

TABLE OF CONTENTS

General Introduction

Chapter 1 Port Scanning

1.1	Introduction.....	6
1.2	APPROACHES TO PORT SCANNING	6
1.2.1	Single-source Port Scans.....	7
1.2.2	Distributed Port Scans	8
1.3	Port Scanning Techniques	9
1.4	TCP/IP Relevant Issues.....	11
1.4.1	Packet Flags	11
1.4.2	TCP Connection Establishment.....	11
1.4.3	Some Implementation details	12
1.5	Nmap	13
1.5.1	Nmap Port Scanning Techniques.....	13
1.5.1.1	TCP SYN scan (-sS).....	13
1.5.1.2	TCP connect scan (-sT)	14
1.5.1.3	UDP scans (-sU)	15
1.5.1.4	SCTP INIT scan (-sY)	16
1.5.1.5	TCP NULL, FIN, and Xmas scans(-sN; -sF; -sX).....	16
1.5.1.6	TCP ACK scan(-sA).....	17
1.5.1.7	TCP Window scan (-sW)	18
1.5.1.8	TCP Maimon scan (-sM)	18
1.5.1.9	Custom TCP scan (--scanflags)	19

1.5.1.10	SCTP COOKIE ECHO scan (-sZ)	19
1.5.1.11	idle scan (-sI <zombie host>[:<probeport>])	20
1.5.1.12	IP protocol scan (-sO)	20
1.5.1.13	FTP bounce scan (-b <FTP relay host>).	21
1.6	Conclusion.....	23
 Chapter 2 Port Scanning Detection		
2.1	Introduction.....	25
2.2	Approaches to port scan detection	25
2.2.1	Single-Source Port Scan Detection Approaches.....	25
2.2.1.1	Algorithmic Approaches.....	26
2.2.1.2	Threshold-based Approaches.....	29
2.2.1.3	Soft Computing Approaches	32
2.2.1.4	Rule-based Approaches	33
2.2.1.5	Visual Approaches.....	34
2.2.1.6	Discussion	35
2.2.2	Distributed Scan Approaches.....	37
2.2.2.1	Algorithmic Approaches.....	38
2.2.2.2	Clustering Approaches	38
2.2.2.3	Soft Computing Based Approaches.....	39
2.2.2.4	Visual Approaches.....	40
2.2.2.5	Discussion	41
2.3	Conclusion	42

Chapter 3 Slow Port Scanning Detection

3.1	Introduction.....	44
3.2	Proposed Method	44
a)	Connect Scan	46
b)	Half-Connect Scan	47
c)	FIN Scan	47
3.3	Algorithm To Detect Slow Port Scan	50
3.4	Discussion	51
3.5	Conclusion	51

Chapter 4 Implementation

4.1	Introduction	53
4.2	Platform	53
4.2.1	Java	53
4.2.2	NetBeans	53
4.3	Winpcap	54
4.3.1	Winpcap structure	54
4.3.2	WinPcap consists of.....	55
4.3.3	The working of a WinPCap.....	55
4.4	Jpcap	56
4.4.1	Function of Jpcap.....	56
4.5	Experiments.....	57
4.6	Nmap	58

4.6.1	Find hosts	58
4.6.2	Port scanning techniques.....	59
4.6.2.1	TCP Syn Scan (-sS)	59
4.6.2.2	Tcp connect scan(-sT).....	60
4.6.2.3	Fin scan (-sF)	60
4.7	Packet Capturing using Jpcap.....	61
4.8	Detection (Port Scan/Slow Port Scan)	68
4.8.1	Detection Port Scan.....	68
4.8.2	Detection Slow Port Scan	68
4.9	Conclusion	69

General Conclusion