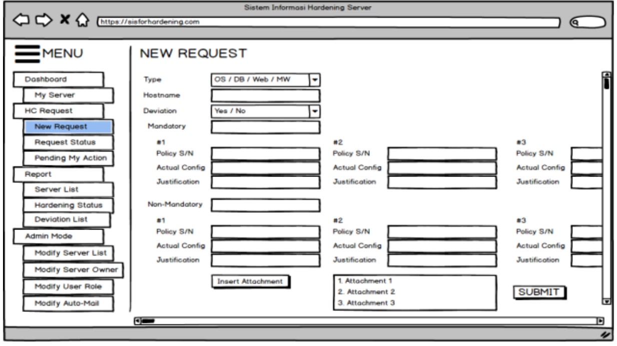


Fig. 7 Dashboard

Figure 8 is a user interface to fill in a form for initiating the review process.



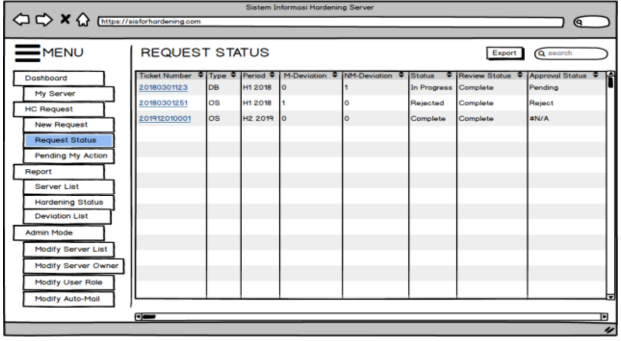
NEW REQUEST

Type: OS / DB / Web / MW
Hostname
Deviation: Yes / No
Mandatory
#1 Policy S/N, Actual Config, Justification
#2 Policy S/N, Actual Config, Justification
#3 Policy S/N, Actual Config, Justification
Non-Mandatory
#1 Policy S/N, Actual Config, Justification
#2 Policy S/N, Actual Config, Justification
#3 Policy S/N, Actual Config, Justification

1. Attachment 1
2. Attachment 2
3. Attachment 3

Fig. 8 Request Form

Figure 9 is menu user can see all their request

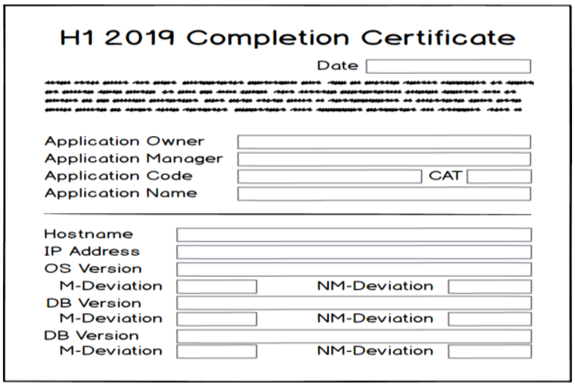


REQUEST STATUS

Ticket Number	Type	Period	M-Deviation	NM-Deviation	Status	Review Status	Approval Status
20180301123	DB	H1 2018	0	1	In Progress	Complete	Pending
20180301251	OS	H1 2018	1	0	Rejected	Complete	Reject
201912010001	OS	H2 2019	0	0	Complete	Complete	#N/A

Fig. 9 All Request

Figure 10 is the certificate user can download after completing the host harden.



H1 2019 Completion Certificate

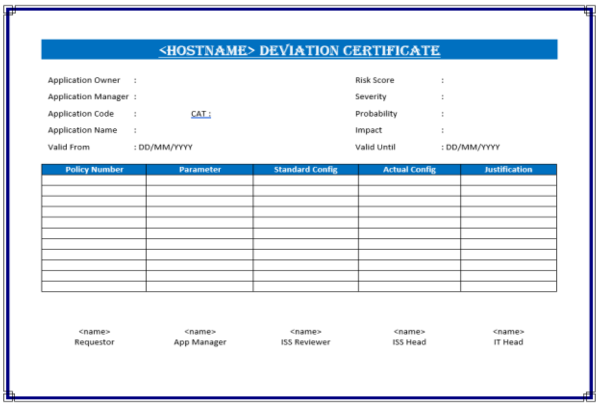
Date

Application Owner
Application Manager
Application Code CAT
Application Name

Hostname
IP Address
OS Version
M-Deviation NM-Deviation
DB Version
M-Deviation NM-Deviation
DB Version
M-Deviation NM-Deviation

Fig. 10 Completion Certificate

Figure 11 is the certificate of approved deviation.



<HOSTNAME> DEVIATION CERTIFICATE

Application Owner : Risk Score :
Application Manager : Severity :
Application Code : CAT : Probability :
Application Name : Impact :
Valid From : DD/MM/YYYY Valid Until : DD/MM/YYYY

Policy Number	Parameter	Standard Config	Actual Config	Justification

<name> Requestor
<name> App Manager
<name> ISS Reviewer
<name> ISS Head
<name> IT Head

Fig. 11 Deviation Approval Certificate

IV.CONCLUSION

An integrated system could minimize human error in inputting data and improve the processing speed by eliminating manual lookup. Besides that, the Security team can be more focused on other duties without the need to generate a weekly report and ad-hoc report. A well-documented process is also good for audit and compliance.

ACKNOWLEDGEMENT

Thank you to Mrs Nia Rahma for helping during the hardest part of this research. Thank you to PT NTT Indonesia for giving a permit for this research in the company. Thank you to Mercu Buana University for giving facility until this research is finished.

REFERENCES

[1] R Majdah Zawawi and Noriah Ramli, Implementation of marketing strategies using the swot method in an effort to increase sales of accident and death insurance services products at pt. Lamongan branch prudential, Legislative Studies, 13(1) (2016) 31–48.

[2] Inge Handriani, Regan Savero, and Arifah Rachmawati, System Business Performance Report about Priority Client In Banking. (2019) 60-65.

[3] Dennis, Allan, Barbara Haley Wixom and David Tegarden. Systems Analysis and Design 5th. Edition, John Wiley & Sons, Inc.(2012).

[4] Rangkuti, Freddy, Dissecting Business Case Techniques SWOT Analysis, How to Calculate Weights, Ratings, and OCAI. Jakarta. Gramedia Main Library. (2014).