

УДК-004

## КИБЕРБЕЗОПАСНОСТЬ. УСИЛЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

## Чуриев Максат Меретмухаммедович

Старший преподаватель, кандидат технических наук, Международного университета нефти и газа имени Ягшыгелди Какаева г. Ашхабад Туркменистан

## Сопыева Огульбайрам

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева г. Ашхабад Туркменистан

## Ишангулыев Гуванч

Студент, Международного университета нефти и газа имени Ягшыгелди Какаева г. Ашхабад Туркменистан

Когда вы начинаете планировать развертывание своей политики и решать, какие параметры следует изменить, чтобы лучше защитить компьютеры, вы усиливаете их защиту, чтобы уменьшить вектор атаки. Вы можете применять принципы стандарта списка типовых конфигураций (ССЕ) для своих компьютеров.

Для оптимизации развертывания вам также следует рассмотреть возможность использования базовых показателей безопасности. Это может помочь вам лучше управлять не только аспектом безопасности компьютера, но и его соответствием политике компании. Для платформы Windows вы можете использовать Microsoft Security Compliance Manager (рис.1).

На панели слева у вас есть все поддерживаемые версии операционной системы и приложения.



Используем Windows Server 2012 в качестве примера. Как только вы нажмете на опцию с названием этой операционной системы, то вызовете различные роли для этого сервера.

Используя в качестве примера шаблон WS2012 Web Server Security 1.0, вы увидите набор из 203 уникальных настроек, которые улучшат общую безопасность сервера.

Tę.			Microsoft Security Compliance	Manager					×
File	View Help							Glob	al setting search
~ ~ ~ ~	Exchange Server 2007 SP3 Exchange Server 2010 SP2 Internet Explorer 10 Internet Explorer 8	<	WS2012 Web Server Security 1.0  Advanced View	•	Import GPO Backup (folder) SCM (.cab)				
	Internet Explorer 9 Microsoft Office 2007 SP2 Microsoft Office 2010 SP1 Windows 7 SP1 Windows 8 Windows Server 2003 SP2 Windows Server 2008 R2 SP1		Anne System Services 203 Setting(s) Peer Networking Identity Manager Windows Driver Foundation - User-moc Power Performance Counter DLL Host SSDP Discovery	Not Defined Manual Automatic Manual Disabled	Not Defined Manual Automatic Manual Disabled	Not Defined Manual Automatic Manual Disabled	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	•	Export Excel_ia/sm) GPO_Backup_(folder) SCAP_v1.0_icab) SCCM_DCM_2007_ica SCM_icab) Baseline
> <b>4</b>	Windows Server 2008 SP2 Windows Server 2012 Attachments \ Guides WS2012 AD Certificate Services Server Security 1.0 WS2012 DHCP Server Security 1.0 WS2012 DNS Server Security 1.0 WS2012 Domain Controller Security Compliance 1.0		Background Intelligent Transfer Service Encrypting File System (EFS) TCP/IP NetBIOS Helper Hyper-V Time Synchronization Service Remote Desktop Licensing Workstation	Manual by default Not Defined Automatic Not Defined Automatic Manual	Automatic Manual Automatic Manual Not Defined Automatic	Automatic Manual Automatic Manual Not Defined Automatic	0 0 0 0 0 0	~	Compare / Merge Delete Duplicate Properties Setting
A 4	WS2012 Domain Security Compliance 1.0 WS2012 Domain Security Compliance 1.0 WS2012 Hyper-V Security 1.0 WS2012 Member Server Security Compliance 1.0 WS2012 Network Policy and Access Services Security 1.0 WS2012 Print Server Security 1.0 WS2012 Remote Desktop Services Security 1.0 WS2012 Remote Desktop Services Security 1.0 WS2012 Remote Desktop Services Security 1.0 WS2012 Web Server Security 1.0 Windows Vista SP2 Windows XP SP3		Microsoft Software Shadow Copy Provis Peer Name Resolution Protocol Windows Internal Database Server For NIS Smart Card Removal Policy Hyper-V Heartbeat Service Data Deduplication Service User Access Logging Service Software Protection Thread Ordering Server	Manual Not Defined Not Defined Manual Not Defined Not Defined Automatic Manual	Manual Not Defined Not Defined Manual Manual Not Defined Automatic Automatic Manual	Manual Not Defined Not Defined Manual Manual Not Defined Automatic Automatic Manual	0 0 0 0 0 0 0 0 0	*	Setting Group Help About Help Topics Release Notes Send Feedback Privacy Statement
0	ther Baselines	-	15 111				1	e	

Чтобы увидеть более подробную информацию о каждом параметре, вы должны нажать на имя конфигурации в панели справа (рис.3).

У всех параметров будет одинаковая этих описание, структура: сведения, уязвимость, потенциальное воздействие дополнительные и контрмеры. Эти предложения основаны на стандарте ССЕ, который является отраслевым стандартом для базовой конфигурации безопасности. После того как вы определили шаблон, который лучше всего подходит для вашего сервера / рабочей станции, вы можете развернуть его через GPO.

Background Intelligent Transfer Service Manual by default Automa	tic Automatic Optiona Computer Configuration\Windows S							
Collapse     Severity:     Opt       Value must be equal to Automatic.     Comments:     Opt       Customize setting value     Automat     Comments:       Setting Details     Setting Details	ional Customize this setting by duplicating the baseline							
UI Path:	-							
Computer Configuration\Windows Settings\Security Settings\Syste Description:	m Services Vulnerability:							
Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information. Additional Details:	Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows that are not installed during a default installation of the operating system. Depending on the version of Windows and the operating system.							
CCE-23764-4 HKLM\SYSTEM\CurrentControlSet\services\BITS\Start REG_SZ:2	Windows you can add these optional services to an existing computer through Add/Remove Programs in Control Panel, Programs and Features in Control Panel, Server Manager, or the Configure Your Server Wizard. Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.							
	Potential Impact:							
	If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment. It is also nocsible to alter the access control list (ACL) for a service, however							

Когда защита объекта усиливается, необходимо убедиться, что вы используете все возможности операционной системы для значительного повышения уровня безопасности компьютера. Для систем Windows вам следует рассмотреть возможность использования набора инструментов Enhanced Mitigation Experience Toolkit (EMET).

EMET помогает предотвратить доступ злоумышленников к вашим компьютерам, предвидя и предотвращая наиболее распространенные методы, используемые ими для эксплуатации уязвимостей в системах Windows. Это не только инструмент обнаружения.

Он осуществляет защиту путем перенаправления, прекращения, блокировки и аннулирования действий злоумышленника. Одним из преимуществ использования EMET для защиты компьютеров является возможность блокировать новые и неизвестные угрозы.

^			Enhanced Mitigal	tion Experience	- Toolkit			- [		×
Import	59		Quick Profi	e Name:	Windows Eve	ent Log	0	0		
Export			Custom se	curity settings	~	Tray Icon				
Group Policy	Wizard	Apps Tri	Skin: Office	2013		Early Warnin	0	Hel	9	
Fie		Configurati	on Sys	tem Settings		Reporting		Info	15	
ystem Status										
Data Exe	cution Prev	ention (DEP)				A4	plication	Opt In		
Structure	d Exception	Handler Over	write Protection (SE	EHOP)		N 14	plication	Opt In		
Address Space Layout Randomization (ASLR)								plication Opt In		
Certificate Trust (Pinning) Ena								abled		
Block Unt	rusted Font	ts (Fonts)				×	ways On			
mains Process										
Process ID	Process	Name					Runnin	O EMET	1	
3300	AmoltoR	ecorder - Amol	to Call Recorder for	Skype				0	- 5	~
12200	Applicati	onFrameHost -	Application Frame	Host				-		
45.16	armsvc -	Adobe Acroba	t Update Service							
43.50	5624 atiectxx - AMD External Events Client Module									
5624			Evente Cervice M	odule						
5624 2844	atesrix	<ul> <li>AMD Externa</li> </ul>	a cryenta pervice Pk							
5624 2844 21500	atiesrxx audiodg	<ul> <li>AMD Externa</li> <li>Windows Aut</li> </ul>	to Device Graph Is	olation						
5624 2844 21500 11316	atiesrxx audiodg backgrow	<ul> <li>AMD Externa</li> <li>Windows Aut undTaskHost -</li> </ul>	to Device Graph Is Background Task H	olation ost						
5624 2844 21500 11316 12664	atiesrxx audiodg backgrow browser	<ul> <li>AMD Externa</li> <li>Windows Aut undTaskHost - _broker - Brow</li> </ul>	io Device Graph Is Background Task H ser_Broker	olation lost						~

В разделе System Status (Состояние системы) показаны настроенные решения проблем безопасности. Хотя идеальный сценарий – это включение их всех, данная конфигурация может варьироваться в зависимости от потребностей каждого компьютера. В нижней части экрана показано, какие процессы были включены. В предыдущем примере только 1 приложение поддерживало ЕМЕТ. ЕМЕТ работает путем внедрения DLL в пространство памяти исполняемого файла, поэтому при настройке нового процесса для защиты с помощью ЕМЕТ вам нужно будет закрыть приложение и открыть его снова (то же самое относится и к службам).

Чтобы защитить еще 1 приложение из списка, щелкните по нему правой кнопкой мыши и выберите Configure Process (Настроить процесс).

• •						Ap	oplicatio	n Config	guration								- 0	×	
Export	Export Selected	Add Application	Add Wildca	Show Full Show All Show Group Path Settings Policy Apps					Stop on exploit     Audit only			y y	Deep Hooks     Anti Detours     Banned Functions						
File Add / Remove							Options D					Default Action			Mitigation Settings				
Enter	text to sear	rch	1	DEP	SEH	V Null	Fir Hea	EAF	Clea	r Ma	Bot	Loa	Me	Caller	Sim	Sta	ASR	Fonts	
Amolt	toRecorder.	exe																	
arms	vc.exe			4	~	~	~	~		~	~	~	~	~	~	~			

В окне Application Configuration (Конфигурация приложения) вы выбираете меры, которые хотите включить для этого приложения.