Windows Firewall: Section 1 Transcript

Introduction

Welcome to the Windows Firewall module.

During this module, we will discuss different types of firewalls, explain different firewall configurations, and demonstrate how to modify firewalls.

Throughout this module, you'll be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Identify different types of firewalls,
- Identify the different firewall configurations on various operating systems, and
- Identify how to view or modify firewalls with Netsh.

Bypass Exam Introduction

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to continue.

Windows Firewall: Section 2 Transcript

Firewalls and Intrusion Detection Systems (IDS) 1/13

Firewalls and Intrusion Detection Systems (IDS) are common security measures used to filter unwanted network traffic and inspect accepted network traffic, respectively. A security solution designed with these technologies is designed to block unauthorized access while permitting authorized communication. The IDS has more advanced monitoring and examination capabilities, which can affect network performance, so it's sometimes T'ed off the switch.

However, IDSs are usually inside firewalls - basically, they serve to let you know if someone has bypassed your firewall. The firewall should keep out intrusions, for the most part, but when it doesn't, the idea is that the IDS will detect it.

Firewalls 2/13

A firewall is a network security system, either hardware, software, or combination of the two, that controls the incoming and outgoing network traffic based on the applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network that is assumed to not be secure and/or trusted.

A firewall can help prevent hackers or malicious software from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

IDS 3/13

An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. An IDS is much like a sniffer, paired with an analytic engine that analyzes traffic against both pre-defined signatures - such as patterns of bytes that appear within network traffic - and heuristic rules - examining behaviors and looking for risky combinations of events.

Firewalls and IDSs both relate to network security; however, an IDS differs from a firewall in that a firewall filters all traffic coming into and out of a network, allowing or blocking each packet as defined in its configuration, while an IDS simply monitors a network or system for malicious activities or policy violations, and produces an alert or report when one is detected. An IDS will not typically take action to stop any suspicious or malicious activity.

Windows Firewall 4/13

Now that we've briefly discussed firewalls and IDSs, let's take a moment to more specifically address Windows Firewall, which is the focus of this module.

Windows Firewall is a built-in, host-based, stateful firewall that is included in:

- Windows Vista,
- Windows Server 2008,
- Windows XP with Service Pack 2 and later, and
- Windows Server 2003 with Service Pack 1 and later.

Windows Firewall allows traffic sent in response to a request by the computer and any traffic that's been explicitly allowed. All other traffic is dropped by default. In some versions, Windows Firewall also filters outbound traffic.

Windows Firewall helps provide protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers.

Windows Firewall Configurations

The Windows Firewall default settings and configuration can vary depending on the version and even the Service Pack of the Windows Operating System.

For example, Windows XP Service Pack 2 was on by default and made it possible for administrators to enable it via Group Policy.

The Vista firewall was built on a new Windows Filtering Platform (WFP), and added the ability to filter outbound traffic via the Advanced Security Microsoft Management Console snap-in.

With Windows 7, Microsoft tweaked the firewall further and made it much more useable, especially on mobile computers, by adding support for multiple active firewall policies. This feature enables each profile, Public, Private, and Domain, to be active on the computer simultaneously.

This means each network connection on the computer receives the degree of firewall protection appropriate to it — more restrictive for the Public or wireless network and less restrictive for the Work or wired network.

Windows Firewall Configurations

Review the Windows Firewall configurations and settings table to better understand the variances and default settings of the Windows Firewall within various Microsoft Windows Operating Systems.

Access Resources for a downloadable version of the Windows Firewall configurations and settings table.

Netsh

Netsh is one of the most powerful networking tools included with Windows.

Netsh is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a computer that's currently running or on. Netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer. Netsh can save a configuration script in a text file for archival purposes or to help you configure other servers.

Using netsh, we are now going to walk-through a few Windows Firewall scenarios using a series of videos. The videos are going to demonstrate Windows Firewall being modified using netsh commands.

The netsh commands being used within the videos will begin very generally with broad modifications being made to the Windows Firewall and then will progress to showing very specific Windows Firewall rules being created.

For a complete transcript of the videos you're about to watch, go to Resources and download the Windows Firewall video transcript.

During this video, we are going to first, view and disable all Windows Firewall policies for the Domain, Private, and Public networks. Then, we are going to be more deliberate and rather than disabling the firewall for all networks, we are going to look for the current profile and only disable the Windows Firewall for that profile.

The following commands are demonstrated during this video:

- netsh advfirewall:
  - show allprofiles,
  - set allprofiles state off,
  - set allprofiles state on,
  - show currentprofile,
  - set currentprofile state off, and
  - set currentprofile state on.

Windows Firewall

We are running the command prompt as an administrator and entering netsh advfirewall show allprofiles. We also have the Windows Firewall GUI running behind the command prompt so we can later use this to visually show when changes to the Windows Firewall have been executed. After entering the command, we see that the Windows Firewall is enabled for the Domain, Private, and Public networks.

Here we are entering netsh advfirewall set allprofiles state off. This turns off the Windows Firewall for all networks. We can see that more clearly on the right side of the screen in the Windows Firewall GUI. Now we are entering netsh advfirewall set allprofiles state on to turn the Firewall back on, and again, we can see that change updated on the Windows Firewall GUI.

Now, we are clearing the screen and entering netsh advfirewall show currentprofile to see which firewall profiles are currently active. We see that the Private network is active and can confirm that in the Windows Firewall GUI.

Here you can see that we are entering netsh advfirewall set currentprofile state off to disable the

firewall for active profiles. This is a much more deliberate action to take when disabling an active firewall profile as opposed to disabling the firewall for all networks.

Finally, we are entering netsh advfirewall set currentprofile state on to turn the firewall back on for the current active profile.

Netsh 10/13

During this video, we're going to review the Windows Firewall rules for the active profile, and then show how to output those rules to use as an analysis tool.

The following commands are demonstrated during this video:

- netsh advfirewall:
  - show currentprofile,
  - firewall show rule profile=private name=all, and
  - firewall show rule profile=private name=all > fwrules.txt.

Windows Firewall Output Rules

As we saw in the previous video, we are going to begin with netsh advfirewall show currentprofile to see which firewall profiles are currently active. We see that the private profile is currently active so the next command we are using is netsh advfirewall firewall show rule profile=private name=all.

Here are all of the enabled Windows Firewall rules for this active profile. To output this information into a more usable format, we are going to enter netsh advfirewall firewall show rule profile=private name=all > fwrules.txt.

This places a text file of those rules on our desktop to review. As we open the file, you can see how this list of rules can begin to help with your analysis of the machine's purpose or if there are any open ports associated with another program that may be of interest.

Netsh 11/13

During this video, we're going to disable a group of rules in Windows Firewall for the entire network.

The following commands are demonstrated during this video:

- netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no
- netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes

Windows Firewall Netsh

As we begin, we are entering netsh advfirewall firewall, firewall set rule group="File and Printer Sharing" new enable=no. We also have the Windows firewall with advanced security GUI running behind the command prompt. We see that after entering the command 46 rules were updated.

Now we are going to look at the Windows firewall GUI and review the inbound and outbound rules to see if the rules were in fact disabled. After clicking refresh we see that the inbound rules under the

enabled column have been set to no. All of the outbound rules have been set to no as well.

Moving back to the command prompt we are entering netsh advfirewall, firewall set rule group ="File and Printer Sharing" new enable=yes. Again, as we move back to the Windows firewall GUI, all rules have been enabled.

Netsh

During this last video, we're going to create a custom and very specific rule. In this video, we are going to create a rule that will allow inbound TCP traffic from a specific IP address and source port to a specific destination port.

Windows Firewall Netsh

As we begin, we are entering a firewall rule named 1337H4X, while also having the Windows firewall GUI running behind the command prompt. As you can see, the rule is very specific as it identifies the rule as inbound, using TCP to a specific port and from a specific socket address. On a side note, you should probably already know, that in this example the name of the rule and the port numbers being used are slightly suspicious.

After entering the command, we are going to access the windows firewall GUI and refresh the page. Upon doing so, we see our new rule 1337H4X appear. As we double click the rule, it opens the properties of the rule where we access the protocols and ports tab. Here we see the protocol type of our rule is TCP the specified local port of 31337, or elite if you have been paying attention, and the remote port of 6666.

After closing the rule properties, and returning the command prompt, we are going to delete our rule by entering netsh advfirewall firewall delete rule name ="1337H4X". One last time we will return to the Windows firewall GUI, refresh the inbound rules, and confirm that 1337H4X has been deleted.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Windows Firewall: Section 3 Transcript

Summary

You have completed the Windows Firewall module.

You should now be able to:

- Identify different types of firewalls,
- Identify the different firewall configurations on various operating systems, and
- Identify how to view or modify firewalls with Netsh.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam.

Click the Next Section button to begin the Module Exam.