WORKSHOP 2:

Ethical Hacking within IoT Ecosystem

About the workshop:

This workshop would enable participants to gain appropriate knowledge for penetration testing and ethical hacking within the IoT ecosystem.

This workshop would demonstrate real-life attacks using various attacking tools and share best practices to mitigate and patch these security vulnerabilities within IoT ecosystem.

The participants can learn how to use free and open source tools instead of using costlier commercial tools in the workshop.

Duration: 1 day (9 am till 5pm)

Prerequisites:

Knowledge on Linux/UNIX command line, computer network, ICMP, TCP and UDP

Target participants:

Regulators, Ethical Hackers, Software Security Architects, Software Engineers, Software Designers, System Administrators, Security Administrators, Penetration Testers and anyone with the interest in understanding security vulnerabilities within the IoT ecosystem.

Workshop Outline

1. Introduction to IOT Eco-system.

2. Security vulnerabilities within IoT Ecosystem.

3. Introduction to Ethical Hacking
    a. What is Ethical Hacking and Penetration Testing
    b. How Does Exploitation work?
    c. Exploitation Phases
    d. Server side and Client-side attacks
    e. Information gathering techniques
    f. Vulnerabilities detection techniques

4. Hands on introduction to the following tools for the hacking within the IoT ecosystem environment
    a. VMware
    b. Kali Linux - Metasploit framework, auto-sploit, airmon, nmap
    c. Android O/S
    d. Wifi
    e. Metasploitable OS

5. Hands on vulnerabilities detection for connected devices using following techniques
    a. Using Shodan
    b. Using Google hacking
    c. Using CLI based search using auto-sploit

6. Hands on vulnerabilities exploitation in the IoT embedded system – Linux, Android and Wifi
    a. Linux Buffer Overflow exploitation
    b. Client-side attacks
    c. Server-side attacks
    d. Phishing attacks
    e. Post exploitation - hacking camera, microphone, address book, files, directory etc
    f. Monitoring and capturing wireless traffic
    g. Flooding wireless beacon broadcast
    h. Dictionary and brute force attack for WPA/WPA2 credentials
    i. Wireless De-authentication

Trainer Profile

Professor Emeritus Dr Sureswaraan Ramadass

Professor Emeritus Dr Sureswaran Ramadass is the currently the Chairman of ITU/UN IPv6 and IOT Centre of Expertise at Malaysian University of Science and Technology (MUST). He is also the Scientist at NLTVC Sdn Bhd. (NLTVC is a next generation communications research and development company).

He is currently the Emeritus Chair of Global IPv6 Forum's IPv6 Education Certification Logo Programme. He is also the Chair of IPv6 Forum Malaysia. He is also the Chairman of IPv6 Working Group of Malaysian Research and Education Network (MYREN). He is also the Head of APAN Malaysia.

He was the former Chairman of APAN (Asia Pacific Advanced Networks) and former Director of the National Advanced IPv6 Centre of Excellence (NAV6) at Universiti Sains Malaysia. He is also former Chairman of the Asia Pacific IPv6 Task Force (APV6TF) whom involved in promoting IPv6 within the region and globally.

His past participation in the global IPv6 arena includes being a consultant to ITU, a Director of the Japanese AI3 project and is also the Head of the AI3 (Asian Internet Interconnections Initiative) for Malaysia.

Prof Sureswaran's academic contributions are vast and have attracted numerous academic and research ventures to the university and state. He has published research papers in over 200 international and national journals, and conference proceedings, filed over 12 patents given numerous keynote addresses, written chapters and provided materials for 7 books, chaired numerous international conferences, and has reviewed papers for over 30 international and national publications.

Mr. Navaneethan C Arjuman

Mr Navaneethan C. Arjuman is currently the Senior Consultant with ITU/UN IPv6 and IOT Centre of Expertise at Malaysian University of Science and Technology (MUST).

He is pursuing his PhD Fellow at National Advanced IPv6 Centre, Universiti Sains Malayisa. He is a trained engineer by profession and holds 1st Class Honours degree in Communication and Signal processing from Staffordshire University, United Kingdom.

Navaneethan C. Arjuman is currently the Coordinator of Global IPv6 Forum's IPv6 Education Certification Logo Program. He holds the position of Co-chair of IPv6 Working Group of Asia Pacific Advanced Network (APAN). He is an IPv6 Global Forum's Certified Trainer for Certified Network Engineer for IPv6 (CNE6), Certified Security Engineer for IPv6 (CSE6) and Certified Network Programmer IPv6 (CNP6).

He has served as a Director of NLTVC Education Sdn Bhd, CEO and Director of KHEC Systems Sdn Bhd and KHEC Solutions (India) Pvt Ltd, Senior Manager at BayCom Sdn. Bhd. prior to his appointment with iNetmon Sdn Bhd as a Director. Mr Nava also served in Maxis Communications Bhd as a Senior Channel Manager. Apart from corporate roles, Mr Nava also lectured in Sedaya University (formerly known as Sedaya College)

Mr. Mohd E Hefaz

Mohd E Hafez is currently a senior trainer at ITU/UN IPv6 and IOT Centre of Expertise in Malaysian University of Science and Technology (MUST). He is also a Ph.D. fellow at the Malaysian University of Science and Technology (MUST).

He was the team leader of security enthusiasts under the Sudanese Internet Society (ISOC Sudan Chapter). He has 9 years of experience in telecommunication company and service providers, besides his activities in NGOs and Internet communities around Africa and the middle east.

He is currently an executive/steering committee member of the Sudan Internet Governance Forum, Sudan Network Operator Group, and Sudan IPv6 Task Force.

In 2016 he founded the Free and Open Source Foundation of Sudan, to leading the tech community in this field and promote the use of Open Source. He also leads a group of researchers and Engineers to deploy the DNSSEC for the Country Top Level Domain (ccTLD) of Sudan.

For more registration and more information, please contact sc2019@wsconferences.com