AMHE18 INTRUSION DETECTION

UNIT-1 DEFINING INTRUSION DETECTION

1.1 The history of intrusion & Detection:
1.2 Audit: Setting
1.3 The Stage for Intrusion Detection,
1.4 The birth of intrusion Detection.

UNIT-2 SECURITY CONCEPTS INTRUSION

2.1 Detection concept,
2.2 Determining strategies for Intrusion Detection

UNIT-3 INFORMATION SOURCES

3.1 Host based information sources ,
3.2 Network based information sources,
3.3 Information other security products,
3.4 Analysis Scheme: A model for intrusion Analysis, Techniques

UNIT-4 RESPONSES

4.1 Requirement of Responses,
4.2 Types of responses,
4.3 Covering tracks during investigation,
4.4 Mapping responses of Policy

UNIT-5 VULNERABILITY ANALYSIS

5.1 Credentialed approaches,
5.2 Technical issues.

UNIT-6 BUILDING CASE FOR SECURITY

6.1 Defining Requirement for Ids,
6.2 Integrating security into legacy environment

UNIT-7 FOR DESIGNER

7.1 Requirement,
7.2 Security Design principles,
7.3 Surviving the designing process.
7.4 Future trends in technology,
7.5 A vision for intrusion Detection.

Reference Book:

1. Stephen Northcutt &Jady Novak, "Network Intrusion Detection, 3rd Edition, New Riders Publishing, 2003