Adhi College of Engineering & Technology
(An ISO 9001:2008 Certified Institution)
No. 6, Munu Adhi Nagar, Sankarapuram, Near Walajabad,
Kanchipuram Dist-631 605. Ph: 044-2729 0096.

Guest Lecture on Security Tools

Guest Lecture was organized to IV year CSE students on 22/9/2016 about Security Tools at computer lab.

Resource person

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

ABOUT THE PROGRAM

Lecture was started with an introduction about the Security tools such as KFsensor, SNORT, and GnuPG.

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.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

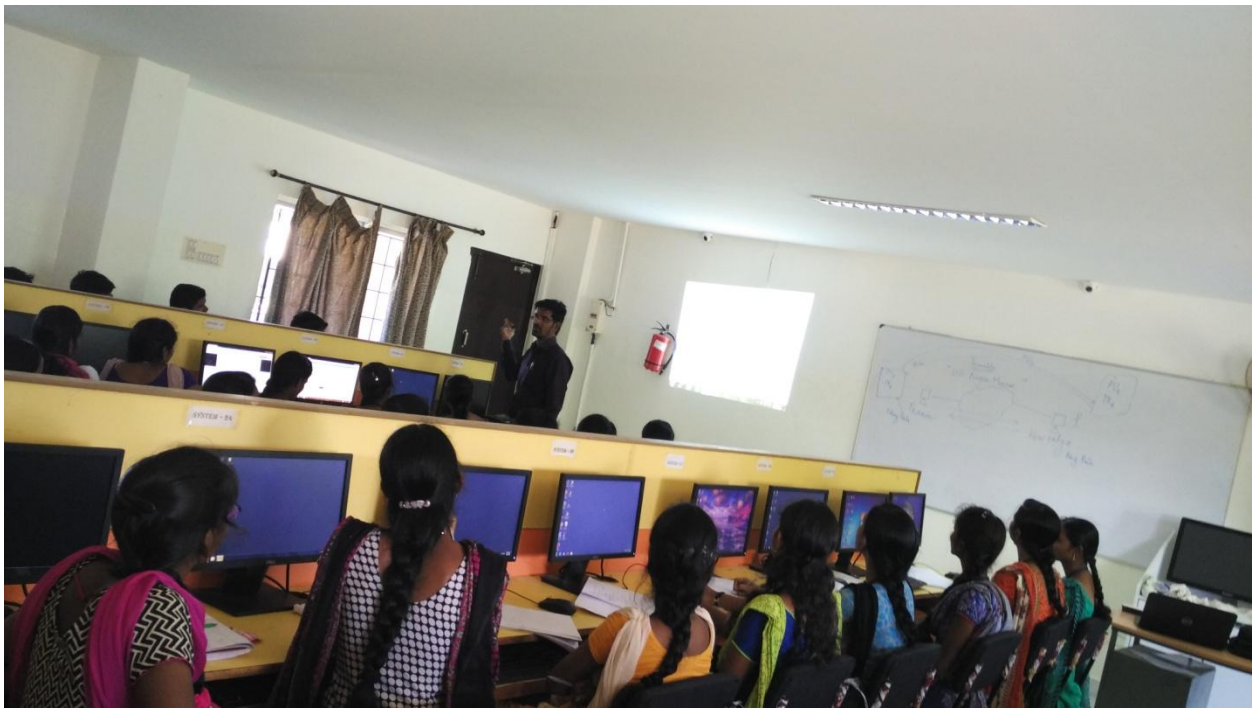
GnuPG:

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.

This lecture was very useful for the students to know about the current leading security tools used in Industry. It is also useful for academic subjects.

Photographs

Resource person, interacting with Students.



Resource person, presenting the Lecture.