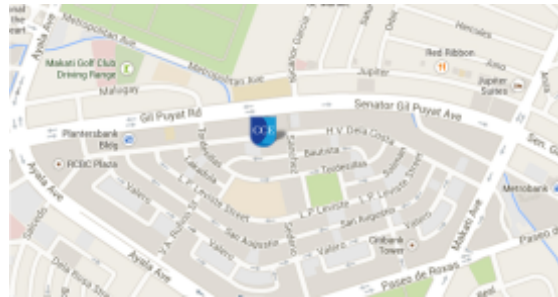## Network and Information Security

Package inclusions:

- Program fee
- Training kit
- AM/PM snacks
- Lunch
- Certificate of course completion

Venue:

Ateneo de Manila University - Salcedo Campus
3/F Ateneo Professional Schools Bldg.,
130 H.V. Dela Costa St., Salcedo Village,
Makati City, Philippines

CUSTOMIZED PROGRAMS

We offer companies our tradition of service and excellence through customized programs fit for special organizational needs. *Call us and lead the change!*

Accreditations:

Member:

Follow us:

cce.ateneo.edu
June 10, 2019

ATENEO DE MANILA UNIVERSITY
GRADUATE SCHOOL OF BUSINESS

Institute for the Digital Enterprise

Network and Information Security

October 11 - 12, 2019

CCE CENTER FOR CONTINUING EDUCATION

DATES
October 11 - 12, 2019
Friday - Saturday
8:30 am - 4:30 pm

PROGRAM FEE
Php 11,800.00 (Early Eagle Rate until Sept. 27)
Php 12,800.00 (Regular Rate)

HOW TO REGISTER
Online
www.cce.ateneo.edu

Email
sales.cce@ateneo.edu

Call
+63(2)830.2043

Schedules and prices may change without prior notice.

Network and Information Security is designed to provide network professionals and IT managers, with a broad view of the field of ethical hacking and information security. Basic concepts to be discussed will include the hacking process, developing an IT security plan and best practices it mitigating breaches in IT security in your company.

You are given hands-on exposure to ethical hacking tools, that enable you to gain the skills and knowledge necessary to understand the technical risks related to managing an information security program within an organization. Case studies and business examples will be included in this course to complement the conceptual coverage to provide real-world context.

Network and Information Security

objectives

After this course, you will:
1. Identify your organization's IT security needs;
2. Develop an IT security plan, customized to the needs of your company;
3. Plan, execute and harden your company's IT security posture; and
4. Hack targets of evaluation to gain insight on how hackers get in and out of your systems.

about CCE

AGSB's Center for Continuing Education (CCE) supplements the degree programs by addressing issue-specific industry concerns that require immediate, purposeful, and focused response. AteneoCCE is an industry resource and partner, doing advocacy on emerging critical issues and convening interested entities so that together, they can tackle a common concern. Conscious of its vital role in society, the Center continuously improves its products and services in a creative, innovative and trend-setting way to address the changing needs of clients. Successful Ateneo CCE participants may earn elective units in AGSB MBA Programs.

who should attend

Networking professionals, IT managers, and decision-makers that need and want to understand the security solutions that exist today.

resource person

MR. CHINO ANTONIO S. RODRIGUEZ is currently the IT Head and Solution Architect of Neural Mechanics and Digenomix, both data science and consulting companies headquartered in Singapore and the Philippines.

He has over a decade of experience in Consulting, IT Management, IT Audit, Project Management, Solution Architecture and Ethical Hacking and Forensics.

Prior to this, he held other posts, such as: PMO Director for ADEC Innovations; Solution Architect and IT Head for Natural Intelligence Solutions; and Solution Architect and IT Head for DANATEQ4. He has held various managerial positions in IT for the Ateneo Graduate School of Business, Ateneo CCE and Ateneo de Manila University.

Mr. Rodriguez holds a Master's Degree in Information Technology from the Ateneo de Manila University, Certifications in Ethical Hacking and Forensics from EC-Council and a Diploma in Applied Project Management from the Ateneo Graduate School of Business-Center for Continuing Education.

program content

I. Introduction to Information Security
II. Introduction to Ethical Hacking and how it differs from "hacking"
III. Top Trends in Information Security
IV. The Hacking Process
(Kali Linux is part of the tool-set of the course.)
   A. Gathering Information
      1. Find information about people
      2. Profile websites
      3. Retrieve lost information from websites
      4. Email Tracking
   B. Gaining Access
      1. Google Hacking
      2. Hacking Passwords
      3. Sniffers
      4. Credit Card Fraud
      5. Identity Theft
      6. Sniffers
      7. Piracy
      8. Web attacks
      9. DOS and DDOS
      10. Piracy
      11. Corporate Espionage
      12. WiFi Hacking and Wire-chalking
      13. Social Engineering
      14. Phishing
   C. Clearing Tracks
      1. How not to get caught
      2. Create Fake Identities
      3. Stay anonymous in the Web
   D. Mitigation Techniques
V. Consultation. Developing your IT Security Plan. (Templates will be provided)

Note: The course does not guarantee proficiency in the tools demonstrated in two days. It guarantees awareness of the hacking techniques and the knowledge of how to prevent such from happening.