nbi
NATIONAL BANKING INSTITUTE
"The Banking Academy of Nepal"

PRESENTS

PROGRAMME ON NETWORKING & CYBER SECURITY

AT STATE BANK INSTITUTE OF INNOVATION AND TECHNOLOGY, HYDERABAD, INDIA

Background:

National Banking institute Ltd. (NBI) an apex level banking and finance academy presents a "Six–Day" residential program on **"Network and Security"** with the collaboration of State Bank Institute of Innovation and Technology (SBIIT) Hyderabad, India. Network and Security program will have 3 days dedicated to **"Networking and Network Securities"** and 3 days to **"IS and Cyber Security".**

SBIIT is an Apex Training Institute in State Bank of India, engaged in IT related training, research, development, innovation and e-learning. It has played a key role in the transition of SBI from a traditional bank to an IT savvy Bank.

The program aims to provide inputs various terms in cyber security and networking including networking essentials, switching concepts, routing protocols, VPN Technologies, WAN Technology, IPV6, Networking audits in Banks, etc.

Target Audience

- IT Heads
- IT Officers
- Sanctioning Officers at head offices

(The audience are recommended to officials handling networking and cyber security for Banks with prior exposure to basic networking)

Program Details:

Date: 25th to 30th November 2019
Time: 9:00am to 5:00pm (Residential)
Venue: SBIIT Campus, Hyderabad, India
Methodology: Classroom Lecture, Practical Exercises, Tools pertaining to the networking and Cyber security, Interactions and Discussions.
Deadline for Nominations: 7th November 2019

Networking and Network Securities

COURSE CONTENT

1. Networking Essentials

• Basics of networking
• Compare & contrast OSI & TCP/IP models
• Compare & contrast TCP & UDP protocols
• Impact of infrastructure components in a network
• Firewalls, Access points, Wireless controllers
• Basic virtual network infrastructure
• Compare & contrast collapsed core and three-tier architecture
• Compare & contrast network topologies "Star, Mesh, Hybrid"
• Select the appropriate cabling type (Straight & Cross)
• Apply troubleshooting methodologies to resolve problems
• Configure, verify & troubleshoot IPv4 addressing & subnetting
• Compare & contrast IPv4 address types
• Unicast, Broadcast, Multicast
• Describe the need for private & public IPv4 addressing

2. Switching Concepts

• Describe & verify switching concepts
• MAC learning & aging, Frame switching, Frame flooding, MAC address table
• Interpret Ethernet frame format
• Troubleshoot interface & cable issues (collisions, errors, duplex, speed)
• Configure, verify, and troubleshoot VLANs (normal/extended Range) spanning multiple switches
• Access ports (data & voice), Default VLAN
• Configure, verify, and troubleshoot inter switch connectivity
• Trunk ports, Add & remove VLANs on a trunk
• DTP, VTP (v1&v2), and 802.1Q Native VLAN
• Configure, verify, & troubleshoot STP protocols
• Port Fast, BPDU guard
• Configure & verify Layer 2 protocols
• Cisco Discovery Protocol, LLDP
• Configure, verify, & troubleshoot (Layer 2/Layer 3)
• Ether Channel—Static, PAGP, LACP
Describe the benefits of switch stacking & chassis aggregation

3. Routing Protocols

• Introduction to Router and Routing Protocols:
• Static Routing, Dynamic Routing, Default Routing
• IP Addressing, Summarization (Auto and Manual)
• EIGRP Features, EIGRP Update Process
• Configuration and Verification of EIGRP Tables
• EQUAL and UNEQUAL Metric Route Load Sharing
• Summarization, EIGRP Metric Tuning
• Manipulating Hello and Hold Timer
• Static Neighbor configuration
• Passive Interfaces, Authentication
• Neighbor ship over WAN, EIGRP Stub features
• Default Route with EIGRP
• Route Filtering by using ACL,
• Forwarding decision based on route lookup
• Frame rewrite
• Interpret the components of a routing table
• Prefix, Network mask, Next hop, Routing protocol code
• Administrative distance, Metric
• Gateway of last resort & Admin distance
• Configure, verify, & troubleshoot inter-VLAN routing
• Router on a stick & SVI
• Compare & contrast static routing & dynamic routing
• Compare & contrast distance vector and link state routing
• protocols
• Compare & contrast interior and exterior routing protocols
• Configure, verify & troubleshoot IPv4 static routing
• Default route, Network route, Host route, Floating static
• Configure, verify & troubleshoot single area & multi-area
• OSPFv2 for IPv4

4. VPN Technologies

• Describe the different methods used in cryptography
• Describe VPN technologies
• Describe the building blocks of IPSec
• IPSec site-to-site VPN with pre-shared key
• Verify VPN operations
• Secure Sockets Layer (SSL) VPN

Networking and Network Securities

5. WAN Technology

- Configure & verify PPP and MLPPP on WAN interfaces using local
- Authentication
- Configure, verify, & troubleshoot PPPoE client-side interfaces using
- local authentication
- Configure, verify, & troubleshoot GRE tunnel connectivity
- Describe WAN topology options
- Point-to-point, Hub and spoke, Full mesh, Single vs dual-homed
- Describe WAN access connectivity options
- MPLS, Metro Ethernet, Broadband PPPoE, Internet VPN (, site-to-site VPN, client VPN)
- Configure and verify single-homed branch connectivity using eBGP
- IPv4 (limited to peering and route advertisement using Network command only)
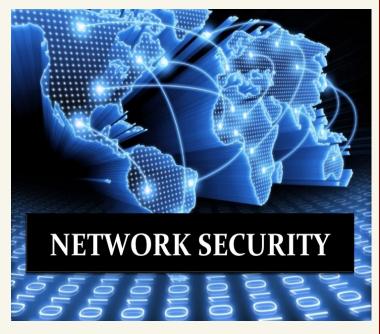- Describe basic QoS concepts

6. IPV6

- IP Version 6 Addressing
- Identify IPv6 addressing to use in LAN/WAN environment
- Configure, verify & troubleshoot IPv6 addressing
- Configure & verify IPv6 Stateless Address Auto Configuration
- Compare & contrast IPv6 address types
- IPV6 Address Representation, Types of IPV6 Addresses
- Global Route Aggregation, Static IPV6 Address Configuration
- Stateful DHCP, Stateless Auto Configuration
- Multicast and other Special IPV6 Addresses,
- IPV6 Routing Protocols and IGP Redistribution

7. Network Security

- Secure Network Management and Reporting
- Describe secure network management
- Implement secure network management
- ACL
- Cisco Firewall Technologies
- Operational strengths and weaknesses of firewall
- Describe stateful firewalls
- Describe the types of NAT used in firewall zone-based policy firewall
- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Common Layer 2 Attacks
- Describe Layer 2 security using Cisco switches
- Describe VLAN security
- Implement VLANs and trunking
- Implement spanning tree

IS and Cyber Security

COURSE CONTENT

8. Understanding IT Risk Management
- Introduction to Information Security and Cyber Security.
- How information security and cyber security are interconnected.
- Understanding Vulnerabilities, Threats and Risks.
- What is threat modeling?
- Demo on Threat Modeling.

9. Cyber Frauds and Investigations
- What is cybercrime and its impact on BFSI industry.
- How do you identify and investigate cybercrime?
- Various types of cybercrimes in BFSI industry.
- How does cyber fraud occurs?
- How do you identify and investigation procedure?
- Foot Printing.
- Identifying and securing the evidence.
- Investigation process and introduction to various tools.
- Preparation of IOC's & Report.
- Presentation of Reports.
- Legal formalities.

10. Auditing Data Centre
- Understanding the DC Infrastructure and Communications.
- Understanding the resources and its accessibility to external world.
- Evaluating the cabling layout, Fire safety and other GDPR compliances.
- Evaluating Operating Systems and its licensing.
- Evaluating IDS and IPS and firmware updates?
- Understanding the gaps and escalating with NC.

11. Network Audit in Banks
- Understanding the networks and switching in banking & financial environment.
- Evaluating the Network Data Flow and Routing patterns.
- Evaluating Switching and implementation security between the networks.
- Evaluating the routing protocols and its effective working.
- Finding the weakness in Switching and Routing structure.
- Identifying the Content Filter rules and evaluating effectiveness.
- Auditing the IDS and IPS in terms of bypassing the firewall.
- Evaluating the effectiveness of Access Control List (ACL)
- Evaluating the banner grabbing attack possibilities.
- Evaluation and assessment of DDoS attacks.
- Preparation of report.

12. Auditing Cyber and Information Security Audit of IT Governance Process
- Overview on GDPR compliance.
- Understanding the systems and infrastructure compliance with various standards of PCIDSS, SOX, GDPR, HIPPA and others.

13. Application security and code review Web Application Security: Threats—Cross Site Scripting/ iFrame Injection/ SQL Injection/ Remote File Inclusion/ OS Command Injection
- DDOS, Mitigating DDOS, Application layer DDOS
- DDOS threat to banks, Mitigating DDOS through Cloud
- Perimeter based defense against DDOS
- Cross siting scripting, iFrame Injection, SQL Injection
- Remote File Inclusion, OS Command Injection

Cyber Security

14. Malware Attacks and Analysis Cryptography and HTTPS Transaction Analysis Defense against APTs Web Application Security Phishing and Countermeasures Authentication Techniques VAPT Mobile Banking Security Antivirus Management Domain Security Management Application White listing

- Malware Attacks and Analysis
- Cryptography and HTTPS
- Transaction Analysis
- Defense against APTs
- Web Application Security
- Defense against DDOS
- Phishing and countermeasures
- Authentication Techniques
- VAPT
- Mobile Banking Security
- Antivirus Management
- Domain Security Management
- Application White listing

NATIONAL BANKING INSTITUTE LTD.

Central Plaza, 6th Floor, Narayanchour, Naxal, Kathmandu.
T: +977 1 4415903/5, 4436001
F: +977 1 4441351

E: programs@nbi.com.np, W: www.nbi.com.np

Mr. Gangaraju Murali Mohan Raju
Sr. Technical Manager
Zoom Technologies Pvt. Ltd., India

Experienced Senior Technical Manager with a demonstrated history of working in the computer and network security industry. Skilled in Network Administration, Routing & Switching and Network Address Translation (NAT), VPN, MPLS. Strong engineering professional with a Master's degree from Osmania University.

Has been deputed by Zoom Technologies to visit Salisbury, Wiltshire, UK in Jan 2003 to Train the Engineers of British Army on Advance Networking and Network Security and also visit to Switzerland in June 2002, for a Network Security Conference.

Mr. Hozefa Z Topiwala
Network Security Engineer
Zoom Technologies Pvt. Ltd., India

Network Security Engineer with 16 years of experience in designing, configuring and implementing Firewalls, IPS, UTM & Anti-Spam solutions, Performing Vulnerability Assessment and Penetration testing, Real time experience in planning and implementing Network Security using Firewalls, IPS & UTM devices.
Certified trainer by Microsoft, Kaspersky, Certified Mobile Forensic Expert by Hancom, Certified Netasq Administrator, Cisco Certified Network Associate, Ethical Hacking & Countermeasure Expert certified by US Council.

Mr. Raghavendra Kumar VS
Network Security Engineer
Zoom Technologies Pvt. Ltd., India

Network Security Engineer with 10 years of experience in designing, configuring and implementing Firewalls, IPS, UTM & Anti-Spam solutions, Performing Vulnerability Assessment and Penetration testing, Auditing and implementing IT Network Security solutions for office campuses, perform troubleshoot and technical support for corporate clients at their location or remotely and provide solutions.
Certified Solutions Expert by Microsoft, Certified Netasq Administrator and Certified Netasq Expert, Cisco Certified Network Associate, Ethical Hacking & countermeasure expert certified bu US council.

NATIONAL BANKING INSTITUTE LTD.

Central Plaza, 6th Floor, Narayanchour, Naxal, Kathmandu.
T: +977 1 4415903/5, 4436001
F: +977 1 4441351
E: programs@nbi.com.np, W: www.nbi.com.np