# David Tomaschik

@ david.tomaschik@gmail.com
Security Engineer/Vulnerability Researcher • OSCP • OSCE

## Education

### GEORGIA STATE UNIVERSITY

BS, Computer Science

Aug 2005 — Atlanta, GA

- Undergraduate Research Award
- Minor in International Relations

## Links

Blog
**https://systemoverlord.com**
GitHub **Matir**
Linkedin **davidtomaschik**

## Coursework

### INDUSTRY TRAININGS

- Penetration Testing with Kali Linux
- Cracking the Perimeter
- Reverse Engineering with Ghidra
- Mastering Burp Suite Pro
- Binary Fuzzing & Dynamic Instrumentation
- Applied Physical Attacks

### UNIVERSITY

- Embedded Systems
- Network Security
- Electronics

## Skills

### SECURITY

Web Security • Embedded/IoT • Code Review • Red Teaming • Fuzzing

### PROGRAMMING

Python • C/C++ • Go

### TOOLS

Burp Suite • Metasploit • Ghidra • Sliver • mitmproxy • Ansible • Kubernetes • nmap

## Vulnerability Research

### SELECTED VULNERABILITIES

- 6 Vulnerabilities in Linksys Range Extenders
- CVE-2019-10071 (Apache Tapestry)
- CVE-2017-17704 (iStar Access Control Systems)
- CVE-2014-5204, CVE-2014-4182, CVE-2014-4183 (Wordpress)

## Experience

### SENIOR SECURITY ENGINEER, OFFENSIVE SECURITY

Google

May 2016 - Present — Mountain View, CA

- **Tech Lead** for our Offensive Security/Red Team Program.
- Design, lead, and execute **Red Team Exercises** covering Google and the broader Alphabet enterprise.
- Identify and exploit vulnerabilities and security weaknesses to test detection & response capabilities as well as highlight issues with business leadership.
- Develop **Red Team Tooling**, including exploit kits, remote access toolkits, and phishing kits for use in Red Team Exercises.
- Regularly present to executive leadership at the VP and SVP level.
- Work with teams to remediate findings and improve security controls and security detection systems.
- Provide Training & Development opportunities to team members and organize knowledge sharing sessions.
- Develop team documentation for exercise processes, rules of engagement, and use of our internal/custom tooling.
- Managed **5 interns**, 3 of which converted to full-time engineers.

### SECURITY ENGINEER, SECURITY ASSESSMENTS

Google

Oct 2013 - May 2016 — Mountain View, CA

- Performed a variety of security assessments and **penetration tests**.
- Worked with 3rd parties to resolve security issues.
- Performed **source code review** of Google products and services to identify vulnerabilities and implement source hardening.
- Offered training on **web security** and **attacker mindset** to engineers across the company.
- Developed internal tooling to help streamline security review process and identify vulnerabilities in an automated fashion.

### SITE RELIABILITY ENGINEER

Google

Feb 2012 - Oct 2013 — Mountain View, CA

- Worked to scale and secure the Google Ads processing pipelines.
- Refactored monitoring for revenue-critical services.
- Developed tooling in Python to automatically scale processing based on load.
- Automated process for production failovers using Paxos-based master election.

### SYSTEMS SUPPORT ENGINEER V

Kennesaw State University

Feb 2009 – Feb 2012 — Kennesaw, GA

- Responsible for systems administration and security tasks for a fleet of Linux and MacOS servers.
- Developed custom software for academic and business needs using PHP and C, including integrations with the Drupal CMS.
- Implemented configuration management and security best practices, including Puppet, centralized authentication, and PKI for servers and applications.

## Selected Projects & Presentations

### BSIDES SAN FRANCISCO CTF

CTF Organizer

2016 - Present | San Francisco, CA

Helped to organize BSidesSF CTF for 6 years straight, including managing infrastructure, developing challenges, and player interactions.

### THE IOT HACKERS TOOLKIT

BSides San Francisco

2018 | San Francisco, CA

I presented the basics of investigating IoT devices for security vulnerabilities, covering a range of basic tools, their use cases, and the general approach I take towards IoT Security Assessment.

### I'M THE ONE WHO DOESN'T KNOCK: UNLOCKING DOORS FROM THE NETWORK

DEF CON 26

August 2018 | Las Vegas, NV

I covered the methodology used to discover vulnerabilities allowing an attacker to send remote door unlock commands to access control systems. I covered the approach and verification of the vulnerability. (CVE-2017-17704)

### OPEN SOURCE CONTRIBUTIONS

I've contributed to a number of open-source projects including:

- The Sliver Remote Access Toolkit (BishopFox/sliver)
- CTFd (CTFd/CTFd)
- CTFScoreboard (google/ctfscoreboard)
- The sshdog embedded SSH Server (matir/sshdog)