EVALUATION OF MANAGEMENT NETWORK SECURITY USING SEKCHECK NETWORK EVALUATOR

Rizal S, Cholil W, Widiyati Q
Computer Science Faculty, Bina Darma University
Palembang, South Sumatera
***syahri_rizal@binadarma.ac.id*, *widya@binadarma.ac.id*,**
qoriani_widayati@binadarma.ac.id

ABSTRACT

The Utilization of Information Technology in business has become a significant part in supporting the business process. The implementation of IT has been implemented as a value chain system which support the business transaction from first level process till documentation, its result a report which could mark the decision making process in manager level. Indeed the information which is the output of the system has a very important role in the process business; therefore the procedure and mechanism how to protect that information also need a special courtesy. There are several tools which has been use as security evaluator both inn system and network. This paper has concern about one of those tools, the tools called Sekcheck Network Evaluator Security Evaluator. This tools has function to analyze the current system in awareness of user in information security substances especially assessment of user role and activities in a network. The papers will analyze the assessments process by Sekcheck Network Evaluator and how the result is and how to accomplish it with Information Technology Audit process that will influence to the factors of awareness and risk level of information security from user perspective. At the end this could use as consideration input for managers to optimize user awareness about security of information in business.

Keywords: Business transaction system, Information Security, Awareness, Assessment, Network,* application *Sekcheck Network Evaluator security evaluator

ABSTRAK

Pemanfaatan Teknologi Informasi dalam bisnis bagian penting dalam mendukung proses bisnis. Implementasi IT telah diimplementasikan sebagai sistem rantai nilai yang mendukung transaksi bisnis dari proses tingkat pertama sampai dokumentasi, hasilnya laporan yang bisa menandai proses pengambilan keputusan di tingkat manajer. Informasi merupakan keluaran dari sistem yang memiliki peran sangat penting dalam proses bisnis. Oleh karena itu prosedur dan mekanisme bagaimana melindungi informasi membutuhkan courtesy khusus. Ada beberapa alat yang telah digunakan sebagai evaluator keamanan baik sistem penginapan dan jaringan. Makalah ini memiliki kekhawatiran tentang salah satu alat yang disebut Sekcheck Jaringan Evaluator Keamanan Evaluator. alat ini berfungsi untuk menganalisis sistem saat di kesadaran pengguna dalam zat keamanan informasi terutama penilaian peran pengguna dan kegiatan dalam jaringan. Koran-koran akan menganalisis proses penilaian oleh Sekcheck Jaringan Evaluator dan bagaimana hasilnya dan bagaimana mencapainya dengan proses Audit Teknologi Informasi yang akan berpengaruh terhadap faktor kesadaran dan tingkat risiko keamanan informasi dari perspektif pengguna. Pada

akhirnya ini bisa digunakan sebagai masukan pertimbangan bagi manajer untuk mengoptimalkan kesadaran pengguna tentang keamanan informasi dalam bisnis.
Kata kunci: sistem transaksi bisnis, Keamanan Informasi, Kesadaran, Pengkajian, Jaringan, aplikasi Sekcheck Jaringan Evaluator evaluator keamanan

I. PENDAHULUAN

Teknologi Informasi saat ini digunakan untuk mendukung semua kegiatan manusia baik pada semua sektor. Sektor Bisnis merupakan bidang yang paling pesat dalam menggunakan Teknologi Informasi dalam mendukung kegiatannya, baik dalam segi software, hardware maupun brainware. Semua komponen tersebut merupakan bagian dari TI yang saling berkaitan dalam mendukung Strategi suatu organisasi dalam mencapai tujuan baik organisasi bidang bisnis maupun pendidikan.

'IT Governance: Specifiying the decision rights and accountability framework to encourage desirable behaviour in the use of IT" [1]. Dalam proses pemanfaatan Teknologi Informasi tersebut, suatu organisasi memiliki tujuan masing-masing sesuai dengan bidang dan proses bisnis mereka. Tetapi pada intinya semua organisasi menganggap bahwa dalam pemanfaatan TI yang terdiri atas perangkat lunak, perangkat keras dan sumber daya manusia. ketiga bagian ini saling berintegrasi dalam menghasilkan suatu informasi atau data yang merupakan bagian terpenting dari seluruh proses. Sehingga pengamanan informasi atau data yang dihasilkan oleh sebuah sistem pada suatu organisasi merupakan hal yang terpenting juga untuk dilaksanakan pada setiap organisasi yang menerapkan TI dalam proses bisnisnya.[5]

II. METODE PENELITIAN

Sehubungan dengan permasalahan yang dihadapi oleh organisasi, maka dalam paper ini peneliti membahas penelitian yang bersifat pengamatan dan analisa pada proses audit system yang diterapkan pada sebuah organisasi yang bergerak di bidang pendanaan/keuangan. System yang diterapkan sudah berbasis jaringan local (LAN). Proses penggunaan system ditentukan dengan adanya prosesdur khusus dengan adanya user-id dan password untuk masing masing pengguna di setiap level pada system ini juga ditentukan hakk akses dari masing-masing user dan hal ini dikelolah oleh seorang admin. Dengan adanya penerapan prosedur serta konfigurasi khusus pada system oleh Unit Pengelolah atau Admin Sistem, hal ini tidak menjamin kesadaran pengguna atau para karyawan berkaitan dengan keamanan data. Hal ini diindikasikan masih adanya data yang tidak validasi, tidak lengkap atau hilang,

dan dari user yang bersangkutan tidak dapat memberi pertanggung jawaban atas kejadian tersebut.

Sehubungan dengan hal tersebut, maka peneliti melakukan penelitian pada organisasi tersebut dengan melakukan evaluasi kinerja system khusus dalam mekanisme pengamanan data dan kesadaran user dalam hal keamanan data pada system yang digunakan pada organisasi tersebut, proses ini sering dikenal sebgai bagian dari proses Audit Teknologi Informasi.[4] Dalam proses evaluasi tersebut, peneliti menggunakan tools atau perangkat lunak khusus yang biasa digunakan dalam audit teknologi informasi yaitu ***Sekchek Security Evaluator.***

Sekchek Security Evaluator adalah sebuah aplikasi yang dirancang khusus dalam menunjang proses audit teknologi informasi khususnya dalam pengenalian keamanan sebuah system yang digunakan pada sebuah organisasi yang berorientasi bisnis. [8]

III. HASIL DAN PEMBAHASAN

Pada Bab ini akan dijelaskan hasil yang didapt dalam proses evaluasi terhadap kinerja pengamanan system dengan menggunakan aplikasi *Sekcheck Network Evaluator Network Evaluator*. Adapun tahapan yang dilaksanakan pada proses evaluasi adalah:

Proses Installasi Aplikasi *Sekcheck Network Evaluator*

Tampilkan proses installasi Sekcheck Network Evaluator pada Server, dan menghasilkan option dibawah dapat dilihat pada Tabel 1.

Tabel 1. Sekcheck Network Evaluator menu option

SekChek Options	
Reference Number	1009090005
Requester	Sunny Ho Yin Wong
Telephone Number	+86 (21) 123 4567
City	Shanghai
Client Country	China
Charge Code	SEK100906
Client Code	SEK001
Client Industry Type	Communications
Host Country	UK
Security Standards Template	0 - SekChek Default
Evaluate Against Industry Type	<All>
Compare Against Previous Analysis	Not Selected
Report Format	Word 2007
Paper Size	A4 (21 x 29.7 cms)
Spelling	English UK
Large Report Format	MS-Excel spreadsheet
Large Report (Max Lines in Word Tables)	1500
Summary Document Requested	Yes
Scan Software Version Used	Version 5.1.0
Scan Software Release Date	08-Nov-2013

Proses konfigurasi

Proses konfigurasi dari fitur-fitur yang akan dievaluasi pada jaringan system pembayaran PT. BFI, Tbk. Langkah tersebut dapat dilihat pada Tabel 2.

Tabel 2. System Details

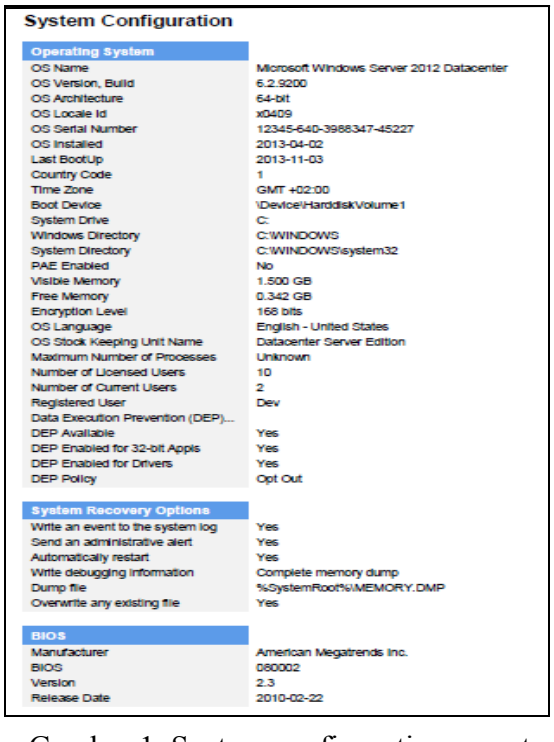
System Details	
Computer Name	PROMETHEUS
Computer Sid (SAM)	S-1-5-21-1234567890-1430676833-796538989
Windows Version	6.2 (Windows 2012)
Scan Time	06-Nov-2013 08:20
Scanned By	AdminNew
Computer Role**	Member Server
Domain / Work Group	OLYMPUS (olympus.com)
Domain Sid	S-1-5-21-3456789012-1181587698-3058679118
Build / Service Pack	9200/
System Locale Id	1033 (x409)

Setelah tahap kofigurasi selesai maka, *Sekcheck Network Evaluator* mengadakan proses *capturing bit-image*

pada server dan menghasilkan output sebagai berikut:

1. Hasil analisa konfigurasi system yang sekarang

Tampilan ini menunjukkan output dari aplikasi *Sekcheck Network Evaluator* setelah melakukan scanning pada system yang digunakan di PT. BFI. dari tampilan ini dapat kita lihat konfigurasi secara lengkap tentang system yang digunakan terutama informasi rinci tentang komponen-komponen pada server, seperti terlihat pada Gambar 1.



System Configuration

Operating System	
OS Name	Microsoft Windows Server 2012 Datacenter
OS Version, Build	6.2.9200
OS Architecture	64-bit
OS Locale Id	x0409
OS Serial Number	12345-640-3988347-45227
OS Installed	2013-04-02
Last BootUp	2013-11-03
Country Code	1
Time Zone	GMT +02:00
Boot Device	\Device\HarddiskVolume1
System Drive	C:
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
PAE Enabled	No
Visible Memory	1.500 GB
Free Memory	0.342 GB
Encryption Level	168 bits
OS Language	English - United States
OS Stock Keeping Unit Name	Datacenter Server Edition
Maximum Number of Processes	Unknown
Number of Licensed Users	10
Number of Current Users	2
Registered User	Dev
Data Execution Prevention (DEP)...	
DEP Available	Yes
DEP Enabled for 32-bit Appls	Yes
DEP Enabled for Drivers	Yes
DEP Policy	Opt Out
System Recovery Options	
Write an event to the system log	Yes
Send an administrative alert	Yes
Automatically restart	Yes
Write debugging information	Complete memory dump
Dump file	%SystemRoot%\MEMORY.DMP
Overwrite any existing file	Yes
BIOS	
Manufacturer	American Megatrends Inc.
BIOS	080002
Version	2.3
Release Date	2010-02-22

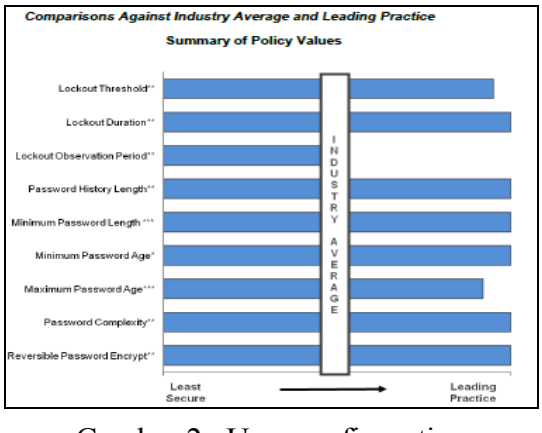
Gambar 1. System configuration report

Selain tampilan diatas, output dari proses ini juga menampilkan penjelasan tentang konfigurasi pada komponen komponen server lainnya seperti:

1. Motherboard,
2. Pagefiles,
3. Computer
4. Firewall
5. Network Adapter
6. Region & language saver
7. User Access Control

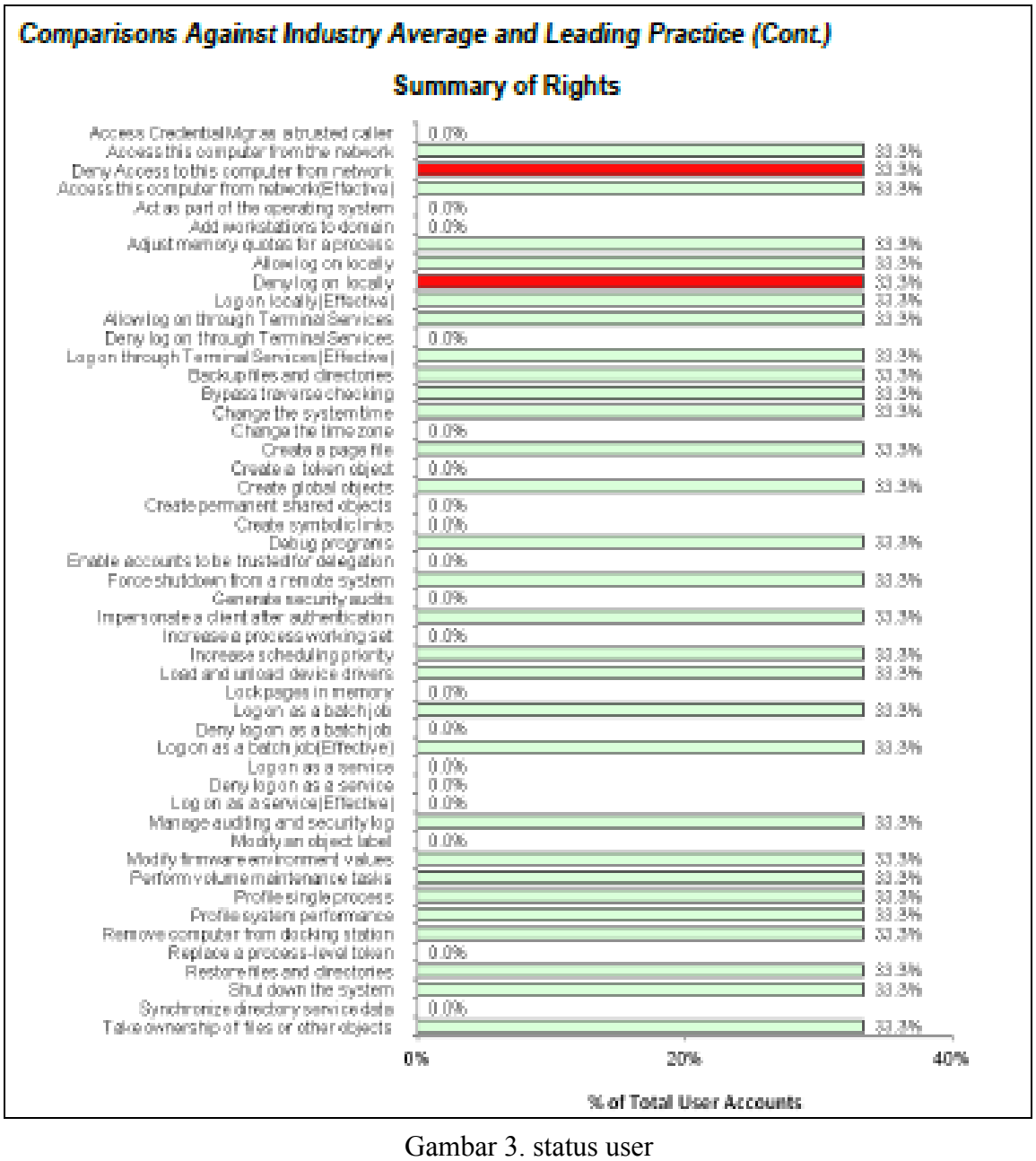
2. Konfigurasi User Account

Tampilan berikut menjelaskan bagaimana kategori pembagian kelompok user account pada PT. BFI. Serta dijelaskan bagaimana perbandingan antara user yang aktif dalam menggunakan system (leading practice) dengan user yang tidak begitu aktif menggunakan system (Industry average). konfigurasi user account dapat di lihat pada Gambar 2.



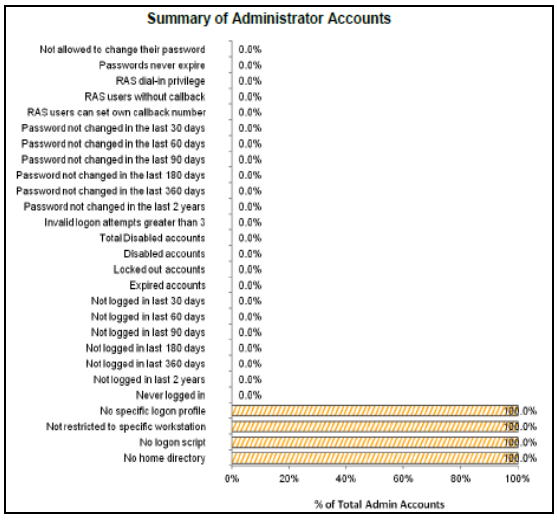
Gambar 2. User configuration

Pada gambar diatar dapat dilihat bahwa kelompok leading practice memiliki kesadaran lebih tinggi dalam menjalankan semua prosedur yang berhubungan dengan keamanana data daripada kelompok industry yang cenderung hanya menggunakan standard setup. Tampilan status user dapat dilihat pada Gambar 3.



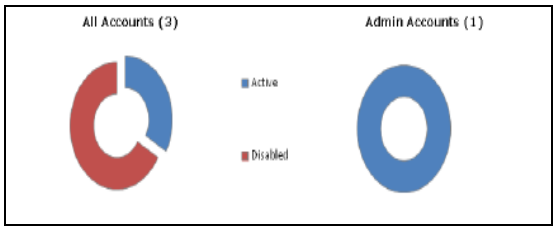
Gambar 3. status user

Tampilan diatas menjelaskan user yang aktif pada jaringan. Dari total user yang aktif maka ada 33,3 % user yang selalu melakukan update dalam user account nya. Pada gambar 3 menunjukkan bagaimana status dari admin user pada jaringan serta update status yang dilakukan oleh admin account tersebut. dari kedua tampilan ini kita dapat melihat bahwa Sekcheck Network Evaluator sangat membantu dalam proses evaluasi pada user di jaringan yang kita evaluasi. Setidaknya dengan hasil ini , admin dapat dilihat bagaimana peranannya dalam meningkatkan keamanan, dilanjutkan dengan seluruh user.



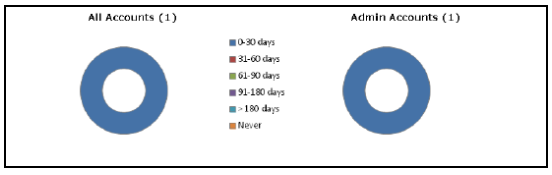
Gambar 4. Administrator Account

Tampilan dibawah ini hanya membandingkan status antara semua user yang aktif dan nonaktik (tidak diaktifkan) , dan account administrator jaringan.



Gambar 5. User Account Kategorize

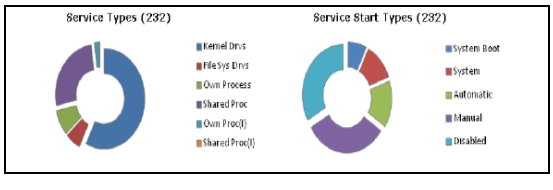
Dari ketiga kategori user account tersebut,Sekcheck Network Evaluator menganalisa keaktifan user dalam ketegori "seberapa aktif user?" dapat dilihat dari hasilnya bahwa baik user maupu admin sangat aktif dalam menggunakan system lebih dari 180 hari (default dari Sekcheck Network Evaluator).



Gambar 6. User active

Seberapa aktif user melakukan "pergantian password' juga dianalisa oleh Sekcheck Network Evaluator , dan hasilny menunjukkan bahwa dalam kurun 30 hari, semua user selalu mengganti passwordnya.

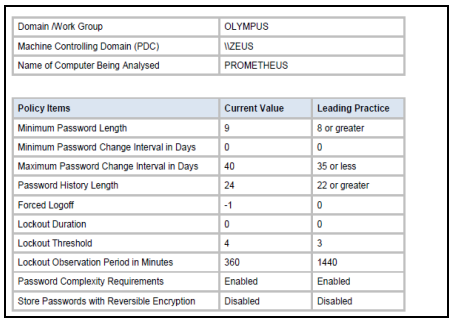
Gambar dibawah ini menunjukan hasil analisa terhadap kepercayaan akses yang diberikan pada masing-masing user pada system serta pelayanan apa saja yang dapat mereka gunakan dari system.



Gambar 7. User priveleges

i. Sistem Account Policy

Fitur ini menjelaskan hasil analisa Sekcheck Network Evaluator terhadapa semua aturan-aturan yang diberikan kepada setiap user yang dapat memperleh hak akses.



Domain /Work Group	OLYMPUS
Machine Controlling Domain (PDC)	\\ZEUS
Name of Computer Being Analysed	PROMETHEUS

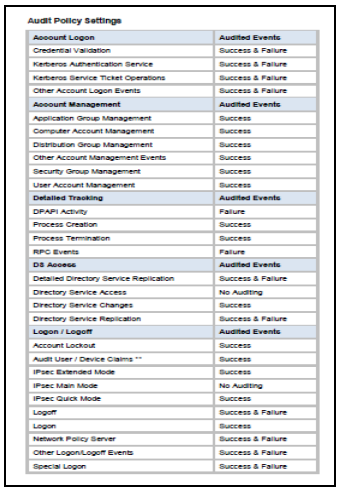
Policy Items	Current Value	Leading Practice
Minimum Password Length	9	8 or greater
Minimum Password Change Interval in Days	0	0
Maximum Password Change Interval in Days	40	35 or less
Password History Length	24	22 or greater
Forced Logoff	-1	0
Lockout Duration	0	0
Lockout Threshold	4	3
Lockout Observation Period in Minutes	360	1440
Password Complexity Requirements	Enabled	Enabled
Store Passwords with Reversible Encryption	Disabled	Disabled

Gambar 8. Sistem Account Policy

Dari tampilan diatas dapat dilihat bahwa adanya domain dan workgroup pada jaringan. Apabila proses dilakukan pada workstation yang tidak terkoneksi dengan jaringan maka statusnya adalah'NONE'. Dari tampilan jaringan hanya memiliki satu PDC yang bertanggung jawab dalam security domain. Pada tampilan ini juga menjelaskan aturan pembuatan password, serta aturan untuk user yang lupa keluar (logoff) dari system.

ii. Audit Policy Setting

Hasil analisa yang menjelaskan tentang kofigurasi aturan-aturan audit yang diterapkan pada system/jaringan yang sedang dievaluasi.

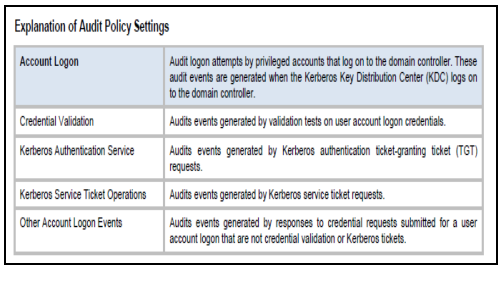


Audit Policy Settings

Account Logon	Audited Events
Credential Validation	Success & Failure
Kerberos Authentication Service	Success & Failure
Kerberos Service Ticket Operations	Success & Failure
Other Account Logon Events	Success & Failure
Account Management	**Audited Events**
Application Group Management	Success
Computer Account Management	Success
Distribution Group Management	Success
Other Account Management Events	Success
Security Group Management	Success
User Account Management	Success
Detailed Tracking	**Audited Events**
DPAPI Activity	Failure
Process Creation	Success
Process Termination	Success
RPC Events	Failure
DS Access	**Audited Events**
Detailed Directory Service Replication	Success & Failure
Directory Service Access	No Auditing
Directory Service Changes	Success
Directory Service Replication	Success & Failure
Logon / Logoff	**Audited Events**
Account Lockout	Success
Audit User / Device Claims **	Success
IPsec Extended Mode	Success
IPsec Main Mode	No Auditing
IPsec Quick Mode	Success
Logoff	Success & Failure
Logon	Success
Network Policy Server	Success & Failure
Other Logon/Logoff Events	Success & Failure
Special Logon	Success & Failure

Gambar 9. Audit policy Setting

Dapat dilihat komponen komponen yang dapat diaudit serta bagaimana hasil akhir dari pelaksanaan audit pada komponen tersebut. Adapun penjelasan tentang aturan-aturan tersebut juga ditampilkan pada hasil analisa ini.



Explanation of Audit Policy Settings

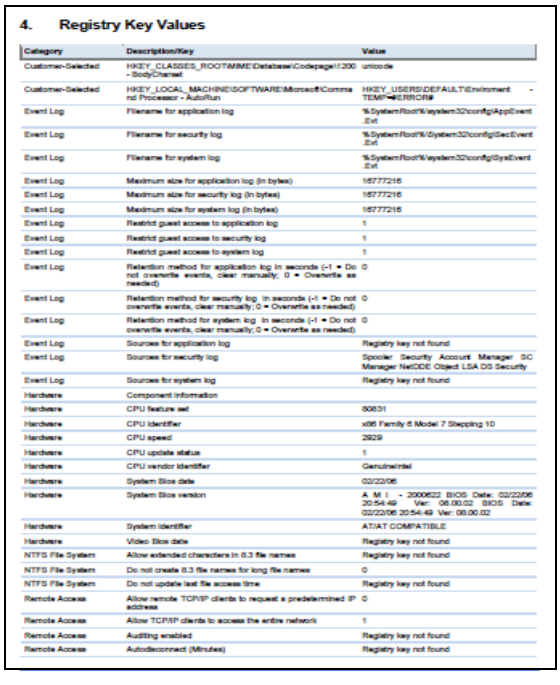
Account Logon	Audit logon attempts by privileged accounts that log on to the domain controller. These audit events are generated when the Kerberos Key Distribution Center (KDC) logs on to the domain controller.
Credential Validation	Audits events generated by validation tests on user account logon credentials.
Kerberos Authentication Service	Audits events generated by Kerberos authentication ticket-granting ticket (TGT) requests.
Kerberos Service Ticket Operations	Audits events generated by Kerberos service ticket requests.
Other Account Logon Events	Audits events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets.

Gambar 10. Expnataiton Policy

iii. Registry Key Values

Tampilan ini menjelaskan informasi tentang key-key yang digunakan dalam system terutama untuk proses evaluasi. Apabila sebuah key terdaftar maka statusnya 'lebih dari 1', dan jika tidak dapt digunakan adalah '1'. Apabila sebuah key disetting dengan benar, maka dapat

memberikan dampak peningkatan keamanan sistem tersebut.



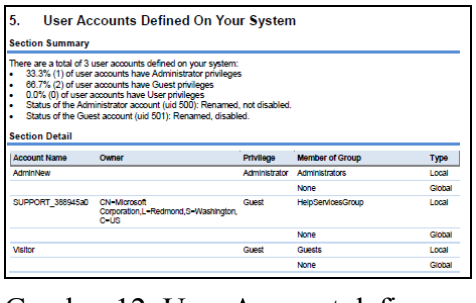
4. Registry Key Values

Category	Description/Key	Value
Customer-Selected	HKEY_CLASSES_ROOT\MIME\Database\Codepage\1200 - BodyCharset	unicode
Customer-Selected	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor - AutoRun	HKEY_USERS\.DEFAULT\Environment - TEMP=%ERROR%
Event Log	Filename for application log	%SystemRoot%\system32\config\AppEvent.Evt
Event Log	Filename for security log	%SystemRoot%\System32\config\SecEvent.Evt
Event Log	Filename for system log	%SystemRoot%\system32\config\SysEvent.Evt
Event Log	Maximum size for application log (in bytes)	16777216
Event Log	Maximum size for security log (in bytes)	16777216
Event Log	Maximum size for system log (in bytes)	16777216
Event Log	Restrict guest access to application log	1
Event Log	Restrict guest access to security log	1
Event Log	Restrict guest access to system log	1
Event Log	Retention method for application log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Retention method for security log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Retention method for system log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Sources for application log	Registry key not found
Event Log	Sources for security log	Spooler Security Account Manager SC Manager NetDDE Object LSA DS Security
Event Log	Sources for system log	Registry key not found
Hardware	Component information	
Hardware	CPU feature set	80831
Hardware	CPU identifier	x86 Family 6 Model 7 Stepping 10
Hardware	CPU speed	2929
Hardware	CPU update status	1
Hardware	CPU vendor identifier	GenuineIntel
Hardware	System Bios date	02/22/06
Hardware	System Bios version	A M I - 2000622 BIOS Date: 02/22/06 20:54:49 Ver: 08.00.02 BIOS Date: 02/22/06 20:54:49 Ver: 08.00.02
Hardware	System identifier	AT/AT COMPATIBLE
Hardware	Video Bios date	Registry key not found
NTFS File System	Allow extended characters in 8.3 file names	Registry key not found
NTFS File System	Do not create 8.3 file names for long file names	0
NTFS File System	Do not update last file access time	Registry key not found
Remote Access	Allow remote TCP/IP clients to request a predetermined IP address	0
Remote Access	Allow TCP/IP clients to access the entire network	1
Remote Access	Auditing enabled	Registry key not found
Remote Access	Autodisconnect (Minutes)	Registry key not found

Gambar 11. Registry Key values

iv. User Account Defined on system

Tampilan ini menjelaskan bagaimana hak akses semua user account yang terdaftar didalam system/domain.



5. User Accounts Defined On Your System

Section Summary

There are a total of 3 user accounts defined on your system:
- 33.3% (1) of user accounts have Administrator privileges
- 66.7% (2) of user accounts have Guest privileges
- 0.0% (0) of user accounts have User privileges
- Status of the Administrator account (uid 500): Renamed, not disabled.
- Status of the Guest account (uid 501): Renamed, disabled.

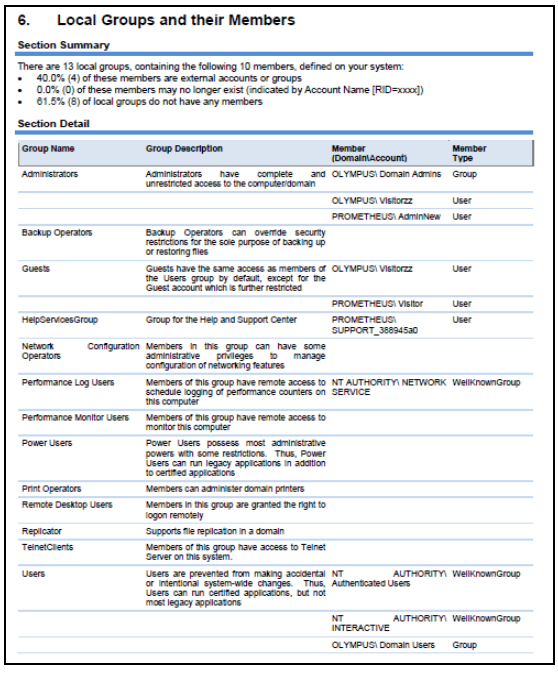
Section Detail

Account Name	Owner	Privilege	Member of Group	Type
AdminNew		Administrator	Administrators	Local
			None	Global
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington, C=US	Guest	HelpServicesGroup	Local
			None	Global
Visitor		Guest	Guests	Local
			None	Global

Gambar 12. User Account define

v. Local Group dan member dalam system

Pada tampilan ini menjelaskan analisa tentang kumpulan user sebagai local group dari domain.yang berfungsi sebagai backup controller dari domain inti. Dapat dilihat bahwa visitor merupaka local group, sehingga visitor memiliki hak akses yang berbeda dengan user dan admin.



6. Local Groups and their Members

Section Summary

There are 13 local groups, containing the following 10 members, defined on your system:
- 40.0% (4) of these members are external accounts or groups
- 0.0% (0) of these members may no longer exist (indicated by Account Name [RID=xxxx])
- 61.5% (8) of local groups do not have any members

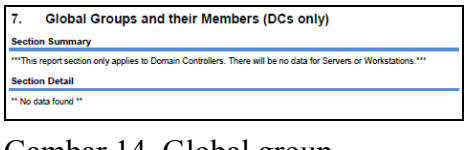
Section Detail

Group Name	Group Description	Member (Domain\Account)	Member Type
Administrators	Administrators have complete and unrestricted access to the computer/domain	OLYMPUS\ Domain Admins	Group
		OLYMPUS\ Visitorzz	User
		PROMETHEUS\ AdminNew	User
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files		
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	OLYMPUS\ Visitorzz	User
		PROMETHEUS\ Visitor	User
HelpServicesGroup	Group for the Help and Support Center	PROMETHEUS\ SUPPORT_388945a0	User
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features		
Performance Log Users	Members of this group have remote access to schedule logging of performance counters on this computer	NT AUTHORITY\ NETWORK SERVICE	WellKnownGroup
Performance Monitor Users	Members of this group have remote access to monitor this computer		
Power Users	Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications		
Print Operators	Members can administer domain printers		
Remote Desktop Users	Members in this group are granted the right to logon remotely		
Replicator	Supports file replication in a domain		
TelnetClients	Members of this group have access to Telnet Server on this system.		
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications	NT AUTHORITY\ Authenticated Users	WellKnownGroup
		NT AUTHORITY\ INTERACTIVE	WellKnownGroup
		OLYMPUS\ Domain Users	Group

Gambar 13. Local group members

vi. Global group dan member

Pada menu ini menampilakan informasi tentang semua group yang termasuk dalam domain serta member (anggota) dari group tersebut. Dari hasil analisa domain jaringan tidak memiliki group global, hal ini bertujuan untuk menjamin sekuriti data agar lebih terjamin dengan tidak memberikan autentikasi akses terlalu banyak.



7. Global Groups and their Members (DCs only)

Section Summary

"This report section only applies to Domain Controllers. There will be no data for Servers or Workstations."

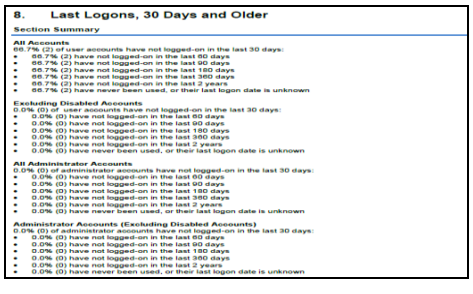
Section Detail

** No data found **

Gambar 14. Global group

vii. Report daftar Logons dalam kurun waktu 30 hari

Pada report ini ditampilkan hasil analisa terhadap aktivitas user pada jaringan, dan dapat dilihat bahwa 66,7 % user yang tidak pernah logged on pada system selama kurun waktu 30 hari atau lebih. Hal ini didapatkan pada user dengan kategori tidak aktif tetapi enabled.


8. Last Logons, 30 Days and Older

Section Summary

All Accounts
66.7% (2) of user accounts have not logged-on in the last 30 days:
- 66.7% (2) have not logged-on in the last 60 days
- 66.7% (2) have not logged-on in the last 90 days
- 66.7% (2) have not logged-on in the last 180 days
- 66.7% (2) have not logged-on in the last 360 days
- 66.7% (2) have not logged-on in the last 2 years
- 66.7% (2) have never been used, or their last logon date is unknown

Excluding Disabled Accounts
0.0% (0) of user accounts have not logged-on in the last 30 days:
- 0.0% (0) have not logged-on in the last 60 days
- 0.0% (0) have not logged-on in the last 90 days
- 0.0% (0) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

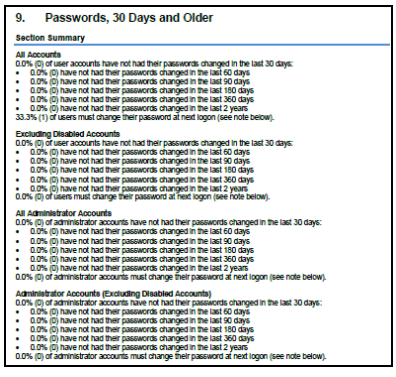
All Administrator Accounts
0.0% (0) of administrator accounts have not logged-on in the last 30 days:
- 0.0% (0) have not logged-on in the last 60 days
- 0.0% (0) have not logged-on in the last 90 days
- 0.0% (0) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

Administrator Accounts (Excluding Disabled Accounts)
0.0% (0) of administrator accounts have not logged-on in the last 30 days:
- 0.0% (0) have not logged-on in the last 60 days
- 0.0% (0) have not logged-on in the last 90 days
- 0.0% (0) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

Gambar 15. Last logon

viii. Report Password policy

Pada menu ini ditampilkan hasil laporan tentang seberapa aktif semua user dalam melakukan penggantian password. Hasilnya ditemukan bahwa ada beberapa user yang tidak pernah mengganti password lebih dari 30 hari. Untuk kategori admin , proses penggantian password cukup aktif, hal ini sesuai dengan tujuan untuk menjaga keamanan system.


9. Passwords, 30 Days and Older

Section Summary

All Accounts
0.0% (0) of user accounts have not had their passwords changed in the last 30 days:
- 0.0% (0) have not had their passwords changed in the last 60 days
- 0.0% (0) have not had their passwords changed in the last 90 days
- 0.0% (0) have not had their passwords changed in the last 180 days
- 0.0% (0) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

33.3% (1) of users must change their password at next logon (see note below).

Excluding Disabled Accounts
0.0% (0) of user accounts have not had their passwords changed in the last 30 days:
- 0.0% (0) have not had their passwords changed in the last 60 days
- 0.0% (0) have not had their passwords changed in the last 90 days
- 0.0% (0) have not had their passwords changed in the last 180 days
- 0.0% (0) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

0.0% (0) of users must change their password at next logon (see note below).

All Administrator Accounts
0.0% (0) of administrator accounts have not had their passwords changed in the last 30 days:
- 0.0% (0) have not had their passwords changed in the last 60 days
- 0.0% (0) have not had their passwords changed in the last 90 days
- 0.0% (0) have not had their passwords changed in the last 180 days
- 0.0% (0) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

0.0% (0) of administrator accounts must change their password at next logon (see note below).

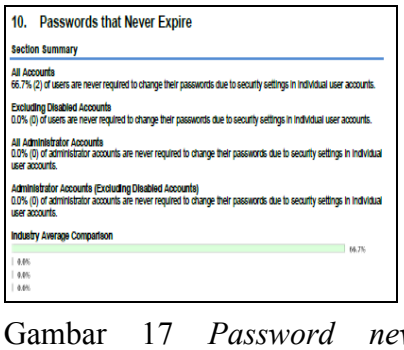
Administrator Accounts (Excluding Disabled Accounts)
0.0% (0) of administrator accounts have not had their passwords changed in the last 30 days:
- 0.0% (0) have not had their passwords changed in the last 60 days
- 0.0% (0) have not had their passwords changed in the last 90 days
- 0.0% (0) have not had their passwords changed in the last 180 days
- 0.0% (0) have not had their passwords changed in the last 360 days
- 0.0% (0) have not had their passwords changed in the last 2 years

0.0% (0) of administrator accounts must change their password at next logon (see note below).

Gambar 16. Password details

ix. Report untuk password yang tidak pernah kadaluarsa

Tampilan ini menjelaskan status dari accounts user yang tidak pernah expire (kadaluarsa) dalam system. Pada password policy sebenarnya sudah ada aturan adanya pergantian password secara berkala oleh system, tetapi kadang-kadang user hanya melakukan update, bahkan tidak mengganti sama sekali. Jika password tidak pernah diganti, resiko keamanan system sangat tinggi.


10. Passwords that Never Expire

Section Summary

All Accounts
66.7% (2) of users are never required to change their passwords due to security settings in individual user accounts.

Excluding Disabled Accounts
0.0% (0) of users are never required to change their passwords due to security settings in individual user accounts.

All Administrator Accounts
0.0% (0) of administrator accounts are never required to change their passwords due to security settings in individual user accounts.

Administrator Accounts (Excluding Disabled Accounts)
0.0% (0) of administrator accounts are never required to change their passwords due to security settings in individual user accounts.

Industry Average Comparison

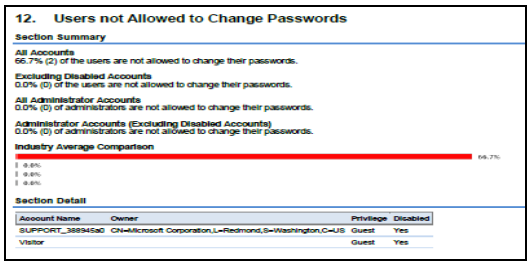
66.7%
0.0%
0.0%
0.0%

Gambar 17 *Password never expire summary*

x. Menu user yang tidak diperbolehkan mengganti password

Pada report ini menjelaskan bahwa pada system juga ditentukan adanya beberapa

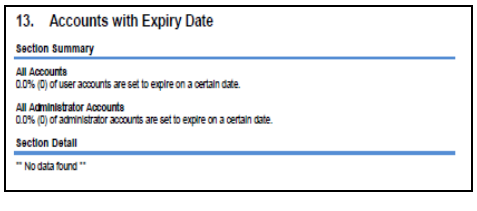
user yang tidak boleh mengganti password. Resiko yang dihadapi pada user ini terhitung rendah, dan pelaksanaan fungsinya secara general.



Gambar 18. *User not allowed change password*

xi. Report user yang sudah kadaluarsa

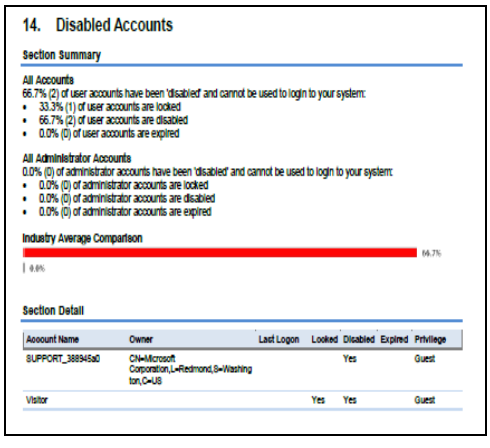
Pada tampilan ini menjelaskan hasil analisa untuk user-user yang accountnya sudah kadaluarsa, dan harus diupdate apabila user masih diperbolehkan mengakses system. Secara praktis dimana sebaiknya untuk menjaga keamanan system memang sebaiknya ditentuka batas waktu seorang user dalam system tersebut.



Gambar 19. *Account expired date*

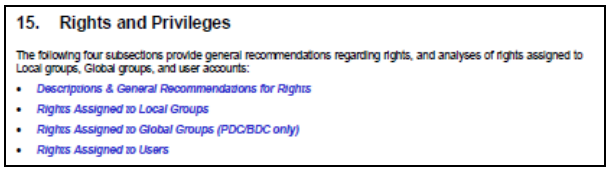
xii. Report Account yang tidak diaktifkan

Tampilan ini menjelaskan berapa jumlah user account yang di nonaktifkan dan tidak bisa mengakses system, hingga di resechedul kembali oleh administrator.



Gambar 20. Report hak akses dan privacy

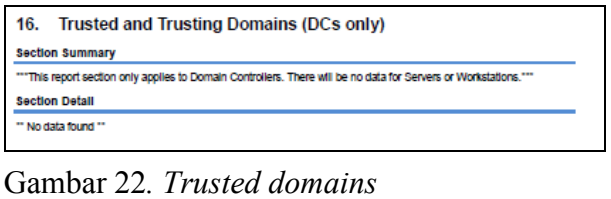
Tampilan ini menjelaskan hak-hak akses setiap user dalam system dan hak privacy apa saja yang mereka dapatkan pada system.



Gambar 21. *Right and Priveleges*

xiii. Report Kepercayaan akses domain

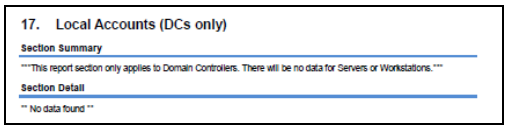
Tampilan ini menjelaskan user yang dapat menggunakan sumber daya (data) pada system berdasarkan domain yang dipercayakan. Penentuan hak ini dilakukan secara standard oleh system bagi setiap user.



Gambar 22. *Trusted domains*

2.2.16 Report Lokal User / account

Tampilan ini menjelaskan tentang hak akses yang diberikan oleh domain kepada user yang regular account nya tidak termasuk didalam trusted domain, mungkin ditentukan oleh network domain. Pada laporan ini tidak terdapat hak report yang termasuk dalam domain.


17. Local Accounts (DCs only)

Section Summary

"""This report section only applies to Domain Controllers. There will be no data for Servers or Workstations."""

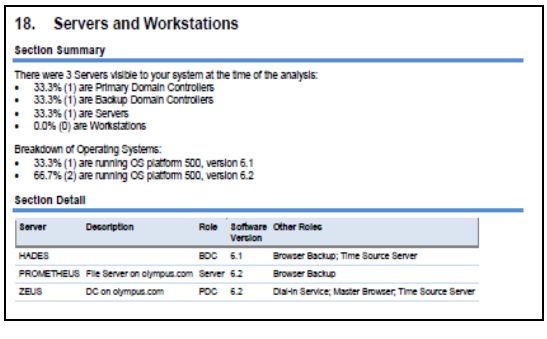
Section Detail

** No data found **

Gambar 23. *Local accounts summary*

2.2.17 Report Server dan workstation

Pada tampilan ini menjelaskan ketersediaan server pada system yang tersedia di jaringan serta pelayanan apa saja yang disediakan oleh masing-masing server tersebut.


18. Servers and Workstations

Section Summary

There were 3 Servers visible to your system at the time of the analysis:
- 33.3% (1) are Primary Domain Controllers
- 33.3% (1) are Backup Domain Controllers
- 33.3% (1) are Servers
- 0.0% (0) are Workstations

Breakdown of Operating Systems:
- 33.3% (1) are running OS platform 500, version 6.1
- 66.7% (2) are running OS platform 500, version 6.2

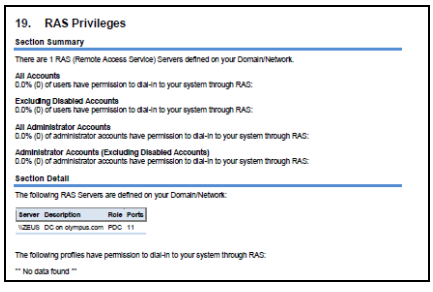
Section Detail

Server	Description	Role	Software Version	Other Roles
HADES		BDC	6.1	Browser Backup; Time Source Server
PROMETHEUS	File Server on olympus.com	Server	6.2	Browser Backup
ZEUS	DC on olympus.com	PDC	6.2	Dial-in Service; Master Browser; Time Source Server

Gambar 24. *Server and workstation summary*

2.2.18 Report RAS Priveleges

Laporan ini menjelaskan Remote Access Service (RAS) yang disediakan oleh domain system , hal ini akan memberi pelayanan bagi user untuk mengakses system secara jarak jauh menggunakan modem.


19. RAS Privileges

Section Summary

There are 1 RAS (Remote Access Service) Servers defined on your Domain/Network.

All Accounts
0.0% (0) of users have permission to dial-in to your system through RAS:

Excluding Disabled Accounts
0.0% (0) of users have permission to dial-in to your system through RAS:

All Administrator Accounts
0.0% (0) of administrator accounts have permission to dial-in to your system through RAS:

Administrator Accounts (Excluding Disabled Accounts)
0.0% (0) of administrator accounts have permission to dial-in to your system through RAS:

Section Detail

The following RAS Servers are defined on your Domain/Network:

Server	Description	Role	Ports
\\ZEUS	DC on olympus.com	PDC	11

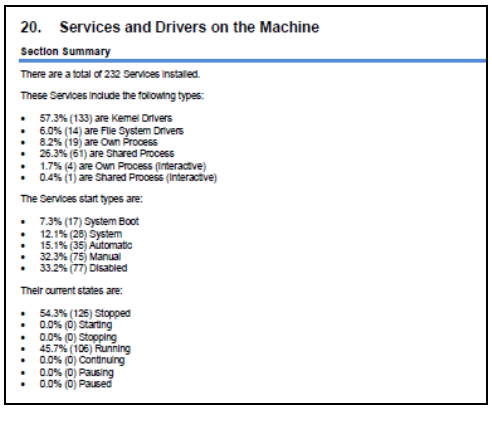
The following profiles have permission to dial-in to your system through RAS:

** No data found **

Gambar 25.*RAS priveleges*

2.2.19 *Report Services and Drivers* pada mesin

Tampilan ini menjelask smua pelayanan dan driver yang tersedia didalam system secara rinci.


20. Services and Drivers on the Machine

Section Summary

There are a total of 232 Services installed.

These Services include the following types:
- 57.3% (133) are Kernel Drivers
- 6.0% (14) are File System Drivers
- 8.2% (19) are Own Process
- 26.3% (61) are Shared Process
- 1.7% (4) are Own Process (Interactive)
- 0.4% (1) are Shared Process (Interactive)

The Services start types are:
- 7.3% (17) System Boot
- 12.1% (28) System
- 15.1% (35) Automatic
- 32.3% (75) Manual
- 33.2% (77) Disabled

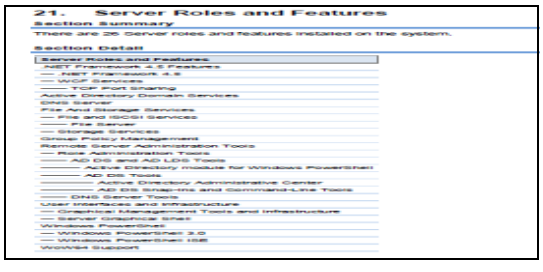
Their current states are:
- 54.3% (126) Stopped
- 0.0% (0) Starting
- 0.0% (0) Stopping
- 45.7% (106) Running
- 0.0% (0) Continuing
- 0.0% (0) Pausing
- 0.0% (0) Paused

Gambar 26.*Services and Drivers summary*

2.2.20 Peranan dan fitur pada server

Tampilan ini menjelaskan apa saja peran server dalam domain system serta fitur-fitur yang tersedia khususnya dalam mendukung proses. Apabila terdapat fitur services dan driver yang tidak layak pada system akan memberikan celah dan media bagi penyusup ke dalam system. Untuk itu

laporan ini cukup penting untuk dianalisa secara teliti.

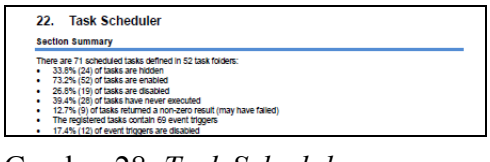


Gambar 27. *Server Roles and Features*

2.2.21 Report Penjadwalan Tugas

Tampilan ini menjelaskan tentang penjadwalan tugas/proses dalam pemeliharaan system serta mendiagnosa fungsi secara regular, adapun jenis penjadwalan yang dilakukan antara lain:

- *Create regular system protection points*
- *Download and install anti virus*
- *Synchronize system time*



Gambar 28. *Task Scheduler summary*

IV. SIMPULAN

Evaluasi yang telah dilakukan pada pada penggunaan Teknologi Informasi di PT. BFI.Tbk. cenderung menggunakan Metode Audit Arround the computer, karena dalam proses evaluasi, peneliti hanya dapat melihat semua aspek diluar system, seperti konfigurasi user, logging jaringan , dan semua aspek yang sudah dijelaskan pada Bab V.

Penggunaan Sekchek dalam proses evaluasi kinerja jaringan pada PT. BFI Tbk. Ini terdapat 22 point khusus yang di analisa secara detail oleh aplikasi tersebut, dann berdasarkan hasil tersebut maka peneliti menyimpulkan bahwa setiap kategori memiliki derajat resiko masing-masing, penjelasan dapat dilihat pada table dibawah.

Tabel 3 Hasil Analisa resiko keamanan system

Section	Description	Risk Rating
1	User Account	NA
2	System Account Policy	NA
3	Audit Policy Setting	NA
4	Registry Key Values	Low
5	User Account Defined	Medium
6	Local Groups and Members	Medium
7	Global Groups	Medium
8	Last Logon in 30 days	Low
9	Passwords 30 days older	Medium
10	Passwords Never expires	Medium
11	Invalid Logon	Low
12	Users not allowed change Password	Medium
13	Account with Expire Date	Low
14	Disabled Account	NA
15	Right and Privileges	Medium
16	Trusted and Trusting Domain	Medium
17	Local Accounts	Low
18	Servers and Workstations	Medium
19	Remote Access Service	Medium
20	Services and Drivers on the Machine	Medium
21	Servers Role and Features	Medium
22	Task Scheduler	Low

Berdasarkan hasil dari table ini dan didukung data dari Sekcheck Network Evaluator maka peneliti memberikan laporan tersebut kepada pihak pimpinan baik CIO maupun CEO untuk diproses tindakan selanjutnya.

Dari hasil penggunaan aplikasi Sekcheck Network Evaluator ini, maka peneliti memberikan saran dan rekomendasi antara lain sebagai berikut

Adanya penelitian selanjutnya berdasarkan hasil dari penelitian ini, yang berhubungan dengan peningkatan kinerja jaringan dalam pengendalian keamanan data.

Sebaiknya hasil yang didapat pada penelitian ini dapat dijadikan dasar bagi pihak pimpinan di PT. BFI.Tbk. dalam proses pengendalian jaringan pada infrastruktur Teknologi Informasi terutama untuk kategori point dengan indicator resiko yang “medium”

DAFTAR PUSTAKA

[1] R. J. W. Weill Peter., IT Governance: How Top Performers Manage IT Decision Rights for Superior Result, Harvard Business School Press, 2004.

[2] T. Sutabri, Analisa Sistem Informasi, Andi , 2003, Jakarta: Andi Offset, 2003.

[3] "Horus FInance," Horus Development FInance, 10 12 2010. [Online]. Available: http://www_horus_df_com/index_php?id=882 . [Accessed 12 12 2013].

[4] "Auditing IT," Jacksonville State University, [Online]. Available: www.jsu.edu/ccba/fea/.../301_ch_13.ppt

[5] D. Cameron, "A Strategic Guide to The Pratical Business Application of Optical Network," Optical Networking, 2001. [Online]. Available: http://www.amazon.com. [Accessed 18 April 2014].

[6] D. D. V.P Gullati, "Information System Audit and Assurance," in *Case Studies and Checklist from The Banking Industry*, USA, Tata Mc Grahill, 2005, p. 205.

[7] I. K. M. C. Minoli D, Network Infrastructure and Architecture, Wiley Interscience, 2008.

[8] "Sekcheck Network Evaluator," Sekcheck Network Evaluator Security Evaluator, [Online]. Available: http://www.sekchek.com/Sekcheck Network Evaluator-at-aglnace.pdf. [Accessed 13 april 2014].