Отчет тестирование уязвимостей

Оглавление

Постановка задачи 1

Удаленная проверка 1

Проведение тестов проникновения под пользователем 2

Проверка системы при наличии прав локального администратора 4

Общие рекомендации 12

Постановка задачи

Компьютер: xx.xx.xx.xx

ОС: Windows 8.1 Профессиональная

Пользователи: user – привилегии пользователя; admin – входит в группу локальных администраторов.

Удаленная проверка

С помощью программы XSpider (сетевой сканер безопасности, программное средство сетевого аудита, предназначенное для поиска уязвимостей на серверах и рабочих станциях) проведена проверка уязвимостей системы, в результате проверке были обнаружены открытые порты:

25 /tcp –smtp

110/tcp – pop3

119/tcp – nntp

143/tcp –imap

563/tcp – nntps

993/tcp –imaps

993/tcp – pop3s

3389/tcp - MsRDP

Данный перечень портов минимальный и является допустимым.

Проведение тестов проникновения под пользователем

Для теста использовались привилегии пользователя user.

В начале бы произведен Quick test. Этот тест показывает, насколько уязвим ваш компьютер к различным интернет-угрозам. Этот тест сочетает Advanced Port Scanner, браузер и тест троянов. Результат проведения быстрого теста:

Проверка на наличие уязвимостей вашей компьютерной системы от удаленных атак

Мы отсканировали систему на наличие открытых портов и портов видимых для других в Интернете. Как правило, открытый порт означает, что ваш компьютер уязвимым для атак взломщиков. Они получают доступ к вашему компьютеру и его файлам через эти открытые порты.

Безопасно!

Проверка «Троянский конь»

Тест сканирования системы, чтобы найти признаки трояна. Если троянский конь на вашем компьютере, злоумышленник может получить доступ в вашим системным файлам и личным данным.

Безопасно!
Не найдено признаков «Троянов» в Вашей системе.

Рекомендации:
Отсутствие троянского коня в вашей системе не означает, что эта проблема не может произойти. Антивирусная и / или анти-Trojan программное обеспечение должно быть установлено и использоваться в вашей системе.

Если вы уже используете этот тип программного обеспечения в вашей системе, её определения вирусов (баз данных вирусов) должны регулярно обновляются.

Браузер проверка конфиденциальности

Тест проверяет, показывает веб-браузер любую личную информацию при посещении веб-сайтов. Обычно такая информация: последний посещенный сайт , Ваша локаль и кто ваш интернет-провайдер.

Предупреждение!
Во время посещения веб-сайтов, Ваш браузер показывает личную информацию о вас и вашем компьютере. Он посылает информацию о предыдущих посещенных вами сайтов. Он также может сохранить специальные куки на вашем жестком диске, цель которых узнать ваши привычки в то время как вы веб-серфите.

Рекомендации:
Мы советуем вам использовать брандмауэр. Если у вас уже есть брандмауэр настроить его, чтобы блокировать распространение такой информации.

Результаты Stealth теста

Используем этот тест, чтобы определить, ваш брандмауэр успешно скрывает системные порты.

Мы направили следующие пакеты по TCP:

- TCP ping packet
- TCP NULL packet
- TCP FIN packet

- TCP XMAS packet
- UDP packet

Вот описание возможных результатов для каждого отправленного пакета:
"Stealthed" - Означает, что ваша система (брандмауэр) уже успешно прошли испытание не отвечая на пакеты, которые мы послали к нему.
"Non-stealthed" - Означает, что ваша система (брандмауэр) ответил на пакете которые мы послали к нему. Что важнее, то, что это также означает, что ваш компьютер виден для других в Интернете, что может быть потенциально опасными.

Packet' type	Status
TCP "ping"	stealthed
TCP NULL	stealthed
TCP FIN	stealthed
TCP XMAS	stealthed
UDP	stealthed

Рекомендации:

Ваш компьютер невидимым для других в Интернете!

Browser тест

Проверка Cookies

 Ваш компьютер может сохранить специальные cookies на вашем жестком диске, которые имеют цель направлять рекламу или узнать ваши привычки в то время как вы серфите.

Рекомендации

Мы советуем вам использовать персональный брандмауэр и / или анти-шпионское программного обеспечения.
Если у вас уже есть брандмауэр или защиты от шпионских программ настроить его блокировать куки. Вы можете также блокировать куки с помощью браузера, если он поддерживает функцию блокировки куки.

 Во время посещения веб-сайтов, Ваш браузер показывает личную информацию (так называемый «'referrer'») о предыдущих посещенных вами сайтов.

Рекомендации

Если у вас уже есть брандмауэр настроить его, чтобы блокировать распространение такой информации (реферера).

Trojans тест

Мы отсканировали порты вашего компьютера, используемые наиболее опасных и распространенных троянских коней. Вот описание статусов возможных портов:

"Stealthed"(by a firewall) - Означает, что ваш компьютер невидимым для других в Интернете и защищен брандмауэром или другим похожим программного обеспечения;
"Closed" (non-stealthed) - означает, что этот порт закрыт, но ваш компьютер виден для других в Интернете, что может быть потенциально опасным;
"Open" - Означает, что этот порт готов установить (или уже установил) соединение с удаленным адресом. Это также означает, что ваш компьютер уязвимым для атак и можно было бы уже взломан или заражен trojan/backdoor;

Trojan:	Port	Status
GiFt	123	stealthed
Infector	146	stealthed
RTB666	623	stealthed
Net-Devil	901	stealthed
Net-Devil	902	stealthed
Net-Devil	903	stealthed
Subseven	1243	stealthed
Duddies Trojan	1560	stealthed
Duddies Trojan	2001	stealthed
Duddies Trojan	2002	stealthed
Theef	2800	stealthed
Theef	3000	stealthed
Theef	3700	stealthed
Optix	5151	stealthed
Subseven	6776	stealthed
Theef	7000	stealthed
Phoenix II	7410	stealthed
Ghost	9696	stealthed
GiFt	10100	stealthed
Host Control	10528	stealthed
Host Control	11051	stealthed
NetBus	12345	stealthed
NetBus	12346	stealthed
BioNet	12348	stealthed
BioNet	12349	stealthed
Host Control	15094	stealthed
Infector	17569	stealthed
NetBus	20034	stealthed
MoonPie	25685	stealthed
MoonPie	25686	stealthed
Subseven	27374	stealthed
BO	31337	stealthed
Infector	34763	stealthed
Infector	35000	stealthed

Все просканированные порты stealthed (возможно защищены фаерволом). Это означает, ваша система не заражена любой из этих Trojan horses.

Exploits тест

Ваша система успешно защищена от атак!

Проверка системы при наличии прав локального администратора

Анализатор Microsoft Baseline Security Analyzer (MBSA) — это простое в использование средство, помогающее малым и средним предприятиям определять их состояние безопасности в соответствии с рекомендациями корпорации Microsoft по безопасности и предлагать конкретные рекомендации по его улучшению. Улучшите процесс управления безопасностью, используя MBSA для обнаружения распространенных неверных настроек безопасности и отсутствующих обновлений безопасности в своих компьютерных системах.

Рекомендовано запустить MBSA, в отчете по сканированию будут рекомендации по устранению возможных предупреждений:

Report Details for WORKGROUP - C1 (2014-09-24 22:00:46)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\C1
IP address:	xx.xx.xx.xx
Security report name:	WORKGROUP - C1 (24.09.2014 22-00)
Scan date:	24.09.2014 22:00
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Security Updates

Score	Issue	Result
	Office Security Updates	31 security updates are missing. 1 service packs or update rollups are missing.

Security Updates

Score	ID	Description	Maximum Severity
Missing	MS14-036	Security Update for Microsoft Office 2007 suites (KB2878233)	Important
Missing	MS14-024	Security Update for Microsoft Office 2007 suites (KB2817330)	Important
Missing	MS12-066	Security Update for Microsoft Office InfoPath 2007 (KB2687440)	Important
Missing	MS07-042	Security Update for the 2007 Microsoft Office System (KB936960)	Important
Missing	MS13-072	Security Update for Microsoft Office 2007 suites (KB2760411)	Important
Missing	MS13-074	Security Update for Microsoft Office 2007 suites (KB2596825)	Important
Missing	MS12-034	Security Update for Microsoft Office 2007 suites (KB2596792)	Important
Missing	MS14-034	Security Update for Microsoft Office Word 2007 (KB2880515)	Important
Missing	MS12-030	Security Update for Microsoft Office 2007 suites (KB2597969)	Important

		Missing	MS14-024	Security Update for Microsoft Office 2007 suites (KB2880507)	Important
		Missing	MS13-072	Security Update for Microsoft Office 2007 suites (KB2597973)	Important
		Missing	MS12-057	Security Update for Microsoft Office 2007 suites (KB2596754)	Important
		Missing	MS12-028	Security Update for Microsoft Office 2007 suites (KB2596871)	Important
		Missing	MS11-094	Security Update for Microsoft Office PowerPoint 2007 (KB2596912)	Important
		Missing	MS09-005	Security Update for Microsoft Office Visio 2007 (KB957831)	Important
		Missing	MS13-106	Security Update for Microsoft Office 2007 suites (KB2850022)	Important
		Missing	MS14-034	Security Update for Microsoft Office 2007 suites (KB2880513)	Important
		Missing	MS07-025	Security Update for Office 2007 (KB934062)	Important
		Missing	MS14-024	Security Update for Microsoft Office 2007 suites (KB2880508)	Important
		Missing	MS13-085	Security Update for Microsoft Office Excel 2007 (KB2827324)	Important
		Missing	MS13-085	Security Update for Microsoft Office 2007 suites (KB2760591)	Important
		Missing	MS13-085	Security Update for Microsoft Office 2007 suites (KB2827326)	Important
		Missing	MS08-055	Security Update for the 2007 Microsoft Office System (KB951944)	Important
		Missing	MS13-085	Security Update for Microsoft Office 2007 suites (KB2760585)	Important
		Missing	MS12-046	Security Update for Microsoft Office 2007 suites (KB2596744)	Important
		Missing	MS13-002	Security Update for Microsoft Office 2007 suites (KB2687499)	Critical
		Missing	MS13-091	Security Update for Microsoft Office 2007 suites (KB2760415)	Important
		Missing	MS11-094	Security Update for Microsoft Office PowerPoint 2007 (KB2596764)	Important
		Missing	MS08-069	Security Update for Microsoft Office 2007 (KB951550)	Important
		Missing	MS13-094	Security Update for Microsoft Office Outlook 2007 (KB2825644)	Important
		Missing	MS14-036	Security Update for Microsoft Office	Important

		2007 suites (KB2881069)
		Update Rollups and Service Packs
		Score: Missing; ID: 2526086; Description: The 2007 Microsoft Office Suite Service Pack 3 (SP3)
		Current Update Compliance
		Score: Installed; ID: 949426; Description: Microsoft Office Accounting 2008 UK Service Pack 1 (KB949426)
		Score: Installed; ID: 949426; Description: Microsoft Office Accounting 2008 US Service Pack 1 (KB949426)
	SQL Server Security Updates	No security updates are missing.
		Current Update Compliance
		Score: Installed; ID: MS06-061; Description: MSXML 6.0 RTM Security Update (925673); Maximum Severity: Critical
	Windows Security Updates	No security updates are missing.
		Current Update Compliance
		Score: Installed; ID: 2894856; Description: Security Update for Microsoft .NET Framework 4.5.1 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2894856)
		Score: Installed; ID: MS14-053; Description: Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2977765); Maximum Severity: Important
		Score: Installed; ID: 890830; Description: Windows Malicious Software Removal Tool for Windows 8, 8.1 and Windows Server 2012, 2012 R2 x64 Edition - September 2014 (KB890830)
		Score: Installed; ID: MS14-052; Description: Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based Systems (KB2977629); Maximum Severity: Critical
		Score: Installed; ID: MS14-049; Description: Security Update for Windows 8.1 for x64-based Systems (KB2918614); Maximum Severity: Important
		Score: Installed; ID: 2981580; Description: Update for Windows 8.1 for x64-based

		Systems (KB2981580)		
Installed	MS14-041	Security Update for Windows 8.1 for x64-based Systems (KB2972280)	Important	
Installed	MS14-038	Security Update for Windows 8.1 for x64-based Systems (KB2971850)	Critical	
Installed	2962140	Security Update for Windows 8.1 for x64-based Systems (KB2962140)		
Installed	MS14-036	Security Update for Windows 8.1 for x64-based Systems (KB2964718)	Critical	
Installed	2987114	Security Update for Internet Explorer Flash Player for Windows 8.1 for x64-based Systems (KB2987114)		
Installed	MS14-030	Security Update for Windows 8.1 for x64-based Systems (KB2965788)	Important	
Installed	MS14-046	Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2966828)	Important	
Installed	MS14-054	Security Update for Windows 8.1 for x64-based Systems (KB2988948)	Important	
Installed	2973351	Security Update for Windows 8.1 for x64-based Systems (KB2973351)		
Installed	MS14-045	Security Update for Windows 8.1 for x64-based Systems (KB2993651)	Important	
Installed	MS14-031	Security Update for Windows 8.1 for x64-based Systems (KB2957189)	Important	
Installed	MS14-026	Security Update for Microsoft .NET Framework 4.5.1 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2931366)	Important	
Installed	MS14-047	Security Update for Windows 8.1 for x64-based Systems (KB2978668)	Important	
Installed	MS14-045	Security Update for Windows 8.1 for x64-based Systems (KB2976897)	Important	
Installed	MS14-051	Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based Systems (KB2976627)	Critical	
Installed	2939153	Update for Windows 8.1 for x64-based Systems (KB2939153)		
Installed	MS14-033	Security Update for Windows 8.1 for x64-based Systems (KB2939576)	Important	
Installed	MS14-039	Security Update for Windows 8.1 for x64-based Systems (KB2973201)	Important	

		Installed	2920189	Security Update for Windows 8.1 for x64-based Systems (KB2920189)	
		Installed	MS14-018	Windows 8.1 Update for x64-based Systems (KB2919355)	Critical
		Installed	MS14-040	Security Update for Windows 8.1 for x64-based Systems (KB2961072)	Important

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	Some user accounts (7 of 9) have non-expiring passwords. User UpdatusUser admin cyg_server maax user Администратор Гость
	Administrators	More than 2 Administrators were found on this computer. User admin cyg_server maax uplog Администратор
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. Connection Name — Firewall — Exceptions All Connections — On — Programs, Services Ethernet — On — Programs*, Services* Беспроводная сеть — On — Programs*, Services* Сетевое подключение Bluetooth — On — Programs*, Services*

	Incomplete Updates	No incomplete software update installations were found.
	Local Account Password Test	Some user accounts (3 of 9) have blank or simple passwords, or could not be analyzed. User / Weak Password / Locked Out / Disabled sshd / Weak / - / Disabled Администратор / Weak / - / Disabled Гость / Weak / - / Disabled UpdatusUser / - / - / - admin / - / - / - cyg_server / - / - / - maax / - / - / - uplog / - / - / - user / - / - / -
	File System	All hard drives (2) are using the NTFS file system. Drive Letter / File System C: / NTFS E: / NTFS
	Guest Account	The Guest account is disabled on this computer.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Automatic Updates	Updates are automatically downloaded and installed on this computer.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 8.1.
	Auditing	Logon Success and Logon Failure auditing are both enabled.

	Shares	3 share(s) are present on your computer. Share: ADMIN$ — Directory: C:\Windows — Share ACL: Admin Share — Directory ACL: NT SERVICE\TrustedInstaller - F, NT AUTHORITY\СИСТЕМА - RWXD, BUILTIN\Администраторы - RWXD, BUILTIN\Пользователи - RX, ЦЕНТР ПАКЕТОВ ПРИЛОЖЕНИЙ\ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ - RX Share: C$ — Directory: C:\ — Share ACL: Admin Share — Directory ACL: BUILTIN\Администраторы - F, NT AUTHORITY\СИСТЕМА - F, BUILTIN\Пользователи - R Share: E$ — Directory: E:\ — Share ACL: Admin Share — Directory ACL: BUILTIN\Администраторы - F, NT AUTHORITY\СИСТЕМА - F, NT AUTHORITY\Прошедшие проверку - RWXD, BUILTIN\Пользователи - RX
	Services	No potentially unnecessary services were found.

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones have secure settings for all users.

Общие рекомендации

В целом настройка безопасности компьютера на высшем уровне. Сторонний доступ ограничен, при этом политики локальных ограничения могут повлиять на удобство администрирования компьютера.

Присутствует несколько замечаний:

1. Отключить или защитить cookies.
2. Установить не достающие обновления безопасности ПО.
3. Установить срок действия пароля для пользователей.
4. Если имеется такая возможность оставить одного локального администратора.
5. Организовать шифрование RDP подключения

   Протокол удаленного рабочего стола является протокол, по которому Терминал Сервис предоставляет доступ удаленным пользователям. Он может быть использован для удаленного входа и взаимодействия с машиной ОС Windows.

   Поскольку RDP передает конфиденциальную информацию о пользователе и системе, он может быть сконфигурирована для использования шифрования для обеспечения конфиденциальности и целостности своих сессий. Можно настроить RDP использовать алгоритмы шифрования.

6. Включить NLA для RDP
   Microsoft Windows Network Authentication (NLA) это метод проверки подлинности, что повышает безопасность на сервере, требуя от пользователя аутентификации перед созданием сеанса. Этот режим нужен для того, что бы подключения по RDP до успешной аутентификации не создавали сессию на сервере и не расходовали ресурсов, - это защита от снижения производительности в результате подборов паролей на RDP.