

Table Of Contents

General Introduction	2
Chapter 1 - Mobile Agent	
1 Introduction	6
2 Agents.....	6
2.1 About Agents.....	6
2.1.1 Definition.....	6
2.2 Classification Of Software Agents	7
2.3 Agent Communication.....	8
2.3.1 The Knowledge Query And Manipulation Language (Kqml)	8
2.3.2 The Knowledge Interchange Format (Kif).....	8
2.3.3 The Fipa Agent Communication Languages.....	8
3 Mobile Agent.....	8
3.1 History	8
3.2 Definition.....	8
3.3 Basic Structure Of A Mobile Agent	9
3.4 Agent Migration	10
3.4.1 Weak And Strength Migration	10
3.5 Mobile Agent Properties.....	10
3.5.1 Mobility.....	11
3.5.2 Autonomy.....	12
3.6 Mobile Agent Advantages	13
3.7 Disadvantages Mobile Agents	13
4 Mobile Agent Applications	14
4.1 Electronic Commerce	14
4.2 Personal Assistance	15
4.3 Distributed Information Retrieval	15
4.4 Telecommunication Networks Services	15

4.5	Workflow Applications And Groupware	15
4.6	Monitoring And Notification.....	15
4.7	Information Dissemination	16
4.8	Agent Architecture Vs. Client/Server Architecture	16
5	Mobile Agent Standardization: Masif	17
6	Contemporary Mobile Agent Systems	18
6.1	Aglets	18
6.2	Odyssey	18
6.3	Concordia.....	18
6.4	Voyager.....	19
6.5	Agent Tcl	19
6.6	Ara	19
6.7	Tacoma.....	20
7	Conclusion.....	20

Chapter 2 - Intrusion Detection

1	Introduction.....	21
2	Intrusion.....	21
3	Intrusion Detection.....	21
4	Definition Of Intrusion Detection System (Ids)	22
5	Types Of Intrusion Detection System (Ids)	22
6	Classification Of Ids.....	23
6.1	Host-Based Systems.....	23

6.2	Network-Based Systems.....	23
6.3	Application Based Ids.....	24
7	Ids Architecture.....	24
8	Limitations Of Existing Ids.....	24
9	Useful Characteristics Of Mas.....	25
10	Advantages And Disadvantages Of Mobile Agents In Intrusion Detection.....	27
10.1	Minimizing The Network Traffic.....	27
10.2	Persistency.....	27
10.3	Structure And Platform Independence.....	27
10.4	Dynamic Nature.....	28
10.5	Heterogeneous Environment.....	28
10.6	Robust In Nature.....	28
10.7	Scalability.....	28
11	Port.....	29
12	Tcp/Ip, Ports And Services.....	30
12.1	Tcp/Ip Background.....	30
12.2	Tcp Flags And Their Usage.....	30
12.2.1	Explicit Congestion Notification.....	31
12.2.2	Congestion Window Reduced.....	31
12.2.3	Urgent.....	31

12.2.4	Acknowledgement.....	32
12.2.5	Push.....	32
12.2.6	Reset.....	32
12.2.7	Syn.....	32
12.2.8	Fin.....	32
12.3	Tcp Connection Establishment.....	32
13	Port Scanning.....	33
14	Types Of Port Scans.....	33
14.1	Stealth Scan.....	33
14.2	Socks Port Probe.....	34
14.3	Bounce Scan.....	34
14.4	Tcp Scanning.....	34
14.5	Udp Scanning.....	34
15	Slow Scan.....	34
16	Approaches To Port Scanning.....	35
16.1	Single-Source Port Scans.....	35
16.2	Distributed Port Scans.....	36
17	Approaches To Port Scan Detection.....	37
17.1	Single-Source Port Scan Detection Approaches.....	37
17.1.1	Algorithmic Approaches.....	38

17.1.2	Threshold-Based Approaches.....	38
17.1.3	Soft Computing Approaches.....	38
17.1.4	Rule-Based Approaches.....	38
17.1.5	Visual Approaches.....	38
17.1.6	Discussion.....	39
17.1.7	Distributed Scan Approaches.....	39
17.1.8	Algorithmic Approaches.....	39
17.1.9	Clustering Approaches.....	39
17.1.10	Soft Computing Based Approaches.....	39
17.1.11	Visual Approaches.....	39
17.1.12	Discussion.....	40
17.1.13	Port Scanning Techniques.....	40
18	Nmap.....	41
18.1	Commonly Used Scans.....	42
18.1.1	Tcp Syn Scan (-Ss)	42
18.1.2	Tcp Connect Scan (-St)	42
18.1.3	Udp Scan (-Su)	43
18.1.4	Null Scan (-Sn)	43
18.1.5	Fin Scan (-Sf)	43
18.1.6	Xmas Scan (-Sx)	43

18.1.7	Tcp Ack Scan (-Sa)	43
18.1.8	Custom Tcp Scan (--Scanflags)	44
18.1.9	Ip Protocol Scan (-So)	44
19	Conclusion.....	45

Chapter 3 - Contribution

1	Introduction	47
2	Description Of Our Work	47
3	Used Tools.....	47
3.1	Netbeans.....	47
3.1.1	Java	47
3.2	Aglets	48
3.2.1	Creation	48
3.2.2	Cloning	48
3.2.3	Dispatching.....	48
3.2.4	Retraction	49
3.2.5	Activation And Deactivation.....	49
3.2.6	Disposal	49
3.2.7	Messaging.....	49
3.3	Winpcap	49
3.4	Jpcap	49
3.5	Mysql	50
4	Organigramme System	51
5	Principal Algorithms.....	52
5.1	Port Scan	52
5.2	Slow Port Scan	54
5.2.1	Connect Scan	54
5.2.2	Half-Connect Scan.....	55
5.2.3	Fin Scan	55

6	The Results	58
6.1	Results Of PortScan Algorithm.....	59
6.2	Results Of Slow Port Scan Algorithm	61
7	Conclusion	63
	General Conclusion	65
	References	66