5 Days Workshop/Training on "eSuraksha" a Practical Approach on Network & Web Application Security (PNWS-2018)

Dated: 10th to 14th December, 2018

PNWS- 2018

Organizations should strengthen and solidify all their security systems and technologies to prevent security breaches of any kind. Preliminary & advanced training's are being organized to make employees understand and feel responsible for safeguarding the assets of the organization.

Under the aegis of **project on Information Security Education and Awareness (ISEA), Ministry of Electronics and Information Technology, Govt. of India**, the aim is to generate quality human resources in the core of Information Security at various levels.

A 5-days training/workshop module on **eSuraksha - " A Practical Approach on Network & Web Application Security"** is being organized to provide deeper insights in the said domain. The training is free of cost and relevant handouts will be given to each participant.

The workshop/training programme looks for significant contributions to all major fields of the **Networks and Web Security** in theoretical and practical aspects. It brings together experts from **C-DAC Mohali**, government and academia, experienced in engineering, design and research. All interested Govt. employees are invited to participate through proper channel in PNWS-2018, which will be held in the **Department of Computer Science & Information Technology, Central University of Jammu**, Jammu & Kashmir, India.

The PNWS-2018 offers a rich program, including theory and hands-on. We seek your participation to make it a successful event. Theme of the workshop/training: **"eSuraksha".**

Important Dates

Submission of Nomination Form Deadline	20 November, 2018
Notification for short listed candidates	30 November, 2018
Workshop/Training Programme	10-14 December, 2018

Venue

Department of Computer Science and Information Technology, Central University of Jammu, PO Bagla (Rahya Suchani), District Samba J&k-181143

Workshop/Training Schedule

“A Practical Approach on Network & Web Application Security”

December 10-14, 2018 (10.30-16.30hrs)

Day 1: Introduction

o Introduction to Information Security
o What is Hacking and why learn it?
o Building your Hacking environment
o Basic overview of Linux – Terminal and Linux Commands
o Browser Security, Privacy and Tracking
o Introduction to Browser Fingerprinting
o Email Forgery/ Hacking/ Tracing/ Tracking/ Spoofing
o The Zero Trust Model
o Threat Modelling and Risk Assessments
o Hackers, Crackers and Cyber Criminals
o Cyber Law - IT Act 2000 and ITA 2008 Introduction
o Defence against Online Attacks
o Hidden Secret Messages behind Images – Steganography
o Building and Writing the Trojans

Day 2: Network Penetration Testing

o Introduction to Network PT
o Network Basics & Information Gathering
o Gathering More information using Autoscan and Zenmap
o MITM - ARP Spoofing using Arpspoof and MITMf
o Detecting ARP Poisoning Attacks
o Bypassing HSTS and Session Hijacking
o Injecting & Spreading JS Malware
o Packet Sniffing – HTTP and HTTPS
o HTTPS Data Sniffing with SSLSTRIP and DSNIFF
o URL and Mail Sniffing with URLSNARF and MAILSNARF
o Basics of Wireless – A Packet Analyzer Tool
o Analysing HTTP Traffic with Wireshark
o Detecting Suspicious Activities with Wireshark
o Nmap Introduction and Basics
o Version and Operating System Detection with Nmap
o Nessus Installation and Scanning
o SSH Remote/ Local Port Forwarding
o SSH Hardening And Configuration
o Network Monitoring with TCPDUMP, Wireshark, Tshark and Iptables
o Finding Malware and Hackers with Wireshark Tool
o Hacking with Netcat – Listening and Exploitation (On both Windows/ Linux)
o Overview of SETOOLKIT – Social Engineering Toolkit
o Cracking Windows/ Linux Passwords – OnLogin

Day 3: Website Penetration Testing

o Introduction – What is a Website?
o Overview of HTTP Status/ Versions

o Scanning HTTP Methods – HEAD/TRACE/OPTIONS/GET/POST/DEBUG/PUT/DELETE
o Information Gathering using HTTP Headers
o Introduction to OWASP Top 10 Attacks
o Discovering Technologies Used on the Website
o Gathering Comprehensive DNS Information
o Sub-domain Brute forcing with Dirbuster
o Basic Input Validation Attacks – Breaking into Databases
o SQL Injection – Threats and Exploitation – Practical Demo
o Dangers of SQL Injection Vulnerabilities – String/ Boolean/ Blind/ Time
o Discovering SQL Injections and Extracting Data using SQLMAP
o Right Way to Prevent SQL Injection
o Discovering and Exploiting File Upload Vulnerabilities
o Local and Remote File Inclusion Attacks
o Cross Site Scripting – Attacks and Types
o Exploiting XSS – Hooking Vulnerable Page Visitors to BeEF
o Preventing XSS Vulnerabilities
o Exploiting Whole Server with HTTP PUT Method
o SSL – Introduction, Types and Configuration
o Session Mismanagement – Hijacking/ Replay Attacks
o WordPress and Joomla CMS Exploitation
o Complete Website Security Testing with Burp Suite/ Acunetix and IBM Appscan
o Best Practices on Secure Coding

Day 4: Wireless & Wi-Fi Security

o Introduction to Wireless Attacks and Threats
o Types of Wireless Protocols
o Wi-Fi Weaknesses – WEP, WPA, WPA2, TKIP and CCMP
o Wi-Fi Weaknesses – WPS, Evil Twin and Rouge AP
o Wireless Security – Secure Configuration and Network Isolation
o Who is on my Wi-Fi Network?
o Targeted Packet Sniffing using Airodump-ng
o WEP Cracking – Theory Behind Cracking WEP Encryption (Practical Demo)
o Fake Authentication and ARP Request Replay Attacks
o Exploiting WPS Security – WPA Cracking
o Capturing the Wireless Handshake with/ without De-authentication
o WPA/ WPA2-PSK Cracking With Evil Twin (MITM)
o WPA/ WPA2-PSK Cracking with Fluxion (Wireless Phishing)
o Cracking Wireless Key using a Wordlist – Dictionary Attack
o Generating Fake Dictionary Lists with Crunch
o Discovering Hidden Wireless Networks with Aireplay-ng Tool
o Bypassing MAC Filtering
o Performing Denial of Service on Wireless Networks

Day 5: Post Exploitation Attacks

o Introduction to Post Exploitation Attack
o Basic Information Gathering and Exploitation
o Introduction to Metasploit Framework

o Installation and Configuration of Metasploitable2
o Exploiting a Code Execution Vulnerability
o Targeted Scanning with Metasploit Framework
o Overview of Armitage Tool
o Nexpose – Installation and Configuration
o Veil Overview and Payload Basics – Malware Kit
o Generating an Undetectable Backdoor using Veil and Weevely
o BeEF Overview and Basics Exploitation with JS Hooking
o Stealing Credentials/ Passwords using Fake Login Prompt
o BeEF – Gaining Full Control over Windows Target
o Detecting Trojans using a Sandbox/ Manually
o Meterpreter Basics – Post Exploitation Module
o Maintaining Access – Using FUD Backdoors
o Exploiting Devices on the same Network
o How Passwords are Cracked using Hashcat and John the Ripper
o Creating & Gaining Access with Reverse Shell
o Persistent Backdooring with MSFVENOM
o Metasploit Attacks over WAN with/without Port Forwarding
o Hacking Windows (XP/7/8/8.1/10) with Metasploit Framework
o Hacking Windows (XP/7/8/8.1/10) with CHAOS Framework
o Android Hacking over LAN/WAN
o Fake APK Generation and Persistence Phone Backdooring
o MITM – Man in the Middle Attacks using Ettercap and Driftnet

---

Resource Persons

A Team of highly experienced and technically proficient Scientists from C-DAC Mohali

---

Workshop Committee Members

Chief Patron
Shri G. Parthasarthi, Chancellor, Central University of Jammu, J&K, India.

Patron
Prof. Ashok Aima, Vice Chancellor, Central University of Jammu, J & K, India

Co-Patron
Prof. Devanand, Dean School of Applied and Basic Sciences, Central University of Jammu, J & K, India

Organizing Committee

- Dr. Yashwant Singh, Head & Associate Professor, Department of CS & IT, Central University of Jammu, J & K, India

- Dr. Arvind Selwal, Assistant Professor, Department of CS & IT, Central University of Jammu, J & K, India
- Dr. Bhavna Arora, Assistant Professor, Department of CS & IT, Central University of Jammu, J & K, India
- Mr. Neerendra Kumar, Assistant Professor, Department of CS & IT, Central University of Jammu, J & K, India
- Dr. Deepti Malhotra, Assistant Professor, Department of CS & IT, Central University of Jammu, J & K, India

---

Registration Fee

No fee will be charged from the participants for attending the workshop

---

Email for workshop related queries: pnws2018@gmail.com

Contact Person(s)

Dr. Yashwant Singh
Head and Associate Professor
Department of Computer Science and Information Technology,
Central University of Jammu.
Mobile No. 9418203623
Email Address:yash22222k1@gmail.com

Dr. Arvind Selwal
Assistant Professor
Department of Computer Science and Information Technology,
Central University of Jammu.
Mobile No. 9896262552
Email Address:arvind.cuj@gmail.com

Mr. Neerendra Kumar
Assistant Professor
Department of Computer Science and Information Technology,
Central University of Jammu.
Mobile No. 9354666851
Email Address:neerendraiimt@gmail.com

5 Days Workshop/Training on "eSuraksha" a Practical Approach on Network & Web Application Security (PNWS-2018) 10th to 14th December, 2018

Nomination Form

Name:……..

Institution:……..

Is the Institution is Govt./Private:……..

Designation:……...

Department:…….

Education Qualification:……

Specialization:……

Communication Address:……..

……..

Contact No.:…….

Email Address:……

Declaration by the candidate

The given information is true to the best of knowledge. I agree to abide by the rules and regulations governing the programmme. If selected, I shall attend the workshop for the entire duration.

Place:

Date:

Signature of Candidate

Signature of the approving Authority with Seal

Note: Registration form to be sent at pnws2018@gmail.com