IEEE COMMUNICATIONS SOCIETY

Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

IEEE

Technical Talk

Cyberspace Security

Kilausuria binti Abdullah
Researcher, Security Audit & Control Dept, Mimos Berhad

Norazah binti Abd Aziz
Researcher, Security Audit & Control Dept, Mimos Berhad

Date : Friday, 12th January 2007

Venue : MCMC Auditorium,
Malaysian Communications and Multimedia
Commission, 63000 Cyberjaya

Registration : 9.00 am
Time : 9.30 a.m. – 11.30 a.m.

Abstract

Due to growing number of intrusion events, organizations are increasingly implementing various system that monitor IT security breaches. Intrusion is a sequence of attack that coming from sources like target computing or networking domain. Intrusion Detection System (IDS) is one of the technologies that widely used now for detection hostile actions. For heterogeneous sources, correlation one of the methods is used to recognize intrusion plan by examining alerts. In essence, correlation can be defined as a form of abstracting the alert data. In this presentation, there are four correlation method approaches are discussed followed by the correlation process. At the end of this presentation, we present our implementation of correlation solution in our intrusion detection system called Cyber Early Warning System (CEWS). In this presentation,

Jointly organized by IEEE Communications Society and Malaysian Communications and Multimedia Commission

For more information, please contact: Yeow (yeow@tmrnd.com.my)

Kilausuria will introduce attack scenarios, intrusion detection technologies and discuss issues and challenges. Norazah will present the alert correlation, the correlation method and process, followed by alert correlation implementation in current system.

Speakers Biographies:

Kilausuria binti Abdullah received her BSc. in Computer Science from University Technology Malaysia, Skudai Johor Bahru in 2000. In Nov 2000, she started her employment with MIMOS Berhad and joined the Security Lab under iLogin project which provides single sign-on solution. In mid of 2001, she joined the Product Development department under the Firewall project. She started her research area in IDS related technologies when she was involved in MSM (Managed Security Monitoring) project which develops a solution for 24x7 monitoring of a customers' network. After that, she moved to Open Source group under the Asia Open Source Centre project. She was involved in the website promotion and moderating the mailing list. In 2003, she joined the Cyber Early Warning System project where she design and develop the Signature Management, Incident Response Management and Vulnerability Assessment modules of the system. Now, she is part of the Security Audit & Control research team where her main area of interest and specialization is in intrusion detection system, incident handling, hacking techniques, responses and signature analysis. She is a GIAC Certified Incident Handler (GCIH) by The SysAdmin, Audit, Network, Security (SANS) Institute, USA since August 2006.

Norazah binti Abd Aziz graduated from the University Technology Malaysia with a bachelor's degree in Computer Science. She started her employment with Imatera Digital Image Services Sdn Bhd as programmer. There, she was involved in the development of Sistem Pengurusan Data Kadaster for the Department of Survey and Mapping of Malaysia (JUPEM), the system was used to generate digital maps of certified plans. Norazah joined MIMOS Berhad in November 2000. Her first project is the iLogin Server which provides single sign-on solution. She had also contributed towards building the Open Source Software Regional Centre of Excellence by developing and maintaining the website for virtual centre to promote open source and free software in Asia and provide a hub of information about open source activities in Asia (www.asiaosc.org). Her involvement in network security began in 2002 when she was involved in the development of the Network Monitoring System and Firewall. After that she joined the Managed Security Monitoring project to develop 24x7 monitoring of a customers' network. This monitoring includes early warning facilities and intrusion detection capabilities. In 2003, she was involved in development of the Cyber Early Warning System which is a network monitoring system with advanced intrusion detection features. Norazah obtained certification as a GIAC Certified Intrusion Analyst (GCIA) from the SANS Institute (SysAdmin, Audit, Network, Security Institute, USA) in August this year. Now, she be is part of the intrusion detection research team where her main area of interest and specialization is in intrusion detection system.