RAMESWAR DHARNEESH LAGUSANI

Mobile: 803 410 5703

E-Mail: David@trovetechs.com

**Professional Summary**

* Cybersecurity professional with 7+ years of experience in Information Security and Medical device security.
* Involved in Software Development Life cycle (SDLC) to ensure security controls are in place.
* Sound understanding of OWASP Top 10, SANS 25 and NIST standards.
* Developed cyber security policies and best practices to maintain confidentiality, integrity and availability of organizational data.
* Experience in Penetration testing and Vulnerability Management using various tools like Burp Suite, Dir-Buster, OWASP ZAP proxy, Nmap, Nessus, Kali Linux, Metasploit, Qualys guard and Nexpose.
* Good understanding and experience on SIEM tools like Splunk and IBM QRadar.
* Worked on the Incident Management part to mitigate the vulnerabilities.
* Profound knowledge on Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) using tools such as Veracode, Checkmarx, HP Fortify, IBM App Scan enterprise.
* Capable of identifying flaws like SQL Injection, XSS, Insecure direct object reference, Security Misconfiguration, Sensitive data exposure, Functional level access control, Encryption and Cryptography.
* Performed multiple Red Team Campaigns using Kali Linux, Cobalt Strike, Metasploit, Powershell Empire are various tools.
* Good understanding and knowledge on Firewall Rules, Firewall Settings, Network layer protocols, TCP/IP, LAN/WAN and IDS/IPS.
* Hands on with medical devices security and extensive knowledge in medical device FDA guidance’s, Security standards including UL2900 and NIST framework.
* Good understanding and knowledge on pre-market and post-market security regulations by FDA on medical devices.
* Profound knowledge on Source Code reviewing and programming skills on Java Script, XML environment.
* Good knowledge and experience on IOT device and Hardware hacking.
* Performed wireless hacking on Bluetooth and Wifi with various hardware and Kali tools.
* Hands on experience with the hacking tools like Rubber Ducky, Bash Bunny, Radio PA Dongle, PiCAN, CAN Buster, JTAG Debugger, USB Blaster, Hack RF and Hak5 tools.
* Performed Cyber Security Operations and huge knowledge on Intrusion Prevention System (IPS) ad Intrusion Detection System (IDS).
* Profound experience in developing and maintaining the documentations for the policies procedures and the best practices in the environment.
* Good team player with excellent analytical, inter-personal, communication & written skills, problem-solving and trouble-shooting capabilities. Highly motivated and can adapt to work in any new environment.

**Technical Skills**

|  |  |
| --- | --- |
| PLATFORMS | Windows, Linux |
| LANGUAGES | C, C++, Java, Python, PHP, Assembly Language |
| TOOLS | Cobalt Strike, Metasploit, Kali Linux, Powershell Empire, Splunk, IBM QRadar, Qualys guard, Tableau, Burp-Suite, Nmap, Wireshark, Veil, Phantom Evasion, Aircrack-ng, Bettercap, Mousejack, Jacket, Snort, UFW |
| HARDWARE HACKING TOOLS | CAN Buster, CAN Utils, PiCAN, JTAG Debugger, USB Blaster, Radio PA Dongle, Rubber Ducky, Bash Bunny, LAN Turtle, Ubertooth One, Hack RF, Hak5 Tools |
| SAST AND DAST | Veracode, Checkmarx, HP Web Inspect, IBM App scan, Cross-Site scripting. |
| SCANNERS/VULNERABILITY ASSESSMENT TOOLS | Carbon Black, Nessus, Burp Suite, BeStorm, InSight VM |

**Certification**

**CEH : Certified Ethical Hacker**

**Professional Experiences**

**FRESENIUS MEDICAL CARE, WALTHAM, MA November 2019 – Present**

**Cyber Security Engineer/ Penetration Tester**

**Responsibilities:**

* Conducted Web Application Vulnerability Assessment, Threat Modelling and secure code reviews on the Medical Devices.
* Performed security risk assessments for on-market products using ISO 27005 threat catalog and evaluated applicable UL 2900 controls to enhance product security using medical device risk assessment tools.
* Identified the risk level (critical, High, Medium, Low) and prioritizing vulnerabilities found in software applications and hardware components.
* Performed code reviews with the help of automation tools.
* Inform security vulnerabilities identified, and recommendations proposed to fix the issues like FTP related vulnerabilities, information disclosure, default username/passwords etc
* Performed numerous penetration tests on Bluetooth and WiFi using Kali Linux tools and hardware tools like ubertooth.
* Managing the tracking and remediation of vulnerabilities by leveraging agreed-upon action plans with the teams.
* Performed hardware testing using the JTAG, USB Blaster and XILINX platform Usb Cable, LAN Turtle, Rubber Ducky and Bash Bunny.
* Worked on CAN Bus hacking using the PiCAN, CAN Buster and CAN Utils .
* Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.
* Suggested the security requirements to the development team in various stages of building a machine to minimize the efforts to work on issues identifies during penetration tests.
* Follow up and ensure the closure of the raised vulnerabilities by revalidating and ensuring 100% Closure.

**SECURIAN FINANCIAL, SAINT PAUL, MN June 2018 - September 2019**

**Red Team Security Engineer/ Penetration Tester**

**Responsibilities:**

* Designed and performed multiple Red Team campaigns to proliferate the security standards of the environment.
* Worked on setting up the attacker Virtual machines and installed the exploitation tools to perform Vulnerability assessment.
* Configured and managed the security operations using IBM QRadar.
* Worked with the Incident managing team to mitigate the Vulnerabilities.
* Performed the periodic vulnerability scans using Nessus.
* Extracted and analyzed the logs using SIEM technologies and Forensics analysis.
* Performed the Social Engineering tasks as a part of the Red Team campaigns.
* Monitored and diagnosed the security incidents in the Carbon Black, IBM QRadar and Qualys Guard.
* Managed the Endpoint protection on anti-malware, firewall features and intrusion prevention.
* Performed multiple exploitations using the tools like Cobalt Strike, Metasploit, Powershell Empire, Veil, Phantom Evasion, Unicorn.
* Training the development team on vulnerabilities, review issues, ease of exploitation, impact, security requirements and remedies for individual issues.
* Performed the Mouse-jacking operations to let the employees know the complications using the vulnerable devices.
* Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality.
* Documented the start to end of the campaigns and the tools used for each campaign.

**STATE OF WI, MADISON, WI March 2017 - May 2018**

**Application Security Engineer**

**Responsibilities:**

* Performed Vulnerability scans to identify, evaluate, treat and report the security vulnerabilities in both the systems and the software.
* Conducted Web Application Vulnerability Assessment, Source Code review and Threat Modelling.
* Acquainted with various approaches to Grey & Black box security testing.
* Doing multiple level of testing before production to ensure smooth deployment cycle.
* Performed vulnerability testing using tools such as Nessus and Qualys-guard.
* Maintains network performance by performing network monitoring and analysis, performance tuning, troubleshooting network problems. Skilled using Burp Suite, NMAP, Dir-Buster, Qualys-guard, Nessus, SQL Map for web application penetration tests and infrastructure testing.
* Tested and performed vulnerability analysis (VA) through Nessus &Qualys Guard Scan.
* Performed Vulnerability Assessment of various Web Applications used by the organization.
* Scanned web and mobile applications prior to deployment using Qualys to identify security vulnerabilities and generated reports and fix recommendations.
* Ensuring compliance with legal and regulatory requirements.
* Security monitoring to identify any possible intrusions.
* Guiding the developers in fixing the issues by simulating the attack.
* Performing a threat analysis on the new requirements and features.
* Generated executive summary reports showing the security assessment results, recommendations and risk mitigation plans and presented them to the senior management.

**CISCO, SAN JOSE, CA March 2016 – March 2017**

**Information Security Engineer**

**Responsibilities:**

* Performed manual security testing on critical client applications.
* Conducted Dynamic and Static Application Security Testing (SAST & DAST).
* Performed vulnerability scans using HP Web Inspect, IBM App Scan, Qualys Guard, Retina, Nessus, Burp Suite, and Metasploit auxiliary modules.
* Performed the code analysis using Checkmarks.
* Uncovered high vulnerabilities at the infrastructure level for internet facing websites.
* Brute force assessment to insure strong passwords and encryption.
* Performed threat modelling of the applications to identify the threats.
* Execute and craft different payloads to attack the system for finding vulnerabilities with respect to input validation, authorization checks, etc.
* Training the development team on the secure coding practices
* Providing details of the issues identified and the remediation plan to the stake holders.
* Update with the new hackings techniques and latest vulnerabilities to ensure no such loopholes are present in the existing system.
* Communicating and coordinating day-to-day project activities within the project team and assure that priorities are developed and known.
* Create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system, and suggestions to mitigate any exposures and testing known vulnerabilities.

**IGATE, INDIA Jan 2013 – July 2015**

**Web Security Analyst**

**Responsibilities:**

* Black box pen testing on internet and intranet facing applications
* Follow information security policies, methods, standards, NIST standards, and practices to organize information systems, IT reference material, and interpret regulations.
* Monitor Intrusion Detection Systems (IDS) console for active alerts and determine priority of response.
* Skilled using Burp Suite, Qualys Guard, Automatic Scanners and Nmap for web application penetration tests.
* Reviewed all incoming IDS alerts and document all identified problems. Monitor for Data Loss Prevention (DLP) using Symantec.
* Monitor, Analyze and respond to security incidents in the infrastructure. Investigate and resolve any security issues found in the infrastructure according to the security standards and procedures.
* Actively search for potential security issues and security gaps that are beyond the ability of detection by any security scanner tool. Initiate and develop new mechanisms to addresses unidentified security holes & challenges.
* Analyze risks and vulnerabilities of the network and propose solutions.
* Established security policies for systems, designed and managed secure networks for clients.
* Risk assessment on the application by identifying the issues and prioritizing the issues based on risk level.

**Education Details**

**Master’s in Computer Information Systems, New England College, NH.**

**Bachelor’s in Information technology, Osmania University, India.**