Al Jokhadar-Mohammad-ISEC2022-As2

W0400411

“Configuring A Windows Firewall with PowerShell”

By Mohammad Al Jokhadar

# Script’s Contents

*<#*

*Filename    : FirewallScript1.ps1*

*Title       : Assignment 3*

*Name        : Mohammad Al Jokhadar*

*Script Start: Feb. 3rd , 2024*

*Last Revised: Feb. 3rd , 2024*

*#>*

*<#  Let us begin by defining the variables that we need to define: #>*

$SERVER1="192.168.4.2"

$TECHSUPPORT1="192.168.4.5"

$UPDATESERVER="192.168.4.7"

*<#  Next, Let us create the new Firewall Rule to allow SSH traffic! -DisplayName gives the rule a name , -Direction indicates if the packets are incoming or outgoing,*

*-Action indicates which action to take when the SSH packet arrives, -LocalPort indicates the port (which is 22 for SSH), and the -Protocol option indicates the protocol*

*to use :#>*

*New-NetFirewallRule* -DisplayName "techsupportssh" -Direction Inbound -RemoteAddress $TECHSUPPORT1 -LocalAddress "192.168.150.136" -Action Allow -LocalPort 22 -Protocol TCP

*<# Let us establish the two rules pertaining to FTP traffic! Let us establish the new rule involving connections from the virtual machine to SERVER1 : #>*

*New-NetFirewallRule* -DisplayName "serverftp" -Direction Outbound -RemoteAddress $SERVER1 -LocalAddress "192.168.150.136" -Action Allow -LocalPort 20,21 -Protocol TCP

*<# ... now for the second rule involving icoming FTP traffic from UPDATESERVER to our virtual machine : #>*

*New-NetFirewallRule* -DisplayName "updateftp" -Direction Inbound -RemoteAddress $UPDATESERVER -LocalAddress "192.168.150.136" -LocalPort 20,21 -Protocol TCP

*<# ... Let us enable active-connections' logging to the "allowedconnectionlog" file : #>*

*Set-NetFirewallProfile* -LogAllowed True -LogFileName "C:\Users\username\Documents\allowedconnectionlog.log"

# Script’s Output

Name : {f0751e60-b61f-4bfd-9ab0-2272178b27cc}

DisplayName : techsupportssh

Description :

DisplayGroup :

Group :

Enabled : True

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

RemoteDynamicKeywordAddresses :

Name : {f7e76390-7f05-4be7-8ba2-9a545131aeda}

DisplayName : serverftp

Description :

DisplayGroup :

Group :

Enabled : True

Profile : Any

Platform : {}

Direction : Outbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

RemoteDynamicKeywordAddresses :

Name : {61b3129e-db9a-47be-9ed3-48ccd0adddb9}

DisplayName : updateftp

Description :

DisplayGroup :

Group :

Enabled : True

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

RemoteDynamicKeywordAddresses :

# Log File’s Contents

#Version: 1.5

#Software: Microsoft Windows Firewall

#Time Format: Local

#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2024-02-15 05:08:39 ALLOW UDP 192.168.150.133 192.168.150.2 54486 53 0 - - - - - - - SEND

2024-02-15 05:08:39 ALLOW TCP 192.168.150.133 104.208.16.91 50609 443 0 - 0 0 0 - - - SEND

2024-02-15 05:08:46 ALLOW UDP 192.168.150.133 192.168.150.2 54323 53 0 - - - - - - - SEND

2024-02-15 05:08:46 ALLOW TCP 192.168.150.133 104.208.16.91 50610 443 0 - 0 0 0 - - - SEND

2024-02-15 05:08:48 ALLOW TCP 192.168.150.133 104.208.16.91 50611 443 0 - 0 0 0 - - - SEND

2024-02-15 05:09:54 ALLOW UDP 192.168.150.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE

2024-02-15 05:09:54 ALLOW UDP fe80::bc88:ef4:8935:309c ff02::fb 5353 5353 0 - - - - - - - RECEIVE

2024-02-15 05:11:28 ALLOW UDP 192.168.150.133 192.168.150.2 57823 53 0 - - - - - - - SEND

2024-02-15 05:11:28 ALLOW TCP 192.168.150.133 23.213.53.41 50612 443 0 - 0 0 0 - - - SEND

2024-02-15 05:11:30 ALLOW UDP 192.168.150.1 239.255.255.250 59142 1900 0 - - - - - - - RECEIVE

2024-02-15 05:11:54 ALLOW UDP 192.168.150.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE

2024-02-15 05:11:54 ALLOW UDP fe80::bc88:ef4:8935:309c ff02::fb 5353 5353 0 - - - - - - - RECEIVE

2024-02-15 05:11:56 ALLOW UDP 192.168.150.1 192.168.150.255 138 138 0 - - - - - - - RECEIVE

2024-02-15 05:12:29 ALLOW UDP 192.168.150.133 192.168.150.255 138 138 0 - - - - - - - SEND

2024-02-15 05:12:29 ALLOW UDP 192.168.150.133 192.168.150.255 138 138 0 - - - - - - - RECEIVE

2024-02-15 05:12:57 ALLOW UDP 192.168.150.133 192.168.150.2 59705 53 0 - - - - - - - SEND

2024-02-15 05:12:57 ALLOW TCP 192.168.150.133 168.61.21.91 50613 443 0 - 0 0 0 - - - SEND

# Log File’s Location

A screenshot of a computer

Description automatically generated