Om Venugopal

College Park, Md | LinkedIn: OmLakshmiShanthi | Mobile: 2407337512 | Email: omvg@umd.edu | Site: omvg

EDUCATION

University Of Maryland College Park, MD

M. Eng Cybersecurity *Graduation Date: May 2023*

- Teaching Assistant: Network Security Jan 2023 - Present
- Grader: Network & Protocols August 2022- Dec 2022
- Relevant Coursework: Network Security, Network Protocols (TCP/IP), Cloud Security, Security Tools for Information Security, Penetration Testing, Secure Operating System, Digital Forensics, and Incidence Response.

PSG College of Arts & Science Coimbatore, India

B.Sc. Computer Science *March 2020*

- Relevant Coursework: Cryptography, Information Security, Database Systems, Computer Networks

SKILLS & INTERESTS

Programming Languages: Bash, Python, C++, C#, PHP, JavaScript, MySQL
Operating Systems: Windows, Kali Linux, Parrot OS, Ubuntu, Mac OS
Tools & Technologies: Wireshark, SIEM, Orca Security, CrowdStrike, Autopsy, MITRE ATT&CK matrix, Git, MS Office, Nmap, Metasploit, Burp Suite, theHarvester, Antigena (Dark Trace), AWS, Azure Active Directory, TCP/IP stack, DHCP, DNS, VLANs, Routers, Firewalls, PCIDSS, Go Phish, SonarQube, OpenSSL, Splunk

WORK EXPERIENCE

The New York Public Library Manhattan, NY

Cybersecurity Intern *June 2022 – August 2022*

- Performed intricate network analysis, scanning 40+ endpoints; identified & mitigated dormant vulnerabilities saving up to 40-man hours of work per week.
- Conducted penetration & forensic investigations to validate 40+ servers with proprietary software and meet compliance objectives, reducing security threats by 12%.
- Drafted policies to meet industry and regulatory compliance standards, such as PCI DSS and HIPAA.

PROJECTS

Home Lab | Kali Linux, Parrot OS, VMware Present

- Setting up and maintaining a home lab environment for security testing, network analysis, web application and penetration testing techniques, using Metasploit, Nessus, and Nmap for exploiting vulnerabilities.
- Regularly conduct Threat Hunting activities and analyzing malware samples using Malware sandbox technologies as a part of proactive threat management to mitigate potential security threats.
- Utilizing Threat Intelligence Platforms (TIP) to stay informed of emerging cyber threats and use Incident Response tools, and process to effectively manage and contain security incidents, minimizing damage to critical data.

Forensic Investigation | Parrot OS, Wireshark, Autopsy, SIFT **December 2022**

- Conducted digital forensic investigations using tools: SIFT, Wireshark and Autopsy for network traffic analysis and digital evidence acquisition.
- Identified and extracted key evidence from various digital artifacts, including system logs, file system structures, application data while analyzing malware traffic and identifying indicators of compromise (IOCs).
- Developed and implemented effective investigation plans with digital forensics best practices, including chain of custody, preservation of evidence, and documentation of findings.

Penetration Test | Metasploit, Nmap, JohnTheRipper **December 2021**

- Used Nmap for reconnaissance, MSI 7-010 Eternal blue in Metasploit and JohnTheRipper for privilege escalation, and Metasploit for Living-Off-the-Land.
- Actively utilized tools and techniques such as port scanning, vulnerability analysis, custom exploit development and privilege escalation to execute a through security assessment.

EXTRACURRICULUARS

Active member of WiCys, Graduate Women in Engineering (UMD), Cybersecurity Club (UMD)