Tyler C. McCann

Senior Lead, Cyber Threat Emulator (Red Team)

Fort Eisenhower, GA

tylerdotrar@gmail.com

+1 (615) 653-8876

@tylerdotrar

ABOUT

I am a hands-on individual; one who is technical-prowess oriented as well as one who values the ability to communicate honestly, learn fast, and self-develop on technical subjects that are daunting at first glance.

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.

August 2016 - May 2018

EXPERIENCE

Cyber Operations Specialist (17C)

SSG, U.S. Army | Active Clearance: **TS-SCI w/ Polygraph**
DoD Directive 8570 Compliance: **IAT-III**

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 my unit's Cyber Threat Emulation (CTE) cell, where we primarily focus on Red Teaming and emulating Advanced Persistent Threats (APTs) to train the analysts within the brigade's Cyber Protection Teams (CPTs).

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

Senior Network Analyst

U.S. Army Cyber Protection Brigade (USACPB)

Senior network analyst on a European Command (EUCOM) based Cyber Protection Team (CPT), engaging in a variety of mission types from network hardening to threat hunting, while gaining familiarity with a multitude of technologies.

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

CERTIFICATIONS

- **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
- **GIAC Certified Enterprise Defender (GCED)** August 2020 | SANS Institute
- **Red Team Apprentice Certified (RTAC)** August 2020 | k>fivefour

SKILLS

- 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
- PenTesting
- Active Directory
- Antivius Evasion
- IEEE 802.11
- Web Exploitation
- SQL
- PrivEsc
- Reverse Shells
- XXE
- XSS
- Template Injection
- Exfiltration
- Bash
- PowerShell
- C#
- .NET
- Microsoft Office
- Windows

PROJECTS

RGBwiki

https://rgbwiki.com

Owner and creator of RGBwiki, a Github Pages hosted wiki 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

ProxmoxMaster

https://github.com/tylerdotrar/ProxmoxMaster

Repository of Proxmox configuration scripts and LXC service installation scripts. Functionality ranges from adding CPU thermal readings to node dashboards to automating service installs with SSL certificate support.

Proxmox | DevOps | Bash | Scripting

Activate-MicrosoftOffice

https://github.com/tylerdotrar/Activate-MicrosoftOffice

PowerShell tool to activate Microsoft Office Professional Plus 2016 - 2021 via KMS client keys.

PowerShell | Microsoft Office | Automation

tc-taps

https://github.com/tylerdotrar/tc-taps

Bash scripts utilizing 'tc' to TAP into VM and LXC network interfaces on Linux based hypervisors (specifically Proxmox) for SIEM ingestion of network traffic.

Bash | Network TAPs | SIEM