Resume of: Michael Mancuso

SECURITY CLEARANCE: Active Top Secret – SCI Security Clearance

QUALIFICATION SUMMARY:

Operational experience performing external and internal ethical hacking assessments of computer network defenses, threat modeling and vulnerability exposure evaluations mitigating technical and non-technical security gaps within a wide range of environments. Closely follow APT and cybercriminal techniques, tactics, and procedures, within customer approved ethical hacking and penetration testing. In-depth knowledge of scripting languages including but not limited to Bash, Python, and PowerShell. Understanding of web frameworks like JavaScript, ASP.NET and PHP.

Experience testing web applications for common security vulnerabilities as referenced by OWASP, including but not limited to, input validation vulnerabilities, broken access controls, sessions management misconfigurations, cross-site issues, SQL injection and web server misconfigurations.

WORK EXPERIENCE

Senior Penetration Tester, Inovalon Healthcare Data Provider (Nov 2022 Current)

- Employ a wide range of security testing tools, including Burp Suite, Postman, and SQL map, for Software Composition Analysis (SCA), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and SQLi pen testing to fortify application security.
- Conduct in-depth web application security assessments, utilizing exploit vulnerabilities such as SQL injection, cross-site scripting (XSS), parameter manipulation, and session hijacking in both cloud and containerized applications.
- Conduct in-depth Red Team testing to identify flaws in authentication and authorization mechanisms, including privilege escalation vulnerabilities with tools like Mimikatz for credential harvesting, BloodHound, Rubeus, and ADRecon for AD analysis post-exploitation.
- Developed custom scripts and payloads available on my GitHub to identify security issues that automated scanners typically miss. This includes crafting payloads for specific vulnerability scenarios like file uploads, Log4j, PHP, WordPress for testing custom attack scenarios.
- Spearhead the integration of secure Software Development Lifecycle (SDLC) principles throughout application development, incorporating robust security testing at every stage.
- Apply industry-leading AWS security practices to penetration testing, utilizing modern tools like PACU, Awspx, and BBOT to execute meticulous cloud vulnerability assessments on IT virtual infrastructure, applications, and associated assets, actively mitigating identified security risks.

Penetration Tester II, Texas Comptroller of Public Accounts (11/19-10/22)

- Provide in-depth pen testing assessments for State of Texas environments ranging from traditional on prem windows server vs open stack driven environments to AWS cloud hosted

infrastructure.

- Replicate tactics and techniques used by modern attackers, common network exploitation and penetration testing while providing expert advice with technical and executive-level reports in order to assist in remediating vulnerabilities.
- Creation and launch of a new pentesting program for a large state agency from startup to include program approved process methodology, startup documentation, scoping guidelines, and rules of engagement and charter creation.
- Built out new pen testing platform within AWS infrastructure to support multiple pen testers with custom AMI's and rolling upgrades of Kali Linux and BurpSuite on AWS.
- Replicate tactics and indicators of attack from advanced remote actors during external web application penetration testing and internal windows domain assessments of internal controls.
- Quarterly internal Active Directory red team security evaluations of our windows internal domain ranging from account management, PowerShell posture, while finding paths of privilege escalation using tools like ADRecon Bloodhound, Purple Knight, and Responder.

Penetration Tester, Delta Risk LLC (02/16 – 11/19)

- Conduct Whitebox/Blackbox web application and network-based penetration testing within client-approved rules of engagement ensuring FISMA and NIST 800 series standards, techniques, guidelines, and methods are met.
- Extensive knowledge and use of mainstream assessment tools which include Metasploit, Nmap, BurpSuite Pro, and PowerShell Empire, Star killer and Cobalt Strike frameworks.
- Provide penetration testing assessment reports, recommended security fixes, elaborate on findings, and make recommendations for customers on premise and cloud infrastructure cybersecurity issues.
- Proactively identify and apply opportunities for continuous process improvement, including application of industry best practices and methodology/reporting process automation in assigned tasks.
- Developed personal OSINT methodology and reconnaissance using tools like AMASS, Certificate Transparency logs, and discover/recon-ng to name a few.
- Conduct security hardening on operating systems/services/applications to bring customer assets within PCI and HIPAA Compliance.

Systems Engineer, NextGen HealthCare (06/13 – 02/16)

- Experience with packet capture and monitoring tools like Wireshark, Network Miner, and Security Onion toolsets to establish baselines and alerts for remote mid-size medical facilities.
- Previous systems and software engineering experience with medical software includes installing, customizing, troubleshooting, and securing medical apps to HIPAA compliance.
- The range of medical applications included Ambulatory Solutions, EHR, Laboratory, Healthcare Information Exchange interoperability, Clinical applications, Population Health, and Medical

Auditing applications.

- Experienced Systems Administrator of Windows SQL and Linux Postgres servers. Configured custom NextGen remote apps using Windows Terminal Services Remote App. Executed performance testing of multiple NextGen applications and databases.
- Configured and secured numerous hospitals and practices with remotely secured SQL based backup solutions with data at rest and data in transit encryption ensuring backups are HIPAA compliant.

Network Support, Computer Science Corporation (12/11 – 06/13)

- Technical support to provide network and server support including active directory, encryption equipment, and software installation remote support.
- Diagnose and troubleshoot network and system connectivity issues across multiple countries with computer and server systems to maintain service level agreements.

MILITARY EXPERIENCE

Cyber Operations (3D0X2) - Cyber Surety (3D0X3) Air Force / Texas Air National Guard
(10/2008 to 10/2015)

Honorable Discharge, SrA/E-4, Top Secret Clearance

- Member of the 221st Combat Communications Squadron. Duties included McAfee ePolicy Orchestrator, Linux firewalls, Blue Coat Proxys, and NetApp storage. Installation, configuration, and administration of Microsoft Exchange, VMware vCenter and ESXi servers. Experience with deploying Cisco routers and switches and encryption devices with associated key management.
- Installation, configuration, and administration of fully functional deployed networks consisting of Top Secret, Secret, and Unclassified data within 48 hours of theater arrival.

EDUCATION

Dallas Baptist University, Dallas, Tx

- Bachelor of Business Administration (September 2001 to August 2006)

CERTIFICATIONS

- EC-Council Certified Security Analyst: Penetration Testing (ECSA)
- CEH (Certified Ethical Hacker)
- AWS Certified Solutions Architect – Associate
- Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- Certified Linux Administrator (LPIC-1)
- VMware Certified Advanced Professional 6.5 - Data Center Virtualization