Contribution ID: **2** Type: **not specified**

# Graph Theory: Unveiling the Microsoft Entra ID Post-Exploitation Landscape

*Tuesday, 4 June 2024 10:15 (45 minutes)*

In today's cloud-driven landscape, Microsoft Azure and 365 (M365) have become essential tools for businesses worldwide. However, beneath their user-friendly facades lie a landscape rife with potential threats stemming from default configurations. Through years of attacking Microsoft cloud environments during red team engagements I have found commonalities across many companies where overlooking default settings have left them vulnerable.

Very recently I released a new post-exploitation tool for Microsoft Entra ID accounts called GraphRunner. This tool leverages the Microsoft Graph API, which is a fundamental piece of infrastructure for much of Microsoft 365 and Azure. I will demonstrate how this API can be leveraged to perform post-exploitation of a Microsoft Entra ID account to perform reconnaissance, establish persistence, escalate privileges, and ultimately pillage data from services such as SharePoint, Teams, and email.

Throughout the talk, I will present real-world examples that underscore the critical importance of proactive defense. These demonstrations will be supported by practical, hands-on showcases featuring custom-built tools crafted specifically for these targeted attack scenarios.

## Length

45 minutes

## Optional: Speaker / convener biography

Beau Bullock is a Senior Security Analyst and Penetration Tester and has been with Black Hills Information Security since 2014. Beau has a multitude of security certifications (OSCP, OSWP, GXPN, GPEN, GWAPT, GCIH, GCIA, GCFA, GSEC) and maintains his extensive skills by routinely taking training, learning as much as he can from his peers, and researching topics that he lacks knowledge in. He is a constant contributor to the infosec community by authoring open-source tools, writing blogs, frequently speaking at conferences and webcasts, and teaching his training class "Breaching the Cloud".

**Primary author:** BULLOCK, Beau (Black Hills Information Security)

**Presenter:** BULLOCK, Beau (Black Hills Information Security)

**Session Classification:** Talks and presentations

**Track Classification:** Talks and presentations