NeSA

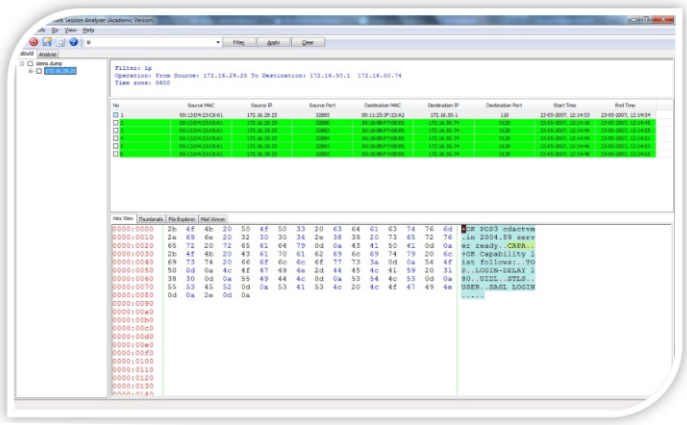
Network Packet Session Analyser

NeSA (Network Session Analyser) is the networks forensics tool to capture and analyse network traffic. Data sent through the network can be captured, recreated and exported using this tool.

Major Features

Data Reconstruction

With the help of flexible and powerful filtering system, data from HTTP, SMTP, POP3 and FTP session can be recreated and visualized in an analysis friendly manner. The tool has built-in data viewers including a Mailview, to help the analyst to concentrate on analysis.



Analysis Modes

NeSA supports both data level and packet level analysis of network data. In data level, the analyst can concentrate on the data and can avoid the nuts and bolts of network protocols. But if he/she wishes to dig deeper, the packet analysis mode is ready to extend its helping hands.

Searching and Filtering

Searching and filtering helps to reach analyst's goals faster. Flexible filter expressions are provided for packet level analysis and for data level analysis. The data level filtering supports filtering based on date, time, IP, MAC and port. The regular expression based searching gives the analyst the full power that he expects from a tool.

Other Features

- Loads pcap formatted dump files and rebuilds TCP sessions.
- Reconstructs files from HTTP, FTP, SMTP and POP3 packets.
- Built in Hex, Thumbnail, File and Mail view.
- Powerful filter for filtering TCP sessions and packets.
- Regular expression based search capability.
- Supports port customization and time zone based analysis.
- Loads multiple pcap files.
- Merging and sorting of packets.
- Can capture from multiple interfaces
- Report generation.

CYBER SECURITY GROUP

Centre for Development of Advanced Computing

R&D Organization of Ministry of Electronics and Information Technology Govt. of India

Technopark Campus, Karyavattom P.O, Thiruvananthapuram - 695 581

Ph.No: +91 471 278 1500, 2781555

Email: cyber-tvm@cdac.in, csg@cdac.in Web: www.cyberforensics.in