DEEPIKA CHICKMAGALUR RAMESH

1644 Parkview Green Circle San Jose CA 95131
crdeepika2@gmail.com | www.linkedin.com/in/deepika-ramesh | 619-993-4936

EDUCATION:

National University, San Diego, California — Mar 2019
Master of Science (MS), Cyber Security (Ethical Hacking & Pen Testing)

Visweswaraiah Technological University (VTU), Belgaum, India
Bachelor of Engineering, Information Science and Engineering

SANS SEC504: Hacker Tools, Techniques, Exploit and Incident Handling
Information Technology Infrastructure Library (ITIL) V3 Foundation Certified.

TECHNICAL SKILLS:

Tools	DarkTrace, Carbon Black, Recorded Future, Kenna Security, Black duck binary analysis, Qualys, Metasploit, Wireshark, Nmap, TCPdump, Burpsuite, Wildfire, Security Onion, Shodan, Maltego, Social Engineering Toolkit (SET), Docker, Exabeam, ServiceNow, Zerofox, Tanium, Symantec DLP, Aperture, CyberArk, Imperva, Tripwire, TrapX
Data Analysis/Monitoring tool	Splunk
Operating systems	Windows, Linux/Unix, Kali Linux, Parrot Security
Programming Languages	HTML
Bug reporting tools	Jira, Bugzilla
Ticketing tools	BMC's Remedy Tools, ServiceNow ITSM
Test management tool	IBM Rational Quality Manager

WORK EXPERIENCE:

Information Security Engineer
Client: eBay Inc, San Jose, CA — July 2019 - Present

- Was involved in investigations of information security incidents to determine impact to the environment and provide root cause analysis of the activity along with any containment, remediation and necessary escalation.
- Responded to notable events from security tooling to triage and determine if there was any malicious activity.
- Involved in analyzing attempted or successful efforts to compromise systems or data. This included exfiltration, malware, phishing emails, network attacks, reconnaissance or abuse of policies.
- Hands on experience with tools like Splunk, ServiceNow, DarkTrace, Carbon Black, Data Loss Prevention (DLP) through Vontu, Recorded Future and Qualys.
- Identified opportunities in automation and worked with the automation team for tuning the alerts.
- Involved in maintaining proficiency in the tools, techniques, countermeasures, and discovered vulnerabilities that would impact eBay's environment.
- Provided information and updates to shift leads, created pass-downs for the next shift, worked closely with supporting teams, provided feedback for new security policy and standards, and engaged with other teams and subsidiaries.
- Involved in researching the latest information technology (IT) security trends and performing hunting of malicious activity within the network.
- Involved in finding vulnerabilities during investigation in application and worked with product teams to go through the SAFE review process which involved performing SAST/DAST.
- Independently performed thorough root cause analysis of alerts that were triggered in our tools, documented the findings and created tickets for false positive alerts.
- Involved in digital forensics for various cases and collected evidence in a forensically sound manner. Consulted with HR and legal subject matter experts to adhere to local country law and regulations as necessary.
- Managed Internal Phishing Campaign at eBay to educate users on how to spot phishing emails and raise awareness. Reported on the program results to company leadership and also identified targeted phishing campaigns and escalated to the communication team to notify customers/employees.
- Involved in creating and updating standard operating procedures (SOP) for alerting.
- Involved in contributing for our department's V2MOM (Vision,Values, Methods, Obstacles and Measures) to outline our initiatives that would align with our future goals in influencing the information security across all the teams at eBay.
- Involved in providing evidence for PCI audits regarding the incidents, Procedures, Logs etc.
- Assisted in training new hires on how to approach alerts, analyze, triage and document.

- Helped create and deliver presentations to leadership and other teams within eBay regarding my team's project work and various findings from incidents. In addition, implemented feedback from leadership for these projects.

Cybersecurity Engineer Intern May 2019 - July 2019
Company: Varian Medical Systems, San Jose, CA
- Involved in Identification of Vulnerabilities in Varian's 3rd party components, management and prioritization of the identified vulnerabilities.
- Involved in Vulnerability scans, review of results, re-formatting of vulnerability data and updating additional information to vulnerability entries.
- Hands on experience on vulnerability management tools like Kenna Security, Black Duck Binary Analysis and custom tools.
- Involved in end-to-end documentation of vulnerability management.

Cybersecurity Researcher April 2019 - May 2019
Company: Space Science Corporation, San Diego, CA
- Developed proposal for cybersecurity applications.
- Proposed security controls and measures for the cybersecurity applications.

Security Engineer: Red Team Assessment December 2018 - February 2019
Company: 227 InfoSec, Inc, San Diego, CA
Client: Confidential
- Conducted a full black box Pen test (Penetration testing) through a real-world simulated attack and provided actionable recommendations.
- Documented Statement of Work (SOW) and testing was conducted in accordance with (IAW) the agreed test scope and Rules of Engagement (RoE).
- Used the NIST and ITIL frameworks.
- Identified exploitable vulnerabilities that could be executed by attackers with limited knowledge by focusing on known vulnerabilities with readily available exploits that represent a high likelihood of exposure.
- Test activities included port and service identification, system fingerprinting, enumeration, vulnerability scanning, exploitation and remediation, security configuration review, DOS attack and password cracking.
- Worked on Amazon Web Services (AWS) to setup phishing attacks using tool Gophish and performed USB Drop.
- Performed Vulnerability Assessment on external facing servers.
- Documented Common Vulnerabilities and Exposures (CVE's), created reports, risk register detailing assessment findings and mitigation.

UNIVERSITY PROJECTS:

Man-in-the-Middle (MITM) Attack using Wi-Fi Pineapple, National University, San Diego, CA
- Demonstrated the usage of Wi-Fi Pineapple's advanced suite of wireless penetration testing tools for man-in-the-middle (MITM) attacks, conveyed that public Wi-Fi can be unsecured and the security risks involved.
- Utilized the different modules available in Wi-Fi Pineapple like DWall, Nmap, tcpdump, OnlineHashCrack, EvilPortal, etc.

Wireless Network Vulnerability and Security Solutions, National University, San Diego, CA
- Completed a project involving gaining access to a Wi-Fi connection, pre-connection attacks, post-connection attacks, penetration software and hardware tools, and the detection of intrusions.
- Performed Wi-Fi network security assessment and WEP/WPA2 password cracking using Aircrack-ng tool in Kali Linux.

Intrusion Detection System Using Snort, National University, San Diego, CA
- Performed real-time analysis of network traffic using Wireshark, prioritized and differentiated potential intrusion attempts and false alarms.
- Added rules in the Snort IDS to establish monitoring of a virtualized system to see the IDS in action.

Threat Modeling and Threat Identification tool Cb Response by Carbon Black, National University, San Diego, CA
- Threat identification and network security tool Cb Response from Carbon Black.
- Monitor activities (Incident Response) within the network and getting solutions quickly and efficiently to mitigate imminent threats and attacks, as well as the ability to determine the root cause or the point of entry of the attack.

OTHER HIGHLIGHTS

- Served as Green Team Member Volunteer at San Diego Mayor's Cup-Cyber Event, 2018.
- Good understanding of OWASP Top 10.