IT Principal Security Analyst 4 IT Principal Security Analyst 4 IT Principal Security Analyst 4 - Oracle Information security consultant with more than 14 years of systems & information security experience. Strengths in various technologies & skill sets such as security-penetration testing, automation, monitoring and virtualization. Always with a thirst for knowledge & new challenges. Work Experience IT Principal Security Analyst 4 Oracle 2015 to Present Built vulnerability management program by automating the detection & communication process for each vulnerability found. This effort includes the automation of detection, prioritization & communication of each finding until remediation. This includes to manually provide evidence of each vulnerability as well as perform SysAdmin tasks to remediate each finding. Responsible to analyze, review & remediate security vulnerabilities found in the different Oracle assets or products. Responsible to review & validate Oracle projects, products and third party engagements follow standard practices by having embedded security on all the different layers from a defensive and offensive perspective by analyzing architectures (technically and logically). Role experience: - Security Analyst (Security reviews, architecture reviews). - Penetration tester (Black box assessments, create p.o.c.'s, 0day exploits, demos). - Vulnerability analysis (Gray box assessments to Oracle products and different architectures). - Vulnerability & remediation management (Follow up with stakeholders to remediate their security weaknesses & vulnerabilities). - Incident response (track incidents, find owners, resolve incidents). - Technical writer (Write POC's, reports, advisories, standard procedures, etc). - External audits verification (verify 3rd parties pentests) Tools - Kali Linux, Qualys (all modules PC, WAS, VA), Burp Suite, AppSpider, Accunetix, metasploit, virtualbox, VMWare, Nessus PRO, AppSpider and so on. - Suricata, Alienvault, Stealthwatch. - Python (several modules such as ldap, MySQL, SMTP, etc), MySQL and Oracle APEX. Sr. Penetration Tester octubre de 2014 - septiembre de 2015 (1 a o) Responsible to execute penetration testing assessments of applications, devices and systems from various industries including retail, government, technology and communications by using different techniques to perform successfully intrusions to the different systems and provide detailed reports to the different stakeholders (executives and technicians) with all the findings and flaws to be remediated. Performed vulnerability research for different customers

and wrote articles through company blog (websec.mx & websec.ca) such as finding remote code execution vulnerabilities and backdoors on SOHO routers (including POC's or exploits published in www.exploit-db.com). Experience performing: - Application Security (web application, mobile and client-server). - Network penetration tests (red-team & blue team). Wireless, external & internal networks. - Social engineering assessments (spear phishing). Technologies used: Kali Linux, veil-framework, metasploit, sqlmap, nmap, python, ida pro, python, netcat, wireshark, vega, accunetix, burp suite professional, .net dissembler, psploit and so on Systems Integration Advisor at Dell julio de 2013 - septiembre de 2015 (2 a os 3 meses) Responsible to gather, analyze, design, test, implement and maintain (from simple to most complex) requirements to convert these into automated self-controlled processes leading to savings and reducing repetitive or human tasks following best practices inside or outside ITIL best practices depending on customer needs. Technical Leader at Softtek agosto de 2009 - julio de 2013 (4 a os) Network/Automation/Monitoring technical leader responsible for planning and delivering technical solutions for most complex requirements. - Cisco Switches - F5 Load Balancers - Checkpoint Firewalls - BMC Patrol - BMC ProactiveNet - UC4 AppWorx (Scripting, PL/SQL, perl, awk, bash, batch, etc) - Windows/Unix/Linux OS monitoring with custom implementations (scripts, SNMP, etc) Security Engineer at Softtek noviembre de 2007 - octubre de 2009 (2 a os) Responsable of executing penetration testing of applications, systems and network components by using intuitive and some help of the following software: - Metasploit, msfvenom, veil (to bypass AV). - Static and automated penetration security tools such as Burp Suite, SQLmap, Nmap, etc. - Backtrack (now Kali Linux) including metasploit, openvas, nessus, johntheripper, etc. - OWASP Testing guide (v1 & v2). - OSSEC for monitoring systems. - Build own programs and own codes to automate penetration tests. - Hardened OS & applications. Education SANS Technology Institute 2016 to 2017 diploma University of Maryland College Park - College Park, MD 2014 to 2014 Bachelor's degree in Informatics Universidad Aut noma de Aguascalientes 2001 to 2006 Skills It Security, Information Security, Cyber Security Certifications/Licenses OSCP Present GWAPT May 2017 to May 2021 Additional Information + IT Security & pentester (OSCP & GWAPT Certified), red team. + Ethical

hacking & blue team hunting activities + Process automation & Infrastructure Monitoring + VMWare VCA - Cloud, Datacenter virtualization & Workforce Mobility Certified. (VMWare-VCA)

Name: David Jones

Email: jacksonbrenda@example.net

Phone: 691-956-0074x44103