ROHAN ANAND GOWDA

CYBER SECURITY ENGINEER

+353 89 989 4250

99agrohan@gmail.com

Dublin, Ireland

www.rohanag.com

PROFILE

A driven cybersecurity professional with over 2 years of expertise in penetration testing and red teaming, recently graduated with an MSc in Cybersecurity. Proficient in black box, grey box, and white box testing across diverse infrastructures (network, web, Android, APIs), and adept at identifying vulnerabilities from low to critical severity. Certified Ethical Hacker (v10) with international client experience spanning India, Singapore, Europe, and Africa. Passionate about advancing cybersecurity efforts and driving security innovation.

EDUCATION

2022 - 2023
NATIONAL COLLEGE OF IRELAND

- Master of Cybersecurity

2017-2021
RNS INSTITUTE OF TECHNOLOGY

- Bachelor of Engineering - Electronics and communication

WORK EXPERIENCE

August 2021 - August 2022
Arridae Infosec Pvt Ltd l Bengaluru, India

Associate Information Security Consultant

- Conducted penetration tests for major pharmaceutical and healthcare clients (under NDA) using industry-standard tools and methodologies.
- Uncovered Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) vulnerabilities in a client's application, leveraging Burp Suite and Browser Exploitation Framework (BeEF) to demonstrate exploitation and remediate issues.
- Exploited DoublePulsar and EternalBlue Trojans in Care Hospital's network using Metasploit Framework, testing over 1000+ IP endpoints across 20-21 subnets, providing strategic insights to mitigate future attacks.
- Created detailed test plans for web applications and mobile app security, identifying key vulnerabilities and proposing solutions for risk mitigation.
- Collaborated with clients to review codebase and provide guidance on issue remediation and security enhancements.

LINKS

WWW.ROHANAG.COM

SKILLS

- VMware and Kali Linux: Booting up and hosting virtual machines such as Kali Linux which is well equipped (Booting process, Grep, SCP, SSH, Permissions, tar, Bash, Basics of Shell, Unix) with tools necessary for maintaining and implementing information security.
- Manual penetration testing: Basic of shell and python scripting, Metasploit and msfconsole, SEToolkit, networking protocols and models manual code review.
- Information gathering and recon: Nmap, maltego, recon-ng, shodan, wireshark, wapplyzer.
- Network vulnerability analysis: Nessus, Openvas GVM, openssl, sslyze, testssl, Telnet, SSH, FTP, SMTP. Redis.
- Penetration tested on a large-scale hospital network and various organisational networks and findings included double pulsar trojans, default camera passwords, blue keep and exploited them with the help of using backdoors created by msfconsole.

February 2020 - October 2020

Triadsquare Infosec Pvt Ltd. l Bengaluru, India

Cyber Security Intern

- Received extensive app security training on penetration testing methodologies and tools, including Burp Suite, Nmap, and Metasploit to assess application frameworks for potential vulnerabilities., as part of my preparation for the Certified Ethical Hacker (CEH v10) certification, which I successfully completed during my internship.
- Gained hands-on experience working on a variety of client projects (all client names under NDA, but included major companies), performing vulnerability assessments and penetration testing across web applications, network infrastructure, and APIs. Worked under senior consultants, assisting in the identification of OWASP Top 10 vulnerabilities such as SQL injection, XSS, and CSRF on multiple client networks.
- Contributed to the security audits of client systems by developing custom scripts in Python to automate parts of the testing process, significantly reducing manual testing time by 20%. Assisted in developing customized test plans and conducted automated testing for mobile and web applications.
- Worked across various environments, including web applications, networks, and cloud-based infrastructures, ensuring thorough security assessments and accurate vulnerability reporting.

PROJECTS & ACHIEVEMENTS

1. Identified and Exploited Key Vulnerabilities: Successfully uncovered critical Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) vulnerabilities for a pharmaceutical client, leading to the development of secure coding practices that improved their security posture by 25%.
2. Led Strategic Hospital Network Security Tests: Spearheaded penetration testing on Care Hospital's network, analyzing over 1000 IP endpoints and identifying critical vulnerabilities using Metasploit. This proactive approach helped the hospital mitigate potential mobile app security breaches and enhance patient data protection.
3. Certified Ethical Hacker (CEH v10): Gained advanced knowledge in app security and penetration testing techniques, using application frameworks like OWASP and NIST as part of CEH certification.
4. Automated Security Testing: Developed custom scripts using Python to automate vulnerability testing, reducing manual testing time by 20% and improving project delivery timelines.
5. Awarded Team Recognition: Received team commendations for consistently meeting tight deadlines while delivering high-quality penetration testing results for key clients, ensuring risk mitigation and strong client satisfaction.

- Web application vulnerability scanning and Penetration Testing: Testing done with OWASP top 10 standards. Web application and API tests and scans with Burpsuite, Accunetix, HCL appscan, Netsparker (SAST and DAST), Nessus and false positive verification and post exploitation.
- Tested multiple websites based on the requirement by client (black/white/grey box) and found vulnerabilities like clickjacking, XSS (both stored and reflected) and exploited them with the help of browser exploitable framework (BEEF). SQL injection was also a finding in some cases which was further tested with the help of SQL map.
- Basic concepts of Web application firewalls, intrusion detection systems and Realtime application self-protection tools like crowdstrike.
- API testing using Burpsuite and postman API.
- Reporting: Excel, Microsoft Word, shell scripting by using developed templates.
- Mobile applications testing: Genymotion emulator for hosting the app. Adb, mobSF, burpsuite, apktool, jadx-gui, Ostorlab.
- Tested android applications before their deployment and brief findings were weak encryption algorithms, Janus (a vulnerability that affects the availability of resources). Learned how to exploit vulnerabilities in a mobile device by crafting basic exploits from msfvenom and exploiting the weakness from msfconsole.
- Security Frameworks: Familiarity with concepts of IS027001, NIST, PCI DSS and MITRE framework.
- SIEM: Arcsight, Splunk. Operating System : Windows, Linux
- Soft Skills: Strong problem-solving, adaptability, and innovative thinking, with experience in mentoring, offering guidance, advising clients and escalation support. Meeting Deadlines and also work independently