Tejas Khairnar

#211, 130 Descanso Drive, San Jose, CA 95134 | Phone: +14802657598 | Email:tkhairna@asu.edu

EDUCATION

- Masters Student (MS) at ASU — Computer Science (Expected 2017) — 3.75 CGPA
- University of Mumbai, India — BE Computer Engineering (Aug 2009-May 2013) — 3.6 CGPA

Academic Project Work

- **Threat Intelligence and Analytics (TIA) Project**
  - Graduate Research Assistant under Dr.Gail-joon Ahn of School of Computing, Informatics and Decision Systems at ASU.
  - Worked as a Python developer for threat intelligence and analytics project. This tool gains its intelligence from four modules namely, Malware, SocialSEAL, Bitcoin and IOC (Indicators of Compromise).
  - Wrote scripts in order to populate data analyzed by cuckoo malware analysis tool into Neo4j Graph database.
  - Developed RESTApi in python for the threat intelligence system.
- **SQLInjection Firewall**
  - Developed SQLInjection Firewall for php based web applications.
  - The logic behind this implementation was to proxy every sql query made to the database via a firewall so that malicious sql queries can be filtered before they get executed in the database.
  - Our solution is also able to through specific exceptions denoting the attempt of an attacker to inject into a SQL database using conditions like always true.
  - Prevented from 2nd Order SQL injections attacks as well. All the queries getting executed on SQL database are proxy through the firewall, hence we were able to defend against 2nd Order SQL injection attacks as well.
- **Virtual Machine Introspection based IDS**
  - Implemented virtual machine introspection in C language over QEMU hypervisor to introspect guest virtual machine running on Linux OS.
  - Using this introspection technique our application was successfully able to detect hidden process deployed using a rootkit. Our application for introspecting Windows guest OS was implemented on the logic of detection of Direct Kernel Object Manipulation (DKOM) based rootkit attacks.
  - To successfully detect hidden process on Unix based OS, we implemented detection of syscall hooks.
  - Our application is able to introspect Windows XP, Windows 7, Ubuntu 14.04 and Fedora OS for intrusions like rootkits or malwares.

WORK EXPERIENCE

Intuit — **Information Security Analyst Intern** — May 2016 till date

- Currently working as Information Security Analyst Intern in the Enterprise Business Solution (EBS) Team at Intuit, Menlo Park office.
- Part of the Identity and Access management team. Working on customization of Agentless Integration Kit by PingIdentity to incorporate the solution into current authentication process for Intuit and its customers.
- Understood Single Sign-On solution architecture implemented at Intuit. Studied various SSO protocols like OAuth, SAML & OpenID connect.
- Configured Apache Integration kit, a product of Ping Identity, in order to enable Single Sign-On for web applications hosted over Apache WebServer.

KPMG, India — **Associate Consultant** — June 2013 to July 2015

- Developed **Anti-Phish detection tool** using Python Scripting language.
- Special recognition and client appreciation for **"Capturing SSL traffic in clear text on mobile (Android) device"** by performing MITM attack using ARP Poisoning and SSL Stripping.
- Performed Web application Security testing for major banking and telecommunication sector clients.
- Imparted training on iOS and BlackBerry mobile application security testing.
- Awarded as "**Above & Beyond**" Employee for successfully performing web application security testing and receiving multiple client appreciations.
- Performed **Mobile application security testing** on various platforms viz., Android, iOS, BlackBerry and Windows.
- Performed configuration review of Oracle Database, Windows and Linux operating system.
- Conducted **Minimum Baseline Security Assessment** review according to the Department of Telecomm guidelines for Major telecom sectors in India.
- Developed automated tool,"ReGeneSys", for generating deliverables to the client using PHP and Javascript web development languages.

CERTIFICATIONS

- Completed Training for **CCNA** certification
- Completed training for **Certified Ethical Hacker** (C|EH)
- **Python for Security Professionals** on www.cybrary.it
- Completed **Linux Lab** Certification course conducted by Dr. Deven Shah and Dr. Ambavde at Sardar Patel Institute of Technology
- **Cyber Forensics and Crime Investigation**(CFCI) certification course at Sadar Patel Institute of Technology conducted by Horizon group a MBI initiative

TECHNICAL SKILLS

- **Programming Languages** : Java, Python, C
- **Databases** : MySQL, Oracle DB, SQL Server
- **Web Technologies** : PHP, Javascript
- **Vulnerability Assessment Tools** : Metasploit, Nessus, IBM AppScan, Burp Suite, Echo Mirage, sqlmap
- **Platforms** : Windows, Linux, Mac OS
- **SIEM Tools** : Splunk
- **Identity & Access Management** : Oracle Access Manager, Oracle Identity Manager, PingIdentity