Security Engineer Security Engineer Security Engineer - Fahrenheit IT Pittsburgh, PA ? Around 8+ 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. ? Proficient in securing networks and servers using Cisco Sourcefire IDS, IPS, Checkpoint Firewall and Antiviruses. ? In-depth knowledge of TCP/IP, IP protocol suite and OSI Model. ? Good experience on Cisco Routers: GSR 12000, 7600, 7500, 7200, 3800, 3600, 2800, 2600, 2500, 1800, 1700, 800 series. ? Experience on Catalyst Switches: 6500, 4000, 3550 and 2900 series. ? Good experience on various firewalls including Cisco ASA 5500 series, Cisco PIX 500 series. ? Proficient in configuring, troubleshooting ACLs (Standard, Extended, and Named), Layer 2 protocols including VTP, STP, RSTP, PVRSTP+ and VLANs. Experience in Security Incident and Event Management (SIEM) such as Splunk. ? Strong Proficiency in Vulnerability Assessment using Rapid7 NeXpose, Nessus and OpenVAS tools. ? Proficient in knowledge of OWASP TOP 10 methodology and web application vulnerability standards. ? 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. ? Understanding of Endpoint Privilege Manager tool called CyberArk to block and contain attacks at the endpoint. Also used CyberArk Password's Vault for Privilege Account Security. ? Good Proficiency in Enumerating & Foot printing using recon-ng, Theharvester, Urlcrazy, Dnsenum, Knockpy, SSLyze, Wappalyzer, shodan.io tools. ? Knowledge of Python as a scripting language in designing penetration testing tools such as MAC changer, network scanners, packet sniffers, vulnerability scanners, code injectors, file interceptor, ARP and DNS spoofers etc. ? Understanding of Incident Handling and Incident Response Procedures. ? Strong experience in Configuring VLANs and implementing inter VLAN routing. ? Experience in upgrading and troubleshooting Cisco IOS to the Cisco Switches and routers. ? Good

knowledge of authentication protocols including PAP, CHAP, WPA, TACACS+, and IPsec. ? Good knowledge of TCP/IP, 802.x protocols, VLSM, DS0, DS1, DS3, SONET/SDH, ISDN, BGP, IPV6, NAT, VPN, Frame-relay and ATM technologies. ? 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 Risk assessment procedures. ? 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. ? Good Knowledge in configuring VM's in windows Hyper-V and VMware. ? 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. Work Experience Security Engineer Fahrenheit IT - King of Prussia, PA August 2018 to Present Responsibilities: ? Involved in the design & configured a LAN using 2691 series Routers and 2950 series switches. ? Used and maintained routing protocols like EIGRP, BGP on the Routers in the network. ? Worked on MPLS connectivity using VRF id and have broad knowledge on multi-protocol label switching for (MPLS-VPN) and traffic engineering (MPLS-TE). ? Managed the LAN Switching Environment including creating and maintaining VLANs, STP, Trunking, Port Security, VLan Security etc. ? Set up and troubleshoot secured wireless access points for

broadband internet. ? Involved in configuration of WAN connection using a 3600 series Router and Frame relay method. ? Implementation of NAT with a pool of 2 public IP addresses.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 Rapid7 NeXpose. ? 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. ? Using Python to create the scripts of tools used in penetration testing such as vulnerability scanners, network scanners, file interceptor, code injectors etc. ? Participating in Risk Assessments to provide appropriate security measures. ? Handling critical incidents and avoiding firm data breach. ? 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 Checkpoint Firewall, Intrusion Prevention System (IPS), Antivirus and Email Gateways. Environment: BurpSuite, SAST, HP fortify (MicroFocus), OpenVAS, Nessus, Python, OWASP Top 10, OWASP ZAP, Sqlmap, Acunetix, Nmap, Qualys, SIEM - Splunk, Kali Linux, Windows 10, Metasploit, Wireshark, Meterpreter, PCI DSS, GDPR, IDS, IPS, Antivirus, Checkpoint Firewall, Risk Assessments, Incident Handling. IT Security Engineer Comcast - Philadelphia, PA January 2017 to July 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. ? Used CyberArk an Enterprise Password Vault to discover, rotate and control access to account passwords. ? Worked with CyberArk Endpoint Privilege Manager to remove barriers to enforcing least privileges and to block and contain attacks at the endpoint. ? Worked with the team to improvise new threats that occur and mitigating the risk factor. ? Secure coding practices using the PCI DSS compliances. ? Wrote scripts for MAC Changer, ARP and DNS spoofers, Packet sniffer and Network scanners using Python. ? 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, CyberArk, Python, PCI DSS 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 Waystar Health - Louisville, KY September 2012 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. ? Involved in HSRP standby troubleshooting and load balancing protocol GLBP, Port channel management of the network. ? Designed VLAN's, access lists (ACL), troubleshooting IP addressing issues and Updating IOS images and other hardware installations. ? Involved in troubleshooting VLAN, STP (Spanning tree protocol), & Switch Trunk and IP subnet issues. ? Dealt with NAT configuration and

troubleshooting issues related to access lists and DNS/DHCP issues within the LAN network. ? Involved in Configuration of Access lists (ACL) on checkpoint firewall for the proper network routing for the B2B network connectivity. ? Provisioning and troubleshooting Ethernet services, Gigabit networks and Connectivity issues with WAN types (T1, E1, DS3, and Frame relay) data circuit debugging. ? 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 Network Security Analyst Franklin Fitch Inc - Austin, TX January 2011 to August 2012 Responsibilities: ? Configuration and Maintenance of Network devices. ? Managed Vulnerability scanning activities and prepared vulnerability reports using NeXpose. ? Documented Vulnerabilities found and suggested the developers for remediation and bug fixing. ? Configuring & troubleshooting networking protocols such as TCP/IP, DNS, SMTP, HTTP/HTTPS, Subnets, VLANs, FTP, Access Control Lists (ACLs). ? Implemented and managed the ACL's to control & filter network traffic. ? Handling request for the port opening in the firewall and make the required ports opened for the legitimate traffic to pass. ? Maintenance and Troubleshooting of connectivity problems using PING,

Traceroute. ? Planning and Implementation of Subnetting, VLSM to conserve IP addresses. ? Configuring STP for loop prevention and VTP for Inter-VLAN Routing. ? Performing the Configuration and troubleshooting of EIGRP, OSPF, and BGP. ? Dealt with the configuration of Standard and Extended ACLs for Security. ? Involved in providing technical assistance for LAN/WAN management and complex customer issues. ? Provided support for troubleshooting and resolving Customer reported issues. ? Planning, designing, installing and configuring LAN/WAN as per organizational requirements, governed by communication protocols. ? Investigated new technologies, software, patches, and security packages, which will improve system performance and systems administration procedures. ? 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, Windows Firewall, IP tables, TCP/IP, DNS, SMTP, HTTP/HTTPS, Subnets, VLANs, FTP, Access Control Lists (ACLs), LAN/WAN, Security Policies. Education Bachelor's

Name: Cheryl Hughes

Email: vhart@example.com

Phone: 001-558-810-4021