Lead Software/Systems Analyst and Security engineer Lead Software/Systems Analyst and Security engineer Lead Software/Systems Analyst and Security engineer - Serversify Work Experience Lead Software/Systems Analyst and Security engineer Serversify January 2013 to Present Skills/Tools used: Metasploit Pro, Backtrack 5, Unix, CentOS, Linux, Windows server 3,8 and 12, Python, Chef, OpenStack, node.js, JavaScript, Nexpose, Powershell, Bash, Django, IDA, Wireshark, Aircrack, OCL-Hashcat, Netcat, regex and stream manipulation tools (Grep, Awk, Sed), dsniff, coreimpact, network sniffers and fuzzers, Qualys, AppDetective, Webinspect, AppScan, Nikto, nCircle, tcpdump, XML, SOAP, REST, Ajax, SSLVPN, KVM, SELinux, Samba, Nagios, Clonezilla**- I am a critical member of the team helping to design and implement end-to-end client/server solutions which control the company's hardware and software product lines Deployed cloud-based and intranet services for multiple companies; often requiring Cloud service management solutions such as: Service Now, ManageEngine, LANDesk, CA Service Desk, and Remedy Penetration testing, vulnerability analysis, malware reverse engineering and detection- and using Python and Django to commit analytics logs Wrote a script to report server analytics using big data storage pods, coupled with an auto-populate cache pod built with direct-wired SSDs. This script would populate our storage cluster with commonly accessed data on-the-fly Internal/ExternalWireless/LAN/WAN network penetration testing, Web/Mobile application penetration testing, Social/Physical engineering penetration testing, and Documentation Commission complex security systems, including access, and network communications. Administration of various systems/databases. Troubleshoot complex problems Technical support of processes for customers. Create and maintain system software libraries, procedures, manuals and supporting documentation. Responsible for preparation, updating and storage of design and construction drawings I became very familiar working with the following protocolos: ARP, DHCP, DNS, DSN, FTP, HTTP, IMAP, ICMP, IDRP, IP, IRC, NFS, POP3, PAR, RLOGIN, SMB, SMTP, SSL, SSH, TCP, TELNET, UDP Senior IT/ Security/Systems Technician PS Distributing June 2009 to November 2012 Skills used: BackTrack Linux, Redhat Server, Unix/Linux, IIS and Windows Server, PostgreSQL, SQL, Metasploit Pro, Windows server 3,8 and 12, Python, Puppet, Chef, OpenStack, node.js, JavaScript, Nexpose, Powershell, Bash,

Django, IDA, Wireshark, Aircrack, OCL-Hashcat, Netcat, regular expression and stream manipulation tools (Grep, Awk, Sed), Nmap, Proxy control, Paros, Nessus, dsniff, coreimpact, network sniffers and fuzzers. OpenVas, W3of, Burp, automated VA, WebSphere Application Server, Jython, ANT, VMware, Oracle and Cisco hardware, Clustered Data OnTap, FC, FcoE, NFS, CIFS, iSCSI, NDMP, and SnapMirror ** - Responsible for the overall planning, management and completion of IT Infrastructure projects- was involved in all aspects of the software development life cycle and knowledge of networking communication protocols Penetration testing and vulnerability analysis (e, g, Cross Site Scripting, SQL Injection, Buffer Overflows, etc.) Network Security Utilized my development experience and strong object oriented design skills to create automated distribution software Maintained our server and systems cluster using a self written analytics UI- which monitored patches, zero-day exploits, malware, network traffic, and a master control panel to apply appropriate fixes Education Bachelor of Science DeVry University 2010

Name: Susan Pineda

Email: william51@example.org

Phone: (804)372-2668x7069