Arpit Deosthale

Penetration tester

Address: Sant Tukaram Nagar , Pimpri , Pune
Phone: 7219268027
Email: arpitdeosthale12@gmail.com
Website(s): LinkedIn : https://www.linkedin.com/in/arpit-deosthale-64b153275/
GitHub : https://github.com/Arpit483

Summary

Aspiring Penetration Tester with hands-on experience from personal projects, labs, and CTFs, skilled in vulnerability assessment, network scanning, and web application testing. Passionate about attacking and understanding Active Directory environments. Strong communicator who enjoys breaking down technical findings for both technical and non-technical audiences.

Projects

🔍 ***Personal Hacking Lab & VM Setup***
Set up a personal penetration testing lab using VirtualBox and Kali Linux to simulate real-world attack scenarios. Regularly practice privilege escalation, Active Directory attacks, and post-exploitation techniques in an isolated environment.

📊 ***SIEM Deployment – Splunk***
*Deployed and configured **Splunk** on a local server to monitor simulated attacks and analyze log data. Used it to build dashboards and detect abnormal behavior patterns — gaining practical knowledge of log correlation and incident detection.*

🧠 ***TryHackMe Labs***
*Completed over **80 days of consecutive hacking streak** on TryHackMe, solving a variety of rooms covering **network enumeration, web exploitation, privilege escalation, cryptography, and Active Directory**.*

*Also successfully completed **Advent of Cyber 2024**, deepening understanding of blue teaming and real-world attack chains.*

🎯 CTF Experience – Mumbai's Largest CTF (2024)
*Participated in Mumbai's largest Capture The Flag event with over 1000+ participants and a ₹5 lakh prize pool. Achieved a **rank of 126**, working in a team under high-pressure conditions and solving challenges across web, forensics, crypto, and reverse engineering.*

Skills & tools

Technical Skills & Tools

- ***Burp Suite:** Proficient in using Burp Suite for manual and automated web application testing — including intercepting requests, performing active scans, and analyzing vulnerabilities aligned with the OWASP Top 10.*

- ***Penetration Testing Tools:** Hands-on experience with industry-standard tools such as **Nmap** (including NSE scripts for service-specific enumeration), **Metasploit** for exploit development and post-exploitation, **Wireshark** for traffic analysis, and **SQLMap** for identifying and exploiting SQL injection vulnerabilities. Completed **OverTheWire's Bandit Wargame**, building a strong foundation in Linux and basic exploitation techniques.*

- ***Scripting & Automation:** Basic to intermediate proficiency in **Python**, used for scripting custom enumeration tools, payload automation, and parsing scan results. Currently improving skills through real-world lab exercises.*

- ***Programming Languages:** Strong foundation in **Java** and **C++**, enabling a deeper understanding of software behavior, memory management, and vulnerability analysis (e.g., buffer overflows and insecure code patterns).*

- ***Android & Web Development:** Knowledge of **Android app development** (Java-based) and **basic web technologies** (HTML, JavaScript, PHP). Helps in understanding the attack surface of mobile and web applications, reverse engineering APKs, and identifying client-side security flaws.Actively learning about **XSS**, **SQL injection**, and other common web vulnerabilities through hands-on labs and writeups.*

Certifications

1. **CyberStorm 2025 (Google Developer Groups, SIES Graduate School of Technology)**
2. **Cybersecurity Job Simulation (Forage, Mastercard)**
3. **ESF - IIT Madras Workshop (CyStar, IIT Madras)**

Education

Bachelor of Engineering (B.E.) in Computer Engineering:

Dr. D.Y. Patil Institute of Engineering, Management and Research, Pimpri, Pune

Currently Pursuing