Swetha B

https://swethab.dev/

Email : swethab@terpmail.umd.edu
Mobile: +1 (240)-604-0483

Executive Summary

OSCP-certified Security Engineer with hands-on experience executing adversary simulations against complex **Active Directory** & **multi-cloud (AWS) environments**. Proficient in emulating **advanced adversary TTPs** to bypass EDR/SIEM detections, **exploit** complex attack chains, and demonstrate critical business risk to leadership.

Professional Experience

Community Dreams Foundation — Remote, USA
Cybersecurity Analyst — *September 2025 - Present*

- Executed comprehensive penetration tests against 10+ web applications, identifying and **exploiting** critical vulnerabilities to demonstrate successful **privilege escalation** paths.
- **Exploited critical IAM and RBAC misconfigurations** to bypass Zero-Trust controls, presenting actionable reports that proved non-compliance with SOC2 principles from an attacker's perspective.
- **Automated 80% of manual reconnaissance tasks** by developing custom **Python** & **Bash** scripts, enabling 2x faster identification of high-value targets during engagements.

University of Maryland Police Department — College Park, MD, USA
Security Operations Center Analyst — *December 2024 - May 2025*

- **Validated and improved SIEM detection logic by 30%** by executing known TTPs (using **Metasploit**, PowerSploit) against a live lab to test rule effectiveness for **Active Directory** lateral movement.
- Authored adversary emulation plans based on **MITRE ATT&CK** to test SOC response and **Tines (SOAR)** playbook effectiveness, identifying and reporting gaps in automated containment.
- Collaborated with SOC analysts to hunt for **APTs**, applying an attacker's perspective to log correlation (**Active Directory**, **Wireshark**) to uncover hidden attack chains.

Wipro Technologies — Bangalore, India
Project Engineer – Cybersecurity Specialist — *July 2022 - August 2023*

- Simulated adversary activity against **AWS** cloud infrastructure (targeting **GuardDuty**, **Security Hub**) to test and validate cloud detection capabilities for the SOC.
- Conducted penetration tests on live **AWS** environments, identifying and **demonstrating the exploitability** of critical data exposure risks via misconfigured **S3** buckets and **EC2** instances.

Ignited Sparks — Visakhapatnam, India
Security Engineer — *July 2020 - December 2021*

- Executed web application penetration tests (**Burp Suite**, **Nessus**), identifying and documenting complex exploit chains for vulnerabilities like SQLi and XSS.
- Conducted post-breach analysis from an offensive perspective, **re-creating attacker exploit chains** to identify failed security controls and gaps in WAF/IDS rule configurations.
- **Executed penetration tests based on ISO 27001 & PCI-DSS** control families, demonstrating the real-world exploitability of theoretical access control gaps.

Certifications

OSCP(PEN-200)OSID: 57183028: Expertise in Active Directory, Red Teaming *September 2025*

AWS Cloud Solutions Architect: Proficient in designing and deploying secure, scalable AWS cloud architectures. *July 2024*

CompTIA Security+ (SY0-701): Strong foundation in risk management, & threat mitigation strategies. *June 2024*

INE Junior Penetration Tester(eJPTv2): Proficient in vulnerability assessment and penetration testing. *December 2024*

AWS Cloud Practitioner: Solid understanding of AWS core services & foundational architecture principles. *March 2023*

Skills

Offensive Operations & TTPs: Red Teaming, Adversary Simulation, MITRE ATT&CK Framework, Bypassing EDR/AV

Offensive Security Tools: Metasploit, Covenant, Burp Suite, BloodHound, Nmap, Impacket Suite, SharpSploit, EvilGinx

Active Directory Attacks: Kerberoasting, AS-REP Roasting, Pass-the-Hash/Ticket, Lateral Movement, GPO Abuse, Mimikatz

Cloud Security: Security Hub, GuardDuty, AWS Lambda, Athena, Macie, IAM, S3, EC2

Network Security: TCP/IP, DNS, HTTPS, IDS/IPS, VPNs, Palo Alto Firewalls, Cisco ASA, Network Monitoring.

Programming Languages Python, GoLang, Bash, SQL, KQL(Kusto Query Language)

Security Research & Projects

Red Team AD Attack & Defense Lab Engineered a multi-domain **Active Directory** forest to execute a full attack chain, from initial compromise to Domain Admin, using **Kerberoasting**, GPO abuse, and **Mimikatz**. Presented findings on how to **bypass SIEM/EDR detections** for these specific TTPs. *Tech Stack: Active Directory, Metasploit, BloodHound, Mimikatz, Covenant, Windows, Kali Linux.*

Red Team AD Attack Simulation for Blue Team Defense: Executed a red-team simulation in a 3-tier Active Directory lab to identify SOC detection gaps, successfully compromising a **domain controller** by chaining exploits **(Metasploit, Nmap)** and **escalating privileges**. Presented actionable recommendations to the blue team, resulting in improved **SIEM** alerting and **log correlation** for lateral movement. **Tech Stack: Active Directory, Metasploit, Nmap, Windows, Linux, SIEM.**

Education

University of Maryland — College Park
Master of Engineering in Cybersecurity — *August 2023 - May 2025*

Key Courses: *Security tools for Incident Response, Penetration Testing, Cloud Security, Network Security.*