# HARDENING WINDOWS COMPUTERS

# **OVERVIEW**

- A. Automatic Updates
  - B. Encrypted File System
  - C. Configure Logging using Event Viewer
  - D. Disable Unused Services and Filter Ports



Image by rawpixel.com

# A. AUTOMATIC UPDATES

### **1.1 Windows Update**



- Quality updates include regular security patches and software updates
- Feature upgrades consist of new features and Windows functionality

Both types contain all previous updates, which helps reduce the chance that a hacker or malware attack might succeed in exploiting a mising update.

- Security updates are distributed on the second Tuesday of every month by Windows Update
- Configure Active Hours to set when updates should NOT be installed

#### **1.2 System Center Configuration Manager**



## **B. ENCRYPTED FILE SYSTEM**

Windows EFS utilizes encryption to enhance the security of files and directories. It is available for Windows 10 Pro / Enterprise / Education on NTFS volumes.
 Any other Windows edition will display Encrypt contents to secure data greyed out on a selected item as follows:
 Compress or Encrypt attributes
 Compress contents to save disk space
 Encrypt contents to secure data
 Details

The following items cannot be encrypted by EFS:

 Transactions
 Compressed Files
 System Files/Directories
 Root Directories

See here for more information.

# C. CONFIGURE LOGGING USING EVENT VIEWER

i Windows Event Viewer is used to access logs regarding system events.

Press Windows Key + R to open Run and type eventvwr.msc

Event Viewer				- 0	×
File Action View Help					
⇐⇒ 2 📰 🛛 🖬					
Event Viewer (Local)	Custom Views		Actions		
Custom Views     Administrative Events	Name	Description	Custom Views		-
> Windows Logs	Administrative Events	Critical, Error and Warning events from all administrative logs	🍯 Open Saved Log		
Applications and Services Logs			Y Create Custom View		
Subscriptions			Import Custom View		
			View		•
			Refresh		
r			I Help		•
			Administrative Events		•
			Open		_
			Properties		
			Help		
1					
-					

There are two types of log files:

- Windows Logs application, security, setup, system events
- Applications & Services Logs other logs from applications and services to record events

Create a custom view to monitor critical system events:

- 1. Under Action, click Create Custom View
- 2. On Filter tab, select Critical check box in Event Level

- 3. In By Log, expand Windows Logs with the down arrow and select only System
  - a. Click OK
- 4. Enter a name, such as System Critical Events and click OK
  - a. Your new custom view will now be located in the left pane under Custom Views

### D. DISABLE UNUSED SERVICES AND FILTER PORTS

i Open Services:						
<ol> <li>Press Win Key + R to</li> <li>Type services.msc</li> </ol>	open R	un				
	🖅 Run		×			
	Type resou	the name of a program, folder, document rce, and Windows will open it for you.	t, or Internet			
	<u>O</u> pen: servi	ices.msc	~			
		OK Cancel	Browse			
3. Press Enter						
Services						
File Action View Help						
	▶					
Services (Local) Services (Local)						
Select an item to view its	description.	Name	Description	Status	Startup Type	Log On As
		WpnUserService_43dc7	This service	Running	Automatic	Local System
		CDPUserSvc_43dc7	This user ser	Running	Automatic	Local System
		Windows Push Notifications	This service r	Running	Automatic	Local System

Each service's status indicates whether it is currently Running or not

Services should be managed accordingly with the purpose of a particular device. For example, if you were setting up a workstation to use a static IP address, you might disable the **DHCP Client** service.

### To disable a service and prevent it from starting up:

1. Right-click on the desired service to bring up a context menu

DHCP Client		Posistor	s an	Running	Automatic
DCOM Serve	Start		ML	Running	Automatic
DbxSvc	Stop		Ser	Running	Automatic
Cryptograph	Pause		thr	Running	Automatic
Corsair Servi	Resume		ervi	Running	Automatic
Corsair MSI F	Postart		UE	Running	Automatic
Corsair LLA S	Restart		UE	Running	Automatic
🎑 Corsair Gami	All Tasks	>		Running	Automatic
CoreMessag	Defeash		CO	Running	Automatic
Background	Refresh	_	inf	Running	Automatic
Sase Filtering	Properties		Filt	Running	Automatic
🖏 Windows Au			au	Running	Automatic
Windows Au	нер		au	Running	Automatic

- 2. Select Properties
- 3. Change Startup type to Disabled

DHCP Cli	ent Prope	erties (Loca	l Computer)	$\times$	
General	Log On	Recovery	Dependencies		
Service	name:	Dhcp			
Display name:		DHCP Clie	ent		
Description:		Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses			
Path to C:\WIN	executabl	e: stem32\svch	ost.exe -k LocalServiceNetworkRestricted -p		
Startup	type:	Automatic	· · ·		
7		Automatic Automatic Manual	c (Delayed Start)		
Service	status:	Disabled Running		1	
S	Start	Stop	Pause Resume		

- 4. Click **Stop** at the bottom to shutdown the service (if running)
- 5. Click **Apply** to save changes and then click **OK**

#### Find all open ports and connections in command prompt:

- 1. Go to Windows search and type cmd
- 2. Right-click to run as administrator



3. Type netstat -ab



Note: Output includes open network ports and related applications/services using them

#### **Close open ports using Windows Firewall:**

 Go to Start > type Windows Firewall > Open Windows Defender Firewall with Advanced Security



2. Once open, select Inbound Rules

Windows Defender Firewall with
 Inbound Rules
 Outbound Rules
 Connection Security Rules
 Monitoring

3. The panel on the right will now display the option to create a **New Rule** for incoming network traffic



4. Click New Rule and then select Port

Dula Tura		
кие туре		
Select the type of firewall rule to	create.	
Steps:		
Rule Type	What type of rule would you like to create?	
Protocol and Ports		
Action	O Program	
Profile	Rule that controls connections for a program.	
Name	Port	
	Rule that controls connections for a TCP or UDP port.	
	O Predefined:	
	@FirewallAPI.dll,-80200	~
	Rule that controls connections for a Windows experience.	
	O Custom	
	Cutanala	

- 5. Click Next at the bottom
- 6. Select **TCP** or **UDP** depending on the service you're trying to block. For this example, we will block Telnet, an unsecure service used to remotely interface into a system. Telnet uses port 23 and TCP

Does this rule apply to TCP or UDP	?
<ul><li>● TCP</li><li>○ UDP</li></ul>	
Does this rule apply to all local ports	s or specific local ports?
◯ All local ports	
Specific local ports:	23
	Example: 80, 443, 5000-5010
Click Next	
Select Block the conn	ection
What action should be take	n when a connection matches the specified conditions?
Allow the connection     This includes connection	<b>n</b> ns that are protected with IPsec as well as those are not.

#### O Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

- Block the connection
- 9. Click Next

7.

8.

10. A rule can be enforced over different connections as desired

When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

Since Telnet is unsecure, leave all selected to block it no matter the connection.

- 11. Click Next
- 12. Enter a name to recognize the rule and note documentation

	Name:
	Block Telnet
	Description (optional):
	Closed port 23 on Domain, Private, and Public connections.
213	iek Einieh

13. Click Finish