Swar Rakesh Shah

| swar7233@gmail.com | https://www.linkedin.com/in/swar-shah-65053713a/ | OSCP | CRTP | (519)-872-1761

With over 4 years as a Security Consultant and Penetration Tester, I hold OSCP and CRTP certifications. Proficient in networking, I specialize in identifying vulnerabilities in web applications, Active Directory, Infrastructure Security, API systems, and network services. Well-versed in NIST, ISO 27001, Cyber Kill Chain, and MITRE ATTACK Framework, I excel in fortifying digital landscapes. Eager to contribute my expertise to enhance cybersecurity in a dynamic environment

Experience

Triage Security Analyst- Contract | Yahoo (Paranoids) | July 2024 - PRESENT

- Evaluate valid vulnerability submission received from security researchers. Assess incoming Bug Bounty submissions and reproduce reports to confirm validity.
- Collaborate with product teams to review and process external reports. Leverage Jira to track project efforts.
- Perform vulnerability scan, analysis, validation and remediation activities and network and application penetration testing.
- Research and assess new threats, vulnerability security trends and security alerts, recommend remedial action.
- Cultivate report metadata to ensure accuracy of metrics reporting. Collaborate with product teams to review and process external reports

Penetration Tester | Sun Life | April 2024 - PRESENT

- Perform Vulnerability Assessment on Web, API and network application build in diverse technologies also suggest remediation for the submitted vulnerabilities.
- Also perform Mobile Security on Android and iOS Penetration testing. Rate the vulnerability according the CVSS methodology.
- Perform Red teaming activates and also build custom tools using (C, python, Bash) languages.
- Cover OWASP top 10, SANS Application Security guide for the Penetration testing at the application.
- Good hands on opensource tools and perform source code reviews.

Security Consultant | SecureLayer7 May 2020 – August 2022

- Working as a security consultant includes vulnerability report writing, showcasing proof-of-concepts, explaining the attack in depth to customer, and recommending fixes.
- Technical Competency in Networking (common protocols, server/client infrastructure, routers, switches, WAPs), Authentication, Perimeter (IDS, IPS, UTM, WAF) and Firewall Security.
- Experienced to perform multiple onsite projects where I was responsible for internal security audit in the network infrastructure, Web applications, APIs and performed pentest in the SDLC process. Then presented to the client through vulnerability reports and presentations.
- . Perform Vulnerability assessment on Web, Mobile, API, Network and Thick client Application.

Certification

CRTP | Dec 2023

- Verify - https://www.credential.net/ef301801-22ec-4e5f-b554-0fb8d97c246c
- Active Directory | Enumeration | Local Privilege Escalation | Bypassing Advanced Threat Analytics and Deception | Lateral Movement | Domain Privilege Escalation and Persistence | Monitoring and Bypassing

OSCP | Dec 2020 

- Verify - https://www.credly.com/badges/05e539be-340b-4925-bdacf599191d1014?source=linked_in_profile
- Report Writing for Penetration Testers | Information Gathering | Vulnerability Scanning | Common Web Application Attacks| Client-Side Attacks | Locating Public Exploits | Fixing Exploits | Antivirus Evasion | Password Attacks | Windows Privilege Escalation | Linux Privilege Escalation | PowerShell | Bash | Python

Skills & Abilities

Network Penetration Testing

- Network Pentesting, Red team activities, Pivoting, Lateral movement, Familiar with Active Directory Assessments. Foot printing, Network Mapping, Routers, Switches, Kerberos Authentication, Local and remote exploits.
- Using METASPLOIT for Compiling and Changing various payloads.
- Using Nessus, Wireshark, BloodHound, Mimikatz, Firewall, IDS
- Solid understanding of Unix, Linux, and Windows server configurations, networking systems, application architecture, and secure coding techniques.

Mobile Penetration Testing

- Able to assess android app build in java, kotlin, react and flutter. Static application testing/Extracting and reviewing source code.
- Ability to find artifacts, identify intruder techniques, and determine the root causes of an incident.
- Reverse engineering the application to bypass security controls to maintain endpoint security.
- Functional Testing, Authorization and Authentication testing, Broken/Weak Cryptography, Server-Side Controls, Deep link exploitation, Web view vulnerabilities

Web Application Assessment

- API Testing - JSON/XML/SOAP/REST/GRAPHQL. Source Code - .net Application, Java Application.
- Client-Side Vulnerabilities - XSS, CSRF, JavaScript exploitation, Cache exploitation and different browser vulnerabilities.
- Server-Side Vulnerabilities - RCE, Privilege escalation, Server-side request forgery, Command Injection, SQLi, Business logical flaws, PII disclosures.
- Functional Testing, Memory Leakage Testing, Authentication Testing, Session Management, Data Validation Testing, Finding logical business flaws.

Education

Offensive Cyber Security | May 2023 - Dec 2023 | York University |

INFORMATION SECURITY MANAGEMENT | Sept 2022 - April 2023 | FANSHAWE COLLEGE | 3.4 GPA

BACHELOR OF COMPUTER ENGINEERING | May 2020 | Parul University, INDIA | 3.3 GPA