Ankur Tyagi

807 Catamaran St, Apt. 2
Foster City, CA 94404

+1 650 542 1134
7h3rAm@gmail.com

in.linkedin.com/in/ankurstyagi
twitter.com/7h3rAm
github.com/7h3rAm
7h3ram.github.io

I'm an infosec enthusiast working in targeted research space with the goal of delivering innovative and intelligent solutions. I've a unique combination of skills that span malware analysis, network security and vulnerability assessment. I'm skilled in applying analytical and technical knowledge to produce practical solutions and have strong interest in solving complex technical issues.

Interests

- Network Security (IDS/IPS)
- OSINT and Vulnerability Assessment
- AntiMalware (Endpoint Detection and Response)
- Research Methodologies and Innovation

Patents

Apr/2017 **Method and Apparatus for Intelligent Aggregation of Threat Behavior for the Detection of Malware**
US10104101B1
An attempt towards automated selection and grouping of aggregated threat behavior indicators depicting dominant malware characteristics.

Dec/2014 **Using A Probability-based Model To Detect Random Content In A Protocol Field Associated With Network Traffic**
US9680832B1
A novel idea based upon stochastic processes derived machine learning model to identify and classify random/malicious content in network traffic.

Sep/2014 **Deobfuscating Scripted Language For Network Intrusion Detection Using A Regular Expression Signature**
US9419991B2
An attempt towards normalizing web scripts for network security appliances to consume and operate upon.

Experience

Jan/2017 – Present (1+ year)

Sr. Malware Research Engineer at **Qualys Inc.**
[+] Research towards automated aggregation of threat behavior, filed for US patent and implemented as part of a customer facing product
[+] Collaborating with various teams as a Subject Matter Expert for AntiMalware and network security research initiatives
[+] Working on multiple research ideas that could be leveraged as Intellectual Property
[+] First responder to provide detection against active malware campaigns

Apr/2015 – Jan/2017 (1 year and 10 months)

Malware Research Engineer at **Qualys Inc.**
[+] Research automated (Yara/IoC) rule creation for generic threat coverage
[+] Automated sourcing, filtering and scanning of malware samples
[+] Reverse engineering and analysis of malware samples
[+] Working on various in-house automation and development projects
[+] Technologies: Python, Shell, Unix, Windows, AntiMalware, EDR

Apr/2012 – Feb/2015 (2 years and 11 months)

Security Research Engineer at **Juniper Networks**
[+] Testing and updating in-house automation tools that help with coverage analysis against various exploitation frameworks
[+] Ensuring coverage against latest vulnerabilities and exploits through signature development for Juniper's security portfolio devices
[+] Regular updates of active signatures to ensure coverage against evolving IDS/IPS evasion techniques as well as for quality assurance
[+] Technologies: Python, Shell, Unix, Windows, IDS, IPS

Dec/2010 - Apr/2012 (1 year and 5 months)

Information Security Engineer at **SecurView Systems**
[+] Vulnerability Researcher / Security Analyst for the Cisco Security IntelliShield Alert Manager Service
[+] Active member of the Secur-I Research Group. Group activities involved monthly publication of critical vulnerability assessments and concentrated vulnerability research
[+] Technologies: Python, Shell, Unix, Windows

Talks

Visual Network and File Forensics
This presentation aims to demo the effectiveness of visual tooling for malware and file-format forensics
DEF CON 25 Packet Hacking Village *July 29, 2017*

Rudra - The Destroyer of Evil
Rudra aims to provide a developer-friendly framework for exhaustive analysis of PCAP and PE files

DEF CON 24 Demo Labs	*August 6, 2016*
Black Hat USA 2016 Arsenal	*August 3, 2016*
OWASP Pune Meet	*July 28, 2016*
Black Hat Asia 2016 Arsenal	*March 31, 2016*
Black Hat EU 2015 Arsenal	*November 13, 2015*
DEF CON 23 Demo Labs	*August 8, 2015*
Black Hat USA 2015 Arsenal	*August 5, 2015*

Flowinspect - Network Inspection Tool on Steroids
Flowinspect is a tool developed specifically for network monitoring and inspection purposes

Black Hat USA 2014 Arsenal	*August 6, 2014*
Nullcon 2014	*February 14, 2014*

Media

Oct/2017 **Visual Malware Forensics**, Virus Bulletin

Sep/2017 **Bossie Awards 2017 - The best networking and security software**, InfoWorld

Sep/2017 **Visual network and file forensics with Rudra**, HelpNet Security

Sep/2015 **Rudra - Framework for automated inspection of network capture files**, HelpNet Security

Mar/2014 **Network Sorcery with ChopShop and Libemu**, PenTest Magazine

Academics

Dec/2014 **M.Tech Software Systems**, **BITS-Pilani**
Thesis: Rudra - Framework for Automated Inspection of Network Flows

Jul/2010 **BE Information Technology**, **Pune University**
Thesis: Insider Threats - Research on ARP Security Flaws and Solutions

Certifications

Mar/2012 **GIAC Penetration Tester (GPEN)**

May/2011 **Certified Ethical Hacker (CEH)**

Jan/2010 **Cisco Certified Network Security Associate (CCNA)**

Independent Courses

Dec/2015 **The Arduino Platform and C Programming**, **Coursera - University of California, Irvine**

Dec/2015 **Software Security**, **Coursera - University of Maryland**

Jan/2014 **An Introduction to Interactive Programming in Python**, **Coursera - Rice University**

Dec/2013 **Internet History, Technology and Security**, **Coursera - University of Michigan**

Sep/2013 **Malicious Software and its Underground Economy**, **Coursera - University of London**

Last updated: Jan 24, 2018