Paavai Aram

+44 7768049802 paavai00@gmail.com linkedin.com/paavai-aram github.com/killswitchp website

Summary

As a PNPT-certified security professional with a strong understanding of networking and information security, I am interested in offensive as well as defensive security, primarily focusing on defensive strategies while leveraging my red team experience to enhance security operations. My expertise in incident handling, malware analysis, digital forensics, SIEM operations, and threat hunting has been honed through various courses and practical labs on platforms like HackTheBox and TryHackMe. Currently, I'm pursuing a Master's in Cybersecurity Engineering alongside the HTB Certified Defensive Security Analyst (CDSA) certification to solidify my skills further.

Education

University of Warwick Coventry, United Kingdom
Master of Science in Cyber Security Engineering *October 2023 – October 2024 (Expected)*

- **Relevant Coursework:** Digital Forensics, Security Architectures, Network Defence, Information Risk Management and Governance, Cyber Security for Virtualisation Systems, Cryptosystems and Data Protection, Cyber Physical System, Enterprise Cybersecurity, Cyber Security Research Methods

Mepco Schlenk Engineering College Tamil Nadu, India
Bachelor of Engineering in Electronics and Communication Engineer (CGPA: 8.41/10) *August 2018 - May 2022*

- **Relevant Coursework:** Computer Communication Network, Cryptography and Network Security, High Speed Networks, Embedded Processor and Application, Linux Commands and Shell Programming

Certifications

HTB Certified Penetration Testing Specialist (HTB CDSA) | *HackTheBox*	October 2024
Hack The Box Pro Lab Offshore | *HackTheBox*	May 2024
Hack The Box Pro Lab Dante | *HackTheBox*	April 2024
Hack The Box Pro Lab Zephyr | *HackTheBox*	January 2024
Practical Network Penetration Tester (PNPT) | *TCM Security*	July 2023
eLearnSecurity Junior Penetration Tester (eJPT) | *eLearnSecurity*	October 2022
CCNAv7: Switching, Routing and Wireless Essentials | *Cisco Networking Academy*	March 2022

Technical Skills

Programming/Scripting Languages: Python, C, Bash, JavaScript, Assembly language Programming, Embedded C
Operating Systems: Windows, Linux
SIEM Tools: Elastic, Splunk
IDS/IPS Tools: Snort, Suricata
Malware Analysis: Floss, PEStudio, Capa, Process Monitor, Cutter, OllyDbg, x32dbg, Yara
Network Traffic Analysis and scanning Tools: Wireshark, Tcpdump, Nmap, Nessus
Forensics Tools: Autopsy, FTK, Eric Zimmerman Tool suite, Event Log explorer, Volatility, Velociraptor
Active Directory Penetration Testing: BloodHound, Responder, CrackMapExec, Impacket, Mimikatz, PowerSploit
Web Application Penetration Testing: Burp Suite, OWASP Zap, SQLmap, Wfuzz, XSSer, Gobuster
C2: Metasploit, Covenant

Experience

Cyber Security Intern September 2022 - November 2022
Verzeo

- Developed expertise in advanced encryption techniques using Python and keylogging detection through practical projects.
- Utilised SQLmap to enumerate databases and retrieve user password hashes, enhancing skills in SQL injection and database security. Acquired familiarity with automated vulnerability scanning tools like BurpSuite and Nikto.
- Documented key cybersecurity concepts including Data Privacy, Secure Coding Practices, Encryption Standards, and Cryptography.

Content Creator September 2022 - Present

Personal Blog

- Developed a Linux-themed website emulating a command-line interface, featuring detailed technical blogs on topics such as WannaCry ransomware analysis, pivoting techniques, and certification experiences. Planning to publish upcoming blogs focused on Active Directory and ADCS attacks.

Projects

Disabling Drones: Command and Control Disruption and Forensic Data Analysis

- Developed and successfully executed methodologies to disrupt the command and control channels of drones, including Deauthentication (Deauth), Man-in-the-Middle (MitM), and signal disruption techniques using Raspberry Pi, ESP32 Microcontroller, and FlipperZero. Collected evidence of disruption, such as command link failures, loss of connectivity, and forced drone landings. Conducted detailed digital forensics, analysing network capture datasets and memory forensics to identify evidences left behind by these disruptions.

Detection Engineering Lab

- Created a security operations lab containing an Ubuntu Server machine with Zeek log collection and Elastic cloud alongside a Windows 10 machine in which three different types of attacks were run. Developed rules to detect these attacks and verified their effectiveness through testing.
- Documented and validated the detections using Python and Elastic API, and the detections were hosted on GitHub and synced with our Elastic instance via GitHub action automation.

Malware Analysis Lab

- Configured a malware analysis lab with a REMnux VM and a Windows 10 machine containing various tools to analyse malware samples and study their behaviour.
- Performed static and dynamic analysis, including reverse engineering, disassembling, and deobfuscation, on various malware samples including WannaCry ransomware. Employed advanced techniques like function call tracing, string analysis, and code flow mapping to thoroughly understand the malware's behaviour. Produced a comprehensive analysis report detailing findings for WannaCry.

Digital Forensics Lab

- Built a digital forensics lab compromising of forensics workstation, victim Windows 10 machine. Launched investigations by running an atomic red team script on the victim machine, followed by the acquisition of memory and disk artefacts. Utilised KAPE for initial data triaging and carried out disk forensics which included registry analysis, execution artifacts and Master File Table (MFT) analysis.
- Conducted memory forensics using Volatility 3 and performed a comprehensive supertimeline analysis to examine the chronological sequence of events on the system.

Active Directory Lab

- Set up an Active directory home lab comprising a domain controller (Windows 2022 Server) and 3 other Windows 10 Machines.
- Practiced various active directory attacks such as LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash, pass-the-password, token impersonation, AS-REP roasting Kerberoasting, GPP attacks, Kerberos Delegation attacks and golden ticket attacks. Developed defence strategies for each and practised techniques to evade antivirus detection.

Achievements

HackTheBox and TryHackMe – Solved 30+ machines, 10+ challenges, and completed two Pro Labs (Zephyr and Dante), achieving a global rank of 527. Ranked among the top 5% in TryHackMe.
SANS BootUp CTF – Secured 15th position solving a wide range of challenges including buffer overflow, cryptography, network traffic analysis, web exploitation, file analysis, and reverse engineering.
Sheffield Siege Inter-University CTF – Represented Warwick University as a team of four, securing 1st place out of 19 teams in the Sheffield Siege Inter-University CTF organised by Sheffield Hallam University and HackTheBox. Successfully solved 12 out of 16 challenges.
Black Hat Europe Conference 2023 – Received a student scholarship to attend the Black Hat Europe Conference 2023 held at London Excel. Also won a Flipper Zero for completing a challenge.

References Available on Request