Udayveer Singh

Portfolio: m4lici0u5.com
Github: github.com/an0nud4y
Twitter: twitter.com/m4lici0u5
LinkedIn: linkedin.com/an0nud4y

Email: anonud4y@gmail.com
Address: Indore (MP)

Education

- **National Institute of Technology Srinagar (NIT Srinagar).** Srinagar (J&K), India *2020 - 2024*
  - **Degree**: Bachelor of Technology (B.Tech) - Information Technology
  - **Courses**: Cryptography, Information Security, Operating Systems, Computer Architecture, Microprocessors, Data Structures, Analysis Of Algorithms, Artificial Intelligence, Machine Learning, Networking, Databases , Java Programming

Skills Summary

- **Programming Languages:** Java, C++, C, C#, Python, JavaScript, Golang, Bash, Powershell
- **Soft Skills:** Report Writing, Blog Writing, Public Speaking
- **Skills:** Red Teaming, Malware Development, Vulnerability Assessment & Penetration Testing (VAPT), Phishing Simulation, Physical Red Teaming, Assume breach, Web Application Security, Windows Security, Windows Defense Evasion, Enterprise Security, Powershell, AV/EDR Evasion, OSINT, Offensive Tool Development, Adversary Simulation, Active Directory Exploitation, Active Directory Certificate Services (AD CS) Exploitation, Risk Assessment, Network Pentesting, Wireless Security, ATM Penetration Testing
- **Tools:** Evilginx, Metasploit, Cobalt Strike C2, Mythic C2, BloodHound, SharpHound, PowerView, Active Directory Module, Certify, Responder, Ping Castle, Havoc C2, Sliver C2, Burp Suite, Nessus, Nikto, Nuclei, SQLMap, Sysinternals Tools, Nmap, Impacket, Rubeus, Mimikatz, CrackMapExec, x64Dbg, Ghidra, Sysmon, Atomic Red Team, Caldera, Aircrack-ng.

Certifications

CESP : Certified Enterprise Security Professional - AD CS (CESP - ADCS) - (Credential ID : ADCSLID263)

CRTO : Certified Red Team Operator - (Credential ID : KRYm5M9ISQyGNxThF4aRvw)

CRTE : Certified Red Team Expert - (Credential ID : RTLID2131)

CRTP : Certified Red Team Professional (Credential ID : ADLID6544)

eJPT : eLearning Junior Penetration Tester (Credential ID : 8776587)

GPCSSI21: Gurugram Police Cybersecurity Summer Intern 21

Sektor7: RTO Windows Evasion, RTO Malware Development Advanced Vol.1 , RTO Intermediate, RTO Essentials

Other Certs : Evilginx Mastery, Windows/Linux Priv Esc for OSCP

Experience

- **Kroll - Associate Consultant - Offensive Security.** Remote - Delhi, India
  Offensive Security *Sep 2024 - Present*
  - **Responsibilities**: Web Application Pentesting, Network Pentesting, API Security Testing, Red/Purple Teaming, Windows Defense Evasion, Adversary Simulation, Offensive Tool Development, EDR Evasion, OSINT, Phishing Engagement, Report Writing.
- **eSecForte - Associate Information Security - Red Team.** Remote - Gurugram, Haryana
  Information Security - Red Teaming *Sep 2023 - Sep 2024*
  - **Responsibilities**: Red Teaming - Internal/External, Physical Red Teaming, Windows Defense Evasion, Adversary Simulation, Offensive Tool Development, AV/EDR Evasion, OSINT, Phishing Engagement, Web Application Pentesting, Network Pentesting, ATM Pentesting, Wireless Pentesting, Report Writing.
- **Chongluadao.vn - Threat Researcher.** Remote - Hanoi, Vietnam
  Threat Researcher *Sep 2022 - Aug 2023*
  - **Responsibilities**: Reproducing, Preventing and Tracking Cyber Attacks and Threats. Presenting Demonstrations for such attacks to help secure the individuals and Organisations.
- **CyberSmithSecure - Security Analyst.** Remote - Mumbai
  Security Analyst - Intern *Jan 2023 - March 2023*
  - **Responsibilities**: Penetration Testing, Web App Pentesting, Network Pentesting, OSINT, Report Writing.
- **Gurugram Police - Cyber Security Intern.** Remote - Gurugram, Haryana
  Cyber Security Intern *June 2021 - July 2021*
  - **Experience**: Cybercrime and fraud case studies, forensics, Participated in CTF challenges

Open Source Projects / Contributions

- **Evilginx2 -: 2FA Bypass using Reverse Proxy (MITM)**: Created various evilginx2 phishlets and bypassed security measures against phishing attacks powered by reverse proxy, Contributed to evilginx2 & encouraged author to publish v2.4 , Open Sourced Evilginx 2.0 phishlets to help community simulate these attacks and prevent them. Evilginx2 is written in Golang.
- **Phishing Infrastructure Setup -: A detailed guide to setup phishing Infra for Red Teaming Phishing Engagement**: Developed detailed guide to help red teamers to setup a robust evilginx phishing infrastruction along with multiple evilginx phishing evasion techniques including source code modifications and IOC removal to avoid singature based detections.
- **AV/EDR Lab Environement Setup -**: A list of references to setup detection lab to test malwares during malware development process. References are mentioned based on different type of detections EDR products perform. Provides a list solid alternative to EDR environments to setup a lab for malware testing.
- **HiddenEye -: Phishing Tool With Advanced Functionality**: Developed basic phishing tool which had capabilities of information gathering and keylogging, Written in Python - Repo Archived

Publications

- **Security Blog** : Publishing my methodologies, research, CTF Writeups, certifications review/notes and cybersecurity learning journey on my Personal Blog.
- **Fido Apac Summit 2023**: Worked with Hieu Monh Ngo to present Phishing attack failed on Passwordless at FIDO APAC SUMMIT 2023 which was held in Nha Trang, Vietnam.

Volunteer Experience

- **Z3r0d4y**: Established the official CyberSecurity Club of NIT Srinagar and conducted numerous Cybersecurity Workshops and CTFs, NIT Srinagar (z3r0d4y) is also an active participant of HackTheBox Universities CTFs.