SANJIV KAWA - OSCP, OSWP, SLAE

sanjiv@popped.io | www.popped.io

SKILLS PROFILE

- Areas of expertise include enterprise network penetration testing, web application and mobile penetration testing, security architecture review and remediation planning.
- Active member in the information security community, presented at large conferences and frequently contribute to GitHub and VulnHub.
- Strong at performing analysis on enterprise network devices, system security configurations and application source code.
- Confident with Ruby, Python, Perl and Bash for scripting and automation. Experience with exploit development in Ruby, Python, IA-32 ASM and C.
- Exposure to large environments that contain VMware, Hyper-V, Citrix, as well as Windows, *NIX, and OS X systems.
- Strong work ethic with exceptional leadership skill. Able to undertake simultaneous projects with enthusiasm and follow them through from initiation to closure. Well-organized, attentive to detail, excellent situational awareness.

EMPLOYMENT HISTORY

Senior Penetration Tester, PSC – Acquired by NCC Group   9/15/2016 — Current
 San Francisco Bay Area, CA.

- iOS mobile application penetration testing, general ReST and SOAP API testing.
- Performed technical interviews for potential candidates.
- Continuation of duties.

Senior Penetration Tester, Payment Software Company (PSC)   6/8/2015 — 9/15/2016
 San Francisco Bay Area, CA.

- Conducted PCI-oriented penetration tests for large-scale retail merchants, payment processors and gateways. In all cases, the success criteria is set as gaining access to the cardholder data environment or to cardholder data.
- Created issue based PCI penetration test reports as a main deliverable for clients. Participated in numerous presentations with clients to deliver findings from these reports to both technical and non-technical audiences.
- Traveled up to 50% to client sites across the USA, Canada and Europe. Conducted all other duties remotely.
- Wrote various tools to aid with penetration testing engagements

Security Consultant, MNP LLP.   3/16/2015 — 5/31/2016
 Calgary, AB.

- Conducted internal and external vulnerability assessments and penetration tests against the computer systems, networks and web applications of a provincial government entity.
- Developed methodologies for computer systems infrastructure, network and web application vulnerability assessments and penetration testing. This was designed to aid MNP LLP's technical security assessment offerings.

Security Consultant, Graycon Group Ltd.   8/31/2013 — 2/19/2015
 Calgary, AB.

- Conducted vulnerability assessments and penetration tests for medium to large education, healthcare, energy and software organizations.
- Performed security health checks and policy development for organizations spanning across various industries.
- Assisted in developing the managed security services offering and an internal incident response plan for Graycon Group.
- Created 3rd party patch management strategies and anti-malware policies for medium to large size organizations. Device protection scope has ranged from single domains to multiple sites that include mobile devices.

Junior System Administrator, Graycon Group Ltd.   1/28/2013 — 8/31/2013
 Calgary, AB.

- Provided server and client side remote support for over 100 small to medium sized clients.
- Daily administration with AD and GPO in Server 2008-2012, administration in Exchange 2003-2010 and 365.
- Developed and maintained a MS-SQL database that related to a front end VBS application for a medium sized client.

Quality Assurance Analyst, Clarity, Inc.   10/10/2010 — 10/31/2012
 Calgary, AB.

- Analyzed and tested ASP .NET web applications for security related issues and development errors.
- Other duties included database development, error testing, report generation, load and distribution testing, and scripting.

Security Response Team, Red Hat   7/24/2012 — 11/10/2012
Brisbane, QLD, Australia.

- Created a Java based application called communityWebCrawler that would perform analysis on the content of the JBoss Community forums in order to find and filter the security-related issues for engineers to address.

CERTIFICATIONS

- Offensive Security Certified Expert (OSCE) - In progress as of January 2017
- x86 Linux Assembly Expert (SLAE) - December 2016
- Offensive Security Wireless Professional (OSWP) - February 2016
- Offensive Security Certified Professional (OSCP) - April 2015

PROJECTS

Wordsmith   11/1/2015 — Current
github.com/skahwah/wordsmith

- Wordsmith assists with creating tailored geo-location based wordlists to improve password-cracking results.
- Presented at BSides Las Vegas 2016.

ACADEMICS

Bachelor of Information Technology – Security and Networking   7/25/2009 — 12/31/2012
Griffith University, QLD, Australia. 6.0/7.0 GPA

- The B. IT program consisted of studies in information security, software development, networking, discrete mathematics and project management.
- Member of the Griffith University Linux Society.
- Graduated with distinctions.

Diploma in Information Technology – Computer Systems   9/14/2009 — 4/29/2011
SAIT, Calgary, AB. 3.97/4.0 GPA

- The ITCS diploma program was based on information technology, information security, client/server administration, networking, software development, and ITIL. I graduated with high distinctions and received the Jason Lang scholarship.

ADDITIONAL INFORMATION

- Dual nationality, British and Canadian. Authorized to work in the USA though a TN-VISA.
- Professional working proficiency with American sign-language.