Студент: Весна Петровска Индекс: 142027 Предмет: Мрежна безбедност

Лабораториска вежба број 3 - Зајакнување на вашите уреди

Зајакнување на безбедноста на лаптоп компјутер (Windows 10)

Апликациите се еден од главните извори на ранливости на компјутерските системи, особено оние кои не се ажурирани. Со цел да ја намалиме површината врз која се воопшто возможни напади, се препорачува да се ослободиме од софтверот кој не го користиме.

Bo Windows 10, деинсталација на апликации се прави преку Apps & features.



Од листата на инсталираните апликации ги одбираме оние кои не ги користиме и ги деинсталираме.

⊙™	Alarms & Cloc Microsoft Cor App Installer Microsoft Cor	Bonjour Please wait while Windows configures Bonjour Gathering required information	
ß	Bonjour Apple Inc. 1.0.106	6/7/2017	Cancel
		Modify Uninstall	

Деинсталација на апликација

Следно нешто што може да го направме е да ги исклучиме сервисите кои не ни се потребни.

=	₽ ₽ ₽	Filters 🗸				
			Services			
	Best match		File Action View Help			
ഹ						
	Services		Services (Local)			
۵	Deckton ann		Select an item to view its description. Name	Description State	us Startup Type	Log On As
	Desktop app		ActiveX Installer (AxInstSV	Provides Us	Manual	Local Syste
_	Apps		🖏 Adobe Acrobat Update Se	v Adobe Acro Run	ning Automatic	Local Syste
Ē	Аррз		🥋 Adobe Genuine Software I	1 Adobe Gen Run	ning Automatic	Local Syste
	Component Services		AdobeUpdateService	Run	ning Automatic	Local Syste
	Services		🖓 AllJoyn Router Service	Routes AllJo	Manual (Trig	Local Service
	Search suggestions		Andrea RT Filters Service	Andrea Serv Run	ning Automatic	Local Syste
	Search suggestions		Apache2.4	Apache/2.4 Run	ning Automatic	Local Syste
	O services - See web results		App Readiness	Gets apps re	Manual	Local Syste
	> Services - See web results		Application Identity	Determines	Manual (Trig	Local Service
	Settings (1)		Application Information	Facilitates t Runi	ning Manual (Trig	Local Syste
	Settings (i)		Application Layer Gateway	Provides su	Manual	Local Service
	Documents (15+)		AppX Deployment Service	Provides int	Disabled	Local Syste
			Auto Time Zone Opdater	Automatica	Manual	Local Service
			Background Tasks Infrastre	Windows in Run	ning Automatic	Local System
			Background Tasks Innovation Background Tasks Innovation	The Base Fil Run	ning Automatic	Local Service
			BitLocker Drive Encryption	BDESVC hos	Manual (Trig	Local Syste
			Block Level Backup Engine	The WBENG	Manual	Local Syste
			Bluetooth Handsfree Servi	e Enables wir	Manual (Trig	Local Service
			Reluetooth Support Service	The Bluetoo	Manual (Trig	Local Service
			🖏 Capability Access Manage	Provides fac	Manual	Local Syste
			🤐 Certificate Propagation	Copies user	Manual	Local Syste
			🔍 Client License Service (Cli	S Provides inf	Manual (Trig	Local Syste
£33			🔐 CNG Key Isolation	The CNG ke Run	ning Manual (Trig	Local Syste
			COM+ Event System	Supports Sy Run	ning Automatic	Local Service
			COM+ System Application	Manages th	Manual	Local Syste
<u></u>			Computer Browser	Maintains a Run	ning Manual (Trig	Local Syste
			Connected Devices Platfor	This service Run	ning Automatic (D	Local Service
	𝒫 services		Connected Devices Platfor	This user se Run	ning Automatic	Local Syste
	(D) 🥰 🚸 🖭	📒 🧿 🚣				

Пристап до Services преку менито

Листа на сервиси

Во колоната Description е даден опис за секој од сервисите, односно пишува за што служи и што ќе биде оневозможено доколку го исклучиме. Бидејќи јас немам принтер, сервисот *Print Spooler* не ми е потребен. Поради тоа можам да го стопирам и онеспособам овој сервис.

		manages porce porcy and por
🖏 Print Spooler		This service spools print jobs an
🌼 Printer Extensions	Start	service opens custom print
RintWorkflow_44	Stop	t Workflow
🌼 Problem Reports i	Pause	service provides support fo
🌼 Program Compat	Resume	service provides support fo
Quality Windows	Postart	ility Windows Audio Video E
🎑 Radio Manageme	Restart	io Management and Airplan
🎑 Realtek Audio Ser	All Tasks	> cooperation with Realtek au
🧠 Realtek Bluetooth	Defeash	
Remote Access A	Kerresh	ates a connection to a remot
🧟 Remote Access Co	Properties	hages dial-up and virtual priv
🧟 Remote Desktop (Lista	note Desktop Configuration
🧠 Remote Desktop	нер	ws users to connect interact





Онеспособување на автоматско вклучување сервисот

Следно нешто што треба да го направиме е да се осигураме дека имаме активен firewall и истиот е соодветно подесен. Во Windows 10 има вграден firewall – **Windows Defender Firewall**



Пристап до Windows Defender Firewall преку менито

Состојбата на Windows Firewall: активен

Може да извршиме детален преглед на сите правила, да додадеме нови (да блокираме или пропуштиме некоја апликација низ firewall-от), да избришеме постоечки правила, итн.

💣 Windows Defender Firewall witl	Inbound Rules						
🔣 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program ^
Connection Security Puler	Sirefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Program Files\Mozilla Firefox\firefox.e
Monitoring	Slaunch		Private	Yes	Block	No	C:\program files\openshot video editor\
2 wontoning	⊘ launch		Private	Yes	Block	No	C:\program files\openshot video editor\
	Lightworks Application		Private	Yes	Allow	No	C:\Program Files\Lightworks\ntcardvt.ex
	Ughtworks Application		Private	Yes	Allow	No	C:\Program Files\Lightworks\ntcardvt.ex
	🔮 mysqld		Private	Yes	Allow	No	C:\xampp\mysql\bin\mysqld.exe
	🔮 mysqld		Private	Yes	Allow	No	C:\xampp\mysql\bin\mysqld.exe
	🕑 naoqi-bin		Private	Yes	Allow	No	C:\program files (x86)\aldebaran robotic
	🕑 naoqi-bin		Private	Yes	Allow	No	C:\program files (x86)\aldebaran robotic
	🥑 Node.js: Server-side JavaScript		Private	Yes	Allow	No	C:\program files\nodejs\node.exe
	🥑 Node.js: Server-side JavaScript		Private	Yes	Allow	No	C:\program files\nodejs\node.exe
	🔮 packettracer7		Private	Yes	Allow	No	C:\program files\cisco packet tracer 7.0\
	🕑 packettracer7		Private	Yes	Allow	No	C:\program files\cisco packet tracer 7.0\
	🔮 Port 3306		All	Yes	Allow	No	Any
	🔮 python		Private	Yes	Allow	No	C:\python27\python.exe
	🔮 python		Private	Yes	Allow	No	C:\python27\python.exe
	Windows Live Communications Platform		All	Yes	Allow	No	C:\Program Files (x86)\Windows Live\Co
	Windows Live Communications Platform		All	Yes	Allow	No	Any
	🔮 Windows Live Communications Platform		All	Yes	Allow	No	Any
	🔮 μTorrent (TCP-In)		All	Yes	Allow	No	C:\Users\v\AppData\Roaming\uTorrent\
	🔮 μTorrent (UDP-In)		All	Yes	Allow	No	C:\Users\v\AppData\Roaming\uTorrent\
	🔇 @{Microsoft.Windows.CloudExperience	@{Microsoft.Windows.Clou	Domai	Yes	Allow	No	Any
	🧭 AllJoyn Router (TCP-In)	AllJoyn Router	Domai	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
	🔮 AllJoyn Router (TCP-In)	AllJoyn Router	Domai	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
	🧭 AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
	🧭 AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
	🧭 App Installer	App Installer	Domai	Yes	Allow	No	Any
	🔮 Cast to Device functionality (qWave-TCP	Cast to Device functionality	Private	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
	🔮 Cast to Device functionality (qWave-UDP	Cast to Device functionality	Private	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
< >	Cast to Daviso SSDD Discovery (LIDD, In)	Cart to Davisa functionality	Dublic	Ver	Allow	Ma	°/SurtamPaat9/\surtam??\surbart ava ↓

Листа на сите inbound правила	(во внатрешна насока)
-------------------------------	-----------------------

÷ g	·····				-
🔮 Lightwor	ks Application		Private	Yes	1
🔮 mysqld			Private	Yes	1
🔮 mysqld			Private	Yes	1
🔇 naoqi bir			Private	Yes	,
🕑 naoqi	Disable Rule		Private	Yes	1
🕑 Node	Cut		Private	Yes	1
🕑 Node	Comy		Private	Yes	1
🔮 packe	Сору		Private	Yes	1
🔮 packe	Delete		Private	Yes	1
🔮 Port 3	Properties		All	Yes	1
🔮 pytho			Private	Yes	1
🔮 pytho	Help]	Private	Yes	1
🕖 Windows	Live Communications Pla	atform	All	Yes	1
🕖 Windows	Live Communications Pla	atform	All	Yes	1
🕑 Windows	Live Communications Pla	atform	All	Yes	1
🔮 μTorrent	(TCP-In)		All	Yes	1
	Брише	ње на правило од листата			

Од клучно значење е софтверот на компјутерот секогаш да е ажуриран, особено оперативниот систем. Поради тоа треба да се осигураме дека **Windows Update** е активен и дека Windows ја има најновата верзија.

Windows Update

Update status



Your device is up to date. Last checked: Today, 3:26 AM

Check for updates

View installed update history

Проверка на статусот на Windows Update

Пожелно е да се подеси автоматска проверка за нови верзии и ажурирање на оперативниот систем со цел секогаш да ја имаме најновата верзија која ги содржи сите мерки против најновите безбедносни закани.

Исто така, многу е важно да инсталираме антивирусен софтвер и истиот да има ажурирани дефиниции. Бидејќи на овој компјутер има Windows 10 со кој доаѓа вграден **Windows Defender**, одлучив да не инсталирам друг.



Дефинициите на Windows Defender се ажурирани. Последното скенирање е пред 5 денови.

Пожелно е Windows Defender да е подесен автоматски да ги ажурира дефинициите и периодично да извршува скенирање на компјутерот.

Last scan

Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.

Last scan: 3/2/2018 (quick scan) No threats found. 25524 files scanned.

Краток преглед на последното скенирање

Зајакнување на безбедноста на безжична точка на поврзување (wireless access point)

Модерните рутери најчесто имаат web интерфејс за администрирање. До истиот може да се пристапи со локалната IP адреса на рутерот. Доколку не ја знаеме, може да се обидеме со преглед на излезот од командата **ipconfig**, во која може да се види кој е Default Gateway на нашиот компјутер, а тоа е најчесто адресата на рутерот.



Пристап до Command Prompt преку менито

Излезот од командата ipconfig



Во мојот случај адресата на рутерот е 192.168.0.1, па преку веб прелистувач пристапив до неговиот интерфејс за конфигурација.

Во зависност од моделот на рутерот, опциите ќе бидат различни но генерално ја следат истата шема. SSID е името на безжичната мрежа. Секогаш е потребно да се промени default вредноста бидејќи најчесто тоа е моделот на рутерот, што за напаѓачите може да биде голема предност ако го знаат (особено ако и лозинката за пристап е оставена на default вредноста). Следно, потребно е да се постави безбедносен режим, односно соодветен безбедносен протокол кој ќе нуди силна енкрипција. Денес, WPA2 е издржан стандард до кој се препорачува да се придржуваме и најбезбедната опција. Бидејќи на мојот рутер беше поставено WPA, го променив во WPA2. Исто така се препорачува да се користи безбедна лозинка, која содржи повеќе од 8 карактери, меѓу кои: големи и мали букви, специјални знаци и броеви.

Wireless Security Setup

Select SSID	▼
Security Mode	WPA - PSK(Recommended)
WPA Algorithms	AES(Recommended)
Security Key	
	Default: 12345678
WPS Settings	To configure a wireless security key, disable the WPS below! Oisable Disable Enable
	Reset OOB
	OK Cancel

Wireless Security Setup

Select SSID		T
Security Mode	WPA - PSK(Recommended)	*
WPA Algorithms	Disable Open Shared WPA - PSK(Recommended)	TKIP&AES
Security Key	WPA2 - PSK Mixed WPA/WPA2 - PSK	
	To configure a wireless security key, d	isable the WPS below!
WPS Settings	Oisable O Enable	
		Reset OOB
	OK Cancel	

Подесување на безбедносен протокол

За потребите на оваа вежба, ја тестирав МАС Filter опцијата на мојот рутер.

Со командата ipconfig /all ја дознав МАС адресата на мојот лаптоп, а потоа на рутерот подесив да се оневозможи пристап на сите други МАС адреси освен на таа.

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Description <u>Realtek RTL8723BE</u> 802.11 bgn Wi-Fi Adapter
Physical Address
DHCP Enabled Yes
Autoconfiguration Enabled : Yes
IPv4 Address
Subnet Mask
Lease Obtained Tuesday, March 6, 2018 11:02:22 PM
Lease Expires Wednesday, March 14, 2018 2:38:23 AM
Default Gateway
DHCP Server
DNS Servers
8.8.4.4

Access Control		
Select SSID		•
MAC Address Filter	Permit	T
MAC Address		Operate
		Add
	OK Cancel	

Сите останати МАС адреси ќе бидат блокирани

Се обидов да се конектирам на мрежата од мојот смартфон, и мојот обид беше неуспешен поради МАС филтрирањето кое го поставив на рутерот. Единствено беше можно да се пристапи од лаптопот чија МАС адреса е дозволена.

Ги тестирав и следните опции на рутерот:

Filter Mode	Forbid Only 🔻
Access Policy	(1)
Policy Name(Optional)	block_fb
Start IP	192.168.0. 104
End IP	192.168.0. 104
URL Character String	facebook.com
Time	0 • : 0 • ~ 0 • : 0 •
Day(s)	Sun 🔻 ~ Sat 🔻
Enable	Clear this item: Clear

Блокирање пристап до facebook.com на IP адресата соодветна на мојот смартфон