Global Event Asia

An attacker has compromised a server in your organization's network using an exploit for the DCOM interface with RPC in Windows Server; allowing for remote arbitrary code execution. You are the IT officer in charge of security operations for

your company and is required to find out how the box was compromised and by whom.

Using only a Snort binary capture file from the remote log server, you are to conduct

a complete analysis of all IDS captures, log files, and an inspectionof the file system.

The question is :
WHAT DO YOU DO NEXT ?

CSi
COMPUTER SYSTEM INVESTIGATION

IT SECURITY & FORENSICS: SECURING & ANALYZING ELECTRONIC EVIDENCE

DATE

18, 19, 20 November 2013

VENUE

JW Marriott Hotel, Kuala Lumpur

Certificate Of Attendance awarded by

STRATEGIC PARTNER

AKATICONSULTING

IT Security & Forensics: Securing & Analyzing Electronic Evidence

Similar to the hugely popular TV series "CSI : Crime Scene Investigation" Computer Systems Investigation is the science of collecting, preserving and analyzing electronic evidence in computer systems and networks. Technology has taken the world by storm in recent decades and the dark side to computers rises, when individuals use them to lash out malicious assaults. Welcome to the front lines of the war on cyber crime…

The current global financial crisis has indeed sparked a rise in cyber crimes. According to the latest surveys, more than a fifth of the malicious activities in the world originate from the Africa and Asia Pacific region. The increase and penetration of internet across Asia has been phenomenal and today the challenges of information security have also grown manifold. This survey should be a wake-up call for every company in Asia and to realize the importance of establishing a proactive information security and forensics program.

Computer Forensics is an emerging area for I.T. practitioners and it is becoming imperative for organisations to take both preventive and corrective actions if their systems are to be protected from any kind of compromise by external malicious elements.

TOP REASONS WHY YOU SHOULD ATTEND THIS!

1. Candid factual information you can use. Yes, really use!
2. Unpublished materials(Yr 2013) presented in the workshop.
3. Interactive Hands-on workshop.
4. Interactive environment to address your concerns.

COURSE LEARNING

- Why it is nearly impossible to "wipe" sensitive data from a computer, and how do you retrieve those data?
- How do you choose the best hardware and software for your Incident Response/Forensic Labs?
- What are the available technologies for forensic hardware and software - A vendor neutral perspective
- Forensics on devices other than computers: USB thumb drives, SD, MMC , Mobile Phones, iPod, Blackberry devices
- Handling evidence for legal action vs. evidence for purely information gathering.
- Conducting remote "live" extraction of data which is forensically sound from a workstation
- Image File Forensics: Fact vs fiction
- Preventable network intrusions. Safe configurations and practices.
- Identity theft: How serious can it get?
- Survivability after successful attacks of your network.

COURSE AUDIENCE

- CISO and Staff
- Chief Technology Officers and Staff
- Computer Security Officers and staff
- Managers at all levels who use networks and are concerned about protecting sensitive information
- Program Managers
- Law Enforcement Community who are responsible for computer systems
- First Responder Communities
- Inspector General Staff
- Digital and Computer Forensic Executives, Managers, and Staff
- Incident Response Executives, Managers and Staff

"One of the things that scares me about the current economic downturn is the increase of cyber crime . . ."

Roger Halbhee, Microsoft's Chief Security Advisor for Europe, the Middle East & Africa

"Revenues from cyber crime now exceed those of drugs crime, and are worth some US$1 trillion annually . . ."

Edward Amoroso, AT&T's Chief Security Officer

"Krishna is one of the best trainer so far I've met in Malaysia. His valuable real lif experience in security hacking made the technical subject become an interesting topic. Great work and highly recommended!"

Chim Chin Kiat, Global Infrastructure Operation Technical Lead (Security Management) - Shell I.T International

COURSE OUTLINE

DAY ONE

Becoming a CSI in Today's World

Information Forensics Process

Incident Response - Critical First Responders

Electronic Discovery v

A Journey through the Gargantuan World of Computer Forensic Tools

Part I Software Forensics Tools

Part II Hardware Forensics Tools

Case Study

DAY TWO

Data Drive Forensics

Part I Recovering Deleted Files

Part II Recovering Deleted Partitions

Image Files Forensics v

Analyzing Firewall & IDS Logs

Investigating Web & Network Attacks

Case Study

DAY THREE

Windows 7 Forensics v

SatNAV & GPS Forensics v

Mobile Forensics - Smartphones & iPods

Mobile Forensics - iPhone, Android & Blackberry v

TSCM - Technical Surveillance Counter Measure v

Writing Investigative Reports

Testifying in the Court of Law

COURSE FACILITATOR *Krishna Rajagopal*

Almost synonymous with the Information Technology field, Krishna Rajagopal holds accreditations as a Certified Ethical Hacker (CEH), and a Certified EC-Council Instructor (CEI). He has been involved in the Infosec & Forensics field for more than a decade and to date, he holds more than 50 various professional certifications and is recognized internationally as one of the best in the industry for Computer Security/Computer Forensics.

In the field of Penetration Testing, Krishna has conducted Penetration Testing for some of the most prestigious organisations in the globe. He has actually conducted Penetration Tests for 3 out of the Top 5 banks in the world. In the field of IT forensics, Krishna has assisted numerous Police Forces around the globe on IT security measures, and is often called up an as an international expert witness on numerous occasions. He is accredited as a specialist in the successful investigation and prosecution of hackers, fraudsters and other scum from the dark, underground world of the internet. Krishna has also been approached by the enforcement in Mexico, and has been consulted on the creation of a customized training and education methodology for the Policia Federal (Federal Police), Mexico, for the sole purpose of investigating cyber criminals.

As a sign of his impeccable training skills and feedback, EC-Council has honored Krishna for two years in a row (2011, 2012) as Instructor Circle of Excellence Award - A prestigious award where winners were selected from more than 87 countries. A distinguished and popular speaker, he has conducted training and given talks at numerous events around the globe, the latest being in Mexico City where he delivered his address on a series of conferences organized by Universidad de Tecnologica de Mexico (UNITEC) where nothing less than 1000 participants arrived every night for his conference on Ethical Hacking and Computer Forensics. He is also regularly interviewed at BFM 89.9 radio station in Malaysia. Krishna also conducts trainings and consulting in various countries across 5 continents of the world and has appeared in numerous television interviews and press releases talking about IT Security and various IT related issues

REGISTRATION FORM

	PARTICIPANTS	DESIGNATION	EMAIL
1.			
2.			
3.			
4.			
5.			

ORGANISATION	
CORRESPONDING ADDRESS	
CONTACT PERSON	
SIGNATURE	
TEL	
FAX	
EMAIL	

TERMS & CONDITIONS

1. **FOR PRIVATE SECTOR** - The organisers reserve the right to stop any registered delegate from taking part in the event if no proof of payment or an undertaking letter is presented.
2. **FOR GOVERNMENT SECTOR** - A Local Order (LO) or Letter of Approval to participate must be presented before or during the event.
3. **CANCELLATION POLICY** - For any cancellations, kindly inform the secretariat in writing / fax 3 days before the event, otherwise the conference fees will be billed. Replacement will / can be accepted. No refund for cancellation made after **13 November.2013**
4. **REGISTRATION FEE** - **RM3,600.00 per delegate**.
5. **GROUP DISCOUNT** - **RM100.00** per delegate will be given for group registration of Five (5) or more from the same organisation (same time and same billing source).
   Fees to include Lunch, Refreshments and Workshop materials / documentation)
6. **PAYMENT MODE** - All Bank Draft / Local Order / Cheques must be crossed and made payable to
   WORLDWIDE CORPORATE RESOURCES SDN BHD
7. **BANK TRANSFER**
   Bank - **Maybank Berhad**
   Account Name - **Worldwide Corporate Resources Sdn Bhd**
   Account No - **5140 5717 4708**

All enquiries must be forwarded to:-

Secretariat
GlobaleventAsia
Worldwide Corporate Resources Sdn Bhd
Level 36 Menara Citibank
165 Jalan Ampang, 50450 Kuala Lumpur
Tel: 603-4142 0960 / 4141 6378 / 2169 6347
Fax: 603-2788 3605 / 2169 6168
Email: noura@globaleventasia.com
globalevents.wcr@gmail.com
Attn: Ms Nora (HP: 016-665 6138)

www.globaleventasia.com

CSI IT SECURITY & FORENSICS

HRDF CLAIMABLE
The Fee is Claimable from HRDF under SBL Scheme
(Subject to HRDC Policies and Procedures)

No Siri: 1378

MINISTRY OF FINANCE

eperolehan

** The organiser reserve the right to make any necessary amendments to the benefits of this workshop.*