

# Ankur Tyagi

@ ankurt.20 • 7h3rAm.github.io • 7h3rAm • ankurstyagi

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

## Experience

• <b>Cisco Talos Intelligence Group</b>	Aug/2023 - Present
• <b>Security Research Engineer, Network Threat Detection &amp; Response (NTDR)</b>	(2 yrs 5 mos)
• Detection Engineering and Vulnerability Research	
• Snort & ClamAV	
• <b>Qualys Inc.</b>	Apr/2015 - Aug/2023
• <b>Principal Engineer, Threat Research Unit (TRU)</b>	(4 yrs 7 mos)
• Breach Simulation, Security Control Validation, Attack Surface Mapping, Asset Remediation Trendmap	
• 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	
• Technologies: Python, Shell, Unix, Windows, AntiMalware, Yara, IoC, EDR, XDR, Threat Intelligence	
• <b>Research Engineer, Malware Lab</b>	(3 yrs 9 mos)
• Research towards automated aggregation of threat behavior and generic (Yara/IoC) rule creation	
• Lead for multiple in-house automation projects (sourcing/filtering/scanning of malware samples)	
• <b>Juniper Networks</b>	Apr/2012 - Feb/2015
• <b>Security Research Engineer, Network Signatures Team</b>	(2 yrs 10 mos)
• 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	
• <b>SecurView Systems</b>	Dec/2010 - Apr/2012
• <b>Information Security Engineer, IntelliShield Alert Manager Team</b>	(1 yr 4 mos)
• 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	

## Research

• Quantification of Security Events using Behavioral, Analytical and Threat Intelligence Attributes	Dec/2021
• Quantification of Adversary TTPs Using Threat Attribute Groupings and Correlation	Nov/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
• 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
• Asset Remediation Trend Map Generation and Utilization for Threat Mitigation	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

• Hackers of India, <a href="#">Hacking Archives of India</a>	Oct/2020
• Bossie Awards 2017 - The best networking and security software, InfoWorld	Sep/2017
• Visual network and file forensics with Rudra, <a href="#">HelpNet Security</a>	Sep/2017
• Rudra - Framework for inspection of network capture files, <a href="#">HelpNet Security</a>	Sep/2015
• Network Sorcery with ChopShop and Libemu, <a href="#">PenTest Magazine</a>	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
- BSides Zurich 2018
- GrrCON 2018
- DEF CON 26 Demo Labs

13/Oct/2018

14/Sep/2018

07/Sep/2018

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
- Virus Bulletin 2017

29/Jul/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
- Black Hat USA 2016 Arsenal
- Black Hat Asia 2016 Arsenal
- Black Hat EU 2015 Arsenal
- DEF CON 23 Demo Labs
- Black Hat USA 2015 Arsenal

06/Aug/2016

03/Aug/2016

31/Mar/2016

13/Nov/2015

08/Aug/2015

05/Aug/2015

- **Flowinspect - Network Inspection Tool on Steroids**

Flowinspect is a tool for network monitoring and inspection purposes

- Black Hat USA 2014 Arsenal
- Nullcon 2014

06/Aug/2014

14/Feb/2014

## Portfolio

### Google Scholar

- Citations: 157
- h-index: 7
- i10-index: 4

### GitHub

- Rank: B (top 25%)
- Commits: 14.3k
- Followers: 179
- Pull Requests: 18
- Stars: 402
- Languages: javascript/html/python/c++/c

### StackOverflow

- Reputation: 1915
- Impact: ~634k people reached
- Badges: gold:2/silver:16/bronze:18

## Certifications/Academics

- Generative AI for Everyone

Nov/2024

- 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

Last update: 28/Jan/2026