

Background

C-DAC (Erstwhile CEDTI) Mohali, established in 1989 in the ELTOP(Electronics Town of Punjab) Complex, caters to the training, consultancy, design and product development needs of electronics and information technology industry and allied sectors. It also promotes potential Entrepreneurs through various services, academic and training programs. The institute has its own aesthetically designed building with covered area of 4300 sq mts. C-DAC (Erstwhile CEDTI) Mohali, an institute under the Government of India, is the first society of Ministry of Communications and Information Technology to have an ISO 9001:2000 certification, which reflects the quality in conceptualization, design, implementation and monitoring of the training programs. The certification is a testimony by international quality in system that governs its well structured and regularity updated training with global acceptance.

Cyber Security & Cyber Forensics

India is on the verge of acquiring excellence in technological advancements. The adoption of technology is accompanied by the need to safeguard and maintain its relevance to have a positive and significant impact on the society.

The ascertainment and preservation of vital information is critical to any enterprise. Cyber Attacks in this space can cause loss of data, threaten the public safety, impact national security, create economic upheaval, or environmental disasters. The traditional methods to secure sensitive enterprise data face many challenges and loopholes. Hence, to administer all spheres of security infrastructure and to impose a high competition to the Blackhat community, the need of the hour is to have a sound cyber security framework.

The state-of-the-art to counter the cyber terrorism calls for enhanced techno-legal measures and standardized procedures. The process has to be supplemented with enhanced knowledge of emerging attack patterns, increasing sophistication and effectiveness of hacker's activities, evolving security exploits, and social engineering elements. This demands the formulation of critical security framework to defend against latest and intelligent intrusions.

Cyber Security Technology division at C-DAC, Mohali

The research and development team of C-DAC, Mohali in the area of cyber security aims to research on cyber crimes through the deployment of Honeynet as single dedicated and as geographically distributed networks, which has been strengthened with advanced and enhanced data capture, data control, and data analysis procedures for detailed inspection of cyber attacks and cyber threats. Our team is also working in close association with user agencies like CERT-In to provide real cyber attack data and formulate dataset formats according to the various Enterprise deployment scenarios of Honeynet. The current focus of R&D team of C-DAC, Mohali pertains to development of Geographically Distributed Honeynet System to enable malware collection and analysis for bot/botnet detection and latest attack trends analysis in cyber space.

About the Workshop

The rapid advancement in information technology has heralded a new age of explosive growth in all fields of life with an increasing demand for practice of security in all applications. Security has moved into the mainstream of every domain of Information Technology and has become a key technology in determining future research and development activities in many academic and industrial branches.

Honeypots are network resources deployed to be probed, attacked, and compromised. Honeypots are closely monitored network decoys serving several purposes: they can distract adversaries from more valuable machines on a network, they can provide early warning about new attack and exploitation trends and they allow in-depth examination of adversaries during and after exploitation of a Honeypot. Honeypots run special software which collect data about the system and greatly aids in post-incident computer and network forensics. HoneyNet is a network comprising of Honeypot and HoneyWall. Because of the wealth of data collected through them, HoneyNets are considered a useful tool to learn more about attack patterns and attacker behavior in real networks.

Prior to the discovery of newer intelligence collection tools, we need to maintain the relevancy of Honeypot/HoneyNet. We aim to address the exposure of HoneyNet Technology and its relevance in Cyber/Intranet security through a sensitizing Workshop at C-DAC, Mohali. The key objective is to throw light on the various perspectives of State-of-the-art HoneyNet Technology and its application areas together with practical demonstrations & discussions on results & findings. The workshop has been titled as **"HoneyNet/ Honeypot: Attack Data Capturing, Analysis & Monitoring"**.

C-DAC, Mohali HoneyNet Project has been working in close relation with CERT-In to bring HoneyNet research to a solid scientific foundation and assessing the value of honeyNet technology as a research and production tool. Hence, the workshop has been enriched to include the enterprise deployment scenarios of HoneyNet and knowledge of HoneyNet dataset formats for user agencies. Areas pertaining to ethical and legal aspects of honeypots and possible directions for further research would also be briefed.

Conclusively, the Workshop would be highlighting the relevance, value and need of HoneyNet technology in cyber/intranet security and malware related cyber threats collection & analysis (bots/botnets, in specific) together with its practical deployment scenario specifications

The workshop conduct and project proposals would facilitate the collaboration of CDAC with Ministry of Defense and hence the workshop would bridge communication gap between the two participating entities.

Targeted Participants/Audience

Representatives from Integrated Defense Services , Delegates from CDAC Centers & CERT-In.

Registration Details:

Rs. 1500/- per participant (For DIARA)

Workshop Schedule:

30th Sep, 2009 (Day 1)	09:00 – 11:00	Opening Session Keynote Talk By Experts
	11:00 – 11:15	Coffee Break
	11:15 – 01:00	Technical Session 1: Honeynets-A High Value Security Resource
	01:00 – 02:00	Lunch Break
	02:00 – 03:00	Technical Session 2: Various Honeynet Sensors <ul style="list-style-type: none"> • GEN 3 Honeynet (High Interaction)
	03:00 – 04:00	Technical Session 3: Various Honeynet Sensors <ul style="list-style-type: none"> • Nepenthes (Low Interaction) • Honeybow (High Interaction)
	04:00 – 04:15	Coffee Break
	04:15 – 05:15	Technical Session 4: Various Honeynet Sensors <ul style="list-style-type: none"> • HoneyD (Virtual Honeypot) • Active Honeybots (Honeyclient)
1st Oct, 2009 (Day 2)	09:00 – 09:30	Keynote Talk by Experts
	09:30 – 10:30	Technical Session 5: Applications of Honeynet Technology in Intranet Scenario
	10:30 – 10:45	Coffee Break
	10:45 – 11:30	Tech. Session 6: Malware / Bot Collection, analysis Principles & Techniques
	11:30 – 12:15	Tech. Session 7: Results & Findings & Practical Demo.
	12:15 – 1:00	OPEN HOUSE : Deliberating & Evaluating the usability & adoption of Honeynet / Honey pots in Defense Service Intranets
	1:00 – 1:45	LUNCH

Contact Information:

For further Information please contact the workshop coordinators

1. Mr. Rakesh Sehgal

Tel: 0172-2236143, 2237056

Mob: 098722-59555

2. Mr. Bharat Bhushan

Mob: 097791-02189

Email: _sehgal_rks@yahoo.com , rks@cdacmohali.in, erbharat1@yahoo.co.in