Navaneetan Mamallan

(780) 716-2711 | mr.navaneetan@gmail.com | Linkedin | Tryhackme Profile

EDUCATION

University of Alberta **Sep 2025 - Present**

Master of Science, Internetworking

- **Coursework:** Internet Laboratory, Physical Layer, Data Communication Layer, The Internet Protocol Suite, Internet Applications and Programming, Internet Security

SKILLS

- **Offensive Security**: OWASP top 10, MITRE Att&ck, Android VAPT, Web VAPT, ISC2 CC
- **Programming Languages**: Python, Bash, Javascript, SQL
- **Governance, Risk and Compliance**: User Access Reviews & Entitlement Review, Security Policies, Standards & Procedures, ISO 27001, PCI DSS, GDPR, Audit Coordination & Evidence Collection
- **AI/ML Libraries**: PyTorch, TensorFlow, Hugging Face Transformers, Scikit-learn
- **Cybersecurity Concepts**: Cybersecurity Concepts, CIA Triad, Common Vulnerability Classes
- **Cloud & Identity Security**: Cloud Infrastructure, Identity And Access Management

EXPERIENCE

Mithra Consulting **Dec 2024 - Jul 2025**

Security Engineer

- Served as the dedicated Red team to small and medium businesses. Engaged with clients, understood the VAPT scope requirements, planned and executed the VAPT programs.
- Discovered critical privilege escalation flaws enabling unauthorized admin access, mapped vulnerabilities to OWASP Top 10 categories, common vulnerability classes, and CIA triad principles for standardized risk communication, and presented findings to non-technical stakeholders with business impact analysis, accelerating security patch deployment by 40%
- Reverse-engineered Android applications using JADX-GUI to analyze source code for security flaws, conducted dynamic runtime testing to identify business logic vulnerabilities including price manipulation, authentication bypass, and insufficient authorization checks, providing developers with secure coding recommendations to prevent exploitation
- Conducted manual penetration testing using Burrow Suite (Repeater, Intruder, Sequencer) to identify and validate authentication flaws, session management weaknesses, and injection vulnerabilities across web applications.
- Developed Python and bash scripts for automated reconnaissance using tools like Katana, Nuclei, and Waybackurls to gather OSINT intelligence and enumerate attack surfaces

M2P Fintech **Apr 2024 - Aug 2024**

Risk & Infosec Intern

- Conducted phishing simulation campaigns using EC-Council Aware platform, targeting employee awareness and behavior analysis, computing phishing prone %, repeated offenders and click rates.
- Assigning awareness training and induction training to all newly on-boarding employees, retaining and revoking access through identity and access management entitlement reviews & user access reviews
- Conducted user access and entitlement reviews for 1200+ users, enforcing least privilege principles across business applications
- Automated access review workflows using Excel macros, enabling bulk email notifications to team leads for retain/revoke decisions
- Responded to client checklists, achieving high satisfaction rate of 90% on audit readiness and compliance.
- Developed a Disaster Recovery (DR) plan, enhancing system resilience. Created a Decommissioning Policy, ensuring secure and compliant removal of outdated systems.
- Supported audit and compliance efforts by gathering evidence, documenting processes, and following up on corrective actions in line with PCI DSS and ISO 27001

PROJECTS

Phishing & Awareness Simulation Report

- Modeled end-to-end phishing campaigns using Python to simulate email delivery, user segmentation, and attack scenarios, then analyzed key metrics-phish-prone percentage, report rate, and repeat offender rate-from the dataset
- Documented process flow, findings, and remediation recommendations in a structured report format, mirroring audit and compliance documentation standards

Home Lab SOC(SIEM and Logging)

- Built a home SOC lab by deploying Wazuh on a Linux VM and Windows host to collect logs and detect attack scenarios such as sudo brute force (T1110) and privilege escalation (T1068)
- Wrote bash scripts to automate log parsing and generate alerts, mapping findings to MITRE ATT&CK and documenting rules and workflows for future reference

Living off the Land (LotL)

- Used PowerShell to download a file from your ”attacker” machine without triggering the basic antivirus. Used Windows Management Instrumentation (WMI) to gather system info and mapped those attacks to the MITRE ATT&CK framework

VOLUNTEERING

Tamil Student Association UofA

Events Director

- Successfully raised funds for the club by conducting Samosa & Chai Sale and Tamil Trivia Night by arranging sponsors. Lead my team in event planning and execution.