

TRACK: InfraGard Track / Cyber-crime, terrorism, and information warfare
SESSION #: ITCT#2
DATE: Monday April 19, 2010
TIME: 10:50am-12:05pm
SESSION TITLE: "Using Network Forensics to Combat Cyber Attacks"
SPEAKER(S): Joe Habib – Director of Professional Services and Education
ORGANIZATION: WildPackets

ABSTRACT: "Using Network Forensics to Combat Cyber Attacks"

Cyber attacks happen every day and in fact, every minute of every day. It is important with these attacks to not only be able to identify them when they happen, but also to track them down historically. Also called digital forensics or packet mining, network forensics is a fundamental process for identifying security breaches, finding rogue device access, and stopping network hacks and viruses. With network forensics, data is always available for reconstruction for easy analysis of cyber attacks and network security breaches.

The basic principle of network forensics is to be able to quickly and efficiently, go back in time, looking at every bit that traversed the network, and find the exact patterns that make up the attack. Using the right network forensics data mining tools, security teams can reconstruct the sequence of events that occurred at the time of a network breach or cyber attack and get the complete picture. Once those patterns are identified, it is also important to take additional steps to find out what other systems an attacker may have touched, or attempted to touch, in the network environment. Again, the speed at which this analysis takes place is very important, as more systems or data could be compromised as time passes. Once the fingerprint of the attacks are identified, precise filters can be built to find these attacks immediately in the future, thus once again, speeding the identification, notification and resolution processes. The real question is how does your tool for network forensics help you to sift through the tremendous amount of network data, quickly and efficiently? This presentation will explain network forensics in-depth and provide tricks and tips for consideration when engaging in network forensics within your organization.

SPEAKER BIO(S): Joe Habib is the Director of Professional Services and Education at WildPackets (which offer network analysis and performance solutions). Mr. Habib is a seasoned executive with proven expertise in Information Technology, eCommerce, and Systems Management. Joe possesses over 15 years experience in designing, developing, and delivering technology and information management solutions. He has managed large information and network services for several Silicon Valley and international companies. Joe holds a BA in Business and Management Information Systems with an emphasis on Telecommunications from San Jose State University. Joe holds certifications with Cisco and Microsoft.

