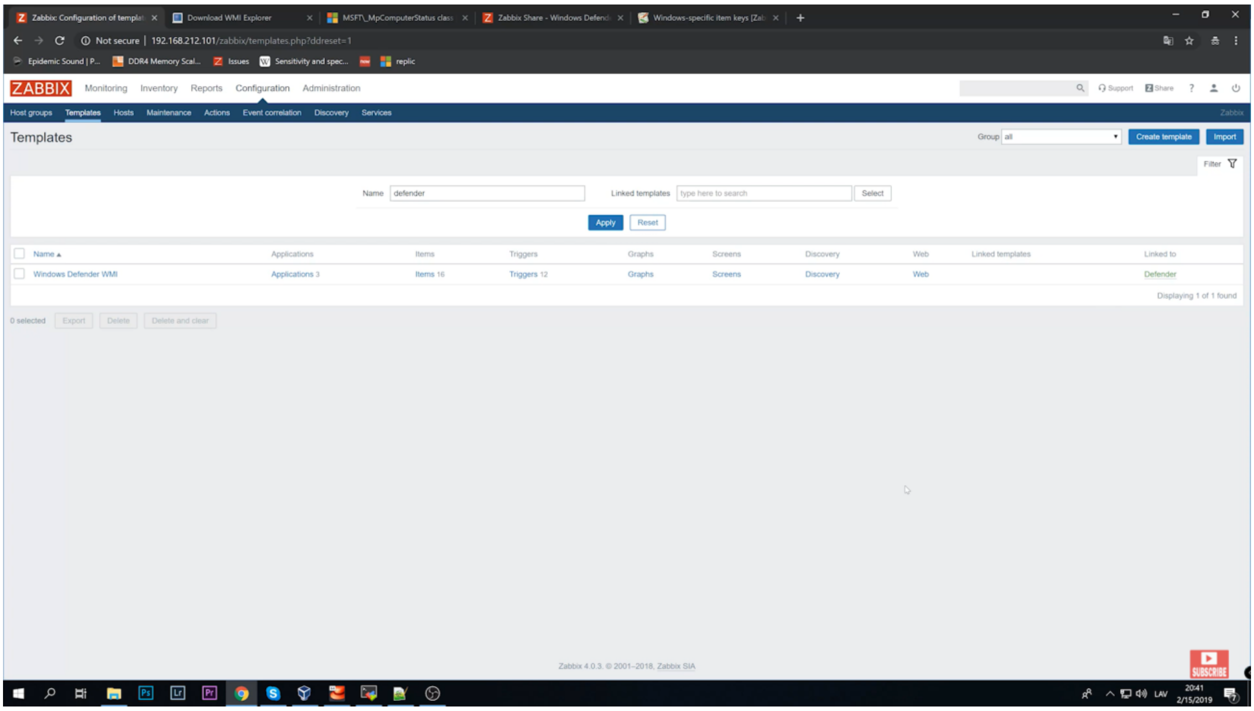
Laboratory work 15. Windows Defender Monitoring with ZABBIX

Aim of laboratory work: get to know how to configure security monitoring

Go to the following link and follow the instructions from the link:

https://www.youtube.com/watch?v=u8AC5EyFnu8



Not secure | 192.168.212.101/zabbix/templates.php?ddreset=1

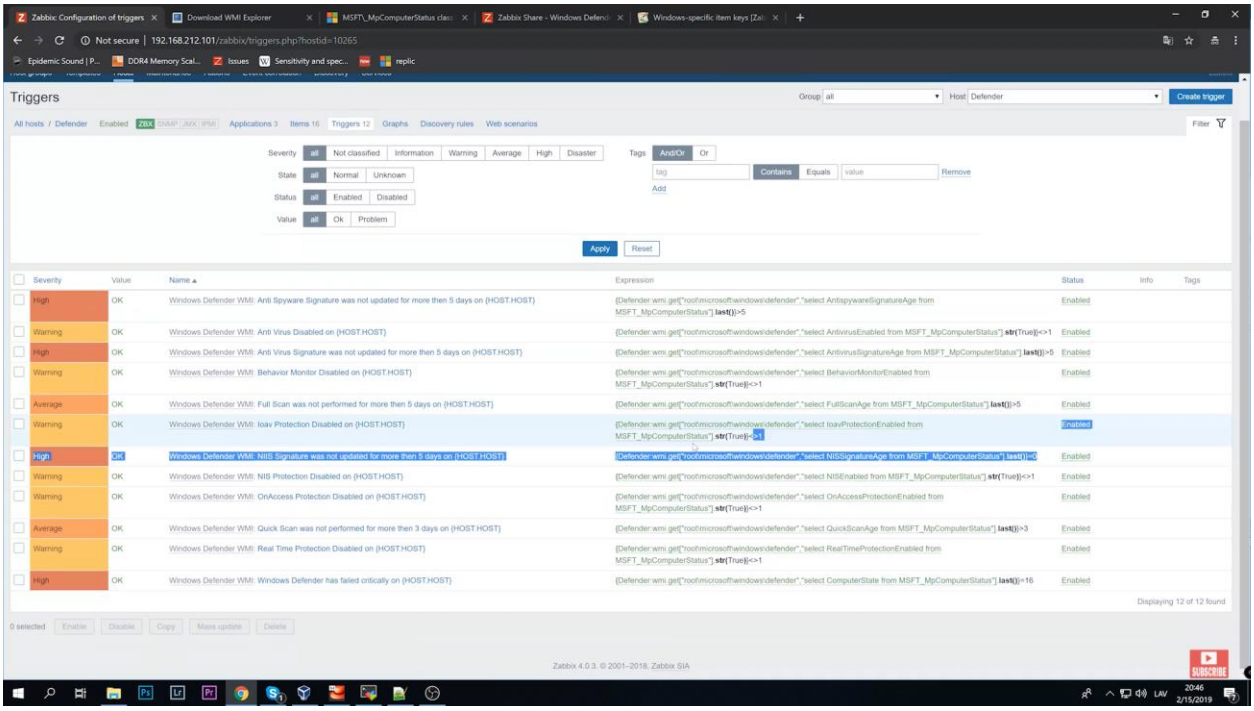
Templates

Name: defender

Name ▲	Applications	Items	Triggers	Graphs	Screens	Discovery	Web	Linked templates	Linked to
Windows Defender WMI	Applications 3	Items 16	Triggers 12	Graphs	Screens	Discovery	Web		Defender

Displaying 1 of 1 found

Zabbix 4.0.3. © 2001–2018, Zabbix SIA



Not secure | 192.168.212.101/zabbix/triggers.php?hostid=10265

Triggers

All hosts / Defender   Enabled   ZBX   Applications 3   Items 16   Triggers 12   Graphs   Discovery rules   Web scenarios

Group: all   Host: Defender

Severity	Value	Name ▲	Expression	Status	Info	Tags
High	OK	Windows Defender WMI: Anti Spyware Signature was not updated for more then 5 days on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select AntispywareSignatureAge from MSFT_MpComputerStatus"].last()}>5	Enabled		
Warning	OK	Windows Defender WMI: Anti Virus Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select AntivirusEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
High	OK	Windows Defender WMI: Anti Virus Signature was not updated for more then 5 days on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select AntivirusSignatureAge from MSFT_MpComputerStatus"].last()}>5	Enabled		
Warning	OK	Windows Defender WMI: Behavior Monitor Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select BehaviorMonitorEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
Average	OK	Windows Defender WMI: Full Scan was not performed for more then 5 days on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select FullScanAge from MSFT_MpComputerStatus"].last()}>5	Enabled		
Warning	OK	Windows Defender WMI: Ioav Protection Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select IoavProtectionEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
High	OK	Windows Defender WMI: NIIS Signature was not updated for more then 5 days on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select NISSignatureAge from MSFT_MpComputerStatus"].last()}>5	Enabled		
Warning	OK	Windows Defender WMI: NIS Protection Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select NISEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
Warning	OK	Windows Defender WMI: OnAccess Protection Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select OnAccessProtectionEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
Average	OK	Windows Defender WMI: Quick Scan was not performed for more then 3 days on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select QuickScanAge from MSFT_MpComputerStatus"].last()}>3	Enabled		
Warning	OK	Windows Defender WMI: Real Time Protection Disabled on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select RealTimeProtectionEnabled from MSFT_MpComputerStatus"].str(True)}<>1	Enabled		
High	OK	Windows Defender WMI: Windows Defender has failed critically on {HOST.HOST}	{Defender:wmi.get["root\microsoft\windows\defender","select ComputerState from MSFT_MpComputerStatus"].last()}=16	Enabled		

Displaying 12 of 12 found

Zabbix 4.0.3. © 2001–2018, Zabbix SIA

Zabbix: Configuration of triggers
Download WMI Explorer
MSFT_MpComputerStatus class
Zabbix Share - Windows Defend
Windows-specific item keys [Zab
Create trigger
Filter
Severity: all, Not classified, Information, Warning, Average, High, Disaster
State: all, Normal, Unknown
Status: all, Enabled, Disabled
Value: all, Ok, Problem
Tags: And/Or, Or
tag
Contains
Equals
value
Remove
Add
Apply
Reset
0 selected
Enable
Disable
Copy
Mass update
Delete
20:46
2/15/2019