

Matthew Andreko

Senior Red Teamer and Penetration Tester

Smart-working and focused security consultant and software developer with 19+ years of experience in Information Technology (IT) providing security services and developing custom applications. Patient and persistent problem solver; excels in supporting and overcoming challenges in complex situations. Quickly masters new technologies and consistently strives to broaden skill set and expand capabilities.

Experience

06.2015 - present **Senior Red Team Consultant**

Accenture (Formerly FusionX)

Perform red-team attack simulations against external customers networks. Maintain persistence on internal networks for goal-oriented results, providing value by identifying detailed attack chains that could be utilized by real attackers. Complete in-depth research and development, establishing new approaches to an ever-changing attack landscape.

- Utilize new techniques to identify and exploit vulnerabilities in customer networks.
- Develop custom command and control (C2) software and other tools to aid in team projects and prevent detection.
- Create comprehensive and accurate reports and presentations for both technical and executive audiences.

09.2012 - 06.2015 **Security Consultant**

Optiv (Formerly Accuvant)

Perform onsite and remote security consulting including penetration testing, vulnerability assessment, web application security assessment, internal and external security assessment, social engineering, and wireless assessment.

- Generate and present technical and executive level reports on security vulnerabilities to external customers.
- Develop custom tools for security testing and workflow management to aid and expedite projects and the work of other consultants.
- Provide tools and mediums to aid in communication between remote consultants.

07.2011 - 09.2012 **Senior Software Analyst**

Leaf Software Solutions

Develop web-based management software for automotive dealer services.

- Refactor and clean a large portion of the codebase to upgrade from .NET 2.0 to 4.0, utilizing Linq, generating the same functionality with fewer lines of code as well as being more easily readable.
- Undertake research assignments for the next generation of the software. Main topics include build/deployment, NoSQL database storage, and best-practice development patterns and standards.
- Identify security weaknesses in the current code-base. Provide demonstration of how malicious actors could cause data loss or cause harm to the company.

06.2010 - 07.2011 **Software Developer III**

Autobase/Dominion Dealer Solutions

Develop web-based automotive CRM software to replace existing client-server software.

- Participate in an Agile SCRUM product lifecycle, utilizing an extreme

Personal Info

Address

10367 N State Road 39
Lizton, IN 46149

Phone

317.331.9089

E-mail

matt@andreko.net

GitHub

github.com/mandreko

WWW

www.mattandreko.com

LinkedIn

linkedin.com/in/mattandreko/

Skills and Tools

OSINT

Attack Simulation

Penetration Testing

Social Engineering

Mentoring

Meming

Software

Metasploit

Cobalt Strike

Burp Suite

Linux (Various Distributions)

Microsoft Windows (NT4 to current)

Source Control (Git, SVN, etc)

Programming Languages

C#, ASP.net

JavaScript (Node, jQuery, React, Angular, etc)

PowerShell

Python

Ruby

C/C++

SQL (MySQL, Microsoft SQL Server, PostgreSQL, etc)

programming model, pairing developers to analyze business requirements given by analysts to implement solutions.

- Lead the initiative to switch from SVN to Git, providing guidance and training to the team.
- Work with outside vendors to understand and implement web-based solutions for scanning driver licenses and other cards from a web-based interface.

04.2007 - Software Developer

05.2010 *Key Benefit Administrators*

Develop in-house applications based on a set of specifications provided by a team lead. Work with several team members to provide stable and scalable services. Provide custom reports on a day-to-day basis.

- Develop and maintain a service that would distribute agent and vendor commissions based on a complex set of rules, handling cash advances, and several other advanced features. Responsible for running monthly, verifying data to finance department and creating custom reports from Microsoft SQL 2008 and Active Reports.
- Manage SVN repositories, including advanced branching and merging scenarios to aid in development amongst multiple team members.
- Train new team members and contractors to learn and use the existing code-bases for various web applications.

08.1999 - Software Developer / System Administrator

04.2007 *On-Ramp Indiana*

Provide technical expertise for a multitude of tasks, including developing custom software, customer support, and network engineering in a team-oriented environment. Delivery of superior service to customers, fielding diagnosing, troubleshooting, and resolving complex and/or unusual support calls.

Instrumental in training new staff.

- Configure and support Cisco network devices on a complex network, providing segmentation from customer and company assets. Harden Microsoft Windows server infrastructure in accord with baselines such as CIS benchmarks.
- Develop several custom applications, integrating into various internal services such as Vircom Modusmail Server, WebTrends, Microsoft IIS, and Microsoft DNS Server to provide automation to previously manual tasks.
- Reverse-engineered Vircom Modusmail to identify a weakness in their webmail interface, allowing an attacker to decode plain-text cookie values to hijack user sessions.

Education

2002 - IUPUI
2004 Computer Technology with minor in Electrical Engineering

Certifications

06.2012 Offensive Security Certified Professional (OSCP)
04.2013 Offensive Security Certified Expert (OSCE)