

11 - Working with the Security Policy

Objectives

- Know how to use Revision Control
- Use the features of the SmartDashboard to Disable, hide and search for objects in the rulebase
- Understand pre-defined services and the timeouts associated with them
- Understand how to create new services (ports) and the risks associated with them
- Understand how to abuse and tunnel services over standard ports
- Adjust the security policy to increase the security checking of the policy
- Understand that even a simple addition to the security policy rules can require careful risk analysis

Prerequisites

- Complete Module 10
- Virtual machines MgmtSite1, fwsite1 & classrouter must be running

Approximate time for completing each section

Section 1	Policy Revision Control	20 minutes
Section 2	Rule display	15 minutes
Section 3	Dealing with Services	30 minutes
Section 4	Adding More Rules	30 minutes
Section 5	Simple Systems Analysis for Rule Evaluation	20 minutes
	Total time	1 Hr 55 Min

Contents

1	Policy Revision Control.....	3
1.1	Database Revision Control	3
1.1.1	Creating Revisions	3
1.1.2	Where are Revisions Stored	4
1.1.3	Viewing Revisions	4
1.1.4	Rolling Back Revisions.....	5
2	Rule Display	8
2.1	Rule Display and Policy Interaction	8
2.1.1	Hiding Rules	8
2.1.2	Disabling Rules.....	8
2.2	Rule Filters	10
2.2.1	Object Location – Where Used	10
2.2.2	Finding Objects in Rules	11
3	Dealing with Services	12
3.1	Predefined Services and the Inspection Engine	12
3.1.1	TCP.....	12
3.1.2	UDP.....	13
3.1.3	ICMP.....	14
3.1.4	RPC	14
3.1.5	DCE RPC.....	15
3.1.6	Other.....	15
3.1.7	Basic Filtering & SmartDefense Interaction	16
3.2	Creating Services.....	16
3.2.1	Creating a TCP Service and Naming Convention	16
3.2.2	Advanced Properties - Session Timeout and Filtering	17
3.2.3	Two Service Objects Using the Same Port Number.....	17
3.2.4	Applying the New Service to a Rule.....	17
3.3	Abusing a Standard Service – Tunneling over DNS (TCP)	18
3.3.1	SmartDefense Filtering for DNS TCP – Default is Off.....	18
3.3.2	Turn on DNS TCP in the Policy Global Properties	18
3.3.3	Edit the Telnet Server Port on www.server.com & Mgmt.site1.com.....	18
3.3.4	Test the Security Policy – Oops	19
4	Adding More Rules	20
4.1	Current Rules check	20

4.2	DNS rule.....	20
4.2.1	Create the DNS Server Objects – Type Host	20
4.2.2	Add the DNS Rule	20
4.2.3	Add the Internal DNS Servers.....	21
4.2.4	Modify the DNS Rule.....	21
4.3	Outgoing Rule for HP FTP Servers	21
4.3.1	Add the FTP Outgoing Rule	21
4.4	Restricting the Outgoing Rule.....	22
4.4.1	Modify the Outgoing Rule.....	22
4.4.2	Modify the FTP Outgoing Rule.....	22
4.4.3	Delete the Disabled Outgoing Rule.....	22
4.5	Current Security Policy Rules Check	22
4.5.1	Verify and Install the policy	23
5	Simple Systems Analysis for Rule Evaluation	24
5.1	How to Evaluate – ‘From A to B allow FTP’ when B is your Server.....	24
5.2	How to Solve the Problem of Abusing Ports	26