

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINILITAS	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xv
DAFTAR ISTILAH	xvi
DAFTAR SINGKATAN	xviii
DAFTAR LAMPIRAN.....	xix
Bab I PENDAHULUAN.....	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah.....	3
I.3 Tujuan Penelitian.....	4
I.4 Batasan Penelitian	4
I.5 Manfaat Penelitian.....	4
Bab II TINJAUAN PUSTAKA.....	5
II.1 <i>Security Hardening</i>	5
II.2 Keamanan Data	5
II.3 <i>Virtual Private Server</i>	6
II.4 NIST SP 800-123	6
II.5 <i>CIS Critical Security Controls</i>	7

II.6	Alasan Pemilihan standar	8
II.7	Kerentanan Sistem Operasi	8
II.7.1	<i>Brute Force</i>	9
II.7.2	<i>Ransomware</i>	9
II.7.3	<i>Worm</i>	9
II.7.4	<i>Virus</i>	9
II.7.5	<i>Man-in-the-middle Attack</i>	10
II.8	Penelitian Terdahulu.....	11
Bab III	METODOLOGI PENELITIAN	13
III.1	Model Konseptual	13
III.2	Sistematika Penelitian	13
III.2.1	Tahap <i>Access</i>	15
III.2.2	Tahap <i>Analyze</i>	15
III.2.3	Tahap <i>Remediate</i>	15
III.3	Pengumpulan Data	15
III.4	Pengolahan data.....	17
III.5	Metode Evaluasi	17
III.6	Alasan Pemilihan Metode.....	17
Bab IV	ANALISIS SISTEM EKSISTING	18
IV.1	Identifikasi Sistem	18
IV.1.1	<i>Hardware</i>	18
IV.1.2	<i>Server</i>	19
IV.2	Topologi Jaringan.....	19
IV.3	Analisis Kondisi Eksisting	20
IV.3.1	Kondisi Eksisting <i>Patch and Upgrade Operating System</i>	21
IV.3.2	Kondisi Eksisting <i>Hardening and Securely Configuring the OS.</i> ..	23

IV.3.3	Kondisi Eksisting <i>Install and Configure Additional Security Controls</i>	32
IV.3.4	Kondisi Eksisting <i>Security Testing The Operating System</i>	34
Bab V	PENGUJIAN SISTEM DAN REKOMENDASI	36
V.1	<i>Patch and Upgrade Operating System</i>	36
V.1.1	<i>Create, Document, and Implement a Patching Process</i>	36
V.1.2	<i>Identify Vulnerabilities and Applicable Patches</i>	39
V.1.3	<i>Mitigate Vulnerabilities Temporarily</i>	41
V.1.4	<i>Install Permanent Fixes</i>	43
V.2	<i>Hardening and Securely Configuring the OS</i>	45
V.2.1	<i>Remove or Disable Unnecessary Services, Applications, and Network Protocols</i>	45
V.2.1.1	<i>Remote Control and Remote Access Programs</i>	46
V.2.1.2	<i>Web Servers and Services</i>	46
V.2.1.3	<i>Language Compilers and System Development Tools</i>	47
V.2.2	<i>Configure OS User Authentication</i>	48
V.2.2.1	<i>Remove or Disable Unneeded Default Accounts</i>	48
V.2.2.2	<i>Disable Non-Interactive Accounts</i>	49
V.2.2.3	<i>Create the User Groups</i>	49
V.2.2.4	<i>Create the User Accounts</i>	50
V.2.2.5	<i>Check the Organization's Password Policy</i>	51
V.2.2.6	<i>Configure Computers to Prevent Password Guessing</i>	51
V.2.2.7	<i>Install and Configure Other Security Mechanisms</i>	54
V.2.3	<i>Configure Resource Controls Appropriately</i>	58
V.3	<i>Install and Configure Additional Security Controls</i>	60
V.3.1	<i>Anti-malware Software</i>	60

V.3.2	<i>Patch Management or Vulnerability Management Software</i>	62
V.4	<i>Security Testing the Operating System</i>	63
V.4.1	<i>The Possible Impact to The Production Server</i>	63
Bab VI	KESIMPULAN DAN SARAN	69
VI.1	Kesimpulan.....	69
VI.2	Saran.....	70
	DAFTAR PUSTAKA	71
	LAMPIRAN.....	77