

Contents:

1. Introduction	1
1.1. Port Scanning	2
1.2. State of the Art	3
1.3. Motivation	4
1.4. Aim of Work	4
1.4.1. Objectives	4
1.5. Work Done	5
1.6. Organization of the Dissertation	5
2. Port Scanning & Its Significance	6
2.1. Classes of Port Scan Attacks	8
2.2. Hiding Scanner Identity	9
2.3. Horizontal Vs Vertical Vs Block Vs Strobe Scans	10
2.4. Co-ordinated Port Scan Attacks	10
2.5. Various Scanning methods and firewall detection possibility	11
2.6. The Various Port Scans Done	13
2.6.1. TCP SYN Scan	13
2.6.2. TCP ACK Scan	15
2.6.3. TCP FIN Scan	16
2.6.4. XMAS Scan	17
2.6.5. TCP NULL Scan	18
2.6.6. MAIMON Scan	20
2.6.7. UDP Scan	21
2.6.8. ICMP (PING) Scan	22
2.7. Discussion	22
3. Intrusion Detection System	23
3.1. IDS Terminology	25
3.2. Generic Architecture of IDS	26
3.3. Types of Intrusion Detection Systems	27
3.3.1. Host-Based Intrusion Detection System (HIDS)	27
3.3.2. Network-Based Intrusion Detection System (NIDS)	28

3.4. Intruders	29
3.5. Limitations	30
4. Live Network Packet Capturing & Feature Extraction	31
4.1. Software Used	32
4.2. Hardware Used	32
4.3. Lab Setup	33
4.4. Live Network Packet Capturing Using Standard Tool	33
4.4.1. Generic Architecture of Network Packet Capturing	33
4.4.2. Launching Real Life Attacks using NMap	34
4.4.2.1. NMap	34
4.4.2.2. NMap Features Include	35
4.4.2.3. NMap Target Specifications	35
4.4.2.4. Privileged Access	36
4.4.2.5. NMap Scanning Techniques	36
4.4.3. Packet Capturing Tool (Wireshark)	38
4.4.3.1. Installing Wireshark in Windows & in UNIX	38
4.4.4. Pre-Processing (Data Captured using Wireshark).....	39
4.5. Feature Extraction	40
4.5.1. Various Types of Features	40
4.5.2. Feature Extraction Using C routines	40
4.5.3. TCPtrace: A TCP connection analysis tool	43
4.6. Dataset Preparation	45
4.7. Discussion	46
5. Analysis of the intrusion dataset	47
5.1. A supervised approach	49
5.1.1. Profile Creation	49
5.1.2. Structure of the profiles	50
5.1.3. Determining the profile elements	50
5.1.4. Classification of the dataset	51
5.1.5. Key issues	53
5.1.6. Reducing the cost of computation	53
5.1.7. The Algorithm	54

5.2. An unsupervised approach	54
5.2.1. Tanagra	54
5.2.2. Orange	56
5.3. Fusion	58
5.4. Labeling Technique	58
5.5. Discussion	58
6. Evaluation and Comparison	59
6.1. Brief description of the algorithms	60
6.1.1. K-Means Clustering	60
6.1.2. C4.5 Decision Tree	60
6.2. Results	61
6.2.1. Classification result for the KDD 10% Dataset	61
6.2.2. Confusion Matrices (5-class)	62
6.2.3. Confusion Matrices (2-class)	63
6.2.4. Comparison with K-means and C4.5	64
6.3. Discussion	64
7. Conclusion and Future Works	65
7.1. Conclusion	66
7.2. Future Work	66
References	67