Tyler C. McCann

Senior Lead, Cyber Threat Emulator (OSCE³)

Fort Eisenhower, GA

tylerdotrar@gmail.com

+1 (615) 653-8876

@tylerdotrar

ABOUT

I am a hands-on individual; one who is aptitude oriented, values the ability to communicate efficiently and honestly, as well as one who thrives on self-development.

ACHIEVEMENTS

Cyber Apocalypse CTF 2023 (HackTheBox)

Team placed in the top 3% globally (245/6483).

EDUCATION

Joint Cyber Analysis Course (JCAC)

1000+ hour NSA accredited course that teaches the knowledge and skills required for offensive and defensive cyber operations.

December 2018 - June 2019

Middle Tennessee State University (MTSU)

Computer Engineering, B.S. (In-Progress)

August 2016 - May 2018

EXPERIENCE

Active Security Clearance:
TS/SCI w/ Polygraph

DoD SkillBridge Internship

SkillBridge Intern | **SIXGEN**

March 2024 - June 2024

Exploit Developer **Network Engineer**

Exploit Developer

SIXGEN

Developed proficiency in Windows User Level exploits for Intel x86 architectures and exploit crafting techniques, bypassing common security mitigations such as DEP and ALSR. Other topics covered include binary obfuscation for endpoint AV evasion.

Intel x86 | Assembly | Reverse Engineering

Network Engineer

SIXGEN

Aided in the development of both scalable and maintainable virtualized networks emulating enterprise Active Directory environments containing user emulation, enabling robust red team operator training. This extended to vulnerability implementation and validation.

Proxmox | DevOps | Active Directory

Cyber Operations Specialist (17C)

Staff Sergeant (SSG) | **U.S. Army**

August 2018 - September 2024

Cyber Threat Emulator **Senior Network Analyst** **Analytic Support Officer**

Cyber Threat Emulator

U.S. Army Cyber Protection Brigade (USACPB)

Senior lead in the unit's Cyber Threat Emulation (CTE) cell, mentoring and developing junior offensive operators while specializing in conducting custom Red and Purple Teaming exercises against the brigade's Cyber Protection Teams (CPTs), emulating Advanced Persistent Threats (APTs). Additionally, focusing on generating data analytics by virtualizing, deploying, and executing CVEs and TTPs on critical infrastructure, ranging from industrial control systems (ICS) to enterprise environments.

Penetration Testing | Active Directory | AV Evasion | Web Exploitation | SQL | DevOps

Senior Network Analyst

U.S. Army Cyber Protection Brigade (USACPB)

Senior network analyst on a U.S. European Command (USEUCOM) based Cyber Protection Team (CPT), engaging in a variety of mission types from incident response to network hardening and threat hunting. During this time, advised and assisted junior analysts during two forward operations in Europe. Gained proficiency in a multitude of technologies, including Splunk, Elastic Stack, and Endgame EDR.

Linux | Windows | Security Onion | Splunk | Elastic Stack (ELK) | ESXi | Sysmon

Analytic Support Officer

U.S. Army Cyber Protection Brigade (USACPB)

Subject Matter Expert (SME) for both detecting information gaps and generating potential analytics for priority information requirements (PIRs) for both upcoming and ongoing missions.

Data Analytics | Dashboards | Digital Forensics

SKILLS

- Intel x86
- Assembly
- DevOps
- Networking
- CI/CD
- Github Pages
- Proxmox
- ESXi
- Automation
- Scripting
- Network TAPs
- SIEM
- Dashboards
- Data Analytics
- Digital Forensics
- Security Onion
- Splunk
- Elastic Stack
- Sysmon
- Linux
- Shellcode
- ROP
- PenTesting
- Active Directory
- AV Evasion
- IEEE 802.11
- Web Exploitation
- SQL
- PrivEsc
- Reverse Shells
- XXE
- XSS
- Template Injection
- Exfiltration
- Bash
- PowerShell
- C#
- .NET
- Microsoft Office
- Windows

CERTIFICATIONS

DoD Directive 8570 Compliance:
IAT-III, CSSP Analyst, CSSP Intrastructure Support, CSSP Incident Responder, CSSP Auditor

- **OffSec Certified Expert 3 (OSCE³)** May 2024 | OffSec
- **OffSec Exploit Developer (OSED)** May 2024 | OffSec
- **OffSec Experienced Penetration Tester (OSEP)** April 2023 | OffSec
- **OffSec Certified Profession (OSCP)** March 2023 | OffSec
- **OffSec Web Expert (OSWE)** March 2024 | OffSec
- **OffSec Web Assessor (OSWA)** December 2023 | OffSec
- **OffSec Wireless Professional (OSWP)** April 2023 | OffSec
- **Red Team Apprentice Certified (RTAC)** March 2024 | k>fivefour
- **Certified Ethical Hacker (CEH)** June 2024 | EC-Council
- **GIAC Certified Enterprise Defender (GCED)** August 2020 | SANS Institute
- **OffSec Defense Analyst (OSDA)** May 2024 | OffSec

PROJECTS

RGBwiki

https://rgbwiki.com

Owner and creator of RGBwiki, a Github Pages hosted site containing an aggregate of offensive (red), DevOps/infrastructure (green), and defensive (blue) knowledge in the form of an Obsidian Vault utilizing mkdocs.

CI/CD | Github Pages | MkDocs | Documentation

Bit-Bandits

https://bit-bandits.com

Co-contributer to Bit-Bandits, a Github Pages hosted wiki dedicated to providing detailed writeups on different CVE's and attacker techniques, from infrastructure deployment to actual exploitation.

CI/CD | Github Pages | MdBook | Documentation

SigmaPotato

https://github.com/tylerdotrar/SigmaPotato

SeImpersonate privilege escalation tool for Windows 8 - 11 and Windows Server 2012 - 2022 with extensive PowerShell and .NET reflection support.

C# | .NET | Privilege Escalation

PoorMansArmory

https://github.com/tylerdotrar/PoorMansArmory

Collection of robust Windows-based payload generators and tools that aim to bypass AMSI, Windows Defender, and self-signed certificate checks. Tools range from a custom python HTTP(s) server, robust PowerShell reverse shell generator, remote template injected .docx generator, XSS and XXE PoC payloads, etc.

PowerShell | Python | Reverse Shells | XXE | XSS | Template Injection | Exfiltration

genrev

https://github.com/tylerdotrar/genrev

Modular Python tool that uses the Python keystone-engine library to convert Intel (x86) assembly instructions into Windows shellcode.

Python | Assembly | Shellcode