Avigyan Mukherjee

West Lafayette, IN | P: +1 7657469944 | mukher58@purdue.edu

EDUCATION

PURDUE UNIVERSITY (ongoing) West Lafayette, IN
Master of Science in Computer Information Technology Aug 2021 - May 2023
Cumulative GPA: ongoing
Relevant Coursework: Advanced Network Security, Project Mgmt. in IT, Wireless Technology, Web Development

SRM UNIVERSITY Chennai, TN, India
Bachelor of Technology in Computer Science and Engineering Jun 2017 - Jun 2021
Cumulative GPA: 7.98/10 (85%)
Relevant Coursework: Computer Hardware and Troubleshooting Lab, Computer Networks, Database security and Privacy, Linux Administration, AI, Web Development, Programming Lab

EXPERIENCE

Alumnus Software Pvt Ltd Kolkata, WB, India
Summer IT Internship May 2019 – Jun 2019
Implemented solutions for company clients helping with ensuring QoS for Network Traffic and management of their internet traffic. Traffic was shaped as per business SLA.

SKILLS

Code: Python3, Flask, C++, Html, Js, CSS, C, Bash, Powershell, Cisco CLI | Windows, Linux
Network: Access Connectivity, Ansible, STP, OSPF, BGP, Core Routing, High Availability and Fast Convergence, IPv4, IPv6, Network Access, Cisco, Firewalls, Security, VLANS, Dot1q, Wireless Configuration
Security: Access Control (ACLs), Data Security, Firewall Config, Mobile and Network Security, Malware Identification and Analysis (Static and Dynamic), Security Configs and Policies, Kali Linux, Snort, Penetration Testing, QRadar, honeypots, IDS, ML in Security, Pfsense

https://github.com/RoughPatch1

THESIS

DYNAMIC HONEYPOT CREATION AND MANAGEMENT WITH DOCKER **ongoing**
Ongoing research project on dynamic creation of honeypots using **docker compose** to **automatically** manage the containers, in an Ubuntu host. Comparison of the **cost benefits** of implementing dynamically deployed honeypots vs deploying the same infrastructure statically using publicly available cloud services is also addressed.

CERTIFICATIONS

CCNA (CISCO) Aug 2022
Network Configuration Labs in Cisco Packet Tracer practicing OSPF, NAT, Port Security, VLSM, VLANs, LLDP, QoS, Wireless LANs and more along with **network automation tools (Ansible, Puppet, Chef)**.
Configurations deployed including but not limited to NAT, PAT, LAN Switching, Network Stacking (Ipv4 and Ipv6 together) along with Subnetting, QoS queueing of networks.

SECURITY + (COMPTIA) Jun 2022
Tested and learnt concepts related but not limited to Incident response, Firewall Configs, Rules, Group Policies, export backups, Cloud and network security, security tools, IT security frameworks, Social engineering, AAA, 802.1x, LDAP, Kerberos, VPN tunnels, ELK/Elastic Stack, Wireless

PROJECTS (Most Relevant shown)

NETWORK SCANNER Sep 2022
Created own network scanner python application that works using **scapy**. Uses the arp protocol to create layer 1 + layer 2 packets to scan for MAC addresses and shows them on a table created using prettytables module. Faster and cleaner than nmap. Future work: TCP, Port Scanner additions to this.

DYNAMIC HONEYPOT CREATION TOOL Apr 2022
Collaborated on a tool that uses **Cowrie** to log data, and **Docker** and mininet to create a **SDN environment** where attacker's actions are logged and new honeypots spin up dynamically. Reduces resources and cost by dynamically spinning up an SSH honeypot instead of having to statically maintain it constantly.

HOME LAB (UBUNTU 20.04) MINI PROJECTS:

DYNAMIC MALWARE ANALYSIS Jan 2022
Contributed to the community by using **RegShot** and **SysInternals Suite** to analyze sample malware in Windows 7, and **Flare VM** with samples taken from malware.com

ACTIVE DIRECTORY LAB Aug 2022
Created a centralized Windows AD setup with 1 Domain Controller and 2 Client [windows] in Virtualbox where attacks on AD systems can be tested. Pushed security configs from DC to Clients.

SIEM LOG ANALYSIS Jun 2022
Applied data comparison techniques with SQL to analyze sample attacks efficiently in **IBMs Qradar** community edition and created a high level technical documentation for it.

ACTIVITIES

Virtual CyberSecurity Analyst Intern Remote
Unpaid virtual internship offered through Forage by ANZ Banking Group Jun 2020 – Jul 2020
Used Wireshark to analyze network traffic and write report on the findings
Conducted qualitative assessment of Phishing emails targeted to employees and reported spam to train their AI spam filter.

Published research paper on a Novel Intrusion Detection System (undergrad thesis) ICIPN Springer 2021
Comparing SVM, ANN algorithms and proposes modes for reducing learning time for an IDS while keeping its accuracy rate up(~90%).
Proposed reduction in feature selection of IDS algorithm from 120+ to only 27 by employing feature wrapping

TryHackMe CyberDefence Labs
Windows Exploitation, Network Exploitation, Fundumentals, AD, Nessus, Yara
Server Hardening
Following the NNT-Hardened-Services Guide to harden a virtual Win 2016 Server ensuring high security meant as a **jumpbox**
Leetcode
Python3 Coding Exercises
Meme server
Learning web development and API concepts by hosting a dedicated server Sept 2022
Future work: integrating network scanner to a dedicated web app server