CSE-711 Intrusion Detection System
L-T-P-C: 3-0-0-3

Introduction: IDS, Types of IDS, host based IDS, Network based IDS, Stack based IDS, signature Based IDS, anomaly based IDS, TCP/IP and security concerns, DNS and security concerns, Mail server and security concerns, Web Server and security concern, firewall, Types of Intrusion, Symptoms that help in intrusion detection, statistical pattern recognition for detection and classification of attacks, vulnerabilities and Threats; Trojan Remote Access Trojan RAT, Virus, Worms and Malwares.

Data Collection Mechanism: Data Sampling, Packet Sampling, Flow Sampling, techniques for visualizing network data, Packet Sampling tools, Tcpdump windump, Wireshark tool, Writing Tcpdump/Windump Filters, libcap/winpcap libraries, pcap file, sniffing and spoofing tools, data and methodologies of computer intrusion detection, statistical & machine approaches to detection of attacks on computers.

Attacks and Packet analysis: network based attacks such as probes & denial of service attacks, host based attacks such as buffer overflows and race conditions, malicious codes, Examining Packet Header Fields, normal and abnormal values in IP, TCP, UDP, and ICMP header fields, Fragmentation theory, packet capture examples, fragmentation-based attacks, ICMP protocol, ICMP based attacks, Network Traffic Analysis: malicious, normal and application traffic; discern malicious traffic from false positives. IDS Patterns, DoS attacks, network mapping, and coordinated attacks, Indications & Warnings and Traffic Correlation, Network correlation, Network Situational Awareness, anomaly detection, signature based analysis, Semantic aware signature, policy based analysis, and host based analysis

IDS infrastructure: IDS Architecture, IDS/IPS Management and Architecture Issues with regard to deploying IDS/IPS systems, end point approach to security, system approach to security, IDS Interoperability models: CIDF (Common Intrusion Detection Framework), IDMEF (Intrusion Detection Message Exchange Format), IODEF (Incident Object Description Exchange Format), CVE (Common Vulnerabilities and Exposures), OVAL (Open Vulnerability and Assessment Language)

Protocol Analysis: Microsoft Protocols, SMB/CIFS, RPC, and Active Directory protocols, SIP protocol, Chat protocol, the key differences between IPv4 and IPv6, IPv6 based attacks

IDS tools: Snort and Bro IDS tools, NIDS Evasion, Insertion, and Checksums to confuse NID systems, Snort Fundamentals and

Configuration, Snort GUIs & Sensor Management, Snort Performance, Active Response & Tagging, Snort Rules, Stimulus Response, hosts response to both normal and abnormal traffic, Advanced Snort Concepts as rule ordering and reduction of false negatives and positives. Evaluation and tuning of IDS, Cross over Rate (CER) of IDS.

Advanced topics: honeypots, shadow honeypots.

Books and References

1. Stephen Northcutt and Judy Novak , Network Intrusion Detection", 3rd edition by. ISBN: 0735712654.
2. Extrusion Detection: Security Monitoring for Internal Intrusions By Bejtlich, Pearson Education.
3. Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations: Recommendations of the National Institute of Standards and Technology by Karen Scarfone and Peter Mell.
4. IETF RFC/RFP/standards related to Intrusion detection.
5. CCNP Security: Intrusion Prevention and Intrusion Detection Systems. By David Burns, OdunayoAdesina, Keith Barker, Cisco Press.
6. Intrusion Detection and correlation: challenges and solutions: by Christopher Kruegel, Fredrik Valeur, Giovanni Vigana, Advances in Information Security Volume 14, ISBN 0-387-23398-9 2005 Springer