

# Ankur Tyagi

@ankurt.20@gmail.com • [linkedin.com/in/ankurstyagi](https://www.linkedin.com/in/ankurstyagi) • [twitter.com/7h3rAm](https://twitter.com/7h3rAm) • [7h3rAm.github.io](https://7h3rAm.github.io)

I'm an infosec enthusiast with a strong background in network security (IDS/IPS), anti-malware technologies (EDR/XDR), research methodologies and innovation.

## Experience

- **Principal Engineer at Qualys Inc.** Jan/2019 - Present
  - Product research, design and PoC: Breach Simulation, Security Control Validation, Attack Surface Mapping, Asset Remediation Trendmap
  - Research and automation: Threat Intelligence feeds evaluation and aggregation, False Positive validation, event whitelisting, risk scoring, rule parsers and converters
  - MITRE ATT&CK TTP correlation (adversary killchain), quantification and scoring
  - Subject Matter Expert for research/innovation and automation workflows
  - Tech/Domain: Python, Shell, Unix, Windows, AntiMalware, EDR, XDR, Threat Intelligence
- **Research Engineer at Qualys Inc.** Apr/2015 - Jan/2019
  - Research towards automated aggregation of threat behavior and generic (Yara/IoC) rule creation
  - Lead architect for in-house automation projects (sourcing/filtering/scanning of malware samples)
  - Subject Matter Expert for AntiMalware and network security research initiatives
  - Tech/Domain: Python, Shell, Unix, Windows, AntiMalware, Yara, IoC
- **Security Research Engineer at Juniper Networks** Apr/2012 - Feb/2015
  - Maintaining in-house automation tools for coverage against multiple exploitation frameworks
  - Signature development for Juniper's security portfolio devices against latest vulnerabilities and exploits
  - Regular updates of active signatures to increase accuracy and coverage against evolving evasion techniques
  - Tech/Domain: Python, Shell, Unix, Windows, IDS, IPS
- **Information Security Engineer at SecurView Systems** Dec/2010 - Apr/2012
  - Vulnerability Researcher / Security Analyst for the Cisco Security IntelliShield Alert Manager Service
  - Active member of the Secur-I Research Group with monthly publication of critical vulnerability assessments
  - Tech/Domain: Python, Shell, Unix, Windows, Vulnerability Research

## Patents

- Quantification of Adversary TTPs Using Threat Attribute Groupings and Correlation Dec/2021
- Security Event Detection Using Behavioral, Analytical and Threat Intelligence Attributes Dec/2021
- [Attack Path and Graph Creation Based on User and System Profiling](#) Jul/2019
- [Attack Kill Chain Generation and Utilization for Threat Analysis](#) Apr/2019
- [Asset Remediation Trend Map Generation and Utilization for Threat Mitigation](#) Apr/2019
- [DSL for Simulating a Threat-Actor and Adversarial TTPs](#) Apr/2019
- [DSL for Defending Against a Threat-Actor and Adversarial TTPs](#) Apr/2019
- [DSL for Threat-Actor Deception](#) Apr/2019
- [Method and Apparatus for Intelligent Aggregation of Threat Behavior](#) Apr/2017
- [Using A Probability-based Model To Detect Random Content In Network Traffic](#) Dec/2014
- [Deobfuscating Scripted Language For Network Intrusion Detection](#) Sep/2014

## Media

- Bossie Awards 2017 - The best networking and security software, [InfoWorld](#) Sep/2017
- Visual network and file forensics with Rudra, [HelpNet Security](#) Sep/2017
- Rudra - Framework for inspection of network capture files, [HelpNet Security](#) Sep/2015
- Network Sorcery with ChopShop and Libemu, [PenTest Magazine](#) Mar/2014

## Talks

- **svachal + machinescli**  
These tools are useful for creating and learning from CTF writeups
  - [DEF CON 30 Demo Labs](#) 13/Aug/2022
- **Breach and Attack Simulation**  
Automated simulation of adversary TTPs mapped to MITRE ATT&CK framework
  - [Qualys Security Conference 2018 - First Look Showcase](#) 14/Nov/2018
- **Angad - Malware Detection using Multi-Dimensional Visualization**  
Angad is a tool that can perform visual malware clustering using Hilbert Curves
  - [SecTor 2018](#) 13/Oct/2018
  - [BSides Zurich 2018](#) 14/Sep/2018
  - [GrrCON 2018](#) 07/Sep/2018
  - [DEF CON 26 Demo Labs](#) 11/Aug/2018
- **Visual Network and File Forensics**  
This presentation showcases the effectiveness of visual tooling for malware and file-format forensics
  - [DEF CON 25 Packet Hacking Village](#) 29/Jul/2017
  - [Virus Bulletin 2017](#) (could not attend)
- **Rudra - The Destroyer of Evil**  
Rudra provides a framework for exhaustive analysis of PCAP and PE files
  - [DEF CON 24 Demo Labs](#) 06/Aug/2016
  - [Black Hat USA 2016 Arsenal](#) 03/Aug/2016
  - [OWASP Pune Meet](#) 28/Jul/2016
  - [Black Hat Asia 2016 Arsenal](#) 31/Mar/2016
  - [Black Hat EU 2015 Arsenal](#) 13/Nov/2015
  - [DEF CON 23 Demo Labs](#) 08/Aug/2015
  - [Black Hat USA 2015 Arsenal](#) 05/Aug/2015
- **Flowinspect - Network Inspection Tool on Steroids**  
Flowinspect is a tool for network monitoring and inspection purposes
  - [Black Hat USA 2014 Arsenal](#) 06/Aug/2014
  - [Nullcon 2014](#) 14/Feb/2014

## Portfolio

### Google Scholar

- citations: 48
- h-index: 3
- i10-index: 3

### GitHub

- Rank: S (top 25%)
- Commits: 16.4k
- Followers: 142
- Pull Requests: 16
- Stars: 338
- Languages: python/c/assembly/shell/tex

### StackOverflow

- Reputation: 1735 (top 22%)
- Impact: ~517k people reached
- Badges: gold:2/silver:15/bronze:17

## Certifications/Academics

- [Attacking and Defending Azure Cloud: Beginner's Edition](#) Mar/2023
- [Amateur Radio Operator \(KN6VLB\)](#) Aug/2022
- [GIAC Penetration Tester \(GPEN\)](#) Mar/2012
- [Cisco Certified Network Security Associate \(CCNA\)](#) Jan/2010
- **M.Tech Software Systems, BITS-Pilani** Dec/2014  
Thesis: [Rudra - Framework for Automated Inspection of Network Flows](#)
- **BE Information Technology, Pune University** Jul/2010  
Thesis: [Insider Threats - Research on ARP Security Flaws and Solutions](#)