Network Security Analyst Network Security Analyst Network Security Analyst Princeton, NJ Authorized to work in the US for any employer Work Experience Network Security Analyst Comcast Corporation, Union August 2016 to March 2017 Responsibilities Conducted application penetration testing of 50+ business applications. Conducted Vulnerability Assessment of Web Applications using Nessus. Manage and maintain Firewall systems and IPS along with VPN access controls. Support in detecting, understanding and resolving information security incidents and remediation. Perform risk analysis to identify points of vulnerability and recommend disaster recovery strategies and business continuity planning. Manage and maintain and troubleshoot Active Directory forest infrastructure. Locate and assimilate information to provide context for security events. Experience in using IAM software(IBM). Identify and evaluate marketing opportunities to increase the website traffic and online production. Evaluate, deploy and manage information security system solutions such as strong authentication, key management, IPS, SIEM, antimalware, vulnerability scanners, MDM and others. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc Developed and delivered IT Services Management (ITSM) solutions based on ITIL best practices that focused on the people, process, and technology perspectives of providing business solutions. Skilled using Burp Suite, IBM APP Scan, Acunetix Automatic Scanner, NMAP, Havij, Dirbuster, Qualysguard, Nessus, SQLMap for web application penetration tests and infrastructure testing. Performing onsite & remote security consulting including penetration testing, application testing, web application security assessment, onsite internet security assessment, social engineering, wireless assessment, and IDS/IPS hardware deployment. Conduct network monitoring and intrusion detection analysis using various Computer Network Defense (CND) tools, such as Intrusion Detection/Prevention Systems (IDS/IPS), Firewalls, Host Based Security System (HBSS), etc. Capturing and analyzing network traffic at all layers of the OSI model. Monitor the Security of Critical System (e.g. e-mail servers, database servers, Web Servers, Application Servers, etc.). Change Management to highly sensitive Computer Security Controls to ensure appropriate system administrative actions, investigate and report on noted

irregularities. Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures. Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality. Network Engineer - -MPLS & Security Capital Metro - Austin, TX October 2015 to July 2016 Responsibilities Experience working with design and deployment of MPLS Layer 3 VPN cloud, involving VRF, Route Distinguisher(RD), Route Target(RT), Label Distribution Protocol (LDP) & MP-BGP. Convert Branch WAN links from TDM circuits to MPLS and to convert encryption from IPsec/GRE to Get VPN. Advanced features in the IP routing protocols such as OSPF tuning (failure detection, flooding, SPF Computation, VPNV4(MP-BGP, peer group, route reflector),MPLS(LDP), Qos [EF,CS,AF,BE], VPN-MPLS(L2[Gb traffic], L3[VOIP and SIGTRAN]) for traffic segregation, MPLS-TE by RSVP-TE/FRR, and security & management (logging, Syslog, SNMP, NTP, DNS ,SSH ,CDP ,TACACS+, VRRP, NSRP, HSRP) Coordinating the implementation of switched networking infrastructure for server and client building blocks. Redesigned F5 load-balancer configuration and topology to eliminate outages during F5 active-standby failovers. Built automation scripts for device inventory, backups, and (some) changes; scope: 800 managed Cisco and F5 network devices. Leveraged a single domain-wide public wildcard SSL certificate to reduce costs of securing servers while maintaining host-level security requirements. Troubleshooting and monitored routing protocols such RIP, OSPF, EIGRP & BGP. Install and maintain security infrastructure, including IPS, IDS, log management, and security assessment systems. Assess threats, risks, and vulnerabilities from emerging security issues Designed and implemented networking for disaster recovery sites. Perform and create procedures for system security audits, penetration-tests, and vulnerability assessments. Develop scripts to maintain and backup key security systems. Periodic data center inspections, and on call participation, and helped other staff members with networking problems. Network Security Engineer Optum - Philadelphia, PA January 2015 to September 2015 Responsibilities Experience working with design and deployment of MPLS Layer 3 VPN cloud, involving VRF, Route Distinguisher(RD), Route Target(RT), Label Distribution Protocol (LDP) & MP-BGP. Conducted security assessment

of PKI Enabled Applications. Experience with design and configure Fiber Channel over Ethernet (FCoE) on Cisco Nexus 5548 devices. Convert Branch WAN links from TDM circuits to MPLS and to convert encryption from IPsec/GRE to Get VPN. Experience with migrating from Cisco ASA 8.2 version to Cisco ASA 8.4 Version. Responsible for Cisco ASA firewall administration across our global networks. Migration of existing IPSEC VPN tunnels from one Data Center to another Data Center, due to decom of existing Data Center, which involved working with Partner Companies. Experience with converting WAN routing from EIGRP/OSPF to BGP (OSPF is used for local routing only) which also involved converting from Point to point circuits to MPLS circuits Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality. Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching. Enabled STP attack mitigation (BPDU Guard, Root Guard), using MD5 authentication for VTP, disabling all unused ports and putting them in unused VLAN. Implement and configured VRRP/GLBP (on distro/core switching), HSRP on different location of office on the switched network and managing the entire multilayer switched network Configuring various advanced features (Profiles, monitors, Redundancy, SSL Termination, Persistence, HA on F5 BIGIP appliances SSL termination and initiation, Persistence, Digital Certificates, executed various migration projects across F5 and hands on with F5 BIGIP LTMs/EM. Managed user accounts for role based access controls, event based alerts and event based alerts and server appliances Monitor the security system logs (i.e., intrusion detection system, firewall system logs, etc.) and reports on discovered anomalies or problems (i.e. insufficient disk space, inappropriate access patterns, etc.). Conducted Compliance Audits. IT Network & Security Analyst ICOMM Tele Ltd - Hyderabad, ANDHRA PRADESH, IN February 2012 to April 2014 Responsibilities Designed & implemented networks for broadband technologies; including BPON, GPON, DSL, HiCap & Wireless. Worked with cutting edge cloud technology using Heroku and Hadoop. Developed hybrid cloud delivery model allowing for customers to choose the mix of public and private clouds to meet their individual needs. Analyzed business necessities & possibilities to implement modern technologies to improve QoS and reduce

cost. Projected & managed several network applications. Ensured consistency among several software & hardware systems. Responding to inquires/issues from end users related to active directory. Worked extensively with engineering, design & record systems; including VISIO, ICGS (Microstation), iVAPP, iBault, vRepair LFACS & TIRKS. Conducted detailed design reviews & audits to ensure that all network objectives are fulfilled Performed field work; including path surveys, installation & commissioning support, troubleshooting & optimization. Recommended modifications to improve speed of operations and system security measures. Configured and managed AD, Exchange, DHCP, WSUS, WDS, Antivirus and backup servers in the corporate network. Established security policies for systems, and designed and managed secure networks for clients. Configured servers to meet specific requirements, including hard drives, memory, planners, video cards, token ring raid arrays, and load software. Education Master of Science degree in Computer Networks & Security Illinois Institute of Technology - Chicago, IL Skills Cisco (1 year), IDS (2 years), IPS (2 years), MPLS (1 year), security (4 years) Additional Information AREAS OF EXPERTISE: Network and Systems Security Research and Development Cost Benefits Analysis Policy Planning / Implementation Data Integrity / Disaster Recovery Risk Assessment / Impact Analysis Technical Skills: Languages C, C++, HTML/HTML 5, Java, JavaScript, PHP. Platforms Windows 98/2000/XP/Vista/Windows 7, Windows Server 2000/2003 Database My SQL 5.0, MS Access, MS SQL 2000 Packages MS-Office, Visual Studio 2005/08/10. Networks Routing & Switching, VPNs, VOIP, PBX, MPLS, WAN and QOS etc. Cloud Platform Google Cloud, Microsoft Azure, AWS. Firewalls Cisco ASA firewalls, Checkpoint, Palo Alto, Fortinet, Sophos. Load Balancers F5 BIG-IP, Citrix Netscalar. Virtualization tools VMware, Citrix. Vulnerability Assessment tools Metasploit, Nessus, Nexpose, Qualysgard, NMAP, OWASP ZAP, Burpsuite, IBM App scan, DIR-Buster, Kali Linux etc. IT & Management Tools GFI LanGuard, Solarwinds, Splunk etc. IDS/IPS Snort, Tipping Point, IBM Proventia, McAfee Network Security Platform

Name: Terry Young

Email: vincent86@example.org

Phone: 318.754.7317x4157