

Ankur Tyagi

+91 721 900 1099
7h3rAm@gmail.com

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

I'm an infosec enthusiast with strong technical background in the field of information security. I've solid combination of skills that span malware analysis, exploitation, reverse engineering, protocol/file-format decoding/analysis 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.

Areas of Interest

- Python, C/C++, x86 Assembly
- Research Methodologies and Innovation
- Malware Analysis, Reverse Engineering
- Security Intelligence, Vulnerability Assessment
- Network/File-format Forensics, Intrusion Detection/Prevention

Research

Dec/2014 **Using A Probability-based Model To Detect Random Content In A Protocol Field Associated With Network Traffic**

United States 2014/586144

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**

United States 2014/501798

An attempt towards normalizing web scripts for network security appliances to consume and operate upon.

Experience

Apr/2015 – **Malware Research Engineer at Qualys Inc.**

- Present (8+ months)
- [+] Reverse engineering and analysis of malware threats
 - [+] Working on inhouse automation and development projects
 - [+] Writing Yara rules and generating IOCs for malware families

Apr/2012 – **Security Research Engineer at Juniper Networks**

- Feb/2015 (2 years and 11 months)
- [+] 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

Dec/2010 – **Information Security Engineer at SecurView Systems**

- Apr/2012 (1 year and 5 months)
- [+] 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.

Academics

Dec/2014 **M.Tech Software Systems, BITS-Pilani**

Thesis: Framework for Automated Inspection of Network Flows
CGPA: 6.65 (*Excellent*)

Jul/2010 **BE Information Technology, Pune University**

Thesis: Research into ARP Implementation Flaws
CGPA: 6.58 (*First Class*)

Independent Courses

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

Grade:

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

Grade: 97.5%

- Jan/2014 **An Introduction to Interactive Programming in Python, Coursera - Rice University**
Grade: 90.8% w/ Distinction
- Dec/2013 **Internet History, Technology and Security, Coursera - University of Michigan**
Grade: 94.6% w/ Distinction
- Sep/2013 **Malicious Software and its Underground Economy, Coursera - University of London**
Grade: 100% w/ Distinction