# SANJIV KAWA

New York, NY | sanjiv@popped.io | www.popped.io | github.com/skahwah | @kawabungah

## SKILLS PROFILE

- Areas of expertise include threat intelligence led red teaming, enterprise network and web application penetration testing, social engineering, security architecture review, risk management and remediation planning.
- Deep understanding of internal networks, both in a centralized and decentralized context. Confident in traversing large enterprise networks, undermining security and segmentation boundaries to achieve success criteria.
- Active member in the information security community. Exposure to presenting at large conferences. Frequent contribution to projects on GitHub and VulnHub.
- Confident with Ruby, Python, Perl and Bash for scripting and automation. Experience with exploit development in Ruby, Python, IA-32 ASM, C and C#.
- Strong work ethic with exceptional leadership skills. 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

**Principal Security Consultant, Nettitude** 5/1/2019 — Current
*New York, NY*

- Direct line management responsibilities for all US-based offensive security personnel.
- Extensive experience dissecting environments with varying technologies and chaining together misconfigurations to achieve success criteria.

**Senior Security Consultant, Nettitude** 2/23/2018 — 5/1/2019
*New York, NY*

- Leadership responsibilities included overseeing key penetration testing engagements, utilization forecasting and project assignment for USA consultants, involvement in the hiring process and mentoring junior and intermediate security consultants.
- Acted as a technical pre-sales specialist for key and strategic accounts. Strong capability with understanding complex client requirements and collaborating with leadership and account managers to build clients solutions.
- Performed threat intelligence led red teaming (CBEST) for extremely mature and capable organizations; such as central banks, exchanges, insurance and healthcare organizations. Able to effectively simulate an adversaries TTP's to reach target objectives.
- Performed infrastructure and web application penetration testing for small, medium and large organizations. Performed physical and remote social engineering campaigns.
- Performed QA of global reports prior to delivery. Participated in debrief presentations.

**Senior Penetration Tester, PSC – Acquired by NCC Group** 9/15/2016 — 2/23/2018
*(Remote Employee) San Francisco Bay Area, CA.*

- Performed technical interviews for potential candidates. Involved in the decision-making process of the hiring cycle.
- Performed technical QA of internal and external penetration testing reports prior to delivery.

**Penetration Tester, Payment Software Company (PSC)** 6/8/2015 — 9/15/2016
*(Remote Employee) 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 was to gain access to the cardholder data environment (CDE) or to cardholder data (CHD).
- Created issue-based PCI penetration test reports as a main deliverable for clients. Each engagement required a debrief presentation to deliver findings from these reports to technical and non-technical audiences.
- iOS mobile application penetration testing, general ReST and SOAP API testing.
- 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 infrastructure, networks and web applications of a provincial government entity.
- Involved with practice development. Created methodologies for infrastructure, network and web application vulnerability assessments and penetration testing.

**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.
- 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 Office 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 functional issues.
- 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.* analysis

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

## CERTIFICATIONS AND PUBLICATIONS

Certified Information Systems Security Professional (CISSP) – June 2019
CREST Certified Simulated Attack Manager (CCSAM) – May 2019
CVE-2018-10956
x86 Linux Assembly Expert (SLAE) – December 2016
Offensive Security Wireless Professional (OSWP) – February 2016
Offensive Security Certified Professional (OSCP) – April 2015

## PROJECTS

**Wordsmith**
*github.com/skahwah/wordsmith*

- Wordsmith creates tailored geo-location based wordlists and usernames to improve password related attacks.
- Presented at Wild West Hackin' Fest 2017, BSides Washington D.C. 2017, and 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. Graduated with high distinctions and received the Jason Lang scholarship.

## ADDITIONAL INFORMATION

- Dual nationality, British and Canadian. Authorized to work in the USA through a TN-VISA.