

1 - Networks and Firewalls

Objectives

- Know how packet filtering works
- Know how application proxies work
- Know how Stateful Inspection works
- Know how to apply basic filters in tcpdump
- Know how to create a pcap file for analysis by WireShark

Approximate time for completing each section

Section 1	Securing Networks	20 minutes
Section 2	Basic Network Packet Analysis	10 minutes
	Total time	35 Minutes

Prerequisites

- Basic understanding of TCP/IP
- Knowledge of MS-Windows
- Have VMWare Workstation or Server Installed
- Have the Virtual Machines ready for use

Contents

1	Securing Networks.....	3
1.1	All Firewalls are Not Equal.....	3
1.1.1	Primary Organization Network	3
1.1.2	Hosted Services Network	4
1.1.3	Remote Office Networks	5
1.2	Basic Protocols	5
1.2.1	IP Protocol	5
1.2.2	TCP Protocol	6
1.2.3	UDP Protocol.....	7
1.2.4	ICMP Protocol	8
1.3	Protection Using Simple Packet Filters	8
1.3.1	Packet Filter Protection	8
1.4	Protection Using Application Proxies.....	8
1.4.1	Application Proxy Protection	9
1.5	Protection Using Hybrids – Stateful Inspection	9
1.5.1	Stateful Inspection Protection	9
1.5.2	Building State Tables	10
1.5.3	Check Point Filtering Modules	11
1.5.4	Check Point State Tables.....	11
2	Basic Network Packet Analysis	13
2.1	Sniffing Packets	13
2.1.1	tcpdump	13
2.1.2	Wireshark.....	13