

# Ankur Tyagi

+91 721 900 1099  
[7h3rAm@gmail.com](mailto:7h3rAm@gmail.com)

[in.linkedin.com/in/ankurstyagi](https://in.linkedin.com/in/ankurstyagi)  
[twitter.com/7h3rAm](https://twitter.com/7h3rAm)  
[github.com/7h3rAm](https://github.com/7h3rAm)  
[7h3ram.github.io](https://7h3ram.github.io)

I'm an infosec enthusiast with strong technical background in the field of information security. I've a solid 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.

## Areas of Interest

- Python, C, x86 Assembly
- Network/File Forensics, IDS/IPS
- Research Methodologies and Innovation
- Security Intelligence, Vulnerability Assessment
- AntiMalware, Endpoint Detection and Response

## Patents

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 – Present (1+ years) **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

### **Rudra - The Destroyer of Evil**

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

[Black Hat USA 2016 Arsenal](#)

*August 3, 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*

## Academics

- Dec/2014 **M.Tech Software Systems, BITS-Pilani**  
Thesis: 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: Oct 2, 2016