AUDIT DAN IMPLEMENTASI CIS BENCHMARK PADA SISTEM OPERASI LINUX DEBIAN SERVER (STUDI KASUS: SERVER LABORATORIUM JARINGAN DAN KOMPUTER 6, INSTITUT SAINS & TEKNOLOGI AKPRIND YOGYAKARTA)

Dika Priska Prastika[1], Joko Triyono[2], Uning Lestari[3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains & Teknologi AKPRIND Yogyakarta
Email : [1]dikapriska@gmail.com, [2]zainjack@akprind.ac.id, [3] uning@akprind.ac.id

ABSTRACT

The Center for Internet Security (CIS) *is a nonprofit organization established in October* 2000*. The mission of this organization is to identify, develop, validate, and market best practices in the cyber world. From some* CIS *work programs, there are two most important (and free) are* CIS *Control and* CIS *Benchmark.*

Vocational High School (SMK) *Program Computer and Network Engineering* (TKJ) *is required to find the existing in the world of work and industry. Although there is one subject that is in the* 2013 *curriculum about using the Debian Linux operating system as a server, but not about the security configuration of the Debian Linux operating system.*

To improve the Linux Debian Server operating system and also to know or score about these ways to the server of Network and Computer Laboratory 6*, Institute of Sains & Technology* AKPRIND *Yogyakarta. After the audit the server gets scored* 129 *or* 70*% out of a total of* 185 *scored.*

Keywords*: Center For Internet Security, audit, CIS Benchmark, Linux Debian, Operating system.*

INTISARI

Center For Internet Security (CIS) adalah organisasi non profit yang didirikan pada bulan Oktober tahun 2000. Misi dari organisasi ini adalah mengidentifikasi, mengembangkan, memvalidasi, dan mempromosikan praktik terbaik pertahanan di dunia siber. Dari beberapa program kerja CIS, ada dua yang paling penting (dan gratis) adalah CIS *Control* dan CIS *Benchmark*.

Sekolah Menengah Kejuruan (SMK) program keahlian Teknik Komputer dan Jaringan (TKJ) dituntut untuk memenuhi kompetensi yang ada di dunia kerja dan dunia industri. Meskipun terdapat satu mata pelajaran yang ada di kurikulum 2013 tentang penggunaan sistem operasi Linux Debian sebagai *server*, tetapi tidak mencakup tentang konfigurasi keamanan pada sistem operasi Linux Debian.

Untuk meningkatkan keamanan sistem dilakukan dengan mengimplementasikan CIS *Benchmark* pada sistem operasi Linux Debian Server serta dapat mengetahui penilaian atau *score* tentang metode tersebut terhadap *server* Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta. Setelah dilakukan audit *server* tersebut mendapatkan *scored* 129 atau 70% dari total 185 *scored*.

Kata kunci: *Center For Internet Security*, audit, CIS *Benchmark*, Linux Debian, Sistem Operasi.

PENDAHULUAN

Center For Internet Security (CIS) adalah organisasi non profit yang didirikan pada bulan Oktober tahun 2000. Misi dari organisasi ini adalah mengidentifikasi, mengembangkan, memvalidasi, dan mempromosikan praktik terbaik pertahanan di dunia siber. Dari beberapa program kerja CIS, ada dua yang paling penting (dan gratis) adalah CIS *Control* dan CIS *Benchmark*. CIS *Control* tidak dibuat untuk menggantikan kerangka kerja (*framework*) yang ada di dunia keamanan *cyber* seperti NIST, ISO 27001/27002, PCI DSS, dll. Akan tetapi digunakan sebagai alternatif panduan untuk melakukan praktik

pertahanan terbaik di dunia siber pada tataran organisasi (Center for Internet Security, 2017). Ada 20 langkah dalam CIS *Control* yang sangat mudah dilakukan, bahkan oleh pemula.

Sekolah Menengah Kejuruan (SMK) program keahlian Teknik Komputer dan Jaringan (TKJ) dituntut untuk memenuhi kompetensi yang ada di dunia kerja dan dunia industri (SK Kemendikbud nomor 330/D.D5/KEP/KR/2017). Meskipun terdapat satu mata pelajaran yang ada di kurikulum 2013 tentang penggunaan sistem operasi Linux Debian sebagai *server*, tetapi tidak mencakup tentang konfigurasi keamanan pada sistem operasi Linux Debian (Ditjen GTK, 2016). Berdasarkan hal tersebut maka penelitian ini membahas bagaimana mengimplementasikan dan hasil audit yang digunakan untuk mengamankan *server* dari kerentanan pada sistem operasi Linux Debian *Server* dengan menerapkan standar *hardening* dari CIS *Benchmark* untuk menjamin keamanan sistem dari ancaman serangan siber.

Tujuan dari penelitian ini adalah mengetahui hasil penilaian atau *score* dari *CIS Bechmark* pada sistem operasi Linux Debian *Server* dan meningkatkan keamanan pada bagian sistem operasi Linux Debian *Server* 8 dengan *CIS Benchmark*.

TINJAUAN PUSTAKA

Penelitian ini menggunakan beberapa literatur yang pernah dilakukan oleh peneliti sebelumnya. Referensi pertama adalah penelitian yang dilakukan oleh (Rahman, 2015) menjelaskan bahwa audit *server* adalah tugas penting untuk memastikan keamanan tingkat platform di infrastruktur TI dan memastikan konfigurasi *server* Linux yang tepat. Alat penilaian konfigurasi berbasis host yang membandingkan konfigurasi sistem dengan pengaturan konfigurasi aman yang direkomendasikan dalam Tolok Ukur CIS yang memanfaatkan sistem operasi Linux (Red Hat) dan *Center for Internet Security Configuration Assessment Tool* (CIS-CAT).

Referensi kedua adalah penelitian yang dilakukan oleh (Jogi, 2017) menjelaskan bahwa peraturan membuat tantangan bagi perusahaan karena mereka harus memenuhi standar keamanan yang ketat untuk kepatuhan keamanan setiap tahun. Audit standar keamanan sistem operasi secara otomatis yang memungkinkan untuk memvalidasi kesenjangan antara konfigurasi standar dan aktual pada mesin virtual menggunakan metode *Proof-of-concept*. Dan terfokus pada pengembangan *hardened virtual machine image* untuk platform *Microsoft Azure* yang sesuai dengan standar *hardening* yang ditetapkan.

Referensi ketiga adalah penelitian yang dilakukan oleh (Nuckols, dkk., 2015) menerapkan konfigurasi standar (*baseline*) dengan sistem operasi Linux (Red Hat). Penelitian ini bertujuan untuk mengamankan sistem operasi Linux (Red Hat) dengan benar, menghasilkan jaringan yang aman dan mengurangi kerentanan dengan memastikan sistem operasi Linux (Red Hat) yang terhubung ke jaringan diperbarui dan diamankan dengan benar sehingga menjadi informasi yang berharga dan bermanfaat bagi *Department of Veterans Affairs*.

Referensi keempat adalah penelitian yang dilakukan oleh (Nepal, 2013) menjelaskan bahwa banyak administrator sistem tidak menyadari kenyataan bahwa, *default* installasi Linux rentan terhadap berbagai serangan. Praktik keamanan dan praktik terbaik untuk mengamankan *server* Linux serta beberapa layanan aplikasi terpopuler yang biasa dijalankan di *server* Linux. Tujuan dari makalah ini adalah untuk mengeksplorasi dan menyoroti konfigurasi keamanan yang harus dilakukan dari standar *hardening* installasi sistem operasi Linux (CentOS), sehingga tidak menjadi sasaran serangan yang mudah.

PEMBAHASAN

Hasil audit dan implementasi CIS *Benchmark* Linux Debian yang dilakukan pada *server* Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta, dapat dilihat pada Tabel 1.

Tabel 1. Hasil CIS *Benchmark*

No.	Control	Scoring	
		Yes	No
1.	***Patching and Software Updates* (*Not Score*)**		v
2	***Filesystem Configuration***		
2.1	Membuat partisi terpisah untuk /*tmp* (*Scored*)	v	
2.2	Tetapkan opsi *nodev* untuk partisi /*tmp* (*Scored*)	v	
2.3	Tetapkan opsi *nosuid* untuk partisi /*tmp* (*Scored*)	v	
2.4	Tetapkan opsi *noexec* untuk partisi /*tmp* (*Scored*)	v	
2.5	Membuat partisi terpisah untuk /*var* (*Scored*)		v
2.6	Bind mount folder /*var*/*tmp* ke /*tmp* (*Scored*)	v	
2.7	Membuat partisi terpisah untuk /*var*/*log* (*Scored*)		v
2.8	Membuat partisi terpisah untuk /*var*/*log*/*audit* (*Scored*)		v
2.9	Membuat partisi terpisah untuk /*home* (*Scored*)	v	
2.10	Tambahkan opsi *nodev* ke partisi /*home* (*Scored*)	v	
2.11	Tambahkan opsi *nodev* ke partisi *Removable Media* (*Not Scored*)		v
2.12	Tambahkan opsi *noexec* ke partisi *Removable Media* (*Not Scored*)		v
2.13	Tambahkan opsi *nosuid* ke partisi *Removable Media* (*Not Scored*)		v
2.14	Tambahkan opsi *nodev* ke partisi /*run*/*shm* (*Scored*)	v	
2.15	Tambahkan opsi *nosuid* ke partisi /*run*/*shm* (*Scored*)	v	
2.16	Tambahkan opsi *noexec* ke partisi /*run*/*shm* (*Scored*)	v	
2.17	Mengatur *Sticky Bit* ke semua folder *Writable* (*Scored*)	v	
2.18	Nonaktifkan *Mounting of cramfs filesystems* (*Not Scored*)		v
2.19	Nonaktifkan *Mounting of freevxfs filesystems* (*Not Scored*)		v
2.20	Nonaktifkan *Mounting of jffs2 filesystems* (*Not Scored*)		v
2.21	Nonaktifkan *Mounting of hfs filesystems* (*Not Scored*)		v
2.22	Nonaktifkan *Mounting of hfsplus filesystems* (*Not Scored*)		v
2.23	Nonaktifkan *Mounting of squashfs filesystems* (*Not Scored*)		v
2.24	Nonaktifkan *Mounting of udf filesystems* (*Not Scored*)		v
2.25	Nonaktifkan *Automounting* (*Scored*)	v	
3	**Secure Boot Settings**		
3.1	Mengatur pemilik *User*/*Group* pada konfigurasi *bootloader* (*Scored*)	v	

3.2	Mengatur *Permissions* pada konfigurasi *bootloader* (*Scored*)	v	
3.3	Mengatur *password bootloader* (*Scored*)		v
3.4	Memerlukan otentikasi untuk mode *single-user* (*Scored*)	v	
4	***Additional Process Hardening***		
4.1	Membatasi *Core Dumps* (*Scored*)	v	
4.2	Mengaktifkan XD/NX *support on* 32-*bit* x86 *systems* (*Not Scored*)		v
4.3	Mengaktifkan *randomized virtual memory* region *placement* (*Scored*)	v	
4.4	Nonaktifkan *Prelink* (*Scored*)	v	
4.5	Mengaktifkan *AppArmor* (*Scored*)		v
5	***OS Services***		
5.1	**Memastikan Layanan Legacy Tidak Diaktifkan**		
5.1.1	*Network Information Service* (NIS) (*Scored*)	v	
5.1.2	*Remote Shell Server* (RSH *Server*) (*Scored*)	v	
5.1.3	*Remote Shell Client (RSH Client) (Scored)*	v	
5.1.4	*Talk Server (Scored)*	v	
5.1.5	*Talk Client (Scored)*	v	
5.1.6	*Telnet Server (Scored)*	v	
5.1.7	*Trivial File Transfer Protokol* (TFTP) (*Scored*)	v	
5.1.8	*Extended InterNet Daemon* (Xinetd) (*Scored*)		v
5.2	Memastikan *chargen* tidak diaktifkan (*Scored*)	v	
5.3	Memastikan *daytime* tidak diaktifkan (*Scored*)	v	
5.4	Memastikan *echo* tidak diaktifkan (*Scored*)	v	
5.5	Memastikan *discard* tidak diaktifkan (*Scored*)	v	
5.6	Memastikan *time* tidak diaktifkan (*Scored*)	v	
6	***Special Purpose Services***		
6.1	Memastikan sistem X *Window* tidak terpasang (*Scored*)	v	
6.2	Memastikan Avahi *Server* tidak diaktifkan (*Scored*)	v	
6.3	Memastikan Print *Server* tidak diaktifkan (*Not Scored*)		v
6.4	Memastikan DHCP *Server* tidak diaktifkan (*Scored*)	v	
6.5	Mengkonfigurasi *Network Time Protocol* (NTP) (*Scored*)	v	
6.6	Memastikan LDAP tidak diaktifkan (*Not Scored*)	v	
6.7	Memastikan NFS dan RPC tidak diaktifkan (*Not Scored*)		v
6.8	Memastikan DNS *Server* tidak diaktifkan (*Not Scored*)		v
6.9	Memastikan FTP *Server* tidak diaktifkan (*Not Scored*)		v
6.10	Memastikan HTTP *Server* tidak diaktifkan (*Not Scored*)		v
6.11	Memastikan IMAP dan POP *Server* tidak diaktifkan (*Not Scored*)		v

6.12	Memastikan Samba tidak diaktifkan (*Not Scored*)		v
6.13	Memastikan HTTP *Proxy Server* tidak diaktifkan (*Not Scored*)		v
6.14	Memastikan SNMP *Server* tidak diaktifkan (*Not Scored*)		v
6.15	Mengkonfigurasi *Mail Transfer Agent* untuk mode *local* (*Scored*)	v	
6.16	Memastikan layanan *rsync* tidak diaktifkan (*Scored*)	v	
7	***Network Configuration and Firewalls***		
7.1	**Memodifikasi Parameter Jaringan (*Host Only*)**		
7.1.1	Menonaktifkan IP *Forwarding* (*Scored*)	v	
7.1.2	Menonaktifkan *Send Packet Redirects* (*Scored*)	v	
7.2	**Memodifikasi Parameter Jaringan (*Host* dan *Router*)**		
7.2.1	Menonaktifkan *Source Routed Packet Acceptance* (*Scored*)		v
7.2.2	Menonaktifkan ICMP *Redirect Acceptance* (*Scored*)		v
7.2.3	Menonaktifkan *Secure* ICMP *Redirect Acceptance* (*Scored*)		v
7.2.4	Log *Suspicious Packets* (*Scored*)		v
7.2.5	Mengaktifkan penolak permintaan *Broadcast* (*Scored*)		v
7.2.6	Mengaktifkan *Bad Error Message Protection* (*Scored*)		v
7.2.7	Mengaktifkan RFC-*recommended Source Route Validation* (*Scored*)		v
7.2.8	Mengaktifkan TCP SYN *Cookies* (*Scored*)		v
7.3	**Konfigurasi IPv6**		
7.3.1	Menonaktifkan IPv6 *Router Advertisements* (*Not Scored*)		v
7.3.2	Menonaktifkan IPv6 *Redirect Acceptance* (*Not Scored*)		v
7.3.3	Menonaktifkan IPv6 (*Not Scored*)		v
7.4	**Install TCP *Wrappers***		
7.4.1	Install TCP Wrappers (*Scored*)	v	
7.4.2	Membuat /*etc*/*hosts.allow* (*Not Scored*)		v
7.4.3	Memverifikasi *Permissions* /*etc*/*hosts.allow* (*Scored*)	v	
7.4.4	Membuat /*etc*/*hosts.deny* (*Not Scored*)		v
7.4.5	Memverifikasi *Permissions* /*etc*/*hosts.deny* (*Scored*)	v	
7.5	***Uncommon Network Protocols***		
7.5.1	Menonaktifkan DCCP (*Not Scored*)		v
7.5.2	Menonaktifkan SCTP (*Not Scored*)		v
7.5.3	Menonaktifkan RDS (*Not Scored*)		v
7.5.4	Menonaktifkan TIPC (*Not Scored*)		v
7.6	Menonaktifkan *Interface Wireless* (*Not Scored*)		v
7.7	Memastikan *Firewall* aktif (*Scored*)	v	
8	***Logging and Auditing***		

8.1	**Konfigurasi Sistem *Accounting* (auditd)**		
8.1.1	***Configure Data Retention***		
8.1.1.1	Mengkonfigurasi ukuran penyimpanan log Audit (*Not Scored*)		v
8.1.1.2	Menonaktifkan sistem saat log Audit penuh (*Not Scored*)		v
8.1.1.3	Menyimpan informasi Audit (*Scored*)	v	
8.1.2	Install dan mangaktifkan layanan auditd (*Scored*)	v	
8.1.3	Mengaktifkan Auditing saat sistem dinyalakan (*Scored*)	v	
8.1.4	Mencatat peristiwa perubahan dengan informasi tanggal dan waktu (*Scored*)	v	
8.1.5	Mencatat peristiwa perubahan dengan informasi *User*/*Group* (*Scored*)	v	
8.1.6	Mencatat peristiwa perubahan *System Network Environment* (*Scored*)	v	
8.1.7	Mencatat peristiwa perubahan *System Mandatory Access Controls* (*Scored*)	v	
8.1.8	Mengumpulkan aktivitas *Login* dan *Logout* (*Scored*)	v	
8.1.9	Mengumpulkan aktivitas *Session Initiation* (*Scored*)	v	
8.1.10	Mengumpulkan perubahan *Discretionary Access Control Permission* (*Scored*)	v	
8.1.11	Mengumpulkan *Unsuccessful Unauthorized Access Attempts* (*Scored*)	v	
8.1.12	Mengumpulkan penggunaan perintah *Privileged* (*Scored*)	v	
8.1.13	Mengumpulkan *Mounts Filesystem* yang berhasil (*Scored*)	v	
8.1.14	Mengumpulkan peristiwa menghapus file oleh pengguna (*Scored*)	v	
8.1.15	Mengumpulkan perubahan pada lingkup administrasi sistem (*sudoers*) (*Scored*)	v	
8.1.16	Mengumpulkan tindakan administrator sistem (*sudolog*) (*Scored*)	v	
8.1.17	Mengumpulkan *Kernel Module Loading* dan *Unloading* (*Scored*)	v	
8.1.18	Membuat konfigurasi audit *Immutable* (*Scored*)	v	
8.2	**Konfigurasi *rsyslog***		
8.2.1	Memasang paket *rsyslog* (*Scored*)	v	
8.2.2	Memastikan layanan *rsyslog* aktif (*Scored*)	v	
8.2.3	Mengkonfigurasi /*etc*/*rsyslog.conf* (*Not Scored*)		v
8.2.4	Membuat dan mengatur *permissions* pada *file log rsyslog* (*Scored*)	v	
8.2.5	Mengkonfigurasi *rsyslog* untuk mengirim log ke *Remote* log *Host* (*Scored*)	v	
8.2.6	Menerima pesan *remote rsyslog* hanya di *Host* log yang dipilih (*Not Scored*)		v
8.3	***Advanced Intrusion Detection Environment* (AIDE)**		

8.3.1	Install AIDE (*Scored*)	v	
8.3.2	Memeriksa *File* secara berkala (*Scored*)	v	
8.4	Mengkonfigurasi *logrotate* (*Not Scored*)		v
9	***System Access, Authentication and Authorization***		
9.1	**Mengkonfigurasi cron**		
9.1.1	Mengaktifkan daemon cron (*Scored*)	v	
9.1.2	Mengatur *permission user* dan *group* di /*etc*/*crontab* (*Scored*)	v	
9.1.3	Mengatur *permission user* dan *group* di /*etc*/*cron.hourly* (*Scored*)	v	
9.1.4	Mengatur *permission user* dan *group* di /*etc*/*cron.daily* (*Scored*)	v	
9.1.5	Mengatur *permission user* dan *group* di /*etc*/*cron.weekly* (*Scored*)	v	
9.1.6	Mengatur *permission user* dan *group* di /*etc*/*cron.monthly* (*Scored*)	v	
9.1.7	Mengatur *permission user* dan *group* di /*etc*/*cron*.d (*Scored*)	v	
9.1.8	Membatasi akses at dan cron ke *Authorized Users* (*Scored*)	v	
9.2	**Mengkonfigurasi PAM**		
9.2.1	Menentapkan parameter syarat membuat *password* dengan *pam_cracklib* (*Scored*)	v	
9.2.2	Mengatur *Lockout* jika gagal memasukkan *password* (*Not Scored*)		v
9.2.3	Membatasi *password reuse* (*Scored*)	v	
9.3	**Mengkonfigurasi SSH**		
9.3.1	Mengatur protokol SSH ke 2 (*Scored*)	v	
9.3.2	Mengatur *LogLevel* ke INFO (*Scored*)	v	
9.3.3	Mengatur *permission* di /*etc*/*ssh*/*sshd_config* (*Scored*)	v	
9.3.4	Menonaktifkan SSH X11 *Forwarding* (*Scored*)	v	
9.3.5	Mengatur SSH *MaxAuthTries* ke 4 (*Scored*)	v	
9.3.6	Mengatur SSH *IgnoreRhosts* ke *Yes* (*Scored*)	v	
9.3.7	Mengatur SSH *HostbasedAuthentication* ke *No* (*Scored*)	v	
9.3.8	Menonaktifkan SSH *Root Login* (*Scored*)	v	
9.3.9	Mengatur SSH *PermitEmptyPasswords* ke No (*Scored*)	v	
9.3.10	Melarang User mengatur pilihan *environment* (*Scored*)	v	
9.3.11	Menggunakan *Cipher* yang disetujui dalam mode *Counter* (*Scored*)	v	
9.3.12	Mengatur interval *idle timeout* untuk *user Login* (*Scored*)	v	
9.3.13	Membatasi akses melalui SSH (*Scored*)	v	
9.3.14	Mengatur *banner* SSH (*Scored*)	v	
9.4	Membatasi *login* root untuk sistem *console* (*Not Scored*)		v
9.5	Membatasi akses ke perintah *superuser* (*Scored*)	v	
10	***User Accounts and Environment***		

10.1	**Mengatur Parameter *Shadow Password Suite* (*/etc/login.defs*)**		
10.1.1	Mengatur *password expiration days* (*Scored*)	v	
10.1.2	Mengatur waktu minimal *password* dapat diubah kembali (*Scored*)	v	
10.1.3	Mengatur peringatan *password* akan kedaluwarsa (*Scored*)	v	
10.2	Menonaktifkan akun sistem (*Scored*)	v	
10.3	Mengatur *group default* untuk akun root (*Scored*)	v	
10.4	Mengatur *umask default* untuk pengguna (*Scored*)	v	
10.5	Kunci akun pengguna ang tidak aktif (*Scored*)	v	
11	**Warning Banners**		
11.1	Mengatur *warning banner* layanan *Login* (*Scored*)	v	
11.2	Menghapus informasi OS dari *Login warning banners* (*Scored*)	v	
11.3	Mengatur grafik *warning banner* (*Not Scored*)		v
12	**Verify System File Permissions**		
12.1	Memverifikasi *permissions* pada /*etc*/*passwd* (*Scored*)	v	
12.2	Memverifikasi *permissions* pada /*etc*/*shadow* (*Scored*)	v	
12.3	Memverifikasi *permissions* pada /*etc*/*group* (*Scored*)	v	
12.4	Memverifikasi kepemilikan *user*/*group* pada /*etc*/*passwd* (*Scored*)	v	
12.5	Memverifikasi kepemilikan *user*/*group* pada /*etc*/*shadow* (*Scored*)	v	
12.6	Memverifikasi kepemilikan *user*/*group* pada /*etc*/*group* (*Scored*)	v	
12.7	Mencari *world writable* files (*Not Scored*)		v
12.8	Mencari *file* dan directori yang tidak memiliki pemilik (*Scored*)	v	
12.9	Mencari *file* dan directori yang tidak memiliki *group* (*Scored*)	v	
12.10	Mencari SUID *system executables* (*Not Scored*)		v
12.11	Mencari SGID *system executables* (*Not Scored*)		v
13	**Review User and Group Settings**		
13.1	Memastikan *password* tidak kosong (*Scored*)	v	
13.2	Memverifikasi tidak ada *legacy* "+" *entries* ada di *file* /*etc*/*passwd* (*Scored*)	v	
13.3	Memverifikasi tidak ada *legacy* "+" *entries* ada di *file* /*etc*/*shadow* (*Scored*)	v	
13.4	Memverifikasi tidak ada *legacy* "+" *entries* ada di *file* /*etc*/*group* (*Scored*)	v	
13.5	Memverifikasi tidak ada akun UID 0 yang tersedia selain root (*Scored*)	v	
13.6	Memastikan integritas PATH root (*Scored*)	v	
13.7	Memastikan *permissions* pada direktori *home* penggunaa (*Scored*)	v	
13.8	Memastikan *permissions* fil e *dot* pengguna (*Scored*)	v	

13.9	Memastikan *permissions* file *.netrc* pengguna (*Scored*)	v	
13.10	Memastikan keberadaan file *.rhosts* pengguna (*Scored*)	v	
13.11	Memastikan *Group* di /*etc*/*passwd* (*Scored*)	v	
13.12	Memastikan pengguna ditetapkan di direktori *home* yang sesuai (*Scored*)	v	
13.13	Memastikan kepemilikan direktori *home* pengguna (*Scored*)	v	
13.14	Memastikan UID yang duplikat (*Scored*)	v	
13.15	Memastikan GID yang duplikat (*Scored*)	v	
13.16	Memastikan nama *user* yang duplikat (*Scored*)	v	
13.17	Memastikan nama *group* yang duplikat (*Scored*)	v	
13.18	Memastikan keberadaan file *.netrc* pengguna (*Scored*)	v	
13.19	Memastikan keberadaan file *.forward* pengguna (*Scored*)	v	
13.20	Memastikan *group shadow* kosong (*Scored*)	v	
JUMLAH		**129**	**56**

Dari Tabel 1 yang meliputi 13 pokok dengan 185 tahap audit dan implementasi CIS *Benchmark*, maka dapat disimpulkan sebagai berikut:

1. *Patching* dan *Software Updates*

   Hasil yang didapat dari *patch* dan *software updates* yaitu *not scored*, hal ini dikarenakan tidak adanya jaringan internet yang menghubungkan ke *server* tersebut. Sehingga, proses audit dari *patch* dan *software updates* tidak dapat dilakukan, padahal ada beberapa *software* yang masih menggunakan versi yang sudah kedaluwarsa.
2. *Filesystem Configuration*

   Hasil yang didapat dari *filesystem configuration* yaitu 12 *scored* dan 13 *not scored* dari 25 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk menempatkan konfigurasi *filesystem* pada partisi yang terpisah pada *server*. Sehingga, proses audit dari *filesystem configuration* hanya 12 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 3 tahap *scored* yang tidak dilakukan (*not scored*), hal ini terjadi karena pada awal installasi tidak dilakukan pemisahan partisi seperti /*var*, /*var*/*log*, dan /*var*/*log*/*audit*. Sedangkan 10 tahap yang tidak dilakukan (*not scored*), terjadi karena ada beberapa *service filesystem* yang digunakan oleh sistem (seperti: *cramfs*, *freevxfs*, *jffs2*, *hfs*, *hfsplus*, *squashfs*, *udf*), begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.
3. *Secure Boot Settings*

   Hasil yang didapat dari *secure boot settings* yaitu 3 *scored* dan 1 *not scored* dari 4 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk mengkonfigurasi keamanan *bootloader* ke pengguna *root*. Sehingga, proses audit dari *secure boot settings* hanya 3 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 1 tahap *scored* yang tidak dilakukan (*not scored*), hal ini terjadi karena *server* hanya bisa dipantau melalui *remote server* dan tidak adanya teknisi yang dapat memantau *server* secara langsung.
4. *Additional Process Hardening*

   Hasil yang didapat dari *additional process hardening* yaitu 3 *scored* dan 2 *not scored* dari 5 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk konfigurasi tambahan proses *hardening* pada *server*. Sehingga, proses audit dari *additional process hardening* hanya 3 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 1 tahap *scored* yang tidak dilakukan (*not scored*) yaitu menginstall *AppArmor*, hal ini terjadi karena tidak adanya jaringan internet untuk menginstall *AppArmor*. Sedangkan 1 tahap yang tidak dilakukan (*not scored*) yaitu

mengaktifkan XD/NX *support on* 32-*bit* x86 *systems*, terjadi karena sistem tidak berjalan pada arsitektur 32-*bit*, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

5. OS *Services*

   Hasil yang didapat dari OS *service* yaitu 12 *scored* dan 1 *not scored* dari 13 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk konfigurasi tambahan dalam proses *hardening* pada *server*. Sehingga, proses audit dari OS *service* hanya 12 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 1 tahap *scored* yang tidak dilakukan (*not scored*) yaitu *Extended InterNet Daemon* (*Xinetd*), hal ini terjadi karena *daemon Xinetd* digunakan oleh *server*.

6. *Special Purpose Services*

   Hasil yang didapat dari *special purpose services* yaitu 7 *scored* dan 9 *not scored* dari 16 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk menjelaskan layanan yang diinstal pada *server* yang secara khusus perlu menjalankan beberapa *service* (layanan) dan untuk mengurangi potensi serangan jika tidak membutuhkan layanan tersebut. Sehingga, proses audit dari *special purpose services* hanya 7 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 1 tahap *not scored* yang dapat dilakukan (*scored*) yaitu memastikan LDAP tidak diaktifkan, hal ini terjadi karena *service* LDAP pada sistem aktif, sehingga perlu di *nonaktifkan*. Sedangkan 9 tahap yang tidak dilakukan (*not scored*), terjadi karena sistem membutuhkan HTTP *server* sebagai *webserver* dan beberapa layanan sudah tidak ada pada saat melakukan audit ini, seperti Print *Server*, NFS dan RPC, DNS *Server*, FTP *Server*, IMAP dan POP *Server*, Samba, HTTP *Proxy Server*, dan SNMP *Server*, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

7. *Network Configuration* dan *Firewalls*

   Hasil yang didapat dari *network configuration* dan *firewalls* yaitu 6 *scored* dan 18 *not scored* dari 24 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk mengatur parameter jaringan yang ada pada *server*. Sehingga, proses audit dari *network configuration* dan *firewalls* hanya 6 tahap yang dapat dilakukan (*scored*).

   Pada tahap ini ada 8 tahap *scored* yang tidak dilakukan (*not scored*) yaitu pada bagian memodifikasi parameter jaringan (*host* dan *router*), *server* tidak digunakan sebagai *router*, sehingga pada bagian ini tidak dilakukan. Sedangkan 10 tahap yang tidak dilakukan (*not scored*), terjadi karena sistem tidak menggunakan IPv6, *file* /*etc*/*hosts.allow* dan /*etc*/*hosts.deny* sudah dibuat oleh sistem, dan beberapa layanan sudah tidak ada pada saat melakukan audit ini, seperti DCCP, SCTP, RDS, TIPC, dan *Interface Wireless*, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

8. *Logging* dan *Auditing*

   Hasil yang didapat dari *logging* dan *auditing* yaitu 24 *scored* dan 5 *not scored* dari 29 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk melakukan *auditing* dan memantau log agar terhindar dari usaha intrusi dan perilaku sistem yang mencurigakan lainnya. Sehingga, proses audit dari *special purpose services* hanya 24 tahap yang dapat dilakukan (*scored*), sedangkan 5 tahap yang tidak dilakukan (*not scored*) terjadi karena beberapa layanan sudah dikonfigurasi secara *default* (seperti konfigurasi ukuran penyimpanan log Audit, konfigurasi /*etc*/*rsyslog.conf*, dan konfigurasi *logrotate* pada layanan AIDE), *server* tidak menerima pesan *remote rsyslog* dari *host* manapun, dan sistem tidak perlu di *nonaktifkan* saat log Audit penuh, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

9. *System Access*, *Authentication* dan *Authorization*

   Hasil yang didapat dari *system access*, *authentication* dan *authorization* yaitu 25 *scored* dan 2 *not scored* dari 27 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan

untuk menentukan bagaimana sistem dapat diakses, menentukan *user* yang dapat mengakses sistem, dan menentukan akses *user* terhadap *resource* tertentu dalam sistem. Sehingga, proses audit dari *system access*, *authentication* dan *authorization* hanya 25 tahap yang dapat dilakukan (*scored*), sedangkan 2 tahap yang tidak dilakukan (*not scored*) terjadi karena *server* tidak membatasi login *root* untuk sistem *console* dan akun pengguna tidak akan di *lock* apabila salah memasukkan *password* beberapa kali, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

10. *User Accounts* dan *Environment*

    Hasil yang didapat dari *user accounts* dan *environment* yaitu 7 *scored* dari 7 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk memberikan panduan instalasi *default* yang aman untuk sistem, akun pengguna dan *environment* sistem. Sehingga, proses audit dari *user accounts* dan *environment* yaitu 7 tahap yang dilakukan (*scored*) dan diutamakan menurut rekomendasi CIS *Benchmark*.

11. *Warning Banners*

    Hasil yang didapat dari *warning banners* yaitu 2 *scored* dan 1 *not scored* dari 3 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk menyembunyikan informasi versi OS dan informasi sistem terperinci lainnya dari penyerang yang mencoba menargetkan eksploitasi tertentu pada sistem. Sehingga, proses audit dari *warning banners* hanya 2 tahap yang dapat dilakukan (*scored*), sedangkan 1 tahap yang tidak dapat dilakukan (*not scored*) yakni mengatur grafik *warning banner* terjadi karena sistem tidak menggunakan tampilan GUI, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

12. *Verify System File Permissions*

    Hasil yang didapat dari *verify system file permissions* yaitu 8 *scored* dan 3 *not scored* dari 11 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk mengendalikan siapa yang bisa membaca, menulis dan mengeksekusi *file* tertentu pada sistem. Sehingga, proses audit dari *verify system file permissions* hanya 8 tahap yang dapat dilakukan (*scored*), sedangkan 3 tahap yang tidak dapat dilakukan (*not scored*) terjadi karena tidak ada file yang *world-writable*, maupun SUID dan SGID sistem yang *executables*, begitu juga hasilnya sudah *not scored* (tidak diutamakan) menurut rekomendasi dari CIS *Benchmark* Linux Debian.

13. *Review User* dan *Group Settings*

    Hasil yang didapat dari *review user* dan *group settings* yaitu 20 *scored* dari 20 tahap rekomendasi CIS *Benchmark*, hal ini bertujuan untuk mengontrol akses ke *file*, *direktori*, dan *peripheral* sistem. Sehingga, proses audit dari *review user* dan *group settings* yaitu 20 tahap yang dilakukan (*scored*) dan diutamakan menurut rekomendasi CIS *Benchmark*.

Berdasarkan hasil pembahasan tersebut, maka total yang didapatkan dari hasil audit dan implementasi CIS *Benchmark* Linux Debian yang dilakukan pada *server* Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta, berjumlah 129 tahap yang mendapatkan nilai (*scored*) dan 56 tahap tidak dinilai (*not scored*) dari 185 total tahap rekomendasi CIS *Benchmark*. Sehingga, *server* yang ada di Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta, berhasil menerapkan praktik terbaik (*best practice*) pengamanan sistem operasi Linux Debian berdasarkan rekomendasi CIS *Benchmark*, dan mendapatkan persentase 70% dari 185 tahap rekomendasi CIS *Benchmark*.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka kesimpulan yang dapat diambil adalah:

1. Berdasarkan hasil audit dan implementasi CIS *Benchmark*, maka *server* Laboratorium Jaringan dan Komputer 6, IST AKPRIND Yogyakarta mendapatkan *scored* 129 atau 70% dari total 185 *scored*.

2. *Server* Laboratorium Jaringan dan Komputer 6, IST AKPRIND Yogyakarta sudah berhasil menerapkan praktik terbaik (*best practice*) pengamanan sistem operasi Linux Debian berdasarkan CIS *Benchmark* yang dikeluarkan oleh *Center for Internet Security*.

SARAN

Saran yang dapat disampaikan untuk pengembangan dan perbaikan pada penelitian selanjutnya yaitu:

1. Untuk pengembangan audit dan implementasi CIS *Benchmark* Linux Debian sebaiknya dilakukan sejak awal *installasi server*.
2. Perlu dilakukan pemeriksaan secara rutin oleh administrator guna memastikan sistem tetap aman dari serangan siber.
3. Penelitian atau perbaikan yang dapat dilakukan selanjutnya yaitu menerapkan praktik keamanan terbaik pada sisi layanan (*service*) yang berjalan di atas sistem operasi (seperti *webserver*, *database server*, dll).

DAFTAR PUSTAKA

Center for Internet Security. (2017). *About Us*. Retrieved 8 November 2017, from cisecurity.org: https://www.cisecurity.org/about-us/

Ditjen GTK. (2016). *Modul Pembelajar Teknik Komputer dan Jaringan (TKJ)*. Jakarta: Ditjen GTK.

Jogi, M. (2017). *Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance*. Thesis. University Of Tartu.

Kemendikbud. (2017). *Kompetensi Inti dan Kompetensi Dasar Mata Pelajaran Muatan Nasional (A), Muatan Kewilayahan (B), Dasar Bidang Keahlian (C1), Dasar Program Keahlian (C2), dan Kompetensi Keahlian (C3),* Jakarta.

Nepal, A. K. (2013). *Linux Server dan Hardening Security*. Thesis. Western Governors University

Nuckols, R. (2015). *Red Hat Enterprise Linux 7 Server Baseline di Department of Veterans Affairs*. VA Baseline Configuration and Security Standard RHEL 7.

Rahman, Muhammad Mushfiqur. (2015). *Auditing Linux/GNU Server Operating Server*. ISACA Journal Vol. 4.