IT Security Analyst IT Security Analyst IT Security Analyst - Centene St. Louis, MO ? Around 5 years of IT security experience in securing the network and protecting the business of the client thus ensuring confidentiality, integrity and availability of data and resources. ? Strong Proficiency in Vulnerability Assessment using Rapid7 NeXpose, Nessus and OpenVAS tools. ? Understanding of Static Application Security Testing (SAST) tools such as HP Fortify (MicroFocus). ? Understanding of Dynamic Application Security Testing (DAST) tools such as Nessus. ? Proficient in major Penetration Testing tools used in Kali Linux such as Metasploit, Meterpreter, Nmap, TcpDump, Wireshark, Setoolkit, Sqlmap, BeEF etc. ? Experience in computer Network Penetration Testing with different technique methods. ? Experience in creating reports after vulnerability assessments and penetration testing. ? Proficient in OSINT (Open Source Intelligence Tool) such as Maltego, Google Dorking etc. ? Good Proficiency in Enumerating & Foot printing using recon-ng, Theharvester, Urlcrazy, Dnsenum, Knockpy, SSLyze, Wappalyzer, shodan.io tools. ? Proficient in knowledge of OWASP TOP 10 methodology and web application vulnerability standards. ? Good knowledge of Web Application Scanners such as BurpSuite, Qualys and OWASP ZAP. ? Familiar with network, web app vulnerabilities attack methods and real-time traffic analysis using Wireshark. ? Understanding of critical web application vulnerabilities such as cross site scripting and SQL Injection. ? Knowledge of open security testing standards and projects, including OWASP secure coding practices and HIPPA, PCI DSS, GDPR Compliance. ? Good experience with SANS Top 20 critical security controls businesses should implement. ? Proficient in securing networks and servers using Cisco Sourcefire IDS, IPS, FireEye, Firewalls and Antiviruses. ? Good Knowledge in configuring VM's in windows Hyper-V and VMware. ? Experience in Security Incident and Event Management (SIEM) such as Splunk. ? Understanding of forensic methodologies and tools such as Cain & Abel, Autopsy, OpenPuff steganography. ? Understanding of various networking protocols such as TCP/IP, DNS, SMTP, HTTP/HTTPS, Subnets, VLANs, FTP, Access Control Lists (ACLs) etc. ? Knowledge of operating system, application security and cyber security tools. ? Ability to interact effectively with different infrastructure teams like network, systems, compliance, database, Exchange, Firewall etc. ? Experience in conducting information security policy awareness campaigns to train and educate employees. ? Meets security challenges energetically and logically to maintain security posture. ? Strong analytical and problem-solving skills needed to perform the job of a security analyst. ? Capable of independently learning new technology by utilizing available documentation and vendor support resources. ? Good experience in Researching, identifying, and mitigating new security threats to information systems. ? Basic Knowledge on Scripting Language. Authorized to work in the US for any employer Work Experience IT Security Analyst Centene - St. Louis, MO February 2018 to Present Responsibilities: ? Performing Web Application security testing using BurpSuite. ? Using a popular SAST (Static Application Security Testing) tool called HP Fortify (MicroFocus) to manually test the web applications for vulnerabilities. ? Performing Vulnerability assessment using Nessus. ? Conducting open security testing standards and projects, including OWASP secure coding practices and HIPPA, PCI DSS, GDPR Compliance. ? Using Wireshark to scan and monitor various ports to observe encoded traffic. ? Escalating and identifing the root cause of failure and find a solution to meet deadline of system handover remote connection tools like SSH, SCP, TELNET. ? Handling critical incidents and avoiding firm data breach. ? Performing real-time monitoring, research, analysis, investigations, reporting and handling escalations on security breach events like network intrusion detection, host intrusion detection, proxy logs, unauthorized application logs detected on DLP, Splunk and Social engineering attempts via call or email. ? Maintaining user access controls, processes, and procedures to prevent unauthorized access, modification, or misuse of the resources. ? Performing network maintenance and system upgrades including service packs, patches, hot fixes and security configurations. ? Creating and managing firewall rules for different teams. ? Using Burp Suite, Acunetix, Sqlmap and Nmap for VAPT, and prepared reports for audit according to OWASP top 10 with all issues and their mitigation. ? Using Qualys for automated scans and vulnerability management, prepared & presented reports to Client & Management, raised Incident for vulnerability mitigation. ? Real-time investigation & analysis of event logs using SIEM tools from Network Security Components and devices such as Firewalls, FireEye, Intrusion Prevention System (IPS), Antivirus and Email Gateways.   Environment: BurpSuite, SAST, HP fortify (MicroFocus), OpenVAS, Nessus, OWASP

Top 10, OWASP ZAP, Sqlmap, Acunetix, Nmap, Qualys, SIEM - Splunk, Kali Linux, Windows 10, Metasploit, Wireshark, Meterpreter, PCI DSS, GDPR, IDS, IPS, Antivirus, Firewall. Security Analyst Comcast - Philadelphia, PA January 2017 to February 2018 Responsibilities: ? Used HP Fortify a SAST (Static Application Security Testing) tool to test the web applications for critical vulnerabilities like cross site scripting and SQL injection. ? Used Nessus to Dynamically test the web application security for vulnerabilities (DAST). ? Tracked the incidents/ security events till closure, co-ordinate with the respective team for resolution and reporting. ? Worked with the team to improvise new threats that occur and mitigating the risk factor. ? Worked with various departments to improve detection of security threats and breaches. ? Used Cisco Sourcefire IDS/IPS for daily Analysis and monitoring network traffic which triggered based on Snort Rules. ? Prevented malicious traffic based on Rule documentation, Packet Text, Affected System, Attacker IP and system vulnerabilities. ? Monitored logs for Syslog servers and Health for IDPS sensors. Prepared daily, weekly and monthly security reports. ? Monitored IDS (Intrusion Detection System) & IPS (Intrusion Prevention System) logs & analyzing them at the packet level, traffic flow analysis, checking false positives and reporting the events. ? Analyzed raw logs coming from different log sources like firewalls, IPS/IDS, Proxy, Antivirus etc. and creating security related use cases using SIEM. ? Incident response for various types of alerts coming from network devices. ? Prepared reports for audit according to OWASP top 10. Environment: BurpSuite, HP Fortify, Nessus, SAST, DAST, OWASP Top 10, Cisco Sourcefire, Kali Linux, Windows 10, Metasploit, Snort, IDS, IPS, Antivirus, Firewall, Incident Response, Proxy, IDPS Sensors, cross site scripting, SQL Injection. Security Analyst Sathya Labs - Hyderabad, Telangana June 2015 to December 2016 Responsibilities: ? Responsible for carrying out System and network wide Vulnerability Assessment and Penetration testing to assess the security level of systems and network devices at client's networks. ? Maintained and analyzed the security risks on to the whole network, servers and the systems through several vulnerability tools. ? Verified weaknesses by leveraging attacker techniques to evaluate the difficulty and effectiveness of potential attack from various threat actors. ? Vulnerability Scanning and Patch Management using s/w tools like Nessus. ? Patch Management, and Antivirus compliance Performing scanning using MBSA tool to maintain patches and security updates. ? Performed enumeration and footprinting using Recon-ng, Urlcrazy, Theharvester, Dnsenum, Knockpy, SSLyze, Wappalyzer, Shodan.io tools. ? Analyzed/Researched activities on hacker exploits and latest security trends. ? Analyzed the Emails and categorized them to Spam/Phishing/Spoofing to determine the impact on the network and act accordingly. ? Analyzed social engineering scams reported by users and taking best suitable action to mitigate those scams. ? Determined the machines which are infected with Malware by performing detailed investigations and validating the data received from them to take appropriate actions. ? Analyzed Phishing and Spam related activities and notifying to the users. Environment: Kali Linux, Windows 10, Nessus, MBSA, Nmap, Wireshark, Mimecast, Netcat, TcpDump, Metasploit, Meterpreter, Recon-ng, Urlcrazy, Theharvester, Dnsenum, Knockpy, SSLyze, Wappalyzer, Shodan.io IT Security Analyst Avontix - Hyderabad, Telangana January 2013 to May 2015 Responsibilities: ? Executed daily vulnerability assessments, threat assessment, mitigation and reporting activities in order to safeguard information assets and ensure protection used automated tools for exploiting vulnerabilities. ? Managed Vulnerability scanning activities and prepared vulnerability reports using NeXpose. ? Documented Vulnerabilities found and suggested the developers for remediation and bug fixing. ? Used penetration testing procedures for vulnerability identification. ? Attempted to break into systems and applications to determine weaknesses. ? Utilized Metasploit, Aircrack Suite, NeXpose, BurpSuite, Sqlmap and Nmap security tools to assist in assessments. ? Performed firewall and router security setting and rule-set audits. ? Directed research pertaining to the latest vulnerabilities, tools and the latest technological advances in combating unauthorized access to information and other security vulnerabilities. ? Planned security policy awareness campaigns for employees of different departments. Environment: Windows 10, Kali Linux, NeXpose, Metasploit, Aircrack suite, Sqlmap, Nmap, Wireshark, Security Policies. Education Master's in computer science in computer science University of Illinois at Springfield - Springfield, IL Bachelor of Technology in Information Science and Engineering in Information Science and Engineering Dr. Ambedkar Institute of Technology Skills Ids, Ips, Metasploit, Nessus, Nexpose

Name: Beverly Benitez

Email: greenalexander@example.org

Phone: +1-400-521-7759x066