

13 - Using User Authentication

Objectives

- Know the Services that can be used with User Authentication
- Know the daemons associated with User Authentication
- Complete User Authentication using telnet
- Complete User Authentication using FTP
- Complete User authentication using HTTP
- Understand the problem with User Auth & Accept rule clashes
- Use 'tcpdump' to sniff Usernames/Passwords

Prerequisites

- Complete Module 12
- Virtual machines MgmtSite1, fwsite1 & classrouter must be running

Approximate time for completing each section

Section 1	User Authentication	35 minutes
Section 2	Using Authentication from internal Networks – Rule clashes	30 minutes
Section 3	User Login Details - tcpdump	15 minutes
	Total time	1 Hr 20 Min

Contents

1	User Authentication	3
1.1	User Authentication Daemons & Process	3
1.1.1	Authentication Daemons and Supported Services	3
1.1.2	User Authentication – Policy Global Properties	4
1.1.3	Welcome Message	4
1.2	Authentication Using Telnet	4
1.2.1	Add a telnet Authentication rule	4
1.2.2	Check Rule Properties – Intersect with User Database	5
1.2.3	Installing the Policy and Testing Authentication	5
1.3	Authentication Using http	6
1.3.1	Add an http Authentication rule	6
1.3.2	Check Rule Properties – Allowed http Servers	6
1.3.3	Adding predefined servers	7
1.3.4	Installing the policy and Testing Authentication	7
1.4	Authentication Using FTP	7
1.4.1	Add an Authentication rule	7
1.4.2	Format of User/Password for Authenticating Using FTP	7
1.4.3	Installing the Policy and Testing Authentication	7
1.5	Basic Authentication – Summary	8
1.5.1	Multiple Rules or a Single Rule	8
1.5.2	Removing the Check Point Prompt	8
2	Using Authentication from Internal Networks – Rule clashes	9
2.1	Authentication Behavior – Source IP Address	9
2.1.1	Changing the Behavior – GuiDBedit	9
2.2	Using http for Authentication from Internal Networks	11
2.2.1	Adding the Internal Out http Authentication Rule	11
2.2.2	Reason for Authentication Not Being Enforced	11
2.2.3	Correctly Implementing the Authentication Rules	12
3	User Login Details – tcpdump	13
3.1	Stealing User Login Information	13
3.1.1	Packet trace using tcpdump	13
3.1.2	Packet trace using tcpdump and Wireshark	14