Penetration Tester Penetration Tester Penetration Tester Dallas, TX Over 7+ years of infrastructure and security experience with specialization in application security, Data Security and SIEM technologies Strong understanding of OWASP top 10 and SANS 25 standards Hands on experience working with tools like Acunetix, Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy and IBM Appscan & HP Fortify etc., Conducted white/gray box penetration testing on the financial systems using Kali Linux, Cobalt Strike for OWASP top 10 Vulnerabilities like XSS, SQL Injection, CSRF, Privilege Escalation and all the test-case of a web application security testing Used LDAP injections techniques of exploiting Web applications that use client supplied data Proficient in analyzing different security threats to organizations by identifying the indicators that a security incident is underway, composing and creating security policies and procedures to be followed when an incident is detected, and investigation methods use to collect evidence for prevention and prosecution. Experience as a privacy/ security analyst, with applicable knowledge of regulatory compliance procedures related to SOX and PCI Perform Vulnerability assessment and policy compliance and PCI compliance using Qualys and IBM App scan Provide consultative support with implementation of remediation steps, standards, and best practices. Work Experience Penetration Tester AIG Insurance - Dallas, TX June 2015 to May 2016 Test the applications & infrastructure using Kali Linux & other security tools Implemented Tenable Nessus, Tenable SecurityCenter, and customized audit compliance dashboards of system configurations and content for the Vulnerability / Configuration Compliance Management and Monitoring Programs. Brute force assessment to insure strong passwords and encryption. Performed dynamic and static analysis of web application using IBM AppScan Analyze systems for potential vulnerabilities with the help of Qualys VM that may result from improper system configuration, hardware or software flaws Port scanned servers using NMAP and closed all unnecessary ports to reduce the attack surface. Performed live packet data capture with Wire shark to examine security flaws. Conducted white/gray box penetration testing on the financial systems using Kali Linux, Cobalt Strike for OWASP top 10 Vulnerabilities like XSS, SQL Injection, CSRF, Privilege Escalation and all the test-case of a web application security testing Used LDAP injections techniques of exploiting

Web applications that use client supplied data Used Websense to protect the company's network from, malware and data theft, as well as prevent users from viewing inappropriate content. Port scanned servers using NMAP and closed all unnecessary ports to reduce the attack surface. Ensure compliance with policies, procedures, and regulations (i.e. PCI DSS) Security Consultant Austco - Dallas, TX October 2014 to May 2015 Served as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure components Monitored SIEM and IDS/IPS feeds to identify possible enterprise threats. Investigate and triage threats to determine nature of incident Troubleshoot and researched security incidents using SIEM applications, IBM QRadar Security Intelligence Platform. Helped to research open-source intelligence feeds for current and emerging threat information Utilized tools such as NMAP, Nessus, Qualys, and Nexpose to accomplish network reconnaissance and surveillance in preparation for exploitation. Assist in engineering integration to other key security systems Create and support security awareness programs to inform and educate employees IT Security Consultant Bajaj Allianz General Insurance Co. Ltd - Hyderabad, Andhra Pradesh May 2012 to August 2014 Hyderabad, India Linux server management (Red Hat, CentOS, Debian). Tasks include; creating/managing backup scripts, creating managing logRotate scripts, manually clearing hard drive space, changing IP addresses, installing Perl modules, installing/upgrading software packages, modifying software/system configs (ex: changing HTTPD variables and server IP), process monitoring while a system is in an alarm state. Installation and testing of new Bajaj's proprietary software releases. The software is used to create and manage configurations of remote enterprise network hardware. Lab hardware is used to test the software and configurations internally before it is installed onto the production servers. Internal support for product launch team

Configuration and troubleshooting of various Cisco and Fortinet routers/firewalls to verify functionality Server Migration from bare metal to virtual machines as part of a one-time project to move away from aging hardware platforms. Test plan development and execution for new products and features as required by new versions of the Bajaj's proprietary software Technical documentation review; process enhancement Review and analyze alerts and logs from Firewalls

(FW), Intrusion Detection Systems (IDS), Antivirus (AV), and other security threat data sources. Maintain SIEM/log analysis solution, including data collection, aggregations, and regular exception reporting. Security Analyst Dhithi Info serve - Dallas, TX June 2009 to April 2012 Bangalore, India Installation and Configuration of Linux systems like CENT OS, Red Hat and Windows Servers. Also involved in user account management Actively involved in Monitoring the server's health status using different tools Responsible for application support on Red Hat servers which included apache configurations Experience working with Storage Area Network (SAN). Experience in Performance monitoring, usage and load the system, changing kernel parameters for better performance. Worked with Perl, Shell Scripting (ksh, bash) to automate administration tasks. RPM package installation & upgrade released by Red Hat in the repository Administration of client machines using SSH and FTP Supported for application upgrade and rollback, Start or Stop services in Linux Servers. Education Bachelors of Technology in Technology Jawaharlal Nehru Technological University Additional Information TECHNICAL SKILLS: Operating Systems Microsoft: Windows XP/Vista/7/Server 2003/Server 2008; Linux: CentOS, Red Hat, Fedora, Ubuntu Server/Desktop, Kali Linux; Backtrack 4 & 5; UNIX: Mac OSX Lion, FreeBSD, Mainframe Exp. OWASP/SANS Vulnerability XSS, SQL Injection, CSRF, Security Misconfiguration, Sensitive Data Exposure, Insecure Direct Object Reference IDS/IPS McAfee Intrushield / NSM, McAfee e-Policy Orchestrator (ePO), Sourcefire, Motorola AirDefense WIDS, ISS SiteProtector SIEMs ArcSight ESM, IBM QRadar, RSA Envision, Splunk Security Tools App Scan, Wireshark, Snort, Tcpdump, Tcprelay, Nmap, Netcat, Iptables, Malwarebytes, Nessus, John-Ripper, SQLmap, Acutenix, Burp Suite, Hydra, Aircrack-ng etc., Protocols Ethernet, LAN/WAN/MAN, TCP/IP, DNS, DHCP, FTP, TELNET, SMTP, POP3, SSH, UDP, ICMP, IPsec, HTTP/HTTPS, Network Topologies, Firewalls, VPNs, IDS, port scanning, and implementing Incident Response Procedures

Name: Mary Mccormick

Email: matthew37@example.com

Phone: 824-644-7840x424