Daipayan Banerjee
9737 Mount Pisgah Road, Apt 1213, Silver Spring MD 20903 | daipayan@terpmail.umd.edu | +1 (206)-581-1903
www.linkedin.com/in/daipayanbanerjee1995 | https://github.com/daipayanb

EDUCATION

University of Maryland at College Park, MD **Expected May 2021**
A. James Clark School of Engineering **GPA 3.7**
Master of Engineering in Cybersecurity
Related Coursework: Hacking of C Programs and Unix Binaries, Penetration Testing, Machine Learning Techniques Applied to Cybersecurity, Network Security, Security Tools, Networks & Protocols, Reverse Engineering, Cloud Security

Maharashtra Institute of Technology, Pune, India **May 2017**
Bachelor of Engineering in Computer Engineering **First Class**

CERTIFICATIONS

Offensive Security Certified Professional **OS-101-39334**
Skills: Active Directory Attacks, Buffer Overflow Exploits, Web Application Attacks, Network Vulnerability Scanning, Antivirus Evasion, Pivoting, Metasploit, PowerShell Empire, Bash, and Python Scripting, Privilege Escalation

CompTIA Security+
Skills: Access Control, Network Security, Firewall Configuration, Cyber Forensics, Data Security, Malware Identification, Threat Detection, Cryptography, OWASP Top 10, Identity and Access Management

TECHNICAL SKILLS

Scripting/Programming Languages: Python, Java, BASH **| DevOps:** Ansible, Puppet, Saltstack, Docker, Kubernetes
Database: MySQL, Redis **| SIEM:** Splunk **| Forensics:** Volatility, FTK Imager, Autopsy
Binary Analysis & Reversing: gdb, gcc, hexdump, objdump, ltrace, strace, Immunity Debugger, Ida Pro, PEDump, PEStudio
Penetration Testing Tools Metasploit, Wireshark, Burp-suite, NMAP, wpscan, dirb, nikto, gobuster, Empire
Cloud Computing GCP GKE, Amazon EKS, AWS: VPC, NACL, IAM, Security Groups, EC2, AMI, Cloud Formation
Container Security CIS Benchmark Scanning, Kube-bench, Trivy, kube-audit, Sysdig Falco, Docker Bench, Anchore

PROFESSIONAL EXPERIENCE

Appsecco Consulting Private Limited **June - August 2020**
Security Intern(Remote) ***Python, BASH, Docker, Kubernetes, Helm Chart, GKE, Redis, Git, Hugo, Netlify***

- Trained in Attacking and Auditing Docker Containers and Kubernetes Clusters.
- Container image vulnerability scanning and Kubernetes Cluster misconfiguration testing.
- Building Content Management Systems (CMS) using Hugo.

Accenture Solutions Pvt. Ltd., Hyderabad, India **September 2017 – December 2018**
Application Development Associate(Mainframes Engineer) ***JAVA, SQL, COBOL, DB2, Remedy ITSM, Sharepoint***

- Supported(L2 and L3) highly critical mainframes-based applications for one of Germany's biggest automobile manufacturers.
- Responsible for developing stored-procedures for DB2 tables, enhancing and optimizing batch & online jobs, debugging failing components, and suggest improvements within SLA, hold discussions with other internal application owners for resolving issues and improving the interfaces.
- As a result of my quick learning and good communication skills, I was assigned with the task of leading the weekly client meetings for both the applications. Responsible for maintaining and updating application service manuals and other docs.

ACADEMIC PROJECTS

RedDelta Malware Analysis | IDA, GDB, PeDump, PEStudio, Wireshark, ProcMon, ApateDNS, x86 Assembly **December 2020**
Performed reverse engineering and analysis of the executable and the supporting 4 DLL files. Studied the different anti-debugging techniques used and then decrypting and deobfuscating the code. Performed Dynamic Analysis using a sandboxed environment.

Kubernetes CIS Benchmark Auditing | Docker, Kubernetes, kube-bench, Python, Flask, Redis **August 2020**
Developed an auditing tool for Kubernetes clusters based on CIS benchmarks using AquaSecurity's Kube-bench. The tool is packaged into a Docker Container which provides the user with a control panel to Start/End scans and displays an aggregated view of the scan results. The master Docker container deploys pods to each of the nodes running within a cluster using a DaemonSet and the worker nodes POST scan results to the master container's Flask server which is stored in a Redis datastore using ReJSON.

ANZ Cyber@ANZ Virtual Internship **May 2020**
Investigated emails and their attachments for any kind of malicious content, suspicious URLs, or Phishing attempts to gather private information. Analyzed packet captures using Wireshark and Hexeditor to identify and investigate any potential threats.

ENPM685 Pentesting Final Project | Metasploit, msfvenom, hashcat, mimikatz, Powershell scripting **December 2019**
The final project expected us to exploit vulnerabilities and gain access to the 4 VMs on the Network to retrieve the final flag. This involved attacking using Metasploit, generating encrypted payloads using msfvenom to evade antivirus installations, escalate to root privileges, pivot to other VMs on the network, and maintain persistence.

Encrypted Email Service | Python, ast, smtplib, Crypto **August 2016**
A Python application that lets users send encrypted emails and decrypt them. Users continued to use their own service providers. The email communications remained encrypted in the service provider's servers. Hybrid Encryption (RSA and AES) was implemented to encrypt the contents of the email.

Actively Participate in online CTFs such as **HackTheBox, TryHackMe, OverTheWire.**