Rukmini Devi Institute of Advanced Studies

Madhuban Chowk, Rohini, Delhi-110085

(Approved By AICTE &Affiliated With GGSIP University)

DOSSIER

Guest Lecture

On

"Network Forensic"

On

January 21, 2014

Ms. Jyoti Arora

Ms. Amandeep Kaur
Chairperson, Literary Club

Prof. Col. (Retd.) Mahander Singh
Director General, RDIAS

FORM A

Proposal:

- **Name of the event to be organized**: Guest Lecture on “Network Forensic”
- **Date:** January 21, 2014
- **Time:** 11:30 a.m. – 01:30 pm
- **Venue:** Lecture Theatre, RDIAS
- **Motivation for the activity**: The session aimed at providing the students fundamental knowledge about computer and network forensics. The added knowledge to forensics will enhance the marketability of our students and serve the students who carry the skills and knowledge forward into their future careers.
- **Organized by: MC**A Department
- **Resource Person**: Mr. Santanoo Pattnaik, Sr. Technology consultant, Sansoft Technologies (India) New Delhi.

FORM B

Part 1

Aim of the event:

The aim of this session was to make students understand the basics of Computer and Network forensics, to consider career as next-generation computer crime investigators. **Network forensics** is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis. The second form of Network forensics relates to law enforcement. In this case, analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.

Part 2

Abstract:

The session was taken by Mr. Santanoo Pattnaik working as Sr. Technology consultant with Sansoft Technologies (India) New Delhi.
His presentation focused on the following discussion points:

1. Forensics Background
2. Operating Systems
3. Select Windows Features
4. Vectors and Payloads
5. Forensic Process
6. Forensic Tools Demonstration

Sir divided the lecture into two sessions. The first session was dedicated to the Computer Forensics concept and the second session to Network Forensics concepts.

Sir started the first session with definition of Computer Forensics. Computer Forensics (sometimes known as Computer Forensic Science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information. After defining the computer forensics, Sir explained the background of computer forensics.

Forensics Background:-

- Inspection of computer system for evidence of:-
    - Crime
    - Unauthorized use
- Evidence gathering/preservation techniques for admissibility in court of law.
- Consideration of suspect’s level of expertise.
- Avoidance of data destruction or compromise.

Further, Sir helped students explore the concept of operating system, vector and payload. He also explained the use of low level and higher level management of operating system. Vector is a route used to gain entry to computer. Payload is delivered via the vector.

Then, he discussed the process of Computer forensics. The investigations usually follow the standard digital forensic process (acquisition, analysis and reporting). Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

Techniques

A number of techniques are used during computer forensics investigations.

Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and for perform anomaly detection.

Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software has their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

In the end, Sir spoke about various terms used in computer forensics like volatile data, non-volatile data, malware footprint, rename files, copying files, printing a file, temporary internet files, windows registry, recovering deleted files and deleted vs. recycled. Sir concluded the first session mentioning that:-

1. Deleting and formatting on a hard drive does not touch the data area.
2. Often evidence can be found in deleted files and the recycle bin.
3. System clocks and default time zone settings are very important.

In the second session, Sir started with the definition of Network Forensic as “It is the capturing, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.”

Following points were discussed:

- Network Forensic Tools
- Attack Phases
- Intruder types and the intrusion process
- Hacking vs. Cracking
- Trace back Methods
- Relationship between network forensic analysis and network security technologies

Part 3

Conclusion

It is important for the students to be well acquainted with the applied aspects of the above mentioned areas and should be aware of the intricacies of implementing this technology. Keeping this in mind the guest lecture was organized for the students to impart them knowledge and make them aware about the technical skill requirement and expectation of IT industries from them in the domain “Network Forensics”. The session was very informative and included the applied and technical aspects. The speaker explained all the points in detail with demo, examples and handled all the queries with expertise. It was a great experience as the guest lecture was highly interactive.

Lecture Moments

HOD MCA, felicitating the guest speaker, Mr. Santanoo Pattnaik…!!

Mr. Santanoo Pattnaik delivering lecture on Network Forensics..!!

Students attentively listening to speaker…!!

Time to handle queries..!!