REPORT FOR WORKSHOP

ADHI
COLLEGE OF ENGINEERING & TECHNOLOGY
No.6, MunuAdhi Nagar, Sankarapuram, Near Walajabad,
KanchipuramDist – 631 605. Ph: 044 – 2729 0096

WORKSHOP ON "CYBER FORENSICS TOOLS"

Guest of honor: Mr.S.Prabhu, M.E.,(Ph.D.), Assistant Professor, S.A. Engineering College.

Date: September 19th, 2017

Time: 9:30 am - 3:30 pm

Venue: CSE Lab, Adhi College of Engineering and Technology

Organizer: Mr. S. Thangavel, Assistant Professor, Department of Computer Science and Engineering

Attending students: Final year CSE

ABOUT THE WORKSHOP

One day Workshop on "Cyber Forensics Tools" for final year CSE students was organized by the Department of Computer Science and Engineering on 19th September, 2017. There were 39 participants, who attended the seminar. The expert was invited from S.A. Engineering College, Chennai.

The program was started with an introduction about the Cyber Forensics tools such as Wireshark, MD5SUM, KFsensor, SNORT, and GnuPG.

Wireshark:

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

MD5SUM:

md5sum is a computer program that calculates and verifies 128-bit MD5 hashes, as described in RFC 1321. The MD5 hash functions as a compact digital fingerprint of a file. As with all such

hashing algorithms, there is theoretically an unlimited number of files that will have any given MD5 hash.

KF Sensor:

Monitors all traffic

KFSensor acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and trojans. KFSensor is pre-configured to monitor all TCP and UDP ports, along with ICMP. It is also configured with the emulation of common services. It starts monitoring right after its installation and can be easily customized to add additional customer services later on.

Interacts with an attacker

By responding with an emulation of a real service KFSensor is able to reveal the nature of an attack whilst maintaining total control and avoiding the risk of compromise. As well as individual service attacks KFSensor detects and responds to port scans and denial of service DOS attacks and prevents itself from being overloaded. By responding with the emulation of a real service, KFSensor is able to reveal the nature of an attack, whilst also maintaining total control of the incident and avoiding the risk of compromise. As well as individual service attacks, KFSensor also detects and responds to port scans and denial of service (DOS) attacks; and prevents itself from being overloaded.

Alerts

KFSensor can send real time alerts by email or via integration with a SEIM system. The KFSensor administration console allows events to be filtered and examined in detail, allowing comprehensive analysis of any attack. KFSensor also makes a full packet dump available for additional analysis, using tools such as Wireshark.

Statistical Analysis

The KFSensor Reports module provides a range of reports and graphs that can be used to analyze many different aspects of the attacks facing an organization. The reports are particularly useful in highlighting patterns of attacks they are only identifiable over time. All reports can be filtered on time period, attack type and the location of the visitors, allowing for detailed study and analysis of a particular threat.

SNORT Tool:

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol

analysis, content searching and matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

GnuPG:

GnuPG is a complex tool with technical, social, and legal issues surrounding it. Technically, it has been designed to be used in situations having drastically different security needs. This complicates key management. Socially, using GnuPG is not strictly a personal decision. To use GnuPG effectively both parties communicating must use it.

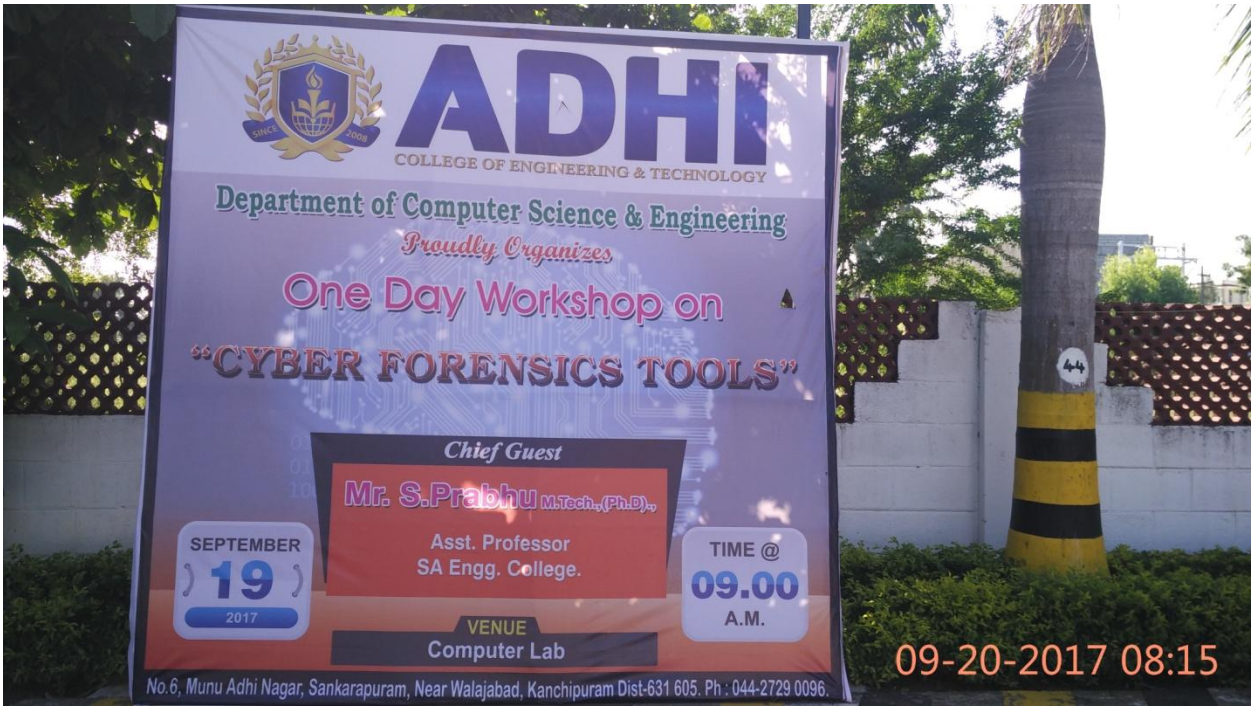
STUDENTS FEEDBACK

The session was highly informative and interesting.

VISITOR FEEDBACK

The hospitality provided by the college was excellent. The students were very interactive and obedient.

PHOTO GALLERY



REPORT FOR WORKSHOP