“Cybersecurity: Preparing the Workforce”

Hosted by Keio University & Sasakawa USA
2-3 March 2017
Keio University, Mita Campus
Website: http://cysec-lab.keio.ac.jp/sympo1703/index.html
Map: https://www.keio.ac.jp/en/maps/mita.html

DAY 1 (Thursday, March 2, 2017) Workshops

13:30 – 17:30

Workshop A: Addressing Cybersecurity across an Organization - Pamela Passman, CREATe
3F Room 532, West School Building

How secure is your company’s critical information? Today’s competitive business environment - marked by collaborative innovation, vast amounts of sensitive data, and complex third party networks - increases cyber risks for companies of all sizes.
Through lectures, panel discussions with experts and real-world examples, and a cyber breach scenario, these and other topics will be addressed:

- Best practices for implementing the right “people, processes and technology” for effective cybersecurity
- Aligning cybersecurity in broader enterprise risk management programs; and adhering to guidance and standards such as ISO 27001 and the NIST Cybersecurity Framework
- The most effective strategy and structure for cyber risk management: from the CISO to third party partners

Workshop B: Hacking Windows AD with PowerShell (1 of 2) – Andy Robbins
1F North Hall, North Building

Description: Between 90 and 95% of the Global 1000 companies use Active Directory as their directory service of choice for managing authentication and access to corporate assets. In nearly all publicly released breach reports, real adversaries are targeting Active Directory for initial access, privilege escalation, lateral movement, and data access and theft. In the last few years, PowerShell has proven a powerful tool for adversaries and defenders alike in attacking Active Directory domains during each of those breach phases. In this workshop, students will learn how to use PowerShell to identify and exploit common misconfigurations in an Active Directory domain.
Hardware requirements: A laptop with at least 16GB of RAM and at least Windows 7 installed.
Prerequisite skills: Students should have basic familiarity with Windows and Active Directory, as well as basic familiarity with networking concepts.

- Why?
  - Why should we be Hacking? Why target Active Directory? Why use PowerShell?
- Initial Access
  - E-mail phishing basics - Command and control infrastructure design and deployment
  - Crafting PowerShell Beacon payloads - Payload delivery techniques
- Privilege Escalation
  - Overview of Active Directory and Windows privileges
- Discovering host-based and network-based privilege escalation opportunities with PowerShell

Workshop C: Mobile Phishing (1 of 2) – Georgia Weidman
1F Meeting Room A/B, Faculty Research Building

Attackers are gaining access to the Enterprise through endpoints, but locking down laptops and desktops does no good when users spend the majority of their time on mobile devices. Mobile isn’t just another endpoint. In this session, students will learn a holistic threat model for mobile, how hackers are specifically exploiting mobile, and penetration tests against mobile phones based upon real world attacks. Students will practice attack vectors and learn which payloads provide what data. Participants should bring a laptop capable of running a VMWare virtual machine and Android Emulators with at least 40GB of free space for virtual machine handouts. An Android and/or iOS mobile phone for testing is also required.

“Cybersecurity: Preparing the Workforce”

Hosted by Keio University & Sasakawa USA
2-3 March 2017
Keio University, Mita Campus
Website: http://cysec-lab.keio.ac.jp/sympo1703/index.html
Map: https://www.keio.ac.jp/en/maps/mita.html

DAY 2 (Friday, March 3, 2017) Workshops

13:30 – 15:00

Workshop E: CYBER CHALLENGE: Responding to a Major Cyber Incident – Riley Repko, Cisco Systems
3F Room 532, West School Building

This cyber workshop, entitled *Sudden Impact*, is the first of its kind for this annual cybersecurity conference. It will allow attendees to contribute as "players" to a realistic emergency scenario, which, with no warning, impacts Japan's daily way-of-life. How can your insights help to solve these challenges?
Tabletop exercises (TTX) are the best way to assess any organization’s emergency preparedness without having to experience an actual disaster. The intent for this workshop is to help raise awareness, validate effective procedures, strengthen relationships with partners, share new ideas and ultimately, identify critical gaps in response and recovery efforts. The TTX will be fast-paced and involve audience participation.
Attendance is limited to 200. Your participation is key and this TTX should also be an excellent learning event.

TTX Timeline: 90 minutes
10-15 Minutes: Scenario overview and execution process by the players (audience). Based on size of attendance, the audience will be divided into 4 groups of approximately 50 players.
45-50 Minutes: TTX takes place. "Events" will be added during this time-frame. Decisions made by each group, led by a group leader, will be documented by Scribes and made available for the Hot Wash discussion.
20 Minutes: Hot Wash. 3-5 experts from government agencies/industry will comment on the collected results from each of the groups.

15:20 – 18:20

Workshop F: Mobile Phishing (2 of 2) – Georgia Weidman
6F G-SEC Lab, East Research Building

This is a second running. Please see Workshop C for details.

Workshop G: Hacking Windows AD with PowerShell (2 of 2) – Andy Robbins
3F Room 532, West School Building

This is a second running. Please see Workshop B for details.

Note: All workshops will be conducted in English without interpretation.